Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Informatiksteuerungsorgan des Bundes ISB
Nachrichtendienst des Bundes NDB

**Melde- und Analysestelle Informationssicherung MELANI**

# INFORMATIONSSICHERUNG

## LAGE IN DER SCHWEIZ UND INTERNATIONAL

Halbjahresbericht 2018/II (Juli – Dezember)


30. APRIL 2019

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

# 1 Übersicht / Inhalt

# 2 Editorial

**Die aktuelle und zukünftige Rolle des Staates im Cyber-Bereich**

*Dr. Myriam Dunn Cavelty ist stellvertretende Leiterin am Center for Security Studies der ETHZürich, wo sie zu Cyber-Sicherheitspolitik forscht und lehrt.*

Noch vor zehn Jahren war die Cyber-Sicherheit ein Nischenthema, welches vor allem in technischen Expertenkreisen diskutiert wurde – in der Zwischenzeit ist sie aufgrund einer sich zuspitzenden Bedrohungslage zu einem sicherheitspolitischen Dauerthema geworden, das in den höchsten Regierungskreisen behandelt wird.

Dabei ist die Rolle des Staats und seiner Bürokratie einem politischen Aushandlungsprozess unterworfen, der in vielen Ländern der Welt noch nicht abgeschlossen ist. Cyber-Sicherheit ist ein Querschnittsthema, das sich mit vielen anderen Politikbereichen überschneidet. Eine der Hauptherausforderungen in Zeiten von knappen Ressourcen ist es, die richtige Mischung zwischen neuen Strukturen und effizienter Nutzung bestehender Kompetenzen zu finden sowie relevante Akteure aus Wirtschaft und Gesellschaft sinnvoll einzubinden. Besonders schwierig erweisen sich im Vergleich die (vertikale) Integration nationaler Cyber-Sicherheitsstrategien in den Rahmen der nationalen Sicherheit und in eine umfassende Gesamtstrategie über alle Politikbereiche hinweg sowie die (horizontale) Koordination und Kontrolle der verschiedenen Stellen im Umfeld der Cyber-Sicherheit.

Man ist sich einig: Ein zufriedenstellendes Niveau an Cyber-Sicherheit kann nur im Verbund zwischen Staat, Wirtschaft und Gesellschaft erreicht werden. Doch verfolgen die einzelnen Sektoren häufig unterschiedliche Ziele und Interessen. Daraus entstehen mindestens drei Spannungsfelder, in denen jede Cyber-Sicherheitspolitik positioniert werden muss.

Im ersten Spannungsfeld zwischen Staat und Wirtschaft muss eine Politik zur Sicherung der kritischen Infrastrukturen formuliert werden, welche die negativen Konsequenzen der Liberalisierung, Privatisierung und Globalisierung aus Sicht der Sicherheitspolitik auffängt, ohne die positiven Effekte zu behindern. Im zweiten Spannungsfeld zwischen Staat und Bürger gilt es, die politisch gewünschte Balance zwischen mehr Sicherheit und Wahrung der Bürgerrechte im digitalen Raum zu finden. Im dritten Spannungsfeld zwischen Bürger und Wirtschaft gilt es, die Rahmenbedingungen für die Entwicklung eines erfolgreichen Sicherheitsökosystems zu setzen, in dem eine optimale Balance zwischen Sicherheit und Funktionalität entsteht sowie Anreize zu mehr Sicherheitsverpflichtung für Anbieter von Dienstleistungen geschaffen werden.

Was für die wirtschaftlichen und zivilgesellschaftlichen Akteure selbstverständlich ist, gilt auch für den Staat: Er nimmt eine Vielzahl von Rollen gleichzeitig ein. Die Erkenntnis der Diversität staatlichen Handelns ist ein guter Ausgangspunkt, um Rollenkonflikte auf politischer Stufe auszutragen und systematisch anzugehen und somit eine proaktive Politik für die Zukunft zu gestalten.

Myriam Dunn Cavelty

# 3 Schwerpunktthema: Umgang mit Herstellern kritischer Hard- und Softwarelösungen

Nicht erst seit den Snowden-Dokumenten stehen Hersteller von Hard- und Software bestimmter Staaten im Rampenlicht. Schon kurz nach dem globalen Markteintritt des chinesischen Herstellers Huawei wurden Zweifel an der Integrität dessen Produkte und Unabhängigkeit von Behörden laut. Mit den Snowden-Leaks 2013 bestätigte sich zumindest in Teilen der Verdacht, dass auch US-Hersteller wie Cisco, Microsoft, Google und andere den Behörden Zugang zu ihren Produkten zwecks Überwachung der Nutzerinnen und Nutzer gewähren. Auf Grund von Vorwürfen russischer Spionage in den USA verhängten die amerikanischen Behörden 2017 ein Verbot für den Einsatz von Kaspersky-Produkten in US-Bundesbehörden. Auch in der Schweiz wird dieses Thema in der Wirtschaft und auf Verwaltungsebene diskutiert.

Einerseits gibt es mit Blick auf vorkehrende Sicherheitsmassnahmen gute Gründe, beim Einsatz von Produkten gewisser Hersteller genauer hinzusehen. Andererseits ist ein nicht unbedeutender Teil dieser Diskussion allerdings auch rein wirtschaftspolitischen Interessen geschuldet. Eine differenzierte, herstellerunabhängige Diskussion drängt sich entsprechend auf.

## 3.1.1 Hard- und Software als Mittel zum Zweck staatlicher Interessen

Mit der zunehmenden Digitalisierung von Geschäftsprozessen bilden die dazu benötigten Hard- und Software-Lösungen eine zentrale und kritische Komponente. Auf den ersten Blick erscheint dabei der Anbietermarkt als äusserst vielfältig und mit Blick auf die unterschiedlichsten Lösungsansätze breit aufgestellt. Betrachtet man die Herkunftsländer der Anbieter, ist es mit dieser scheinbaren Diversität aber nicht mehr weit her. Der Markt wird klar von US-Unternehmen dominiert, dicht gefolgt von China und vereinzelten, globalen Mitspielern wie beispielsweise Korea (Samsung), Russland (Kaspersky) und Deutschland (SAP).

Analysiert man die in den Herkunftsländern geltenden Rechtsgrundlagen mit Bezug auf die ansässige Industrie der Informations- und Kommunikationstechnik (IKT) wird deutlich, dass diese nicht nur einen willkommenen Wirtschaftsmotor darstellt. Deren zentrale Stellung bei der Bearbeitung, Zustellung und Speicherung von Informationen ist sehr wohl erkannt und entsprechende Begehrlichkeiten staatlicher Stellen sind rechtlich verankert.

Fakt ist: Ohne Hard- und Software Lösungen von US-amerikanischen, chinesischen und anderen Unternehmen, findet die dichte Digitalisierung von Prozessen, wie wir sie heute kennen, nicht statt. Und mit dieser Digitalisierung einher geht die theoretische Vereinfachung des Zugriffes auf IKT-Systeme der heimischen Hersteller und damit auf die gespeicherten, bearbeiteten oder zugestellten Informationen.

## 3.1.2 Herstellerausschluss, Cyber-Souveränität und internationale Normen

Der potenzielle Zugriff auf IKT-Hersteller durch die jeweiligen Sitzstaaten und die damit verbunden Möglichkeit, globale Kontrolle über Hard- und Software zu erlangen, führen zu Diskussionen über den richtigen Umgang mit diesen Risiken.

Grundsätzlich zielen dabei einige der praktizierten Ansätze im weitesten Sinne auf die Hersteller und Anbieter von Hard- und Software-Lösungen.

Hersteller können generell aus dem Beschaffungsprozess ausgeschlossen werden, wenn sie im Verdacht stehen, Mittel zum Zweck eines Staates zu sein. Dies geschah beispielsweise in der US-Verwaltung, die im Dezember 2017 die Verwendung von Produkten der in Russland

domizilierten Kaspersky-Gruppe untersagte. Auch mit Blick auf die Beschaffung von Huawei-Produkten tauchten in den letzten Wochen und Monaten in verschiedensten Ländern Forderungen auf, diese Hersteller aus dem Beschaffungsprozess auszuschliessen.

Diese Ansätze können zwar kurz- bis mittelfristig scheinbare (Sicherheits-)Lösungen bieten, um einer möglichen, staatlichen Fremdkontrolle digitaler Prozesse zu entgehen. In mehreren Ländern, darunter auch in der Schweiz, wird eine generelle Diskussion geführt, wie man sich aus der Abhängigkeit von den zwei de facto Technologie-Giganten USA und China emanzipieren könnte.

Auch auf der Ebene der internationalen Sicherheitspolitik ist das Thema der staatlichen Zu- und Durchgriffe auf Hersteller von IKT-Lösungen seit geraumer Zeit ein Thema. Beispielsweise legte der Bericht 2015 der «UN Group of Governmental Experts» erste Normen fest, die Teilaspekte solches Handeln eindämmen sollen. Der Folgebericht 2017, der diese Normen hätte konkretisieren sollen, verfehlte aber den nötigen Konsens in einem unterdessen wesentlich raueren zwischenstaatlichen Klima.

### 3.1.3 Hard- und Software-Hersteller sind und bleiben Spielball staatlicher Interessen

In Orwells «Nineteen Eighty-Four», einer pessimistischen Allegorie zur Beschaffenheit absoluter Macht, fällt mehrmals das Credo, wer die Vergangenheit kontrolliere, kontrolliere die Zukunft, und wer die Gegenwart kontrolliere, kontrolliere die Vergangenheit. Im Zentrum dieser Aussage steht die Idee des absoluten, ungehinderten Zugriffs auf Informationen und Daten. Keinem der Ursprungsländer der führenden IKT-Hersteller sei hier die gleiche globaltotalitäre Absicht unterstellt. Die Tatsache, im Rahmen der existierenden rechtlichen Grundlagen punktuell über die heimischen Hard- und Software-Hersteller auf Informationen und Daten zuzugreifen, stellt allerdings einen schlagenden komparativen Vorteil dar, den keiner dieser Staaten freiwillig und selbstlimitierend aus der Hand geben wird.

Vor diesem Hintergrund sind denn auch die öffentlichen Aussagen der USA zu sehen, die nicht zulassen wollen, dass China die USA in Sachen Technologieführung ablöst. Entsprechend sind Sanktionen und Herstellerverbote durchaus als rein wirtschaftspolitische und sicherheitspolitische Entscheide zu verstehen, die nur bedingt auf differenzierten Sicherheitsbedenken im Sinne des Eigenschutzes basieren. Ein Rückgang der IKT-Komponenten, welche von US-amerikanischen Herstellern verkauft werden, geht einher mit einem Verlust der punktuell zielführenden Kontrolle über diese Hard- und Software-Lösungen im Betrieb beim Endkunden.

Hersteller von IKT-Lösungen werden Spielball der Interessen ihrer Herkunftsländer und werden auch künftig - entsprechend den geltenden rechtlichen Grundlagen - zu einer Zusammenarbeit mit den entsprechenden staatlichen Einheiten verpflichtet sein. Es ist nicht davon auszugehen, dass sich selbst im Extremfall irgendein privatwirtschaftliches Unternehmen gegen geltendes Recht in seinem Heimatstaat stellt. Und es ist weiter absehbar, dass sich China und die USA im Kampf um weltweite Anteile an IKT-Produkten weiterhin um die Vorherrschaft streiten werden.

### 3.1.4 Mangelnde Alternativen

Es ist mehr als fraglich, ob die Schweiz als Industriestandort in absehbarer Zeit überhaupt Alternativen zu den vorherrschenden Hard- und Software-Lösungen ausländischer Anbieter aufbauen könnte. Auch eine koordinierte - für die Schweiz untypische - Industriepolitik in diesem Bereich würde, wenn überhaupt, erst langfristig Wirkung zeigen. Die Digitalisierung von

Geschäftsprozessen, eHealth, der Aufbau von 5G und dergleichen findet aber bereits heute statt und die dafür benötigten IKT-Komponenten und Lösungen werden praktisch gar nicht, oder nur zu kleinen Teilen, mit hohem Aufwand in der Schweiz hergestellt.

Die Schweiz als kleine, offene Volkswirtschaft ist zum einen abhängig von ausländischen IKT-Herstellern. Gleichzeitig kann sie aber auch davon profitieren, dass sie die verschiedenen unterschiedlichen Interessen der Staaten mit entsprechenden führenden IKT-Industrien gegeneinander abwägen kann. Die Schweizer Wirtschaft wird bezüglich Digitalisierung auch weiterhin in Teilen von ausländischen IKT-Herstellern abhängig sein. Somit sollte ein konsequentes Risikomanagement aufgebaut werden, welches durchgehend den Umgang mit Herstellern, Lieferanten und Zulieferern von Hard- und Software-Lösungen adressiert, auch mit Blick auf die Möglichkeit staatlicher Zu- und Durchgriffe.

Beurteilung:

Die oben aufgeführten Feststellungen führen zu folgenden grundsätzlichen Einschätzungen betreffend Bedrohungslage im Bereich von IKT-Herstellern mit ausländischen Mutterkonzernen:

- Das rechtliche Instrumentarium jener Länder, in denen die global wichtigsten Akteure im Bereich Hard- und Software-Lösungen heimisch sind, legitimiert praktisch jegliche Informationsbeschaffung über ausländische Ziele, sofern dies im Interesse der jeweiligen Staaten liegt.
- Eine rein vertraglich festgehaltene Verpflichtung der IKT-Unternehmen, Schweizer Recht zu wahren, ist nicht als genügende Garantie zu werten. Diese müssten mit Auflagen verbunden und von periodischen Vor-Ort-Audits begleitet werden. Dies umfasst auch Einrichtungen im Ausland, sofern diese geeignet sind, auf das organisatorisch bzw. durch Besitzanteile verbundene Schweizer Unternehmen technisch oder organisatorisch Einfluss zu nehmen.
- Je nach Hard- und Software sowie Auswahl von Dienstleistern sollten angemessene Massnahmen ergriffen werden, mit denen unberechtigte Zugriffe auf Systeme und Daten möglichst verhindert, jedoch zumindest erkannt und gestoppt werden können.
- Risikoadäquate Massnahmen sind bei jedem Beschaffungsprojekt einzuplanen und in den Kosten auszuweisen. So kann es vorkommen, dass die scheinbar kostengünstigste Offerte eines Anbieters infolge angezeigter flankierender Massnahmen zu internen Mehrkosten führt bzw. eine weitere Dienstleistung zur Kontrolle und Absicherung eingekauft werden müsste.

# 4 Lage national

## 4.1 Spionage

### 4.1.1 Cyber-Angriff auf OPCW – Labor Spiez auch im Visier

Im letzten Halbjahresbericht hat MELANI an dieser Stelle über die missbräuchliche Verwendung einer öffentlich verfügbaren Einladung für eine internationale Konferenz des Labors Spiez berichtet. Um einen gezielten Angriff durchzuführen und die Empfänger zum Öffnen eines Anhangs zu verleiten, nahmen die Angreifer diese Einladung als Vorlage und versendeten sie anschliessend mit gefälschtem Absender im Namen des Bundesamtes für Bevölkerungsschutz (BABS) und des Labors Spiez an diverse Empfänger.

Dass das Labor Spiez auch direkt im Visier von Angreifern ist, zeigt die im September 2018 öffentlich bekannt gewordene Nachricht über die Verhaftung von vier Personen, die am 13. April 2018 in den Niederlanden[1] stattgefunden hat. Den Verhafteten wird versuchtes Eindringen in das Wireless-Netzwerk der internationalen «Organisation für das Verbot chemischer Waffen (OPWC)» vorgeworfen. Die vier mutmasslich russischen Mitarbeiter des militärischen Nachrichtendienstes «GRU» sollen via Flughafen Schiphol mit Diplomatenpässen in die Niederlande eingereist sein und sich anschliessend ein Auto gemietet haben, das sie auf dem Parkplatz des Marriot Hotels in Den Haag positionierten. Dieses befindet sich direkt bei den Büros der OPCW. Im Kofferraum des Autos wurde eine Ausrüstung sichergestellt, die zum Eindringen in Funknetzwerke verwendet wird und für Cyber-Angriffe eingesetzt werden kann. Die Antenne für das betriebsbereite Gerät lag versteckt unter einem Mantel auf der hinteren Ablage des Autos. Die vier Verhafteten wurden noch am selben Tag aus den Niederlanden ausgeschafft und mussten ihre Ausrüstung zurücklassen.

Wie sich herausstellte, war auch das Labor Spiez im Interesse dieser Gruppe. Im Gepäck der Verhafteten fand man unter anderem ein Zugticket für die Reise von Utrecht nach Basel. Auf einem Notebook entdeckten die Ermittler Suchanfragen zur Konsularabteilung der russischen Botschaft in Bern sowie über des Labor Spiez.[2] Sowohl die OPCW als auch das Labor Spiez waren in die Untersuchungen über den Giftanschlag auf den ehemaligen russischen Doppelagenten Sergei Skripal und seine Tochter vom März 2018 im englischen Salisbury involviert. Wie der Nachrichtendienst des Bundes (NDB) bestätigte, war er zusammen mit seinen holländischen und britischen Partnern aktiv an dieser Operation beteiligt und hat damit zur Verhinderung illegaler Aktionen gegen eine kritische Schweizer Infrastruktur beigetragen.

Das Labor Spiez hatte schon im Vorfeld die Vorschriften für besonders gefährdete Objekte erfüllt. Trotzdem wurde der Schutz weiter hochgefahren und noch zusätzliche Massnahmen getroffen, um den Sicherheitsstandard nochmals auszubauen.

---

1 https://www.government.nl/government/members-of-cabinet/ank-bijleveld/news/2018/10/04/netherlands-defence-intelligence-and-security-service-disrupts-russian-cyber-operation-targeting-opcw (Stand: 31. Januar 2019)

2 https://www.justice.gov/opa/page/file/1098571/download (Stand: 31. Januar 2019)

### 4.1.2 Operation «Sharpshooter» zielt auf kritische Infrastrukturen

Das Sicherheitsunternehmen «McAfee» publizierte im Dezember 2018 einen Bericht zu einer neu entdeckten APT-Kampagne gegen Unternehmen im Bereich Verteidigung, Energie-, Atom- und Finanzunternehmen.[3] Die Kampagne mit dem Namen «Sharpshooter» begann am 25. Oktober 2018 mit dem Versand verseuchter Dokumente an Personen von 87 Organisationen auf der ganzen Welt, hauptsächlich aber in den USA. Gemäss Bericht sollen auch Schweizer Unternehmen im Finanzsektor von der Kampagne betroffen gewesen sein. Der Nachrichtendienst des Bundes NDB hat bislang keine Spuren von Infektionen bei potentiell betroffenen Firmen in der Schweiz gefunden.

Mittels Social Engineering sollten die Empfänger zum Öffnen der infizierten Dokumente gebracht werden. Das Schreiben war als Bewerbungsschreiben getarnt und enthielt einen Link zu einem Dokument auf «Dropbox», in dem sich angeblich das Bewerbungsdossier befand. Diese Methode ist deswegen besonders heimtückisch, weil Personalabteilungen häufig Spontanbewerbungen erhalten und daher üblicherweise solche Dokumente öffnen. Unternehmen mit korrekt implementieren Sicherheitsvorkehrungen liefen indes keine grosse Gefahr, Opfer dieses Angriffs zu werden. Die Infektion erfolgte über ein im Word-Dokument enthaltenes Makro. Solche Makros sind mittlerweile bei vielen Firmen gesperrt, respektive werden erst nach einer Bestätigung einer entsprechenden Warnmeldung aktiviert. Wird das Makro trotz allen Warnungen ausgeführt, schleust die Malware Sharpshooter in den Arbeitsspeicher von Word ein. Anschliessend installiert die Malware eine modulare Hintertür mit dem Namen «Rising Sun». Die Funktionen dieser Komponente umfassen das Zusammentragen und Versenden von Informationen über Dokumente, Nutzernamen, Netzwerkkonfiguration und Systemeinstellungen. Die Malware kann zudem weitere Funktionen nachladen. Ebenfalls besitzt die Schadsoftware die Fähigkeit, Spuren zu verwischen, um nicht entdeckt zu werden. So kann sie den Speicher leeren beziehungsweise ihre Aktivitäten löschen. Die Schadsoftware kommuniziert dabei über einen von den Angreifern kontrollierten Command and Control Server.

Bei der Analyse der Kampagne hat McAfee Hinweise auf Verbindungen mit der «Lazarus»-Gruppe gefunden: «Rising Sun» enthält Code und Konfigurationsdaten, die von der Trojaner-Familie «Duuzer» stammen. Duuzer kam auch beim Hackerangriff auf «Sony» zum Einsatz, welcher mit der Lazarus-Gruppe in Verbindung gebracht wird. Verschiedene Cyber-Sicherheitsfirmen bringen diese Angriffe mit Nordkorea in Verbindung. Allerdings wird im aktuellen Fall eine andere Entschlüsselungsroutine verwendet. Dies wiederum lässt darauf schliessen, dass Rising Sun eine Weiterentwicklung von Duuzer sein könnte. Ob diese Kampagne tatsächlich der «Lazarus» Gruppe zuzuordnen ist, lässt sich somit nicht abschliessend klären. Methoden, Spuren und Malware sind mittlerweile weltweit bekannt, und wären auch für sogenannte «False-Flag»-Operationen geeignet. Dabei wird versucht, den Verdacht auf unbeteiligte Dritte zu lenken.

