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 2016/II (Juli – Dezember)

20. APRIL 2017

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

1 Übersicht / Inhalt

2 Editorial

Philippe Vuilleumier trägt seit September 2015 als Head of Group Security die Verantwortung für die logische und physische Sicherheit bei Swisscom

Liebe Leserinnen, liebe Leser

Früher fragte sich ein Sicherheitsverantwortlicher: «Was muss ich tun, damit die Angriffe auf meine Organisation keinen Erfolg haben?» Heute stellt man etwas ernüchtert fest, dass die Frage wohl eher lautet: «Wie lange wird es dauern, bis ein Angriff erfolgreich sein wird?» Aufgrund der laufenden Professionalisierung der Angreifer, der wachsenden technischen Möglichkeiten und der damit verbundenen Perfektion vieler Angriffe, ist man in der Tat gut beraten davon auszugehen, dass die eigene Umgebung schon kompromittiert ist oder sie es zumindest bald sein wird.

Diese Tatsache zu akzeptieren, ist das eine, die richtigen Schlussfolgerungen und Massnahmen daraus zu ziehen das andere. «Assume breach», hört sich für viele zunächst revolutionär an, was folgt aber danach? Was kann eine Organisation als Ganzes und ein Sicherheitsteam als deren Speerspitze tun?

Bei Swisscom sind wir zum Schluss gekommen, dass wir drei Dinge tun müssen:

1. Unsere Basissicherheit weiterpflegen! Dazu gehört, dass wir unsere Inventare über Infrastruktur, Daten und Mitarbeitende aktuell halten, in kurzen Abständen die notwendigen Updates für unsere Systeme und Anwendungen einspielen, mit Konsequenz unsere Risiken managen und bei all diesen Tätigkeiten auf Effizienz achten.

2. Einfache Sicherheitslösungen bauen! Und zwar einfach für den Endbenutzer. Die Security leistet einen grossen Beitrag an die geforderte Agilität im Unternehmen, indem sie ihre technischen Lösungen auf Einfachheit und Transparenz trimmt.

3. Auf Detektion und Reaktion setzen! Natürlich ist die Prävention nach wie vor sehr wichtig (sie gehört in die Basissicherheit) aber aufgrund der sich ständig ändernden Angriffslandschaft stösst sie irgendwann an ihre Grenzen. Angriffe und Kompromittierungen rasch erkennen, eingrenzen und bekämpfen können, das sind wichtige Fähigkeiten, die wir laufend verbessern wollen. Gerne nenne ich hier auch MELANI als ein wichtiger und kompetenter Partner für Swisscom in diesem Bestreben.

In diesem Bericht bildet das Internet der Dinge das Schwerpunktthema. Auch vor diesem Hintergrund und den damit verknüpften Herausforderungen ergeben die drei Schwergewichte Basissicherheit, Einfachheit und Detektion Sinn.

Ich wünsche Ihnen eine interessante Lektüre.

Philippe Vuilleumier

3 Schwerpunktthema: Internet der Dinge

Alles was verbunden werden kann, wird in Zukunft auch mit dem Internet vernetzt werden. Diese zugegebenermassen etwas überspitzte Aussage deutet an, wie sich das Internet in den nächsten Jahren entwickeln und neben all den Annehmlichkeiten sicherlich auch zu zahlreichen Sicherheitsdiskussionen führen wird. Immer mehr Alltagsgegenstände werden künftig ans Internet angeschlossen. Erste Hersteller sprechen deshalb schon vom «Internet of Everything» (IoE), das Menschen, Prozesse, Geräte und Daten in ein alles umspannendes Netz einbindet. Der viel zitierte Kühlschrank, der automatisch die Milch bestellt, ist dabei ein anschauliches Beispiel. Aber es ist nur eines von vielen. Gerade im Bereich Gebäude-Management und Lichtsteuerung ist in den letzten Jahren ein Boom ausgebrochen. Das Internet der Dinge wird in Zukunft viel mehr sein, als es heute ist. Laut den Analysten von Gartner[1] hingen 2016 bereits über 6 Milliarden «Dinge» am Netz. Bis ins Jahr 2020 wird mit einer Zunahme auf über 20 Milliarden Dinge gerechnet. Und die Möglichkeiten von am Internet angeschlossenen Dingen sind noch lange nicht ausgeschöpft. Diese werden sich immer mehr in unseren Alltag einfügen und diesen auch beeinflussen. Gewisse Entwicklungen zeichnen sich bereits ab: Die sogenannten «Wearables», Anwendungen, die am Körper des Benutzers getragen oder in Kleider eingenäht werden und eine Vielzahl an Daten liefern, stecken zwar noch in den Kinderschuhen, werden aber weit über die bereits etablierten Fitness-Tracker hinausgehen. Auch im Medizinbereich ist mit einer Vielzahl an Anwendungen zu rechnen, die eine permanente und bessere Diagnostik ermöglichen werden. So ist es denkbar, dass auf dem Smartphone jederzeit der Status aller lebenswichtigen Organe abgerufen werden kann. Ein anderes zentrales Gebiet wird das der selbstfahrenden Fahrzeuge sein. Erste Versuche damit gab es bereits. Um jedoch eine reibungslose und sichere Funktionsweise garantieren zu können, sind zahlreiche Sensoren im und um das Autonotwendig. Unabhängig von der Entwicklung solcher Fahrzeuge, werden auch auf der Strasse zahlreiche Sensoren verbaut werden, um dem immer grösser werdendem Verkehrsfluss Herr zu werden. Somit ist hier die Erfassung von Daten das zentrale Thema: Autark und autonom funktionierende Sensoren, die ihre Daten übers Internet an einen Server senden, sollen in Zukunft helfen, Entscheidungen zu treffen, Aktionen auszulösen und in diesem Rahmen auch Gefahren frühzeitig zu erkennen, um diese schliesslich abwenden zu können.

3.1 Definition

Der Begriff «Internet der Dinge» bezeichnet die zunehmende Vernetzung von Alltagsgegenständen und -geräten via Internet. Das erste Mal tauchte der Begriff Ende der 90er Jahre auf und wurde vom Technologie-Pionier Kevin Ashton als eine wichtige Grundlage für den Datenaustausch zweier intelligenter Geräte verwendet.[2] Eine einheitliche Definition existiert bis heute allerdings nicht. Man kann den Begriff auch sehr weit fassen und als Synonym für die Verbindung der realen mit der virtuellen Welt verstehen.[3] Eine konkrete Umsetzung ist bei-

[1] http://www.gartner.com/newsroom/id/3598917 (Stand: 28. Februar 2017).
[2] http://www.rfidjournal.com/articles/view?4986 (Stand: 28. Februar 2017).
[3] http://www.computerwoche.de/a/industrie-4-0-ist-das-internet-der-ingenieure,2538117 (Stand: 28. Februar 2017).

spielsweise die Identifizierung gegenständlicher Objekte mittels RFID-Chips, QR- und Barcodes. Mit Hilfe eines Scanners wird eine Verbindung zum Internet hergestellt. Damit lässt sich ein simpler Gegenstand in einen intelligenten, d.h. mit Informationen und Diensten angereicherten Gegenstand verwandeln. In der Industrie benutzt man beim Einsatz von intelligenten Objekten und Sensoren häufig den Begriff Industrie 4.0 und meint dabei die vierte industrielle Revolution, welche die Digitalisierung mit sich bringt.

3.2 Das unsichere Internet der Dinge?

Mit den zunehmenden Möglichkeiten des Internets (der Dinge) werden uns auch die Risiken und Nebenwirkungen umso mehr beschäftigen. Es sollte zum Beispiel immer sichergestellt sein, dass der Kühlschrank die Milch bestellt und nicht die Milch beginnt, Kühlschränke zu bestellen. Es werden sich grundlegende Fragen stellen, die nicht nur Wartung und Sicherheitsstandards beinhalten, sondern insbesondere auch Fragen zum Datenschutz. Sinn und Zweck des Internets der Dinge ist vor allem, anhand von Sensordaten automatisierte und optimierte Entscheide zu treffen. Dementsprechend fallen Millionen von Datensätzen an, die in ihrer Gesamtheit geschützt werden müssen. Um beim vielfach zitierten Kühlschrank zu bleiben, geben die erhobenen Daten einen interessanten Einblick nicht nur bezüglich dem Milchkonsum des Haushaltes, sondern über die gesamte Kühlschranknutzung. Solche Daten können beispielsweise für Marketingzwecke verwendet werden. Im Extremfall könnte man so auch feststellen, ob das Essverhalten eines Haushalts gesund oder ungesund ist, was zum Beispiel den Krankenkassen als Indikator für die Berechnung deren Prämien dienen könnte.

Im zweiten Halbjahr 2016 sorgte das Internet der Dinge vor allem aufgrund des Botnets «Mirai» für Schlagzeilen. Eine grosse Anzahl schlecht geschützter Geräte wurde gehackt. Am 21. Oktober 2016 kam es zu einem Angriff auf den Infrastrukturanbieter «Dyn», was zum Ausfall vieler populärer Internetdienste wie Amazon, Spotify und Netflix führte. Dieser Angriff zeigte auf, weshalb die Sicherheit der am Internet der Dinge angeschlossenen Geräte nicht vernachlässigt werden darf. Die mehreren hunderttausend gehackten Geräte wurden so programmiert, dass sie gleichzeitig Verbindung mit den Servern des Angriffsziels aufnahmen. Der Angriff gehörte mit einem Datenverkehrsvolumen von 1.2 Terabit / Sekunde zu den stärksten DDoS-Angriffen, die bisher beobachtet worden waren.

Das Internet der Dinge unterscheidet sich in wesentlichen Dingen von konventioneller Informations- und Kommunikationstechnik (IKT): Im Gegensatz zu Computern sind diese internetfähigen Alltagsgeräte häufig nur beschränkt gegen unbefugten Zugriff gesichert, weshalb sie von den Angreifern mit Schadsoftware infiziert werden können. Einerseits können für den Zugriff auf diese Geräte vielfach deren Standardpasswörter ausgenutzt werden. Diese Passwörter werden nach der Installation häufig nicht geändert, respektive können gar nicht geändert werden. Andererseits ist die Aktualisierung der eingesetzten Software ein grundlegendes Problem: Der Update-Prozess ist in den wenigsten Fällen geregelt und in den seltensten Fällen automatisiert. Daraus ergeben sich zahlreiche Herausforderungen, die sich in den nächsten Jahren noch verschärfen werden: Im Gegensatz zu konventionellen IKT-

Geräten, die durchschnittlich nur einige Jahre in Betrieb sind, können Internetdinge durchaus bis zu 10 Jahre und länger im Einsatz sein.

3.3 Auswirkungen auf die Zukunft

Dass das Internet der Dinge für DDoS-Angriffe missbraucht wird, dürfte allerdings in Zukunft kaum das zentrale Risiko für die Gesellschaft werden. Ein viel grösseres Gefährdungspotential ist in der Manipulation solcher Systeme zu sehen. Besonders in der Logistikbranche erleben ans Internet angeschlossene Geräte einen Boom. Gleichzeitig können in dieser Branche aber auch die Schäden enorm sein, die durch eine Manipulation ausgelöst werden könnten. Liefert beispielsweise eine manipulierte Arzneimittellogistik die dringend benötigten Medikamente an den falschen Ort, kann dies sehr schnell zu einer Frage von Leben und Tod führen. Kriminelle könnten versuchen, mit solchen Angriffen Geld zu erpressen. Und Terroristen könnten versuchen, die Gesellschaft mit derartigen Angriffen zu verunsichern und zu destabilisieren.

Die Problematik rund um die Sicherheit beim Internet der Dinge liegt vor allem im fehlenden Sicherheitsbewusstsein der Betreiber. Der Sicherheitsexperte Lucas Lundgren hat im Rahmen der letzten RSA-Sicherheitskonferenz in San Francisco erneut auf die Problematik der schlecht geschützten «Message Queue Telemetry Transport»-Kommunikation, kurz MQTT, hingewiesen.[4] Diese wird oft verwendet, um die Kommunikation der Dinge anhand von Sensoren sicherzustellen. Das Problem ist nicht das MQTT-Protokoll an sich. Vielmehr gibt es Betreiber, die schlichtweg auf Passwortschutz und Verschlüsselung verzichten. Im Fall von batteriebetriebenen Sensoren kann man den Verzicht noch mit höherer CPU-Belastung und damit einhergehend mit der höheren Strombelastung erklären, in vielen Fällen steckt dahinter allerdings einzig Unwissenheit oder Bequemlichkeit.[5] Die ungeschützt über das Netz kommunizierenden Sensoren finden sich unter anderem in Autos, Erdbebensensoren, Geldautomaten, Klimageräten, Leuchten und Medizintechnikgeräten.

3.4 Richtlinien und Vorsichtsmassnahmen

Die diversen Einsatzmöglichkeiten des Internets der Dinge in den verschiedenen Branchen und die immense und immer schneller wachsende Zahl der verschiedenen Geräte erschweren es, Richtlinien zu erarbeiten. Dennoch hat die Organisation Cloud Security Alliance im Oktober 2016 einen gut 80-seitigen Bericht veröffentlicht.[6] Er bietet unter anderem einen Überblick über Sicherheitsfunktionen, die in den verschiedenen Software-Entwicklungsplattformen verfügbar sind. Ebenfalls finden sich im Bericht Richtlinien für den Design- und Produktionsprozess sowie eine Checkliste, die Ingenieure für den Entwicklungsprozess konsultieren können.[7] MELANI hat auf ihrer Website ebenfalls einige Mass-

---

4 https://www.rsaconference.com/events/us17/agenda/sessions/6671-lightweight-protocol-serious-equipment-critical (Stand: 28. Februar 2017).

5 https://www.heise.de/newsticker/meldung/MQTT-Protokoll-IoT-Kommunikation-von-Reaktoren-und-Gefaengnissen-oeffentlich-einsehbar-3629650.html (Stand: 28. Februar 2017).

6 https://cloudsecurityalliance.org/download/future-proofing-the-connected-world/ (Stand: 28. Februar 2017).

7 http://www.inside-it.ch/articles/45282 (Stand: 28. Februar 2017).

nahmen veröffentlicht, die den Umgang bezüglich Sicherheit mit dem Internet der Dinge verbessern sollen.[8]

Empfehlung:

Alle ans Internet angeschlossenen Geräte müssen sowohl abgesichert (individuelle Passwörter, eingeschränkter Zugang) als auch regelmässig aktualisiert werden. Eine Aktualisierung sollte immer rasch erfolgen, sobald entsprechende Updates verfügbar sind. Anders als beim Desktop-Computer oder Smartphone denkt beim intelligenten Lichtschalter oder Kühlschrank jedoch kaum jemand daran, dass auch bei diesen Geräten allenfalls Software-Updates durchgeführt werden müssen.

Ein noch grösseres Gefahrenpotenzial geht von Gegenständen und Geräten aus, auf welche über das Internet mit Standard-Zugangsdaten (Benutzername und Passwort) zugegriffen werden kann. Solche Geräte können grundsätzlich von jedem gefunden werden (beispielsweise mit einem Portscan oder einer Suchmaschine wie «Shodan») und bieten daher eine besonders grosse Angriffsfläche.

MELANI stellt Informationen bereit, wie man sich vor solchen Bedrohungen schützen kann:

DOKU

Sicherheit im «Internet of Things» (IoT)
https://www.melani.admin.ch/melani/de/home/themen/internet_of_things.html

4 Lage national

4.1 Spionage

4.1.1 Die Schweiz als indirektes Ziel von möglichen Spionageaktivitäten

Am 11. August 2016 gab Anonymous Polen bekannt, die Netze der Welt-Anti-Doping-Agentur (WADA) und des Sportschiedsgericht (TAS) gehackt zu haben.[9] Zudem sei das TAS Ziel eines DDoS-Angriffs der Gruppe gewesen. Das TAS mit Sitz in Lausanne ist eine internationale Schlichtungs- und Schiedsstelle für Fälle im Sportbereich, wobei Doping zu den aktuellsten Themenbereichen zählen dürfte, zu dem das TAS momentan angerufen wird. Die genauen Umstände und die Rolle, die Anonymous Polen gespielt hat, sind noch nicht restlos geklärt. Das Interesse für diese Schiedsstelle liegt jedoch in Zusammenhang mit dem Ausschluss russischer Athleten wegen Dopings und den dazugehörenden politischen Implikationen auf der Hand. Obwohl die Schweiz nicht das eigentliche Ziel dieser Operationen gewe-

[8] https://www.melani.admin.ch/melani/de/home/themen/internet_of_things.html (Stand: 28. Februar 2017).

[9] Siehe auch Kapitel 5.1.2

sen ist und die zugrundeliegenden Zusammenhänge sie nur indirekt betroffen haben, befindet sie sich allein durch die Tatsache, dass sich der Sitz von der TAS in der Schweiz befindet, immer wieder im Zentrum der Aufmerksamkeit. Die grosse Dichte an internationalen Organisationen mit Sitz in der Schweiz erhöht deshalb das Risiko für Cyber-Operationen, dem die Schweiz im Rahmen der Sicherung ihres Territoriums mit den geeigneten Mitteln Rechnung tragen muss.

Die Veröffentlichung von Listen infizierter Domains und IP-Adressen am 13. August 2016 durch eine Gruppe, die unter dem Namen «Shadow Brokers» auftritt, ist ein weiterer Fall, der auch die Schweiz betroffen hat. Auf der Liste haben sich unter anderem drei Adressen von Servern der Universität Genf befunden. Die Server stehen mutmasslich im Zusammenhang mit potentiellen Angriffen der «Equation Group».[10] Die Betreiberin von Schweizer Hochschulnetzen «Switch», hat bestätigt, dass zwischen 2001 und 2003 drei Server betroffen waren. Laut Switch seien zwei dieser Server seit 2009 nicht mehr aktiv und der dritte sei von aussen nicht erreichbar gewesen.[11] Auch wenn der Fall bereits einige Zeit zurückliegt und seither Massnahmen ergriffen worden sind, zeigt er doch, dass die Schweiz nicht nur ein attraktives Angriffsziel ist, sondern auch als Zwischenstation und Host von Spionageinfrastruktur genutzt werden kann. Diese Infrastruktur wird teils bei Dienstleistern untergebracht, die es anscheinend mit der Sicherheit nicht so genau nehmen[12], die Unterbringung kann aber auch durch Infizierung von legitimen Servern erfolgen.

In früheren Halbjahresberichten wurde bereits mehrfach erwähnt, welche Gründe aus der Schweiz ein beliebtes Angriffsziel machen.[13] Auch wurden in der Vergangenheit konkrete Fälle aufgezeigt, in denen auf spezifisches Knowhow oder sensible Informationen von Schweizer Firmen und Institutionen abgezielt wurde. Der prominenteste Fall, der in letzter Zeit bekannt geworden ist, ist sicherlich der Angriff gegen die Rüstungsfirma RUAG[14]. Die beiden oben beschriebenen Fälle machen aber deutlich, dass die Schweiz auch ein «Kollateralopfer» von Spionagetätigkeiten sein kann, bei welchen nicht direkt auf Schweizer Interessen abgezielt wird.

---

10 Siehe auch Kapitel 5.1

11 http://www.watson.ch/Digital/NSA/715933955-NSA-hackte-Uni-Genf-und-missbrauchte-drei-Server-f%C3%BCr-Cyberangriffe (Stand: 28. Februar 2017).

