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/I (Januar – Juni)

28. OKTOBER 2016

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

1 Übersicht / Inhalt

2 Editorial

Martin Sibler, seit 2001 bei Swiss Re in diversen Bereichen der Informationssicherheit tätig

Liebe Leserinnen, liebe Leser

Information ist für die Versicherungsbranche ein zentrales Element der Wertschöpfungskette. Die Bewertung von zu versichernden Risiken benötigt nebst mathematischen Formeln auch historische Informationen zu dem entsprechenden Ereignis – zum Beispiel ein Hurrikan in Florida –, damit die Wahrscheinlichkeit des Eintreffens berechnet werden kann. Zudem werden oftmals diverse Angaben von Kunden, zum Beispiel die Lage der zu versichernden Gebäude, für diese Analysen verwendet. Dabei müssen die Integrität, die Vertraulichkeit sowie die Verfügbarkeit dieser Information gewährleistet sein. Die Verfügbarkeit der richtigen Informationen zum richtigen Zeitpunkt ermöglicht, das Risiko besser zu verstehen und zu einem gewissen Masse vorauszusagen.

Bei der Bewertung von Cyber-Risiken besteht eine ähnliche Ausgangslage, jedoch gibt es diverse dynamische Faktoren, die es schwieriger machen, das Risiko einzuschätzen. Zum einen gibt es wenig umfangreiche Informationen zu früheren Ereignissen und zum anderen ist diese Information oft nicht mehr relevant, da sich die Technologie und die Art der Attacken in der Zwischenzeit geändert haben. Bei Hurrikans sind die Rahmenbedingen immer etwa gleich: die Windstärke ist unterschiedlich und der Pfad der Verwüstung ändert sich, doch es gibt diverse Aufzeichnungen von Hurrikans, welche berücksichtigt werden können. Bei einem Ereignis im Cyberspace ändern sich nicht nur die Windstärke und der Pfad, sondern anstelle eines Hurrikans ist man plötzlich mit einem Erdbeben konfrontiert. Der Vergleich hinkt etwas, doch zeigt er auf, dass man sich bei Cyber-Risiken auf das Unerwartete einstellen muss, denn die Informationen über Hacker-Angriffe der letzten 20 Jahre helfen nur bedingt, um die Bedrohungslage einzuschätzen.

Aus diesem Grund ist Cyber Intelligence, das heisst der zeitnahe Austausch von aktuellen Angriffen, besonders hilfreich, um abzuwägen, ob man sich vor einem Hurrikan oder einem Erdbeben schützen muss. In diesem Bereich erbringt MELANI einen wichtigen Service, welcher der Schweizer Wirtschaft hilft, sich besser vor solchen Risiken zu schützen.

Ich wünsche viel Spass beim Lesen,

Martin Sibler

3 Schwerpunktthema: Cybererpressung – Krimineller Trend im Netz

Cryptolocker, Armada Collective, Rex Mundi: Was haben all diese in den Schlagzeilen aufgetauchten Bedrohungen gemeinsam? Es handelt sich um Cyber-Erpressung. Diese profitable Masche ist bei Kriminellen seit einigen Jahren sehr beliebt. Statt das Geld direkt zu stehlen, wird ein Druckmittel eingesetzt und das Opfer dazu bewegt, ein Lösegeld zu bezahlen. Die jüngsten Entwicklungen dieser Angriffsmethoden werden in den Kapiteln 4.6.2 und 4.6.3 (Ransomware) sowie 4.4.1 (DDoS und Erpressung) dieses Halbjahresberichts behandelt. Werfen wir aber zuerst einen Blick auf die Frage nach den Gründen für den Erfolg und die rasende Entwicklung in diesem Bereich.

3.1 Das Erfolgsrezept

Für die Täter bietet diese Methode zahlreiche Vorteile: Die Angriffe sind nicht auf Systeme beschränkt, mit welchen Gelder verwaltet oder bearbeitet werden. Der Kreis potentieller Ziele erweitert sich deshalb enorm und ist praktisch unbegrenzt. Von Nutzen für die Angreifer sind im Prinzip alle diejenigen Daten oder Systeme, die für einen Benutzer oder ein Unternehmen einen Wert haben und wichtig genug sind, dass diese bereit sind zu bezahlen, um sie wiederzubekommen. Dieser Angriffsmethode hat zudem für die Kriminellen den Vorteil, dass das Geld viel einfacher und anonymer zu ihnen gelangt und es nicht mehr über Drittpersonen gewaschen werden muss. Man lässt sich direkt in der Währung seiner Wahl – die am wenigsten nachverfolgt werden kann – bezahlen. Es ist somit auch kein Zufall, dass sich diese Methoden mit dem Aufkommen neuer Zahlungsmittel wie Bitcoin und Co, womit sich die Identität des Empfängers verschleiern lässt, stark verbreitet haben. Die Identifikation der Empfänger von Bitcoin-Zahlungen wird von den Kriminellen mit Anonymisierern praktisch verunmöglicht.

Die Entwicklung im Bereich solcher Erpressungsangriffe ist charakteristisch für die Vorgehensweise von Tätergruppen, welche zurzeit im Netz aktiv sind. Dabei bewegt sich der vorherrschende unternehmerische Ansatz oft zwischen Opportunismus, Effizienzoptimierung und Anpassungsfähigkeit. Solange sich ein Angriffsmuster bezahlt macht, wird es beibehalten und weiterentwickelt. Ransomware veranschaulicht diese Entwicklung eindrücklich. Obschon die Funktionsweise seit einigen Jahren bekannt ist, verbreitet sich Ransomware in zahlreichen Varianten weiter und wird mit noch wirksameren Funktionalitäten ausgestattet. Der Teufelskreis: Je mehr Geld diese kriminellen Unternehmen von den Opfern erpressen, über desto mehr Mittel verfügen sie, um ihre Infrastruktur zu finanzieren und ihre Forschung und Entwicklung voranzutreiben. Mit diesen Verbesserungen werden sie noch effizienter und können trotz immer besser werdenden Schutzmassnahmen aufs Neue genügend weitere Opfer erpressen.

3.2 Dynamik des kriminellen Ökosystems

Die Dynamik und Suche nach Effizienz der Kriminellen ist im Endeffekt nichts anderes, als man es von gewinnorientierten Unternehmen her kennt. Als Erstes müssen die Kriminellen sicherstellen, dass sie bei der Technologie einen Vorsprung gegenüber den Sicherheitsdienstleistern haben. Ein Grundpfeiler jedes kriminellen Unternehmens im Bereich der Ransomware sind Verschlüsselungsmethoden, welche nicht geknackt werden können. Zu diesem Zweck müssen die Kriminellen dauernd die Entwicklung ihrer Software überwachen

und für den Fall, dass jemand ihre Verschlüsselung umgeht, diese sofort wieder verbessern. Zweitens müssen die Kriminellen versuchen, den Kreis ihrer potenziellen Kunden (d.h. ihrer möglichen Opfer) laufend zu erweitern. Das wird vor allem über die Verbesserung der verwendeten Methoden zur Infizierung der Opfer erreicht. So sollen präparierte Mails Spamfilter überlisten, indem sie vom kompromittierten Konto eines Kontakts geschickt werden, welcher mit dem Opfer in Verbindung steht. Oder sie werden im Namen einer Behörde verschickt. Es werden auch neue Kompromittierungsmethoden beobachtet: So wurde in einigen Fällen die Ransomware über einen so genannten RDP-Zugang (Remote Desktop Protocol für den Fernzugriff auf einen Windows-Server) eingeschleust, der zuvor mit einem *Brute-Force-Angriff* kompromittiert worden ist. Gleichzeitig versuchen die Kriminellen ihren Opferkreis zu vergrössern, indem sie zum Beispiel nicht mehr nur Daten von Nutzern oder Unternehmen verschlüsseln, sondern direkt den Inhalt von Webseiten. Attacken werden auch dahingehend optimiert, Ziele auszuwählen, für welche die Nicht-Verfügbarkeit von Daten dramatische Konsequenzen hat. Die Bereitschaft ein Lösegeld zu bezahlen, nimmt hier logischerweise zu. Dazu gehören unter anderem die beobachteten Angriffe gegen Spitäler. Mit dem Internet der Dinge und nicht nur der blossen Anbindung, sondern der effektiven Vernetzung zahlreicher Geräte wird der Anwendungsbereich für Ransomware scheinbar unbegrenzt. Ist ein System einmal kompromittiert, gilt es das Maximum an Profit aus diesem herauszuholen. Die Kriminellen praktizieren dabei analog der Geschäftswelt einen «kundenorientierten» Ansatz. Sie kommunizieren über direkte Kanäle (live chats) mit ihren Opfern, um ihnen zu erklären, wie sie ihr Lösegeld am besten bezahlen können. Ausserdem suchen sie Mittel, um den Druck auf die Opfer zu erhöhen und begnügen sich nicht damit, die Daten unlesbar zu machen, sondern drohen auch mit der Veröffentlichung sensibler Daten.

3.3 Ein Erfolg, der Nachahmer anzieht

Diese Angriffe sind so profitabel, dass zahlreiche Nachahmer angelockt werden. Mittlerweile gibt es Verschlüsselungstrojaner in unzählbaren Varianten. Diese Dynamik ist aber auch bei anderen Cyber-Erpressungsarten wie DDoS-Attacken zu beobachten. Im Bereich DDoS ist ein riesiges Tummelfeld von Angreifern mit unterschiedlichsten Fähigkeiten entstanden. Dazu gehören vorab zahlreiche Copycats sogenannte Nachahmer, die das Vorgehen der ursprünglichen Täter imitieren. Ihnen hilft nicht zuletzt, dass man mittlerweile ohne grossen Aufwand einen DDoS-Angriff bei einem «Angriffsdienst» (Booter, Stresser) kaufen kann. In letzter Zeit sind es aber vor allem reine Mitläufer, die aktiv sind. Sie begnügen sich damit, «auf der Welle zu reiten» und Erpressermails zu schicken, ohne sich dabei die Mühe zu nehmen einen wirklichen Angriff durchzuführen, für welchen sie höchstwahrscheinlich auch gar nicht die Möglichkeiten hätten. Sie geben sich als Gruppen (wie beispielsweise Armada Collective) aus, welche durch die Medien bekanntgeworden sind und hoffen, dass die Angst vor einem Angriff schon genügt, damit die Opfer zahlen.

So sehen wir uns einem äusserst profitablen Erpressungsmarkt gegenüber, der verschiedene Täter anlockt, von denen einige grossen Erfindungsgeist an den Tag legen. Daher ist zu befürchten, dass diese Attacken andauern und laufend weiterentwickelt werden. Dieser ganze Markt beruht aber am Ende auf der Voraussetzung, dass eine kritische Masse von zahlungsbereiten Opfern vorhanden sein muss, damit diese Gruppen genügend Profit machen und ihre Tätigkeit finanzieren können. Ohne diese Finanzierungsquelle fällt das System in sich zusammen. Man kann deshalb nicht oft genug betonen wie wichtig es ist, nicht auf solche Erpressungen einzugehen. Damit ist es aber nicht getan. Gleichzeitig muss laufend über die Schutzmöglichketen vor solchen Angriffen informiert werden. Jedes Unternehmen muss sich damit befassen und sich die Fragen stellen, welche Systeme oder Informationen so

sensibel sind, dass es deswegen erpresst werden kann, mit welchen Methoden jemand an die Daten oder Systeme herankommen kann, wie diese geschützt sind und ob es Prozesse gibt, auf einen erpresserischen Angriff zu reagieren. Nutzer oder Unternehmen, die nicht genügend auf solche Eventualitäten vorbereitet sind, werden bedauerlicherweise auf die Erpressung eingehen und bezahlen.

Empfehlung:

MELANI stellt verschiedene Dokumente bereit, wie man sich vor Bedrohungen schützen kann:

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

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

4 Lage national

4.1 Spionage

4.1.1 Turla bei einer Rüstungsfirma

Am 4. Mai 2016 publizierte das Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) eine Medienmitteilung[1], wonach die Bundesanwaltschaft im Januar 2016 durch den Nachrichtendienst des Bundes (NDB) informiert worden war, dass Computer der Rüstungsfirma RUAG mit einer Spionagesoftware infiziert worden seien. Die Bundesanwaltschaft hatte am 25. Januar 2016 eine Strafuntersuchung gegen Unbekannt eingeleitet. Als Folge dieser Medienmitteilung war das mediale Interesse sehr gross, und die politische Aufarbeitung dieses Falles ist aktuell noch nicht abgeschlossen. Die Melde- und Analysestelle Informationssicherung (MELANI) publizierte am 23. Mai 2016 im Auftrag des Bundesrates einen Bericht mit den technischen Erkenntnissen zum Fall RUAG. Ziel dieser Massnahme war es, anderen Firmen die Möglichkeit zu geben, ihre eigenen Netzwerke zu überprüfen und geeignete Schutzmassnahmen zu ergreifen.[2,3]

[1] https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-61618.html (Stand: 31. August 2016).

[2] https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-61788.html (Stand: 31. August 2016).

[3] https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/fachberichte/technical-report_apt_case_ruag.html (Stand: 31. August 2016).

Die Angreifer verwendeten eine sich seit mehreren Jahren im Umlauf befindliche Schadsoftware des Trojanertyps «Turla». Die im Netzwerk der RUAG beobachtete Variante hatte zwar keine *Rootkit*-Funktionalität, setzte aber auf Tarnung, um unerkannt zu bleiben. Die Angreifer zeigten viel Geduld bei der Infiltration und auch beim weiteren Vordringen innerhalb des Netzwerkes. Sie griffen nur Ziele an, an denen sie Interesse hatten.

Ein wichtiges Teilziel des Angriffs war der Verzeichnisdienst, das *Active Directory*. Hat man Zugriff auf dieses zentrale Adressbuch, kann auf weitere Anwendungen und Geräte mit interessanten Daten zugegriffen werden, indem entsprechende Berechtigungen und Gruppenzugehörigkeiten gesetzt werden. Um die Kommunikation möglichst gut zu verstecken, nutzte die Schadsoftware das Protokoll «http» für den Datentransfer zu mehreren *Command & Control Servern*. Diese Kontrollserver sendeten wiederum Aufträge, sogenannte Tasks an die infizierten Geräte, wie beispielsweise das Herunterladen neuer Binär- und Konfigurationsdateien oder *Batchjobs*. Es kam ein hierarchisches System zum Einsatz: Bei dieser Architektur kommuniziert nicht jedes infizierte Gerät mit den Kontroll-Servern, sondern es herrscht eine Arbeitsteilung. Einige Systeme, sogenannte Kommunikationsdrohnen, haben die Aufgabe, mit der Aussenwelt zu kommunizieren. Andere sogenannte Arbeiterdrohnen, werden ausschliesslich zum Entwenden und zur Weitergabe der Daten an die Kommunikationsdrohnen benutzt.

Den effektiven Schaden abzuschätzen, ist schwierig und war weder Bestandteil des von MELANI publizierten RUAG Berichts noch dieses Berichts. Die Analyse der *Proxylogs* zeigten allerdings, dass nicht zu jedem Zeitpunkt Daten ausgelesen wurden. Es gab Phasen mit sehr geringer Aktivität sowohl bezüglich Anfragen als auch der abgeflossenen Datenmengen, aber auch Phasen mit einer grossen Zahl an Anfragen und grossen abgeflossenen Datenmengen.

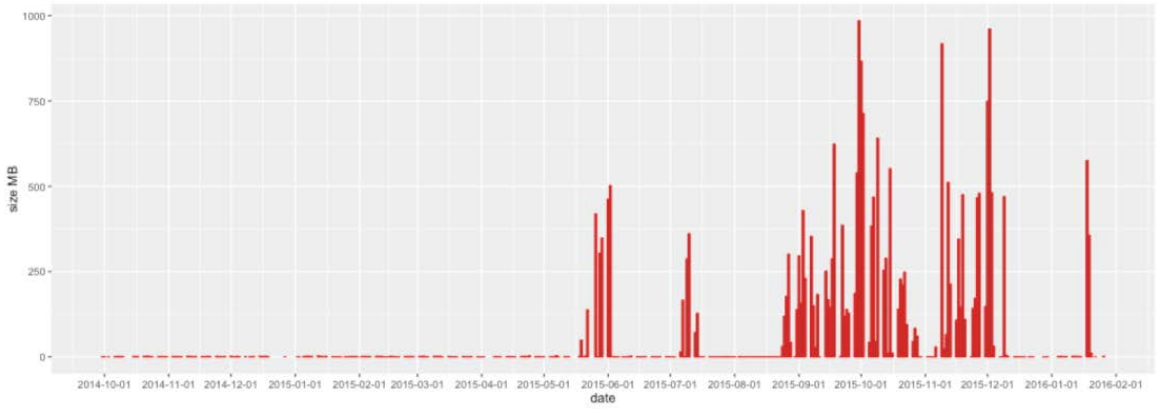


Abbildung 1: Abgeflossene Datenmengen pro Tag

Ein vollständiger Schutz vor so ausgeklügelten Angriffen ist schwierig zu bewerkstelligen. Viele Gegenmassnahmen sind allerdings nicht sehr teuer und können mit vernünftigem Aufwand implementiert werden. Insbesondere wenn ein Angreifer einen Fehler macht, besteht die Möglichkeit, einen Vorfall zu erkennen. Dazu müssen jedoch die Mitarbeitenden entsprechend sensibilisiert werden, Fehlfunktionen und verdächtiges Verhalten in den Systemen zu

erkennen, richtig zu deuten und entsprechend zu reagieren. Eine Auflistung solcher Massnahmen sind im MELANI/GovCERT Ruag Report[4] ab Seite 27 aufgelistet.

Ebenfalls ist die Sensibilisierung für die Wichtigkeit des Erfahrungs- und Informationsaustausches mit anderen Firmen, dem jeweiligen Wirtschaftssektor oder der Bundesverwaltung ein wichtiger Punkt. Der geschlossene Kundenkreis (GK) von MELANI mit mittlerweile über 190 Firmen aus dem Umfeld der kritischen Infrastrukturen ist ein wichtiges Gefäss, um solche Informationen zwischen den Firmen, wenn nötig auch anonym, auszutauschen. Das internationale Netzwerk von MELANI leistet zusätzlich einen wichtigen Beitrag, Angriffe zu erkennen, da Cyber-Vorfälle nicht an der Grenze halt machen. Täglich kommen diverse Hinweise aus dem In- und Ausland, die möglicherweise zum Durchbruch führen. Im Rahmen Ihrer Aufgaben und der Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) fördert MELANI den Informationsaustausch unter Betreibern kritischer Infrastrukturen, damit auch in Zukunft vermehrt gezielte Angriffe entdeckt und bestenfalls vereitelt werden können.

Für einen Überblick über den Fall sind die Ereignisse in der untenstehenden Abbildung chronologisch dargestellt:

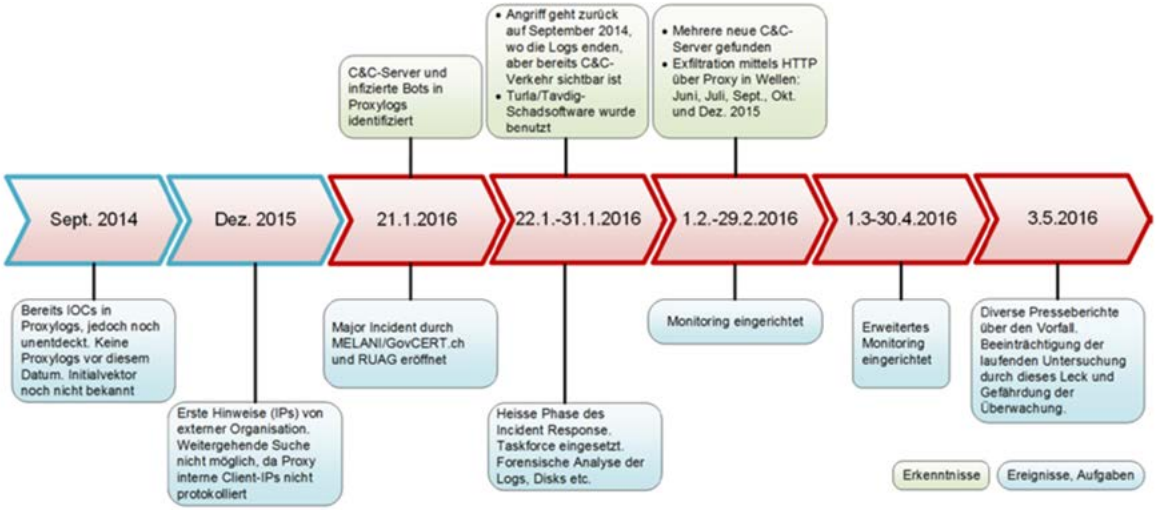


Abbildung 2: zeitlicher Ablauf der Aufklärung des Angriffes

[4] https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/fachberichte/technical-report_apt_case_ruag.html (Stand: 31. August 2016).