[3] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-sharpshooter.pdf (Stand: 31. Januar 2019)

## 4.2 Industrielle Kontrollsysteme

### 4.2.1 Industrielle Kontrollsysteme und IoT

Spektakuläre Sabotageangriffe blieben im zweiten Halbjahr 2018 glücklicherweise aus. Es wurden keine gezielten Angriffe gegen industrielle Kontrollsysteme publik, jedoch generierten Infektionen mit herkömmlicher Malware, wie Ransomware in Kontrollsystem-Netzwerken im Ausland einige Aufmerksamkeit[4] (siehe auch Kapitel 5.3.5). Moderne vernetzte Anlagen werden laufend in Betrieb genommen und auch ältere, früher isolierte Systeme werden ans Internet angebunden, um die Effizienz durch Integration in weitere Geschäftsabläufe zu steigern. Mit der Vernetzung und dem Einbinden verschiedenster Dinge ans Internet (Internet of things IoT) steigt aber auch das Risiko, von den vielschichtigen Gefahren des Internets betroffen zu werden, die sich möglicherweise gegen erreichbare verwundbare Systeme richten.

### 4.2.2 Kein Erfolg für Hacker in Ebikon - Gemeinde wehrt mutmassliche Angriffe auf Wasserversorgung ab

Die Schweiz ist für ihr qualitativ hochwertiges Trinkwasser bekannt. Um die Versorgung sicher zu stellen, betreiben die Gemeinden einen hohen Aufwand und erneuern ihre Anlagen in regelmässigen Abständen. Bei solchen Erneuerungen werden auch modernste Steuerungen eingebaut. Selbst Delegationen aus dem europäischen Ausland lassen sich in der Schweiz gerne über die betrieblichen Erfahrungen mit den neuen Systemen informieren[5].

Leider interessieren sich aber auch Angreifer aus aller Welt für solche Anlagen. So registrierte die Gemeinde Ebikon im vergangenen Herbst mehrere tausend Eindringungsversuche ins Netzwerk der autonomen Betriebssteuerung ihrer Wasserversorgung[6].

Angreifer verschiedenster Motivation sind laufend auf der Suche nach von aussen erreichbaren Diensten. Sie testen diese auf Schwachstellen und versuchen, sowohl mit bekannten Standard-Zugangsdaten, wie auch mit andernorts abgeflossenen Identitäten, in die gefundenen Systeme einzudringen. Im Falle von Ebikon blieben die Versuche glücklicherweise ohne Erfolg und als Nebeneffekt dienten die entdeckten Angriffsversuche dazu, eine Nachjustierung der Sicherheitsmassnahmen vorzunehmen. Auch bei einem erfolgreichen Angriff und beim Versagen der Prävention und Detektion, wäre die Gemeinde aber in der Lage gewesen, die automatisierten Systeme herunterzufahren und die Anlagen manuell weiter zu betreiben.

Der Fall Ebikon zeigt exemplarisch auf, wie Massnahmen in verschiedenen Phasen des Cyber Security-Frameworks[7] dazu beitragen, die realen Angriffsversuche auf eine lebensnotwendige Infrastruktur abzuwehren und wenn nötig darauf zu reagieren. Es lohnt sich nicht nur in den präventiven Schutz zu investieren, sondern für den Ereignisfall vorzusorgen. Einen Ansatz zur Umsetzung bietet dabei der IKT-Minimalstandard des Bundesamtes für wirtschaftliche Landesversorgung (BWL), welche auf dem Cyber-Security Framework aufbauen.

---

4 https://dragos.com/year-in-review/ (Stand: 31. Januar 2019)

5 https://www.ebikon.ch/verwaltung/aktuelles/news/daenemark-auf-besuch-in-ebikon (Stand: 31. Januar 2019)

6 https://www.inside-it.ch/articles/53204 (Stand: 31. Januar 2019)

7 https://www.nist.gov/cyberframework (Stand: 31. Januar 2019)

Empfehlung:

Im Rahmen der vom Bundesrat 2012 beschlossenen «Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)» führte das Bundesamt für wirtschaftliche Landesversorgung (BWL) Verwundbarkeitsanalysen zu Cyber-Risiken in verschiedenen lebenswichtigen Branchen durch. Untersucht wurden etwa die Stromversorgung, die Trinkwasser- und Lebensmittelversorgung und auch der Strassen- und Schienenverkehr. Auf Basis der Ergebnisse entwickelte das BWL den «Minimalstandard zur Stärkung der IKT-Resilienz». Der Standard richtet sich insbesondere an die Betreiber von kritischen Infrastrukturen in der Schweiz. Er kann jedoch von jedem Unternehmen in Teilen oder als Ganzes angewendet werden.

Der «Minimalstandard zur Stärkung der IKT-Resilienz» umfasst die Funktionen Identifizieren, Schützen, Detektieren, Reagieren» und Wiederherstellen. Zudem bietet er Anwendern 106 konkrete Handlungsanweisungen zur Verbesserung ihrer IKT-Resilienz gegenüber Cyber-Risiken:


Minimalstandard zur Stärkung der IKT-Resilienz

https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html

### 4.2.3 MadIoT – Das Gefahrenpotential eines Botnets aus Haushaltsgeräten

Der Stromausfall in Italien am 28. September 2003 dürfte vielen noch in Erinnerung sein. Eine Kettenreaktion führte zur Überlastung der Übertragungsnetze und liess den Strom im ganzen Land ausfallen[8]. Am Anfang dieses Blackouts stand ein elektrischer Überschlag auf einen Baum in der Schweiz. Mehrere unglückliche Umstände führten zu dieser Instabilität und Überlastung des Stromnetzes. Was wäre aber, wenn die Instabilität absichtlich durch Manipulation des Stromverbrauchs an einer Vielzahl von Haushaltsgeräten herbeigeführt würde?

Überlegungen dieser Art machten sich Forscher der «Princeton Universität» im Rahmen einer Studie[9], die sie an der «USENIX Security Konferenz» im August 2018 präsentierten. Der Studie liegt die Annahme zu Grunde, dass es einem böswilligen Akteur gelingt, ein Botnet aus Geräten des Internets der Dinge (Internet of things IoT) mit hoher Leistungsaufnahme wie Klimaanlagen, Heizungen und Waschmaschinen aufzubauen. Wird deren Leistungsaufnahme geografisch koordiniert und in grossem Ausmass unerwartet beeinflusst, konnten in den Szenarien der Forscher ähnliche Instabilitäten im Stromnetz herbeigeführt werden, wie diejenige, welche den anfangs erwähnten Blackout in Italien provoziert hatten[10].

8 http://www.rae.gr/old/cases/C13/italy/UCTE_rept.pdf (Stand: 31. Januar 2019)

9 https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-soltan.pdf (Stand: 31. Januar 2019)

10 https://securityintelligence.com/how-an-iot-botnet-could-breach-the-power-grid-and-cause-widespread-blackouts/ (Stand: 31. Januar 2019)

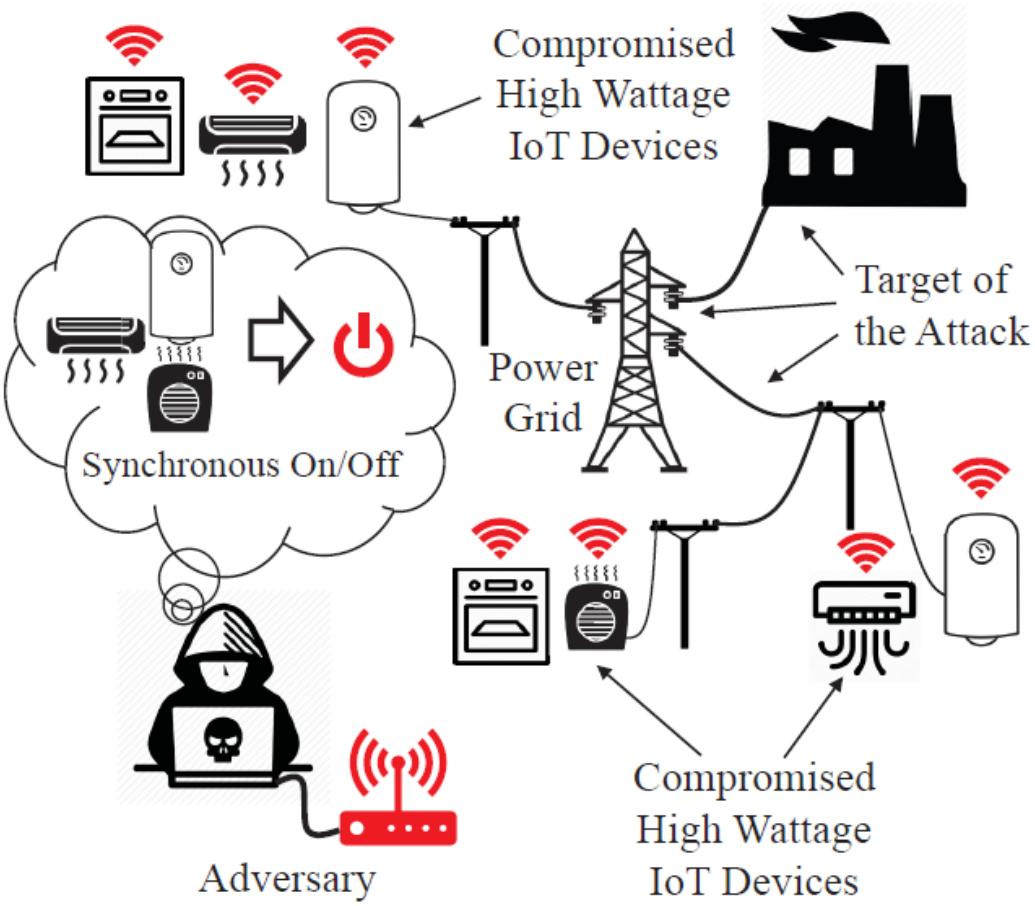



Abbildung 1: Angriffsschema «Manipulation of demand via IoT» (Quelle: usenix.org, https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-soltan.pdf )

Das Neuartige an den beschriebenen Angriffsszenarien ist, dass die Ausfälle nicht durch Beeinträchtigung der Energieproduktion oder Übertragung verursacht werden, sondern die Verbraucherseite ins Visier genommen wird. Die Endgeräte der Abnehmer sind vielfach nur marginal geschützt, speziell im Vergleich zu Kraftwerken oder Übertragungsnetzen, bei welchen seit Jahren viele Ressourcen in die Sicherheit investiert werden.

Die Stabilität des Stromnetzes baut auf der Verlässlichkeit von Verbrauchsprognosen auf, die sich hauptsächlich auf Erfahrungswerte der Vergangenheit stützen. Durch eine koordinierte Manipulation verwundbarer Geräte mit hohem Verbrauch, entgegen der Verbrauchsprognosen, liessen sich die üblichen Toleranzreserven überschreiten. Als Beispiel könnten im Hochsommer alle elektrischen Heizungen von einem Angreifer synchron auf Volllast geschaltet werden. Diese Vorgehensweise wird «Manipulation of demand via IoT (MadIoT)» genannt.

Die den Simulationen zu Grunde liegenden Annahmen mögen weit hergeholt erscheinen. Die Auswirkungen des «Mirai»-Botnets im Jahr 2016 zeigten jedoch eindrücklich das Schadenspotential eines IoT-Botnets. Bereits 2017 demonstrierte der britische Hersteller von Sicherheits-Software «Sophos» in einem Versuch, dass exponierte IoT-Geräte in Smart-Homes in

kurzer Zeit von vielen Seiten angegriffen werden können[11]. Dabei stellte der Sicherheitsdienstleister auch eine hohe Konzentration von solchen exponierten IoT-Geräten in der Schweiz fest.

Nicht nur Betreiber der Energieinfrastrukturen, auch Hersteller von IoT-Geräten müssen ihren Beitrag leisten, damit solche Angriffe nicht zur Realität werden. Es gibt viele Bestrebungen, minimale Best-Practices vorzugeben. Obligatorisch sind diese aber noch in den wenigsten Regionen und Bereichen. Eine Auslegeordnung[12] des britischen «Department for Digital, Culture, Media & Sport (DCMS)» bietet eine gute Übersicht und vergleicht existierende Vorgaben und Leitlinien.

Empfehlung:

Entdecken Sie offen erreichbare oder schlecht gesicherte Steuerungssysteme im Internet, melden Sie uns die entsprechenden Angaben, damit wir den Betreiber informieren können.


Meldeformular MELANI

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


Checkliste mit Massnahmen zum Schutz industrieller Kontrollsysteme

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

## 4.3 Angriffe (DDoS, Defacements, Drive-By)

Privatpersonen, Organisationen und Unternehmen in der Schweiz sind weiterhin Ziele verschiedener Angriffsarten.

### 4.3.1 Quickline-Modems für SNMP-Amplification Attacken missbraucht

Wie der Internetanbieter «Quickline» am 11. Oktober 2018 in einer Medienmitteilung publizierte, hatte der Provider während zweier Wochen mit unregelmässigen Störungen zu kämpfen. Beeinträchtig von der Störung waren sowohl die Dienste Fernsehen, Internet und Telefonie, wobei das Problem nicht bei allen Kunden gleich und auch nicht in gleichem Ausmass auftrat. Als Ursache konnte eine Schwachstelle bei einem Modem-Typ identifiziert werden. Analysen ergaben, dass die Kunden nicht direkt im Visier der Angreifer standen. Sie dienten nur als Mittel zum Zweck, um einen Angriff gegen Dritte durchzuführen. Es handelte sich um einen sogenannten «SNMP-Amplification» Angriff. Dabei wird das Simple Network Management der Geräte verwendet, um eine Anfrage zu verstärken und diese schlussendlich auf das Ziel zu lenken, um dieses zu überlasten. Die Modems werden zu diesem Zweck nicht infiziert,

[11] https://www.computerworld.ch/security/hacking/smart-home-in-minuten-hacker-da-1435426.html (Stand: 31. Januar 2019)

[12] https://iotsecuritymapping.uk/ (Stand: 31. Januar 2019)

sondern der Angreifer nutzt lediglich den Umstand, dass das SNMP System gegen aussen offen verfügbar ist. Die Störungen bei den Kunden sind aufgetreten, weil die Anfragen unabsichtlich auch die Modems überlastet und somit Instabilitäten hervorgerufen haben dürften. Da nicht alle Quickline-Kunden den gleichen Modem-Typen benutzen, waren nur 5% oder rund 9000 Kunden betroffen. Wie lange die Modems anfällig auf die SNMP-Amplification Angriffe waren, ist nicht bekannt. Um die Schwachstelle zu beheben, hat Quickline mehrere Massnahmen ergriffen. Dabei handelte es sich vor allem um Filter im Netz und ein zusätzliches Absichern der betroffenen Modems. Quickline hat rechtliche Schritte eingeleitet.

### 4.3.2 Steuerdaten im Netz - App mit falscher Einstellung

Die Steuererklärung auszufüllen, ist für viele Menschen nicht gerade eine Lieblingsbeschäftigung und oft mühsam. Deshalb entwickelte eine Zürcher Firma namens «Zurich Financial Solutions» (www.zufiso.ch) die Smartphone-App «Steuern59.ch», welche den ganzen Prozess erleichtern soll. «Steuern59.ch» kann im «PlayStore» oder im «AppleStore» gekauft und heruntergeladen werden. Die App verspricht, für nur 59.00 CHF das Ausfüllen der Steuererklärung zu übernehmen. Man muss dafür nur die notwendigen Dokumente mit dem Smartphone fotografieren und auf die App laden. Allerdings stellte sich heraus, dass alle diese sensiblen Dokumente auf einen ungesicherten Cloud-Server der «Amazon Web Services (AWS)» geladen wurden und so für alle AWS-Benutzer frei zugänglich waren. Die Daten sind in den Standardeinstellungen «privat» und somit nicht öffentlich einsehbar. Wenn man diese Einstellungen auf «öffentlich» ändert, wird eine entsprechende Warnung angezeigt[13]. Den angeblich indischen Programmieren, welche für die App-Entwicklung angeheuert worden waren, unterlief jedoch ein Fehler: Sie setzten diese Einstellung auf «öffentlich» und vergassen anscheinend, diese Einstellung wieder auf «privat» zurückzusetzen. Ein Sicherheitsforscher entdeckte diese Fehlkonfiguration und informierte die Betreiberfirma. Erst nachdem er sich an das deutsche Heise-Magazin gewendet hatte, wurde er von der Firma kontaktiert.[14] Dies wirft die Frage mit dem Umgang entdeckter Schwachstellen auf («Responsible Disclosure»): Wie sollen Sicherheitsforscher entdeckte Lücken melden und wie sollen diese Meldungen dann von den Firmen gehandhabt werden. Die Firma, welche «Steuern59.ch» betreut, gab an, die Produktion der App nach Indien ausgelagert zu haben. Man sei sich nicht bewusst gewesen, wie unsorgfältig die Entwickler arbeiteten. Betroffen waren 80 Kunden, welche die App benutzten. Diese wurden über den Vorfall informiert, nachdem die Sicherheitslücke in Zusammenarbeit mit dem Sicherheitsforscher geschlossen worden war. Ebenfalls werden die Daten jetzt auf einer Schweizer Cloud namens «n'cloud» gespeichert. [15]

---

13 https://docs.aws.amazon.com/AmazonS3/latest/dev/s3-access-control.html (Stand: 31. Januar 2019)

14 https://www.inside-it.ch/articles/52273 (Stand: 31. Januar 2019)

15 https://www.heise.de/newsticker/meldung/Steuern59-ch-Geschaeftsfuehrung-entschuldigt-sich-fuer-Daten-leck-4169772.html (Stand: 31. Januar 2019)

## 4.4 Social Engineering und Phishing

### 4.4.1 Wieder vermehrt betrügerische Anrufe bei Firmen

Anfang Juli 2018 wurden wiederum Anrufe registriert, bei welchen sich Angreifer als Bankmitarbeitende ausgegeben hatten. Dabei bitten die Anrufer jeweils um die Ausführung von Zahlungen oder geben vor, ein Update beim E-Banking durchführen zu müssen, das anschliessend getestet werden soll.

Die Angreifer versuchen typischerweise die Mitarbeitenden der Firma zu überzeugen, eine Fernzugriffs-Software (zum Beispiel «NTR-Cloud», «Teamviewer») zu installieren. Anschliessend verbinden sie sich mit dem Computer des Opfers und täuschen vor, ein E-Banking-Update durchzuführen. Daraufhin gaukeln die Täter vor, dass das Update getestet werden müsse und drängen das Opfer dazu, seine Zugangsdaten für das E-Banking der Firma einzugeben und eine Testzahlung durchzuführen, damit die Funktionsweise des Systems überprüft werden könne. Ist die Zahlung durch eine Kollektivunterschrift geschützt, versuchen die Betrüger das Opfer zu überzeugen, alle Unterschriftsberechtigten zu organisieren, um die Zahlung freizugeben.

In einer anderen Variante werden die Opfer angewiesen, aufgrund von dringenden E-Banking Updates für einige Tage auf das E-Banking zu verzichten. Im Falle von dringenden Transaktionen soll das Opfer eine durch die Betrüger angegebene Rufnummer kontaktieren. Ruft das Opfer den vermeintlichen Bankmitarbeitende an, um eine E-Banking Transaktion durchzuführen, werden sowohl Benutzername und Passwort als auch das Einmalpasswort nachgefragt. Der Angreifer bekommt so Zugang zum E-Banking der Firma. Dieses Vorgehen kann so lange wiederholt werden, bis das Opfer misstrauisch wird.

Empfehlung:

Die Beispiele zeigen, wie aktuell Social Engineering-Methoden weiterhin sind. Unternehmen sollten kontrollieren, welche Informationen über die eigene Firma online zugänglich sind. Geben Sie auf Ihrer Firmen-Website nie die E-Mail-Adressen von Vorstand bzw. Mitarbeitenden preis – verwenden Sie unpersönliche E-Mail Adressen (z. B. «buchhaltung@xyz.ch»).

Seien Sie misstrauisch, falls sich jemand mit ungewohnten Anliegen bei Ihnen meldet und überprüfen Sie den Anrufenden kritisch. Bei ungewöhnlichen Kontaktaufnahmen und Aufforderungen ist es empfehlenswert, innerhalb der Firma Rücksprache zu nehmen, um die Richtigkeit des Auftrages zu verifizieren. Sensibilisieren Sie die Mitarbeitenden bezüglich dieser Vorfälle, insbesondere die Mitarbeitenden in Schlüsselpositionen.

Geben Sie niemals per Telefon, E-Mail oder im Internet persönliche Zugangsdaten an Dritte weiter. Finanzinstitute werden Sie nie in einem Telefongespräch, E-Mail oder einer Kurznachricht dazu auffordern, vertrauliche Personendaten anzugeben.

Installieren Sie niemals Software und folgen Sie keinen Links, wenn Sie telefonisch oder schriftlich dazu aufgefordert werden. Erlauben Sie niemals einen Fremdzugriff auf Ihren Computer. Keine Bank wird Sie auffordern, an Tests von irgendwelchen Sicherheits-Updates mitzuwirken.

Sämtliche den Zahlungsverkehr betreffenden Prozesse sollten firmenintern klar geregelt sein und von den Mitarbeitenden in allen Fällen konsequent eingehalten werden.

### 4.4.2 Erpressungsversuche – Mit einem Bluff lässt sich gut Geld verdienen

Seit einiger Zeit gibt es eine Betrugsmasche, welche eng mit der Nutzung von Sozialen Medien zusammenhängt. Meistens erfolgt eine Kontaktaufnahme durch eine sehr attraktive Person über die Sozialen Medien. Diese flirtet mit dem potenziellen Opfer und verleitet dieses, sich vor der Webcam zu entblössen. Das Opfer weiss nicht, dass es dabei gefilmt wird. Mit diesem Videomaterial wird das Opfer danach erpresst. Diese Erpressungsmethode wird «Sextortion» genannt. Wird kein Geld bezahlt, wird das Material veröffentlicht. Diese Masche ist mit einigem Aufwand verbunden. Da ein direkter Kontakt zwischen Täter und Opfer stattfindet, ist auch das Risiko, verhaftet zu werden, erhöht.