12 Dieser Fall ist beispielsweise in Kapitel 3.3 des MELANI-Halbjahresberichts 1/2014 erwähnt https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2014-1.html (Stand: 28. Februar 2017).

13 Siehe besonders MELANI Halbjahresbericht 2/2015, Kapitel 4.1 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2-2015.html (Stand: 28. Februar 2017).

14 Siehe Kapitel 4.1.1 im MELANI Halbjahresbericht 1/2016 https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/rapporto-semestrale-2016-1.html (Stand: 28. Februar 2017).

Schlussfolgerung / Empfehlung:

MELANI setzt sich in Partnerschaft mit verschiedenen staatlichen und privaten Einheiten seit 13 Jahren für den Schutz vor IKT-Gefahren ein. Zur Meldung von Vorfällen stellt MELANI auf ihrer Website ein Meldeformular zur Verfügung:

Meldeformular MELANI:

https://www.melani.admin.ch/melani/fr/home/meldeformular/formulaire.html

Der Nachrichtendienst des Bundes (NDB) führt mit seinem Programm «Prophylax» eine Präventions- und Sensibilisierungsaktion im Bereich der Nonproliferation und der Wirtschaftsspionage durch. Sie dient zur Sensibilisierung von Unternehmen und Bildungsinstitutionen:

Programm Prophylax:

http://www.vbs.admin.ch/de/themen/nachrichtenbeschaffung/wirtschaftsspionage.detail.publication.html/vbs-internet/de/publications/nachrichtendienst/Prophylax.pdf.html

http://www.vbs.admin.ch/de/themen/nachrichtenbeschaffung/wirtschaftsspionage.html

4.2 Datenabflüsse

4.2.1 Erpressung mit angeblichen Kundendaten

Die Liechtensteinische Bank Valartis gab am 17. November 2016 in einer Medienmittelung bekannt, sie sei Ziel eines Hackerangriffs geworden. Der Angreifer erlangte verschiedene Informationen zu Zahlungsaufträgen, die vor Mai 2013 erfolgt waren und primär dem Firmen-Kundenbereich zuzuordnen waren. Eine Manipulation der Zahlungsaufträge zu Lasten der Kunden schloss die Bank aus. Das Kernsystem der Bank sei vom Hackerangriff nicht tangiert gewesen. Auch Angaben über Kontostände und dergleichen habe der Angreifer nicht einsehen können. Die Kunden, die vom Hackerangriff hätten betroffen sein können, wurden von der Bank informiert. Die Bank erfuhr von diesem Angriff, als eine Person das Finanzinstitut per E-Mail kontaktierte und mitteilte, ein Datenleck gefunden zu haben. Gleichzeitig bot diese ihre Dienste anonym an, um die Sicherheitslücken gegen Entgelt zu schliessen. Valartis ging nicht auf das Angebot beziehungsweise die Forderungen ein. [15]

[15] http://www.valartisbank.li/Download.aspx?mode=download&id=IqzI6qVOde5v%2foNBMJr8xg%3d%3d (Stand: 28. Februar 2017).

Da der Angreifer auf diesem Wege nicht zu seinem Erfolg respektive zu seinem Geld kam, versuchte er laut Inside-IT in einem zweiten Schritt, sich per E-Mail direkt an Kunden der Bank zu wenden. Zumindest gewisse E-Mail-Adressen von Kunden schienen tatsächlich im Besitz des Angreifers zu sein. In diesem Erpressungsschreiben behauptete er, die Kontostände und weitere Kundendaten zu kennen. Bei Nichtbezahlung drohte er, die Daten an die Finanzbehörden und Medien weiterzugeben. Der Erpresser verlangte zehn Prozent des Kontostands in Form von Bitcoins.[16]

Da die Kunden vorher durch die Bank informiert worden sind, geht MELANI davon aus, dass wohl kein Opfer den Forderungen der Erpresser nachgekommen ist. Ein interessantes Detail ist, dass der Angreifer gar nicht hätte verifizieren können, ob die Opfer überhaupt zehn Prozent ihres Kontostandes oder weniger überwiesen hätten, da die Information über den Kontostandes laut Bank nicht in die Hände des Erpressers fielen. Hier hatte der Angreifer wohl einfach auf die Ehrlichkeit des Opfers spekuliert.

Schlussfolgerung / Empfehlung:

MELANI rät in solchen Fällen ausdrücklich von einer Zahlung ab, da man sich dadurch in eine Abhängigkeit zum Erpresser begibt. Gleichzeitig ist aber eine proaktive Kommunikation wichtig, um den Angreifern den Wind aus den Segeln zu nehmen.

MELANI wurden ähnlich gelagerte Fälle in der Berichtsperiode mehrfach zur Kenntnis gebracht. In den meisten Fällen wird dabei mit einer so genannten «SQL-Injection» auf eine schlecht gesicherte Datenbank zugegriffen, um an die Daten zu gelangen. Die Motivation der Angreifer variiert dabei stark: Es gibt auf der einen Seite tatsächlich diejenigen, die diese Vorgehensweise als «Geschäftsmodell» verfolgen und das Schliessen von Sicherheitslücken gegen Geld anbieten. In anderen Fällen dient die ganze Geschichte jedoch nur als Vorwand, um möglichst viel Geld zu erpressen.

Hacker versuchen sich mit diversem Hintergrund und verschiedenen Motivationen voneinander abzugrenzen. Dabei haben sich die Begriffe «White Hat», «Grey Hat» und «Black Hat» durchgesetzt: White Hats (Weiss-Hüte) verwenden ihr Wissen innerhalb der gesetzlichen Schranken. Black-Hats (Schwarz-Hüte) handeln typischerweise mit krimineller Energie. Sie versuchen, in ein Zielsystem einzudringen – entweder nur um zu sehen, ob sie es können, vielleicht aber auch, um es zu beschädigen oder Daten zu stehlen. Dazwischen stehen die Grey Hats, die gegen Gesetze verstossen, allerdings ein höheres Ziel verfolgen, beispielsweise die Verantwortlichen zu zwingen, Sicherheit ernster zu nehmen und zu verbessern. Grey Hats handeln häufig illegal, jedoch meist mehr oder weniger nach einer «Hacker-Ethik».

[16] http://www.inside-it.ch/articles/45798 (Stand: 28. Februar 2017).

4.3 Industrielle Kontrollsysteme (IKS)

Die zentrale Steuerung eines Hauses meldet dem Besitzer, dass die Sonnenstoren zu Hause geschlossen wurden. Bei dieser Gelegenheit startet der Hausbesitzer gleich die Klimaanlage aus der Ferne, um bei angenehmer Raumtemperatur anzukommen. Oftmals erfolgt die Steuerung über das Smartphone. Durch vermehrte Nutzung dieser Annehmlichkeiten kommen immer mehr Privatanwender in Kontakt mit der Gebäudeautomation, einer Variante industrieller Kontrollsysteme.

Was in privaten Haushalten zunehmend integriert wird, ist in grossen Komplexen wie Bürogebäuden, Fabriken und Spitälern seit langem Standard. Hier ist die Zentralisierung der Steuermöglichkeiten von immer zahlreicheren Systemen und Geräten notwendig, um Qualität und Effizienz der Verwaltung zu steigern. Diese Zentralisierung erhöht aber auch die potenziellen Konsequenzen bei unberechtigtem Zugriff und Manipulation der zentralen Steuerung.

4.3.1 Sensibilisierung für die Bedrohung vernetzter IKS

Um die Annehmlichkeiten der Fernwartung zu nutzen, werden industrielle Kontrollsysteme (IKS) in vielen Fällen mit dem Internet verbunden. So kann der Zustand der Geräte überwacht und Steuerbefehle abgesetzt werden, ohne dafür vor Ort sein zu müssen. Geschieht die Anbindung ans Internet ohne ausreichende Schutzmassnahmen, besteht das Risiko, dass die Kontrollsysteme durch unberechtigte Dritte in nicht gewünschter Weise bedient werden. Spezialisierten Suchmaschinen wie «Shodan»[17] ermöglichen es auch Laien, solche offen zugängliche Systeme zu entdecken. Das kann nicht im Sinne des Betreibers sein.

Entdeckt MELANI solch potenziell gefährdete Systeme in der Schweiz oder werden diese MELANI gemeldet, werden die Betreiber kontaktiert, um abzuklären, ob sie sich der Erreichbarkeit ihres Systems bewusst sind. In jedem Falle wird eine Empfehlung zur Sicherung der Kontrollsysteme abgegeben.

Private Sicherheitsforscher meldeten Ende letzten Jahres MELANI ein offen erreichbares Gebäudeautomationssystem. Es sei möglich, unberechtigt auf die klimatischen Bedingungen im Gebäude einzuwirken.

Abbildung 1: Ausschnitt Gebäudesteuerung

Glücklicherweise stellte sich heraus, dass es sich bei der Steuerung um ein System handelte, welches sich noch im Test befand. Das entsprechende Gebäude war noch gar nicht bezogen worden. Nach Abschluss der letzten Tests wurde das System vom Internet abge-

[17] https://www.shodan.io/ (Stand: 28. Februar 2017).

schottet und ist seither nur noch für die mit dem Betrieb und Wartung betrauten Techniker zugänglich.

Empfehlung:

Entdecken Sie offen erreichbare Steuerungssysteme im Internet, melden Sie uns die entsprechenden Angaben, damit wir den Betreiber informieren können:

Meldeformular MELANI:

https://www.melani.admin.ch/melani/fr/home/meldeformular/formulaire.html

Checkliste mit Massnahmen zum Schutz industrieller Kontrollsysteme

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

4.4 Angriffe

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

4.4.1 DDoS und Erpressung: aktuelle Entwicklung in der Schweiz

Im letzten MELANI-Halbjahresbericht wurde auf die verschiedenen Erpressungsformen im Zusammenhang mit DDoS-Angriffen aufmerksam gemacht. Dabei hat sich im zweiten Halbjahr 2016 der Trend bestätigt, dass Erpresser ihrem Angriffsziel drohen, ohne dass sie je in der Lage wären, einen DDoS-Angriff durchzuführen. Wie zu erwarten, haben Kriminelle sofort die Ängste ausgenutzt, die durch die grossen, mittels Botnet «Mirai»[18] durchgeführten DDoS-Angriffe geschürt worden sind, um von Opfern Bitcoins zu erpressen. So trat Ende Jahr eine Gruppe mit dem angeblichem Namen «NewWorldHacker» auf, welche die Opfer mit einer anstehenden Attacke zu erpressen versuchte. Ein DDoS-Angriff fand aber nie statt. Zur Erinnerung: Die Gruppe «NewWorldHacker» hat sich zu den massiven Attacken auf den Anbieter DNS Dyn bekannt.

Trotz dieses Trends haben einige andere Fälle daran erinnert, dass ein tatsächlicher Angriff nie ausgeschlossen werden darf. Dabei müssen nicht zwingend alle Opfer angegriffen werden, sondern unter Umständen reicht auch ein Exempel, das als Warnung für die anderen

[18] Siehe Kapitel 3 e 5.4

Angriffsziele dient. Ein typisches Beispiel für dieses Vorgehen ist eine Gruppe namens «DD-Crew DDoS», deren Merkmal es ist, sich auf eine bestimmte Firmenbranche zu konzentrieren. Der Angriff erfolgt ausschliesslich auf einen Marktteilnehmer in dieser Branche. Mit Bezugnahme auf diesen Angriff, werden dann die anderen Unternehmen der Branche einzeln kontaktiert und damit erpresst, einen Betrag in Bitcoins zu bezahlen, damit sie vom gleichen Schicksal wie ihr Konkurrent verschont bleiben. Interessanterweise variieren in diesen Fällen die verlangten Geldbeträge je nach Bekanntheit (gemäss Google Rank) und Grösse des Unternehmens.

Schlussfolgerung:

Die Kombination von Erpressung und Androhung eines DDoS-Angriffs wird wahrscheinlich anhalten und die durch Mirai geschürte Angst vor Grossangriffen weiterhin ausgenutzt werden. Zudem kann jeder beliebige Täter, dank verschiedenen Diensten, die DDoS-Angriffe «anbieten» (Siehe Kapitel 6.1), solche Angriffe lancieren. Dadurch ist dieses kriminelle Betätigungsfeld mit einer Vielzahl von Tätern mit ähnlichen Vorgehensweisen ständig in Bewegung.

4.5 Social Engineering, Phishing

Neben all den technischen Angriffen sind vor allem solche beliebt und erfolgreich, welche menschliche Schwächen ausnützen.

4.5.1 Betrugsversuche in unterschiedlicher Qualität

Auch im zweiten Halbjahr 2016 wurden MELANI diverse CEO-Betrugsfälle gemeldet. Von CEO-Betrug ist dann die Rede, wenn Täter im Namen des Firmenchefs oder anderer führender Personen die Buchhaltung oder den Finanzdienst anweisen, eine Zahlung auf ein Konto vorzunehmen, das in Wirklichkeit den Betrügern gehört und typischerweise im Ausland liegt.[19] Die Begründungen für die Zahlung sind unterschiedlich, wobei es meist um eine angeblich dringende und äusserst heikle, vertrauliche Angelegenheit gehe. Die Qualität der einzelnen Betrugsversuche variiert dabei stark. Während bei den einen Vorfällen nur eine allgemeingültige Anfrage zwecks dringender Überweisung gestellt wird, sammeln die Betrüger in anderen Fällen zahlreiche Informationen über die anzugreifende Firma, um eine passende Geschichte zu erfinden und den Betrug sehr gezielt abzuwickeln. Oft sind auch ein Berater oder eine falsche respektive behauptete Anwaltskanzlei Teil des Szenarios. Um den Anfragen einen seriöseren Eindruck zu geben, werden manchmal auch Websites von Banken oder Anwaltsbüros kopiert oder imitiert.

Auch Bundesstellen wurden in der Berichtsperiode nicht verschont. Bei Finanzabteilungen der Bundesverwaltung gingen ebenfalls solch betrügerische Anweisungen für Geldüberwei-

[19] Siehe MELANI Halbjahresbericht 1/2016, Kapitel 4.5.2 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2016-1.html (Stand: 28. Februar 2017).

sungen ein. In einem weitere Fall wurde die Website der Finanzmarktaufsicht (FINMA) imitiert, um die Opfer zu einer Zahlung zu bewegen.

Dass die Betrüger immer trickreicher werden und ihre Angriffe bis ins Detail planen, zeigen Fälle, wo sich Betrüger am Telefon sogar als Bundesstelle ausgaben. Der Hintergrund ist klar: Durch das Vortäuschen einer offiziellen staatlichen Stelle, kann beim Opfer ein grösserer Druck aufgebaut werden, um es zu bewegen eine durch den Angreifer gewünschte Aktion auszuführen. Erstaunlich war, dass auf dem Telefon-Display der Opfer tatsächlich die Nummer der Bundesverwaltung angezeigt wurde. Die Nummer wurde durch die Betrüger gefälscht.

Empfehlung:

Bei Social Engineering-Angriffen wird die Hilfsbereitschaft, Gutgläubigkeit oder die Unsicherheit von Personen ausgenützt, um beispielsweise an vertrauliche Daten zu gelangen oder die Opfer zu bestimmten Aktionen zu bewegen. Neben allen Angriffsmöglichkeiten ist dies nach wie vor eine der erfolgreichsten. MELANI hat Tipps publiziert, wie man sich vor solchen Angriffen schützen kann.

INFO

Aktuelle Gefahren: Social Engineering

https://www.melani.admin.ch/melani/de/home/themen/socialengineering.html

4.5.2 Phishing

Auch im zweiten Halbjahr 2016 wurden zahlreiche Phishing-E-Mails versendet. Dabei werden immer wieder die gleichen Typen von E-Mails beobachtet: Die einen fragen nach Kreditkartendaten, damit diese «verifiziert» werden können, andere fordern auf der verlinkten Seite nach Login und Passwort zu Internetdiensten. Regelmässig werden in solchen Phishing-Mails auch Firmenlogos von bekannten Unternehmen respektive des betroffenen Dienstes missbraucht, um den E-Mails einen offiziellen Anstrich zu geben.

Insgesamt wurden im Jahr 2016 über 4500 verschiedene Phishing-Seiten über das von MELANI betriebene Portal antiphishing.ch gemeldet. Auf Abbildung 2 sind die gemeldeten Phishing-Webseiten pro Woche dargestellt, wobei die Anzahl über das ganze Jahr gesehen variiert. Die Gründe hierzu sind sehr verschieden: Zum einen gibt es ferienbedingte Schwankungen, da in der Ferienzeit weniger Phishing-Seiten gemeldet werden und zum anderen verschieben die Kriminellen ihre Angriffe regelmässig von Land zu Land.

Abbildung 2: Gemeldete und bestätigte Phishing-Seiten pro Woche auf antiphishing.ch im zweiten Halbjahr 2016

4.5.3 Phishing-Seiten, die keine sind

Bereits im Halbjahresbericht 1/2012[20] hat MELANI darauf hingewiesen, wie wichtig eine wohlüberlegte Kundenkommunikation im Zeitalter von Phishing ist. Immer wieder lösen echte E-Mails an Kunden Verunsicherung aus. In der Berichtsperiode haben die Bürgermeldungen über angebliche Phishing-Seiten zugenommen. Einerseits hat das sicherlich mit einer erhöhten Sensibilisierung der Bürgerinnen und Bürger zu tun auf, andererseits aber auch damit, dass sich einige Firmen nicht an gewisse Richtlinien (siehe nächste Info-Box) halten.

4.5.3.1 Der Klassiker - Änderungen der Paypal-AGBs

Ein immer wiederkehrender Anlass für Meldungen zu angeblichen Phishing-Seiten sind die Hinweise von Paypal, eBay und Co zu Änderungen der AGB. Auch wenn in der E-Mail jeweils kein Link zu einer Login-Seite vorhanden ist, erzeugt allein die Tatsache, dass die Nutzer unerwartet E-Mails von Paypal erhalten, eine gewisse Verunsicherung und löst immer zahlreiche Meldungen an MELANI aus. Dies dürfte nicht zuletzt daher kommen, dass Paypal bezüglich Phishing einer der am meisten angegriffenen Internetdienste ist und viele Nutzer auch schon entsprechende Phishing-Mails erhalten haben.

4.5.3.2 Versteckter Link und Link auf einen Drittserver

Auch E-Mails von Schweizer Firmen lösten bei MELANI Meldungen angeblicher Phishing-Seiten aus. So wurde in der Berichtsperiode von einer Firma eine Werbemeldung versandt, dass der Kunde eine Gutschrift erhalte. Der angegebene und hinter einem Formularfeld versteckte Link ging aber nicht auf die Website der Firma selbst, sondern auf eine Domäne einer auf Werbung spezialisierten Firma. Dies rief bei den Empfängern berechtigterweise Skepsis hervor. In einem weiteren Fall schrieb eine andere Firma Kunden per E-Mail an, dass ein Betrag für Umtriebe bezahlt werden müsse, wenn innerhalb einer Frist keine

[20] MELANI Halbjahresbericht 1/2012, Kapitel 3.8 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2012-1.html (Stand: 28. Februar 2017).

Rückmeldung erfolge. Eine persönliche Anrede fehlte und der versteckte Link führte auf eine Webseite, auf der man seinen Benutzernamen und sein Passwort eingeben sollte. Viele sensibilisierte Bürger schöpften hier Verdacht und wendeten sich an MELANI. Die E-Mail stammte allerdings tatsächlich von der Firma und der Link verwies auch auf ihre Website.