Schlussfolgerung / Empfehlung:

Cyberspionage ist Realität. In den vergangenen MELANI-Halbjahresberichten wurde bereits über verschiedene Fälle berichtet. Auch der Jahresbericht des Nachrichtendienstes des Bundes (NDB) befasst sich mit dieser Thematik. Dabei ist Prävention eine äussert wichtige Komponente im Kampf gegen Cyber-Spionage. Hierbei ist der erste und wichtigste Schritt für ein Unternehmen die Erkenntnis, dass es sich um eine reale und nicht um eine hypothetische Gefahr handelt. Zahlreiche Fälle, die MELANI bekannt sind, bestätigen dies. Damit Spionage effizient bekämpft werden kann, muss zudem der Informationsfluss gewährleistet sein. Werden Spionagefälle gemeldet, können die zuständigen Behörden Massnahmen ergreifen, sowie die wesentlichen Erkenntnisse zuhanden der Entscheidungsträger in Politik und Wirtschaft aufbereiten. Schliesslich können andere Organisationen dank diesen Informationen allfällige Angriffe auf ihre Systeme erkennen. Für die Behörden hat die vertrauliche Behandlung der Informationen selbstverständlich oberste Priorität.

MELANI setzt sich in Partnerschaft mit verschiedenen privaten Einheiten seit 12 Jahren für den Schutz vor IT-Gefahren ein. Zur Meldung von Vorfällen im Bereich der Informationssicherung 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 Berechenbare Passwörter bei Routern

Router der Firma UPC werden mit einem werkseitig generierten Passwort ausgeliefert. Dabei enthält der Name des *WLAN*s, die sogenannte *SSID*, eine zufällige siebenstellige Zahl. Das Passwort wird für alle Router vom Hersteller werkseitig erzeugt und sieht dementsprechend individuell und zufällig aus. Mit einer Publikation, die über den letzten Jahreswechsel im Internet aufgetaucht ist, bestand die Möglichkeit, dass Unbefugte das standardisierte WLAN Passwort erraten. Jene Benutzer, die aber ihr Passwort beim Router von Beginn an geändert haben, waren davon selbstverständlich nicht betroffen. Mit diesem Tool ist es möglich, bei

gewissen UPC-Geräten anhand des *WLAN*-Namens eine Auswahl von 8 bis 12 Passwörtern für den *WPA2 Schlüssel* zu berechnen. Zusätzlich zu diesem Tool, das eher für Experten bestimmt war, stellte der Entdecker dieser Sicherheitslücke einige Tage später ein Onlinetool ins Netz, das von allen auf einfache Weise verwendet werden konnte. Der Entdecker der Lücke wollte mit der Aktion auf den Umstand hinweisen, dass gewisse Hersteller die Sicherheit bei der Generierung von Passwörtern vernachlässigen. Die ausgenutzte Sicherheitslücke war nicht wirklich neu: Sie basierte auf einer wissenschaftlichen Forschungsarbeit aus den Niederlanden, die bereits im Frühjahr 2015 publiziert und im Sommer 2015 auf einer Sicherheitskonferenz in Las Vegas vorgestellt worden war.

Anfang Juli 2016 wiederholte sich die Geschichte. Diesmal betraf der Vorfall den auch in der Schweiz eingesetzten Router «Ubee EVW3226». In diesem Fall war nicht die SSID für die Berechnung notwendig, sondern die so genannte *MAC-Adresse* des Gerätes. Diese lässt sich im Funkradius eines WLAN-Netzes mit diversen Werkzeugen ohne grossen Aufwand auslesen. In diesem Fall war es möglich, aus dieser Information die korrelierenden werkseitig eingestellten Standard-Passwörter und die SSID zu berechnen. Auch hier betrifft das ausschliesslich jene Benutzer, die ihr Passwort nicht, wie empfohlen, sofort ändern.

Schlussfolgerung / Empfehlung:

Der Einsatz von Standardpasswörtern ist in jedem Fall zu vermeiden, insbesondere im IT-Umfeld, wenn auf die Geräte ein Zugriff aus dem Internet respektive via Funksignal erfolgt. Manche Hersteller haben darauf reagiert und setzen statt der üblichen «123456»-Kombination ein individuelles Werks-Passwort. Umso ärgerlicher ist es, wenn dieses werkseitig eingestellte individuelle Passwort von Drittpersonen berechnet werden kann und somit eine Sicherheitslücke entsteht. Es gilt deshalb weiterhin die Regel, das Passwort auf jeden Fall zu ändern, wenn das Gerät in Betrieb genommen wird und bevor es mit dem Internet verbunden ist. Die meisten Geräte bieten übrigens eine Reset-Funktion für den Fall, dass das Passwort vergessen worden ist. Hierzu muss man jedoch lokal vor Ort sein und in den meisten Fällen einen Resetknopf am Gerät betätigen. Es wird empfohlen, das Standard-Passwort – genauso wie auch bei vielen anderen Geräten oder Logins für die eigene Sicherheit von Beginn an zu ändern. Das ist nicht nur sicherer, sondern auch einfacher für den täglichen Gebrauch.

4.2.2 Passwörter von 6‘000 Schweizer E-Mail-Konten im Umlauf

Am 16. März 2016 wurden MELANI 6‘000 gehackte E-Mail-/Passwortkombinationen zugespielt, welche durch Hacker im Vorfeld gestohlen wurden. Diese Konten hätten für illegale Zwecke wie beispielsweise Betrügereien, Erpressung usw. missbraucht werden können, sofern das Passwort vom Inhaber nicht umgehend geändert wurde. MELANI publizierte deshalb ein Online-Tool, mit dem sich überprüfen liess, ob die eigene E-Mail-Adresse betroffen ist. Für die Überprüfung war nur die Eingabe der E-Mail-Adresse notwendig. Diese wurde verschlüsselt übermittelt und auch nicht gespeichert.

Die Reaktionen auf diese Aktion waren mehrheitlich positiv. Allerdings waren auch kritische Stimmen zu hören und es wurde mehrfach gefragt, ob die Seite wirklich legitim sei und aus der Feder von MELANI stamme. Aus der Sicht von Sensibilisierung und Prävention ist diese Reaktion begrüssenswert. Eine gesunde Skepsis ist bei solchen Aktionen angebracht und es ist sicherlich gut, einmal mehr nachzufragen und zu verifizieren, ob eine Seite legitim ist. Im vorliegenden Fall schien MELANI eine schnelle Publikation dieses Onlinetools der gangbars-

te und effizienteste Weg zu sein, um potenziell Betroffenen eine Möglichkeit zur Prüfung zu bieten.

4.2.3 Datenbank der Schweizerischen Volkspartei gehackt

Bei einem Angriff auf eine Datenbank der Schweizerischen Volkspartei (SVP) wurden Mitte März 2016 rund 50'000 E-Mail-Adressen kopiert. Eine Gruppe mit dem Namen «NSHC» bekannte sich zu diesem Angriff. NSHC hatte sich gegenüber der Zeitschrift «inside-channels.ch» dahingehend geäussert, man wolle mit dem Angriff zeigen, dass die Schweiz nicht ausreichend gegen Cyber-Angriffe geschützt sei.[5] Die Gruppe bezeichnet sich selbst als «*Grey Hats*» also Hacker, die sich zwar nicht an das Gesetz halten, aber keinen direkten Schaden anrichten wollen. Gleichzeitig bekannte sich die Gruppe sich zu *DDoS*-Angriffen gegen Interdiscount, Microspot und die SBB , die ebenfalls in dieser Woche stattgefunden hatten. Auch hier soll die Motivation der Gruppe ein Wachrütteln der IT-Sicherheitsverantwortlichen gewesen sein. Ob die Gruppe tatsächlich auch DDoS-Fähigkeiten besitzt oder nur auf den fahrenden Zug der im März vermehrt aufgetretenen DDoS-Angriffe aufspringen wollte, ist nicht bekannt. Die Gruppe NSHC war bis dahin nicht in Erscheinung getreten und trat auch nachher nicht mehr in Erscheinung.

4.3 Industrielle Kontrollsysteme

Ist heute eine Internetseite oder ein Onlineservice nicht erreichbar, denkt man unweigerlich an einen möglichen Hackerangriff. Technische Störungen gehören aber immer noch zu den Hauptgründen für Ausfälle bei industriellen Kontrollsystemen. Dies zeigte sich beispielsweise an folgendem, zwar schon längere Zeit zurückliegenden Ereignis eindrücklich: Am 22. Juni 2005 war das Stromnetz der SBB zusammengebrochen, weil zwei von drei alpenquerenden Stromleitungen aufgrund von Bauarbeiten unterbrochen und die Übertragungskapazität der dritten Leitung zu hoch eingeschätzt worden war. Dies führte in der Folge zu einer Schutzabschaltung der dritten Leitung und zu einer Trennung der Stromnetze in einen Alpensüd- und Alpennord-Teil. Die Ereignisse im ersten Halbjahr 2016 hatten zwar nicht diese Dimension, die Auswirkungen waren aber trotzdem gravierend und zeigten die Abhängigkeit von modernen Kommunikationsmitteln.

4.3.1 Störung bei Bezahlterminals

Am 20. Juni 2016 kam es zu Einschränkungen beim bargeldlosen Bezahlen. Betroffen waren Dienstleister sowohl in allen Regionen der Schweiz als auch in Österreich, die ein vom Finanzdienstleister SIX betriebenes *Bezahlterminal* einsetzten. Allerdings trat das Problem weder flächendeckend noch permanent auf. Dies machte die Fehlersuche kompliziert. Ursache war ein Fehler auf der Netzwerkebene.

4.3.2 Ausfall des Internets für Geschäftskunden

Einen Monat zuvor kämpfte die Swisscom mit Problemen. Das Internet für Geschäftskunden war von einer massiven Störung betroffen. Am Mittag des 24. Mai 2016 fiel bei diversen Kunden das Internet aus. Zeitweise waren auch Geldautomaten betroffen. Die Störung

[5] http://www.inside-it.ch/articles/43272 (Stand: 31. August 2016).

konnte schliesslich einem Problem der «Ethernet Access Platform» der Swisscom im Raum Lausanne zugeordnet werden.

4.3.3 Brandanschlag auf Kabelkanal der SBB

Die Ursache für den Ausfall der wichtigen Eisenbahnverbindung zum Flughafen Zürich war dagegen ein physischer Angriff im Raum Zürich Oerlikon. Unbekannte legten am frühen Morgen des 7. Juni an zwei Stellen in einem parallel zum Gleis verlaufenden Kabelkanal Feuer. Die Brandstifter waren auf das Gelände der Bahn eingedrungen und beschädigten die Kabel massiv. In mühsamer Handarbeit mussten Spezialisten die versengten Kabel Stück für Stück reparieren. Der Bahnbetrieb im Raum Oerlikon - Zürich Flughafen war den ganzen Tag massiv beeinträchtigt. Die Bahnlinie zum Flughafen Zürich blieb bis in die Abendstunden gesperrt.

Schlussfolgerung:

Neben dem Risiko von elektronischen Angriffen darf das Risiko von physischen Angriffen auf elektronische Anlagen nicht vernachlässigt werden. Gerade Strom- und Telekommunikationskabel können über weite Strecken ihres Verlaufes nur bedingt geschützt werden. Ein physisches Einwirken hat zwar in der Regel nur eine lokale Auswirkung, der Schutz gerade von neuralgischen Punkten und Systemen sollte sich aber nicht nur auf die elektronische Ebene beschränken, sondern auch die physische Ebene umfassen.

4.4 Angriffe

Privatpersonen und Unternehmen in der Schweiz sind weiterhin das Ziel verschiedener Arten von Angriffen. 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

Cyber-Erpressung ist das Schwerpunktthema dieses Berichts. In diesem Kapitel wird die Entwicklung «Erpressung kombiniert mit DDoS-Drohung» beleuchtet. Über Gruppen wie DD4BC und Armada Collective haben wir schon früher berichtet (Halbjahresberichte 2015/1 und 2015/2). Diese Täter gingen nach der mittlerweile bekannten und dokumentierten Methode vor: Nach einem ersten DDoS-Angriff zur Demonstration erpressen die Angreifer das Opfer. Wird nicht innert einer bestimmten Frist ein Betrag in Bitcoin bezahlt, droht eine zweite, intensivere Attacke als die erste.

Das erste Halbjahr 2016 hat mit einer Erfolgsmeldung im Strafverfolgungsbereich begonnen. Europol hat im Januar bekanntgegeben, dass zwei DD4BC-Mitglieder verhaftet worden sind.[6] Seither wurde kein Angriff im Namen von Armada Collective oder DD4BC mit der «ursprünglichen», oben beschriebenen Methode beobachtet. Dies könnte für die These spre-

[6] https://www.europol.europa.eu/content/international-action-against-dd4bc-cybercriminal-group (Stand: 31. August 2016).

chen, dass Armada Collective und DD4BC in Wirklichkeit ein- und dieselbe Gruppe sind und die wichtigsten Köpfe nun hinter Gittern sitzen.

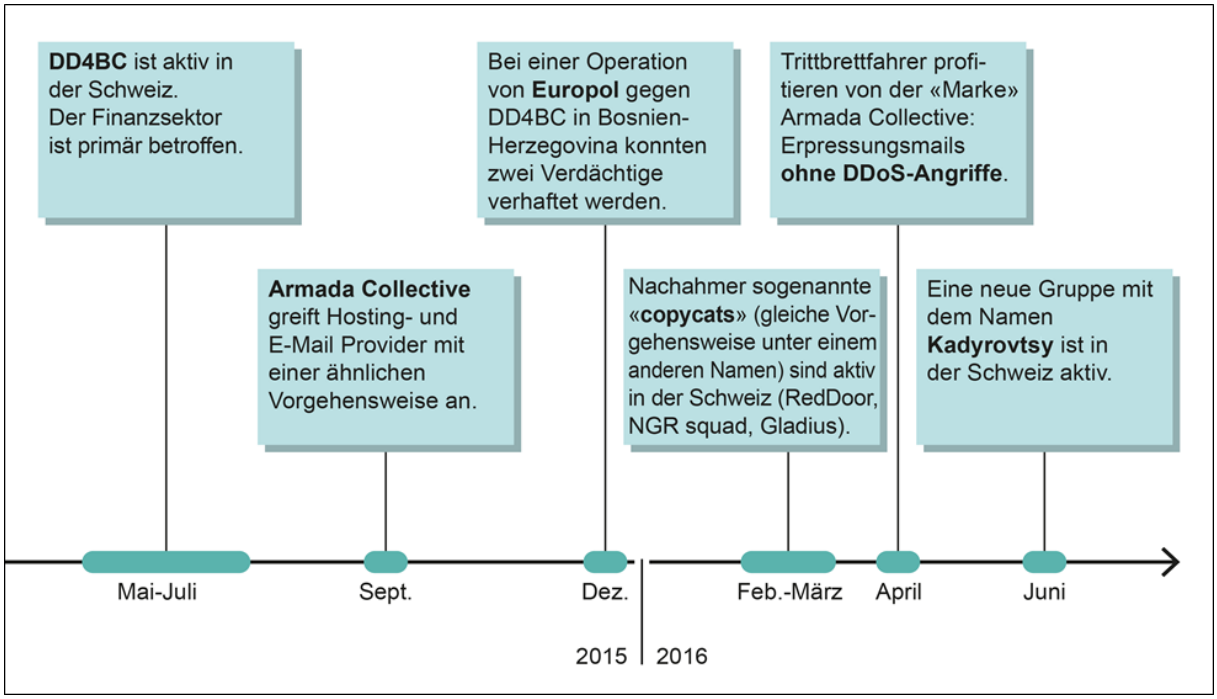


Abbildung 3: DDoS und Erpressung – Timeline

Nach der Verhaftung hat sich die Bedrohung verändert. So sind inzwischen andere Gruppen in Erscheinung getreten, die Teile dieser Angriffsmethode verwenden. Verschiedene Tätergruppen haben Angriffe nach dem typischen DD4BC/Armada-Muster – DDoS-Attacke zur Demonstration gefolgt von einer Erpressung – durchgeführt. Dabei handelt es sich um so genannte Copycats. Diese Gruppen operierten zwischen März und Juni unter den Namen RedDoor, NGR Squad, Gladius und Kadyrovtsy. Im ersten Halbjahr war jedoch am prägendsten das Auftauchen von Mitläufern, die unter dem Namen Armada Collective zahlreiche Erpressermails mit einer DDoS-Drohung verschickten. In diesen Fällen fand aber nie ein Angriff, auch nur zur Demonstration, statt. Sie nutzten lediglich die Angst aus, die nach den diversen Veröffentlichungen über Armada Collective vor dieser Gruppe herrschte, um Geld zu erpressen. Typisch in diesen Fällen war, dass den Opfern jeweils die gleiche Bitcoin-Adresse angegeben wurde, auf die das Lösegeld bezahlt werden sollte. Auf diese Weise wäre es den Angreifern gar nicht möglich gewesen, herauszufinden, wer bezahlt hat und wer nicht und somit angegriffen werden soll. Ausserdem erfolgten zahlreiche Drohungen für den gleichen Tag und die gleiche Uhrzeit, was eine immense DDoS-Kapazität seitens Angreifer nötig gemacht hätte. In solchen Fällen ist jeweils mit grösster Wahrscheinlichkeit ein Mitläufer am Werk. Interessant ist ausserdem, dass eine sich als Armada Collective ausgebende Person bei MELANI über den Missbrauch der Marke «Armada Collective» beklagt hat:

> I'm member of original Armada Collective and I have just noticed your report on Twitter. Armada Collective is dead. We have stopped all operations, because it wasn't profitable enough and risk was too big. When I realized that somebody is using our name I got mad. It is obviously an amateur copycat using our name who copied our text (maybe from your site) and is probably not even capable of launching DDoS attacks. Good luck with your investigation.

Abbildung 4: Bei MELANI via Meldeformular eingegangene Nachricht

Die Zunahme der verschiedenen Aktivitäten zeigen, wie rentabel Erpressung für Kriminelle sein kann. Dabei stellen die Kriminellen nicht nur auf konkrete Angriffe ab, sondern auch auf die blosse Angst davor. Angesichts dieser Dynamik ist schwer abzuschätzen, inwieweit jeweils Berichte mit genauen Angaben zum Vorgehen der Täter eine Inspirationsquelle darstellen. Aus unserer Sicht ist es wichtig, über die Vorgehensweise zu berichten. Es ist aber nicht ausgeschlossen, dass Veröffentlichungen Nachahmer anlocken oder so den Angreifern eine Plattform geboten wird, aus der sie durch die erlangte öffentliche Bekanntheit Profit schlagen können.

Auf der anderen Seite zeigen gerade die Fälle, in denen viele Unternehmen gleichzeitig Erpressermails erhalten haben, wie wichtig der Austausch solcher Ereignisse untereinander respektive die Meldung eines solchen ist. Dank der Meldung an eine zentrale Stelle wie MELANI kann eine Übersicht über vergleichbare Fälle erstellt und die Lage dadurch besser eingeschätzt werden. In diesem Zusammenhang sind die Informationen über die angegebene Bitcoin-Adresse oder die Daten der Angriffsstärke von grosser Bedeutung. Weiter ist daran zu erinnern, dass dem Schutz vor DDoS-Angriffen – einer Angriffsart, die bei unterschiedlichen Kriminellen mit verschiedenen Absichten zum Einsatz kommt – weiterhin Priorität zukommen muss.