Seit März 2018 (in der Schweiz seit Juli 2018) bedienen sich die Kriminellen einer Masche, die mit bedeutend weniger Aufwand und Risiko verbunden ist. Sie behaupten, in einer Mail, Zugang zu Computer und Webcam zu haben und drohen damit, Bilder und Videos mit sexuellem Inhalt zu veröffentlichen. In diesen Fällen bluffen die Angreifer allerdings und verfügen auch über keinen Zugang zum Computer der erpressten Person. Diese Betrugsmasche wird «Fake-Sextortion» genannt. Mit dieser Betrugsmethode haben Kriminelle in der zweiten Jahreshälfte von 2018 trotz der einzelnen, kleinen geforderten Summen insgesamt ziemlich viel Geld kassiert. Basierend auf der Analyse der Bitcoin-Adressen in den E-Mails, die MELANI gemeldet worden sind und auf die das Lösegeld bezahlt werden sollte, sind in der zweiten Jahreshälfte 2018 fast 100 Bitcoins einbezahlt worden. Das entspricht aktuell einem Gegenwert von ungefähr CHF 360'000. Weil der Versand von Massen-E-Mails praktisch kostenlos ist, ist der Gewinn entsprechend hoch. Ob diese Bitcoin-Adressen ausschliesslich für Fake-Sextortion und nur von Schweizer Opfern verwendet werden, ist nicht bekannt.

Als «Beweis» für die Kompromittierung des Computers ist in den E-Mails meist ein Passwort aus vergangenen Datenabflüssen angegeben. In den meisten Fällen ist dieses Passwort jedoch veraltet. Um das Opfer zu überzeugen, dass das Mobiltelefon kompromittiert worden sei, werden mittlerweile auch Mobiltelefonnummern verwendet. Solche «nicht sensiblen» Daten aus diversen Datenabflüssen sind in letzter Zeit vermehrt publiziert worden. In einer anderen Variante wird als Beweis, dass das E-Mail-Konto kompromittiert worden sei, die Nachricht mit der eigenen Mail-Adresse als Absender versendet. In Tat und Wahrheit ist der Absender jedoch nur gefälscht, was sehr einfach und ohne grosse Kenntnisse gemacht werden kann. Der Angreifer braucht zu diesem Zweck keinen Zugriff auf das E-Mail Konto.

Erpresser-E-Mails werden in mehreren Sprachen verfasst, darunter auch Deutsch, Französisch, Italienisch und Englisch. Die Vorgehensweise hat sich im Grossen und Ganzen nicht verändert. Jedoch arbeiten die Kriminellen kontinuierlich an der Optimierung der Erpressungsversuche, um den Druck auf die Opfer zu erhöhen und sie zum Bezahlen zu bewegen. Die nachfolgende Grafik zeigt die wichtigsten Neuerungen, die von den Kriminellen im Laufe des Jahres 2018 vorgenommen wurden.

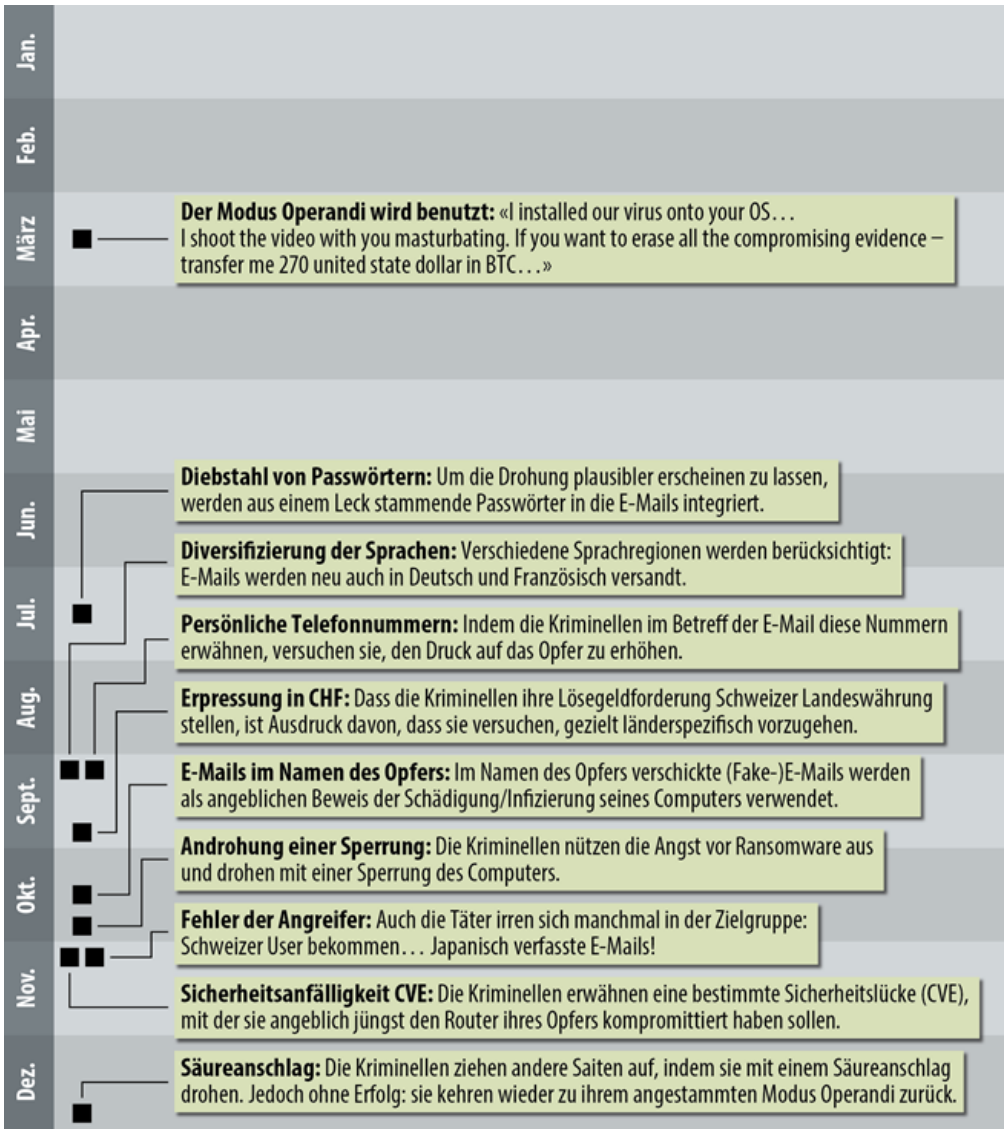



Abbildung 2: Entwicklung der Fake-Sextortion Varianten im Jahr 2018

Eine Unterart dieses Phänomens sind Erpressungen mit der Androhung eines Säure- oder Bombenanschlags. Bei beiden Varianten wird ebenfalls Lösegeld in Form von Bitcoins gefordert, um den Anschlag zu verhindern. Man hat allerdings festgestellt, dass mit der Androhung von physischen Konsequenzen die Empfänger die Behörden eher kontaktieren, bevor sie Lösegeld bezahlen. Dies mag am grösseren Einschüchterungspotenzial liegen, sowie der Absenz von scheinbar kompromittierendem Material im Besitz der Täter. Jedenfalls konnte auf den an MELANI gemeldeten Bitcoin-Adressen im Zusammenhang mit dieser Drohungsart keine Transaktionen festgestellt werden.

Empfehlung:

Solange die betroffenen Empfänger nicht aufhören, Lösegeld zu bezahlen, wird diese Masche befeuert. Es ist zu erwarten, dass diese Wellen weitergehen, Nachahmungstäter auf den Zug aufspringen und die Anzahl noch weiter zunehmen wird. Zahlen Sie unter keinen Umständen ein Lösegeld. Sie können zur Prävention beitragen, indem Sie diese Vorgehensweise von Kriminellen in Ihrem beruflichen und persönlichen Umfeld thematisieren. Sensibilisieren Sie Mitarbeitende, Bekannte und Verwandte, damit diese nicht auf solche Machenschaften hereinfallen.


Auf der Webseite www.stop-sextortion.ch , die von den Behörden lanciert worden ist, finden Sie Informationen und können Fake-Sextortion E-Mails melden.

### 4.4.3 Office 365-Zugangsdaten für Überweisungsbetrug verwendet

Dass Zugangsdaten zu «Office365», der Online-Version der Office-Produkte, bei Kriminellen sehr beliebt sind, ist in früheren Halbjahresberichten[16] bereits thematisiert worden. Mit über 100 Millionen monatlichen Nutzern sind Office 365-Konten zu einem populären Ziel für Angreifer geworden. Der Angriff startet jeweils mit einer gewöhnlichen Phishing-E-Mail. Diese gibt beispielsweise vor, dass die Grenze des Speicherplatzes überschritten sei und dass man sich zur Behebung des Problems einloggen soll. Der angegebene Link führt selbstverständlich auf eine betrügerische Webseite.

In der Berichtsperiode kam es mit auf diese Weise ergatterten Office-365-Zugangsdaten vermehrt zu sogenanntem Überweisungsbetrug (Wire-Fraud). Davon spricht man, wenn Betrüger in kompromittierten Konten nach bestehenden elektronischen Rechnungen suchen, diese dann kopieren, mit einer anderen IBAN versehen und erneut zustellen. Im Visier sind dabei besonders Firmen, welche grosse Rechnungsbeträge an ausländische Rechnungsempfänger stellen. Einerseits ist der Profit in diesen Fällen besonders lukrativ, andererseits ist es schwieriger, ein missbräuchliches Empfängerkonto zu detektieren, da sich es sich um ausländische Empfängerkonten handelt.

Wie ausgeklügelt solche Angriffe sind, zeigt ein Beispiel des Sicherheitsdienstleisters «Proofpoint». Nachdem sich die Angreifer Zugriff auf das Office 365-Konto des CEOs einer Firma verschafft hatten, suchten sie in den E-Mails und im Kalender nach Informationen, um eine passende Geschichte zu kreieren. Während eines im Kalender eingetragenen Treffens des CEOs mit einem wichtigen Lieferanten schrieb der Angreifer dem Finanzchef, dass er 1 Million US-Dollar überweisen solle, um diesen Deal abzuschliessen. Er schrieb weiter, dass er selbst

[16] MELANI Halbjahresbericht 2/2017 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2017-2.html (Stand: 31. Januar 2019)

an der Sitzung festsitze und nicht telefonieren könne. Der Finanzchef folgte dieser Aufforderung und zahlte.[17]

Gemäss der US-Sicherheitsbehörde «FBI» gehört diese Vorgehensweise, die als «Business E-Mail Compromise (BEC)» bezeichnet wird, mittlerweile zu jenen mit den grössten finanziellen Schäden. So wurden dem «Internet Crime Complaint Center (IC3) » im Jahr 2018 Fälle von BEC und seinen Varianten mit einem Gesamtverlust von 1,2 Milliarden US-Dollar gemeldet. Vor allem der Immobiliensektor sei von diesem Angriffstyp besonders betroffen.[18]

Empfehlung:

Arbeitet eine Firma in der «Office 365-Cloud», haben Angreifer mit den gestohlenen Zugangsdaten auch Zugriff auf sämtliche Dokumente der Firma. Solche Daten nur mit Benutzernamen und Passwort zu sichern, ist heutzutage äusserst fahrlässig. Aktivieren Sie deshalb wo immer möglich die 2-Faktor-Authentisierung. Allerdings ist eine saubere Implementierung wichtig. Auch beim Einsatz von Single Sign-On oder Multi-Faktor-Authentifizierung (MFA) ist eine Kompromittierung möglich, wenn die Authentifizierung nicht systemübergreifend implementiert ist. Diese Lücken können dann von Angreifern genutzt werden.

Die Mitarbeitenden sollten dahingehend sensibilisiert werden, dass definierte Prozesse des Unternehmens und Vorsichtsmassnahmen von allen jederzeit zu befolgen sind. Bei Überweisungen ist beispielsweise das Vieraugenprinzip mit Kollektivunterschrift empfehlenswert.

### 4.4.4 Gefälschte Gewinnspiele

Ein Jahr lang Schokolade als Geschenk, ein Gutschein von «IKEA» oder ein neues iPhone: Vermeintliche Gewinnspiele sind im Internet sehr verbreitet. Wir haben bereits in unserem letzten Halbjahresbericht darüber berichtet[19]. Die Fragen sind bei all diesen Gewinnspielen so gewählt, dass alle sie leicht beantworten können. Die Autoren wollen nämlich, dass möglichst viele Mitspieler «gewinnen», und sie dadurch möglichst viele Opfer erhalten. In der Berichtsperiode trat eine neue Variante auf. Dabei wurden potenzielle Gewinner via Facebook auf eine vermeintliche Denner-Webseite gelockt, weil sie angeblich 750 CHF gewonnen haben. Nach der Angabe von Telefonnummer und Name wurden die Teilnehmer aufgefordert, eine kostenpflichtige 0901-Nummer anzurufen. Um an den vermeintlichen Gewinn zu kommen, müssen möglichst viele Fragen beantwortet werden. In Wirklichkeit dient die Vielzahl an Fragen nur dazu, die Opfer möglichst lange in der kostenpflichtigen Leitung zu halten. Es versteht sich von selbst, dass der Gewinn in Tat und Wahrheit nicht existiert.

---

17 https://www.proofpoint.com/us/corporate-blog/post/microsoft-office-365-attacks-circumvent-multi-factor-authentication-lead-account (Stand: 31. Januar 2019)

18 https://www.ic3.gov/media/annualreport/2018_IC3Report.pdf (Stand: 25. April 2019)
https://www.ic3.gov/media/2018/180712.aspx#fn2 (Stand: 31. Januar 2019)

19 MELANI Halbjahresbericht 1/2018
https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2018-1.html (Stand: 31. Januar 2019)

Empfehlung:

Hinterfragen Sie Nachrichten mit verlockenden Gewinnversprechen kritisch und leiten Sie diese keinesfalls weiter. Am besten ignorieren Sie diese grundsätzlich.

INFO

Der Konsumentenschutz hat zu diesem Thema diverse Tipps zusammengestellt:

https://www.konsumentenschutz.ch/was-tun-bei-einer-abofalle/

### 4.4.5 Phishing

Auch im zweiten Halbjahr 2018 wurden zahlreiche Phishing-E-Mails versendet. Der Inhalt der Mails ändert sich dabei nicht markant: Die einen fragen nach Kreditkartendaten, damit diese «verifiziert» werden können, andere fordern auf der verlinkten Seite nach Login und Passwort zu Internetdiensten. Regelmässig werden in solchen Phishing-Mails auch Firmenlogos von bekannten Unternehmen respektive des betroffenen Dienstes missbraucht, um den E-Mails einen offiziellen Anstrich zu geben.


Abbildung 3: Gemeldete und bestätigte Phishing-Seiten pro Woche auf antiphishing.ch in der zweiten Jahreshälfte 2018

Insgesamt wurden im Jahr 2018 5756 verschiedene eindeutige Phishing-Seiten über das von MELANI betriebene Portal antiphishing.ch gemeldet. Auf Abbildung 3 sind die gemeldeten Phishing-Webseiten pro Woche dargestellt. Auffällig sind die Spitzen in den letzten drei Monaten des Jahres 2018. Der Hauptgrund war ein grosses UBS Kreditkarten-Phishing in diesem Zeitraum.


Abbildung 4: UBS Kreditkartenphishing in den letzten drei Monaten des Jahres 2018.

Schon vor mehreren Jahren prophezeite MELANI, dass auch für Phishing-Seiten zunehmend verschlüsselte Webseiten mit der URL «https://» verwendet werden. Diese Entwicklung fand jedoch langsamer statt als erwartet. Seit dem dritten Quartal 2016 verzeichnet nun der Sicherheitsdienstleister «PhishLab» eine kontinuierliche Zunahme und hat Ende 2018 das erste Mal einen Anteil von 50 Prozent an verschlüsselten Phishing-Seiten ausgemacht.[20] Diese Beobachtung dürfte allerdings in einem grossen Masse damit zu tun haben, dass allgemein immer häufiger Webseiten verschlüsselt werden. Da es sich bei einem grossen Teil der Phishing-Seiten um gehackte Webseiten handelt, «profitieren» die Kriminellen von diesem Umstand und benutzen die Verschlüsselung wissentlich oder zum Teil auch unwissentlich gleich mit.

### 4.4.6 Blockierungsanträge

Um Missbrauch von Schweizer Internetadressen zu bekämpfen und akute Gefahren für Internetbenutzer abzuwehren, wurde bei der Revision der Verordnung über die Adressierungselemente im Fernmeldebereich (AEFV, SR 784.104; in Kraft per 1. Januar 2010) ein neuer Artikel eingeführt. Gemäss diesem Artikel muss die «.ch»-Registerbetreiberin (SWITCH) Domain-Namen blockieren und die entsprechende Zuweisung zu einem Namenserver aufheben, wenn der begründete Verdacht besteht, dass dieser Domain-Name benutzt wird, um entweder mit unrechtmässigen Methoden an schützenswerte Daten zu gelangen (so genanntes Phishing) oder über diese Domain schädliche Software (so genannte Malware) verbreitet wird. Eine weitere Voraussetzung ist, dass eine in der Bekämpfung der Cyberkriminalität vom Bundesamt für Kommunikation (BAKOM) anerkannte Stelle die Blockierung beantragt hat.

Seit dem 15. Juni 2010 ist MELANI vom BAKOM als entsprechende Stelle anerkannt und kann bei SWITCH die Blockierung und Aufhebung der diesbezüglichen Zuweisung zu einem Namenserver von «.ch»-Domain-Namen bei begründetem Verdacht auf Phishing oder Verbreitung von Malware beantragen.

Bei den von MELANI beantragten Blockierungen handelt es sich mehrheitlich um Phishingseiten. Nachdem in den Jahren 2016 und 2017 über 30 Seiten blockiert wurden, sank diese Zahl im Jahr 2018 auf 16. Dies lässt sich dadurch erklären, dass nur Seiten blockiert werden, die ausschliesslich für Phishing oder Malwareverteilung verwendet werden. Phishingseiten befinden sich aber mehrheitlich auf kompromittierten Systemen, auf denen auch noch anderer Inhalt gespeichert ist. In diesen Fällen wird die Domäne nicht blockiert, sondern es wird über den Provider versucht, die betrügerische Seite vom Netz zu nehmen.

[20] https://info.phishlabs.com/blog/49-percent-of-phishing-sites-now-use-https (Stand: 31. Januar 2019)

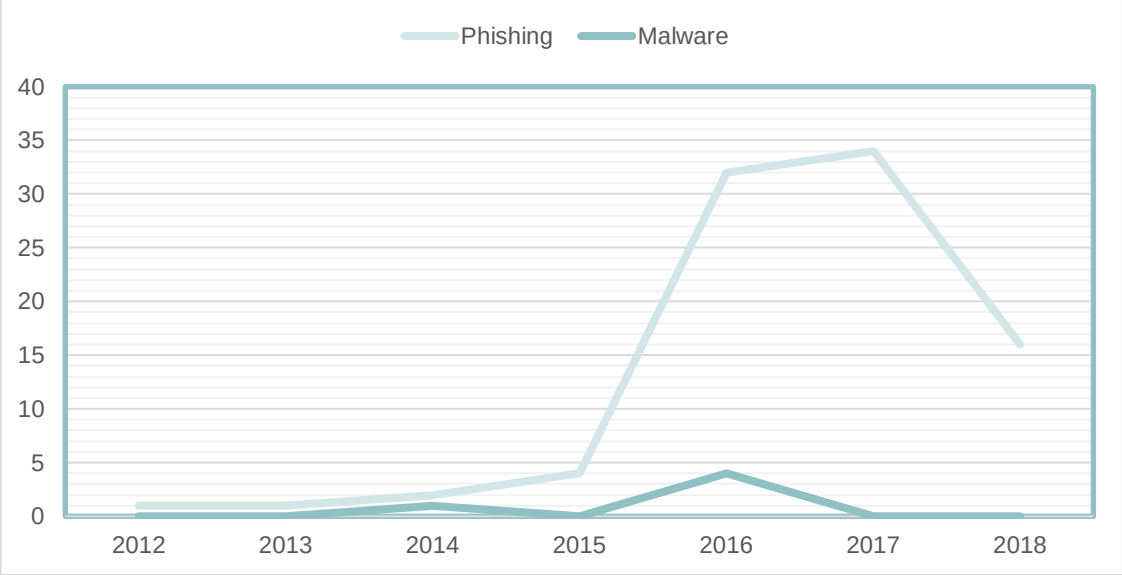



Abbildung 5: Blockierungsanträge von MELANI gemäss VID 15. Blockierungsanträge von Phishingseiten sind hellblau dargestellt, Anträge von Seiten mit Malware sind dunkelblau dargestellt.

## 4.5 Crimeware

Auch im ersten Halbjahr 2018 gab es zahlreiche Infektionen mit krimineller Software (Crimeware). Die Statistik in Abbildung 6 zeigt die Verteilung der wichtigsten Schadsoftware in der Schweiz auf. Es gibt auch Malware, die zwar ebenfalls eine hohe Bedeutung hat, aber nicht in der Statistik erscheint wie zum Beispiel die E-Banking-Malware «Retefe».