Schlussfolgerung / Empfehlung:

«Keine seriöse Firma wird Sie je per E-Mail nach Login und Passwörtern fragen.» Das ist die Standard-Antwort, die MELANI jeweils gibt, wenn Personen eine E-Mail melden, bei dem sie nicht sicher sind, ob dieses nun tatsächlich von der besagten Firma stammt oder nicht. Diese Aussage, die zunächst einfach klingt, stellt die Firmen im Zeitalter der elektronischen Kundenkommunikation aber oft vor Herausforderungen: Wie soll eine Firma mit den Kunden kommunizieren, damit diese eine E-Mail nicht als betrügerisch auffassen? Und noch wichtiger: Eine allzu sorglose Kundenkommunikation durch eine Firma kann auch das Kundenverhalten bezüglich betrügerischen E-Mails negativ beeinflussen.

Folgende Punkte sollten beim Versand von E-Mails durch Firmen beachtet werden:

- E-Mails wenn möglich im Nur-Text-Format versenden, damit allenfalls enthaltene Links klar ersichtlich sind und sich nicht hinter anderem Text wie zum Beispiel «klicken Sie hier» verbergen.
- Mit Links in E-Mails sparsam umgehen und nur auf die eigene Domäne verlinken. Wenn möglich Links auf durch Verschlüsselung gesicherte Seiten (https) verwenden und dies dem Empfänger auch mitteilen.
- Nicht auf Webseiten verlinken, die Benutzername und Passwort oder andere Eingaben verlangen.
- Newsletter-E-Mails möglichst regelmässig versenden.
- Auf der Startseite des Webauftrittes auf den Newsletter hinweisen oder die Information direkt verlinken, damit der Empfänger die Möglichkeit hat, die Hauptadresse manuell einzugeben und dann den Newsletter von dort anzuklicken.
- Kunden mit Vor- und Nachnamen anschreiben, sofern diese Information vorhanden ist.

Gerade im Finanzsektor sollten wichtige Informationen zu Konten schriftlich per Brief versendet werden.

4.5.4 Zunahme von Phishing-Awareness-Kampagnen

Die Sensibilisierung der eigenen Mitarbeitenden ist zentral, wenn es um die Sicherheit der Firma geht. Deshalb führen immer mehr Firmen so genannte Phishing-Awareness-Kampagnen durch. Während einer solchen Kampagne werden präparierte Phishing-E-Mails an die Mitarbeitenden gesendet. Anschliessend wird analysiert, wer die Links angeklickt hat. Das ermöglicht der Firma, nicht nur die Mitarbeitenden zu sensibilisieren, sondern gleichzeitig den Awareness-Grad zu bestimmen und anschliessend geeignete Massnahmen zu treffen. Die Phishing-Seite ist dabei auf einer Domäne gespeichert, die zuvor extra für diesen Zweck gelöst wurde. Es liegt im Sinn der Sache, dass gut sensibilisierte Mitarbeitende solche E-Mails auch an Anti-Phishing-Meldestellen, wie die von MELANI betriebene Site «an-

tiphishing.ch», weiterleiten. Mit diesem Vorgang werden dann allerdings diverse Massnahmen wie Website-Take-Down-Prozess und diverse Einträge bei Filterprogrammen ausgelöst. Diese Reaktionen stören dann logischerweise den Awareness-Test. Bei blockierter oder gelöschter Website können keine Informationen über den Sensibilisierungsgrad der Mitarbeitenden mehr gewonnen werden.

Empfehlung:

Eine gute und immer wiederkehrende Sensibilisierung der Mitarbeitenden in einer Firma aber auch der Bevölkerung ist einer der Hauptpfeiler, wenn es um Sicherheit im Internet geht. Phishing-Awareness-Kampagnen sind eine Möglichkeit, eine solche Sensibilisierung durchzuführen. Um einen reibungslosen Ablauf zu garantieren, sollten vor der Durchführung eines solchen Tests zumindest alle an der Infrastruktur beteiligten Akteure informiert werden: Es sind dies insbesondere die Registrierungsstelle der Top-Level-Domain (für .ch-Domänen ist dies SWITCH), Registrar und Hosting-Provider sowie gegebenenfalls der (externe) E-Mail-Anbieter. Schliesslich ist auch eine Ankündigung an MELANI sinnvoll, damit allfällige Meldungen im Sinne der Veranstalter der Awareness-Kampagne beantwortet werden können und keine Massnahmen gegen die Website durch MELANI eingeleitet werden.

4.6 Crimeware

Crimeware ist eine Form von Schadsoftware, die kriminologisch zur Computerkriminalität zählt und rechtlich bei Datenbeschädigung sowie betrügerischem Missbrauch einer Datenverarbeitungsanlage anzusiedeln ist. Der grösste Teil an Infektionen ging auch im zweiten Halbjahr 2016 auf das Konto der Schadsoftware «Downadup» (auch bekannt als «Conficker»). Der Wurm existiert bereits seit über acht Jahren und verbreitet sich über eine im Jahr 2008 entdeckte und ebenso lange geschlossene Sicherheitslücke in Windows-Betriebssystemen. An zweiter Stelle folgt die Anzahl Infektionen durch die Schadsoftware «Necurs», die sich sowohl auf das Versenden des Verschlüsselungstrojaners «Locky» als auch auf die E-Banking-Schadsoftware «Dridex» spezialisiert hat. An dritter Stelle ist das seit dem Angriff auf den Internetdienstleister «Dyn» bekannt gewordene Bot-Netzwerk «Mirai», welches Geräte im Internet der Dinge infiziert.

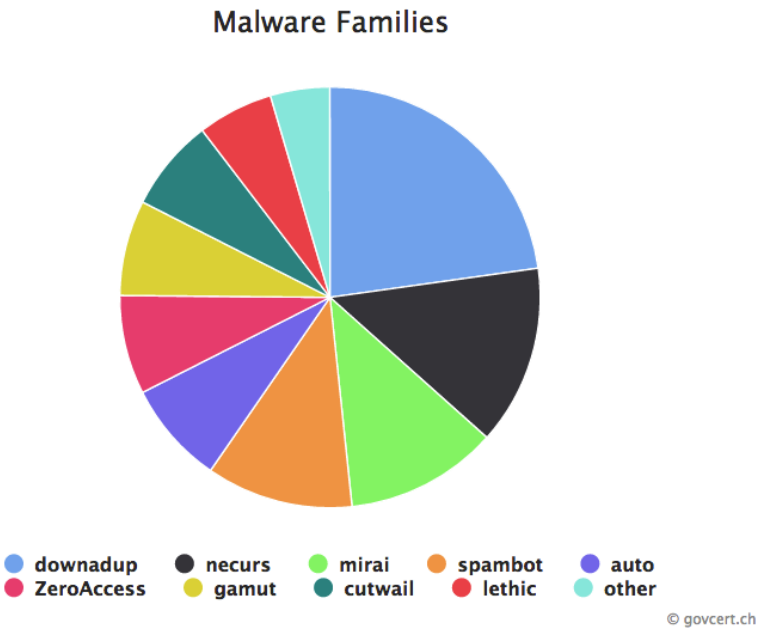

Abbildung 3: Verteilung der Schadsoftware in der Schweiz, welche MELANI bekannt ist. Stichtag ist der 31. Dezember 2016. Aktuelle Daten finden Sie unter: http://www.govcert.admin.ch/statistics/dronemap/

4.6.1 E-Banking-Trojaner – Fokus auf Firmen

Das Feld der E-Banking-Trojanerfamilien hat sich im letzten Halbjahr nicht gross verändert. Weiterhin aktiv in der Schweiz sind die Schadsoftware-Familien «Retefe» und «Gozi». Während Gozi auch über Webseiten-Infektionen verteilt wird, wird Retefe mittels E-Mail mit gefälschten Rechnungen von existierenden, mehr oder weniger bekannten Firmen verbreitet. Das jeweils angehängte Word-Dokument enthält dabei ein JavaScript oder eine ausführbare Datei, welche die Webbrowser-Einstellungen des Internet Explorers oder Firefox dahingehend ändern, dass ein Proxyserver eingetragen wird, der den Angreifern gehört. Die Angreifer können dann, falls gewollt, jede vom Benutzer aufgerufene Domäne auf einen Server ihrer Wahl umleiten. Zusätzlich hat Retefe auch die Fähigkeit, Mobiltelefone zu infizieren und anschliessend das SMS mit der mobilen TAN an die Betrüger umzuleiten. Gemäss Berichten des Sicherheitsdienstleisters Trendmicro[21] wurde zudem die Android-Malware, welche das per SMS gesendete Einmalpasswort abfängt, durch die Betrüger verfeinert. Kriminelle haben nun anscheinend die Malware mit Anti-Analyse, Device Routing und Remote Access-Fähigkeiten ausgestattet. Die Malware verleitet die Benutzer zudem der App verschiedene Rechte zu gebe, so zum Beispiel den Accessibility Service, welcher es erlaubt, Benutzerinteraktionen zu simulieren.

Auch «Dridex» wird via E-Mail mit gefälschten Rechnungen verbreitet. Nachdem mit Dridex zumindest in der Schweiz bis Juni 2016 nur E-Banking-Privatkunden angegriffen wurden, änderte die Täterschaft im Juli 2016 die Angriffsmethode und nahm von da an auch Offline-Zahlungs-Softwarelösungen ins Visier. Solche Software wird von vielen Unternehmen ver-

[21] http://blog.trendmicro.com/trendlabs-security-intelligence/new-smssecurity-variant-roots-phones-abuses-accessibility-features-teamviewer/ (Stand: 28. Februar 2017).

wendet, um grössere Mengen an Zahlungen via Internet an eine oder mehrere Banken zu übermitteln. Entdecken die Angreifer nach der Erstinfektion eine solche Zahlungssoftware, wird die auf solche Fälle spezialisierte Schadsoftware «Carbanak» nachgeladen. Eine schematische Darstellung des Infektionsweges ist in Abbildung 6 dargestellt.[22]

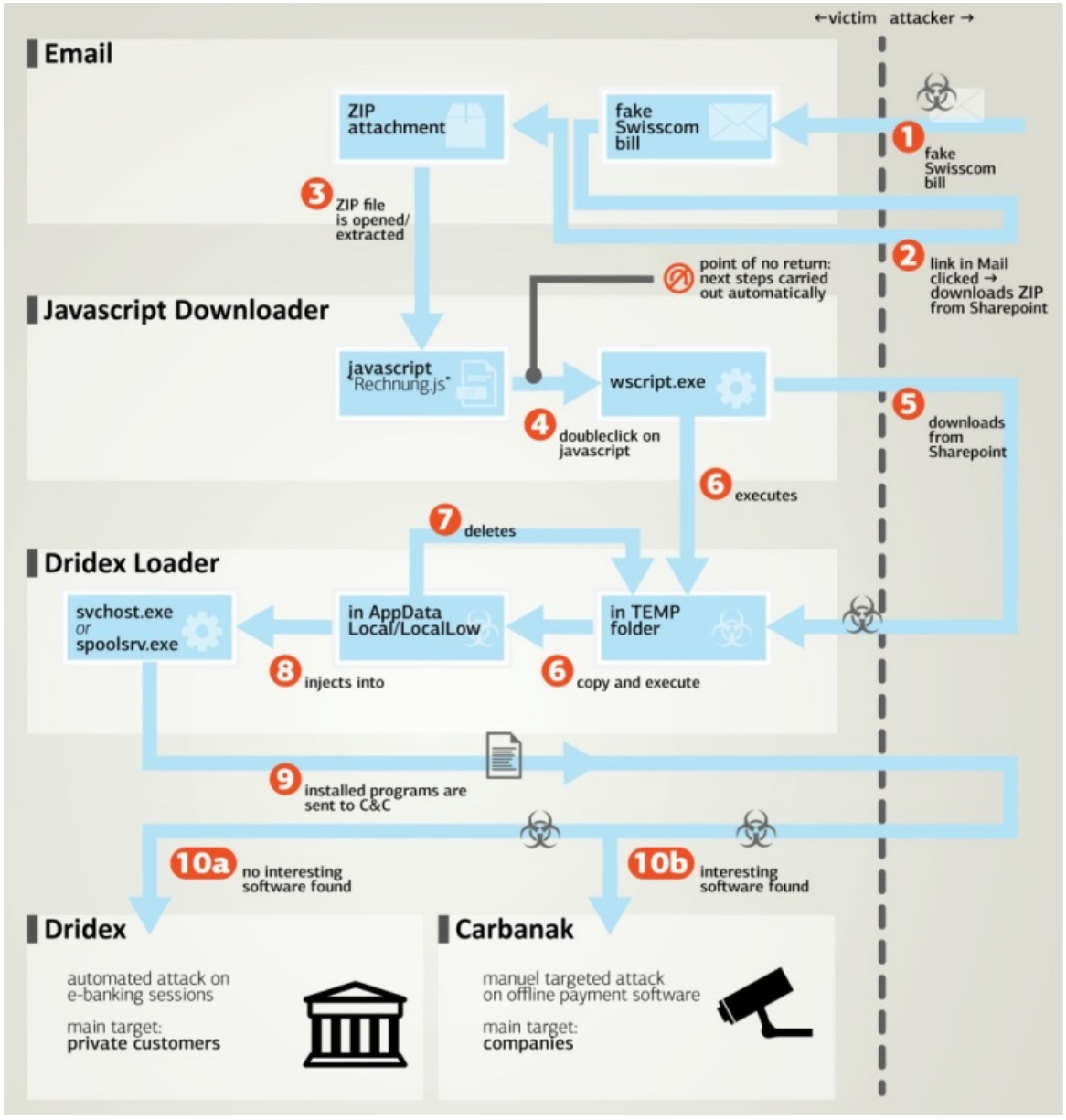

Abbildung 4: Schematische Darstellung des Infektionsweges während der Spamwelle mit gefälschten Swisscom Rechnungen im Februar 2017

[22] Die Schadsoftware meldete sich Ende Februar 2017 mit einer grossen Spamwelle zurück: Mittels gefälschten Swisscom-Rechnungen wurde versucht, die Empfänger zur Installation des Trojaners zu verleiten. https://www.govcert.admin.ch/blog/28/the-rise-of-dridex-and-the-role-of-esps (Stand: 28. Februar 2017).

Empfehlung:

Bei Computern, die für den Zahlungsverkehr eingesetzt werden, sind folgende Grundsätze zu beachten:

- Verwenden Sie für offline Zahlungs-Software und E-Banking einen dedizierten Computer, auf welchem Sie nicht im Internet surfen oder E-Mails empfangen.
- Verwenden Sie für die Visierung von Zahlungen eine Kollektivunterschrift über einen Zweitkanal (z. B. E-Banking). Erkundigen Sie sich bei Ihrer Bank über entsprechende Möglichkeiten.
- Falls Sie einen Hardware-Token (z. B. Smart Card, USB-Dongle) verwenden, entfernen Sie diesen nach Gebrauch der Zahlungs-Software.
- Speichern Sie Zugangsdaten (Vertragsnummer, Passwort, usw.) für E-Banking und Zahlungs-Software nicht auf dem Computer bzw. in der Software.
- Erkundigen Sie sich beim Hersteller Ihrer Zahlungs-Software über zusätzliche Sicherheitsmassnahmen und aktivieren Sie die automatischen Softwareupdates.
- Melden Sie verdächtige Zahlungen umgehend Ihrer Bank.
- Um eine Infektion mit Dridex und anderer Schadsoftware in Ihrem Unternehmen zu verhindern, empfiehlt MELANI zudem folgende Massnahmen:
  - Stellen Sie sicher, dass potenziell schädliche E-Mail-Anhänge bereits auf Ihrem E-Mail-Gateway bzw. Spam-Filter blockiert bzw. gefiltert werden. Gefährliche E-Mail Anhänge verwenden unter anderem Dateiendungen, wie sie im folgenden MELANI-Newsletter aufgeführt sind: https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/offline-payment-software.html
  - Versichern Sie sich, dass solche gefährlichen E-Mail-Anhänge auch dann blockiert werden, wenn diese in Archiv-Dateien wie beispielsweise ZIP, RAR oder aber auch in geschützten Archiv-Dateien (z. B. in einem passwortgeschützten ZIP) an Empfänger in Ihrem Unternehmen versendet werden.
  - Zusätzlich sollten sämtliche E-Mail-Anhänge blockiert werden, welche Makros enthalten (z. B. Word, Excel oder PowerPoint Anhänge mit Makros), sofern diese nicht unbedingt benötigt werden. Gegebenenfalls könnte der Versand/Empfang solcher Anhänge auf bestimmte Absender/Empfänger beschränkt werden.

4.6.2 E-Banking-Trojaner missbrauchen die Nachlässigkeit der Benutzer

Auch moderne Zweifaktor-Authentifizierung, wie «CrontoSign», «PhotoTAN» oder «SecureSign» sind vor Betrugsversuchen nicht gefeit, obschon diese Authentifizierungsmethoden als sicher gelten. Ende November 2016 wurden MELANI mehrere Fälle gemeldet, bei welchen es Hackern gelungen war, genau diese Systeme für Betrugszahlungen zu missbrauchen. Dabei werden E-Banking-Kunden mittels Social Engineering dazu animiert, betrügerische Zahlungen via PhotoTAN, CrontoSign oder SecureSign zu visieren.

Abbildung 5: Mosaik (links) und QR-Code (rechts) wie er zum Login und Visieren einer Zahlung verwendet wird

Dem Kunden wird beim Login oder zum Visieren einer Zahlung ein QR-Code oder Mosaik im E-Banking-Portal angezeigt (siehe Abbildung 6). Diesen kann er mit einer App auf seinem Smartphone oder einem unabhängigen Gerät einscannen. Danach wird, je nach Produkt, das Login bzw. die Visierung der Zahlung direkt in einer App bestätigt oder diese generiert einen Code, welchen der Kunde im E-Banking-Portal eingeben muss. Kunden lassen sich jedoch in vielen Fällen durch Social Engineering täuschen und visieren die Zahlungen auch dann, wenn sie den Vorgang als betrügerisch erkennen könnten, beispielsweise wenn in der App ein offensichtlich falsches Empfängerkonto angezeigt wird oder wenn bereits beim Login-Vorgang Zahlungsdaten eingeblendet werden.

Die Hersteller haben reagiert und eine verbesserte Visibilität implementiert, damit der Benutzer noch besser zwischen dem Login-Vorgang und der Freigabe einer Zahlung unterscheiden kann.

Abbildung 6: Neue verbesserte Anzeige des Einmalpasswortgenerators, dass es sich nicht um einen Login, sondern um die Freigabe einer Zahlung handelt.

Empfehlung:

Im Umgang mit Authentifizierungsmethoden via Smartphone wie beispielsweise mTAN, PhotoTAN, CrontoSign oder SecureSign empfiehlt MELANI:

- Stellen Sie sicher, dass Sie beim Login-Vorgang ins E-Banking auf dem mobilen Gerät (beispielsweise Smartphone oder dediziertes PhotoTAN-Gerät) wirklich das Login bestätigen und dass es sich nicht bereits um die Visierung einer Zahlung handelt.
- Falls Sie eine Zahlung visieren, lesen Sie immer den ganzen Text auf dem mobilen Gerät und überprüfen Sie Betrag und Empfänger (Name, IBAN) der Zahlung, bevor Sie diese freigeben.
- Informieren Sie sich über weitere Sicherheitsmassnahmen, welche Ihr Finanzdienstleister anbietet (z.B. Standardmässiger Ausschluss von Zahlungen in Länder, in welchen Sie keine Geschäftsbeziehungen unterhalten).