Empfehlung:

Trifft ein DDoS-Angriff eine Firma unvorbereitet, sind schnelle und effiziente Gegenmassnahmen kaum mehr möglich. In Unternehmen, die stark von Online-Verkäufen abhängig sind, muss der Sicherung dieses höchst kritischen Geschäftsprozesses absolute Priorität eingeräumt werden. Deshalb sollte in erster Linie eine Strategie für den Fall einer DDoS-Attacke entwickelt werden. Die zuständigen internen und externen Stellen sowie weitere Personen, die im Falle eines Angriffs agieren können, müssen bekannt sein. Idealerweise befasst sich ein Unternehmen im Rahmen des allgemeinen Risikomanagements schon vor einem Angriff auf Stufe der Geschäftsleitung mit der DDoS-Problematik und etabliert auf Betriebsebene eine gewisse DDoS-Abwehrbereitschaft. Ein DDoS-Angriff kann jede Organisation treffen. Sprechen Sie mit Ihrem Internet-Anbieter über Ihre Bedürfnisse und angemessene Vorkehrungen. Eine Checkliste und Anleitung mit Massnahmen gegen DDoS-Angriffe finden Sie auf der Website von MELANI:

Checkliste und Anleitung mit Massnahmen gegen DDoS-Angriffe:

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

4.4.2 Infektion auf 20min.ch[7]

Bereits im letzten Halbjahr wurde der E-Banking-*Trojaner* «Gozi ISFB» über diverse Newsportale der Mediengruppe Tamedia, verbreitet. Der letzte MELANI-Halbjahresbericht hat darüber berichtet.[8] Anfang April dieses Jahres hat sich dieser Vorfall wiederholt, diesmal auf der Website der Gratiszeitung 20 Minuten, die ebenfalls zur Tamedia Gruppe gehört. Die Bundesverwaltung und verschiedene Unternehmen sperrten ab dem 7. April vorübergehend den Zugang zur Website 20min.ch. Tamedia wurde über diese Massnahme informiert. Ursache des von MELANI entdeckten Vorfalls war ein *Java-Script*, das in eine Multimediadatei (*SWF-Animationsdatei) auf der Webseite* eingefügt worden war. Beim Besuch der Website wurde das Script gestartet und führte den Besucher zum *Exploit-Kit* «Niteris», welches automatisch den Trojaner «Gozi» auf den Computer des Opfers herunterlud. Nach der Säuberung der Website stand diese nur wenige Tage später wieder im Visier von Angreifern. In diesem weiteren Fall war allerdings nicht die Website von 20 Minuten selbst betroffen, sondern das Netzwerk eines externen Werbeanbieters, dessen Werbefenster in der Webseite von 20 Minuten eingebaut war. Verteilt wurde die Schadsoftware «Bedep» über das bekannte Exploit-Kit «Angler». Dieses wurde ebenfalls für ähnliche Angriffe auf die Websites von nytimes.com und bbc.com verwendet.[9] Elektronische Tageszeitungen werden jeden Tag von Millionen von Besuchern angeklickt. Sie sind deshalb ideal für Drive-by-Download-Attacken. Diese Vorgehensweise wird in der Schweiz seit Frühling 2015 vermehrt beobachtet. [10] Laut Aussage von «20 Minuten» werden die firmeneigenen Server jeden Tag zwischen 20 und 50 Mal angegriffen.[11]

---

7 http://www.srf.ch/news/schweiz/nach-malware-attacke-auf-20-minuten-was-sie-jetzt-tun-koennen
http://www.20min.ch/digital/news/story/20minuten-ch-erneut-Ziel-von-Malware-Attacke-15457508
http://www.nzz.ch/digital/malware-auf-20minch-tamedia-gab-zu-frueh-entwarnung-ld.12431
http://www.tagesanzeiger.ch/digital/internet/Erneut-ein-Trojaner-auf-20minutench/story/19684342 (Stand: 31. August 2016).

8 MELANI Halbjahresbericht 2015/2, Kapitel 4.3.1.1
https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2-2015.html (Stand: 31. August 2016).

9 http://www.nzz.ch/digital/newssite-gesperrt-mittels-20minch-malware-verbreitet-ld.12263 (Stand: 31. August 2016).

10 https://www.govcert.admin.ch/blog/21/20min.ch-malvertising-incident (Stand: 31. August 2016).
https://www.govcert.admin.ch/blog/13/swiss-advertising-network-compromised-and-distributing-a-trojan
https://www.govcert.admin.ch/blog/18/gozi-isfb-when-a-bug-really-is-a-feature (Stand: 31. August 2016).

11 http://www.20min.ch/digital/news/story/Keine-Gefahr-fuer-die-Nutzer-der-20-Min-App-10440966 (Stand: 31. August 2016).

Empfehlung:

Um solche Infizierungen auf Endkundenseite zu vermeiden, müssen Betriebssysteme und Anwendungen regelmässig – wenn möglich automatisch – aktualisiert werden. Schränken Sie die Ausführung von JavaScripts (Active Scripting) mittels Browsereinstellungen oder zusätzlich installierten Programmen soweit als möglich ein oder deaktivieren Sie JavaScript vollständig. Bei der Deaktivierung von JavaScript ist allerdings darauf hinzuweisen, dass viele Webseiten nicht mehr korrekt funktionieren werden. Sollte Sie das beim Surfen zu stark behindern, so lockern Sie die Einschränkungen (stufenweise) auf das für Sie tragbare Mass. Je nach gewählter Methode ist es auch möglich gewisse Seiten zu definieren, auf welchen Javascript erlaubt ist (White Listing).

Wenn Sie den Verdacht haben, dass Ihr Computer infiziert ist, wenden Sie sich an eine Fachperson, welche den Computer untersuchen und gegebenenfalls säubern oder frisch installieren kann.

Verhaltensregeln ➔ Surfen:

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

4.4.3 OpnessunDorma von Anonymous gegen Stellenportale im Tessin und Italien

37 italienische und sieben Job-Portale aus anderen Ländern (darunter vier aus dem Tessin) wurden zwischen dem 9. und 11. April 2016 Opfer eines Cyber-Angriffes. Die Webseiten der Unternehmen wurden verunstaltet und Millionen von Daten erbeutet. Die Gruppe «Anonymous Italia» und «LulzSecITA» bekannten sich zum Angriff. Sie veröffentlichten die Login-Daten von Usern sowie Informationen zur Struktur verschiedener Datenbanken und Dokumentennamen mehrerer tausend Lebensläufe (die Lebensläufe selbst wurden jedoch nicht veröffentlicht). Die beiden Organisationen nannten zwei Gründe für den Angriff: Einerseits wollte man darauf aufmerksam machen, dass «Arbeitsvermittlungen die Arbeitnehmer wie Schmarotzer ausbeuten». Andererseits wollten die Angreifer die Anfälligkeit und schlechte Sicherheit von IT-Plattformen aufdecken, auf welchen Nutzerdaten gespeichert sind.[12] ticinoonline.ch publizierte einen Screenshot der verunstalteten Website von e-lavoro.ch – der Website des Tessiner Industrieverbands (Associazione industrie Ticinesi AITI) – welche neben BFKconsulting.ch, helvia.com und workandwork.ch vom Angriff betroffen war.[13] Den

[12] https://share.cyberguerrilla.info/?3263d9dcba87924c#nxVUhZU/s/diAc9ZJ1v+cjkH1F+oT3K+iiljOHLLT+0= (Stand: 31. August 2016).

[13] http://www.rsi.ch/news/ticino-e-grigioni-e-insubria/Siti-ticinesi-hackerati-7176668.html (Stand: 31. August 2016).
http://www.radiondadurto.org/2016/04/12/anonymous-italia-operazione-nessundorma-e-la-violazione-della-legge-sulla-privacy/ (Stand: 31. August 2016).
http://www.tio.ch/News/Ticino/Cronaca/1079978/Attacco-hacker-colpiti-4-siti-ticinesi--Rubati-milioni-di-dati/ (Stand: 31. August 2016).

Tessiner Opfern wird dort vorgeworfen, sich «fremdenfeindlichen und rassistischen Schweizer Rechten» unterzuordnen und auch Stellenanzeigen zu publizieren, die sich nur an die Schweizer Wohnbevölkerung richteten.[14]

4.4.4 Hacker an der ETH

Ein Täter hatte sich im Januar 2016 während einigen Tagen unter Verwendung fremder Zugangsdaten ins Netzwerk der ETH Zürich eingeloggt, über das ETH-System Software bestellt und zudem sensible Daten heruntergeladen. Nachdem die ETH die missbräuchliche Verwendung ihres Netzwerkes festgestellt hatte, erfolgte eine Kontaktnahme mit der Staatsanwältin des Zürcher Kompetenzzentrums für Cybercrime, die zusammen mit den polizeilichen Ermittlern unverzüglich die ersten Sicherungsmassnahmen in die Wege leitete und die Ermittlungen vorantrieb. Der mutmassliche Täter konnte bereits 10 Tage nach Einleitung der Untersuchung verhaftet werden. Der Beschuldigte befindet sich in Untersuchungshaft. Es wurde ein Strafverfahren wegen unbefugten Eindringens in ein Datenverarbeitungssystem und unbefugter Datenbeschaffung eröffnet.[15]

4.5 Social Engineering, Phishing

Neben den technischen Angriffen sind auch Methoden, welche die menschlichen Schwächen ausnützen, bei den Angreifern beliebt.

4.5.1 Phishing-Statistik

In den vergangenen Jahren ist die Zahl der durch MELANI bearbeiteten Anfragen bezüglich *Phishing* stark angestiegen. Um die Vielzahl der eingehenden Meldungen betreffend Phishing effizienter bearbeiten zu können, hat MELANI im Jahr 2015 die Website «antiphishing.ch» aufgeschaltet, auf welcher Phishing-Seiten gemeldet werden können. Insgesamt wurden im ersten Halbjahr 2016 2343 verschiedene Phishing-Seiten über dieses Portal gemeldet. Auf Abbildung 5 sind die gemeldeten Phishingseiten pro Woche dargestellt. wobei die Anzahl über die Zeit 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 Angreifer ihre Angriffe regelmässig von Land zu Land.

[14] Erwähnt wird hier insbesondere eine Unternehmensgruppe, die in der Produktion sowie im Verkauf von orthopädischen Prothesen tätig ist.

[15] https://www.ethz.ch/de/news-und-veranstaltungen/eth-news/news/2016/02/mm-mutmasslicher-hacker-verhaftet.html (Stand: 31. August 2016).

Abbildung 5: Gemeldete und bestätigte Phishingseiten pro Woche auf antiphishing.ch

4.5.1 Perfektionierter «CEO-Fraud» hält weiter an

«CEO-Fraud» – diese Methode wurde von MELANI schon mehrfach in Newslettern und Halbjahresberichten thematisiert. Von CEO-Betrug ist dann die Rede, wenn Täter im Namen des Firmenchefs die Buchhaltung oder den Finanzdienst anweisen, eine Zahlung auf ein (typischerweise ausländisches) Konto der Betrüger vorzunehmen. Meist erfolgt die Anweisung von einer gefälschten E-Mail-Adresse aus. Es wurden aber auch Fälle beobachtet, in denen von einem kompromittierten echten E-Mail-Konto aus operiert wurde. Die Begründungen für die Zahlung sind unterschiedlich, wobei es meist um eine angeblich dringende und äusserst heikle Zahlung (insbesondere Akquisition) geht. Ein Berater oder eine falsche oder kompromittierte Anwaltskanzlei sind ebenfalls oft Teil des Szenarios. Die Angreifer wissen genau, wie sie mit einer angeblich dringenden Situation Druck auf den betreffenden Mitarbeiter oder die betreffende Mitarbeiterin ausüben müssen, damit er oder sie die Zahlung vornimmt und dabei allfällige Prozessvorgaben umgeht.

Im Berichtshalbjahr machten einige Fälle im Ausland Schlagzeilen. Dazu gehört das im Raumfahrtbereich tätige österreichische Unternehmen FACC, das bei einem solchen Betrug 42 Millionen Euro verloren hat und sich danach von seinem CEO trennte[16]. MELANI sind einige Fälle in der Schweiz bekannt. Ob im In- oder im Ausland – diese Art Betrug nimmt nicht ab, sondern scheint noch weiter perfektioniert zu werden.. Es handelt sich um ein typisches Muster von im Internet aktiven kriminellen Gruppen: Bewährt sich eine Methode, wird sie beibehalten, wobei die einzelnen Vorgehensschritte verbessert und verfeinert werden.

Für das Beschaffen von Erstinformationen über das Unternehmen sind die sozialen Netzwerke jeweils eine Goldmine. LinkedIn ist für Betrüger besonders interessant, weil dort zum Beispiel Informationen über geschäftliche Beziehungen oder die Identität und Funktion von Mitarbeitenden zu finden sind. Auch das Handelsregister oder nur schon die Webseite des Unternehmens können nützliche Informationen liefern. Sind die benötigten Informationen nicht online verfügbar, nehmen die Betrüger per Telefon Kontakt auf, um an Informationen zu kommen. Es gab auch Fälle, in denen ein Fax mit dem offiziellen Briefkopf einer kantonalen Verwaltung verschickt wurde, um an entsprechende Firmeninformationen zu kommen. Zu den gesuchten Daten gehören vor allem die Mailadressen der Mitarbeitenden in der Buchhaltung, die am Ende die Zahlungen für die Betrüger vornehmen sollen. Mit den Angaben

[16] http://www.reuters.com/article/us-facc-ceo-idUSKCN0YG0ZF (Stand: 31. August 2016).

aus diesen Erstkontakten werden dann gezielte E-Mails mit für das jeweilige Unternehmen plausiblen Angaben verschickt.

Für den Versand von E-Mails, die auf den ersten Blick täuschend echt scheinen, verwenden die Betrüger vor allem unternehmensähnliche Domainnamen. So hat MELANI Kenntnis, dass im Juni 2016 gleich zwanzig Schweizer Domainnamen registriert wurden, welche Unternehmensadressen imitierten. Mit E-Mail-Adressen von diesen Domains, wollten die Betrüger den Empfängern vortäuschen, es mit dem echten Unternehmen zu tun zu haben. Eine ebenfalls von den Betrügern gern verwendete Absenderart sind Mails, die auf eine bestimmte Position oder einen Beruf schliessen lassen wie «lawyer.com», «president.com», «consultant.com».

Empfehlung:

Der Versand solcher Betrugs-E-Mails kann kaum verhindert werden. Die Betrüger verschleiern ihre Identität und Herkunft und können bei Bedarf jederzeit die Adresse wechseln. Die wichtigste Empfehlung zur Vorbeugung ist deshalb die Sensibilisierung des Personals besonders in den für diesen Betrug benötigten Positionen wie Buchhaltung, Finanzabteilung, usw. Als Grundregel ist folgendes zu beachten: Bei ungewöhnlichen oder zweifelhaften Kontaktaufnahmen keine Information herausgeben und keine Anweisungen befolgen, auch wenn man unter Druck gesetzt wird. Weiter wird jedem Unternehmen empfohlen zu kontrollieren, welche Informationen über die eigene Firma online zugänglich sind. Schliesslich sollten Prozesse definiert werden, die alle jederzeit zu befolgen haben. Bei Überweisungen wird ein Vieraugenprinzip mit Kollektivunterschrift empfohlen.

4.6 Crimeware

Crimeware ist eine von Wirtschaftskriminellen weiterentwickelte Form der Schadsoftware, die kriminologisch zur Computerkriminalität zählt und rechtlich unter Datenbeschädigung sowie betrügerischem Missbrauch einer Datenverarbeitungsanlage anzusiedeln ist. Der grösste Teil an Infektionen geht auch im ersten Halbjahr 2016 auf das Konto von «Downadup» (auch bekannt als «Conficker»). Der Wurm existiert bereits über acht Jahre und verbreitet sich über eine im Jahr 2008 entdeckte und ebenso lange geschlossene Sicherheitslücke in Windows Betriebssystemen. Auf den vorderen Plätzen gab es aber im ersten Halbjahr 2016 Änderungen und es sind neu Spambots zu finden, welche die e-Banking Trojaner prozentual verdrängt haben. Die Schadsoftware lethic auf dem zweiten Platz verteilt Medikamentenspam und Werbung zu gefälschten Gütern. Necurs auf Platz 3 hat sich sowohl auf das Versenden des Verschlüsselungstrojaners Locky als auch der e-Banking Schadsoftware Dridex spezialisiert. Auffallend ist das Verschwinden der e-Banking Schadsoftware Dyre aus den vorderen Plätzen der Statistik. Verhaftungen im Zusammenhang mit Dyre haben diese Schadsoftware zumindest kurzzeitig praktisch zum Verschwinden gebracht. Mehr dazu in Kapitel 5.5.3.

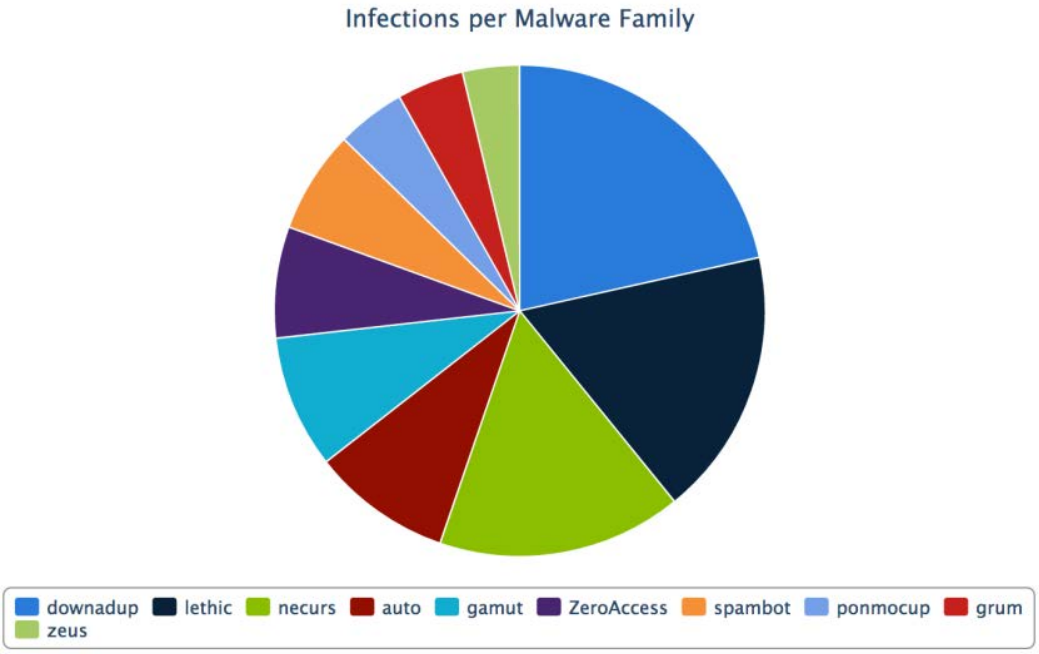


Abbildung 6: Verteilung der Schadsoftware in der Schweiz, welche MELANI bekannt ist. Stichtag ist der 30. Juni 2016. Aktuelle Daten finden Sie unter: http://www.govcert.admin.ch/statistics/dronemap/

4.6.1 Vermehrt schädliche Android Apps in der Schweiz

In den Monaten Juni und Juli 2016 wurden tausende SMS an Empfänger in der Schweiz versendet, die vorgaben, von der Schweizerischen Post zu stammen und jedoch einen Link auf eine Webseite in Lettland enthielten. Beim Anklicken des Links wurde das Opfer auf eine gehackte Webseite weitergeleitet, um es dann zu verleiten, von dieser Seite eine schädliche Android-App zu installieren[17]. Ignorierte der Empfänger die eingeblendeten Sicherheitshinweise von Android und installierte die App, infizierte er sein Gerät mit Schadsoftware.

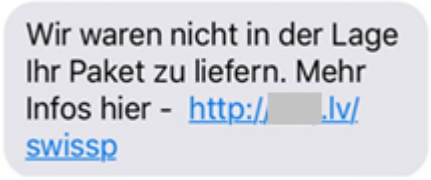


Abbildung 7: Gefälschte SMS, welche angeblich von der Post stammt

Die Schadsoftware tarnte sich unter dem Namen *«SwissPost»* und verwendete das Logo der Schweizerischen Post. Die App kopierte im Hintergrund vom Benutzer unbemerkt Zugangsdaten von populären Apps wie Facebook, Uber oder Viber und übermittelte diese an die Hacker.