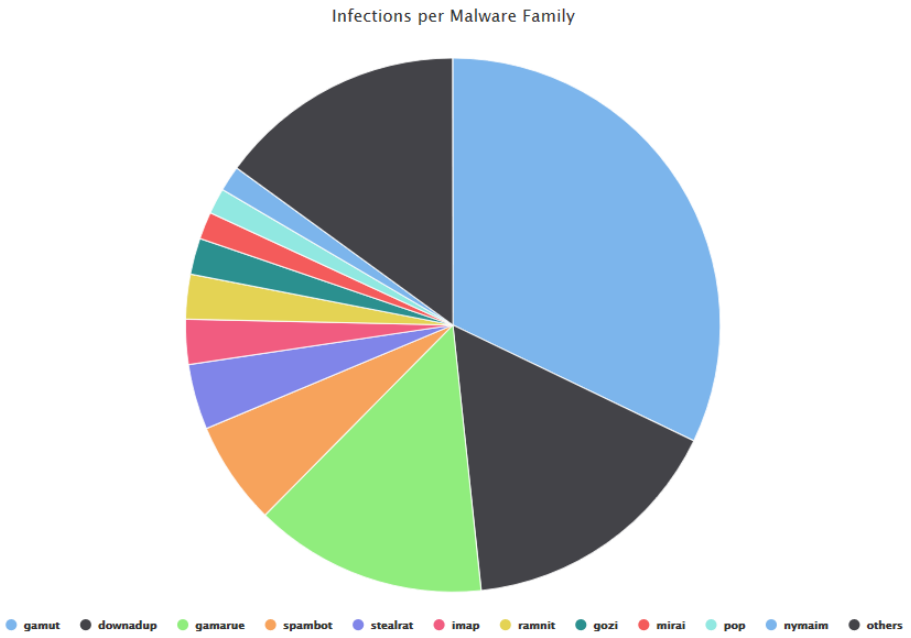



Abbildung 6: Verteilung der Schadsoftware in der Schweiz, welche MELANI bekannt ist. Stichtag ist der 31. Dezember 2018. Aktuelle Daten finden Sie unter: http://www.govcert.admin.ch/statistics/dronemap/

Das erste Mal seit Erstellen dieser Statistik befindet sich die Schadsoftware «Downadup» (auch bekannt als «Conficker») nicht mehr auf Platz eins. Neuer Spitzenreiter war im zweiten Halbjahr 2018 die Schadsoftware «Gamut», welche für den Grossteil des weltweiten Spam-Aufkommens verantwortlich ist. Das «Gamut Botnet» sendet vor allem Spam zu Jobangeboten zwecks «Money Mule»-Rekrutierung.[21] Auf Platz drei folgt «gamarue»[22], auch bekannt unter dem Namen «andromeda», ein Downloader, der weitere Schadsoftware nachladen kann. An vierter und fünfter Stelle folgen die Schadsoftware «Spambot» und «Stealrat». Auch diese beiden sind für den Versand von Spam zuständig. «Stealrat» tut dies über infizierte Domänen, unter denen «WordPress», «Joomla!» und «Drupal» laufen. Spam-Nachrichten werden dadurch über legitime Mail-Server versendet und sind schwieriger zu filtern. Auf Platz acht folgt der erste E-Banking-Trojaner «Gozi». Das seit dem Angriff auf den Internetdienstleister «Dyn» bekannt gewordene Bot-Netzwerk «Mirai» hat es wieder in die Top-Ten geschafft und verdrängt die Cryptominer-Schadsoftware «Monerominer», die nicht mehr in der Liste vertreten ist.

### 4.5.1 E-Banking Trojaner Retefe – bedeutendster Bankentrojaner der Schweiz

Retefe ist weiterhin einer der bedeutendsten Bankentrojaner in der Schweiz. Die Schadsoftware wird per E-Mail im Namen von bekannten Firmen oder Institutionen verschickt und zielt sowohl auf Windows als auch auf macOS-Systeme. Im Anhang des E-Mails befindet sich meist ein bösartiges Worddokument, z.B. eine angebliche Rechnung eines Online-Shops, eine Zustellbestätigung eines Paketlieferanten oder Informationen der Bundesverwaltung zu verseuchtem Trinkwasser. Abbildung 7 zeigt die Anzahl Spamwellen der letzten drei Jahre.

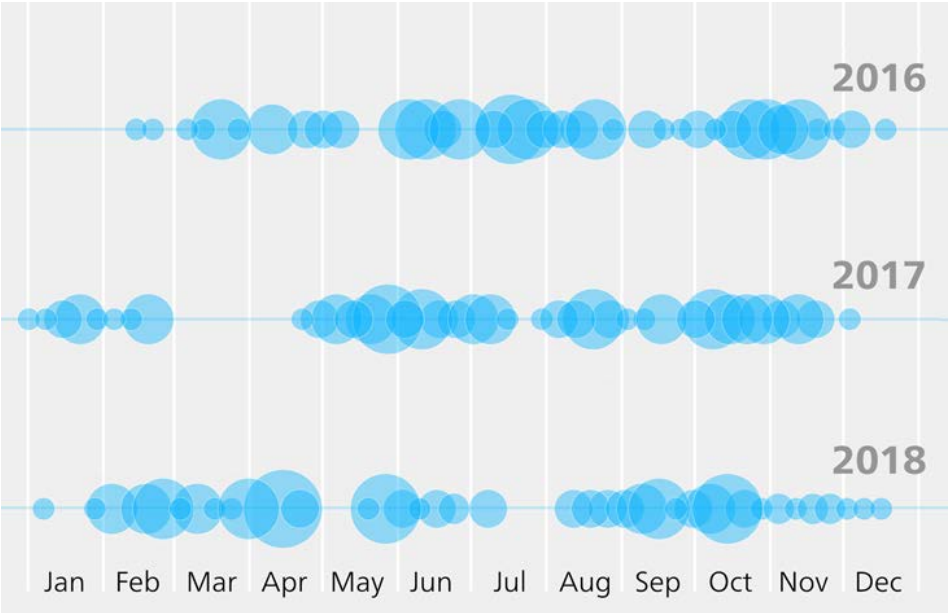



Abbildung 7: Retefe Wellen der letzten drei Jahre. Die blauen Kreise stehen für die Anzahl und Grösse der verschiedenen Spamwellen

[21] https://sensorstechforum.com/de/necurs-gamut-botnets-spam/ (Stand: 31. Januar 2018).

[22] https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/BotNetze/Avalanche/Schadsoftware/Andromeda_Gamarue.html (Stand: 31. Januar 2018).

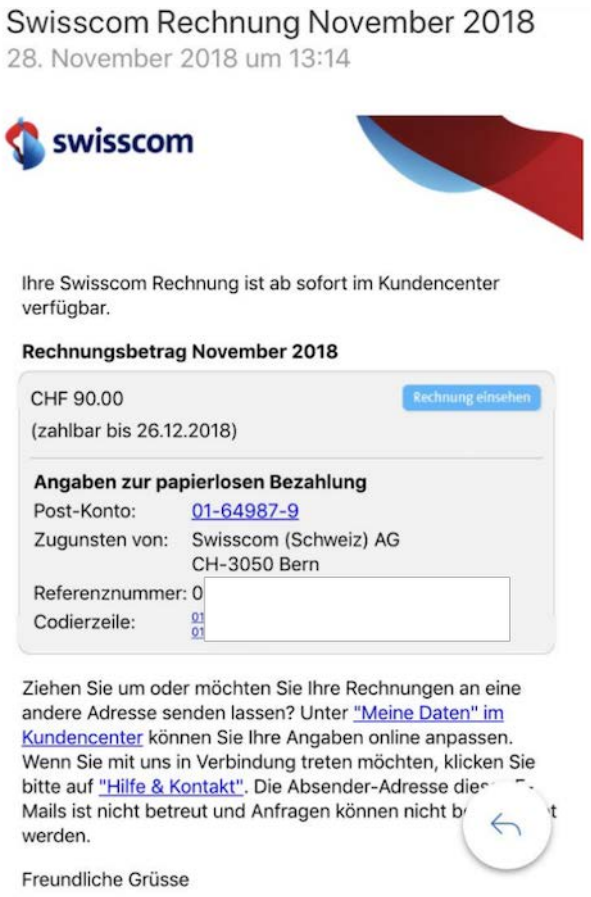
Zudem versucht Retefe die Glaubwürdigkeit der E-Mails zu erhöhen, indem persönliche Informationen wie Telefonnummern oder Anschrift des Empfängers genannt werden. Diese Angaben stammen aus Datenabflüssen. Retefe zielt momentan nur auf Privatkunden in der Schweiz, Liechtenstein und Norwegen. Firmenkunden sind von Retefe weniger betroffen. Zum einen werden Offlinezahlungssysteme nicht direkt angegriffen, zum anderen muss Retefe die Proxyeinstellungen verändern, sowie ein Stammzertifikat und Tor installieren. Bei Firmencomputern sollten diese Rechte eingeschränkt sein, so dass eine solche Manipulation nicht möglich ist.

Empfehlung:

Seien Sie besonders vorsichtig beim Öffnen von Word-Dokumenten, Normalerweise versenden Firmen und Organisationen im Geschäftsverkehr (beispielsweise Rechnungen, Offerten usw.) pdf-Dateien und keine Word-Dokumente.

### 4.5.2 Gozi wieder aktiv

Nach einer recht langen Zeit mit wenig Gozi-Angriffen in der Schweiz, ist am 28. November 2018 eine E-Mail-Welle mit einer gefälschten Swisscom Rechnung aufgetaucht. Dabei nutzen die Angreifer geschickt Social Engineering Methoden.


Swisscom Rechnung November 2018
28. November 2018 um 13:14

swisscom

Ihre Swisscom Rechnung ist ab sofort im Kundencenter verfügbar.

**Rechnungsbetrag November 2018**

CHF 90.00 Rechnung einsehen
(zahlbar bis 26.12.2018)

**Angaben zur papierlosen Bezahlung**
Post-Konto: 01-64987-9
Zugunsten von: Swisscom (Schweiz) AG
CH-3050 Bern
Referenznummer: 0
Codierzeile:

Ziehen Sie um oder möchten Sie Ihre Rechnungen an eine andere Adresse senden lassen? Unter "Meine Daten" im Kundencenter können Sie Ihre Angaben online anpassen. Wenn Sie mit uns in Verbindung treten möchten, klicken Sie bitte auf "Hilfe & Kontakt". Die Absender-Adresse dies... E-Mails ist nicht betreut und Anfragen können nicht b... werden.

Freundliche Grüsse

Abbildung 8: Gefälschte Swisscom-Rechnung mit Link auf eine bösartige Datei

Das Mail enthält einen Link zu einer ZIP-Datei, welche ein obfuskiertes (verschleiertes) Visual Basic Skript enthält, das via Powershell «bitsadmin»[23], gestartet wird. So wird die eigentliche Malware heruntergeladen, ins temporäre Profil des jeweiligen Benutzers gespeichert und dann gestartet.

Neben den Angaben zu den fixen Command und Control Servern enthält die Konfiguration von Gozi Angaben, die für den Einsatz eines Domain Generation Algorithmus notwendig sind. Diese Domainamen basieren auf Wörtern der US Verfassung, die zufällig gewählt und neu zusammengesetzt werden[24]. So können dynamische Kontaktpunkte für Kontrollserver definiert werden, falls die fix programmierten nicht mehr funktionieren. Im aktuellen Fall wurde diese Funktion aber nicht verwendet.

Gozi enthält in seiner Konfiguration einerseits anzugreifende Banken und andererseits Software Produkte, die überwacht werden sollen. Dabei zielt die Malware auch auf Offline Payment Software und nimmt damit auch direkt Firmen ins Visier.

Empfehlung:

Wir empfehlen insbesondere KMUs für Zahlungen eigene, dedizierte Geräte mit eingeschränktem Internet Zugang zu verwenden, darauf weder zu surfen noch zu mailen, das Gerät und die installierte Software aktuell zu halten, und Passwörter in einem Passwort Safe zu speichern. Bei der Freigabe von Zahlungen wird das 4-Augenprinzip empfohlen und die Freigabe auf einem zweiten, ebenso abgesicherten Gerät durchzuführen. Verdächtige Zahlungen sollten immer so rasch als möglich an die Bank gemeldet werden.

### 4.5.3 Gefälschte Banken Apps

Im Zeitalter der Smartphones spielen Apps eine wichtige Rolle. Der Nachteil für die Kriminellen ist hierbei, dass Apps im Gegensatz zu einem Standard-Browser zumeist proprietär aufgebaut sind. Wird eine App missbraucht, hat der Anbieter und Entwickler im Gegensatz zu einem Standard-Browser, direkt die Möglichkeit den Code anzupassen und auf Angriffe mit entsprechenden Sicherheitsmechanismen zu reagieren. Es ist für einen Kriminellen also schwieriger, eine App anzugreifen und diese zu manipulieren.

Deshalb versuchen Kriminelle vor allem, gefälschte Apps in Umlauf zu bringen statt rechtmässige Apps zu manipulieren. Gerade im Finanzbereich finden regelmässig zahlreiche solcher gefälschten Apps den Weg in offizielle und inoffizielle Stores. Solche Fake Apps sind relativ einfach aufgebaut und blenden nach dem Start irgendwelche Formularfelder ein, in denen Kreditkartendaten, Login und Passwörter angegeben werden sollen. Mit ähnlichen Namen und Logos der Banken werden die Opfer geködert, solche Apps herunterzuladen. Auch andere Social Engineering-Methoden gehören zum Repertoire der Angreifer: So behaupteten beispielsweise die Kriminellen, dass die Kreditlimite bei den entsprechenden Banken mit einer (gefälschten) App erhöht werden könne.

---

23 https://docs.microsoft.com/en-us/windows/desktop/bits/bitsadmin-tool (Stand: 31. Januar 2018).

24 Gozi Blog: https://www.govcert.admin.ch/blog/18/gozi-isfb-when-a-bug-really-is-a-feature (Stand: 31. Januar 2018).

Mit «Google Play Protect» hat Google zwar einen Filter entwickelt, der im vergangenen Jahr erstmals für einen Rückgang der Malware-Verbreitung unter «Android» gesorgt hat. Trotzdem tauchen immer wieder Fake-Apps auf.

Ende September war auch die «Postfinance» von einer solchen Fake App betroffen. Bei der gefälschten Postfinance-App wurden keine Zugangsdaten zum E-Banking oder andere Passwörter abgefragt. Die Angreifer hatten es auf die Kreditkartendaten abgesehen. Hatte das Opfer diese Daten eingegeben, erschien eine Dankesseite und die App wurde wieder beendet. Spätestens dann sollten Opfer stutzig werden und Kontakt mit dem jeweiligen Internetdienstleister oder der Kreditkartenfirma aufnehmen.[25]

### 4.5.4 Ransomware

Erpressungen mittels Verschlüsselungs-Software, sogenannter Ransomware, gehört zur Zeit sicherlich zu den Angriffsarten mit den grössten Auswirkungen für KMUs aber auch für kritische Informationsinfrastrukturen, wie die Beispiele in Kapitel 5.3.5 zeigen. Am Verbreitesten sind zur Zeit die Typen «Ryuk», «GandCrab», «Dharma» und «Locky». Eine Übersicht aller Ransomware-Typen ist auf der Webseite «botfrei.de» aufgeführt[26].

Die Ransomware «Ryuk» fällt vor allem durch ihre Vorgehensweise auf, im Vorfeld Daten zu sammeln, um danach gezielt Systeme von lukrativen Opfern zu verschlüsseln. Am 12. Dezember 2018 publizierte MELANI eine entsprechenden Warnung vor verschiedenen Malspam-Wellen mit infiziertem Word-Dokumenten im Anhang.[27] Die Verteilung von Ryuk geschah über den bereits länger bekannten Trojaner «Emotet». Dieser versucht, mit gefälschten E-Mails im Namen von Kollegen, Geschäftspartnern oder Bekannten mittels Social Engineering den Empfänger zum Öffnen des angehängten Word-Dokuments sowie zum Ausführen der darin enthaltenen Office-Makros zu verleiten. Ursprünglich als E-Banking-Trojaner bekannt, wird Emotet heute vor allem für den Versand von Spam, sowie das Nachladen von weiterer Schadsoftware verwendet. In diesem Fall wurde die Malware «Trickbot» nachgeladen, welche versuchte, sich Rechte auf den infizierten Computern zu verschaffen. Einmal installiert, führte Trickbot eine umfassende Netzwerkanalyse durch, um zu erkennen, ob der Rechner Teil einer grösseren Firma oder Organisation ist und versuchte sich innerhalb dieses Netzwerkes mittels der bekannten Sicherheitslücke «SMB» zu verbreiten. Immer wieder kommuniziert der Schädling mit dem Kontrollserver. Nur wenn das Ziel von den Tätern als als gross genug erachtet wird, wird schliesslich die Ransomware Ryuk nachgeladen, welche die Daten auf den Computern und Servern im Firmennetzwerk verschlüsselt. Durch diesen sehr gezielten Einsatz soll die Täterschaft seit August 2018 Bitcoins im Gegenwert von rund 3,7 Millionen US-Dollar eingenommen haben[28]. Wie viel davon in physisches Geld umgesetzt werden konnte, ist nicht bekannt. Ebenso ist noch nicht bekannt, von wo aus die Täter operieren.

---

25 https://www.blick.ch/news/wirtschaft/ueber-1000-opfer-falsche-postfinance-app-in-play-store-gebracht-id8881643.html (Stand: 31. Januar 2019)

26 https://www.botfrei.de/de/ransomware/galerie.html (Stand: 31. Januar 2019)

27 https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/Trojaner_Emotet_greift_Unternehmensnetzwerke_an.html (Stand: 31. Januar 2019)

28 https://derstandard.at/2000096143241/Ryuk-Neue-Ransomware-brachte-Cyberkriminellen-vier-Millionen-Dollar (Stand: 31. Januar 2019)

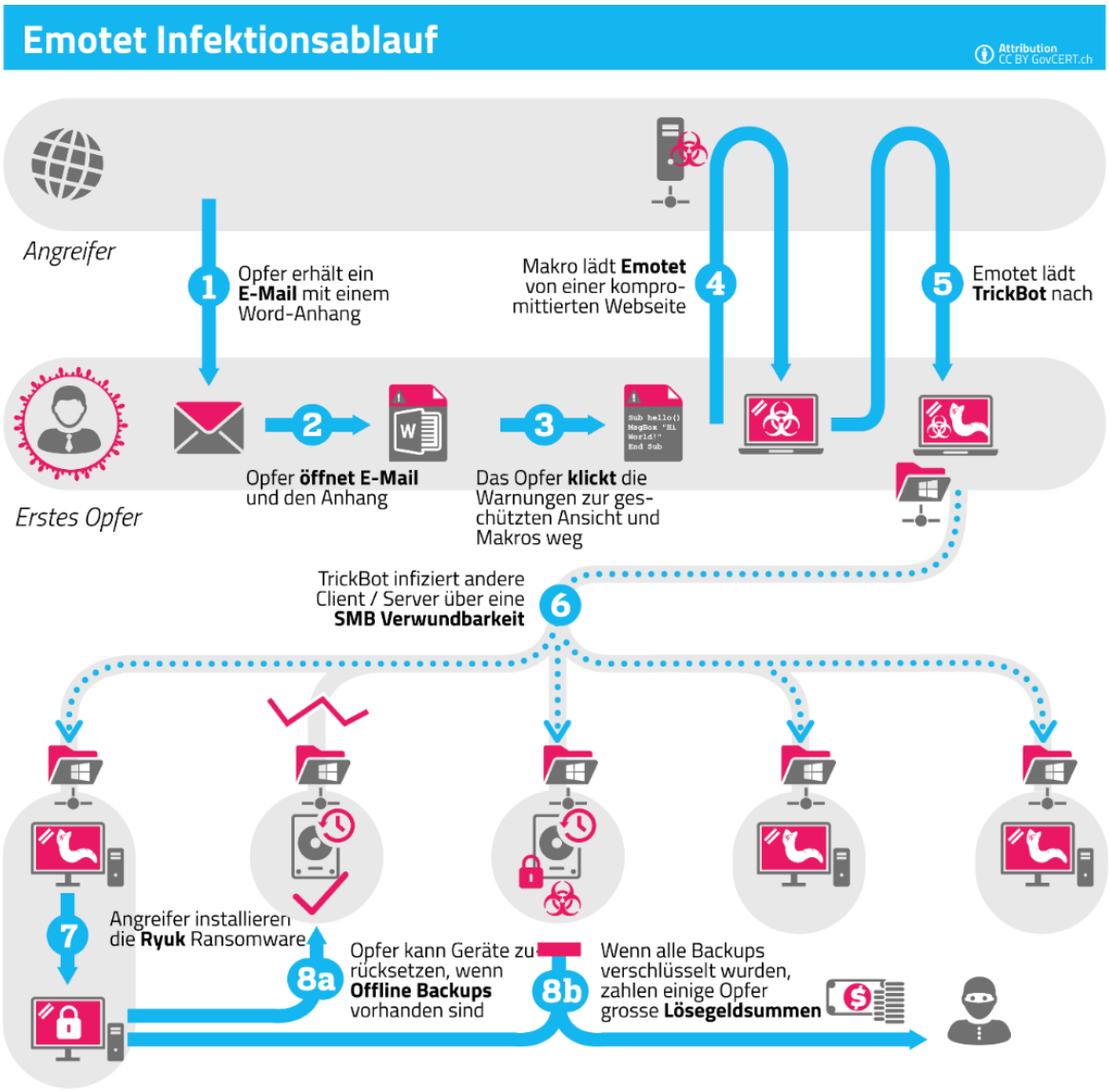



Abbildung 9: Schematischer Infektionsablauf der Schadsoftware Emotet

Auch Fälle mit der Ransomware «GandCrab» wurden im zweiten Halbjahr 2018 mehrfach an MELANI gemeldet. Die Ransomware tauchte im Januar 2018 erstmals auf[29] und zeichnet sich vor allem durch eine Vielzahl von Infektionsvektoren aus. Zunächst wurde GandCrab durch Spam-E-Mails verbreitet. Im Sommer 2018 änderten die Angreifer mit der Version 4 die Vorgehensweise und nutzten zur Verbreitung Webseiten, auf denen illegale gecrackte Versionen von kostenpflichtiger Software angeboten werden. Oft handelt es sich dabei um gefälschte Seiten, die von den Erpressern selbst aufgeschaltet wurden und die via Google-Suche gefunden werden. Manipulierte Bewerbungsunterlagen gehören ebenfalls zum Repertoire der Verbreitungsmethoden.[30] Zudem berichtete die Sicherheitsfirma «FireEye» im August 2018, dass

29 https://blog.comodo.com/comodo-news/gandcrab-the-new-version-of-ransomware/ (Stand: 31. Januar 2019)

30 https://www.heise.de/security/meldung/Erpressungstrojaner-Gandcrab-verbreitet-sich-ueber-gefaelschte-Bewerbungsmails-4154167.html (Stand: 31. Januar 2019)

die Ransomware Gandcrab auf manipulierten Webseiten ein Exploit-Kit einsetzt. Dieses wird auf infizierten Webseiten eingebettet und nutzt zwei Sicherheitslücken in Windows aus.[31].