4.6.3 Ransomware

Auch in dieser Berichtsperiode wurden MELANI wieder zahlreiche Fälle von Verschlüsselungstrojanern gemeldet. Darunter waren Angriffe gegen Verwaltungen und KMUs. Ein funktionierendes Backup auf einem externen Medium, dass durch die Verschlüsselungsschadsoftware nicht in Mitleidenschaft gezogen werden kann, ist dabei das A und O. Besser ist aber, es gar nicht so weit kommen zu lassen und entsprechende Vorkehrungen zu treffen. MELANI hat solche Empfehlungen publiziert (siehe nachfolgende Infobox). Die Verschlüsselung und somit der temporäre Verlust der Daten ist nämlich nur ein Teil des Problems. Ebenfalls berücksichtigt werden muss, dass in der Zeit des Zurückspielens des Backups allenfalls ein grosser Teil des Betriebes still steht. Da heute die meisten Firmen auf eine funktionierende IKT angewiesen sind, kann ein Stillstand je nach dem einen erheblichen finanziellen Verlust zur Folge haben. Hinzukommt, dass gerade bei kritischen Infrastrukturen ein Nichtfunktionieren des Betriebes noch viel gravierendere Auswirkungen haben kann.

In der Schweiz sind vor allem folgende Ransomware-Typen verbreitet: «Cerber», «Locky» und «Mischa/Petya». Cerber wurde unter anderem durch ein angebliches Gewinnversprechen per E-Mail verbreitet. In Sachen Infektionsweg immer noch sehr problematisch sind auch E-Mails mit vermeintlichen Bewerbungen, die gezielt an Personalabteilungen versendet werden. Gerade in den Personalabteilungen, aber auch in den Pressestellen müssen Mitarbeitende laufend Dokumente von unbekannter Quelle öffnen. Hier empfiehlt es sich, vom eigentlichen Netzwerk abgetrennte Computer zu betreiben, und anschliessend die Bewerbungen zu drucken. Aber auch Versuche, mit gefälschten Rechnungen oder gefälschten Gerichtsvorladungen sind beliebte Methoden der Kriminellen. Generell lässt sich sagen, dass Betrüger Eigenschaften wie Neugier, Angst und Aussicht auf Geld oder Glück der Opfer ausnutzen.

Empfehlung:

- Regelmässige Sicherungskopie (Backup) der Daten durchführen. Die Sicherungskopie sollte offline, das heisst auf einem externen Medium wie beispielsweise einer externen Festplatte gespeichert werden. Stellen Sie sicher, dass Sie das Medium, auf welchem Sie die Sicherungskopie erstellen, nach dem Backup-Vorgang vom Computer trennen.
- Installierte Software und Plug-Ins immer aktuell halten (z.B. Virenschutz, Browser).
- MELANI empfiehlt, keine verdächtigen E-Mail-Anhänge zu öffnen, auch wenn diese von vermeintlich vertrauenswürdigen Absendern stammen. Fragen Sie im Zweifelsfalle beim (bekannten) Absender nach, worum es sich beim Anhang genau handelt.
- Stellen, die aufgrund ihrer Funktion E-Mails von unbekannten Empfängern erhalten und Anhänge öffnen müssen, sollten hierfür einen dedizierten Computer verwenden, der vom restlichen Unternehmensnetzwerk möglichst gut abgeschottet ist, damit sich eine allfällige Infektion nicht auf dieses ausbreiten kann.

Massnahmen gegen Verschlüsselungstrojaner:

https://www.melani.admin.ch/melani/de/home/themen/Ransomware.html

Ransomware: Bedrohungslage, Prävention & Reaktion vom BSI

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.html

Projekt No More Ransom:

https://www.nomoreransom.org/decryption-tools.html

Verhaltensregeln ➔ E-Mail

https://www.melani.admin.ch/melani/de/home/schuetzen/verhaltensregeln.html

4.7 Präventive Massnahmen

4.7.1 Präventiv blockierte Domains dank Analyse der Malware Tofsee

Schadsoftware enthält oft einen Domain-Generation-Algorithmus, kurz DGA. Dieser hat die Aufgabe, Domainnamen für die Command- und Controlserver (C&C) zu generieren, mit denen infizierte Rechner (Bots) dann kommunizieren. Ein dynamisches und laufendes Generieren von Domainnamen hat gegenüber der fixen Vorausdefinition den Vorteil, dass allfällige Massnahmen gegen die Kommunikation der Bots mit der C&C-Infrastruktur sehr viel komplizierter werden. So muss der verwendete Algorithmus zuerst verstanden werden, damit die Domain-Namen, welche die Täter registrieren und dann verwenden, vorausgesagt werden können. Ende Dezember 2016 hat MELANI den DGA der Schadsoftware «Tofsee» analysiert, wobei sich herausgestellte, dass fast die Hälfte der generierten Domainnamen die Top-Level-Domain (ccTLD) .ch verwendeten. Die Malware Tofsee wird zum breitflächigen Spam-Versand über infizierte Rechner verwendet. MELANI hat daraufhin in Zusammenarbeit mit der Registrierungsstelle Switch und der Stiftung zur Bekämpfung von schädlichen Domain-

namen «Registrar of Last Resort» die Registrierung von über 500 der vom DGA erzeugten .ch-Domainnamen während 12 Monaten verhindern können.

4.8 Weitere Themen

4.8.1 E-Voting-Quellcode auf Github

Im Dezember hat der Kanton Genf einen Teil des Quellcodes seines E-Voting-Systems auf dem Online-Dienst Github veröffentlicht. Der Schritt erfolgte vorwiegend im Sinne der Transparenz, kann aber dank externen Beiträgen ebenfalls zu einer Verbesserung des Systems führen. Das Genfer E-Voting-System ist auch in anderen Kantonen in Betrieb, die es erworben haben.

4.8.2 Switch bleibt Registrierungsstelle für Internet-Domain «.ch»

Die Verwaltung der .ch-Domainnamen wurde Anfang 2016 vom Bundesamt für Kommunikation (BAKOM) öffentlich ausgeschrieben.[23] Die Stiftung SWITCH erhielt den Zuschlag, weil ihre Offerte die höchste Gesamtpunktzahl unter den eingereichten Angeboten erzielt hat.[24] Insbesondere hob sie sich durch ein herausragendes Konzept zur Bekämpfung der Cyber-Kriminalität ab. Die Funktion der Registerbetreiberin für die .ch-Domainnamen wird bereits heute von SWITCH ausgeübt. Sie wird nun für mindestens weitere 5 Jahre die nationale Datenbank der .ch-Domain-Namen verwalten und die elektronische Verknüpfung mit dem weltweiten Domain-Namen-System (DNS) sicherstellen.

Der Bundesrat hat die Schweizer Top-Level-Domain als kritische Infrastruktur eingestuft. Als solche bedarf sie eines besonderen Schutzes, weil ein Ausfall weite Teile des öffentlichen Lebens in der Schweiz beeinträchtigen würde. MELANI arbeitet eng mit der Registerbetreiberin zusammen, um die Sicherheit und Verfügbarkeit der Schweizer Domainnamen zu garantieren.

---

[23] https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-61133.html (Stand: 28. Februar 2017).

[24] https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-63597.html; https://www.switch.ch/de/news/SWITCH-wins-tender/ (Stand: 28. Februar 2017).

5 Lage International

5.1 Spionage

5.1.1 Angriff auf demokratische Parteileitung (DNC) in den USA: offizielle Stellungnahme

Bereits im letzten Halbjahresbericht[25] wurde über den Cyber-Angriff auf die demokratische Parteileitung (DNC) der USA berichtet. Ein Bericht der Firma Crowdstrike hatte diese Angriffe «Cozy Bear» und «Fancy Bear» zugeschrieben[26]. Im zweiten Halbjahr 2016 wurden auf den Plattformen Wikileaks und DCLeaks weitere, offenbar von der gleichen Kampagne stammende, Informationen enthüllt. Darunter waren insbesondere rund 58 000 Mails vom infizierten Konto des Wahlkampagnenleiters von Hillary Clinton, John Podesta,

Am 7. Oktober haben das US-Heimatschutzministerium und das Büro des nationalen Geheimdienstdirektors in einer gemeinsamen Stellungnahme der russischen Regierung vorgeworfen, mit Angriffen auf E-Mail-Konten von politischen Persönlichkeiten und Institutionen versucht zu haben, sich in den US-Wahlkampf einzumischen[27]. Ein Untersuchungsbericht vom 29. Dezember 2016 wies wiederum auf die Kampagnen «Cozy Bear» und «Fancy Bear» als Ursprung hin[28]. In der Folge wurden Sanktionen gegen russische Stellen und Personen angekündigt.

Das Besondere an diesem Fall ist zweifellos die konkrete Art, mit der die russischen Behörden durch die höchste Ebene eines anderen Staates als die Urheber eines Cyber-Angriffs bezeichnet wurden. Zudem war die Resonanz in dem stark umkämpften US-Präsidentschaftswahlkampf ohnehin bereits erhöht[29].

---

[25] Halbjahresbericht 2016/1, Kapitel 5.1.1 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2016-1.html (Stand: 28. Februar 2017).

[26] https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/ (Stand: 28. Februar 2017).

[27] https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national (Stand: 28. Februar 2017).

[28] https://www.us-cert.gov/security-publications/GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity (Stand: 28. Februar 2017).

[29] Zur Thematik «Einflussnahme bei den letzten US-Präsidentschaftswahlen» siehe Kapitel 5.1 des letzten Berichts 1/2016: https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2016-1.html (Stand: 28. Februar 2017).

5.1.2 APT 28 im Zusammenhang mit zahlreichen Vorfällen genannt

In der Berichtsperiode wurde die unter den Namen «Sofacy», «Fancy Bear», «Pawn Storm» oder «APT 28»[30] auftretende Gruppe als mutmasslich Verantwortliche für zahlreiche weitere Angriffe in der Berichtsperiode genannt.

Am 11. August 2016 gab Anonymous Polen bekannt, die Welt-Anti-Doping-Agentur (WADA) und das Sportschiedsgericht (TAS) gehackt zu haben[31]. Die genaue Identität und die tatsächliche Rolle der Gruppe bei diesem Vorfall sind unklar. In einer am 19. August 2016 von der Firma Threat Connect veröffentlichten Analyse wird ein Verbindung zu «Fancy Bear» hergestellt[32]. Diese Aussage stützte sich insbesondere auf die Art, wie Domainnamen registriert wurden, welche die beiden Organisationen imitierten.

Im Falle von WADA benutzten die Angreifer eine solche Domäne für einen Spear Phishing Angriff. Die Angreifer versuchten so, sich Zugang zum «Anti-Doping Administration & Management System» zu verschaffen, auf dem die Angaben zu Dopingkontrollen der Athleten erfasst sind. Der Angriff wurde von der Agentur bestätigt. Es gelang damit insbesondere, das Konto von Julia Stepanowa zu kompromittieren. Die russische Leichtathletin hatte mit ihren Enthüllungen die Sanktionen gegen russische Athleten im Dopingfall ermöglicht. In der Folge wurden im September von einer Gruppe «Fancy Bears», zahlreiche Daten über Athleten auf der ganzen Welt veröffentlicht, die angeblich aus den WADA-Datenbanken stammten. Die WADA äusserte sich dahingehend, dass einige dieser Daten gefälscht sein könnten.

Am 20. September haben die Süddeutsche Zeitung und die deutschen Radiosender NDR und WDR berichtet, deutsche Politiker seien im August Ziel eines Angriffs mit Spear-Phishing-Mails geworden[33], die angeblich von der Nato kamen. Wie bei den Angriffen auf den Bundestag 2015 zitiert die Zeitung regierungsnahe Quellen, die den Angriff dem Spionagekomplex «Sofacy» zuschrieben. Am 24. September wurde enthüllt, dass auch der Westdeutsche Rundfunk WDR vom Angriff betroffen gewesen sei[34].

Im Dezember erschienen weitere Berichte über Vorfälle, bei denen die gleiche Urheberschaft vermutet wurde. So berichtete die Zeitung Le Monde, die OECD sei Ziel eines Angriffs geworden[35]. Die OECD hat den Angriff bestätigt. Ende Dezember berichtete Crowdstrike über «Sofacy»-Aktivitäten einer ganz anderen Dimension[36]. Bei der Analyse einer von einem uk-

---

30 Diese Namen wurden von den Firmen oder Behörden genannt, die die Angriffe untersucht haben.

31 Der Sitz ist in Lausanne. Der Fall kommt im Teil Schweiz dieses Berichts zur Sprache.

32 https://www.threatconnect.com/blog/fancy-bear-anti-doping-agency-phishing/ (Stand: 28. Februar 2017).

33 http://www.sueddeutsche.de/politik/bundesregierung-ist-alarmiert-hackerangriff-aufdeutsche-parteien-1.3170347 (Stand: 28. Februar 2017).

34 http://www.spiegel.de/politik/deutschland/cyberattacke-russische-hacker-attackieren-wdr-journalisten-a-1113780.html (Stand: 28. Februar 2017).

35 http://www.lemonde.fr/international/article/2016/12/28/l-osce-victime-d-une-attaque-informatique_5054744_3210.html (Stand: 28. Februar 2017).

36 https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/ (Stand: 28. Februar 2017).

rainischen Offizier für die ukrainische Artillerie entwickelten Android-App[37] seien Spuren der ausschliesslich von «Fancy Bear» (alias «Sofacy») verwendeten Malware «x-Agent» gefunden worden. Mit dieser Infizierung hätten beispielsweise die Stellungen der ukrainischen Geschütze leichter geortet werden und so potenziell unschädlich gemacht werden können.

5.1.3 «Winnti» wird erwachsen – Von gestohlenem Online Spielgeld zu ausgefeilter Industriespionage gegen Stahlwerke

Der deutsche Industriekonzern Thyssenkrupp gab Anfang Dezember 2016 gegenüber der Wirtschaftswoche bekannt, dass er Opfer eines Cyber-Spionageangriffs geworden war.[38] Bereits im Frühjahr war es der als «Winnti» bekannten Gruppe gelungen, in die Netzwerke des Unternehmens einzudringen. Nach der Entdeckung durch das interne Sicherheitsteam und einer sechsmonatigen Abwehr konnte das System bereinigt werden. Den Angreifern gelang es aber, einige Datensätze auszuspähen.

Neben den Standorten des Konzernteils «Industrial Solutions» in Europa, Indien, Argentinien und den Vereinigten Staaten, war auch die Stahlindustrie mit dem Walzwerk Hohenlimburg unter den Zielen. Physische Schäden mussten glücklicherweise keine verzeichnet werden. Die Motivationt der Gruppe beschränkte sich anscheinend auf das Ausspionieren.

Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) hat bestätigt, dass es im Zusammenhang mit «Winnti» auch noch Fälle gegen andere Unternehmen gibt. Die Gruppe zeichnet sich durch das Einschleusen gut versteckter Fernzugriffe in fremde Systemumgebungen aus. Bekannt wurde Winnti im Jahre 2009 durch Angriffe auf Online-Spiele, wo Spielgeld abgezweigt und anschliessend auf dem Schwarzmarkt verkauft worden war. Seit 2015 erweiterte sie Ihren Tätigkeitsbereich nun anscheinend auf Cyber-Spionage gegen Unternehmen.

5.1.4 Netbotz - Die Kamera, die nicht nur den Bildausschnitt überwacht

In äusserst sensitiven Bereichen von Behörden und Grossunternehmen wird verbreitet Überwachungstechnik, wie beispielsweise Überwachungskameras oder Servermonitoring-Systeme, des US-Herstellers Netbotz eingesetzt. Allerdings sollen laut dem deutschen ARD-Magazin «Fakt» in diesen Geräten geheime Zugänge für die amerikanischen Geheimdienste eingebaut sein.[39] Fakt beruft sich dabei auf einen als geheim eingestuften Bericht des deutschen Bundesnachrichtendienstes (BND). Darin wird geschildert, dass der BND bereits 2004 von einer Quelle auf die mögliche Hintertür in Netbotz-Produkten hingewiesen worden war. Bei der technischen Überprüfung des Hinweises konnte anscheinend verifiziert werden, dass das Netbotz-System versuchte, verdeckt eine Verbindung mit einem Server des US-Verteidigungsministeriums aufzubauen. Netbotz trat offenbar mit aggressiven Tiefpreis-Angeboten an das Deutsche Auswärtige Amt und potenzielle Kunden aus dem Hightech- und Rüstungsbereich heran, um seine Systeme zu verkaufen. Das Recherchemagazin pran-

---

37 Die App sei auf Militärforen verteilt worden und sollte den Einsatz der Haubitzen D-30 Howitzer verbessern.

38 http://www.wiwo.de/unternehmen/industrie/spionageangriff-auf-thyssenkrupp-grossalarm-haette-die-risiken-erhoeht/14948264.html (Stand: 28. Februar 2017).

39 http://www.mdr.de/fakt/industriespionage-100.html (Stand: 28. Februar 2017).

gert vor allem an, dass der BND weder das Bundesamt für Verfassungsschutz noch betroffene Firmen über die Erkenntnisse bezüglich des verdeckten Fernzugriffs informiert hatte. Netbotz ist heute Teil des französischen Unternehmens Schneider Electric, welches viele elementare Komponenten verschiedenster Industriesteuerungen herstellt.

5.1.5 Welche Kampagnen sonst noch Schlagzeilen machten

«Sofacy» war in den letzten sechs Berichtsmonaten sicher eine der meistgenannten Spionagekampagnen. Daneben wurden aber zahlreiche weitere Fälle von Cyber-Spionage in der ganzen Welt aufgedeckt. Meist erfolgt die Publikation durch Sicherheitsunternehmen, basierend auf Nachforschungen, die jeweils bei betroffenen Kunden gemacht wurden. Da an dieser Stelle aufgrund der Vielzahl an Kampagnen nicht alle genannt werden können, fokussieren wir uns auf einige Beispiele: Der nicht sehr raffinierte Spionagekomplex «Dropping Elephant»[40] soll gemäss Kaspersky aus Indien stammen, «On the StrongPity»[41] hat es vor allem auf Chiffriersysteme abgesehen und Symantec hat über Aktivitäten einer Gruppe namens Strider[42] (bei Kaspersky auch «ProjectSauron»[43] genannt) berichtet, die ausgeklügelte Angriffe gegen wenige ausgewählte Ziele vornimmt. Schliesslich wurde eine israelische Gruppe («NSO Group») für das Ausnutzen von Schwachstellen des iPhone zu Überwachungszwecken beschuldigt. Apple hat die Schwachstellen anschliessend behoben[44].