[17] https://www.govcert.admin.ch/blog/24/sms-spam-run-targeting-android-users-in-switzerland (Stand: 31. August 2016).

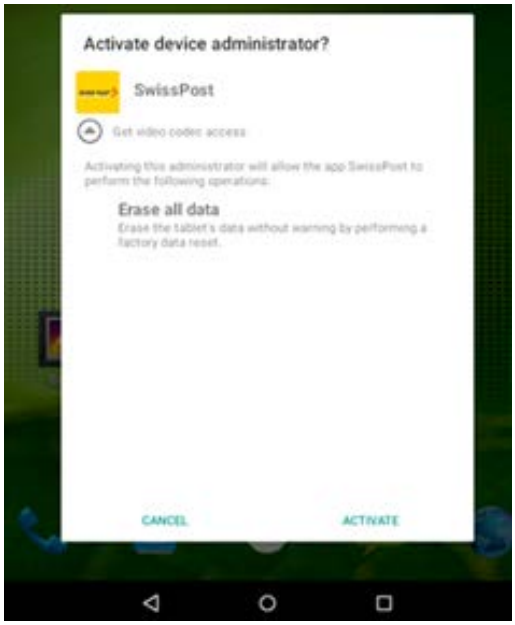


Abbildung 8: Schadsoftware tarnt sich als App der Schweizerischen Post

Empfehlung:

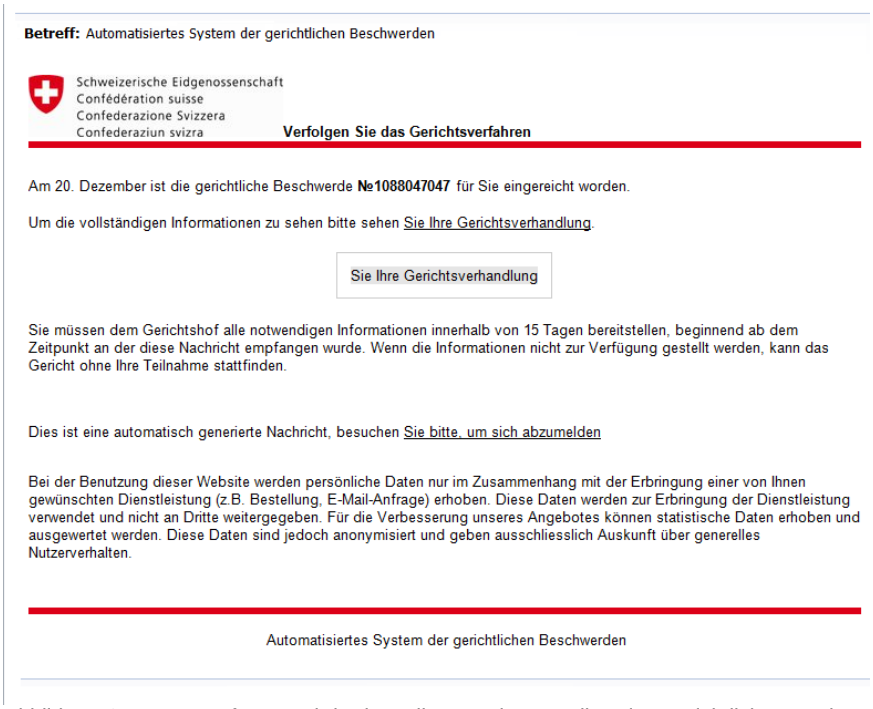
Generell sollten keine Apps aus Drittquellen installiert werden. Stattdessen ist ausschliesslich der offizielle App Store des Herstellers zu verwenden.

4.6.2 Gefälschte Vorladung führt zu Verschlüsselungstrojaner

Die Bedrohung durch sogenannte *Verschlüsselungstrojaner* ist auch im Berichtszeitraum weiter gestiegen. Die Einfachheit der Vorgehensweise, sowie die immer noch zu grosse Bereitschaft der Opfer, den Lösegeldforderungen nachzugeben, hat dazu geführt, dass sich *Ransomware* immer mehr verbreitet.

Um den Nutzer dazu zu bringen, auf einen E-Mail-Link zu klicken oder Anhänge zu öffnen und sich somit die Ransomware auf den Computer zu holen, muss es dem Angreifer gelingen, den Inhalt der E-Mail so plausibel wie möglich zu gestalten. In vielen Fällen stammt die Nachricht angeblich von einer Institution, die dem Empfänger bekannt ist und die er für vertrauenswürdig hält. So schöpft dieser keinen Verdacht. Auf einen solchen Vorfall wies MELANI in ihrem GovCERT-Blog im Januar 2016 hin[18]: Es ging dabei um eine E-Mail-Welle, welche die Ransomware «TorrentLocker» verbreitete. Im Betrugsmail wurde dem Empfänger mitgeteilt, es sei gegen ihn eine Beschwerde eingereicht worden und er werde zu einer Gerichtsverhandlung vorgeladen. Um weitere Informationen zu erhalten, musste der Empfänger auf einen Link klicken und Dokumente herunterladen. In diesem Fall nutzte man nicht nur die Vertrauenswürdigkeit einer Behörde, sondern auch die Unsicherheit und Angst der Nutzerinnen und Nutzer aus. Einschüchterungen sind ein gutes Mittel, um Opfer dazu zu verleiten, auf einen Link zu klicken. Gerichte verwenden für eine offizielle Vorladung jedoch niemals das Medium E-Mail.

[18] https://www.govcert.admin.ch/blog/17/torrentlocker-ransomware-targeting-swiss-internet-users (Stand: 31. August 2016).



Betreff: Automatisiertes System der gerichtlichen Beschwerden

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Verfolgen Sie das Gerichtsverfahren

Am 20. Dezember ist die gerichtliche Beschwerde **№1088047047** für Sie eingereicht worden.

Um die vollständigen Informationen zu sehen bitte sehen Sie Ihre Gerichtsverhandlung.

Sie Ihre Gerichtsverhandlung

Sie müssen dem Gerichtshof alle notwendigen Informationen innerhalb von 15 Tagen bereitstellen, beginnend ab dem Zeitpunkt an der diese Nachricht empfangen wurde. Wenn die Informationen nicht zur Verfügung gestellt werden, kann das Gericht ohne Ihre Teilnahme stattfinden.

Dies ist eine automatisch generierte Nachricht, besuchen Sie bitte, um sich abzumelden

Bei der Benutzung dieser Website werden persönliche Daten nur im Zusammenhang mit der Erbringung einer von Ihnen gewünschten Dienstleistung (z.B. Bestellung, E-Mail-Anfrage) erhoben. Diese Daten werden zur Erbringung der Dienstleistung verwendet und nicht an Dritte weitergegeben. Für die Verbesserung unseres Angebotes können statistische Daten erhoben und ausgewertet werden. Diese Daten sind jedoch anonymisiert und geben ausschliesslich Auskunft über generelles Nutzerverhalten.

Automatisiertes System der gerichtlichen Beschwerden

Abbildung 9: Dem Empfänger wird mitgeteilt, es sei gegen ihn eine gerichtliche Beschwerde eingereicht worden. Um weitere Informationen zu erhalten, soll der Empfänger auf einen Link klicken und Dokumente herunterladen. Diese Dokumente enthalten eine Schadsoftware.

4.6.3 Spontanbewerbungen mit Verschlüsselungstrojaner

Weitere beliebte Methoden, um die Empfängerinnen und Empfänger zum Anklicken eines Links oder zum Öffnen einer Datei zu verleiten, bestehen darin, die Interessen oder Bedürfnisse des Opfers anzusprechen oder dessen Vertrauen zu gewinnen, beispielsweise indem man es mit Vor- und Nachnamen anspricht. Im vergangenen Mai waren in der Schweiz E-Mails im Umlauf, die genau diese Methoden verwendeten. Die Opfer wurden gezielt ausgewählt und erhielten E-Mails mit Spontanbewerbungen. Um Zugriff auf das ganze Dossier zu erhalten, wurden die Empfänger dazu aufgefordert, einen Link anzuklicken, der den Zugriff auf das gesamte Dossier ermöglichen sollte. Der Dropbox-Link führte allerdings direkt auf die Verschlüsselungs-Trojaner «Petya» und «Mischa». Auch die Schadsoftware «Locky», die sowohl in der Schweiz wie auch im Ausland immer noch sehr aktiv ist, versteckt sich in letzter Zeit hinter harmlos aussehenden Spontanbewerbungen.

4.6.4 Verschlüsselungstrojaner – technische Aspekte

Unter den technischen Aspekten fiel im ersten Halbjahr vor allem die Version 3.1 von CryptXXX auf. Dieser *Virus* verschlüsselt nicht nur die Daten auf dem Computer der Opfer, sowie die Daten, die sich auf dem Computer angeschlossenen Speichermedien befinden; er ist auch in der Lage, sich durch das Herunterladen einer anderen *Malware* («stiller.dll») Passwörter und andere Zugangsdaten zu beschaffen.[19]

Auch «CTB-Locker», eine Ransomware, die vor allem im Sommer 2014 sehr aktiv war, ist wieder aufgetaucht. Es handelt sich um eine neue Version, die sich darauf spezialisiert hat,

[19] https://www.proofpoint.com/us/threat-insight/post/cryptxxx-ransomware-learns-samba-other-new-tricks-with-version3100 (Stand: 31. August 2016). Der im April erstmals entdeckte Krypto-Trojaner CryptXXX ist in der Lage, das von KasperskyLab entwickelte Dechiffrierungs-Tool zu umgehen.

den Inhalt von Webseiten zu verschlüsseln. Mit welcher Methode der Virus verbreitet wird, ist noch nicht ganz klar. Analysen verschiedener Quellen deuten aber darauf hin, dass der Angriff über verwundbare Wordpress-Seiten stattfindet. Ist die Website infiziert, erscheint eine Mitteilung, die über das weitere Vorgehen zur Wiedererlangung der persönlichen Daten informiert. Die Schadsoftware entschlüsselt nach dem Zufallsprinzip zwei Dateien, um zu zeigen, dass die Angreifer in der Lage sind, die Daten überhaupt zu dechiffrieren. Ausserdem wird ebenfalls ein Video gezeigt, das wie die Persiflage eines Kundensupports wirkt: Darin wird erklärt, wie man die zur Zahlung des Lösegelds nötigen *Bitcoins* erhält. Weiter wird eine Chatfunktion angeboten, über die man mit den Angreifern Kontakt aufnehmen kann, sofern man noch zusätzliche Informationen benötigt.[20] CTB-Locker ist jedoch nicht der einzige Kryptotrojaner, der seine Opfer auf fantasievolle Art und Weise über die Infektion informiert. Die *Makro-Malware* «Cerber», die im letzten Halbjahr auch in der Schweiz auftauchte, ist beispielsweise die erste, die ihre Lösegeldforderung auch akustisch stellt: «Attention! Attention! Attention! Your documents, photos, databases and other important files have been encrypted!» tönt es aus dem Computer-Lautsprecher.

Um den psychologischen Druck auf das Opfer weiter zu erhöhen, wählt der Erpressungstrojaner «Jigsaw» eine besonders hinterhältige Methode: Für jede verstrichene Stunde löscht die Ransomware eine bestimme Anzahl Dokumente, gleichzeitig erhöht sich die Lösegeldsumme. Innerhalb von 72 Stunden werden alle Dokumente gelöscht.[21]

Mittlerweile können sich auch Mac-Benutzer nicht mehr in Sicherheit wähnen. Die Ransomware «KeRanger», die im März entdeckt wurde, ist der erste Kryptotrojaner, der auch in der Lage ist, OS X-Plattformen anzugreifen.[22] Mit einem für Mac-Anwendungen gültigen Zertifikat haben die Kriminellen zwei Installationsprogramme des BitTorrent Programms «Transmission» für OS X in der Version 2.90 infiziert. Die Malware war zwischen dem 4. und 5. März 2016 auf der Webseite verfügbar. Wer in dieser Zeit das Programm Transmission» für OS X heruntergeladen hat, wurde infiziert. Dann wurden die infizierten Installationsdateien von Transmission gelöscht. Apple hat in der Zwischenzeit das *Zertifikat* zurückgezogen[23].

---

20 http://www.bleepingcomputer.com/news/security/ctb-locker-for-websites-reinventing-an-old-ransomware/ http://www.heise.de/security/meldung/Admins-aufgepasst-Krypto-Trojaner-befaellt-hunderte-Webserver-3116470.html (Stand: 31. August 2016).

21 http://blog.trendmicro.com/trendlabs-security-intelligence/jigsaw-ransomware-plays-games-victims/ (Stand: 31. August 2016).

22 Die Ransomware FileCoder, welche im Jahr 2014 von Kaspersky Lab entdeckt wurde, war zum Zeitpunkt ihrer Entdeckung noch unvollständig und konnte deshalb OS X-Betriebssysteme nicht schädigen. http://researchcenter.paloaltonetworks.com/2016/03/new-os-x-ransomware-keranger-infected-transmission-bittorrent-client-installer/ (Stand: 31. August 2016).

23 http://www.welivesecurity.com/2016/03/07/new-mac-ransomware-appears-keranger-spread-via-transmission-app/ (Stand: 31. August 2016).

Empfehlung:

Laut Kaspersky Lab hat sich die Anzahl Ransomware zwischen April 2015 und März 2016 gegenüber der Vorjahresperiode verfünffacht . Dieser exponentielle Anstieg hat dazu geführt, dass in den letzten sechs Monaten verschiedene Organisationen vermehrt Warnmeldungen publizierten. Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) hat im Mai einen ausführlichen Bericht zum Thema Ransomware veröffentlicht; die niederländischen Polizei hat in Zusammenarbeit mit Europol und zwei IT-Sicherheitsfirmen (Kaspersky Lab und Intel Security) die Website «nomoreransom.org» ins Leben gerufen. MELANI hat im Mai in Zusammenarbeit mit verschiedenen Schweizer Partnern einen Awareness-Tag zu «Ransomware» organisiert und auf vier Massnahmen aufmerksam gemacht:

- 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 welche Sie die Sicherungskopie erstellen, nach dem Backup-Vorgang vom Computer trennen.
- Installierte Software und Plug-Ins immer aktuell halten.
- MELANI empfiehlt Internetbenutzenden, keine verdächtigen E-Mail-Anhänge zu öffnen, auch wenn diese von vermeintlich vertrauenswürdigen Absendern stammen.
- Zusätzlich sollte sichergestellt werden, dass ein Virenschutz installiert ist und dieser stets auf dem aktuellen Stand gehalten wird.

INFO

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 Erster MELANI Awareness-Tag: Ransomwareday

Zusammen mit zahlreichen Partnern lancierte MELANI am 19. Mai 2016 zum ersten Mal einen Awareness-Tag. Um die Bevölkerung zum Thema *Ransomware* zu sensibilisieren, haben Organisationen aus verschiedenen Sektoren, Softwarehersteller, Bundesämter sowie diverse Schweizer Vereine und Konsumentenschutzorganisationen an diesem Tag das Thema aufgenommen und diverse Publikationen veröffentlicht. Es wird zur Zeit noch abgeklärt, inwiefern sich ein solcher Tag wiederholen lässt.

5 Lage International

5.1 Spionage

5.1.1 Spionageangriff stört Wahlkampf

Am Vorabend des nationalen Kongresses der US-amerikanischen demokratischen Partei in Philadelphia (USA) trat die Vorsitzende des nationalen Komitees (Democratic National Committee, DNC), Debbie Wasserman Schultz, von ihrem Posten zurück[24]. Ein offensichtlich unglücklicher Zeitpunkt für einen Wechsel in der Führungsriege der Partei. Was war passiert? Zwei Tage zuvor publizierte Wikileaks[25] rund 20‘000 interne E-Mails der Führungsriege des DNC. Den Mails war zu entnehmen, dass das Komitee nicht nur eine Kandidatur Hillary Clintons bevorzugte, sondern koordinierte Anstrengungen unternahm, um sie gegenüber ihrem härtesten Konkurrenten, Bernie Sanders, zu bevorteilen.

Die Geschichte startete jedoch bereits über einen Monat früher, als die «Washington Post» [26] über einen Hackerangriff auf die digitale Infrastruktur des DNC berichtete. Bereits ein Jahr lang durchstöberten die Angreifer die Analysen zum republikanischen Gegner Donald Trump und lasen, wie die Wikileaks Publikation eindrücklich zeigte, auch bei der E-Mail-Kommunikation mit.

Ende April 2016 fielen den IT-Verantwortlichen des DNC seltsame Vorgänge auf, worauf Experten der Firma Crowdstrike beigezogen wurden. Das Incident-Response Team von Crowdstrike entdeckte daraufhin zwei separat agierende Angreifer im Netzwerk der Partei, welche sie als die ihnen bereits bekannten Gruppen «COZY BEAR» und «FANCY BEAR» identifizierten. «FANCY BEAR», bekannt durch den Angriff auf den deutschen Bundestag im Jahr 2015, soll laut Crowdstrike bereits seit Sommer 2015 im DNC-Netz aktiv gewesen sein. «COZY BEAR» konnte erst seit April 2016 nachgewiesen werden. In ihrem Bericht [27] vermutet Crowdstrike zwei verschiedene russische Nachrichtendienste hinter den Angriffen. Noch am gleichen Tag bekannte sich ein angeblich rumänischer Hacker mit dem Pseudonym «Guccifer 2.0» zum Angriff und behauptete, alleine für den Angriff verantwortlich zu sein. Er kündigte zudem die Publikation von Auszügen seiner Beute auf Wikileaks an. Dies veranlasste Crowdstrike zu einem Update des Berichts, um Guccifer 2.0 blosszustellen. Unterstützung erhielt Crowdstrike später von den Cyber-Sicherheitsunternehmen Fidelis Cybersecurity und Mandiant, welche die selben Schlüsse zogen[28], sowie von Thomas Rid, seines Zeichens Professor am King’s College in London. Er fand einen identischen Command and Control (C&C) Server in der DNC-Malware, der bereits beim Angriff auf den deutschen Bundestag eingesetzt worden war. Die rumänische Herkunft von «Guccifer 2.0» und somit des-

---

[24] https://www.washingtonpost.com/politics/hacked-emails-cast-doubt-on-hopes-for-party-unity-at-democratic-convention/2016/07/24/a446c260-51a9-11e6-b7de-dfe509430c39_story.html (Stand: 31. August 2016).

[25] https://wikileaks.org/dnc-emails/ (Stand: 31. August 2016).

[26] https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html (Stand: 31. August 2016).

[27] https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/ (Stand: 31. August 2016).

[28] https://www.wired.com/2016/07/heres-know-russia-dnc-hack/ (Stand: 31. August 2016).

sen Glaubwürdigkeit wurden spätestens dann angezweifelt, als er es nicht schaffte, sich mit einem muttersprachlich rumänischen Journalisten flüssig und verständlich zu unterhalten.

Schlussfolgerung:

Der Vorfall zeigt eindrücklich, wie sich machtpolitische Einflussnahme im Cyberraum gestalten kann. Die öffentliche Meinung lässt sich durch Ausspionieren von sensiblen Daten eines Kontrahenten und durch selektive Publikation diffamierender Daten schnell beeinflussen.

5.2 Datenabflüsse

5.2.1 Unerwünschtes öffentliches Auszählen von Wählerregistern

Gleich zweimal machten im ersten Halbjahr 2016 Datenlecks bei Wahlregistern Schlagzeilen. Am 30. März 2016 publizierte ein anonymer Hacker eine Datei, welche die persönlichen Informationen von 50 Millionen türkischen Bürgern enthielt[29]. Die Informationen umfassten Namen, Adressen, Vornamen der Eltern, Geburtsorte, Geburtsdaten, sowie nationale Identifikationsnummern. Neben den Daten wurde eine Stellungnahme veröffentlicht, welche der Regierung Erdogan vorwarf, die Daten der Bürger nicht ausreichend schützen zu können. Es stellte sich heraus, dass die Daten nicht aktuell sind, sondern aus dem Jahre 2008 stammen. Ihre Authentizität wurde aber durch die Nachrichtenagentur Associated Press bestätigt. Bei der Publikation solcher Daten besteht immer die Gefahr, dass diese als Grundlage für Identitätsdiebstahl dienen können.