Die Ransomware «Dharma» ist schon seit 2016 aktiv. Trotzdem gehört diese immer noch zu den gefährlichsten Verschlüsselungs-Trojanern. Die Täter hinter dieser Malware veröffentlichen weiterhin neue Varianten mit neuen Verschlüsselungen, die nicht zu knacken sind. Die Ransomware Dharma fiel im zweiten Halbjahr 2018 vor allem aufgrund zweier Opfer auf, die grosses mediales Interesse auslösten: Die schottische Brauerei «Arran Brewery» und ein grosser Seehafen waren von Dharma betroffen (siehe auch Kapitel 5.3.5)

Es gab in der Berichtsperiode aber auch gute Nachrichten zu vermelden: Das FBI gab am 26. November 2018 bekannt, zwei Hintermänner der Ransomware «SamSam» identifiziert zu haben. Es handelte sich um zwei iranische Staatsbürger im Alter von 28 und 35 Jahren. Das US-Justizministerium hat dazu eine entsprechende Anklage veröffentlicht. Die Täter sollen über 6 Millionen US-Dollar an Lösegeldzahlungen von Opfern aus verschiedenen Sektoren erhalten haben, darunter auch kritische Infrastrukturen in den Sektoren Gesundheit, Transport und Verwaltung.

Empfehlung:

Erstellen Sie regelmässig eine Sicherungskopie (Backup) Ihrer Daten. Die Sicherungskopie sollte offline, das heisst auf einem externen Medium wie beispielsweise einer externen Festplatte gespeichert werden. Trennen Sie das externe Medium, auf welchem Sie die Sicherungskopie erstellen, nach dem Backup-Vorgang vom Computer. Ansonsten werden bei einem Befall durch Ransomware möglicherweise auch die Daten auf dem Backup-Medium verschlüsselt und unbrauchbar.

Segmentieren Sie Ihr Netzwerk. Trennen Sie besonders gefährdete Stellen wie beispielsweise die Personalabteilung oder die Medienstelle, welche Anhänge von unbekannten Sendern öffnen müssen, vom Rest des Netzwerkes ab.


MELANI-Infoseite bezüglich Verschlüsselungstrojanern

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

31 https://www.fireeye.com/blog/threat-research/2018/09/fallout-exploit-kit-used-in-malvertising-campaign-to-deliver-gandcrab-ransomware.html (Stand: 31. Januar 2019)

# 5 Lage International

## 5.1 Spionage

### 5.1.1 APT 10

Am 20. Dezember 2018 klagte das US-Departement für Justiz (DoJ) zwei chinesische Staatsbürger an, in Computer eingedrungen zu sein, sowie Überweisungsbetrug und Identitätsdiebstahl begangen zu haben. Die zwei Männer sollen Mitglieder der Cyber-Spionagekampagne «APT10» gewesen sein. Diese Kampagne ist auch unter den Namen «menuPass», «CVNX», «StonePanda» und «POTASSIUM» bekannt, welche seit mindestens 2016 wichtige «Managed IT Service Provider (MSP) » weltweit angegriffen haben soll (siehe auch MELANI Halbjahresbericht 2017/1, Kap. 5.1.1[32]). In der öffentlichen Publikation des DoJ werden Ziele in 12 Ländern genannt, darunter auch in der Schweiz.

MSP sind ein attraktives Ziel, da sie grosse Firmen beim Betreuen ihrer IKT-Infrastruktur unterstützen und direkte Zugriffsrechte auf Systeme und Daten ihrer Kunden haben. So waren MSP in dieser Kampagne auch nicht das eigentliche Ziel, sondern dienten dazu, sich Zugang zu Netzwerken in zahlreichen grossen Unternehmen zu verschaffen. Allerdings wählte die Gruppe diesen Weg erst seit 2016. Vorher wurden die Ziele direkt angegriffen. Die Gruppe ist bereits seit 2006 aktiv und hat sich seither unbefugten Zugang zu Computernetzwerken von mehr als 45 Technologieunternehmen, dem US-Energieministerium und der NASA verschafft. Darüber hinaus sollen die Angreifer persönliche Informationen von Angehörigen des Militärs gestohlen haben, einschliesslich Sozialversicherungsnummern, E-Mail-Adressen und Gehaltsdaten von 100’000 Mitarbeitenden der US-Marine.

Das US-Department für Justiz streicht die Verflechtung der zwei Angeklagten mit dem chinesischen Ministerium für Staatssicherheit (MSS) heraus. Gleichzeitig haben die restlichen vier Mitglieder der «Five Eyes»-Staaten[33] die Aussagen der USA in Bezug auf eine Beteiligung der chinesischen Regierung an der Spionagekampagne mittels öffentlicher Stellungnahmen unterstützt. Sie erklärten, auf Möglichkeiten der öffentlichen Attribution bei Cyber-Vorfällen zurückzugreifen. Dies insbesondere, wenn das globale Wirtschaftswachstum, die nationale Sicherheit und die internationale Stabilität gefährdet seien. Ferner wurden China sowie alle anderen beteiligten Ländern aufgefordert, die Verpflichtungen der verschiedenen internationalen Übereinkommen einzuhalten.

### 5.1.2 APT 28-Entwicklungen

Über die Spionagegruppe «APT28», welche auch unter dem Namen «Sofacy» oder «Fancy Bear» bekannt ist, wird an dieser Stelle regelmässig berichtet. Es handelt sich wohl um die aktivste und bekannteste Kampagne weltweit. Auch im zweiten Halbjahr 2018 haben sich die technischen Fähigkeiten der Gruppe weiterentwickelt und sich der Funktionsumfang erweitert. Dabei sticht vor allem die Verwendung von «LoJax» einem UEFI-Rootkit ins Auge. Wie der

---

[32] MELANI Halbjahresbericht 2017/1, Kap. 5.1.1 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2017-1.html (Stand: 31. Januar 2019)

[33] USA, UK, Australien, Neuseeland, Kanada

Sicherheitsdienstleister «ESET» Ende September 2018 berichtete, wurde das Rootkit für Operationen gegen Organisationen im Balkan, sowie in Zentral- und Osteuropa eingesetzt.[34] UEFI-Rootkits sind ausgeklügelte Tools für die Vorbereitung von Cyber-Attacken. Sie sind sehr schwer aufzuspüren und sind selbst in der Lage, radikale Sicherheitsmassnahmen wie die Neuinstallation eines Betriebssystems oder einen Festplattenaustausch zu überstehen. Es war das erste Mal, dass ein UEFI-Rootkit in wirklicher Aktion entdeckt wurde.

Sofacy soll ebenfalls für eine Funktion verantwortlich sein, die die Analyse von Dokumenten in einer automatisierten Sandbox-Umgebung erschweren kann. Die Methode basiert auf der sogenannten «AutoClose»-Funktion, bei der ein Makro im Word-Dokument erst dann ausgeführt wird und Schadcode herunterlädt, wenn das Dokument vom Benutzer geschlossen wird. Bei der automatischen Analyse bleiben die Dokumente in der Regel zwar über eine bestimmte Zeitdauer offen und werden auf ihr Verhalten geprüft, geschlossen werden sie allerdings nicht. Da der Schadcode erst zum Zeitpunkt des Schliessens von einem externen Server heruntergeladen werden muss und nicht im Word-Dokument implementiert ist, ist ein erfolgreicher Angriff nur dann möglich, wenn dieser Server auch wirklich zu diesem Zeitpunkt online ist, ansonsten wird kein Schaden angerichtet. Die Kampagne richtete sich an mehrere Regierungsstellen auf der ganzen Welt. In einem Fall wurde auf den Absturz einer «Lion-Air» Maschine vom 29. Oktober 2018 Bezug genommen und der Dateiname «crash list (Lion Air Boeing 737).docx.» verwendet.

Über die Verwendung der Schadsoftware «Zebrocy» durch Sofacy haben wir im letzten Halbjahresbericht berichtet. Zebrocy ist eine Sammlung von Downloadern, Droppern und Hintertüren. Downloader und Dropper dienen dabei der Aufklärung, die Hintertüren sichern den persistenten Zugriff der Spionageaktivitäten. In der Berichtsperiode wurden neue Komponenten eingesetzt und Zebrocy erlebte einen Aufschwung. Die neuen Komponenten nutzen beispielsweise Protokolle der Mail-Dienste SMTP und POP3, um gestohlene Daten aus dem Netzwerk des Opfers herauszubringen. Im Dezember 2018 berichtete zudem das Sicherheitsunternehmen «PaloAlto»[35], dass eine neue Zebrocy-Variante mit den praktisch gleichen Funktionen aufgetaucht sei, aber in der für Sofacy neuen Programmiersprache «Go» geschrieben wurde. Bislang wurden Varianten in «AutoIt», «Delphi», «VB.NET», «C#» und «Visual C++» gesichtet. Der Hintergrund ist nicht klar. Es wird vermutet, dass die Vielfalt der Programmiersprachen die Detektion erschweren soll.

### 5.1.3 Gezielter Angriff auf italienische Marine- und Rüstungsindustrie?

Zwischen dem 9. und 15. Oktober 2018 wurden E-Mails mit einem präparierten Excel-Dokument gezielt an Mitarbeitende der italienischen Marine- und Rüstungsindustrie gesendet.[36] Gemäss der italienischen Sicherheitsfirma «Yoroi» ging es in den E-Mails um eine Anfrage zu Ersatzteilen für Schiffsmotoren. Der Angreifer bat darin, ein Angebot für die in der Excel-Datei enthaltenen Artikel zu unterbreiten. Der Empfänger war also gezwungen, die Excel-Datei öffnen. Die Angreifer scheinen im Vorfeld gut recherchiert zu haben, um die Anfrage so echt wie möglich aussehen zu lassen. So ging die Anfrage an die richtige Stelle und auch die Sprache war klar und korrekt. Nach dem Öffnen der Datei wurde das Fernzugriffstool «QuasarRAT»

---

34 https://www.welivesecurity.com/2018/09/27/lojax-first-uefi-rootkit-found-wild-courtesy-sednit-group/ (Stand: 31. Januar 2019)

35 https://unit42.paloaltonetworks.com/sofacy-creates-new-go-variant-of-zebrocy-tool/ (Stand: 31. Januar 2019)

36 https://securityaffairs.co/wordpress/77195/malware/martymcfly-malware-cyber-espionage.html (Stand: 31. Januar 2019)

auf das System des Opfers heruntergeladen. Mit diesem Tool hatten die Angreifer vollen Zugriff auf das System und waren in der Lage, Daten zu stehlen und Manipulationen am Computer durchzuführen. Der Quellcode von QuasarRAT ist publik und auf dem Online-Dienst «GitHub» verfügbar. Während Yoroi davon ausgeht, dass ein staatlicher Akteur hinter den Angriffen steckt, tendiert das Softwareunternehmen «Kaspersky» in seiner Analyse eher zu einem kriminellen Hintergrund. Laut Kaspersky hat die Kampagne ein grösseres Ausmass und die Dokumente wurden unter verschiedenen Namen an Unternehmen in vielen verschiedenen Ländern verschickt, darunter Deutschland, Spanien, Bulgarien, Indien und Rumänien[37].

## 5.2 Industrielle Kontrollsysteme

Gezielte Angriffe gegen Prozesssteuerungen mit grossem Ausmass blieben in der Berichtsperiode weitgehend aus. Das heisst aber nicht, dass die Gruppierungen, die sich in der Vergangenheit mit solchen Angriffen profiliert haben, ihre Aktivitäten aufgegeben hätten. So beschuldigten ukrainische Sicherheitsdienste den russischen Militärgeheimdienst «GRU», eine Wasseraufbereitungsanalage mit der Malware «VPNFilter» angegriffen zu haben[38]. Zudem traten neue Gruppierungen im Umfeld von industrieller Kontrollsysteme in Erscheinung. Die USA, Europa, der mittlere Osten und Ost-Asien beobachteten verschiedene Aktivitäten. Sicherheitsdienstleister[39] führen diese unter den Bezeichnungen «RASPITE»[40] oder «Leafminer»[41]. Auf drei weitere Beispiele von andauernden vorbereitenden Aufklärungsversuchen gehen wir in den folgenden Unterkapiteln detaillierter ein.

### 5.2.1 GreyEnergy: Weiterentwicklung der Werkzeuge einer der aggressivsten Bedrohungen im Sektor Energie

Die Schadsoftware «BlackEnergy» machte nach Weihnachten 2015 Schlagzeilen: Angreifer drangen auf Bedienstationen der Steuerungssysteme mehrerer ukrainischer Stromversorger vor und verursachten einen mehrstündigen Stromausfall in der Region mit über 220'000 Betroffenen[42].

Der slowakische Sicherheitsdienstleister «ESET» beobachtete seither ein weiteres Schadsoftware-Framework. Angelehnt an den zuvor erwähnten Vorfall bezeichnete ESET dieses als «GreyEnergy»[43]. In den vergangenen drei Jahren wurde die Malware-Familie gemäss ESET gegen mehrere Ziele in der Ukraine und Polen eingesetzt. Neben der Feststellung, dass das Verschwinden der BlackEnergy-Schadsoftware mit dem Auftauchen von GreyEnergy einher-

---

37 https://ics-cert.kaspersky.com/news/2018/10/22/yoroi/ (Stand: 31. Januar 2019)

38 https://www.theregister.co.uk/2018/07/13/ukraine_vpnfilter_attack/ (Stand: 31. Januar 2019)

39 https://ics-cert.kaspersky.com/news/2018/08/06/raspite/ (Stand: 31. Januar 2019)

40 https://dragos.com/resource/raspite/ (Stand: 31. Januar 2019)

41 https://www.symantec.com/blogs/threat-intelligence/leafminer-espionage-middle-east (Stand: 31. Januar 2019)

42 MELANI Halbjahresbericht 2/2015, Kapitel 5.3.1, 26.04.2016 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2-2015.html (Stand: 31. Januar 2019)

43 https://www.welivesecurity.com/2018/10/17/greyenergy-updated-arsenal-dangerous-threat-actors/ (Stand: 31. Januar 2019)

geht, sieht ESET die Verbindung vorwiegend in derselben modularen Architektur, der Durchführung der Angriffe und der ähnlichen Auswahl der Ziele. Bisher wurde kein spezifisches Modul für Industrielle Kontrollsysteme in der GreyEnergy-Familie entdeckt. Die Angreifer wurden aber dabei beobachtet, wie sie strategisch gezielt Arbeitsstationen mit darauf betriebenen Steuerungssystemen ins Visier nahmen.

Neben dem grundlegend moderneren Aufbau von GreyEnergy gegenüber dem mutmasslichen Vorgänger, ist der Einsatz von Zertifikaten des taiwanesischen Herstellers von industrieller und IoT-Hardware «Advantech» bemerkenswert. Diese höchstwahrscheinlich gestohlenen Zertifikate wurden verwendet, um die eigene Malware vertrauenswürdig zu signieren und so die Erfolgschancen einer Infektion zu erhöhen. Eine Vorgehensweise, die auch bei «Stuxnet», der ersten bekannten Malware gegen industrielle Prozesse[44], angewendet wurde.

GreyEnergy zeigt, dass Angreifer weiterhin Aufklärungsversuche gegen Betreiber kritischer Infrastrukturen durchführen. Wie 2015 gezeigt hat, sind sie auch bereit, im für sie günstigen Moment, den Schritt von der Aufklärungsarbeit hin zur Sabotage zu machen.

### 5.2.2 Shamoon vernichtet Daten und Konfigurationen – Infrastrukturausfall bei Saipem

«300-400 Server und ungefähr 100 persönliche Arbeitsstationen wurden durch einen Angriff für einige Zeit unbrauchbar», präzisierte Mauro Piasere, der Leiter «Digitales und Innovation» des italienischen Erdöldienstleisters «Saipem» gegenüber «Reuters»[45]. Dies nachdem die Firma am 10. Dezember 2018 per Medienmitteilung[46] einen Cyber-Angriff vermeldet hatte. Am 12. Dezember aktualisierte Saipem die Mitteilung[47] und gab bekannt, dass Server im mittleren Osten, Indien, Schottland und zu einem eingeschränkten Teil in Italien der «Shamoon»-Malware zum Opfer gefallen waren. Die befallenen Systeme konnten durch Einsatz von Backup-Infrastruktur schrittweise wiederhergestellt werden.

In dieser Zeit analysierte das Sicherheitsunternehmen «Chronicle» eine neue Variante[48] der Shamoon-Malware, welche von einer italienischen IP-Adresse auf die öffentliche Analyseplattform «Virustotal» hochgeladen worden war. Shamoon wurde 2012 durch einen Angriff auf «Saudi Aramco» bekannt, bei welchem Daten auf 35'000 Systemen vernichtet worden waren. Vier Jahre später traf eine neue Welle der Malware dieselbe Region. Die aktualisierte Malware-Version zeichnet sich durch die zusätzliche Fähigkeit aus, Dateien und den «Master Boot Record (MBR)», einen Teil der Festplatte der zum Starten des Systems notwendig ist, mit zufälligen Daten zu überschreiben. Saudi Aramco ist einer der grössten Kunden von Saipem, was den Verdacht erhärtet, dass es eine Verbindung zu früheren Shamoon-Vorfällen gibt. Ob die

---

44 https://www.welivesecurity.com/2010/07/19/win32stuxnet-signed-binaries/ (Stand: 31. Januar 2019)

45 https://www.reuters.com/article/us-cyber-shamoon/saipem-says-shamoon-variant-crippled-hundreds-of-computers-idUSKBN1OB2FA (Stand: 31. Januar 2019)

46 http://www.saipem.com/sites/SAIPEM_en_IT/con-side-dx/Press%20releases/2018/Cyber%20attack.page (Stand: 31. Januar 2019)

47 http://www.saipem.com/sites/SAIPEM_en_IT/con-side-dx/Press%20releases/2018/Cyber%20attack%20update.page (Stand: 31. Januar 2019)

48 https://www.bleepingcomputer.com/news/security/shamoon-disk-wiping-malware-re-emerges-with-a-third-variant/ (Stand: 31. Januar 2019)

durch Chronicle und Palo Alto Networks[49] analysierte Malware-Variante wirklich beim Angriff auf Saipem zum Einsatz gekommen ist, ist nicht bekannt.

### 5.2.3 Drohnen am Flughafen

Drohnen gibt es in vielen Formen, Grössen und Funktionen. Diese starten beim einfachen Spielzeug, gehen über zu Drohnen für Lieferdienste und enden im militärischen Bereich. Klar ist, dass sich Anzahl und Möglichkeiten in den nächsten Jahren vervielfachen werden. Was Drohnen bewirken können, zeigt der Vorfall rund um den englischen Flughafen «Gatwick»: Genau zu Beginn der Weihnachtsferien, am 19. Dezember 2018, haben Unbekannte mit Drohnen den Flugbetrieb auf dem Flughafen für 36 Stunden lahmgelegt. Insgesamt wurden über 200 Drohnensichtungen gemeldet. Der Polizei und auch dem aufgebotenen Militär war es nicht gelungen, in dieser Zeit die Täterschaft zu finden und den Drohnenflug zu unterbinden. Die für die Zwischenfälle bei Gatwick verantwortlichen Täter wurden bis heute nicht gefasst. Kleinere Drohnenzwischenfälle gibt es weltweit mittlerweile regelmässig. Am 12. Dezember 2018 landete eine «Boeing» der mexikanischen Fluggesellschaft «Aeromexico» mit aufgerissener Nase, nachdem sie vermutlich mit einer Drohne zusammengestossen war. Zwar gab es in all diesen Fällen keine Hinweise auf kompromittierte Systeme, trotzdem steigt die Gefahr solcher Vorfälle.

Beurteilung:

Aus den Vorfällen hat die britische Regierung Konsequenzen gezogen und den Schutz vor Drohnen verschärft. In der Schweiz benötigt man für den Betrieb von Drohnen und Flugmodellen mit einem Gewicht von über 30 Kilogramm eine Bewilligung des Bundesamtes für Zivilluftfahrt (BAZL). Die Vorgaben für den Betrieb von Drohnen und Flugmodellen bis zu einem Gewicht von 30 Kilogramm sind in der «Verordnung des UVEK über Luftfahrzeuge besonderer Kategorien» geregelt. So ist beispielsweise der Betrieb einer Drohne im Umkreis von 5km rund um Flugplätze und Heliports ohne Bewilligung nicht gestattet. Diese Regeln schützen aber nicht vor mutwilligen Aktionen oder wenn eine Drohne von einer Drittperson gehackt und übernommen werden kann.