Ebenfalls erwähnenswert sind Werkzeuge und Schadsoftware, die angeblich aus dem Arsenal der «Equation Group» stammen und die eine Gruppe namens «Shadow Brokers» am 13. August 2016 veröffentlicht hat. Zur Erinnerung: «Equation Group» ist eine Gruppe, die ausgeklügelte Cyber-Spionage betreibt und hinter der die NSA vermutet wird. «Shadow Brokers» gab an, das veröffentliche Material sei nur ein Teil dessen, was sie besässen und dass der Rest versteigert werde. Zahlreiche Experten haben in der Folge die Authentizität der Dateien bestätigt. Am 31. Oktober veröffentlichte die Gruppe ein neues Archiv mit infizierten Domainnamen und IP-Adressen, mit welchen Angriffe verübt worden sein sollen[45]. Über die Identität von «Shadow Brokers» und die Herkunft der Informationen wurde heftig spekuliert.

---

40 https://securelist.com/blog/research/75328/the-dropping-elephant-actor/ (Stand: 28. Februar 2017).

41 https://securelist.com/blog/research/76147/on-the-strongpity-waterhole-attacks-targeting-italian-and-belgian-encryption-users/ (Stand: 28. Februar 2017).

42 http://www.symantec.com/connect/blogs/strider-cyberespionage-group-turns-eye-sauron-targets (Stand: 28. Februar 2017).

43 https://securelist.com/analysis/publications/75533/faq-the-projectsauron-apt/ (Stand: 28. Februar 2017).

44 https://motherboard.vice.com/en_us/article/nso-group-new-big-player-in-government-spyware?trk_source=recommended (Stand: 28. Februar 2017).

45 Siehe Kapitel 4 inwiefern die Schweiz davon betroffen war.

Die Zuschreibung ausgeklügelter Angriffe (des Typs APT) erfolgt meist gestützt auf technische Elemente (typischerweise die verwendete Infrastruktur) oder ganz spezifische Vorgehensweisen. Die Zuverlässigkeit dieser Zuschreibungen ist sehr unterschiedlich. Eine erste Einschätzung muss oft mit Überlegungen politischer und strategischer Art ergänzt werden. Denn die Ziele von Angriffen werden ja nicht zufällig gewählt, sondern nach einem spezifischen Muster. So muss man nach dem Grund fragen, weshalb Täter ein Interesse an einer bestimmten Organisation haben könnten. Gibt es darauf eine Antwort nicht nur für einen Einzelfall, sondern eine ganze Fallkonstellation, wird das die Zuschreibung des Angriffs erleichtern.

5.2 Datenabflüsse

Daten sind ein, wenn nicht der Rohstoff in einer digitalen Wirtschaft und Gesellschaft. Praktisch jede Firma betreibt eine Datenbank mit einer Vielzahl personenbezogener (Kunden-) Daten. Der Sicherheit muss dabei angemessen Rechnung getragen werden. Trotzdem werden in regelmässigen Abständen Datenabflüsse, d.h. unbefugte Datenbeschaffungen publik.

5.2.1 Yahoo Data Breach - Ein Datenabfluss unvorstellbaren Ausmasses

Yahoo hat Mitte Dezember 2016 einen Datenabfluss von schier unvorstellbarem Ausmass bekannt gegeben. Bei einem Vorfall von 2013 hätten Unbekannte auf über eine Milliarde Datensätze zugegriffen. Glücklicherweise sollen darunter keine Kreditkartendaten gewesen sein. Trotzdem haben auch persönliche Daten wie Name, Geburtsdatum, Telefonnummern und E-Mail-Adressen einen Wert in kriminellen Kreisen. Diese bieten die Basis für weitere Social Engineering-Angriffe. Damit lässt sich auch erklären, wieso Angreifer immer häufiger Namen mit E-Mail-Adressen in Verbindung bringen und die Empfänger dann persönlich ansprechen können. Bereits im September 2016 hat Yahoo einen Datenabfluss aus dem Jahre 2014 bekannt gemacht, der über 500 Millionen Yahoo Benutzerkonten betraf.

5.2.2 Datenabfluss durch Insider

Die Sage Group ist weltweit als eine der grössten Anbieterinnen von Unternehmens- und Finanzsoftware für kleine und mittlere Unternehmen bekannt. Der Angriff, der anscheinend Anfang August 2016 auf die Sage Group stattgefunden hat, soll Datensätze von bis zu 300 Unternehmen betroffen haben, die Finanzsoftware von Sage einsetzen. Die Firma Sage speichert verschiedene Daten ihrer Kunden, darunter Namen, Anschriften, Geburtsdaten, Sozialversicherungsnummern, Kontoverbindungen und andere Finanzdaten. Da der Zugriff mit einem regulären Login erfolgte, wurde von Anfang an vermutet, dass es sich um die Tat eines Insiders handelte. Diese Vermutung wurde dann auch bestätigt. Dieser Vorfall zeigt jedem Sicherheitsverantwortlichen einmal mehr, dass man neben dem Schutz vor Angriffen von aussen die Angriffe von innen nicht vernachlässigen sollte.

5.2.3 Auch Adultfriendfinder wieder betroffen

Das Erwachsenenportal Adultfriendfinder wurde zum erneuten Mal Opfer eines unbefugten Datenzugriffs. Im November 2016 wurde der Abfluss von insgesamt 412 Millionen Datensät-

zen bekannt. Bereits 2015 war das Portal wegen einem solchen Vorfall in den Schlagzeilen: Damals waren 3.5 Millionen Datensätze betroffen. Gerade Daten aus Erwachsenenportalen sind für Kriminelle ein lukratives Geschäft und lassen sich gewinnbringend weiterverwenden. Gemäss dem Portal LeakedSource umfassen die ausgespähten Daten E-Mail-Adressen, Passwörter, zum Teil sogar ungeschützt, Benutzernamen, IP-Adressen und Browser-Informationen.[46] LeakedSource prangerte an, dass der Anbieter die Daten nicht sauber verschlüsselt und die Passwörter im Klartext gespeichert oder nur mit der veralteten Hash-Funktion «SHA 1» gesichert hat.

[46] http://www.leakedsource.com/blog/friendfinder (Stand: 28. Februar 2017).

Empfehlung:

Wenn man einen Blick auf die E-Mail-Adressen wirft, welche bei solch gehackten Datenbanken zum Vorschein kommen, fällt auf, dass diese jeweils auch zahlreiche Firmen-E-Mails umfassen, obschon der zugehörige Internetdienst mit der Arbeitstätigkeit ziemlich sicher nichts zu tun hat. Viele Firmen erlauben eine angemessene private Nutzung der Firmeninfrastruktur – insbesondere des Internetzugangs. Die Verwendung von Firmen-E-Mail-Adressen zu privaten Zwecken sollte allerdings klar geregelt sein. Auch die Verwendung der Firmen-IT zwecks privatem E-Mail-Verkehr birgt Gefahren: Auf das Öffnen von verdächtigen Anhängen sollte im Büro wie zu Hause verzichtet werden.

Verhaltensregeln für den Umgang mit E-Mails

https://www.melani.admin.ch/melani/de/home/schuetzen/verhaltensregeln.html ➔ E-Mail

Verhaltensregeln für Passwörter

Ein Passwort sollte in regelmässigen Abständen (ca. alle 3 Monate) gewechselt werden, jedoch spätestens dann, wenn Sie vermuten, dass es Dritten bekannt sein könnte.

Weitere Regeln:
https://www.melani.admin.ch/melani/de/home/schuetzen/verhaltensregeln.html ➔ Passwort

Wenn Sie als Unternehmen selber Kundendatenbanken verwalten, auf welche die Kunden online zugreifen können, sollten Sie sicherstellen, dass Sie nicht das Opfer des nächsten Datenlecks werden. Unterstützung bietet die Checkliste auf unserer Website.

Merkblatt IT-Sicherheit für KMUs

https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/checkliste-online-auftritt-kmu.html

KMU-Portal des Bundes

https://www.kmu.admin.ch/kmu/de/home.html

5.3 Industrielle Kontrollsysteme (IKS)

Das Internet der Dinge wird im Schwerpunktthema dieses Halbjahresberichts näher beleuchtet. Dabei sind Dinge, welche netzwerktechnisch erschlossen wurden, bereits seit langem im Einsatz. Sensoren und Aktoren werden mit Steuerungen zentral koordiniert, automatisiert und optimiert. Solche Steuerungen kontrollieren Stromnetze, Verkehrsströme, das Gebäudeklima oder die medizintechnischen Geräte im Spital.

5.3.1 Déjà-vu in Kiew - Erneuter Stromausfall in der Ukraine

Ziemlich genau ein Jahr nach dem Stromausfall in Teilen der Ukraine Ende 2015, über welchen wir im vorletzten Halbjahresbericht[47] berichtetet hatten, wurde es im Norden Kiews erneut dunkel. Wieder kurz vor Weihnachten, am Samstag, dem 17. Dezember 2016, kurz vor Mitternacht, blieben die Kunden des staatlichen Energieversorgers Ukrenergo, welche vom Pivnichna Unterwerk versorgt werden, für knapp eine Stunde ohne Strom[48]. Ukrenergo informierte seine Kunden, dass nicht klar sei, ob der Ausfall von Komponenten oder ein Hackerangriff Schuld am Ausfall sei. Einige Wochen später verkündete Oleksandr Tkachuk, der Stabschef der ukrainischen Sicherheitsdienste, dass sowohl dieser Stromausfall, wie auch Angriffe auf das Finanzsystem und weitere Infrastrukturen, durch russische Sicherheitsdienste in Zusammenarbeit mit privaten Software-Firmen und Cyber-Kriminellen orchestriert worden war[49]. Seiner Aussage nach seien die Attacken von den gleichen Personen konstruiert worden, die auch in frühere Angriffe mit der BlackEnergy-Malware involviert waren. Seine Behauptungen konnten bisher nicht von unabhängigen Spezialisten verifiziert werden. Die Anschuldigungen werden bisher einzig von ukrainischen Sicherheitsforschern der «Information Systems Security Partners (ISSB) » sowie des «Honeywell Cyber Security Labs» an einem Vortrag während der IKS-Sicherheitskonferenz «S4 2017» gestützt[50]. Laut eigenen Aussagen sollen diese Spezialisten an der Untersuchung des Vorfalls beteiligt gewesen sein. Gemäss den Ausführungen wurden die aus der Ferne kontrollierbaren Steuereinheiten (RTUs) nicht wie im Vorjahr durch Überschreiben der Firmware unbrauchbar gemacht. Im jüngsten Angriff wurden sie einfach aus der Ferne abgeschaltet, weshalb die Wiederherstellung der Stromversorgung auch schneller von statten ging. Laut den Sicherheitsforschern hätten die Angreifer die Möglichkeit gehabt, bedeutend schwerwiegendere Schäden anzurichten. Insofern war der Angriff nicht auf maximalen Schaden ausgelegt, was die Vermutung nahelegt, dass es sich dabei eher um eine Machtdemonstration seitens der Saboteure gehandelt hat.

Infiltriert wurden die Ziele mit einer massiven E-Mail-Kampagne im Juli 2016, durch welche Schadsoftware eingeschleust wurde. Anschliessend verweilten die Angreifer mehrere Monate in den Netzwerken, um diese zu analysieren und sich zu den Zielgeräten vorzuarbeiten.

---

47 MELANI Halbjahresbericht 2/2015 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2-2015.html (Stand: 28. Februar 2017).

48 https://motherboard.vice.com/en_us/article/ukrainian-power-station-hacking-december-2016-report (Stand: 28. Februar 2017).

49 http://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN15U2CN (Stand: 28. Februar 2017).

50 https://www.youtube.com/watch?v=lTwsDLO3C44 (Stand: 28. Februar 2017).

Neben dem Stromversorger waren das Finanzministerium, das Schatzamt sowie der staatliche Pensionsfonds der Ukraine weitere Opfer. Am 6. Dezember 2016 wurde eine DDoS-Attacke gegen diese Ziele verübt, während intern Netzwerkkomponenten beschädigt und Datenbanken zerstört wurden. Dies führte zu einem Unterbruch und einer Verzögerung des staatlichen Zahlungsverkehrs.

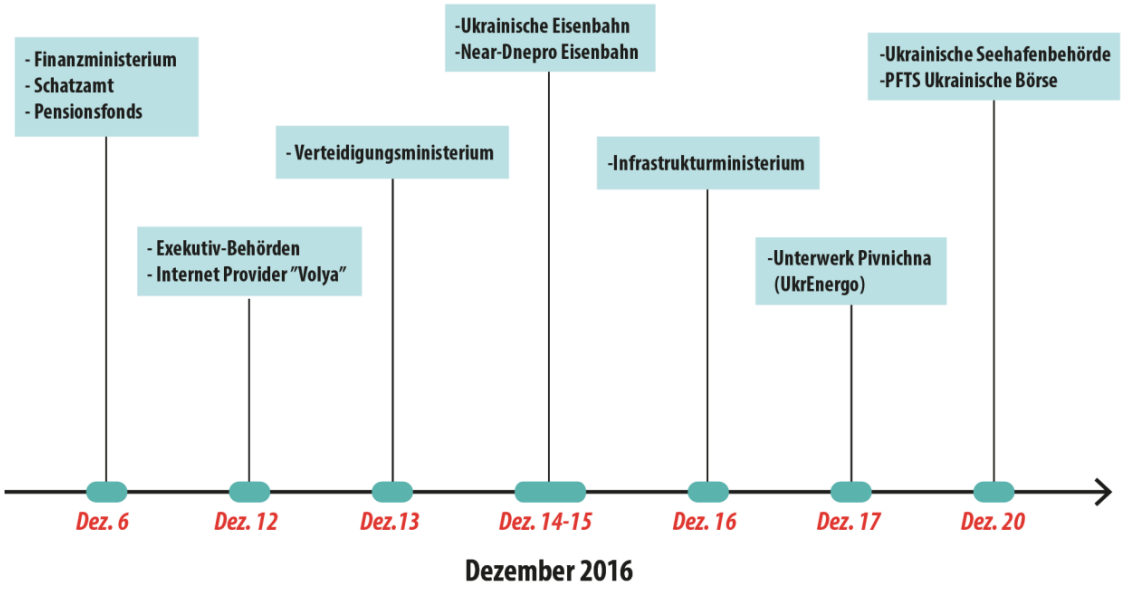

Abbildung 7: Die verschiedenen Angriffe auf der Zeitachse (Quelle: S4 Events)

Am 14. Dezember 2016 wurde zudem die staatliche Eisenbahnverwaltung der Ukraine Ziel der Saboteure. Wiederum wurde zur Ablenkung ein DDoS-Angriff gestartet. Dieser zielte auf den Online-Ticketshop. Währenddessen wurde das automatisierte Frachtmanagement der Güterzüge manipuliert. Die Parallelen zum Angriff 2015 ziehen die Forscher anhand der beobachteten Strategien, wie sich die Saboteure in den infiltrierten Netzwerken ausbreiteten. Fortschritte stellten sie anhand der in den gezielten E-Mail-Angriffen enthaltenen Makroviren fest. Gegenüber den simplen Makros von 2015 war nur noch ein Prozent des Codes für die eigentliche Funktionalität zuständig. 30% der programmierten Zeilen sollten die Analyse des Makros erschweren und weitere 69% dienten einzig der Absicht, die Bösartigkeit der Schadsoftware zu verschleiern.

Für die beteiligten Sicherheitsforscher entstand der Eindruck, dass die Ukraine zu einem Trainingsspielplatz für solche Cyber-Angriffe missbraucht wurde, auf welchem die gegnerische Seite ihre Kapazitäten auslotete. Die Sicherheitsforscher teilen mit, dass die vertieften Analysen des Vorfalls noch mehrere Monate in Anspruch nehmen. Bis dahin werden die präsentierten Erkenntnisse kaum von unabhängigen Spezialisten verifiziert werden können.

Im Umfeld der industriellen Kontrollsysteme ist primär bezüglich des aufkommenden Alarmismus bei scheinbar spektakulären Entdeckungen von Angriffen Vorsicht geboten . Dies schreibt Robert M. Lee, welcher bei der Analyse des Vorfalls 2015 mitwirken durfte. Werden angemessene Sicherungsmassnahmen konsequent umgesetzt, können auch in den Auswirkungen beängstigende Attacken entdeckt und verhindert werden. So fühlte sich beispiels-

weise die Cyber-Sicherheitsfirma SentinelOne genötigt, bei einer ihrer Malware-Analysen eine Richtigstellung anzubringen, nachdem die Presse basierend darauf von staatlichen Angriffen gegen den Energiesektor in den USA berichtete. Als einziges Indiz diente die Tatsache, dass auf einem Opfersystem auch ein Energiemanagementsystem betrieben wurde. Die Malware selbst wies jedoch keine Charakteristiken auf, die spezifisch auf die Kontrollsysteme abzielte.

5.3.2 Distributed Denial of Heating – Frieren nach DDoS-Angriff

Im Osten Finnlands mussten die Bewohner von zwei Gebäuden in der Stadt Lappeenranta für einige Zeit ohne Heizung und warmes Wasser auskommen. Grund für den Ausfall war ein DDoS-Angriff, der die übergeordnete Gebäudeautomationssteuerung in fataler Weise tangierte[51]: Das System versuchte sich durch Neustarts gegen die Angriffe zu stemmen, blieb aber in einer Endlosschlaufe hängen und die Heizung blieb ausgeschaltet. Auf der Suche nach unsicher konfigurierten oder Schwachstellen enthaltenden Geräten gerieten finnische Gebäudeautomationssteuerungen ins Visier von Bot-Netz-Betreibern. Die Heizung konnte schliesslich wieder gestartet werden, indem auf den übergeordneten Netzwerkebenen der Datenverkehr gedrosselt und der DDoS-Angriff auf diese Weise abgewehrt wurde. Der Hersteller des Systems erklärte, dass mehrere solche Attacken im Land beobachtet worden waren.

Ein sicherer Betrieb wäre möglich, wenn die Systeme, wie empfohlen, abgeschottet betrieben werden würden. Aus Bequemlichkeit und zwecks einfacher Benutzerführung werden diese aber immer wieder mit dem Internet verbunden.

Schlussfolgerung / Empfehlung:

Die zunehmende Computerisierung und Vernetzung von allerlei Gegenständen des alltäglichen Gebrauchs (Internet der Dinge) bietet viele neue und sinnvolle Funktionen und Annehmlichkeiten. Dabei dürfen jedoch die damit verbundenen Risiken nicht unbeachtet bleiben. Neue Möglichkeiten bergen immer auch neue Gefahren, die bereits bei der Entwicklung berücksichtigt werden müssen (Security by Design).

Checkliste mit Massnahmen zum Schutz industrieller Kontrollsysteme

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

[51] http://metropolitan.fi/entry/ddos-attack-halts-heating-in-finland-amidst-winter (Stand: 28. Februar 2017).

5.4 Angriffe

5.4.1 Ausfall des Internets bei 900'000 Kunden der deutschen Telekom

Am 27. November 2016 wurde ein weltweiter Angriff auf zahlreiche Heimnetzwerkrouter verzeichnet. Dieser führte in Deutschland zum Ausfall des Internets bei 900‘000 Telekom-Kunden. Grund des Ausfalls war der Einsatz einer neuen Version der Schadsoftware Mirai, die bereits für den Angriff auf die DNS-Server der Firma Dyn am 21. Oktober 2016 verwendet worden war[52]. Mirai ist eine Schadsoftware gegen das Betriebssystem Linux, das vor allem in Geräten des Internet of Things verwendet wird. In diesem Falle durchsuchte die Schadsoftware Heimnetzwerkrouter von Endkunden nach einer Schwachstelle zur Installation der Schadsoftware. Da Heimnetzwerkrouter der Deutschen Telekom ein proprietäres Betriebssystem haben, war allerdings die Installation der Schadsoftware nicht möglich. Die zahlreichen Angriffsversuche haben allerdings die Geräte zum Absturz gebracht. Die deutsche Telekom hat ihren Kunden ein Update der Software zur Verfügung gestellt.