Nur eine Woche später wurde auf den Philippinen ein noch umfassenderes Datenleck publik.[30] 55 Mio. philippinische Wähler wurden durch einen Hack auf die Datenbank der philippinischen Commission on Elections (COMELEC[31]) veröffentlicht. Darunter waren laut dem Anbieter von Sicherheitssoftware, Trend Micro,[32] auch sensible Informationen wie beispielsweise Passwörter und 15.8 Millionen registrierte Fingerabdrücke. Der eigentliche Vorfall fand bereits am 27. März 2016 statt, als «Anonymous Philippines» die COMELEC Website verunstaltete. Ein Facebooknutzer mit Namen «Lulzsec Pilipinas» hat die gestohlenen Daten einige Tage später online gestellt.

5.2.2 Was man mit dem beruflichen Netzwerk nicht teilen wollte

Neben den Daten, die man wie in Kapitel 5.2.1 beschrieben bei Behörden angeben muss, stellen viele Internetnutzer ihre Daten freiwillig und in grosser Zahl privaten Unternehmen zur Verfügung. Selbstverständlich sind auch diese nicht vor Datenlecks gefeit sind. Das berufliche Netzwerk LinkedIn wurde bereits 2014 Opfer eines Angriffs. Damals wurden 6.5 Millionen verschlüsselte Passwörter online gestellt. Mitte Mai bot nun ein Hacker mit dem Namen «Pace» 117 Mio. Kontoinformationen inklusive E-Mail-Adressen und verschlüsselten Pass-

---

29 https://www.wired.com/2016/04/hack-brief-turkey-breach-spills-info-half-citizens/ (Stand: 31. August 2016).

30 http://www.theregister.co.uk/2016/04/07/philippine_voter_data_breach/ (Stand: 31. August 2016).

31 COMELEC ist eine von drei Philippinischen Regierungskommissionen. Ihre Hauptaufgabe ist es Gesetze und Regulierungen durchzusetzen, um Wahlen auf den Philippinen durchführen zu können.

32 http://blog.trendmicro.com/trendlabs-security-intelligence/55m-registered-voters-risk-philippine-commission-elections-hacked/ (Stand: 31. August 2016).

wörtern für 5 Bitcoins (damals ca. Fr. 2‘000.-) zum Verkauf an.[33] LinkedIn bestätigte die Richtigkeit der Daten. Auch wenn diese bereits vier Jahre alt sind, stellt der Verkauf solcher Daten dennoch eine Gefahr dar, da zahlreiche Internetnutzende dazu tendieren, ihre Passwörter nie oder nur selten zu wechseln und dasselbe Passwort auch bei anderen Diensten zu verwenden.

Empfehlung:

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

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

Verhaltensregeln für Passwörter

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

5.2.3 Twitter Zugangsdaten auf dem Schwarzmarkt

Nicht immer ist die Schuld bei Onlineanbietern zu suchen, wenn Zugangsdaten in kriminelle Hände gelangen. Im Juni wurden auf dem Schwarzmarkt 32 Millionen Twitter-Zugangsdaten inklusive Passwort angeboten.[34] In diesem Fall ging man davon aus, dass die Passwörter durch eine Schadsoftware, welche sich in den Browsern der Endanwender eingenistet hat, kopiert und dann an die Angreifer weitergeleitet wurden. Das Kopieren und Verkaufen von Zugangsdaten ist meist ein lukrativer Zusatzerwerb für Kriminelle. Auch Schadsoftware, die eigentlich für andere Aufgaben wie beispielsweise E-Banking Betrug oder Verschlüsselung konzipiert wurde, enthält meist als Nebenfunktion einen *Keylogger*.

5.3 Industrielle Kontrollsysteme

5.3.1 Malware in deutschem Kernkraftwerk

Im isolierten Bereich des Kernkraftwerks Gundremmingen (Deutschland) wurde im Rahmen von revisionsvorbereitenden Prüfarbeiten auf 18 Wechseldatenträgern und einem Computer zwei verschiedene Schadsoftware gefunden. Das betroffene System gehört laut Angaben des Kernkraftwerks zur Brennelement-Lademaschine und wurde nur zur Visualisierung ver-

[33] http://motherboard.vice.com/read/another-day-another-hack-117-million-linkedin-emails-and-password (Stand: 31. August 2016).

[34] https://techcrunch.com/2016/06/08/twitter-hack/ (Stand: 31. August 2016).

wendet. Es soll somit keinen Einfluss auf die Prozesssteuerung gehabt haben. Laut Medienberichten soll es sich dabei einerseits um die bereits seit 2008 bekannte und weitverbreitete *Schadsoftware* «Conficker» handeln. Obschon Microsoft kurz nach dem Auftauchen dieser Schadsoftware ein Sicherheitsupdate zur Verfügung gestellt hat, ist «Conficker» laut Statistik von MELANI/GovCERT.ch auch in der Schweiz immer noch die meist verbreitete Schadsoftware. Bei der zweiten gefundenen Schadsoftware soll es sich um «Ramnit» handeln. Die Schadsoftware war ab 2010 aktiv. Das entsprechende Botnetz wurde 2015 durch Europol und den Sicherheitsdienstleister Symantec deaktiviert.

Dass eine vor acht Jahren erkannte *Windowslücke* in einem Kernkraftwerk nicht geschlossen worden ist, mag zunächst erstaunen. Das betroffene System stand jedoch im isolierten – also nicht mit dem Internet verbundenen – Bereich der Anlage. Zudem werden Anlagen im industriellen Bereich häufig bei der Installation zertifiziert; das heisst, dass der Hersteller das einwandfreie Funktionieren in genau dieser Konfiguration garantiert. Bei jeglicher Veränderung des Systems – auch durch ein Sicherheitsupdate – fällt diese Garantie weg. Da die Systeme isoliert betrieben werden, ist das Risiko einer durch ein Update verursachten Fehlfunktion um Einiges grösser als die Bedrohung, die von der Sicherheitslücke ausgeht. Aufgrund des vollständigen Abschottens der Systeme sollten interne Sicherheitslücken irrelevant sein. Es gibt aber dennoch Möglichkeiten, wie eine Schadsoftware in so geschützte Bereiche eingeschleppt werden kann:

- Aufgrund der fehlenden Internetverbindung können die Systeme nicht online gewartet und kontrolliert werden. Eine gewisse Gefährdung des Netzwerks entsteht hier, wenn externe Systeme, z. B. Notebook oder *USB-Stick* zwecks Wartung, Import oder Export von Daten an das Netzwerk angeschlossenen werden. Über einen solchen Vorgang könnte die sogenannte *Air-Gap* – die Abschottung des Systems – umgangen und ein Virus in das System eingeschleppt worden sein. Ein reales Beispiel ist der Computerwurm «Stuxnet», der vor einigen Jahren mittels USB-Stick in ein iranisches Urananreicherungswerk eingeschleust worden ist.

- Der Wurm war von Anfang an auf dem Computer, fiel aber bislang nicht auf. Dies könnte der Fall sein, wenn der Computer bei der Installation ans Internet angeschlossen und erst danach isoliert wurde respektive wenn der Datenträger, mit welchem Installationsdateien auf den Computer gebracht wurden, bereits infiziert war.

Schlussfolgerung :

Für gezielte Angriffe wird in der Regel eigens dafür programmierte Schadsoftware verwendet, die nur eingeschränkt in Umlauf gebracht wird, um möglichst unter der Wahrnehmungsschwelle zu bleiben. Ein gezielter Angriff auf das Kernkraftwerk kann in diesem Fall somit weitgehend ausgeschlossen werden.

Jedoch besteht auch bei «versehentlichen» Infektionen immer das Risiko eines Kollateralschadens: Die Schadsoftware könnte Fehlfunktionen im System auslösen, welche dann dazu führen, dass es zum Beispiel spontan herunterfährt. Die sensiblen Bereiche eines Kernkraftwerks werden allerdings analog gesteuert, sodass auch ein solcher Vorgang wie in Gundremmingen keine Auswirkungen auf die kritischen Prozesse gehabt hätte.

5.3.2 Publikation über Cyberangriff auf ein Wasserwerk

Die Sicherheitsfirma Verizon publizierte im März 2016[35] in ihrem «Data Breach Report» die Ergebnisse eines proaktiven Assessments bei einer Trinkwasserversorgungsfirma. Die Firma wurde als «Kemuri Water Company (KWC) » bezeichnet. Genauere Informationen über die Firma veröffentlichte Verizon jedoch nicht. Bei diesem Assessment wurden Spuren eines Hackerangriffs auf die Website der Firma festgestellt. Die webbasierte Payment-Anwendung wurde mittels bekannter Schwachstellen kompromittiert. Auf diesem Front-End-Server waren ebenfalls die Zugangsdaten für den Back-End Server (IBM AS/400) im Klartext auf einer *.ini Datei* gespeichert und konnten durch die Angreifer abgegriffen werden. Auf dem Back-End System, welches um die Jahrtausendwende vielfach eingesetzt wurde, lief nicht nur die Datenbank für die Zahlungsabwicklung sondern unter anderem auch die Buchhaltung, die Kundendatenverwaltung sowie das *ICS*-System von KWC. Dieses kontrollierte Hunderte von Speicherprogrammierbaren Steuerungen (SPS), welche die Ventile und Sensoren der Wasserversorgung steuern. Da das System direkt mit dem Internet verbunden war, konnte mit den erbeuteten Zugangsdaten direkt auf die SPS zugegriffen und die Zugabe von verschiedenen Chemikalien in die öffentliche Trinkwasserversorgung manipuliert werden. Die Untersuchung zeigte, dass das Management von KWC über unerklärliche Vorgänge an Ventilen und Leitungen informiert war, die sich in den letzten 60 Tagen ereignet hatten. Diese Vorgänge hatten zu unkontrollierter Zumischung von Chemikalien in die Trinkwasseraufbereitung geführt. Aufgrund der systemunabhängigen Überwachung der Wasserqualität konnte dank manueller Eingriffe eine Gefährdung der Wasserbezüger verhindert werden.

Diese Vorgänge waren allerdings zu diesem Zeitpunkt nicht als Cyber-Angriff erkannt worden. Die nachfolgende Untersuchung kam zum Schluss, dass die Angreifer keine detaillierten Informationen über die Anlage hatten und somit nur eingeschränkten Schaden anrichten konnten. Mit mehr Zeit und Informationen hätte dieser Angriff weitaus kritischer ausgehen können.

5.3.3 Neuartige Malware mit klarem ICS-Bezug aber unklarem Ziel

Die Anbieterin von Sicherheitssoftware, FireEye, publizierte im Juni 2016 einen Untersuchungsbericht über die *ICS-Schadsoftware* «IronGate» [36], welche FireEye im letzten Halbjahr entdeckt hatte und gleich in mehrerer Hinsicht bemerkenswerte Funktionen enthält. Sie besitzt beispielsweise die Fähigkeit, via *Man-In-The-Middle* während fünf Sekunden Informationen aufzuzeichnen, welche von der Speicherprogrammierbaren Steuerung (SPS) an das User-Interface gesendet werden. Diese werden anschliessend wieder abgespielt. Während der Operator den aufgezeichneten unverdächtigen Verkehr sieht und keinen Verdacht schöpft, können im Hintergrund manipulierte Befehle an die SPS gesendet werden. Zu diesem Zweck manipuliert die Schadsoftware eine *Dynamic Link Library (DLL)*, welche als Vermittler zwischen SPS und der Monitoring Software dient. Die Schadsoftware prüft ebenfalls die Laufumgebung auf die Existenz von Sandboxen und Analysewerkzeugen, wie diese vor allem von Sicherheitsforschern und Analysten verwendet werden. So funktionieren gewisse *Dropper* der *Schadsoftware* in einer Cuckoo oder VMware Umgebung nicht.

---

[35] http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest_xg_en.pdf (Stand: 31. August 2016).

[36] https://www.fireeye.com/blog/threat-research/2016/06/irongate_ics_malware.html (Stand: 31. August 2016).

Die Schadsoftware zielt auf die von Siemens entwickelte Software «S7 PLCSIM» ab und scheint spezifisch auf eine bestimmte Anlage ausgerichtet worden sein. FireEye vermutet das Ziel in der Biogas-Industrie. Dies lässt zumindest eine gefundene Datei mit Namen biogas.exe vermuten. Das ProductCERT von Siemens bestätigte, dass der Schadcode in einer Standard-Kontrollumgebung nicht funktioniert. Die Schadsoftware ist anscheinend auf das Funktionieren in einem Simulator ausgerichtet, was eher drauf hindeutet, dass es sich um ein Forschungsprojekt oder um einen Test handelt. Die Malware zeigt aber eine sehr hohe Qualität und Wandelbarkeit der Entwicklung, so dass hier von einer nächsten Generation von Stuxnet gesprochen werden kann. Urheber und Verwendungszweck dieser Malware bleiben unbekannt. Die Schadsoftware wurde 2014 auf Virustotal hochgeladen, was die Existenz seit mindestens diesem Datum bestätigt.

5.3.4 US-Regierung und Autohersteller vereinbaren Sicherheitszusammenarbeit

Die Sicherheit von Transportmitteln und insbesondere von Autos hat MELANI bereits in seinen beiden letzten Halbjahresberichten thematisiert. Das US-amerikanische Transportministerium hat Anfang dieses Jahres eine Absichtserklärung bezüglich Sicherheit bei Fahrzeugen mit 18 namhaften Autoherstellern unterzeichnet. Dies unter anderem in Anbetracht der zunehmend eingesetzten Informatik bei normalen Autos und der Entwicklungen im Bereich der autonomen Fahrzeuge. Neben allgemeinen Bekenntnissen zu vorausschauender Beachtung von Sicherheitsrisiken, gegenseitigem Informationsaustausch und Zusammenarbeit zur Erhöhung der Sicherheit im Strassenverkehr, bezieht sich ein explizit ausgewiesener Punkt auf die Verbesserung der Cyber-Sicherheit von Fahrzeugen. Der Fokus liegt aber primär bei der physischen Unversehrtheit von Personen (safety); die Sicherheit von Systemen (security) wird dabei subsidiär, als mögliche Ursache für die Gefährdung der Personensicherheit, behandelt.

Schlussfolgerung:

Immer mehr Assistenzdienste werden in Autos eingebaut und funktionieren computergesteuert. Das Vertrauen der Nutzer in das korrekte Funktionieren dieser Systeme ist unabdingbar. Besonders deutlich wird das bei selbstfahrenden Autos: Damit diese dereinst auf der Strasse allgemein akzeptiert werden, müssen ihnen alle Verkehrsteilnehmer ein grosses Mass an Grundvertrauen entgegenbringen.

5.3.5 Autoklau per Elektronik

Die Personensicherheit (safety) wird von Autoherstellern sehr ernst genommen (siehe Kapitel 5.3.4). Dieser Bereich ist tendenziell reguliert. Die Hersteller müssen mit Schadenersatzklagen rechnen und gegebenenfalls aufwändige Rückrufaktionen tätigen, sollten sie mangelhafte Produkte ausliefern, die Schaden verursachen oder Leben gefährden. Auf der anderen Seite befinden sich Systeme im und am Auto, die mit dem Fahren an sich nichts zu tun haben: Statt herkömmliche physische Schlüssel werden beispielsweise Funk-Schlüssel eingesetzt oder die Öffnung der Türen erfolgt sogar bereits über eine Handy-*App*. Viele Neuwagen haben gar keine Schlüssellöcher mehr, sondern werden ausschliesslich auf elektronischem Weg ver- und aufgeschlossen.

Bei dieser Entwicklung scheinen einige Hersteller die Funktionalität oder Geschwindigkeit der Markteinführung zu Lasten der Sicherheit (security) zu priorisieren: Zuerst waren manche

Funkschlösser so simpel, dass ein Autodieb lediglich das Signal abfangen und aufzeichnen musste. Das alleinige Wiederabspielen des aufgezeichneten Signals ermöglichte es dem Angreifer, die Autotür zu öffnen. Als dann Produkte auf den Markt kamen, die das Auto automatisch entsperren, sobald man sich ihm nähert, fanden Autodiebe schnell heraus, dass die Anwesenheit des Schlüssels mit präparierten Funkgeräten vorgetäuscht werden kann. Ein Komplize muss sich dazu lediglich in die Nähe des Besitzers begeben und das vom «Schlüssel» ausgehende Signal per Funk an den Dieb weiterleiten, der neben dem Auto steht (Relais-Attacke oder Relay Station Attack). Erschwerend kommt hinzu, dass bei diesen Systemen häufig auch der Motor per Knopfdruck gestartet werden kann, wenn das System das Funksignal des Schlüssels im Inneren des Autos erkennt. Oft kann die Methode, wie das Auto gestohlen wurde, nicht oder nur schwer nachvollzogen werden. So werden die Diebstähle einfach angezeigt und der Versicherung angemeldet. Die Hersteller haben keinen grossen Druck, ihre Produkte mit möglichst sicheren Schliesssystemen auszurüsten, solange die Versicherungen für den Schaden aufkommen.

Die Informatisierung bei Autos birgt nicht nur die Gefahr, dass sie gehackt und gestohlen werden. Wenn das Handy zum Interface zwischen Fahrer und Fahrzeug wird, kann man durch Infiltration des Mobiltelefons oder sonstiger Ausnützung dieser Schnittstelle auch Unfug treiben: Zum Beispiel war es beim Elektroauto «Nissan Leaf» möglich, mit der entsprechenden App und der Kenntnis der Fahrgestellnummer, die im Frontfenster des Wagens ablesbar ist, Daten auszulesen und die Klimaanlage zu bedienen. Zwar liess diese App keinen Zugriff auf die Fahrzeugelektronik zu. Es war aber immerhin möglich, durch die Aktivierung der Klimaanlage den Akku des Autos langsam aber sicher zu entladen.

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).

DOKU

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

5.4 Angriffe

5.4.1 Cyberbankräuber stehlen 81 Mio US-Dollar

Gemäss der Nationalbank von Bangladesch stahlen Hacker die Zugangsdaten zu ihrem internen Zahlungssystem[37]. Hacker drangen in die Systeme der Nationalbank von Bangladesch ein und Installieren ihrer speziell für diese Systeme programmierten Softwarewerkzeuge. Die Angreifer manipulierten die Datenbank, z. B. die Schnittstellen zur Swift-Clientsoftware, die für den internationalen Zahlungsverkehr zuständig ist. Dabei wurden nicht nur gefälschte Transaktionen ausgelöst, sondern auch die Spuren in den Protokollen verwischt. So wurde z. B. das Ausdrucken von Bestätigungen der Transaktionen unterbunden, damit die Transaktionen so lange wie möglich unentdeckt blieben. Am 4. und 5. Februar 2016 missbrauchten Kriminelle das System zum Erstellen von mehreren Dutzend Aufträgen an die Federal Reserve Bank in New York, um vom Konto der Nationalbank von Bangladesch grosse Beträge auf Konten in den Philippinen und Sri Lanka zu überweisen. Vier solcher Aufträge im Umfang von 81 Mio. US-Dollar und mit dem Ziel Philippinen wurden erfolgreich transferiert. Bei der fünften Transaktion im Umfang von weiteren 20 Mio. US-Dollar fiel der vermittelnden Leitbank ein Tippfehler auf. Die Hacker buchstabierten den Namen einer Nichtregierungsorganisation in Sri Lanka falsch, was die Leitbank veranlasste, bei der Nationalbank von Bangladesch nachzufragen. Diese stoppte umgehend die Transaktion. Gleichzeitig fiel der Federal Reserve Bank of New York eine unüblich hohe Anzahl von Zahlungsaufträgen an private Empfänger auf. Die alarmierte Nationalbank von Bangladesch konnte auch diese gefälschten Transaktionen stornieren und damit einen Verlust von rund 850 Mio. US-Dollar verhindern. Die vier erfolgreichen Transaktionen wurden in philippinischen Casinos in Spielchips getauscht, wo sich die Spur des Geldes verliert, da im Spielbankenwesen eine geringere Aufsichtsdichte besteht als im klassischen Finanzsystem.