## 5.3 Angriffe (DDoS, Defacements, Drive-By usw.)

### 5.3.1 Digitales Skimming – Prominente Opfer

Im August 2018 gelang es Hackern, die Daten von mehr als 380’000 Kunden der Britischen Fluggesellschaft «British Airways» zu stehlen. Darunter befanden sich nicht nur Namen, Post- und E-Mail-Adressen, sondern auch Kreditkarten- und Kontodaten. Was auf den ersten Blick wie ein weiterer Angriff auf eine Datenbank aussah, entpuppte sich als eine Manipulation der Webseite und der App von British Airways. Dabei setzten die Angreifer sogenanntes digitales Skimming ein. Beim klassischen Skimming wird ein Lesegerät durch Kriminelle in einem Geldautomaten so platziert, dass der Magnetstreifen der Geldkarte gelesen und gespeichert wird. Beim digitalen Skimming wird ebenfalls versucht die Kreditkartennummer und deren Sicherheitsmerkmale abzufangen, allerdings nicht bei einem Geldautomaten, sondern beim Zah-

[49] https://unit42.paloaltonetworks.com/shamoon-3-targets-oil-gas-organization/ (Stand: 31. Januar 2019)

lungsprozess auf einem Webshop. So wurden bei British Airways nur die Kundendaten gestohlen, die bei der Buchung eines Tickets zwischen dem 21. August und dem 5. September 2018 in das Bezahlformular eingegeben worden waren. Die Daten zum Flug und dem Reiseziel waren von dem Hack nicht betroffen.

Ein weiterer Fall wurde am 23 Juni 2018 entdeckt: Die britische Ticketverkaufsstelle «Ticketmaster» identifizierte eine Malware, die einem unbekannten Dritten seit Februar 2018 Zugriff auf Kundennamen, E-Mail-Adressen, Telefonnummern, Zahlungsdaten und Login-Informationen ermöglicht hatte.

Auch die Zahlungsseite des Britischen Online-Händlers «Newegg» war von dieser Vorgehensweise betroffen. Hier schleusten Hacker am 14. August 2018 15 Zeilen des Schadcode in die Webseite ein. Dieser Schadcode blieb bis zum 18. September 2018, also mehr als einen Monat, unentdeckt. Der installierte Schadcode sendete die Kreditkartendaten von Kunden an einen Server, der von den Angreifern kontrolliert wurde.

E-Commerce Seiten stehen schon seit den Anfängen des Internets im Fokus von Angreifern. Der Grund ist relativ einfach: Wenn ein Angreifer an gültige Kreditkartendaten kommen will, ist er bei Webshops goldrichtig. Bereits im Jahr 2000 ermöglichte die Entdeckung einer Schwachstelle in der damals weit verbreiteten Webshop-Software «Cart32» für Microsoft Server den Angreifern Administratorzugang auf die Anwendung. Sie konnten damit Kreditkartendaten auslesen und Befehle auf dem Hosting-Server ausführen. Im Jahr 2011 standen vor allem Schwachstellen der Software «OSCommerce» im Interesse der Kriminellen. Auch in der Schweiz gab es damals zahlreiche Fälle von kompromittierten Webseiten, was MELANI zu einer Warnung veranlasste[50]

Seit März 2016 beobachtet der Sicherheitsdienstleister «RiskIQ» die verschiedenen Kampagnen mit immer wieder neuen Angriffs-Infrastrukturen,[51] und fasst diese unter dem Oberbegriff «Magecart» zusammenfasst. Dahinter verstecken sich mindestens sieben Gruppen, welche digitale Kreditkarten-Skimmer auf kompromittierten E-Commerce-Websites einschleusen. Ausgenutzt werden vor allem Schwachstellen in den Erweiterungen, sogenannten Extensions, der Software «Magento». Diese Onlineshop-Software wurde 2008 als Open-Source-E-Commerce-Plattform veröffentlicht. Der niederländische Sicherheitsexperte, Willem de Groot, identifizierte in mindestens zwei Magento-Extensions Zero-Day-Schwachstellen und bat um Hilfe, auch die restlichen 18 Extensions nach Schwachstellen zu durchsuchen. Aber auch die Webshop Software «Powerfront CMS» und «OpenCart» stehen im Interesse dieser Angreifer.[52]

### 5.3.2 Risiken in Zusammenhang mit VPN: Beispiel VPN von «Hola»

Ein virtuelles privates Netzwerk (Virtual Private Network, VPN) ist ein verschlüsselter Kommunikationskanal, der eine Verbindung zwischen zwei entfernten Computern über das Internet ermöglicht. Für viele Benutzer bedeutet die Verwendung eines VPN grössere Sicherheit ihrer Online-Tätigkeiten. Es sind aber nicht alle VPN-Dienste von gleicher Qualität. Die Benutzer müssen sich vergewissern, dass ihr VPN vertrauenswürdig ist und die Sicherheitsstandards erfüllt. Auch VPN-Dienstleister können angegriffen werden, wie es im vergangenen Juli der

50 https://www.computerworld.ch/business/politik/melani-warnt-schweizer-webshop-betreiber-1321089.html (Stand: 31. Januar 2019)

51 https://www.riskiq.com/blog/external-threat-management/inside-magecart/ (Stand: 31. Januar 2019)

52 https://www.riskiq.com/blog/labs/magecart-keylogger-injection/ (Stand: 31. Januar 2019)

Fall gewesen ist. Nutzer der beliebten Schnittstelle «MyEtherWallet (MEW)» zur Verwaltung des Ethereum-Kryptowährung-Portfolios wurden über das Risiko bei der Verwendung der VPN-Chrome-Erweiterung der Firma «Hola» informiert. «Hola» sei am 9. Juli während fünf Stunden kompromittiert gewesen. Wer in dieser Zeit auf die MEW-Dienste zugegriffen habe, habe sich der Gefahr des Diebstahls seines Kryptogeldes ausgesetzt. «Hola» bestätigte in einer Medienmitteilung den Vorfall und erklärte, ihr Firmenkonto im Google-Chrome-Store sei kompromittiert worden. Den Benutzern sei nach der Verbindung mit ihrem MEW-Konto eine modifizierte Version der Chrome-Erweiterung zur Installation vorgeschlagen worden, die dann die Zugangsdaten abgefangen habe. «Hola» hat die betrügerische Erweiterung entfernt und das Konto gesichert.

Empfehlung:


Empfehlungen von MELANI im Umgang mit der Nutzung von VPN.

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

### 5.3.3 Angriff auf Banken über physischen Netzzugang

Im Dezember hat die Sicherheitsfirma «Kaspersky» die Ergebnisse einer Reihe von Cyber-Vorfällen gegen verschiedene osteuropäische Banken veröffentlicht. Besonders interessant ist dabei der Eintrittspunkt, denn die Täter schlossen ihre Geräte direkt an das Netzwerk der Bank an. Anders als bei den zahlreichen Angriffen, die aus der Ferne stattfinden, haben sich die Täter hier physisch Zutritt zum Unternehmen verschafft, indem sie sich beispielsweise als Stellensuchende oder Lieferanten ausgaben. Vor Ort schlossen sie ihre Geräte direkt an das Netzwerk an, je nach Gegebenheit mit einem kleinen Laptop, einem Raspberry Pi oder einem Bash Bunny Nanocomputer via USB-Anschluss. Über diesen ersten Zugang wurden Identifikatoren und Arbeitsplätze ausgespäht, aus welchen Zahlungen getätigt wurden. Anschliessend wurde versucht, auf diese Arbeitsplätze einen dauerhaften Fernzugriff einzurichten.

Diese Angriffsart erinnert daran, wie wichtig eine umfassende Sicherheitsstrategie ist, zu der neben technischen auch physische und organisatorische Massnahmen gehören. Zentral ist in diesem Zusammenhang die Zutrittskontrolle zu den Räumlichkeiten. Netzeintrittspunkte (Geräte, Ethernet-Ports) müssen dokumentiert, überwacht und bei Nichtbenutzung allenfalls deaktiviert werden.

### 5.3.4 «Lazarus» – ungebrochene Angriffsversuche

Die «Lazarus»-Gruppe wird von zahlreichen Experten mit dem nordkoreanischen Regime in Verbindung gebracht und soll in den vergangenen Jahren verschiedene Angriffe auf Banken durchgeführt haben. Das bekannteste Beispiel war der Angriff auf die Nationalbank von Bangladesch im Jahre 2016. Auch bei einem Vorfall Ende Dezember 2018 bei der chilenischen «Redbanc» wurde «Lazarus» als möglicher Urheber genannt. Laut der Firma «Flashpoint» gehört die beim Angriff verwendete Malware «PowerRatankba» zum Instrumentarium von «Lazarus». Besonders interessant war die Methode, um den Schadcode in das Netzwerk der Banken zu bringen. Die Angreifer gaben sich zu diesem Zweck als Personalfirma aus. Sie kontaktierten einen Bankmitarbeiter über die sozialen Netzwerke und boten ihm ein Vorstellungsge-

spräch via «Skype» an. Beim Gespräch wurde der Bewerber gebeten ein Formular herunterzuladen, das für den Rekrutierungsprozess benötigt werde – in Wirklichkeit handelte es sich allerdings um eine ausführbare Datei («.exe»), die eine Malware aktivierte. Nach den vorliegenden Informationen wurde der Vorfall rechtzeitig erkannt, sodass er keine Auswirkungen auf die Infrastruktur oder die Tätigkeiten der Bank hatte.

Bereits im Oktober hat das Computer Emergency Response Team «US-CERT» über die Gruppe «Hidden Cobra» informiert. Seit 2016 hatte die Gruppe mit der Kampagne «FastCash» asiatische und afrikanische Banken ins Visier genommen, um an Geldautomaten hohe Summen auf einmal freizugeben, die dann von einem Komplizen abgeholt wurden. Bei einem Vorfall 2017 wurden solche Abhebungen in mehr als 30 Ländern gleichzeitig gemeldet. Laut einigen Experten soll «Lazarus» hinter «Hidden Cobra» stecken. Gemäss «Symantec» werden die für die Automaten zuständigen Server nach der Kompromittierung von einem Trojaner («Trojan.Fastcash») infiziert. Der Trojaner gibt anschliessend die betrügerischen Transaktionen in Auftrag.

Inzwischen ist bekannt, dass «Lazarus» grosses Interesse am Kryptogeldmarkt hat und darin eine Möglichkeit zur Diversifizierung seiner Einnahmequellen sieht. Gemäss einer «Kaspersky»-Analyse vom August 2018 ist die Gruppe für einen Angriff auf eine asiatische Kryptowährungsplattform verantwortlich. Eintrittspunkt war dabei eine von einem Mitarbeiter heruntergeladene Trading-Anwendung eines Drittanbieters. Der Schadcode wurde über ein Update installiert. Das Besondere an diesem Fall ist, dass verschiedene Versionen für verschiedene Betriebssysteme zur Verfügung gestellt wurden. Bislang hatte es «Lazarus» meist auf Windows-Systeme abgesehen. Nun tauchte erstmals auch Malware für das Mac OS-System auf.

### 5.3.5 Ransomware

Wenn von Verschlüsselungsschadsoftware, sogenannter Ransomware, gesprochen wird, denkt man zuallererst an zerstörte Daten und an das Backup, das hoffentlich funktionieren wird. Was in der Vorsorgeplanung aber nicht vergessen werden sollte, ist der Produktionsausfall, den eine solche Malware mit sich bringt, bis das Backup wieder eingespielt ist und alle Systeme wieder einwandfrei funktionieren. Dies ist besonders gravierend, wenn ganze Produktionsanlagen von solchen Attacken betroffen sind. Zahlreiche solche Fälle machten im Berichtshalbjahr Schlagzeilen.

Im August 2018 wurde der taiwanesische Chip-Hersteller «TSMC» (Taiwan Semiconductor Manufacturing Company) angegriffen. Auch in diesem Fall musste die Firma aufgrund der eingesetzten Verschlüsselungsschadsoftware die Produktion in mehreren Fabriken stilllegen. TSMC ist der weltweit grösste Hersteller von Halbleitern und Prozessoren und insbesondere Zulieferer von «Apple»'s iPhone. Als Ursache wurde eine Variante der Schadsoftware «WannaCry» identifiziert. WannaCry machte im Mai 2017 Schlagzeilen und hatte weltweit grosse Auswirkungen. Die für die Ausbreitung dieser Schadsoftware verantwortliche Windows-Schwachstelle im SMB-Protokoll wurde zwar bereits im März 2017 geschlossen. Gerade bei Steuersystemen ist es aber zum Teil schwierig, ein zeitnahes Patchmanagement durchzuführen. So liefen die betroffenen Computer der «Material-Handling-Systeme» auf ungepatchten Windows 7 Systemen. Eingeschleust wurde die Schadsoftware über ein neu zu installierendes Softwaretool, bei dem versäumt worden war, einen Virencheck durchzuführen.

Zwei Häfen hatten in der zweiten Jahreshälfte 2018 mit Cyber-Angriffen zu kämpfen: Der Hafen von Barcelona beklagte am 20. September 2018 einen Angriff mit Ransomware auf die Sicherheitsinfrastruktur des Hafens. Um was für eine Art von Ransomware es sich gehandelt

hat, ist nicht bekannt. Der Schiffsbetrieb konnte aufrecht erhalten werden, da es für solche Ereignisse eine Vorsorgeplanung gibt. Eine Woche später, am 27. September 2018, war der Hafen von San Diego durch eine Ransomware beeinträchtigt. Auch hier blieb der Hafen mit seinen Dienstleistungen offen und die Mitarbeitenden konnten weiter arbeiten. Gewisse Funktionen und Zugriffe auf Daten waren jedoch eingeschränkt.

Am 21. November 2018 hatte die deutsche Maschinenbaufirma «KraussMaffei» mit den Folgen eines Ransomware-Angriffs auf Computer zu kämpfen. KraussMaffei zählt weltweit zu den grössten Anbietern von Maschinen zur Kunststoff- und Gummiherstellung. Durch den Angriff konnten Maschinen, die für die Steuerung einzelner Prozesse in der Fertigung und Montage notwendig sind, zu Beginn der Attacke nicht gestartet werden. Gemäss mehreren Berichten musste in der Folge die Produktion gedrosselt werden. Mit dem Backup konnte KraussMaffei wichtige Computer zwar wieder zum Laufen bringen, dennoch wird das Unternehmen wohl noch lange mit den Auswirkungen zu kämpfen haben. Ein Sprecher bestätigte im Januar 2019, dass erst drei Viertel der betriebsrelevanten Systeme wieder normal laufen würden.[53] Über die Art der Ransomware wurden keine Informationen bekannt gegeben, ebenfalls wurde nicht über die Höhe der Lösegeldforderung berichtet und ob Lösegeldzahlungen geleistet wurden.

Beurteilung /Empfehlung

Ein besonders beliebtes Einfallstor für Schadsoftware sind die Personalabteilungen von Unternehmen. Bewerbungen beinhalten in der Regel Dokumente aller Art, die geöffnet werden müssen. Im zweiten Halbjahr 2018 tauchte diese Angriffsart vermehrt im Bereich Ransomware auf. Aber auch Firmenveranstaltungen oder Pressemitteilungen sind Möglichkeiten um Schadsoftware zu verbreiten.

Mittlerweile haben Cyber-Kriminelle auch Angriffe auf Mobilgeräte als lohnendes Geschäft entdeckt. Dementsprechend nehmen mobile Ransomware-Attacken weiter zu. Am häufigsten tritt auf Android- und anderen Mobilgeräten die Variante der «Locker»-Ransomware auf. Anstatt Dateien zu verschlüsseln, sperrt die Schadsoftware das ganze Gerät. Mit der steigenden Masse an IoT-Geräten wird sich wohl ein weiteres Geschäftsfeld für die Kriminellen öffnen.

Eine entscheidende Massnahme, wie sich Industrieunternehmen vor Cyber-Angriffen schützen können, ist das Trennen der operationalen Netze von den IT-Netzen. Selbst wenn die Office-IT angegriffen wird, laufen die Maschinen problemlos weiter. Zwecks Usability sind die Netze allerdings häufig direkt miteinander verbunden, beispielsweise um Befehle einfach an Maschinen zu senden.

## 5.4 Datenabflüsse

### 5.4.1 Plattform «Ariane» des französischen Aussenministeriums gehackt

Am 13. Dezember 2018 gab das französisches Aussenministerium bekannt, dass seine Plattform «Ariane» gehackt worden war und dabei auch Personendaten betroffen waren. «Ariane»

[53] https://www.zeit.de/2019/03/datenschutz-cyberangriffe-unternehmen-digitalisierung-risiken-datendiebstahl-hacker (Stand: 31. Januar 2019)

ist ein Online-Dienst, der 2010 ins Leben gerufen worden ist. Französische Staatsangehörige, die einen Auslandsaufenthalt planen, können sich für Sicherheitsempfehlungen über das jeweilige Land registrieren. Bei Bedarf werden die registrierten Personen und die angegebenen Kontaktpersonen direkt kontaktiert. Der Datenabfluss umfasste Namen, Vornamen, Adresse, Telefonnummer und E-Mail dieser Kontaktpersonen. Besonders schützenswerte Daten waren laut «Aussenministerium» nicht darunter. Die gestohlenen Daten könnten aber beispielsweise für gezielte E-Mails oder Betrugsversuche verwendet werden. Die Betroffenen, darunter auch Schweizerinnen und Schweizer, wurden per E-Mail über den Vorfall informiert. Manchen Empfängern war jedoch nicht bewusst, dass ihre Daten auf dieser Plattform gespeichert waren und dachten, es handle sich bei der Mail um eine Phishing-Mail.

### 5.4.2 Lücke bei der «View-as»-Funktion von Facebook

Am 28. September 2018 gab Facebook Details zu seinem vielleicht bislang grössten Sicherheitsvorfall bekannt. Die Lücke betraf die Funktion «View as», welche das eigene Profil so anzeigt, wie es für andere sichtbar ist. Aus Sicherheitsgründen wurden alle 50 Millionen betroffenen Nutzer abgemeldet und mussten ein neues Passwort wählen und sich neu anmelden, bei weiteren 40 Millionen Nutzern wurde die Massnahme vorsorglich ergriffen. Der Dienst «View as» wurde abgestellt. Die Angreifer hätten über die identifizierte Schwachstelle das Token übernehmen können, mit dem Benutzer mit ihrem Konto verbunden bleiben. Potenzielle Angreifer hätten so vollen Zugriff auf das Konto und auf jeden anderen Dienst erhalten können, bei dem Facebook als Identifikationskonto verwendet wird. Es ist mittlerweile verbreitete Praxis, einen als sicher geltenden Dienst für die Identifikation anderer Dienste zu verwenden. Nutzer bringen dadurch ihre Identität bereits mit und müssen sich folglich keine neue bei einem Internetdienstleister anlegen. Dass diese Praxis auch ein Sicherheitsrisiko sein kann, zeigt dieser Vorfall deutlich.

### 5.4.3 Abfluss von Gesundheitsdaten in Singapur

Im Juli wurden Details zu einem massiven Angriff auf den Gesundheitssektor Singapurs bekannt. Es wurden Personendaten von 1,5 Millionen Menschen gestohlen, die zwischen Anfang Mai und Anfang Juli 2018 Patienten der grössten Gesundheitsgruppe des Landes «SingHealth» waren. Von 150 000 Patienten wurden zusätzlich Daten von Arztrezepten entwendet, darunter dasjenige von Premierminister Lee Hsien Loong, auf die es die Täterschaft nach Angaben der Behörden gezielt abgesehen hatten.

### 5.4.4 Lücke beim Online-Portal «Movistar»

Im Juli 2018 deckte die spanische Konsumentenorganisation FACUA eine grössere Lücke beim spanischen Telekomunternehmen «Telefonica» auf. Aufgrund eines Programmierfehlers im Online-Portal konnten Kunden mit einem «Movistar»-Konto auf die Namen, Adressen und Telefonnummern aller anderen «Movistar-Kunden» zugreifen. «Telefonica» hat den Fehler korrigiert, konnte aber keine Angaben darüber machen, ob bereits Personendaten abgeflossen waren.

### 5.4.5 Hotelkette «Starwood» über Jahre Opfer eines Datenlecks

Am 30. November 2018 gab das Hotelunternehmen «Marriott» bekannt, dass Unbefugte Zugriff auf Daten von 500 Millionen Hotelgästen ihrer Tochterunternehmung «Starwood» hatten. Die Zahl wurde im Januar nach unten korrigiert und es war noch die Rede von maximal 383 Millionen Registrierungen. Neben Personendaten wie Adressen und Telefonnummern

sind in einigen Fällen auch heiklere Daten, wie Passnummern und Kreditkartendaten abgeflossen. Die Kreditkartendaten und teilweise auch die Passnummern waren zwar verschlüsselt abgespeichert. «Marriott» kann aber nicht ausschliessen, dass die Angreifer in den Besitz der entsprechenden Schlüssel gelangt sein könnten. Die Angreifer sollen seit 2014 bis zur Entdeckung des Vorfalls im September 2018 Zugriff auf die Daten gehabt haben.

Zum Hotelunternehmen «Starwood» gehören über 1'200 Hotels in fast 100 Ländern. Das im November 2018 gemeldete Leck ist sowohl aufgrund der Anzahl Betroffener und der Dauer des unbefugten Zugriffs als auch bezüglich der gestohlenen Daten bemerkenswert. Personendaten, Kreditkartendaten und Passnummern bieten Möglichkeiten für Betrug oder Identitätsdiebstahl. Es ist aber auch denkbar, dass Spionagedienste daran interessiert sein könnten, wann sich gewisse Personen in welchem Hotel aufhalten. In der Vergangenheit waren Hotels mehrfach Ziel ausgeklügelter Cyber-Spionagekampagnen. MELANI hat bereits 2014 bei der Kampagne «Darkhotel» auf diese Möglichkeit aufmerksam gemacht.[54] Damals wurden die Drahtlosnetzwerke grosser Hotels angegriffen, um Geschäftsleute auszuspionieren. Durch das Leck bei «Starwood» wurden diese Informationen den Angreifern möglicherweise auf dem Silbertablett serviert. Auch wenn der Auftraggeber und der genaue Zweck des «Starwood»-Angriffs nicht bekannt sind, ist nicht auszuschliessen, dass die Informationen zur Vorbereitung eines Cyber- oder physischen Spionageangriffs hätten dienen können. Dabei kann ein Angreifer die Informationen durchaus von einem anderen Akteur erworben haben.