5.4.2 Angriffsziel Finanztransaktionen

In der Berichtsperiode waren verschiedentlich Fälle in den Schlagzeilen, bei denen Kriminelle versucht haben, Finanztransaktionen zu manipulieren. Die nachfolgenden Beispiele sollen aufzeigen, wie vielfältig die potenziellen Ziele solcher Angriffe sind.

Am 6. November gab die britische TESCO-Bank bekannt, dass bei rund 40‘000 Konten schädliche Aktivitäten stattgefunden hätten, bei etwa der Hälfte habe es Verluste gegeben. Die Bank sah sich gezwungen, Notmassnahmen zu ergreifen und die Transaktionen zu stoppen. Auch nach ein paar Monaten liegen noch viele Fragen zum genauen Vorgehen der Angreifer im Dunkeln. In Grossbritannien wurde Kritik an der fehlenden Kommunikation der Bank laut. Neben der Entschädigung betroffener Kunden könnten zusätzliche finanzielle Konsequenzen auf die Bank zukommen, da der britische Finanzmarktregulator die Bank je nach Verantwortung bei diesem Vorfall büssen kann.

Neben Angriffen, die es direkt auf die Bankensysteme und hier insbesondere das Zahlungssystem SWIFT[53] abgesehen haben, sind auch Geldautomaten mögliche Ziele von Cyber-Kriminellen. So wurde in Thailand im August 2016 in einer Reihe von Angriffen 12 Millionen Baht (umgerechnet CHF 343‘000) entwendet. In einer Analyse bezeichnete der Sicherheitsdienstleister «FireEye» eine Malware namens «Ripper»[54] als mit grosser Wahrscheinlichkeit für den Angriff verantwortlich. Ist diese im System des Geldautomaten installiert, muss die Schadsoftware mit einer manipulierten Chipkarte aktiviert werden. Das zeugt von einer bemerkenswerten Organisation der Kriminellen, die die Automaten zuerst kompromittieren, die Karten produzieren und am Ende physischen Zugang zu den Automaten haben müssen. Im

---

52 Siehe Schwerpunktskapitel 3

53 Siehe Halbjahresbericht 2016/1, Kapitel 5.4.1 «Cyber-Bankräuber stehlen 81 Millionen US-Dollar» https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2016-1.html (Stand: 28. Februar 2017).

54 https://www.fireeye.com/blog/threat-research/2016/08/ripper_atm_malwarea.html (Stand: 28. Februar 2017).

November hat die Sicherheitsfirma «Group-IB» einen Bericht über eine Tätergruppe namens «Cobalt» veröffentlicht, die hinter einer Reihe von Vorfällen in Europa vermutet wird. Dabei soll Geld direkt von Geldautomaten abgehoben worden sein, nachdem die Systeme verschiedener Banken kompromittiert worden waren[55]. Das Besondere ist, dass die Angriffe ohne physische Manipulation an den Bankomaten erfolgt sein sollen.

Wie bereits in früheren Berichten erwähnt, sind mit zunehmendem Erfolg auch Dienstleister im Zusammenhang mit digitalen Währungen das Ziel von Angriffen[56]. In der aktuellen Berichtsperiode war die Tauschbörse «Bitfinex» Opfer eines massiven Angriffs, der zum Diebstahl von 120 000 Bitcoin führte, was nach heutigem Kurs (Februar 2017) über 130 Millionen Franken entspricht. Damit der Angriff gelang, mussten die Täter das bei den Bitfinex-Kunden eingesetzte System mit Mehrfachunterschriften infizieren. Die Auswirkung des Diebstahls auf die Märkte liess nicht auf sich warten: Der Bitcoin-Kurs fiel nach der Meldung innert zwei Tagen um 13 Prozent.

Schliesslich hat sich auch der Trend zur Weiterentwicklung der Gruppe rund um die Malware «Carbanak» bestätigt. «Carbanak» war 2015 aufgrund massiver Angriffe auf Banken in den Schlagzeilen[57]. Laut den Forschern von Trustwave[58] nahm die Malware 2016 den Hotelleriesektor ins Visier. Unter Zuhilfenahme von Spear-Phishing-Angriffen sollten Verkaufsterminals infiziert werden, um anschliessend an die Kreditkartendaten heranzukommen.

Schlussfolgerung / Empfehlung:

Die in den letzten Jahren beobachteten Entwicklungen zeigen, dass der Endkunde nicht mehr die einzige potenzielle Schwachstelle in der Zahlungskette darstellt. Die Banken selbst sind über ihre internen Systeme oder ihre Geldautomaten oft direkt Ziel von Angriffen. Ebenfalls im Visier der Cyber-Kriminellen sind die neuen, ausschliesslich digitalen Währungen.

5.4.3 Ransomware-Markt nach wie vor sehr zersplittert

Bei der Ransomware war das zweite Halbjahr 2016 sehr dynamisch, wie aus Kapitel 4 dieses Berichtes hervorgeht. Zahlreiche gemeldete Vorfälle auf internationaler Ebene zeugen von vielfältigen Angriffen, Zielen und Vorgehensweisen. Die unternehmerische Logik, der diese Kriminellen folgen, wurde in unserem letzten Bericht dargestellt. Sie verbessern ihre

---

55 http://www.reuters.com/article/us-cyber-banks-atms-idUSKBN13G24Q (Stand: 28. Februar 2017).

56 Siehe dazu Halbjahresbericht 2014/1, Kapitel 4.10 «Angriffe auf virtuelle Währungen» https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2014-1.html (Stand: 28. Februar 2017).

57 Siehe Jahresbericht 2015/1, Kapitel 5.1.2 «Carbanak – der elektronische Banküberfall» https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2015-1.html (Stand: 28. Februar 2017).

58 https://www.trustwave.com/Resources/SpiderLabs-Blog/New-Carbanak-/-Anunak-Attack-Methodology/ (Stand: 28. Februar 2017).

Produkte laufend, suchen nach neuen Möglichkeiten und gehen sogar so weit, ihre Opfer zu «betreuen». Das geschieht zum Beispiel über FAQs[59] oder durch den Aufbau eines direkten Dialogs mit den Opfern. Der Ransomware-Markt mit vielen verschiedenen Gruppen und sehr unterschiedlichen Zielen und Vorgehensweisen befindet sich offenbar nach wie vor in der Konsolidierungsphase. Anders sieht es in anderen Cybercrime-Bereichen wie den Banking-Trojanern aus, wo mittlerweile einige gut etablierte Gruppen den grössten Marktanteil untereinander aufzuteilen scheinen.

Ein Fall, der im letzten Halbjahr hervorstach, betraf die Verkehrsbetriebe der Stadt San Francisco. Am 25. November 2016 legte ein Angriff das Ticketsystem lahm. Die Betreiber waren gezwungen, die Fahrgäste kostenlos zu transportieren, bis die Systeme mittels Backup wiederhergestellt waren. Der Angreifer hatte ausserdem behauptet, sensible Daten zu besitzen, was der Betreiber allerdings dementierte. Einige Tage später konnte mit zusätzlichen Informationen[60] ein genaueres Profil der Täterschaft eruiert werden, die offenbar auch für weitere Angriffe dieser Art verantwortlich war. Dabei sollen die Angreifer die Verkehrsbetriebe in San Francisco nicht gezielt im Visier gehabt, sondern einfach nach verwundbaren Systemen gesucht haben.

Schlussfolgerung:

Auch ursprünglich nicht gezielte Angriffe auf Büromatiksysteme können Kettenreaktionen auslösen und konkrete Schäden anrichten. Das Problem in solchen Fällen ist nicht so sehr, die Systeme insgesamt wiederherstellen zu können, sondern vor allem die dafür benötigte Zeit. Denn in dieser Zeit müssen provisorische Lösungen und ein wirksames Krisenmanagement eingerichtet werden.

5.5 Schwachstellen

Neben den zahlreichen Schwachstellen, die auch im zweiten Halbjahr 2016 veröffentlicht wurden, beleuchtet dieser Bericht drei Lücken, die exemplarisch die Verwundbarkeit unserer Systeme und Programme in drei verschiedenen Bereichen verdeutlichen.

5.5.1 Schwachstelle in USB-Schnittstelle

Jeder weiss, dass das Einstecken eines fremden USB-Stick in den eigenen Computer ein gewisses Risiko birgt und man dies besser unterlassen sollte. Betriebssysteme sind zudem mittlerweile so eingerichtet, dass sie Dateien auf einen USB-Stick nicht mehr automatisch ausführen, sondern zuerst den Benutzer fragen, welche Benutzeraktion er nun getätigt haben möchte. Was ist aber, wenn genau dieses Sicherheitselement ausgehebelt wird? Wie der Sicherheitsexperte Samy Kamkar in seinem Blog erklärt[61], kann das Einstecken eines

[59] Liste der Antworten auf Fragen, die sich das Opfer stellen könnten, sind in der Erpressungsnachricht aufgeführt.

[60] https://krebsonsecurity.com/2016/11/san-francisco-rail-system-hacker-hacked/ (Stand: 28. Februar 2017).

[61] https://samy.pl/poisontap/ (Stand: 28. Februar 2017).

von ihm präparierten USB-Geräts, Einfallstor für die Installation von Schadsoftware sein. Dies funktioniere selbst dann, wenn der Computer gesperrt ist. Die von ihm entwickelte Software gibt sich an der USB-Schnittstelle als Ethernetgerät aus und simuliert so eine Internet-over-USB-Verbindung. Auf diese Weise ist es nicht nur möglich, Cookies abzugreifen und den Internetverkehr zu kapern, es ist auch möglich, dauerhaft eine Backdoor zu installieren. Als einzige Voraussetzung für einen erfolgreichen Angriff muss auf dem anzugreifenden Computer ein Browser installiert sein.

Schlussfolgerung / Empfehlung:

Wie oft haben Sie an einer Konferenz, in der Bibliothek oder im Café den Computer während einer Mittags- oder Toilettenpause unbeaufsichtigt stehen lassen? Gerade bei gezielten Spionageversuchen wäre eine solche Gelegenheit für einen Angreifer optimal. Gegenmassnahmen sind, den Computer nie unbeaufsichtigt zu lassen oder die USB- und andere Schnittstellen zu deaktivieren.

5.5.2 Passwort-Manager - Eine zentrale Schwachstelle?

Diskussionen über den Gebrauch und die Sicherheit von Passwort-Managern gibt es viele. Die einen schwören auf diese Werkzeuge, da sie die Möglichkeit schaffen, sehr sichere, lange und komplizierte Passwörter zu verwenden. Einige Programme machen sogar auf einen fälligen Passwortwechsel aufmerksam oder schlagen ein sicheres Passwort vor. Merken muss man sich nur noch das Masterpasswort. Genau hier intervenieren die Skeptiker: Gelingt es nämlich einem Angreifer, die Datenbank zu stehlen oder das Masterpasswort zu knacken, wären auf einen Schlag alle Passwörter offengelegt. Eine Goldgrube für die Kriminellen. Noch schlimmer wäre es, wenn ein solcher Passwort-Manager eine Schwachstelle enthält. Genauso eine Schwachstelle wurde Ende Juli 2016 in der Firefox Erweiterung vom Programm «LastPass» gefunden. Bei einem Besuch einer präparierten Webseite soll es möglich gewesen sein, Zugriff auf Passwörter zu erhalten.[62] Die Schwachstelle wurde geschlossen.

5.5.3 Masque -Attacken im iOS

So genannte Masque Attacks wurden im Jahre 2014 zum ersten Mal gesehen und erlaubten es Hackern, eine echte App aus dem App Store von Apple durch eine manipulierte, unternehmenssignierte App mit demselben Bundle Identifier[63] zu ersetzen. Kriminelle können so bösartige Inhalte erstellen, die die gleiche Bundle ID wie das Original haben. Ist das Original beliebt, steigt natürlich auch die Reichweite und die Wahrscheinlichkeit, dass Nutzer diese manipulierte App herunterladen. Die dafür verantwortlichen Sicherheitslücken wurden zwar

[62] https://blog.lastpass.com/2016/07/lastpass-security-updates.html/ (Stand: 28. Februar 2017).

[63] Bundle Identifier ist ein Ausdruck zur Identifikation, der bei der Entwicklung einer App definiert und beibehalten wird, üblicherweise in der Form com.your-company.app-name.

von Apple geschlossen. Trendmicro bemerkte jedoch erneut zahlreiche manipulierte Apps[64]. In einem im November 2016 veröffentlichten Bericht wurde nun der Grund beschrieben. Kriminelle nutzen eine Funktionalität im Signierprozess aus, die es ermöglichte, eine Daten-Vererbung zu erreichen. Zusammen mit Apple wurde das Problem in iOS 10 beseitigt. Geräte unter iOS 9.3.5 oder älter sind allerdings immer noch angreifbar.

5.6 Präventive Massnahmen

Neben der Sensibilisierung der Nutzer sind Verhaftungen von Cyber-Kriminellen die effektivste präventive Massnahme bezüglich Internetkriminalität. Vielerorts herrscht die Meinung, das Identifizieren von Tätern und ihre Verhaftung seien hier schwierig bis unmöglich. Doch auch auf diesem Gebiet können Erfolge erzielt werden.

5.6.1 Avalanche-Netzwerk: Verhaftungen und Hausdurchsuchungen

Kriminelle haben die internationale kriminelle Netzwerk mit dem Namen Avalanche seit 2009 benutzt, um Malware-, Phishing- und Spam-Aktivitäten durchzuführen. Sie versendeten dabei wöchentlich mehr als 1 Million E-Mails mit schadhaften Anhängen oder Links an ahnungslose Opfer. Das Avalanche-Netzwerk wurde auch als Lieferplattform benutzt, um globale Massenangriffe zu steuern und um Finanzagenten zu rekrutieren. Der weltweite Gesamtschaden wird auf mehrere hundert Millionen Euro geschätzt, wobei der tatsächliche Schaden schwierig einzuschätzen ist, da diverse Malware-Familien über dieses Portal administriert wurden. Die Ermittlungen zur Plattform begannen im Jahre 2012. Am 30. November 2016 konnte dann die Infrastruktur ausser Betrieb genommen werden. Ermittler aus 30 Ländern waren bei der Deaktivierung der Plattform involviert. 5 Personen wurden verhaftet, 37 Hausdurchsuchungen durchgeführt und 39 Server beschlagnahmt. Die Strafverfolger konnten Opfer in über 180 Länder identifizieren. 221 Server wurden abgeschaltet, nachdem die entsprechenden Provider angeschrieben und um einen Take-Down gebeten wurden.[65]

Schlussfolgerung:

Das Beispiel zeigt, dass Strafverfolgungsbehörden insbesondere dann erfolgreich gegen Internetkriminalität vorgehen können, wenn sie international und auch mit privaten Firmen zusammenarbeiten.

64 http://blog.trendmicro.de/masque-attack-missbraucht-das-code-signing-in-ios-fuer-faelschungen/ (Stand: 28. Februar 2017).

65 http://www.staatsanwaltschaften.niedersachsen.de/download/113197 (Stand: 28. Februar 2017).

5.7 Weitere Themen

5.7.1 US-Aufsicht über die globale Internetadressverwaltung beendet

Am 30. September 2016 endete die historische Aufsichtsrolle der USA über die Verwaltungsstelle von Internetadressen (ICANN).[66] Die weltweite Internetadressverwaltung wird seither von einer global zusammengestellten Gemeinschaft beaufsichtigt, in der alle Interessensgruppen (Stakeholder) vertreten sind. Damit ist man der internationalen Multi-Stakeholder-Verwaltung des Domain-Namen- und Internetprotokoll-Adress-Systems (DNS) einen wichtigen Schritt nähergekommen.

Seit 1998 übte die US-Regierung gemäss dem sogenannten IANA-Vertrag[67] zwischen der US-Regierung und der ICANN die Oberaufsicht über die Verwaltung des DNS aus. Sie hatte insofern eine Prüfungs- und Validierungsfunktion bezüglich Änderungen der zentralen Datenbank aller Top-Level-Domains (z. B. .swiss, .com oder Ländercodes wie .ch). Der IANA-Vertrag lief Ende September 2016 aus und wurde nicht mehr erneuert.[68]

Der neue institutionelle Rahmen, der eine globale und demokratischere Aufsicht über das Internet gewähren soll, räumt den ICANN-Suborganisationen (inklusive dem Regierungsbeirat GAC, in welchem das BAKOM für die Schweiz einsitzt) gewisse Kontrollbefugnisse über den ICANN-Verwaltungsrat (das ICANN-Board) ein: Blockierung des Budgets, Genehmigung von Änderungen der Statuten, Abberufung des Verwaltungsrats sowie einzelner Ratsmitglieder.

Die ICANN hat ihren Sitz weiterhin in Kalifornien und untersteht somit primär US-Recht und den Eingriffsmöglichkeiten amerikanischer Behörden. Trotzdem ist dieser Schritt ein wichtiger Meilenstein in der Transition der ICANN hin zu einer globalen Institution. Weitere Schritte zur Stärkung ihrer Diversität und der Berücksichtigung der Bedürfnisse und Interessen der globalen Gemeinschaft sind aber erforderlich und werden vom BAKOM wie auch von anderen Schweizer Stakeholdern angeregt und unterstützt.

Die Internetnutzenden dürften allerdings von dieser Veränderung wenig bemerken, da sich die alltägliche technische Funktionsweise des DNS mit dieser Transition nicht verändert hat.

5.7.2 Internetknotenbetreiber DE-CIX will Überwachungsmassnahmen gerichtlich prüfen lassen

Die Betreibergesellschaft des Frankfurter Internetknotens DE-CIX hat Klage gegen die Bundesrepublik Deutschland beim Bundesverwaltungsgericht in Leipzig eingereicht.[69] Mit der

---

66 https://www.bakom.admin.ch/bakom/de/home/das-bakom/medieninformationen/bakom-infomailing/bakom-infomailing-43/us-aufsicht-ueber-die-globale-netzverwaltung-beendet.html;
https://digitalwatch.giplatform.org/processes/iana (Stand: 28. Februar 2017).

67 https://www.ntia.doc.gov/files/ntia/publications/ianacontract.pdf;
https://www.icann.org/en/system/files/files/contract-01oct12-en.pdf (Stand: 28. Februar 2017).

68 https://www.icann.org/news/announcement-2016-10-01-en (Stand: 28. Februar 2017).

69 https://www.de-cix.net/de/about-de-cix/media-center/press-releases/information-on-the-lawsuit-against-the-federal-republic-of-germany (Stand: 28. Februar 2017).

Klage wird beabsichtigt, die Praxis der strategischen Fernmeldeüberwachung durch den deutschen Bundesnachrichtendienst (BND) einer gerichtlichen Überprüfung zu unterziehen.

Die Klage stützt sich unter anderem auf eine gutachterliche Stellungnahme[70] von Dr. Hans-Jürgen Papier, einem Rechtsprofessor und ehemaligen Präsidenten des Bundesverfassungsgerichtes. Er hegt gewichtige Zweifel an der Rechtmäßigkeit der derzeitigen Praxis und macht geltend, dass das Telekommunikationsgeheimnis als Menschenrecht zu betrachten sei. Insofern steht dieses Recht auch ausländischen Personen zu und seine Einschränkung müsste formell-gesetzlich korrekt vorgesehen sein. Demgegenüber stellt sich die Bundesregierung auf den Standpunkt, dass es für die Überwachung von reinen Auslandsdaten kein Gesetz brauche.