Bei diesem bisher grössten Cyber-Betrug gegen eine einzige Bank beschuldigten die Verantwortlichen der Strafverfolgungsbehörden Bangladeschs die Swift der Nachlässigkeit. Nach ihrer Ansicht sei die Swift dafür zuständig, nach Installation ihres Systems die ganze Systemlandschaft der Bank nach Schwachstellen abzusuchen. Die Swift ihrerseits wies umgehend jede Verantwortung bezüglich des erfolgten Angriffs von sich. Die Nationalbank von Bangladesch sei wie alle anderen Swift-Kunden für die Sicherheit ihrer Systeme und Umgebung zuständig, die Schnittstellen zum Swift-System aufweisen. Dies erinnert an die Diskussionen, die nach den ersten Betrugsfällen mit Schadsoftware im E-Banking geführt wurden; Inwiefern hat eine Bank eine betrügerische Zahlung zu verantworten bzw. inwiefern hat der Kunde seine Sorgfaltspflicht verletzt, wenn der Computer des Kunden mit Schadsoftware infiziert ist? Die Banken haben damals reagiert und die Sicherheit der E-Banking-Systeme erhöht. Auch die Swift hat inzwischen reagiert und pocht strenger auf die Einhaltung der Sicherheitsvorgaben[38].

Am 12. Mai 2016 wurde ein weiterer Vorfall gegen eine Geschäftsbank in Vietnam entdeckt. Dabei soll unter Verwendung des Swift -Netzwerks, das für standardisierte Transaktionen

---

[37] http://www.reuters.com/article/us-usa-nyfed-bangladesh-malware-exclusiv-idUSKCN0XM0DR (Stand: 31. August 2016).

[38] http://www.theregister.co.uk/2016/06/03/swift_threatens_insecure_bank_suspensions/ (Stand: 31. August 2016).

verwendet wird, eine betrügerische Transaktion von 1,13 Mio. US-Dollar ausgelöst worden sein. In einem dritten Fall soll eine ecuadorianische Bank betroffen sein .

Im Bericht des Sicherheitsdienstleisters Symantec[39] wird erwähnt, dass die Schadsoftware-Komponente, welche die Spuren verwischt (*Wipe-Komponente*), schon in der «Operation Blockbuster» verwendet worden ist. «Blockbuster» war für den Angriff auf Sony im November 2014 verantwortlich. Im Fall in Vietnam wurden identische, im Fall Bangladesch modifizierte Funktionen dieser Komponente gefunden. Es ist nicht klar, ob die gleichen Angreifer hinter den Angriffen auf die Banksysteme stecken, oder ob dieser Programmcode im Cyber-Untergrund verkauft oder geteilt worden ist.

Schlussfolgerung:

Angriffe auf E-Banking Kunden gehören seit Jahren zum Standardrepertoire von Cyberkriminellen. Spätestens, seit vor eineinhalb Jahren mit der Schadsoftware Carbanak auch direkt Bankennetzwerke angegriffen wurden, ist klar, dass beim elektronischen Bankraub ein ähnlich grosser Aufwand wie im Bereich hochentwickelter Spionage betrieben wird, sofern die Ertragsaussichten stimmen. Eine ausführliche Einschätzung zu diesem Trend finden Sie in Kapitel 6.1.

5.4.2 Carbanak 2.0 und ähnliche Angriffe

Vor zwei Jahren sorgte ein Angriff mit dem Namen «Carbanak» für Unruhe in der internationalen Finanzwelt. Das erste Mal zielten die Cyberbetrüger nicht auf einen Endkunden, sondern direkt auf die Bank. Die angewendeten Werkzeuge, die Professionalität und Hartnäckigkeit glichen den Angriffen, wie man diese von sogenannten *Advanced Persistent Threats (APT)* her kennt. Die Logik der Kriminellen ist relativ einfach: Der Aufwand ist zwar grösser, der Ertrag steigt aber auch um ein Vielfaches. Zwischenzeitlich war die Gruppe für einige Zeit ruhig. Bereits im September 2015 gab es aber wieder Anzeichen einer Aktivität bei einem Opfer.[40] Im Februar 2016 bestätigte das Softwareunternehmen Kaspersky die Rückkehr von «Carbanak 2.0». In einem weiteren Artikel will ein Forscherteam des Unternehmens für Cyber-Sicherheit, Proofpoint, Vorbereitungen der Carbanak-Bande zu Angriffen auf Banken in Europa, dem Mittleren Osten und den USA entdeckt haben.[41]

Ein Merkmal von «Carbanak 2.0» ist, dass die Gruppe nicht nur Banken im Visier hat, sondern seinen Opferkreis auch auf Buchhaltungsabteilungen anderer Unternehmen ausgeweitet hat. In einem Fall änderten die Angreifer Eigentumsverhältnisse eines grossen Unternehmens. Ein Strohmann wurde als Anteilseigner des Unternehmens eingeschleust. Was die Angreifer allerdings damit vorhatten ist nicht bekannt. Der Vorfall wurde entdeckt, bevor ein Schaden entstanden ist[42]

---

39 http://www.symantec.com/connect/blogs/swift-attackers-malware-linked-more-financial-attacks (Stand: 31. August 2016).

40 https://www.csis.dk/en/csis/blog/4710/ (Stand: 31. August 2016).

41 https://www.proofpoint.com/uk/threat-insight/post/carbanak-cybercrime-group-targets-executives-of-financial-organizations-in-middle-east (Stand: 31. August 2016).

42 https://securelist.com/blog/research/73638/apt-style-bank-robberies-increase-with-metel-gcman-and-carbanak-2-0-attacks/ (Stand: 31. August 2016).

«Carbanak» ist allerdings nur der erste Fall einer Serie von ähnlichen Vorfällen. Die Cyber-Kriminellen lernen schnell, integrieren neue Techniken in ihre Operationen und greifen immer öfter die Banken direkt an. Zwei weitere Gruppen mit dem Namen «Metel» und «GCMAN» operieren beispielsweise nach dem gleichen Schema. Die Gruppe «Metel» agiert ähnlich der Gruppe «Carbanak». In den bislang beobachteten Fällen leerten Kriminelle nachts in russischen Städten Geldautomaten unterschiedlicher Banken. Der andere Teil der kriminellen Gruppe manipulierte die betroffenen Konten dahingehend, dass der Kontostand wieder auf den Betrag von vor dem Geldbezug angehoben wurde. «GCMAN» hingegen führt Transaktionen von 200 US-Dollar im Minutentakt auf *e-Currency Dienste* wie BitCoin, Perfect Money oder Payza aus. Das spezielle an «GCMAN» ist, dass sich die Angreifer während 18 Monaten unbemerkt im Netzwerk bewegt hatten.

5.4.3 Ransomware in Spitälern

Die seit Jahresbeginn beobachtete Welle an *Ransomware* trifft auch kritische Infrastrukturen. In letzten Zeit waren häufig Spitäler ein Ziel der Erpresser. Mit der Digitalisierung ist die Informatik eines Spitals auch für die Behandlung der Patienten zentral geworden. Im ersten Halbjahr 2016 wurden mehrere Fälle in Spitälern in Deutschland und den USA bekannt, in denen teils grosse Summen erpresst und auch bezahlt wurden, um wieder auf die Infrastruktur zugreifen zu können. Im Kansas Heart Hospital haben die Täter nach einer ersten Zahlung nicht alle Dateien freigegeben und erneut Lösegeld verlangt. Die Spitäler scheinen zur Zielkategorie mit den höchsten Erpressungssummen zu werden. Die Täter wissen, dass ein Spital schnell reagieren und seine Informatikinfrastruktur zur Verfügung haben muss, um Leben zu retten. Deshalb stellt dieser Sektor ein bevorzugtes Ziel dar.

Eine weitere Herausforderung für Spitäler ist, dass Diagnose- und Analysegeräte zunehmend computergesteuert sind. Diese Geräte werden für die Anwendung im medizinischen Bereich getestet und zertifiziert. Meist kann die Informatikabteilung des Spitals deren Betriebssystem nicht aktualisieren oder Virenschutzprogramme darauf installieren, weil sonst das Gerät verändert würde und die Zertifizierung verloren ginge. Zudem fehlt es den Informatikabteilungen der Spitäler oft an Ressourcen oder Fachwissen, um ein Update solch spezifischer Systeme vorzunehmen.

Früher konnten diese Systeme netzunabhängig betrieben werden. Mit der Vernetzung der Geräte zur digitalen Behandlungskontrolle werden aber immer mehr anfällige Systeme, deren Sicherheit nicht gewährleistet werden kann, an das Informatiknetz eines Spitals angebunden. In diesem Zusammenhang ist die Zusammenarbeit mit den Gerätelieferanten und deren Sensibilisierung von grösster Bedeutung.

Schliesslich können auch digitalisierte Patientendaten einen Wert für die Angreifer haben. Die persönliche Krankenakte kann zu einem Spionage- oder Sabotageziel werden. Massendaten über Behandlungen, ihre Ergebnisse und Merkmale sind sehr hilfreich für die Weiterentwicklung von bestehenden und die Suche nach neuen Behandlungen mit der sogenannten Big-Data-Analyse. So werden sie auch für Einzelpersonen und Unternehmen mit illegalen Absichten zum begehrten Objekt. Deshalb sind bei der Digitalisierung der Patientenakten die richtigen Fragen zu stellen, namentlich welche Risiken bestehen, wie diese minimiert werden können und schliesslich ein Vorgehen festzulegen, falls Patientinnen und Patienten der Verlust ihrer Daten kommuniziert werden muss.

5.4.4 Geldautomaten in Japan geplündert

In einer gross angelegten und koordinierten Aktion wurden in Japan am Sonntag, dem 15. Mai 2016, zwischen 5 und 8 Uhr morgens rund 1‘700 Geldautomaten um umgerechnet fast

17 Millionen Franken erleichtert. Damit die über 14‘000 Abhebungen in so kurzer Zeit ausgeführt werden konnten, wurden ungefähr 600 Personen mit bis zu 1‘600 gefälschten Kreditkarten ausgestattet. Auf den Magnetstreifen der gefälschten Karten waren gestohlenen Daten von Kunden der South African Standard Bank gespeichert.

Ausländische Kreditkarten wurden von japanischen Geldautomaten früher kaum akzeptiert. Die Regierung hatte deshalb vor einiger Zeit die Banken dazu aufgerufen, dies zu ändern, um ausländischen Touristen die Geldbezüge zu erleichtern. Eine Vielzahl von Geldautomaten ist aber scheinbar noch nicht darauf ausgerichtet, den Chip auf der Kreditkarte auszulesen. Diese Geräte greifen deshalb immer noch auf den einfach zu kopierenden Magnetstreifen zurück. Die Vorfälle zeigten auch, dass die Detektion betrügerischer Abhebungen mit ausländischen Kreditkarten noch verbessert werden muss.

Ein Grund für die ausserordentliche Höhe des Schadens dürfte darin liegen, dass die Bezugslimite bis zum Zeitpunkt des Vorfalls an vielen Geldautomaten entweder 100‘000 oder 200‘000 Yen betrug (dies entspricht etwa Fr. 900.- respektive Fr. 1‘800.-). Als Reaktion wurden die Limiten auf maximal 50‘000 Yen reduziert.

5.4.5 Anonymous & Co: #Kampagnen

Das erste Halbjahr 2016 war geprägt durch zahlreiche teils intensive Aktivitäten von Hacktivisten gegen Organisationen, die diese als Machtzentren betrachten.

Bereits Anfang Jahr rief das Anonymous-Kollektiv dazu auf, «zu den Waffen zu greifen». Geplant war ein erneuter Angriff auf das globale Finanzsystem mit dem mythologischen Namen «Operation Ikarus». «Wie Ikarus seien die Mächtigen zu nahe an der Sonne geflogen und es sei die Zeit gekommen, die Schwingen des Imperiums in Brand zu setzen ...».[43] Die Operation sei bereits zum Zeitpunkt von Occupy Wallstreet im Jahr 2011 geplant gewesen - als Online-Pendant zu den Protesten vor Ort.[44] Am 4. Mai 2016 wurde dann in einem auf YouTube ausgestrahlten Video eine «30-day campaign against central bank sites across the world» angekündigt. Anonymous überflutete gleichentags mit Hilfe der Hackergruppe «Ghost Squad» die Website der griechischen Zentralbank mit Webanfragen, so dass deren Server über mehrere Stunden nicht erreichbar waren. Über den ganzen Monat Mai legte die Kampagne #OpIcarus unter anderem die Websites von über 30 Zentralbanken lahm. Die berühmtesten Opfer waren die Bank of England, die New Yorker Börse und die Vatikanbank. Die Angriffe hatten eine Stärke von gut 250 Gbps.[45] Anonymous veröffentlichte die vollständige Liste der Ziele, die über 200 Websites enthielt und kündigte auf Twitter an, dass dies noch nicht alles sei.

Die Hackergruppe Ghost Squad, eine frühere Untergruppe von Anonymous[46], hatte dann für den Monat Juni analog die Operation «#OpSilence» angekündigt. Ziel war es, diejenigen

---

43 https://opicarus.wordpress.com/ (Stand: 31. August 2016).

44 http://www.ibtimes.co.uk/opicarus-anonymous-hacker-reveals-inspiration-behind-latest-operation-evolution-hacktivism-1561457 (Stand: 31. August 2016).

45 http://thefreethoughtproject.com/anonymous-hits-york-stock-exchange-world-bank-vatican-total-corporate-media-blackout-ensues/ (Stand: 31. August 2016).

46 http://thefreethoughtproject.com/not-anonymous-hacking-group-declares-war-mainstream-takes-cnn-fox/ http://anonhq.com/anonymous-opsilence/ (Stand: 31. August 2016).

Medien zu bestrafen, die gar nicht oder nur einseitig über den Krieg in Palästina oder die tatsächlichen Verbrechen in Syrien berichteten.[47] «Ghost Squad»[48] hielt sich allerdings nicht an den Termin und legte bereits am 31. Mai los, indem sie die E-Mail-Systeme der Nachrichtendienste CNN und FOX News während mehreren Stunden ausser Gefecht setzten. Ausserdem kündigten sie für den ganzen Monat Juni weitere Attacken gegen Medien an. Als mögliche Ziele wurden NBC und MSN genannt; es blieb jedoch bei leeren Drohungen. Interessanter Nebenschauplatz war, dass die Gruppe Ghost Squad Wert darauf legte, dass es sich um eine eigenständige Operation handelt und sie nichts (mehr) mit Anonymous zu tun habe

Schlussfolgerung:

Die lockere Anbindung von Anonymous und ähnlichen Gruppen wie GhostSquad resultiert in einer Reihe unkoordinierter, mehr oder weniger spektakulärer Ankündigungen und Angriffen. Da es strukturinhärent keine Mitgliedschaft bei Anonymous gibt und keine offiziellen Sprecher oder sonst wie für die gesamte Bewegung verantwortliche Personen existieren, kann prinzipiell jeder im Namen von Anonymous Mitteilungen veröffentlichen und so ein Medieninteresse generieren.

5.4.1 xDedic: Zugang zu gehackten Servern im Online-Laden kaufen

Im Juni hat Kaspersky Einzelheiten zu einer Ermittlung zum Untergrundmarkt namens xDedic veröffentlicht, welche zusammen mit einem europäischen Internetdienstleister durchgeführt worden ist. Seit 2014 wurde dort der Zugang zu rund 70 000 gehackten Servern mittels *Remote Desktop Protocol* (für den Fernzugriff auf einen Windows-Server) angeboten - und war schon ab 6 US-Dollar zu haben. Solche Server werden dann als Ausgangspunkt für weitere Angriffe (*DDoS, Spam* etc.) genutzt, oder der Zugriff zielt direkt auf die Daten oder Programme auf dem Server ab. Besonders interessant sind beispielsweise Server mit Zugang zu Bezahlterminals. Kurz nach dem Kaspersky-Bericht war die Seite verschwunden, tauchte später aber auf dem *TOR-Netzwerk* wieder auf.

Schlussfolgerung:

Dieser Fall ist repräsentativ für den Trend zu immer mehr Arbeitsteilung im kriminellen Cyber-Untergrund. So können Akteure mit kleinerem Knowhow auf eine ganze Palette von Diensten zurückgreifen, um mit minimalem Zeitaufwand und Fachwissen Angriffe vorzunehmen. Nach der Aufdeckung durch Kaspersky verschwand die Seite, um dann auf einer Plattform mit mehr Anonymität für Administratoren, Verkäufer und Käufer wieder aufzutauchen. Das zeigt, dass Betreiber einen rentablen Markt an die Gegebenheiten anzupassen wissen, um ihn am Laufen zu halten.

[47] http://news.softpedia.com/news/anonymous-announces-opsilence-month-long-attacks-on-mainstream-media-504760.shtml (Stand: 31. August 2016).

[48] http://thefreethoughtproject.com/not-anonymous-hacking-group-declares-war-mainstream-takes-cnn-fox/ (Stand: 31. August 2016).

5.5 Präventive Massnahmen

Neben der Sensibilisierung ist die effektivste präventive Massnahme das Verhaften der Cyberkriminellen. Vielerorts herrscht die Meinung, Verhaftungen im Cyberbereich seien schwierig bis unmöglich. Diversen Razzien zeigen jedoch, dass auch auf diesem Gebiet Erfolge erzielt werden.

5.5.1 Razzia im Darknet

So wurde bei einer internationalen Razzia gegen Betreiber und Nutzer illegaler Webplattformen neun Verdächtige festgenommen. Zusätzlich wurden 69 Wohnungen und Firmen in Deutschland, der Schweiz, Frankreich, den Niederlanden, Litauen und Russland durchsucht. Neun dringend Tatverdächtige wurden festgenommen. Die Ermittlungen richteten sich gegen verschiedene deutschsprachige Foren der Underground Economy. In diesen wurden illegale Güter wie Waffen, Betäubungsmittel, Falschgeld, gefälschte amtliche Ausweise und ausgespähte Daten wie Kreditkarten- und Online-Banking-Daten gehandelt. Darüber hinaus umfasste die Angebotspalette auch kriminelle Dienstleistungen, beispielsweise *DDoS*-Attacken oder die Infektion von Computern mit *Schadsoftware*.

Mutmasslicher Hauptbetreiber von insgesamt drei Foren ist ein 27-jähriger bosnischer Staatsangehöriger. Der Beschuldigte wurde am 24. Februar 2016 in Bosnien-Herzegowina festgenommen und befindet sich in Untersuchungshaft.

Es konnte umfangreiches Beweismaterial sichergestellt werden, insbesondere zahlreiche PCs und Speichermedien, eine Schusswaffe, Betäubungsmittel und Vermögenswerte in Höhe von ca. 150‘000,00 Euro. Zudem wurden mehrere Server in Frankreich, den Niederlanden, Litauen und Russland beschlagnahmt, auf welchen kriminelle Online-Marktplätze betrieben wurden. Ein entsprechender Hinweis, dass die Server beschlagnahmt wurden, wurde auf den zugehörigen Webseiten aufgeschaltet.[49]

49 https://www.bka.de/SharedDocs/Pressemitteilungen/DE/Presse_2016/pm160229_UndergroundEconomy.pdf?__blob=publicationFile&v=1 (Stand: 31. August 2016).

Abbildung 10: Banner, das die Polizei auf den beschlagnahmten Webservern hinaufgeladen hat.

Schlussfolgerung:

Die vorliegende Aktion ist ein erneuter Beweis dafür, dass es im Internet keine vollständige Anonymität gibt. Sie unterstreicht zudem die Bedeutung der internationalen Zusammenarbeit bei der Bekämpfung der Internetkriminalität.