## 5.5 Präventive Massnahmen

### 5.5.1 Kampf gegen Computer-Support-Betrüger

Wenn das Telefon unerwartet klingelt und sich am anderen Ende der Leitung ein «Microsoft»-Mitarbeiter meldet, dürfte es sich um einen Betrüger handeln. Auch hinter beim Surfen plötzlich aufpoppenden Meldungen, in welchen behauptet wird, dass der Computer gefährdet oder sogar infiziert sei und man eine Nummer anrufen solle, stecken Betrüger. Mit dieser Masche versuchen die Täter, sich Fernzugang zu Computern zu verschaffen und sich neben den dort gespeicherten Daten auch noch etwas Geld zu besorgen, da sie ihre «Support-Leistungen» in Rechnung stellen und erfundene Lizenzen verkaufen. Von dieser Masche sind weiterhin auch Personen in der Schweiz betroffen.[55] Die Täter fälschen beim Anrufen vielfach ihre Nummer und lassen sogar Schweizer Nummern auf dem Display der Angerufenen erscheinen. In Pop-ups angezeigte Schweizer Nummern sind typischerweise über ausländische VoIP-Anbieter vergeben worden.[56]

---

[54] MELANI Halbjahresbericht 2/2014 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2014-2.html (Stand: 31. Januar 2019)

[55] MELANI warnt seit 2011 vor dieser Masche: https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/anrufe-von-betruegern--die-sich-als-microsoft-kundenservice-ausg.html; auf Grund des anhaltenden Trends ist sie weiterhin in den «Aktuellen Gefahren» zu finden: https://www.melani.admin.ch/melani/de/home/themen/fake_support.html (Stand: 31. Januar 2019)

[56] Im Rahmen der aktuellen Teilrevision des Fernmeldegesetzes (FMG) sollen dem Staatssekretariat für Wirtschaft (SECO) Kompetenzen zur schnellen Blockierung solcher Nummern gegeben werden.

Da sich die Betrüger meistens als «Microsoft»-Mitarbeiter ausgeben und Windows nach wie vor das meistverbreitete Betriebssystem ist, hat auch Microsoft ein grosses Interesse daran, den Akteuren das Handwerk zu legen und arbeitet aktiv mit Strafverfolgungsbehörden zusammen.[57] Von gefälschtem Support betroffene Personen können eine Strafanzeige bei der lokalen Polizei erstatten sowie Microsoft direkt informieren.[58]

Während die kriminellen Auftraggeber und Infrastrukturbetreiber über die ganze Welt verteilt sind,[59] führen die Spuren der Anrufe regelmässig zu Callcentern in Indien. Im vergangenen Herbst hat die Indische Polizei 26 Callcenter in Neu Delhi durchsucht und über 60 Personen festgenommen.[60] Inwiefern diese Verhaftungen zu einer nachhaltigen Reduktion des Phänomens führen, bleibt abzuwarten. Es ist jedenfalls erfreulich, dass die internationale Strafverfolgung immer mehr Erfolge vorweisen kann und sich global agierende, organisierte Kriminelle nicht vor Ahndung ihrer Taten in Sicherheit wähnen dürfen.

### 5.5.2 Rufnummernfälschung soll eingedämmt werden

Der britische Telekommunikationsregulator «OfCom» hat per 1. Oktober 2018 überarbeitete «Allgemeine Bedingungen für Telefonanbieter» in Kraft gesetzt.[61] Darin werden die Anbieter neu verpflichtet, die Rufnummernanzeige gratis zur Verfügung zu stellen und sicherzustellen, dass die angezeigte Nummer auch tatsächlich zum Anrufenden gehört. Anrufe mit gefälschten Nummern müssen geblockt werden. Mit dieser Massnahme sollen Konsumentinnen und Konsumenten besser vor betrügerischen und vor sonst lästigen Anrufen geschützt werden.

Ob solche Vorschriften sinnvoll umgesetzt werden können, ist umstritten. In der Schweiz wird aktuell das Fernmeldegesetz teilrevidiert. In der Botschaft des Bundesrats[62] wird die Problematik der Rufnummernfälschung aufgezeigt und erklärt, dass die Einführung eines effektiven Verfahrens zur globalen Verifizierung von Anrufernummern trotz internationalen Bestrebungen viele Jahre dauern dürfte. Immerhin ist vorgesehen, die gesetzliche Pflicht von Fernmeldedienstanbieterinnen zur grundsätzlichen Bekämpfung von Spam auch auf unlautere Werbeanrufe auszudehnen. Insofern wäre die Schweiz bereit, Massnahmen auf Verordnungsebene vorzuschreiben und umzusetzen, sobald solche nach Stand der Technik möglich sind.

### 5.5.3 Koordinierte Operation gegen Voice Phishing-Akteure

Eine international aktive Gruppierung steht im Verdacht, mittels Spam-E-Mails und Telefonanrufen E-Banking-Daten erlangt und rechtswidrig verwendet zu haben (Voice Phishing). Betroffen sind auch Kunden von Finanzinstituten in der Schweiz.

---

57 https://blogs.microsoft.com/on-the-issues/2018/11/29/new-breakthroughs-in-combatting-tech-support-scams/; https://www.zdnet.com/article/after-microsoft-complaints-indian-police-arrest-tech-support-scammers-at-26-call-centers/ (Stand: 31. Januar 2019)

58 Das Meldeformular von Microsoft befindet sich hier: https://www.microsoft.com/de-ch/concern/scam

59 U.a. in Deutschland und England: https://winfuture.de/news,96690.html; https://www.t-online.de/digital/sicherheit/id_81548210/trickbetrueger-mit-microsoft-masche-verhaftet.html (Stand: 31. Januar 2019)

60 https://www.nytimes.com/2018/11/28/technology/scams-india-call-center-raids.html (Stand: 31. Januar 2019)

61 https://www.ofcom.org.uk/about-ofcom/latest/features-and-news/new-rules-protect-consumers

62 https://www.admin.ch/opc/de/federal-gazette/2017/6559.pdf, Seiten 6581 und 6596 (Stand: 31. Januar 2019)

Mittels rechtshilfeweiser Zusammenarbeit mit den Niederlanden konnten die mutmasslichen Täter identifiziert, und deren Operationsbasis im Grossraum Rotterdam lokalisiert werden. Mit Unterstützung der niederländischen Strafverfolgungsbehörden, vom Bundesamt für Polizei (fedpol) und dank der Koordination durch die EU-Justizbehörde Eurojust fand am 17. Juli 2018 in den Niederlanden eine koordinierte Operation statt. Dabei wurden zwei Personen verhaftet und Hausdurchsuchungen durchgeführt. Bezüglich der Person, welche mutmasslich für die Phishing-Anrufe in die Schweiz verantwortlich ist, wurde um Auslieferung ersucht. Die andere Person wird im Rahmen eines niederländischen Strafverfahrens verfolgt.[63]

Beurteilung:

Wie die erfolgreich koordinierte Operation in den Niederlanden zeigt, ist die strafrechtliche Verfolgung der Cyber-Kriminalität auf internationaler Ebene anzugehen.

### 5.5.4 Internet Provider kappen Verbindungen zu BGP Hijack Factory

Das Border Gateway Protocol (BGP) ist das im Internet eingesetzte Routingprotokoll und verbindet einzelne Netzwerke, so genannte autonome Systeme (AS) miteinander. Zu jedem AS gehören IP-Adressen und die Gesamtheit der AS machen das Internet aus. Unter «BGP Hijacking» (engl.: to hijack = entführen / kapern) versteht man die unberechtigte Übernahme von IP-Adressen durch Betreiber eines AS mittels Manipulation von Internet Routing-Tabellen.

Eine portugiesische Firma ist mehrfach durch solche Übernahmen aufgefallen. Sie habe die entführten IP-Adressen dann vornehmlich an Versender von Spam vermietet, da deren Adressen typischerweise schnell auf Block-Listen figurieren und sie immer wieder neue Adressen brauchen, damit ihre E-Mails zugestellt werden. Über die letzten Jahre sollen insgesamt 130 falsche Routen eingespiesen worden sein, wodurch fast 225'000 IP-Adressen unrechtmässig genutzt werden konnten. Dieser Umstand wurde auf verschiedenen Mailing-Listen thematisiert und schliesslich haben Internet Transit Provider und Internet Exchange Punkte nach gemeinsamer Absprache entschieden, alle Verbindungen zum AS dieser Firma zu kappen.[64]

Beurteilung:

Man kann sich darüber streiten, ob solches Vorgehen als Selbstregulierung oder Selbstjustiz angesehen werden soll. Im Ergebnis kann diese erste derartige Verbannung als Warnung an alle Netzbetreiber gesehen werden, sich an gewisse Regeln im Internet zu halten, auch wenn diese keine formellen und durchsetzbaren Gesetze sind. Insbesondere wer an der Basis-Infrastruktur herummanipuliert, sieht sich einer globalen Gemeinschaft gegenüber, die solche Aktionen nicht goutiert und gemeinsam Gegenmassnahmen treffen kann.

---

63 https://www.bundesanwaltschaft.ch/mpc/de/home/medien/archiv-medienmitteilungen/news-seite.msg-id-71647.html (Stand: 31. Januar 2019)

64 https://www.bleepingcomputer.com/news/security/internet-transit-providers-disconnect-infamous-bgp-hijack-factory/ (Stand: 31. Januar 2019)

# 6 Tendenzen und Ausblick

## 6.1 Manipulation und Desinformation im Informationszeitalter

Informationen können das Verhalten oder die Meinungsbildung beeinflussen, weshalb es immer wieder zu Desinformation oder zur Manipulation von Informationen kommt. Bereits im 4. Jahrhundert v. Chr. beschrieb der chinesische Philosoph «Sun Tzu» diese Methoden in seinem Buch «Kriegskunst». Unsere hypervernetzte Gesellschaft bietet enorme Möglichkeiten für das Übermitteln von Informationen. Die Kehrseite der Medaille ist die Manipulation gewisser Informationen. Im Kontext gesellschaftlicher, medialer und politischer Aufmerksamkeit verliert die Debatte manchmal an Klarheit, und es wird schwierig, zwischen Fakenews, Junknews, Propaganda, Influencing usw. zu unterscheiden. Diese Themen sind im gegenwärtigen eidgenössischen Wahljahr aktueller denn je. Wie Beispiele aus dem Ausland zeigen, ist die Debatte vor Wahlen für die Manipulation von Informationen besonders attraktiv, insbesondere in Form massiver und organisierter Verbreitung von falschen, verzerrten oder nicht für die Öffentlichkeit bestimmten (persönlichen oder geheimen) Informationen zum Schaden des politischen Gegners.

### 6.1.1 Gesellschaftlicher und technologischer Nährboden

Manipulationskampagnen beruhen auf menschlichen Merkmalen wie kognitiver Verzerrung oder falscher Wahrnehmung. In manchen aktuellen Trends finden sie einen fruchtbaren Nährboden.

Online-Medien und die sozialen Netzwerke werden für viele Menschen immer mehr zur wichtigsten Informationsquelle.[65] Jede und jeder kann selbst Nachrichten verbreiten, ohne sich um journalistische Qualitätsstandards kümmern zu müssen. Über die sozialen Netzwerke lassen sich spezifische Gruppen ansprechen. Man kann eine Botschaft gezielt an einen Teil der Bevölkerung senden, von dem man weiss, dass er dafür empfänglich ist. Die sozialen Netzwerke und das Internet sind nicht nur ein Vorteil in Bezug auf gezielte Botschaften. Sie ermöglichen auch die Vielfachverbreitung einer Information mit automatisierten Systemen, sogenannten Bots. So lässt sich auch durch eine kleine Anzahl von Akteuren eine Dominanz in den sozialen Netzwerken erreichen.

Manipulierte Informationen zirkulieren oft schneller als korrekte.[66] Sie sind aufsehenerregend, einfach und unterhaltsam. Das erhöht ihre Chancen, von anderen Benutzerinnen und Benutzern geteilt zu werden. Neben unbedachten Normalnutzern gibt es auch Akteure, die bewusst manipulierte Informationen verbreiten und diesen den Anschein von Legitimität verleihen, indem sie diese in Blogs oder sogar Online-Zeitungen verwenden.

---

65 Dem Reuters Digital News Report 2016 zufolge sind die sozialen Netzwerke für 62 % der Erwachsenen in den USA und 48 % in Europa eine Informationsquelle. (Stand: 31. Januar 2019)

66 Siehe insbesondere Studie von M.I.T: http://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308 (Stand: 31. Januar 2019)

### 6.1.2 Illustrative Beispiele

Manipulationen, die in den letzten Jahren aufgedeckt wurden, erfolgten jeweils in einem spezifischen Kontext. Besonders im Visier sind dabei Wahlen oder Abstimmungen. Das bekannteste Beispiel ist sicher die US-amerikanische Präsidentschaftswahl 2016. In einem ohnehin schon sehr aufgeheizten Klima wurden Inhalte von E-Mail-Konten politischer Persönlichkeiten und Organisationen publik gemacht. Am 7. Oktober 2016 warfen die amerikanischen Behörden der russischen Regierung vor, sie habe versucht, die Wahlen zu stören. Ein Anklagedokument[67] des Sonderstaatsanwalts Mueller vom Februar 2018 enthielt zudem Einzelheiten über einen Versuch der «Internet Research Agency» mit Sitz in St. Petersburg, falsche Nachrichten zu erstellen und systematisch zu verbreiten. Das Ziel soll die Beeinflussung der Wahlen 2016 gewesen sein. Man habe die Untergrabung des Vertrauens in die demokratische Instutionen, die Akzentuierung gesellschaftlicher Gräben und die Radikalisierung von Wählern erreichen wollen. Man habe vorgegeben, frei erfundene Inhalte zu polarisierenden Themen wie Schusswaffen oder Rassismus stammten aus den USA. Sie wurden von lokalen Sympathisanten oder Gruppen aufgenommen und weiterverbreitet. Soziale Netzwerke, insbesondere «Facebook», spielen bei dieser Verbreitung eine wichtige Rolle.

Auch in Europa kam es zu ähnlichen Ereignissen. Im französischen Wahlkampf 2017 wurden gezielt falsche Informationen verbreitet. Der später zum Präsidenten gewählte Kandidat Emmanuel Macron soll über ein angebliches Offshore-Konto verfügt haben. Ebenso wurden kurz vor der Wahl Dokumente aus gehackten Konten von engen Mitarbeitenden Macrons publik gemacht. Einige Experten machten offen Russland für den Angriff verantwortlich. Den Nachweis konnten die französischen Behörden aber nicht erbringen. Manipulationen können auch auf Abstimmungen abzielen, beispielsweise bei einem Referendum. Gerüchten zufolge soll Russland auch die Abstimmungen über den Brexit oder den Unabhängigkeitskampf Kataloniens beeinflusst haben.

### 6.1.3 Perspektiven in der Schweiz

Theoretisch sind Ereignisse wie in den USA oder Frankreich zwar auch für die Schweiz nicht auszuschliessen. Sie sind jedoch nur sehr schwer vorstellbar: Die Schweiz hat keine vergleichbare poltisch-strategische Rolle. Ausserdem sind eidgenössische Wahlen aufgrund der politischen Kultur und der Proporzwahl nicht im gleichen Masse polarisierend. Stärker polarisiert allerdings der politische Diskurs im Vorfeld von Abstimmungen über Referenden oder Volksinitiativen zu Einwanderungsthemen oder zur Unabhängigkeit von der EU. Sachvorlagen bei Abstimmungen im Rahmen der direkten Demokratie könnten deshalb eher durch Destabilisierungsversuche gefährdet sein.

Auch spezifische, nicht vorhersehbare Ereignisse können für punktuelle Manipulationen missbraucht werden. Der Absturz des Flugzeuges MH17 der Malaysia-Airlines hat laut einigen Experten zu einer intensiven Desinformation seitens Russlands geführt, das beschuldigt worden war, das Flugzeug abgeschossen zu haben. Das Gleiche gilt für den Giftanschlag auf den ehemaligen russischen Agenten Sergei Skripal auf englischem Boden. Insofern kann eine Desinformationskampagne jedes Land treffen, sofern ein Ereignis für einen Drittstaat von Interesse ist. Deshalb dürfen wir nicht davon ausgehen, dass die Schweiz von einer solchen Bedrohung ausgenommen ist. Das Störpotenzial solcher Kampagnen ist nicht zu unterschätzen. Denn Zweifel an der Legitimität der Ergebnisse bei einer kritischen Abstimmung kann

[67] https://www.justice.gov/file/1035477/download (Stand: 31. Januar 2019)

Sand in das Getriebe der politischen Debatte streuen und das Vertrauen in die Institutionen in der Schweiz erheblich beeinträchtigen.

### 6.1.4 Was tun?

Auf dem Weg zu Massnahmen gegen allfällige Informationsmanipulationen sind verschiedene Punkte zu klären. Zuerst muss die Debatte geführt und die Konzepte müssen geklärt werden. Der Begriff «Fakenews» ist vage und bietet grossen Interpretationsspielraum. Das Problem ist klar zu definieren. Auf dieser Grundlage ist zu entscheiden, was in einer Demokratie akzeptabel ist und was nicht. Falsche Informationen und das Verbreiten von Gerüchten, denen eher eine schlechte journalistische Arbeit als böse Absicht zugrunde liegt, und eine aus dem Ausland gesteuerte Desinformation, um die öffentliche Meinung zu beeinflussen, sind zwei verschiedene Dinge. Zweitens muss die Fähigkeit entwickelt werden, böswillige Kampagnen zu erkennen. Welche Hinweise gibt es? In diesem Bereich ist die intensive Zusammenarbeit mit privaten Akteuren (Contentmanager, Internetprovider) und internationalen Partnern notwendig, die sich mit denselben Fragen befassen. Schlüsselereignisse (z. B. heikle Abstimmungen) sind besonders aufmerksam zu beobachten. Solche Massnahmen erfordern auch eine enge Zusammenarbeit mit privaten Akteuren, die problematische Inhalte erkennen und dagegen vorgehen können. Hier wird sich die Vorarbeit bei der Definition auszahlen. Wird die Thematik zu weit gefasst, könnte dies als Zensur aufgefasst werden. Neben technischen oder rechtlichen Massnahmen (insbesondere Strafverfolgung) kommt der Sensibilisierungsarbeit grosse Bedeutung zu. Massnahmen der Aufklärung und der politischen Bildung auf allen Stufen sind die Grundlage für den Schutz von Gesellschaften, Gruppen und Individuen vor der manipulativen Wirkung von Beeinflussungsoperationen. Funktionierende Institutionen der Zivilgesellschaft sind hierzu unabdingbar. Der Erfolg einer Manipulationskampagne hängt davon ab, wie die manipulierten Information aufgenommen und von den Benutzern weitergeleitet werden. Eine Verbesserung der Medien- und Technologiekompetenz kann dazu beitragen, die Wirkung einer Kampagne zu begrenzen. Zu diesen Kompetenzen gehört beispielsweise die Fähigkeit, die Quelle einer Information oder die Legitimität einer Plattform zu überprüfen und zu bewerten und generell noch kritischere Blicke in Bezug auf Informationen zu entwickeln.

## 6.2 Normentwicklung

Wer regiert das Internet? Lange Zeit haben viele Staaten dieses neue Medium und seine Nutzer ignoriert oder belächelt. Die Zivilgesellschaft nutzte das Internet in jeder Weise, die angeboten wurde und möglich war. Unternehmen machten es genauso. Die Internet-Akteure, das heisst insbesondere die Telekommunikationsfirmen, welche Leitungen und Anschlüsse bereitstellen und auch die Domainnamen-Industrie, regulierte sich weitgehend selbst. Im Fokus waren Verbreitung und Wachstum. Die Kontrolle über Nutzende und die Überwachung dessen, was sie tun, war kein zentrales Thema. Denn das Internet war der freie Raum, in welchem alle ihre Meinung ohne Einschränkung äussern konnten. Doch die Zeiten, in welchen das Internet nur zum Austausch von Informationen genutzt wurde, sind schon lange vorbei. Mittlerweile durchdringt die Vernetzung fast alle Lebensbereiche und ein Leben ohne das Internet ist kaum mehr vorstellbar. Viele wichtige wirtschaftliche und gesellschaftliche Prozesse benötigen dieses Medium. Es soll deshalb zuverlässig und sicher funktionieren. Da Sicherheit traditionell eine hoheitliche Aufgabe ist, versuchen nun viele Behörden, diese Verantwortung auch bezüglich dem Internet wahrzunehmen und verpasste Regulierungen nachzuholen. Doch der traditionell territorial beschränkte Ansatz nationaler Gesetzgebungen greift nur beschränkt und Staaten müssen die globale Dimension des Internets berücksichtigen.

Eine globale Regulierung durch Staaten scheint kaum realistisch. Zwar hat die UNO schon mehrere Expertengruppen zusammengerufen (United Nations Group of Government Experts, UN GGE), um über Risiken und Massnahmen für die internationale Sicherheit und den Frieden im Kontext des Internet zu beraten. Der Prozess ist jedoch langfädig und beim letzten Expertentreffen 2017 konnte kein konsensuales Ergebnis präsentiert werden. Dies reflektiert nicht zuletzt die steigenden geopolitischen Spannungen, welche sich in allen Bereichen internationaler Kooperation niederschlagen. Eine multilaterale Lösung, mit welcher alle Länder der Welt einverstanden sind, dürfte deshalb weiter auf sich warten lassen.