In der Schweiz wurde mit dem Nachrichtendienstgesetz die formelle Grundlage für Kabelaufklärung von ausländischer Telekommunikation geschaffen. Jede diesbezügliche Massnahme muss vorgängig nicht nur vom Vorsteher des VBS, sondern auch vom Bundesverwaltungsgericht genehmigt werden und untersteht insofern einer politischen wie auch unabhängigen richterlichen Kontrolle.

6 Tendenzen und Ausblick

6.1 Cybercrime-as-a-Service und Cyber-Erpressung: ein Teufelskreis

Cybercrime-as-a-Service besteht aus einer Palette von Angeboten, um einen Cyber-Angriff ohne grosses Fachwissen durchzuführen. Diese Leistungen umfassen beispielsweise die Nutzung verschiedener Arten von Schadsoftware, das Mieten eines Botnetzes, die Durchführung eines DDoS-Angriffs oder eines Geldwäschereidienstes. Das Phänomen ist nicht neu, zahlreiche derartiger Dienste sind schon seit einigen Jahren auf Undergroundforen erhältlich. Sie waren aber bislang mehrheitlich geschlossenen cyber-kriminellen Gruppen vorbehalten, die damit eine Arbeitsteilung für mehr Effizienz sicherstellten. Diese Art von Organisation erlaubt es den Tätern, sich zu spezialisieren und ihre besonderen Kompetenzen zu verfeinern und sie anschliessend zum Verkauf oder Tausch anzubieten.

Mit dem Aufkommen der Cyber-Erpressung hat sich die Lage weiterentwickelt. Eine ganze Reihe von neuen Angeboten auf dem Markt führte zu einer Öffnung. Nehmen wir als Beispiel die erpresserischen DDoS-Attacken: Heute kann praktisch jeder einen Stresser/Booter-Dienst[71] kaufen, um einen solchen Angriff durchzuführen. Man muss nur das Ziel und eine Angriffsform – mit unterschiedlicher Wirksamkeit und unterschiedlichen Preisen – auswählen. Sogar die Verwendung eines Botnets mit «Mirai»-kompromittierten Objekten ist käuflich zu erwerben. Ähnlich sieht es bei der Ransomware aus. Diese Art von Angriffen ist «schlüs-

[70] http://rsw.beck.de/rsw/upload/NVwZ/NVwZ-Extra_2016_15.pdf; https://netzpolitik.org/2016/ex-praesident-des-bundesverfassungsgerichts-bnd-zugriff-auf-internet-knoten-wie-de-cix-ist-insgesamt-rechtswidrig/ (Stand: 28. Februar 2017).

[71] «DDoS-as-a-Service»-Dienstleistungen können gemietet werden und werden teils als «Stress-Test» deklariert online angeboten.

selfertig» erhältlich und kann auch von technisch nicht versierten Personen durchgeführt werden.

Angesichts dieser Situation stellt sich die Frage der Eigendynamik dieses Marktes: Hat eine grosse Nachfrage an solchen Dienstleistungen die Cyber-Kriminellen dazu veranlasst, diesen Markt zu schaffen oder ist es das Angebot, das Begehrlichkeiten geweckt und viele Täter angezogen hat? Die Antwort lautet wohl: Von beidem etwas! Es scheint sich hier also um einen Teufelskreis zu handeln.

Um die zu Grunde liegende Dynamik zu verstehen, muss zuerst untersucht werden, warum Cyber-Erpressung von Natur aus prädestiniert war, grosse Popularität bei einer breiten Palette von Tätern zu erlangen. Auf der einen Seite können durch diese Angriffsart wie schon mehrfach dargelegt grosse Summen rasch in Geld umgemünzt werden[72]: Eine Zahlung in Bitcoin wird direkt vom Opfer zum Täter geschickt und über einen Bitcoin-Mixing-Dienst «gewaschen», so dass der Geldfluss nicht mehr nachverfolgt werden kann. Zudem ist die Suche nach Zielen in Anbetracht der praktisch unendlichen Fülle an potenziellen Opfern sehr einfach. Auch wurde diese Angriffsart sehr stark mediatisiert und es sind zahlreiche Opfer und «kriminelle Erfolgsstories» bekannt, aber kaum Verurteilungen. Das erweckt bei Tätern den Eindruck, dass sie mit solchen Taten ungestraft davonkommen können, was zu einem starken Anreiz führt: Viele Täter im realen Raum, besonders aus der traditionellen Kleinkriminellenszene versuchen ihr Glück dann im virtuellen Raum. Sobald eine Nachfrage besteht, passt sich der Markt an und bietet eine ganze Palette von möglichst benutzerfreundlichen Dienstleistungen an. Dieses massgeschneiderte Angebot und seine grosse Verfügbarkeit wiederum geben dem Markt noch mehr Auftrieb und erlauben es noch mehr Tätern, in dieses Geschäft einzusteigen.

Das eigentliche Problem sind natürlich die Anbieter solcher Angebote. Offenbar soll es aber nur eine beschränkte Anzahl davon geben. Nach Schätzungen von Andy Archibald aus dem Jahre 2015, Direktor der britischen National-Crime Agency, sollen es nicht mehr als 100-200 Personen sein, die aber einen erheblichen Hebeleffekt auslösen.[73] Durch diese Öffnung und die grosse Anzahl an Tätern und verwendeten Produkten ist es ausserdem sehr schwierig, den Überblick über diese cyber-kriminellen Aktivitäten zu behalten. Dadurch wird auch die Arbeit der Strafverfolgungsbehörden stark erschwert.

6.2 Künftige Gestaltung der Zweifaktor respektive Mehrfaktor-Authentifizierung

Das amerikanische «National Institute of Standards and Technology (NIST)» kündigte im Juli 2016 an[74], in künftigen Richtlinien zu digitalen Identitäten die Authentifizierung via SMS nicht mehr zu empfehlen, ja sogar davon abzuraten. Während vielerorts noch versucht wird, die Internetnutzer zu einer konsequenten Nutzung der Zwei-Faktor-Authentifizierung zu bewe-

---

[72] Übergang von krimineller Tätigkeit zum Erhalt eines gewaschenen Geldbetrags, der direkt verwendet werden kann.

[73] https://www.connectinternetsolutions.com/cyber-crime/ (Stand: 28. Februar 2017).

[74] https://pages.nist.gov/800-63-3/sp800-63b.html (Stand: 28. Februar 2017).

gen, wird dem beliebtesten und einfach anzuwendenden zweiten Faktor SMS, die Eignung als solchen bereits wieder abgesprochen.

Um sich bei einem Internetdienst wie E-Banking sicher anmelden zu können, wird neben dem Passwort mindestens ein zweiter Authentifizierungsmechanismus eingesetzt. Idealerweise läuft dieser über einen zweiten, unabhängigen Kommunikationskanal, häufig eben via Mobiltelefon mit SMS. Da die meisten Mobiltelefone heutzutage Smartphones und somit kleine Computer sind, können diese mit Schadsoftware infiziert werden, welche unter anderem Nachrichten abfangen und an Betrüger weiterleiten kann. Zudem werden Bankgeschäfte heute vielfach direkt über das Smartphone getätigt, so dass Login und Zweitauthentifizierung über das gleiche Gerät erfolgen. Damit wird die zusätzliche Sicherheit ausgehebelt, die durch das SMS-Einmalpasswort gewährleistet werden sollte.

Aber nicht nur unsichere Endgeräte gefährden den SMS-Zweitfaktor: Auch auf Netzebene können diese Informationen abgegriffen oder umgeleitet werden. Schon vor Jahren machten Sicherheitsforscher auf die Sicherheitsprobleme des Protokolls SS7 aufmerksam[75], welches unter anderem Roaming zwischen verschiedenen Mobilfunkanbietern ermöglicht. Mobiltelefone können sich im Ausland bei fremden Netzen anmelden; der fremde Netzbetreiber meldet diesen Vorgang ins Heimatnetz des Abonnenten, das danach Anrufe und SMS-Nachrichten zur Auslieferung ans fremde Netz übermittelt. Dieser Vorgang kann vorgetäuscht werden, ohne dass sich das Mobiltelefon im Ausland befindet. Die SMS-Nachrichten werden dann zu Netzbetreibern im Ausland umgeleitet und können dort ausgelesen werden. Dies funktioniert, weil das zugrundeliegende SS7-Protokoll ursprünglich offen konzipiert wurde. Man ging von einem Grundvertrauen zwischen allen Mobilfunkprovidern aus. Mit der wachsenden Anzahl von Anbietern in aller Welt besteht aber mittlerweile die Möglichkeit, dass sich einzelne Firmen nicht an alle Regeln halten und unter Umständen betrügerische Aktivitäten nicht verhindern oder sogar mit Betrügern zusammenarbeiten.

Auf der nicht technischen Seite sind Fälle unter zu Hilfenahme von Social Engineering möglich. In einem konkreten Fall wurden hilfreiche Telekom-Kundendienstmitarbeiter von Betrügern überzeugt, eine Ersatz-SIM-Karte an eine für die Kriminellen zugängliche Adresse zu senden[76], was in der Folge die Übernahme von mehreren Online-Konten ermöglichte.

Die Mehrfaktor-Authentifizierung basiert auf mindestens zwei Komponenten. Dies kann entweder Wissen sein (z. B. ein Passwort), Besitz (z. B. eine Schlüsselkarte) oder auch ein einzigartiges Merkmal (z. B. ein Fingerabdruck). Wegen der zunehmenden Verschmelzung von Telefon und Computer sowie der Zusammenführung von Kommunikationsnetzen kann das Mobilfunknetz nicht mehr als eigenständiger und vom Internet unabhängiger Kommunikationskanal betrachtet werden. Das SMS erfüllt so die Komponente «Besitz» nur noch beschränkt. Entsprechend sollte, wenn möglich, bei Online-Diensten – insbesondere solchen mit Schadenspotential – auf andere Authentifizierungsmethoden gewechselt werden. Ein Beispiel für eine sichere Authentifizierungsmethode basierend auf einem Mobiltelefon sind

---

75 https://www.blackhat.com/presentations/bh-europe-07/Langlois/Presentation/bh-eu-07-langlois-ppt-apr19.pdf (Stand: 28. Februar 2017).

76 http://www.forbes.com/sites/laurashin/2016/12/20/hackers-have-stolen-millions-of-dollars-in-bitcoin-using-only-phone-numbers/#42981a5c22db (Stand: 28. Februar 2017).

bei korrekter Verwendung Smartphone-Applikationen, die ein vom Dienstanbieter verschlüsseltes Einmalpasswort decodieren. Eine weitere Alternative ist das System Mobile ID, bei dem die Authentifizierungsmerkmale bereits auf der SIM-Karte verschlüsselt werden. Da Dienste immer häufiger auf dem Smartphone selbst genutzt werden, empfehlen sich für die Authentifizierung davon unabhängige Elemente wie separate Hardware-Sicherheitsschlüssel, deren Einsatz von vielen grossen Web-Diensten bereits angeboten wird[77].

Schlussfolgerung:

Sollte nun Ihr Online-Dienst immer noch SMS zur Authentifizierung oder für die Passwortrückstellung verwenden, müssen Sie aber nicht in Panik verfallen. Auch wenn diese Methode mittlerweile einige Schwachstellen hat und nicht mehr die sicherste Variante ist, ist die Verwendung von zwei und mehr Faktoren immer noch um ein Vielfaches sicherer, als ein Schutz, der nur auf Benutzername und Passwort beruht.

6.3 Sicherheitstechnologien unter konstantem Druck

Um die Sicherheit zu erhöhen, kommen neben den üblichen Sicherheitsprodukten wie Antiviren-Scannern, Micro-Virtualisierungsansätzen und Host Intrusion Detection/Prevention-Systemen, häufig Windows Bordmittel wie «AppLocker» und «EMET»[78] zum Einsatz. Diese beiden Programme erhöhen die Sicherheit von Windows-Systemen entscheidend. So kann mit Hilfe von «AppLocker» genau festgelegt werden, in welchem Verzeichnis welche Programme ausgeführt werden dürfen, was die Hürde für den Angreifer erhöht, eine initiale Infektion erfolgreich durchführen zu können. Auf der anderen Seite erschwert «EMET» das Ausführen von Exploits.

Programmierer von Schadsoftware versuchen natürlich, diese Schutzmechanismen zu umgehen. Diese Tatsache ist zwar keine neue Erkenntnis und wurde bereits mehrfach beschrieben[79,80], seit dem letzten Herbst ist aber eine deutliche Zunahme solcher Angriffe zu verzeichnen. Angreifer betten beispielsweise Makrocode in Office-Dokumente ein, welcher ein PowerShell-Script enthält. Dabei nutzt der Angreifer die Tatsache aus, dass in den meisten Umgebungen PowerShell-Scripts zugelassen sind. Andere Ansätze verwenden regsvr32 und Scriptlets, um dasselbe Ziel zu erreichen. Das Angler Exploit-Kit hat zudem die Fähigkeit erhalten, Exploits so zu starten, dass die Schutzwirkung von EMET ins Leere läuft. Dabei

---

77 http://fc16.ifca.ai/preproceedings/25_Lang.pdf (Stand: 28. Februar 2017).

78 Das Microsoft Enhanced Mitigation Experience Toolkit (EMET) enthält unter anderem mit die Funktionen «Address Space Layout Randomization (ASLR)» und «Data Execution Prevention (DEP)»

79 http://subt0x10.blogspot.ch/2016/04/bypass-application-whitelisting-script.html (Stand: 28. Februar 2017).

80 http://leastprivilege.blogspot.ch/2013/04/bypass-applocker-by-loading-dlls-from.html (Stand: 28. Februar 2017).

rufen die Angreifer Routinen zur Speicherallozierung auf, welche direkt den angegriffenen Programmen (z. B. Flash) gehören.[81]

Schlussfolgerung / Empfehlung:

Die neuen Schutztechnologien werden immer häufiger eingesetzt und sind gegen viele bisherige Angriffsvektoren wirksam. Angreifer sind aber fähig und willens, für jeden neuen Sicherheitsmechanismus eine Umgehungsmöglichkeit zu suchen (und zu finden). Dennoch bleibt der Einsatz dieser Schutzmechanismen sinnvoll, da sie den Aufwand für die Angreifer erhöhen und nach wie vor eine Vielzahl von aktuell genutzten Angriffsvektoren unbrauchbar machen. Wir empfehlen aber, die Möglichkeiten, welche PowerShell für Angreifer bietet, genau im Auge zu behalten und beispielsweise entsprechende Sicherungsmassnahmen, wie eine digitale Signierung von allen Scripts und Makros einzuführen. Es gibt auch verschiedene Behaviour Blocking Engines, die solche Angriffe zumindest teilweise zu erkennen vermögen. Ebenso hat Microsoft weitere Funktionen im DeviceGuard von Windows 10 implementiert, welche die Hürde für Angreifer ebenfalls erhöhen.

[81] https://www.fireeye.com/blog/threat-research/2016/06/angler_exploit_kite.html (Stand: 28. Februar 2017).

7 Politik, Forschung, Policy

7.1 CH: Parlamentarische Vorstösse

Geschäft	Nummer	Titel	Eingereicht von	Datum Einreichung	Rat	Amt	Stand Beratung & Link
Ip	16.4115	E-ID. Elektronische Identität	Rosmarie Quadranti	16.12.2016	NR	EJPD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164115
Mo	16.4089	Stärkung der sicherheitspolitischen Instrumente im Ausland	Damian Müller	15.12.2016	SR	VBS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164089
Po	16.4073	Cyber-Risiken. Für einen umfassenden, unabhängigen und wirksamen Schutz	Roger Golay	15.12.2016	NR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164073
Po	16.3706	Digitale Wirtschaft und Arbeitsmarkt	Beat Vonlanthen	27.09.2016	SR	WBF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163706
Ip	16.3694	Sind wir fit für die Arbeitswelt 4.0?	Stefan Müller-Altermatt	22.09.2016	NR	WBF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163694
Ip	16.4161	Julian Assange - ein Verteidiger der Menschenrechte, den es zu schützen gilt?	Jean-Luc Addor	16.12.2016	NR	EDA	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164161
Ip	16.4131	Wie kann die Schweiz an der Forschung zu künstlicher Intelligenz teilnehmen, damit universelle moralische Werte in der digitalen Welt gut vertreten sind?	Claude Béglé	16.12.2016	NR	WBF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164131
Ip	16.4012	Duale Bildung. Wie bleiben wir an der Weltspitze?	Claude Béglé	14.12.2016	NR	WBF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164012
Ip	16.4001	Airbnb and Co. Gelten in Bezug auf die Haftung die Regeln der Internetplattform oder die Schweizer Gesetze?	Carlo Sommaruga	14.12.2016	NR	EJPD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164001
Ip	16.3960	Anpassung unseres Bildungssystems an das von der Digitalisierung geprägten neue Weltbild	Claude Béglé	08.12.2016	NR	WBF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163960

Po	16.3914	Wie bringt man Ethik in die Algorithmen?	Claude Béglé	28.11.2016	NR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163914
Mo	16.3902	Verbot von Knebelverträgen der Online-Buchungsplattformen gegen die Hotellerie	Pirmin Bischof	30.09.2016	SR	WAK-SR	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163902
Ip	16.3861	Gründung einer Expertengruppe «Digitale Schweiz»	Fathi Derder	30.09.2016	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163861
Ip	16.3837	Zivile Drohnen. Kritische Infrastrukturen besser schützen	Manuel Tornare	30.09.2016	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163837
Ip	16.3829	Cybersecurity-Einheit des Bundes und Darknet	Christian Imark	29.09.2016	NR	EJPD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163829
Fr	16.1058	Entwicklung des Werbemarktes. Abfluss von Geldern ins Ausland und Finanzierung der Medien	Jacqueline Badran	28.09.2016	NR	EJPD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20161058
Ip	16.4003	Digitalisierung. Datenstandort Schweiz nicht gefährden	Marcel Dobler	14.12.2016	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164003
Ip	16.4002	Verkehrsperspektiven 2040. Wo bleibt die Digitalisierung im Referenzszenario?	Thierry Burkart	14.12.2016	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164002
Po	16.3918	Digitale Revolution. Wie können die Offliner integriert werden?	Claude Béglé	29.11.2016	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163918
Po	16.3789	Digitalisierung im öffentlichen Verkehr. Herausforderungen im Bereich Datenschutz	Evi Allemann	29.09.2016	NR		https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163789
Fr	16.1059	Angriffe von Terroristen. Sicherheit der Atomkraftwerke?	Balthasar Glättli	28.09.2016	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20161059

Ip	16.4050	Digitalisierung des Schweizer Zollwesens. Reduktion des administrativen Aufwands	Viola Amherd	15.12.2016	NR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164050
Po	16.4078	Digitalisierung. Papierloses E-Voting ermöglichen	Marcel Dobler	15.12.2018	NR	BK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164078
Mo	16.4011	Digitalisierung. Keine Doppelspurigkeiten bei der Datenerhebung	Daniela Schneeberger	14.12.2016	NR	EDI	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164011
Fr	16.5429	Tisa-Informationsleck. Angriffe auf Datenschutz, Netzneutralität und Open-Source-Software	Balthasar Glättli	21.09.2016	NR	WBF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20165429

7.2 Strategie «Digitale Schweiz»

Der Bundesrat hat 2016 die Strategie «Digitale Schweiz» verabschiedet. Diese löst die bundesrätliche Strategie für eine Informationsgesellschaft in der Schweiz von 2012 ab.