5.5.2 Aktivität von «Angler» und «Nuclear» Explot Kits verschwunden

Die beiden wohl bekanntesten *Exploit Kits* sind im ersten Halbjahr 2016 nahezu von der Bildfläche verschwunden. Die Gründe für deren Verschwinden sind allerdings unterschiedlich. Im April 2016 wurde durch das Sicherheitsunternehmen Check Point eine Analyse mit zahlreichen Details über «Nuclear» enthüllt. Dies dürfte die Betreiber derart erschreckt haben, dass diese untergetaucht sind und zumindest temporär ihr Geschäft eingestellt haben. Seit dem 30. April wurden vom französischen Exploit-Kit-Experten «Kafeine» keine Attacken durch «Nuclear» mehr festgestellt.[50]

Das «Angler»-Exploit ist laut Kafeine seit dem siebten Juni total verschwunden. Es stellt sich auch hier die Frage, was der Auslöser dieses plötzlichen Verschwindens ist. Eine mögliche Erklärung ist eine durch die russischen Behörden zu diesem Zeitpunkt durchgeführte Verhaftung von 50 mutmasslichen Cyber-Kriminellen, welche mit der Schadsoftware «Lurk» in Verbindung standen. Die Verhafteten sollen Gelder von russischen Bankkonten mittels einem Trojaner gestohlen haben. Der Infektionsvektor von diesen Angriffen steht in direktem Zusammenhang mit dem «Angler» Exploit Kit. Fraglich ist, ob tatsächlich Teile der Autoren des «Angler» Exploit Kits verhaftet worden sind oder ob diese lediglich kalte Füsse bekommen haben, aus Angst, dass die Verhafteten andere Kriminelle verraten könnten. Wer jedoch gehofft hat, dass die Verwendung von Exploit Kits bei Kriminellen nach dem Wegfall von «Angler» abnimmt, wurde leider enttäuscht. Der Einsatz der Kits hat sich lediglich verschoben: Nach dem Ende vom «Angler» hat die Benutzung des «Neutrino» Exploit Kits stark zugenommen

[50] http://www.securityweek.com/exploit-kit-activity-down-96-april (Stand: 31. August 2016).

5.5.3 Mehrere Verhaftungen in verschiedenen Ländern der Hintermänner zu «Dyre»

Im Februar meldete die Nachrichtenseite Forbes[51], im November 2015 hätten russische Behörden das *Botnetz* des e-Banking Trojaners Dyre lahmgelegt und die führenden Mitglieder der kriminellen Organisation festgenommen. Der laut IBM aktivste Banking-Trojaner des Jahres 2015, der für ungefähr 25% der weltweiten Bank-Betrugsfälle verantwortlich war, verbreitete sich zuvor auch in der Schweiz lawinenartig. Zu Beginn hatte der Trojaner vor allem KMUs im Visier. So gelang es den Betrügern, ein Unternehmen aus dem Kanton Freiburg um einen siebenstelligen Betrag zu erleichtern.[52] Zwischenzeitlich konzentrierte sich «Dyre» auch auf Privatanwender. Obwohl die vermutlich von russischer Seite angeordnete Razzia offiziell nicht bestätigt wurde, haben die Aktivitäten von «Dyre» aufgehört, was die Malware-Statistik des GovCERT.ch deutlich zeigt. Es verbleiben nunmehr die Infektionen nie bereinigter Systeme. Gemäss Forbes ist dies jedoch noch nicht das Ende der «Dyre»-Malware; der *Source-Code* ist seit kurzem frei im Internet erhältlich.

6 Tendenzen und Ausblick

6.1 Hochentwickelte Angriffe – APT nun auch bei Kriminellen

Vermehrt betreiben Kriminelle für höhere Erträge auch einen grösseren Aufwand, gehen gezielter vor und versuchen, Aufwand und Ertrag zu optimieren. Neben den Angriffen auf das Interbanken-Nachrichtensystem Swift zu Beginn dieses Jahres (Kapitel 5.4.1) und den Angriffen, die sich «Carbanak» zuschreiben lassen (Kapitel 5.4.2), entwickeln sich auch die Angriffe gegen die Endkunden rasant weiter. Die Arbeitsteilung und Wiederverwertung von Schadsoftware im digitalen Untergrundmarkt begünstigt diesen Trend.

Lange Zeit galt bei Betrügereien der Grundsatz, dass der Aufwand möglichst klein gehalten wird. Somit war das am schlechtesten geschützte System das lohnendste Ziel. Diese «Low hanging fruits» waren vor allem Computer von Endkunden, über welche beispielsweise E-Banking-Geschäfte getätigt werden. Ein direkter Angriff auf Finanzinstitute war noch vor ein paar Jahren Film und Fernsehen vorbehalten. Der Aufwand und die erforderliche Professionalität wurden damals als zu hoch eingeschätzt. Der Trend zu spektakulären Cyber-Raubzügen erstaunt allerdings dennoch nicht und hat verschiedene Gründe:

- Zum einen ist die für solch komplexe Angriffe notwendige Software mittlerweile im Untergrundmarkt erhältlich. Das Know-How ist auch bei den Kriminellen angekommen. Dieser Umstand wird unter anderem dadurch begünstigt, dass die Trennlinie zwischen staatlich unterstützten und kriminellen Angriffen immer unschärfer wird.

- Ein weiterer wichtiger Grund ist das mittlerweile schwieriger gewordene Waschen des Geldes. Personen zu finden, die naiv genug sind, sich als sogenannte Finanzagenten (Money Mules) rekrutieren zu lassen, ist glücklicherweise eine Herausforderung geworden. Für die Kriminellen kommt erschwerend hinzu, dass ein Finanzagent in der

[51] http://www.forbes.com/sites/thomasbrewster/2016/02/08/russia-arrests-dyre-malware-masterminds/#5d5cf29a1e02 (Stand: 31. August 2016).

[52] http://www.20min.ch/digital/news/story/E-Banking-Trojaner-zielt-auf-Schweizer-Firmen-ab-23497999 (Stand: 31. August 2016).

Regel bereits nach einem einzigen Versuch aus dem Verkehr gezogen werden kann. Die Kriminellen suchen deshalb nach Alternativen, welche ohne Money Mules auskommen oder bei denen Money Mules effizient eingesetzt werden können. Die einfachste Möglichkeit, das Geld effizienter zu waschen, ist der Transfer von höheren Summen pro Money Mule. Dabei sind vor allem Firmen ins Visier der Kriminellen geraten, da dort grössere Überweisungssummen weniger auffallen.

Die in Kapitel 5.4.1 und 5.4.2 beschriebenen Vorfälle zeigen exemplarisch, dass weitere Wege gesucht und leider auch gefunden werden, um die Spuren des Geldflusses zu verwischen. So hat die Gruppe rund um die Schadsoftware «Carbanak» und «Metel» Geldautomaten so manipuliert, dass sie zu einer bestimmten Zeit Geld ausspuckten. Da die Auszahlung in bar erfolgt, erübrigt sich die Geldwäsche. Bei der Gruppe «GCMAN» wurden elektronische Währungen verwendet, bei denen eine Nachverfolgung des Geldflusses ebenfalls schwieriger ist. Beim Cyber-Bankraub gegen die Nationalbank von Bangladesch wurde das Geld aus den vier erfolgreichen Transaktionen in philippinischen Casinos in Spielchips getauscht, wo sich die Spur des Geldes anschliessend verliert. Im Spielbankenwesen besteht eine geringere Aufsichtsdichte als im klassischen Finanzsystem. Alles in allem lässt sich sagen, dass ein grösserer Ertrag auf Seiten der Kriminellen auch eine aufwändigere und professionellere Geldwäsche möglich macht.

Wer jetzt aber glaubt, dass die professionellen Angriffe die einfachen Angriffe verdrängen, der irrt. Die Erfahrung zeigt, dass die alten Angriffsformen nicht aussterben, sondern an eine andere Täterschaft weitergereicht werden. So sieht man immer noch zahlreiche *Phishing*-Versuche. Diese Angriffe sind zwar nicht mehr so erfolgreich wie früher, trotzdem finden diese immer noch statt und müssen abgewehrt werden. Der Kuchen wird also auf der einen Seite nicht nur neu verteilt, sondern insgesamt auch grösser.

6.2 Die Zukunft des Internets – Aus technischer und gesellschaftlicher Sicht

Die ersten Autos hatten kein Dach, geschweige denn einen Sicherheitsgurt oder sonst irgendwelche Vorrichtungen, um den Fahrer zu schützen. Man war ja sowieso praktische alleine auf der Strasse und war froh, dass sich das Gefährt überhaupt in die gewünschte Richtung bewegte. Ähnlich war es in den Pionierzeiten des Internets. Wie der US-amerikanische Computeringenieur, Danny Hillis, in den 80iger Jahren schön illustrierte: «There were only two other Dannys on the Internet then. I knew them both. We didn't all know each other, but we all kind of trusted each other.»[53] Man war froh, dass das Netzwerk überhaupt funktionierte. Im Strassenverkehr hat man mit der Zeit und nach steigender Anzahl von Unfällen Verkehrsregeln eingeführt, sichere Strassen gebaut und Vorschriften erlassen, dass die Autos mit Sicherheitsgurten, Knautschzonen, ABS und Airbags ausgerüstet werden müssen. Im Internet wurde jedoch die ursprüngliche Architektur grösstenteils belassen und verbindliche Internetverkehrsregeln gab es keine. Die Sicherheit wurde den Anwendern und Diensten überlassen, die das Internet nutzen. Um in unserer Analogie zu bleiben, müsste der Autofahrer einfach einen immer grösseren Helm tragen, aber dies auch nur freiwillig.

Physikalisch besteht das Internet aus 60‘000 einzelnen Netzwerken, sogenannten *Autonomen Systemen (AS)*. Diese werden vor allem von den grossen Telekomanbietern betrieben,

[53] https://www.ted.com/talks/danny_hillis_the_internet_could_crash_we_need_a_plan_b/transcript (Stand: 31. August 2016).

aber auch grössere und kleinere private und öffentliche Organisationen betreiben ihre AS. Innerhalb eines einzelnen AS hat der Betreiber die Kontrolle über sein Netzwerk, über die Grenzen des eigenen AS hinweg folgt man aber einem gemeinsamen Regelwerk, dem *Border Gateway Protokoll (BGP)*. BGP wurde in den 1980er Jahren für das Zusammenspiel einiger weniger Netzwerke entwickelt und regelt noch heute, welche Pfade unsere Datenpakete durchs weltweite Netz nehmen. Das macht das Rückgrat fehleranfällig und einfach zu beeinflussen. Wie der Fundus an Snowden-Dokumenten beweist, wurde dies auch ausgenutzt.

Eine Variante wäre nun, ein neues Internet auf der grünen Wiese zu bauen. Ansätze dazu wären vorhanden. So bietet beispielsweise das Projekt SCION der ETH Zürich einen schlanken Architekturansatz, der Pfadkontrolle, Fehlerisolation und vertrauensbasierte End-to-End Kommunikation ermöglichen würde. Doch bis sich so ein Ansatz bei den 60‘000 AS-Betreibern durchsetzt, wird wohl noch einige Zeit verstreichen. Anstatt die Basisstruktur für die Zukunft fit zu machen, wird weiter an neuen Applikationen getüftelt, die auf diesem veralteten Fundament immer neue Funktionaltäten anbieten. So dominieren die Big-Data und Blockchain Anwendungen die Schlagzeilen. Ob dies dazu führt, dass der Kern des jetzigen Internets doch noch aufgefrischt wird oder parallel eine neue Struktur entsteht, wird sich zeigen.

Wer Teil des Netzwerks sein will, muss notgedrungen auch die Nachteile in Kauf nehmen. Mit den Unzulänglichkeiten des Internets im Hinterkopf, steigt allerdings das Bewusstsein der Endanwender, dass sie selbst für die Wahrung ihrer Privatsphäre und ihrer Sicherheit sorgen müssen. So finden Anonymisierungs-Tools wie der *TOR-Browser* immer breitere Anwendung und End-to-End Verschlüsselung etabliert sich seit den Veröffentlichungen von Edward Snowden. Durch die Einbindung des Signal-Protokolls[54] im beliebten Whatsapp-Kurzmitteilungsdienst wird früher umständlich zu bedienende Spezialsoftware mehr und mehr massentauglich.

Am Ende liegt das Risikomanagement jedoch in der Verantwortung jedes Einzelnen, jeder Organisation, jedes Unternehmens. Fragen wie, wo sind welche Daten von mir gespeichert, wer kann darauf zugreifen, wie werden diese genutzt und wem verschaffen sie finanzielle Vorteile? nehmen dabei einen immer grösseren Stellenwert ein. Das Internet ist mittlerweile einem konstanten Spannungsfeld zwischen Innovation, Privatsphäre, Datensicherheit und letztlich der Rechtssicherheit ausgesetzt. Aufgrund der unaufhaltsamen Innovation können sich die Benutzer zudem nicht auf den einmal gegebenen Antworten ausruhen. Jeder wird laufend mit neuen Fragen konfrontiert. Anonymität und Privatsphäre werden immer schwieriger durchsetzbar. Diese Entwicklung illustriert der russische Service «Find Face» eindrücklich: Mit nur einem Porträtfoto einer Person ist es möglich, deren Account im sozialen Netzwerk VK.com zu finden. Derzeit gibt es diese App nur auf Russisch und ihr Zugriff beschränkt sich auf VK.com. Doch ist es lediglich eine Frage der Zeit, bis sich die Gesichtserkennung als App weltweit verbreitet. Ein Foto wird genügen, um eine Person zu identifizieren und sämtliche zugehörigen Informationen im Internet zu finden. Anonymität in der Öffentlichkeit ist dann Geschichte. Der Fortschritt im Internet wird das Recht auf Privatsphäre aufs Empfindlichste konkurrenzieren.

Die Gesellschaft muss darauf Antworten finden und vielleicht sogar eines Tages Grenzen definieren. Die Entwicklung des Internets aber auch die Entwicklung und die Veränderung

[54] Signal ist ein modernes Open Source Protokoll mit starker Verschlüsselung, das für asynchrone Messaging Systeme entwickelt wurde.

der gesellschaftlichen Normen sind noch lange nicht abgeschlossen. Es erwarten uns interessante Phasen der Entwicklung des Internets sowohl aus technischer, gesellschaftlicher aber auch aus rechtlicher und politischer Sicht.

7 Politik, Forschung, Policy

7.1 CH: Parlamentarische Vorstösse

Geschäft	Nummer	Titel	Eingereicht von	Datum Einreichung	Rat	Amt	Stand Beratung & Link
Ip	16.3606	Wer kümmert sich um die Cyber-Sicherheit in der Schweiz?	Derder Fathi	17.06.2016	NR	VBS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163606
Ip	16.3561	Nato-Erklärung. Hacker Angriffe können einen Bündnisfall auslösen	Josef Dittli	17.06.2016	SR	VBS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163561
Mo	16.3528	Kompetenz bei der Cyber-Defense	Ida Glanz-mann-Hunkeler	16.06.2016	NR	VBS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163528
Ip	16.3462	Sicherheit der elektroni-schen Patientendaten gewährleisten	Edith Graf-Litscher	15.06.2016	NR	EDI	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163462
Ip	16.3413	Cyber-Risiken und Nukle-ar-Anlagen	Bea Heim	09.06.2016	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163413
Ip	16.3394	Zusammenarbeit im Si-cherheitsbereich mit dem Fürstentum Liechtenstein	Josef Dittli	07.06.2016	SR	VBS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163394
Fr	16.1024	Interpol, Cyberrisiken und Cyberkriminalität	Hansjörg Knecht	07.06.2016	NR	EJPD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20161024
Po	16.3382	Sicherheit im Internet der Dinge. Kompetenzförde-rung	Claude Béglé	06.06.2016	NR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163382
Fr	16.1022	Aufklärung des Cyberan-griffs auf die Ruag	CVP Fraktion	02.06.2016	NR	VBS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20161022
Fr	16.1021	Cyberattacke auf die Ruag und das VBS. Die not-wendigen Konsequenzen ziehen!	Grüne Frak-tion	02.06.2016	NR	VBS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20161021
Fr	16.1020	Kontrollsystem und Kom-petenzzentrum als zu-kunftsweisende Instru-mente im Kampf gegen Cyberrisiken	Fraktion BD	02.06.2016	NR	VBS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20161020
Ip	16.3359	Wie unterstützt der Bund die Kantone in der Straf-verfolgung von DDOS-Attacken (Cyberangriffen) bei fehlendem Know-how?	Marcel Dobler	31.05.2016	NR	EJPD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163359
Ip	16.3356	Endlich Finanzen und Personal auf Kampf für Cyber-Sicherheit umverte-ilen	Sozialdemo-kratische Fraktion	31.05.2016	NR	VBS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163356
Ip	16.3353	Zweck des Sicherheits-verbundes Schweiz	Werner Salzmann	30.05.2016	NR	VBS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163353
Po	16.3348	Schaffung eines Rates für Cyberverteidigung. Vor-dringlich für unsere Sou-veränität und unsere Sicherheit	Claude Béglé	27.04.2016	NR	VBS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163348
Mo	16.3186	Cyberrisiken.Austausch technischer Informationen	Corina Eichenber-ger	17.03.2016	NR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163186
Po	16.3058	Abschaltung der analogen Telefonanschlüsse. Aus-wirkungen auf die Lifttele-fonie und andere Alarmsysteme	Hans Egloff	08.03.2016	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163058
Ip	16.3440	Was gibt es für technische Möglichkeiten, um die gesamte Schweizer Be-völkerung im Katastro-phenfall zu warnen?	Mathias Reynard	15.06.2016	NR	VBS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163440
Po	16.3381	Industrie 4.0. Schaffung	Claude	06.06.2016	NR	WBF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-

		einer nationalen Koordinationsstelle	Béglé				vista/geschaeft?AffairId=20163381
Ip	16.3337	Dynamische Festlegung der Mindestbandbreite gemäss Fernmeldedienstverordnung	Martin Candinas	24.04.2016	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163337
Mo	16.3336	Erhöhung der Internet-Mindestgeschwindigkeit in der Grundversorgung auf 10 Megabit pro Sekunde	Martin Candinas	27.04.2016	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163336
Po	16.3313	Massnahmen gegen Gaffer prüfen, welche Einsätze behindern oder Persönlichkeitsrechte verletzen	Bernhard Guhl	27.04.2016	NR	EJPD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163313
Ip	16.3296	Überall Wi-Fi, nur nicht in Schweizer Zügen?	Derder Fathi	26.04.2016	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163296
Ip	16.3272	Fintech als Herausforderung für die Schweiz	Elisabeth Schneider-Schneiter	26.04.2016	NR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163272
Po	16.3245	Prüfung der Aufteilung der Swisscom in eine öffentliche Netzgesellschaft und eine private Dienstleistungsfirma	Balthasar Glättli	18.03.2016	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163245
Po	16.3219	Roadmap für die elektronische Stimmabgabe	Marco Romano	18.03.2016	NR	BK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163219
Mo	16.3184	Digitalisierung und informatische Bildung. Gemeinsame Weiterentwicklung des digitalen Bildungsraums	Jonas Fricker	17.03.2016	NR	WBF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163184
Ip	16.3162	Rachepornografie	Yvonne Feri	17.03.2016	NR	EJPD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163184
Mo	16.3128	Nationaler Aktionsplan zur Reduzierung des digitalen Grabens	Jean Christophe Schwaab	16.03.2016	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163128
Mo	16.3120	Die KMU retten und stärken. Mit dem Innovationsbon und weiteren konkreten Instrumenten	Corrado Pardini	16.03.2016	NR	WBF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163120
Po	16.3051	Abschaltung der analogen Telefonanschlüsse. Auswirkungen auf die Lifttelefonie und andere Alarmsysteme	Joachim Eder	08.03.2016	SR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163051
Mo	16.3007	Modernisierung der Mobilfunknetze raschestmöglich sicherstellen	Kommission für Verkehr und Fernmeldewesen NR	01.02.2016	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163007
Ip	16.3555	Autonomes Fahren. Rahmenbedingungen und Folgen	Susanne Leutenegger Oberholzer	17.06.2016	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163555
Mo	16.3526	Stopp der Täuschung der Schweizer Konsumentinnen und Konsumenten. Keine Schweizer Telefonnummern zur Vortäuschung wirtschaftlicher Tätigkeiten in der Schweiz	Jean-François Steiert	16.06.2016	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163526
Mo	16.3452	Roaminggebühren. Jetzt ist genug	Elisabeth Schneider-Schneiter	15.06.2016	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163452
Fr	16.5294	Wie gedenkt der Bundesrat die Steuerung der „Digitalen Schweiz“ zu verstärken?	Derder Fathi	08.01.1900	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20165294
Ip	16.3387	Ist die elektronische Rechnung ohne digitale Signatur mehrwertsteuerkonform?	Fabio Regazzi	07.06.2016	NR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163387

Mo	16.3310	Drohnen. Bevölkerung vor Gefährdung schützen	Susanne Leutenegger Oberholzer	27.04.2016	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163310
Po	16.3260	Einführung eines Steuerungsinstruments für digitale Fragen	Claude Béglé	18.03.2016	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163260
Fr	16.5056	Autofahren ohne Fahrerin oder Fahrer	Susanne Leutenegger Oberholzer	02.03.2016	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20165056
Mo	16.3228	Der Bund soll nicht mehr Mehrheitseigner der Swisscom sein müssen	Ruedi Noser	18.03.2016	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163228
Mo	16.3484	Die dominante Stellung der Schweiz in der Blockchain-Technologie festigen	Claude Béglé	16.06.2016	NR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163484
	16.044	Werterhalt von Polycom. Gesamtkredit	Geschäft des Bundesrates	25.05.2016	BR		https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20160044
Po	16.3256	Förderung der Digitalisierung in der Regulierung (Regtech)	Martin Landolt	18.03.2016	NR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163256

7.2 EU: Richtlinie zur Netz-und Informationssicherheit (NIS-Richtlinie)

Das EU-Parlament hat sich Anfang Juli 2016 auf das erste europäische Gesetz zur Cybersicherheit geeinigt. Mit der sogenannten Richtlinie zur Netz- und Informationssicherheit (NIS) will die EU die europäische Widerstandsfähigkeit gegen Cyberangriffe stärken. Firmen, die wesentliche Dienste wie zum Beispiel im Energie-, Verkehrs-, Banken- und Gesundheitsbereich betreiben, oder Anbieter digitaler Dienste wie Suchmaschinen, Online-Marktplätze oder *Cloud-Dienste* müssen angemessene Sicherheitsmassnahmen zur Verbesserung der Widerstandsfähigkeit gegen Cyberangriffe ergreifen. Schwere Hackerangriffe auf Firmen-Systeme müssen gemeldet werden. Bei Missachtung dieser Meldepflicht drohen Strafen. Das EU-Parlament ist überzeugt, dass die Festlegung gemeinsamer Cyber-Sicherheitsstandards und die Verstärkung der Zusammenarbeit die Unternehmen unterstützen wird, sich gegen die steigende Zahl von Cyberangriffen zu schützen.

Die NIS-Richtlinie ist seit August 2016 rechtskräftig und muss nun von den Mitgliedstaaten binnen 21 Monaten in nationales Recht umgesetzt werden. Sie haben zusätzlich sechs Monate, um die «Betreiber wesentlicher Dienste» festzulegen.

Für die Schweiz hat die Verabschiedung der NIS-Richtlinie vorerst keine Auswirkungen. Inwiefern die Bestimmungen der NIS und die Anforderungen zur Teilnahme am Digital Single Market allerdings im Rahmen des autonomen Nachvollzugs durch die Schweiz auch zu einer hiesigen Übernahme von Vorschlägen wie gemeinsame Cyber-Sicherheitsstandards und Meldepflicht führen wird, bleibt abzuwarten. Die Schweiz setzt bislang im Bereich der Informationssicherung erfolgreich auf die freiwillige Zusammenarbeit von Staat und Wirtschaft. Fest steht, dass die Statuierung von nebenstrafrechtlichen Erlassen mit Meldepflichten von Cyber-Vorfällen einen Auf- und Ausbau der bestehenden Kapazitäten sowie die Schaffung von entsprechenden Kontrollorganen erfordert.

7.3 Frankreich: neue Vorschriften für kritische Infrastrukturen

In Frankreich wurden von der ANSSI (Agence nationale de sécurité des systèmes d'information) erste Vorschriften publiziert, welche die Betreiber kritischer Infrastrukturen («Opérateurs d'importance vitale») gesetzlich zu Schutzmassnahmen vor Cyberangriffen verpflichten. Sie

sind seit 1. Juli 2016 in Kraft und betreffen vorerst Unternehmen in den Sektoren Gesundheit, Lebensmittel und Wasserwirtschaft. Weitere Sektoren sollen folgen. Diese Gesetzesgrundlage wurde im Zuge des französischen Militärplanungsgesetzes vom Dezember 2013 geschaffen. Für kritische Infrastrukturen sind das Ergreifen von Schutzmassnahmen und die Meldung von Sicherheitsvorfällen Pflicht. Für den Fall, dass diese Vorschriften nicht eingehalten werden sind Sanktionen vorgesehen.

Frankreich hat damit europaweit die ersten Vorschriften dieser Art eingeführt – noch vor den Massnahmen, die sich aus der Richtlinie für Netzwerk- und Informationssicherheit (NIS) für alle EU-Mitgliedstaaten ergeben werden. Die NIS-Richtlinie wird aber breiter angelegt sein und auch die den französischen Vorschriften nicht unterstellte Unternehmen erfassen.

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 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, we have 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 institutions 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

8.1.3 Technical Report about the RUAG espionage case

23.05.2016 - After several months of Incident Response and Analysis in the RUAG cyber espionage case, we got the assignment from the Federal Council to write and publish a report about the findings. The following is a purely technical report, intending to inform the public about Indicators of Compromise (IOCs) and the Modus Operandi of the attacker group behind this case. We strongly believe in sharing information as one of the most powerful countermeasures against such threats; this is the main reason we publish this report not only within our constituency, but to the public as well.

➔ https://www.govcert.admin.ch/blog/22/technical-report-about-the-ruag-espionage-case

8.1.4 20min.ch Malvertising Incident

08.04.2016 - With this blog post we would like to share Indicators Of Compromise (IOCs) related to the attacks against 20min.ch, a popular newspaper website in Switzerland which got compromised and abused by hackers to infect visitors with an ebanking Trojan called Gozi ISFB. The IOCs shared in this blogpost may be used to spot infections within corporate networks.

➔ https://www.govcert.admin.ch/blog/21/20min.ch-malvertising-incident

8.1.5 Leaked Mail Accounts

18.03.2016 - MELANI/GovCERT has been informed about potentially leaked eMail Accounts that are in danger of being abused. MELANI/GovCERT provides a tool for checking whether your account might be affected: https://checktool.ch.

➔ https://www.govcert.admin.ch/blog/20/leaked-mail-accounts

8.1.6 Armada Collective is back, extorting Financial Institutions in Switzerland

11.03.2016 - A new wave of extortion emails has arrived in different Swiss Onlineshops. We have strong indications, that those extortioner are a copycat of Armada Collective.

➔ https://www.govcert.admin.ch/blog/19/armada-collective-is-back-extorting-financial-institutions-in-switzerland

8.1.7 Gozi ISFB - When A Bug Really Is A Feature

05.02.2016 - Gozi ISFB is an eBanking Trojan we already know for quite some time. Just recently, a new wave was launched against financial institutions in Switzerland. Similar to the attack we had already reported in September 2015, Cybercriminals once again compromised a major advertising network in Switzerland daily visited by a large number of Swiss internet users; they all become potential victims of the Gozi eBanking Trojan.

➔ https://www.govcert.admin.ch/blog/18/gozi-isfb-when-a-bug-really-is-a-feature

8.1.8 TorrentLocker Ransomware targeting Swiss Internet Users

21.01.2016 - On Wednesday, Jan 20 2016, we have noticed a major spam campaign hitting the Swiss cyberspace, distributing a ransomware called TorrentLocker. We have already warned about similar TorrentLocker attacks against Swiss internet users last year via Twitter. TorrentLocker is one of many ransomware families that encrypts any local file on a victim's computer and demands that the victim pays a ransom to have his files decrypted again. Since some ransomware families do not only encrypt files stored locally on the infected machine but also on any mapped network share, ransomware also represent a serious threat to corporate networks. To make sure that the malicious email goes through spam filters and gets opened by the recipient swiftly, the TorrentLocker gang is using a handful of tricks.

➔ https://www.govcert.admin.ch/blog/17/torrentlocker-ransomware-targeting-swiss-internet-users

8.2 MELANI Newsletter

Im ersten Halbjahr 2016 hat MELANI folgende Newsletter publiziert:

8.2.1 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

8.2.2 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

8.2.3 Technischer Bericht zur eingesetzten Schadsoftware beim Cyberangriff auf die RUAG

23.05.16 - Die Melde- und Analysestelle Informationssicherung MELANI hat im Auftrag des Bundesrates einen Bericht mit den technischen Erkenntnissen zum Fall RUAG publiziert. Er richtet sich an Sicherheitsverantwortliche und Fachpersonen im Bereich Netzwerksicherheit, um diese bei der Erkennung von Risiken im eigenen Netz und bei der Implementierung von möglichen Sicherheitsmassnahmen zu unterstützen.

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

8.2.4 Schweizweiter Ransomware Awareness Tag

19.05.16 - Zusammen mit Partnern veranstaltet die Melde- und Analysestelle Informationssicherung MELANI am heutigen Donnerstag einen Awareness Tag zu «Ransomware». Unter den Teilnehmenden sind Organisationen aus verschiedenen Sektoren, Softwarehersteller, Bundesämter sowie diverse Schweizer Vereine und Konsumentenschutz Organisationen.

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

8.2.5 Der Umgang mit Sicherheitslücken, verwundbare Infrastrukturen und verschiedene DDoS-Angriffe - 22. MELANI-Halbjahresbericht

28.04.2016 - Im zweiten Halbjahr 2015 kam es weltweit wiederum zu einigen teilweise spektakulären Cyber-Vorfällen. Im Fokus standen unter Anderem verschiedene DDoS-Attacken, Angriffe mittels Phishing sowie Angriffe auf industrielle Kontrollsysteme. Das Schwerpunktthema des 22. MELANI-Halbjahresberichts, der heute veröffentlicht wurde, bildet der Umgang mit Sicherheitslücken.

➔https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/halbjahresbericht-2-2015.html

8.2.6 Passwörter von 6‘000 E-Mail-Konten im Umlauf

18.03.2016 - Die Melde- und Analysestelle Informationssicherung hat 6‘000 Adressen zu E-Mail Konten erhalten, die offenbar gehackt wurden und nun möglicherweise für illegale Zwecke missbraucht werden.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/passwoerter-von-6000-e-mail-konten-im-umlauf.html

8.2.7 Betrügerische Telefonanrufe gegen KMUs im Zusammenhang mit dem E-Banking Trojaner «Retefe»

16.02.2016 - Seit Anfang Februar 2016 erreichen die Melde- und Analysestelle Informationssicherung MELANI sowie die Koordinationsstelle zur Bekämpfung der Internetkriminalität KOBIK vermehrt Meldungen aus der Bevölkerung betreffend betrügerischen Telefonanrufen, welche das Ziel haben, E-Banking Betrug zu ermöglichen.

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

8.3 Checklisten und Anleitungen

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

9 Glossar

Begriff	Beschreibung
.ini-Datei	Eine Initialisierungsdatei (kurz INI-Datei) ist eine Textdatei, die Wertepaare enthält. Initialisierungsdateien werden häufig von Microsoft-Windows-Anwendungen als Konfigurationsdatei genutzt.
Active Directory	Active Directory (AD) heisst der Verzeichnisdienst von Microsoft Windows Server, wobei ab der Version Windows Server 2008 der Dienst in fünf Rollen untergliedert und deren Kernkomponente als Active Directory Domain Services (ADDS) bezeichnet wird.
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.
Air-Gap	Als Air Gap wird in der Informatik ein Prozess bezeichnet, der zwei IT-Systeme voneinander physikalisch und

	logisch trennt, aber dennoch die Übertragung von Nutzdaten zulässt.
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.
Autonomes System (AS)	Ein autonomes System (AS) ist eine Ansammlung von IP-Netzen, welche als Einheit verwaltet werden und über ein gemeinsames internes Routing-Protokoll (IGP) (oder auch mehrere) verbunden sind.
Batchjob	Stapelverarbeitung, auch Batchverarbeitung genannt, ist ein Begriff aus der Datenverarbeitung und bezeichnet die Arbeitsweise von Computerprogrammen, bei der die Menge an Aufgaben oder Daten vollständig, automatisch und meist sequenziell verarbeitet wird.
Binärdatei	Eine Binärdatei ist eine Datei, die im Unterschied zu einer reinen Textdatei auch nicht-alphabetische Zeichen enthält. Es kann somit jeder beliebige Bytewert vorkommen. Dateien im Binärformat werden eher zur Speicherung von Daten verwendet.
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»).
Border Gateway Protocol (BGP)	Das Border Gateway Protocol ist das im Internet eingesetzte Routingprotokoll und verbindet autonome Systeme miteinander.
Botnetz	Eine Ansammlung von Computern, die mit Schadsoftware infiziert sind. Diese lassen sich durch einen Angreifer (den Botnetzbesitzer) komplett fernsteuern. Je nach Grösse kann ein Botnetz aus einigen Hundert bis Millionen kompromittierter Rechnern bestehen.
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.
Cloud-Dienst	Cloud Computing (Synonym: Cloud IT, deutsch etwa Rechnen in der Wolke) ist ein Begriff aus der Informati-

	onstechnik (IT). Die IT-Landschaft wird durch den Anwender nicht mehr selbst betrieben/bereitgestellt, sondern über einen oder mehrere Anbieter bezogen. Die Anwendungen und Daten befinden sich nicht mehr auf dem lokalen Rechner oder im Firmenrechenzentrum, sondern in der Wolke (Cloud). Der Zugriff auf diese entfernten Systeme erfolgt über ein Netzwerk.
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.
DDoS	Distributed-Denial-of-Service Attacke Eine DoS-Attacke, bei der das Opfer von vielen verscheiden Systemen aus gleichzeitig angegriffen wird.
Digitales Zertifikat	Beglaubigt die Zugehörigkeit eines öffentlichen Schlüssels (PKI) zu einem Subjekt.
Drive-by Download	Infektion eines Computers mit Malware allein durch Besuch einer Webseite. Vielfach beinhalten die betroffenen Webseiten seriöse Angebote und sind zwecks Verteilung der Malware zuvor kompromittiert worden. Die Infektion erfolgt meistens durch das Ausprobieren von Exploits für vom Besucher noch nicht geschlossene Sicherheitslücken.
Dropper	Ein Dropper ist eine eigenständig ausführbare Programm-Datei, die der meist erstmaligen Freisetzung eines Computervirus dient.
Dynamic Link Library	Dynamic Link Library (DLL) bezeichnet allgemein eine dynamische Programmbibliothek.
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
Exploit-Kit	Baukasten, mit denen Kriminelle Programme, Scripts oder Codezeilen generieren können, mit denen sich Schwachstellen in Computersystemen ausnutzen lassen.
Grey-Hat	Grey-Hats verstossen möglicherweise gegen Gesetze oder restriktive Auslegungen der Hackerethik, allerdings zum Erreichen eines ethischen Ziels.
Javascript	Eine objektbasierte Scriptingsprache 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.
Keylogger	Geräte oder Programme, die zwischen den Rechner und die Tastatur geschaltet werden, um Tastatureingaben aufzuzeichnen.
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.
MAC-Adresse	Media Access Control Hardware-Adresse eines Netzwerkadapters zu dessen weltweiten und eindeutigen Identifizierung. Die MAC-Adresse wird vom jeweiligen Hersteller in das ROM des Adapters geschrieben (Beispiel: 00:0d:93:ff:fe:a1:96:72).
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).
Man-In-The-Middle	Ein Man-in-the-Middle-Angriff (MITM-Angriff), auch Mittelsmannangriff genannt, ist eine Angriffsform, die in Rechnernetzen ihre Anwendung findet. Der Angreifer steht dabei entweder physisch oder – heute meist – logisch zwischen den beiden Kommunikationspartnern, hat dabei mit seinem System vollständige Kontrolle über den Datenverkehr zwischen zwei oder mehreren Netzwerkteilnehmern.
Phishing	Mittels Phishing versuchen Betrüger, an vertrauliche Daten von ahnungslosen Internet-Benutzern zu gelangen. Dabei kann es sich beispielsweise um Kontoinformationen von Online-Auktionsanbietern (z.B. eBay) oder Zugangsdaten für das Internet-Banking handeln. Die Betrüger nutzen die Gutgläubigkeit und Hilfsbereitschaft ihrer Opfer aus, indem sie ihnen beispielsweise E-Mails mit gefälschten Absenderadressen zustellen.

Pipe	Eine Pipe oder Pipeline ist ein Datenstrom zwischen zwei Prozessen. Dabei gilt, dass diejenigen Daten die zuerst eingelesen werden, auch diejenigen sind, die zuerst wieder ausgegeben werden (First In, First Out).
Point of Sales / Bezahlterminal	Terminals in Geschäften, an denen bargeldloses Zahlen mit Debit- und Kreditkarten möglich ist.
Programmable Logic Controller (PLC)	Englisch für Speicherprogrammierbaren Steuerungen (SPS).
Remote Desktop Protocol	Das Remote Desktop Protocol (RDP) ist ein proprietäres Netzwerkprotokoll von Microsoft zum Darstellen und Steuern des Bildschirminhalts (Desktop) entfernter Computer.
Rootkit	Auswahl an Programmen und Technologien, welche den unbemerkten Zugang und die unbemerkte Kontrolle eines Computers ermöglichen.
Router	Geräte aus dem Bereich Computernetzwerke, Telekommunikation oder auch Internet, die mehrere Rechnernetze koppeln oder trennen. Router werden beispielsweise in Heimnetzwerken eingesetzt und machen die Verbindung zwischen internem Netz und dem Intranet.
SCADA System	Supervisory Control And Data Acquisition Systeme. Werden zur Überwachung und Steuerung von technischen Prozessen eingesetzt (z. B. Energie- und Wasserversorgung).
Schwachstelle / Lücke	Schwachstelle in Hard- oder Software, über die Angreifer Zugriff auf ein System erlangen können.
Sourcecode	Englisch für Quelltext. Für den Menschen lesbare Form eines Computerprogrammes.
Spam	Unaufgefordert und automatisiert zugesandte Massenwerbung, worunter auch Spam-E-Mails fallen. Als Spammer bezeichnet man den Absender dieser Mitteilungen, während das Versenden selbst als Spamming bezeichnet wird.
Speicher Programmierte Steuerung	Eine Speicherprogrammierbare Steuerung (SPS), englisch Programmable Logic Controller (PLC), ist ein Gerät, das zur Steuerung oder Regelung einer Maschine oder Anlage eingesetzt wird und auf digitaler Basis programmiert wird. Seit einigen Jahren löst sie die «festverdrahtete» verbindungsprogrammierte Steuerung in den meisten Bereichen ab.
SSID	Service Set Identifier. Identifiziert den Netzwerknamen des WLAN. Sämtliche Access Points und Endgeräte des

	WLAN müssen den selben SSID verwenden, um miteinander kommunizieren zu können.
SWF-Animationsdatei	Das Kürzel SWF steht für Shockwave Flash. Unter dem Namen Shockwave vermarktete der damalige Hersteller Macromedia Flash. Flash ist der Name einer Plattform zur Programmierung und Darstellung multimedialer und interaktiver Inhalte.
TOR-Netzwerk	Tor ist ein Netzwerk zur Anonymisierung von Verbindungsdaten.
Trojaner	Trojanische Pferde (häufig als Trojaner bezeichnet) sind Programme, die im Verborgenen schädliche Aktionen ausführen und sich dabei für den Benutzer als nützliche Anwendung oder Datei tarnen.
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.
User-Interface	Das User-Interface (oder zu deutsch: Benutzerschnittstelle) ist die Stelle oder Handlung, mit der ein Mensch mit einer Maschine in Kontakt tritt.
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.
Virus	Ein selbstreplizierbares, mit schädlichen Funktionen versehenes Computerprogramm, welches sich zur Verbreitung an ein Wirteprogramm oder eine Wirtedatei hängt.
Wipe	Wipe (vom englischen für «wischen» oder «putzen») ist eine Eraser-Software, die zum sicheren Löschen von Dateien dient. Wird eine Datei mit Wipe gelöscht, so überschreibt es diese mehrmals mit Nullen, speziellen Bit-Mustern und/oder Zufallsdaten.
WLAN	WLAN (oder Wireless Local Area Network) steht für drahtloses lokales Netzwerk.
WPA2 Schlüssel	Wi-Fi Protected Access 2 Neuer Sicherheitsstandard für Funknetzwerke für Funknetzwerke nach der Spezifikation IEEE 802.11i. Nachfolgeversion der Verschlüsselungsmethode WPA und des als unsicher geltenden WEP.