Das Papier legt im Rahmen des Ansatzes «free, open and secure Internet» die strategischen Ziele für den Teil des «free and open Internet» für die Schweiz fest.

Die Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) dagegen fokussiert auf den Bereich «secure Internet» und legt die strategischen Ziele zu den Themen Sicherheit, Vertrauen, Verlässlichkeit und Widerstandsfähigkeit für die Schweiz fest.

Im Zentrum der Strategie «Digitale Schweiz» steht die konsequente Nutzung der Chancen der Digitalisierung, damit sich die Schweiz als attraktiver Lebensraum und innovativer, zukunftsorientierter Wirtschafts- und Forschungsstandort positionieren kann. Dabei strebt der Bundesrat die Kernziele «Innovation, Wachstum und Wohlstand in der digitalen Welt», «Chancengleichheit und Partizipation aller», «Transparenz und Sicherheit» sowie «Beitrag zur nachhaltigen Entwicklung» an und legt die Grundsätze fest, nach denen sich der digitale Wandel vollziehen soll.

7.3 Schweizer Teilnahme an der Übung «Cyber Europe 2016»

Mit ihrer vierten Ausgabe hat sich «Cyber Europe» mittlerweile zu einer der grössten und umfassendsten Cyber-Übungen der Welt entwickelt. Die zwei-jährliche Übung wird jeweils von der ENISA organisiert und fokussiert sowohl auf den technischen als auch auf den operativen Aspekt einer Cyber-Krise. 29 EU-Mitgliedstaaten und EFTA-Länder, darunter auch die Schweiz, beteiligten sich an der letztjährigen Ausgabe. Der erste technische Teil startete bereits im April 2016 und ermöglichte es Mitarbeitenden im Cybersecurity-Bereich, komple-

xe, innovative und realistische technische Vorfälle zu verschiedensten Themen zu analysieren. Am 13. und 14. Oktober folgte dann der operative Teil, an welchem Experten von mehr als 300 Organisationen unter anderem aus den Bereichen Telekommunikation, Cloud Service Provider, Cybersecurity Software und Service Provider, Cybersecurity Abteilungen, Ministerien und EU-Institutionen teilnahmen. Cyber Europe 2016 malte ein sehr düsteres Szenario, dass von den Stromausfällen in der Ukraine im Dezember 2015 inspiriert wurde. Es behandelte Themen wie «Internet of Things», «Dronen», «Cloud Computing», «Mobile Malware» und «Ransomware». Zum ersten Mal wurde das ganze Szenario mit Schauspielern, Journalisten, simulierten Firmen und Sozialen Medien ergänzt, um dem Aspekt der «Public Affairs» genügend Rechnung zu tragen. Das Cyber Europe Motto «stronger together» drückt aus, dass die Zusammenarbeit auf allen Ebenen der Schlüssel zu einer erfolgreichen Bewältigung von grossen, grenzüberschreitenden Cyber-Vorfällen ist.

8 Publizierte MELANI Produkte

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

8.1 GovCERT.ch Blog

8.1.1 Tofsee Spambot features .ch DGA - Reversal and Countermesaures

22.12.2016 - The malware, which MELANI / GovCERT identified as Tofsee, has tried to spam out hundreds of emails within a couple of minutes. However, this wasn't the reason why it popped up on the radar. The reason why this particular sample caught our attention were the domains queried by the malware. The domains appear to be algorithmically generated, and about half of the domains use the country code top level domain (ccTLD) of Switzerland.

➔ https://www.govcert.admin.ch/blog/26/tofsee-spambot-features-.ch-dga-reversal-and-countermesaures

8.1.2 When Mirai meets Ranbyus

15.12.2016 - In the past weeks, MELAN / GovCERT has seen a rise of malicious Microsoft office documents that are being spammed out to Swiss internet users with the aim to infect them with a malicious software (malware) called Dridex. Dridex is an ebanking Trojan which is already around for some time now.

➔ https://www.govcert.admin.ch/blog/23/dridex-targeting-swiss-internet-users

8.1.1 SMS spam run targeting Android Users in Switzerland

13.07.2016 - MELANI / GovCERT.ch received several reports today about malicious SMS that have been sent to Swiss mobile numbers. The SMS is written in German and claims to come from the Swiss Post. But in fact, the SMS has been sent by hackers with the aim to infect Smartphones in Switzerland with a Trojan horse.

➔ https://www.govcert.admin.ch/blog/24/sms-spam-run-targeting-android-users-in-switzerland

8.1.2 Dridex targeting Swiss Internet Users

08.07.2016 - In the past weeks, MELANI / GovCERT has seen a rise of malicious Microsoft office documents that are being spammed out to Swiss internet users with the aim to infect them with a malicious software (malware) called Dridex. Dridex is an ebanking Trojan which is already around for some time now. The attackers are operating various botnets with Dridex infected computers. While most of these botnets do have a strong focus on financial institu-

tions from abroad (such as US or UK), one particular botnet is also targeting financial institutions in Switzerland.

➔ https://www.govcert.admin.ch/blog/23/dridex-targeting-swiss-internet-users

8.2 MELANI Newsletter

Im zweiten Halbjahr 2016 hat MELANI folgende Newsletter publiziert:

8.2.1 Social Engineering: Neue Angriffsmethode richtet sich gegen Firmen

20.01.2017 - In den letzten Tagen wurden der Melde- und Analysestelle Informationssicherung MELANI mehrere Fälle gemeldet, bei denen Betrüger Firmen anrufen, sich als Bank ausgeben und behaupten, dass am nächsten Tag ein E-Banking-Update durchgeführt würde. Sie verlangen, dass an diesem Termin verschiedene Mitarbeitende der Finanzabteilung anwesend sind. Dies hat den Zweck, das Sicherheitselement «Kollektivunterschrift» auszuhebeln und so eine betrügerische Zahlung auszulösen.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/social-engineering--neue-angriffsmethode-richtet-sich-gegen-firmen.html

8.2.2 E-Banking: Angreifer zielen auf mobile Authentifizierungsmethoden

29.11.2016 - In den vergangenen Wochen wurden MELANI mehrere Fälle gemeldet, bei welchen es Hackern gelang, mittels Social Engineering Opfer dazu zu animieren, betrügerische Zahlungen im E-Banking zu visieren.

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

8.2.3 Cyber-Erpressung: Schwerpunktthema im Halbjahresbericht MELANI

26.10.2016 - Der heute veröffentlichte 23. Halbjahresbericht der Melde- und Analysestelle Informationssicherung (MELANI) zeigt die wichtigsten Cyber-Vorfälle der ersten Jahreshälfte 2016 national und international auf. Der Bericht widmet sich im Schwerpunktthema den vermehrten Angriffen durch Cyber-Erpressung. Ausserdem stehen verschiedene Datenabflüsse im Fokus.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/halbjahresbericht-2016-1.html

8.2.4 Offline Zahlungs-Software im Visier von Hackern - Schweizer Unternehmen betroffen

25.07.2016 - In den letzten Tagen hat MELANI mehrere Fälle der Schadsoftware Dridex beobachtet, die sich gegen Offline Zahlungs-Softwarelösungen richtet. Solche Software wird in

der Regel von Unternehmen verwendet, um eine grössere Anzahl an Zahlungen via Internet an eine oder mehrere Banken zu übermitteln. Werden Computer, welche solche Software verwenden, kompromittiert, sind die potenziellen Schäden entsprechend hoch. MELANI empfiehlt Unternehmen deshalb dringend, Computer, welche für den Zahlungsverkehr verwendet werden, entsprechend zu schützen.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/offline-payment-software.html

8.2.5 Vermehrt schädliche Office-Dokumente im Umlauf

08.07.2016 - In den vergangenen Wochen ist eine Vielzahl von Meldungen bei der Melde- und Analysestelle Informationssicherung MELANI über schädliche Microsoft Office-Dokumente eingegangen, welche via E-Mail verbreitet werden und das Ziel haben, den Computer des Opfers mit Schadsoftware (Malware) zu infizieren. MELANI warnt deshalb explizit vor dem Öffnen solcher Office-Dokumente und empfiehlt Internet-Benutzern erhöhte Wachsamkeit im Umgang mit Office-Dokumenten sowie keine Office-Makros auszuführen.

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

8.3 Checklisten und Anleitungen

Im ersten Halbjahr 2016 hat MELANI keine neuen Checklisten und Anleitungen publiziert.

9 Glossar

Begriff	Beschreibung
Accessibility Service	Ein Accessibility Service ist eine Applikation welche ein Benutzerschnittstelle zur Verfügung stellt um Benutzer mit einem Handicap oder Benutzer, die zwischenzeitlich nicht voll mit Ihrem Gerät interagieren können, zu unterstützen.
Advanced Persistent Threats (APT)	Diese Bedrohung führt zu einem sehr hohen Schaden, der auf eine einzelne Organisation oder auf ein Land wirkt. Der Angreifer ist bereit, sehr viel Zeit, Geld und Wissen in den Angriff zu investieren und verfügt in der Regel über grosse Ressourcen.
App	Der Begriff App (von der englischen Kurzform für Application) bezeichnet im Allgemeinen jede Form von Anwendungsprogrammen. Im Sprachgebrauch sind damit mittlerweile jedoch meist Anwendungen für moderne

	Smartphones und Tablet-Computer gemeint.
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.
Barcode	Als Strichcode, Balkencode oder Barcode wird eine optoelektronisch lesbare Schrift bezeichnet, die aus verschieden breiten, parallelen Strichen und Lücken besteht.
Bitcoin	Bitcoin ist ein weltweit verwendbares dezentrales Zahlungssystem und der Name einer digitalen Geldeinheit.
Booter / Stresser	Werkzeuge, welche gegen Bezahlung DDoS Angriffe auslösen («DDoS as a service»).
Browser	Computerprogramme, die vorwiegend dazu verwendet werden, verschiedene Inhalte im World Wide Web anzuzeigen. Die bekanntesten Browser sind Internet Explorer, Opera, Firefox und Safari.
Brute Force	Die Brute-Force-Methode ist eine Lösungsmethode für Probleme aus den Bereichen Informatik, Kryptologie und Spieltheorie, die auf dem Ausprobieren aller möglichen Fälle beruht.
Bundle Identifier	Bundle Identifier ist ein Ausdruck zur Identifikation, der bei der Entwicklung einer App definiert und beibehalten wird, üblicherweise in der Form com.your-company.appname.
Command & Control Server	Die meisten Bots können von einem Botmaster über einen Kommunikationskanal überwacht werden und Befehle empfangen. Dieser wird als Command and Control-Server bezeichnet.
Cookies	Kleine Textdateien, die beim Besuch einer Webseite auf dem Rechner des Benutzers abgelegt werden. Mit Hilfe von Cookies lassen sich beispielsweise persönliche Einstellungen einer Internet-Seite speichern. Allerdings können sie auch dazu missbraucht werden, die Surfgewohnheiten des Benutzers zu erfassen und damit ein Nutzerprofil zu erstellen.

DDoS	Distributed-Denial-of-Service Attacke Eine DoS-Attacke, bei der das Opfer von vielen verscheiden Systemen aus gleichzeitig angegriffen wird.
Defacement	Verunstaltung von Webseiten.
Domain Generation Algorhytmus	Domain Generation Algorithmen werden von zahlreichen Schadsoftwarefamilien verwendet um periodisch eine grosse Anzahl Domänennamen zu generieren, welche dann als Kontaktpunkt zu Command & Control Servern verwendet werden.
Domain Name System	Domain Name System. Mit Hilfe von DNS lassen sich das Internet und deren Dienste benutzerfreundlich nutzen, da die Benutzer anstelle von IP-Adressen Namen verwenden können (z.B. www.melani.admin.ch).
Fast Flux	Fast Flux ist eine von Botnetzen genutzte DNS-Technik, mit der der Standort von Webservern verschleiert werden kann.
e-Currency Dienste	Ein monetärer Wert in Form einer Forderung gegen die ausgebende Stelle, der auf einem Datenträger gespeichert ist, gegen Entgegennahme eines Geldbetrags ausgegeben wird, dessen Wert nicht geringer ist als der ausgegebene monetäre Wert, von anderen Unternehmen als der ausgebenden Stelle als Zahlungsmittel akzeptiert wird
Ethernet	Ethernet ist eine Technologie für kabelgebundene Datennetze
Google-Rank	Der PageRank-Algorithmus ist ein Verfahren, eine Menge verlinkter Dokumente, wie beispielsweise das World Wide Web, anhand ihrer Struktur zu bewerten bzw. zu gewichten.
Grey-Hat	Grey-Hats verstossen möglicherweise gegen Gesetze oder restriktive Auslegungen der Hacker-Ethik, allerdings zum Erreichen eines ethischen Ziels.
Hacker-Ethik	Die Hackerethik bezeichnet eine Sammlung ethischer Werte, die für die Hackerkultur ausschlaggebend sein sollen. Zentrale Werte sind Freiheit, Kooperation, freiwillige und selbstgewählte Arbeit sowie Teilen.
ICANN	Internet Corporation for Assigned Names and Numbers (ICANN) Die ICANN ist eine privatrechtliche Non-Profit-Organisation mit Sitz in der kalifornischen Küstenkleinstadt Marina del Rey. ICANN entscheidet über die

	Grundlagen der Verwaltung der Top-Level-Domains. Auf diese Weise koordiniert ICANN technische Aspekte des Internets, ohne jedoch verbindliches Recht zu setzen.
Internet der Dinge	Der Begriff Internet der Dinge beschreibt, dass der Computer in der digitalen Welt zunehmend von «intelligenten Gegenständen» bis hin zu «KI», künstlicher Intelligenz ergänzt wird.
Javascript	Eine objektbasierte Scripting-Sprache zur Entwicklung von Applikationen. JavaScripts sind im HTML-Code integrierte Programmteile, die bestimmte Funktionen im Internet Browser ermöglichen. Ein Beispiel kann das Kontrollieren von Benutzereingaben bei einem Webformular sein. So kann überprüft werden, ob alle eingegebenen Zeichen bei geforderter Angabe einer Telefonnummer auch wirklich Zahlen sind. Wie ActiveX Controls werden JavaScripts auf dem Rechner des Webseitenbesuchers ausgeführt. Neben nützlichen, lassen sich leider auch schädliche Funktionen programmieren. Im Gegensatz zu ActiveX werden JavaScripts von allen Browsern unterstützt.
Kontroll- oder Steuerungssysteme (IKS)	Kontroll- oder Steuerungssysteme (IKS) bestehen aus einem oder mehreren Geräten, welche das Verhalten von anderen Geräten oder Systemen steuern, regeln und/oder überwachen. In der industriellen Produktion ist der Begriff «Industrielle Kontrollsysteme» (engl. Industrial Control Systems, ICS) geläufig.
Makro-Malware	Schadsoftware, die mittels Makro installiert wird. Ein Makro ist eine Folge von Anweisungen, die mit nur einem einfachen Aufruf ausgeführt werden können.
Malware	Oberbegriff für Software, die schädliche Funktionen auf einem Rechner ausführt (wie beispielsweise Viren, Würmer, Trojanische Pferde).
mobileTAN	Mobile TAN besteht aus der Einbindung des Übertragungskanals SMS. Dabei wird dem Onlinebanking-Kunden nach Übersendung der ausgefüllten Überweisung im Internet seitens der Bank per SMS eine nur für diesen Vorgang verwendbare TAN auf sein Mobiltelefon gesendet.
Offline Zahlungssoftware	Zahlungserfassungssoftware die lokal installiert ist.
Phishing	Mittels Phishing versuchen Betrüger, an vertrauliche Daten von ahnungslosen Internet-Benutzern zu gelangen. Dabei kann es sich beispielsweise um Kontoinformatio-

	nen 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.
Plaintext	Mit Plaintext werden Daten bezeichnet, die direkt unter Verwendung einer Zeichenkodierung in Text umgesetzt werden können.
Plug-Ins	Ein Plug-in ist ein optionales Software-Modul, das eine bestehende Software erweitert bzw. verändert.
Portscanner	Ein Portscanner ist eine Software, mit der überprüft werden kann, welche Dienste ein mit TCP oder UDP arbeitendes System über das Internetprotokoll anbietet.
PowerShellScript	PowerShell ist ein plattformübergreifendes Framework von Microsoft zur Automatisierung, Konfiguration und Verwaltung von Systemen, bestehend aus einem Kommandozeileninterpreter, sowie einer Skriptsprache.
Proxy	Ein Proxy ist eine Kommunikationsschnittstelle in einem Netzwerk. Er arbeitet als Vermittler, der auf der einen Seite Anfragen entgegennimmt, um dann über seine eigene Adresse eine Verbindung zur anderen Seite herzustellen.
QR-Code	Der QR-Code (Quick Response Code) besteht aus einer quadratischen Matrix aus schwarzen und weißen Quadraten, die die kodierten Daten binär darstellen.
RFID-Code	RFID bezeichnet eine Technologie für Sender-Empfänger-Systeme zum automatischen und berührungslosen Identifizieren und Lokalisieren von Objekten und Lebewesen mit Radiowellen.
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.
Schadsoftware	Oberbegriff für Software, die schädliche Funktionen auf einem Rechner ausführt (wie beispielsweise Viren, Würmer, Trojanische Pferde).
Schwachstelle / Lücke	Schwachstelle in Hard- oder Software, über die Angreifer Zugriff auf ein System erlangen können.

SHA	Der Begriff secure hash algorithm (SHA) bezeichnet eine Gruppe standardisierter kryptologischer Hashfunktionen.
SIM-Karte	Die SIM-Karte (englisch: Subscriber Identity Module) ist eine Chipkarte, die in ein Mobiltelefon eingesteckt wird und zur Identifikation des Nutzers im Netz dient.
Smartphone	Ein Smartphone ist ein Mobiltelefon, das mehr Computerfunktionalität und -konnektivität als ein herkömmliches fortschrittliches Mobiltelefon zur Verfügung stellt.
SMS	Short Message Service Dienst zum Versenden von Kurzmitteilungen (maximal 160 Zeichen) an Mobiltelefonbenutzer.
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.
SS7	Das Signalling System #7 (SS7) ist eine Sammlung von Protokollen und Verfahren für die Signalisierung in Telekommunikationsnetzen. Es kommt im öffentlichen Telefonnetz, in Zusammenhang mit ISDN, Fest- und Mobilfunknetz und seit etwa 2000 auch verstärkt in VoIP-Netzen zum Einsatz.
Take-Down	Ausdruck, der verwendet wird, wenn ein Provider, eine Seite aufgrund betrügerischen Inhalts vom Netz nimmt.
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.
Verschlüsselungstrojaner / 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.
Webbrowser	Computerprogramme, die vorwiegend dazu verwendet

	werden, verschiedene Inhalte im World Wide Web anzuzeigen. Die bekanntesten Browser sind Internet Explorer, Firefox und Safari.
WLAN	WLAN (oder Wireless Local Area Network) steht für drahtloses lokales Netzwerk.
Zweifaktorauthentifizierung	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.)