Es wollen oder können jedoch nicht alle warten. Die Digitalisierung schreitet voran und der Druck von verschiedensten Seiten auf die Akteure im Internet – das sind nun nicht mehr nur einige Internet-Infrastruktur-Betreiber, sondern jegliche Anbieter und Nutzer – steigt spürbar. Einige Staaten versuchen, das Internet zumindest in ihrem Territorium zu regulieren und zu kontrollieren; indem sie beispielsweise ausländischen Plattform-Anbietern Vorschriften zu Datenschutz sowie zur Löschung von gewissen Inhalten machen, Informationen zensieren oder die Abschottung ihres Internet-Segments üben. Auf der anderen Seite stehen global agierende Unternehmen («Google», «Facebook», «Microsoft», etc. ), welche das weltweite Netzwerk als solches (wie auch den globalen Markt) erhalten wollen und nicht Spielball geopolitischer Konflikte sein möchten. Hinzu kommen Vertreter der Zivilgesellschaft, die sich sowohl ausufernder Staatsmacht als auch unternehmerischer Profitgier entgegenstellen.

Es braucht also auch im häufig als «rechtsfreien Raum» bezeichneten Internet gewisse Regeln. Da von Seiten der Staaten keine globale Rechtssicherheit geboten wird, springen vermehrt private Akteure in die Lücke und machen Vorschläge für Verhaltensnormen oder geben Erklärungen ab, nach was für Prinzipien sie agieren. Häufig stammen solche Initiativen aus der IKT-Industrie im weitesten Sinne oder von Multi-Stakeholder-Gremien.

Folgende drei Beispiele zeigen die Bestrebungen, das Internet und die IKT-Nutzung vorhersehbar, zuverlässig und sicherer zu machen:

### 6.2.1 Global Commission on the Stability of Cyberspace (GCSC)[68]

Die Global Commission on the Stability of Cyberspace (GCSC) vereint herausragende Personen von Regierungen, Unternehmen, Technischer- und Zivilgesellschaft je aus verschiedensten geographischen Regionen. Ihre Mission ist das Fördern von Frieden, Sicherheit und Stabilität im internationalen Raum, indem Normen und Initiativen zum verantwortungsvollen Verhalten der staatlichen und nichtstaatlichen Akteure im Cyberspace vorgeschlagen werden.

### 6.2.2 Cyber Security Tech Accord[69]

Der Cyber Security Tech Accord wurde bislang von rund 80 IT-Unternehmen unterzeichnet.[70] Sie bekennen sich damit zu folgenden Prinzipien, um die Sicherheit, Stabilität und Resilienz des Cyberspace zu verbessern:

- Verteidigung und Schutz: Alle Nutzenden sind weltweit, unabhängig von ihrer Herkunft, vor Angriffen zu schützen.

---

68 https://cyberstability.org/ (Stand: 31. Januar 2019)

69 https://cybertechaccord.org/ (Stand: 31. Januar 2019)

70 https://cybertechaccord.org/about/ (Stand: 31. Januar 2019)

- Keine Angriffe: Regierungen wird nicht geholfen, Angriffe auf unschuldige Bürger oder Unternehmen zu lancieren. Zudem soll verhindert werden, dass Produkte oder Dienste manipuliert werden.
- Aufbau von Kapazitäten: Fähigkeiten zum Selbstschutz sollen bei Entwicklern und Anwendern verbessert werden.
- Kollektives Handeln: Technische Zusammenarbeit und koordinierte Offenlegung von Schwachstellen soll weiter verbessert und die Verbreitung von Schadsoftware bekämpft werden.

### 6.2.3 Paris Call for Trust and Security in Cyberspace[71]

Über 400 Organisationen, Unternehmen und Staaten haben den Pariser Appell für Vertrauen und Sicherheit im Cyberspace unterzeichnet, der die Erarbeitung gemeinsamer Grundlagen für die Sicherheit im Internet vorantreiben will. Die Unterstützer des Pariser Appells verpflichten sich zu einer Zusammenarbeit mit folgenden Zielen:

- die Vorbeugung und die Widerstandsfähigkeit angesichts böswilliger Online-Aktivitäten verbessern;
- die Zugänglichkeit und die Funktionsfähigkeit des Internets schützen;
- gemeinsam Einmischungen in Wahlen vorbeugen;
- gemeinsam gegen Missachtung von geistigem Eigentum im Internet vorgehen;
- die Verbreitung von Schadsoftware und böswilligen Internet-Technologien verhindern;
- die Sicherheit digitaler Produkte und Dienstleistungen sowie die allgemeine «Cyber-Hygiene» verbessern;
- Massnahmen gegen Cyber-Söldner und offensive Aktivitäten nichtstaatlicher Akteure ergreifen;
- gemeinsam massgebliche internationale Standards verbessern.

71 https://www.diplomatie.gouv.fr/de/aussenpolitik-frankreichs/neuigkeiten/article/die-paris-digital-week-bietet-die-moglichkeit-zur-begrundung-einer-vielfaltigen (Stand: 31. Januar 2019)

# 7 Politik, Forschung, Policy

## 7.1 CH: Parlamentarische Vorstösse

| Geschäft | Nummer | Titel | Eingereicht von | Datum Einreichung | Rat | Amt | Stand Beratung & Link |
|---|---|---|---|---|---|---|---|
| **Mo** | 18.4387 | 2019 Bundesrat und VBS geben der Cyber Security höchste Priorität | Guggger Niklaus-Samuel | 14.12.2018 | NR | EFD | https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184387 |
| **Mo** | 18.4051 | Cybersicherheit, Cyberabwehr. Wo stehen wir? | Golay Roger | 28.09.2018 | NR | EFD | https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184051 |
| **Mo** | 18.4000 | Die Schweiz tritt dem Kompetenzzentrum für Cyberabwehr der Nato in Tallinn bei | Fridez Pierre-Alain | 28.09.2018 | NR | VBS | https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184000 |
| **Mo** | 18.4375 | E-Voting: ein schneller und entschlossener Einsatz für ein System auf Opens-Source-Basis und in öffentlicher Hand | Sommaruga Carlo | 14.12.2018 | NR | BK | https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184375 |
| **Po** | 18.4346 | Vergleichsportale müssen ehrlicher werden: Offenlegung aller offenen und versteckten Provisionen von Vergleichsdiensten | Reimann Lukas | 14.12.2018 | NR | WBF | https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184346 |
| **Ip** | 18.4230 | Kostenloses WLAN in den Zügen der SBB: ein Minimum im Zeitalter der digitalen Schweiz | Tornare Manuel | 13.12.2018 | NR | UVEK | https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184230 |
| **Ip** | 18.4178 | Umsetzbares Smart Farming | Page Pierre-André | 12.12.2018 | NR | WBF | https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184178 |
| **Ip** | 18.4121 | Immer mehr Kinder werden im Internet von fremden Personen sexuell angemacht. Was macht der Bundesrat? | Frei Yvonne | 29.11.2018 | NR | EJPD | https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184121 |
| **Po** | 18.4004 | Das Pauschalreisegesetz der heutigen Konsumrealität anpassen | Birrer-Heimo Prisca | 28.09.2018 | NR | EJPD | https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184004 |
| **Po** | 18.3858 | Pornografiekonsum von Kindern und Jugendlichen im Internet einschränken | Nordmann Roger | 26.09.2018 | NR | EDI | https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183858 |
| **Mo** | 18.3856 | Mehr Rücksicht auf die Gesundheit im Mobilfunk (1) | Estermann Yvette | 26.09.2018 | NR | UVEK | https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183856 |
| **Mo** | 18.3855 | Mehr Rücksicht auf die Gesundheit im Mobilfunk (2) | Estermann Yvette | 26.09.2018 | NR | UVEK | https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183855 |
| **Ip** | 18.3800 | Was kann man gegen den visuellen Analphabetismus tun? | Fehlmann Rielle Laurence | 20.09.2018 | NR | WBF | https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183800 |
| **Fr** | 18.5450 | Hat das Radio eine Zukunft? | Wasserfallen Flavia | 12.09.2018 | NR | UVEK | https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185450 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Ip** | 18.4404 | Strategie «Digitale Schweiz»: das Verfahren zur Konsultation von Unternehmen vereinfachen | Derder Fathi | 14.12.2018 | NR | UVEK | https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184404 |
| **Mo** | 18.4037 | Kompetenzzentrum für künstliche Intelligenz in der Bundesverwaltung | Bendahan Samuel | 28.09.2018 | NR | WBF | https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184037 |
| **Mo** | 18.3788 | Digitaler Fahrzeug- und Führerausweis | Grüter Franz | 19.09.2018 | NR | UVEK | https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183788 |
| **Fr** | 18.5478 | Strategie Digitale Schweiz. Erlaubt die politische Steuerung eine rasche Umsetzung des Aktionsplans? | Derder Fathi | 12.09.2018 | NR | UVEK | https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185478 |
| **Fr** | 18.5476 | Strategie Digitale Schweiz. In der Wissenschaft tätige und in der Digitalisierung spezialisierte Unternehmen in den Aktionsplan einbeziehen | Derder Fathi | 12.09.2018 | NR | UVEK | https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185476 |
| **Mo** | 18.3958 | Einmalige Erhebung von Daten durch den Staat | Müller-Altermatt Stefan | 27.09.2018 | NR | EFD | https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183958 |
| **Ip** | 18.3853 | Fragwürdiges Informatik-Outsourcing trifft langjährige ältere Bundesangestellte | Gyse Barbara | 26.09.2018 | NR | EFD | https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183853 |
| **Po** | 18.3783 | Effizienzsteigerung beim Bund durch intelligente Prozessautomatisierung in der Verwaltung | FDP-Liberale Fraktion Dobler Marcel | 19.09.2018 | NR | EFD | https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183783 |
| **Ip** | 18.4299 | Potential von Open Source Software im Schweizer Bildungswesen | Quadranti Rosmarie | 14.12.2018 | NR | WBF | https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184299 |
| **Ip** | 18.4197 | IT-Sicherheit kritischer Infrastrukturen - Welche Mittel und Massnahmen ergreift der Bund? | Wasserfallen Christian | 12.12.2018 | NR | EFD | https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184197 |
| **Mo** | 18.4276 | Erleichterter Informationsaustausch durch Einführung von elektronischen Schnittstellen in der Bundesverwaltung | Vonlanthen Beat | 13.12.2018 | SR | EFD | https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184276 |
| **Ip** | 18.4235 | Schwei bei Digital Health abgeschlagen: Welche Massnahmen sieht der Bundesrat vor? | Graf-Litscher Edith | 13.12.2018 | NR | EDI | https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184235 |

## 7.2 Die Entwicklung der gesetzlichen Rahmenbedingungen für Blockchain-Technologie

Das Thema Blockchain ist zurzeit in aller Munde, insbesondere schaut man gebannt auf die Entwicklung der Kryptowährungen und den Kosmos des Schweizer Krypto-Valleys. Wie allerdings das Schweizer Rechtssystem die dahinterliegende Technologie erfassen und entsprechende Rechtssicherheit für die Wirtschaft bieten kann – Voraussetzung für Förderung und Entwicklung - hat unlängst verschiedene Fragen aufgeworfen.

Um Antworten zu finden hat das Staatssekretariat für internationale Finanzfragen (SIF) im Januar 2018 eine Arbeitsgruppe zum Thema Blockchain/ Initial Coin Offering (ICO) gegründet. Da die Blockchain-Technologie nicht nur das Finanzmarktrecht, sondern auch andere Rechtsgebiete wie das Zivil- und Obligationenrecht betrifft, nehmen auch das Bundesamt für Justiz (BJ), die FINMA sowie Vertreter der Finanzbranche Einsitz in der Arbeitsgruppe. Ziel der Arbeiten sind die Erhöhung der Rechtssicherheit, die Aufrechterhaltung der Integrität des Finanzplatzes sowie die Sicherstellung einer technologieneutralen Regulierung.

Im August 2018 konsultierte die Arbeitsgruppe die Finanz- und Fintech-Branche und gab ihr Gelegenheit, zu den bisherigen Arbeiten und Empfehlungen Stellung zu nehmen. Die Konsultation warf neben allgemeinen Fragen wie der Zugang zu Bankkonten für Fintech-Unternehmen, auch Fragestellungen im Zivilrecht, der Bekämpfung von Geldwäscherei und Terrorismusfinanzierung sowie Finanzmarktrecht auf. Potentieller Handlungsbedarf wurde insbesondere bei der zivilrechtlichen Qualifikation und Übertragung von Token, deren insolvenzrechtliche Behandlung sowie der Schaffung neuer Möglichkeiten im Bereich der Finanzmarktinfrastrukturen verortet.

Mitte Dezember 2018 verabschiedete der Bundesrat den Bericht «Rechtliche Grundlagen für Distributed Ledger-Technologie und Blockchain in der Schweiz» der Arbeitsgruppe Blockchain/ ICO und beschloss, auf ein spezifisches Blockchain-Gesetz zu verzichten. Der Bericht zeigt auf, dass der Schweizer Rechtsrahmen gut geeignet ist, mit den neuen Technologien umzugehen. Dennoch besteht punktuell gesetzlicher Anpassungsbedarf. Der Bundesrat hat das Eidgenössische Finanzdepartement (EFD) und das Eidgenössisches Justiz- und Polizeidepartement (EJPD) beauftragt, 2019 eine Vernehmlassungsvorlage zu erarbeiten, welche folgende Aspekte regelt:

- im Zivilrecht die Rechtssicherheit bei der Übertragung von Rechten mittels digitalen Registern zu erhöhen,
- im Insolvenzrecht die Aussonderung im Konkurs von kryptobasierten Vermögenswerten weiter zu klären sowie eine Aussonderung von nicht vermögenswerten Daten zu prüfen,
- im Finanzmarktrecht ein neues und flexibles Bewilligungsgefäss für blockchainbasierte Finanzmarktinfrastruktruen auszuarbeiten,
- im Bankenreicht die bankinsolvenzrechtlichen Bestimmungen mit den Anpassungen im allgemeinen Insolvenzrecht abzustimmen und
- im Geldwäschereirecht die heutige Praxis zur Unterstellung dezentraler Handelsplattformen unter das Geldwäschereigesetz expliziter zu verankern.

Zusammengefasst will der Bundesrat bestmögliche Rahmenbedingungen zur Förderung der Schweiz als Standort für Fintech- und Blockchain-Unternehmen schaffen, sowie Missbräuche konsequent bekämpfen, um die Integrität und Reputation des Finanz- und Wirtschaftsplatzes Schweiz zu gewährleisten.

Gleichzeitig hat der Bundesrat einen Bericht der interdepartementalen Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (KGGT) zu «Geldwäscherei- und Terrorismusfinanzierungsrisiken von Krypto-Assets und Crowdfunding» veröffentlicht. Der Bericht hält fest, dass kryptobasierte Vermögenswerte im Bereich Geldwäscherei und Terrorismusfinanzierung eine Gefährdung darstellen. Aufgrund geringer Fallzahlen könne das reelle Risiko in der Schweiz jedoch nicht abschliessend geschätzt werden. Verbesserungen sollen in diesem Bereich vor allem mittels international koordinierter Massnahmen angestrebt werden. Hingegen wurde das EFD mit der Prüfung beauftragt, ob das Geldwäschereirecht in Bezug auf gewisse Formen des Crowdfundings angepasst werde soll.

Ob diese Massnahmen ausreichen werden, um die Attraktivität des Blockchain-Standortes und der Verankerung des Krypto Valleys Schweiz nachhaltig zu sichern, wird die Zukunft zeigen. Die unlängst neu gegründete «Swiss Blockchain Federation» will sich unter der Führung des Zuger Regierungsrates Heinz Tännler für den Erhalt und Ausbau der Attraktivität und der Konkurrenzfähigkeit des Blockchain-Standorts Schweiz einsetzen, relevante Akteure vernetzen und das Blockchain-Ökosystem in der Schweiz stärken.

Diese Aufgabe scheint zentral, lockt doch Liechtenstein mit einem Blockchain-Gesetz, welches im Sommer 2019 in Kraft treten soll. Diese Rahmenbedingungen ziehen auch Firmen aus dem Schweizer Krypto Valley an.

Das Fürstentum Liechtenstein beobachtet, dass aufgrund der hohen Regulierungsdichte im Finanzmarkt, innovative Unternehmen immer wieder an gesetzliche Grenzen stossen. Aus staatlicher Sicht ist es dem Regierungschef Liechtensteins, Adrian Hasler, wichtig, dass solche Unternehmen Klarheit über Möglichkeiten und Grenzen haben. Weiter sei klar, dass das Potenzial der Blockchain-Technologie nicht nur im Finanzdienstleistungsbereich liege, sondern dass eine viel grössere Palette an Vermögensobjekten digital abgebildet und für jede erdenkliche Dienstleistung zur Verfügung gestellt werden könne. Liechtenstein hat sich für ein Blockchain-Gesetz entschieden, weil die Anwendungsfelder der Token-Ökonomie die gesamte Wirtschaft umfassen und einen weiteren Schritt der Digitalisierung darstellen. Mit dem «Token» als neuem Rechtselement schafft Liechtenstein also ein Instrument, mit dem jedes beliebige Recht aus der analogen Welt digital abgebildet werden kann. Aber auch Grenzen und schutzwürdige Tätigkeiten sollen im neuen Gesetz reguliert werden, um das Missbrauchsrisiko einzugrenzen.

Dieser Ansatz schafft Sicherheit und stellt eine wichtige Grundlage für Innovation und Investition dar.

Informationen:

INFO

Bericht «Rechtliche Grundlagen für Distributed Ledger-Technologie und Blockchain in der Schweiz»:

https://www.newsd.admin.ch/newsd/message/attachments/55150.pdf

Bericht der Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung zu «Geldwäscherei- und Terrorismusfinanzierungsrisiken von Krypto-Assets und Crowdfunding»:

https://www.newsd.admin.ch/newsd/message/attachments/55111.pdf

FINMA Wegleitung für Unterstellungsfragen betreffend Initial Coin Offerings (ICOs):

https://www.finma.ch/de/news/20v18/02/20180216-mm-ico-wegleitung/

Vernehmlassungsbericht der Regierung Liechtensteins betreffend die Schaffung eines Gesetzes über auf vertrauenswürdigen Technologien (VT) beruhende Transaktionssysteme (Blockchain-Gesetz; VT-Gesetz; VTG):

https://www.llv.li/files/srk/vnb-blockchain-gesetz.pdf

# 8 Publizierte MELANI Produkte

## 8.1 GovCERT.ch Blog

### 8.1.1 Reversing Retefe

Approximately one year ago, we have published our blog post The Retefe Saga. Not much has changed since last year except that we have seen a rise of malspam runs in the last couple of weeks and we want to use the opportunity to show how to reverse engineer the Retefe malware.

➔ https://www.govcert.ch/blog/35/reversing-retefe

## 8.2 MELANI Newsletter

### 8.2.1 Wieder vermehrt betrügerische Anrufe bei Firmen

05.07.2018 - In den letzten Tagen mehren sich wiederum Anrufe bei potenziellen Opferfirmen, in denen sich Angreifer als Bankmitarbeiter ausgeben. Die Anrufer bitten um die Ausführung von Zahlungen oder geben vor, ein Update beim E-Banking durchführen zu müssen, das anschliessend getestet werden soll.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/truffe-via-e-mail-e-telefono-in-aumento.html ¨

### 8.2.2 Phishing-Attacken auf Online Datenaustausch - und Kollaborationsplattformen

02.10.2018 - Viele Firmen erlauben ihren Angestellten, Dokumente online zu teilen und sogar auf ganze Bürosysteme online zuzugreifen. Manchmal reicht nur ein Passwort, um Zugriff auf ein E-Mail-Konto, aber auch auf diverse andere Dokumente zu erhalten. Es ist deshalb nicht verwunderlich, dass diese Zugangsdaten von grossem Interesse für Phishing-Angriffe sind. Das Kompromittieren eines ersten Kontos wird daher oft als weiterführender Angriffsvektor gegen die anderen Mitarbeitenden verwendet.

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

### 8.2.3 Wer das gleiche Passwort mehrfach nutzt, hilft den Angreifern

08.11.2018 - Der am 8. November 2018 veröffentlichte 27. Halbjahresbericht der Melde- und Analysestelle Informationssicherung (MELANI) befasst sich mit den wichtigsten Cyber-Vorfällen der ersten Jahreshälfte 2018 im In- und Ausland. Das Schwerpunktthema ist den Lücken in Hardware gewidmet. Im Fokus stehen zudem unter anderem der gezielte Malware-Angriff, für den der Name des Labors Spiez missbraucht worden ist sowie verschiedene Datenabflüsse und die Problematik bei der Mehrfachnutzung eines Passwortes.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/melani-halbjahresbericht-1-2018.html

### 8.2.4 Trojaner Emotet greift Unternehmensnetzwerke an

12.12.2018 - Aktuell beobachtetet MELANI verschiedene Malspam-Wellen mit infiziertem Word-Dokumenten im Anhang. Dabei handelt es sich um einen bereits länger bekannten Trojaner namens «Emotet» (auch bekannt als Heodo). Ursprünglich als E-Banking-Trojaner bekannt, wird Emotet heute vor allem für den Versand von Spam sowie das Nachladen von weiterer Schadsoftware (Malware) verwendet. Emotet versucht - mit gefälschten E-Mails im Namen von Kollegen, Geschäftspartnern oder Bekannten - mittels Social-Engineering den Empfänger zum Öffnen des Word-Dokuments sowie zum Ausführen der darin enthaltenen Office-Makros zu verleiten.

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

## 8.3 Checklisten und Anleitungen

Im zweiten Halbjahr 2018 hat MELANI keine neuen Checklisten und Anleitungen publiziert.

# 9 Glossar

| Begriff | Beschreibung |
|---|---|
| Advanced Persistent Threats (APT) | Bei dieser Angriffsweise kommen verschiedene Techniken und Taktiken zum Einsatz. Sie wird sehr gezielt auf eine einzelne Organisation oder auf ein Land durchgeführt. Meist kann damit sehr hoher Schaden angerichtet werden. Deshalb ist der Angreifer bereit, sehr viel Zeit, Geld und Wissen in den Angriff zu investieren und verfügt dazu in der Regel über grosse Ressourcen. |
| Backdoor | Backdoor (deutsch: Hintertür) bezeichnet einen oftmals absichtlich eingebauten Teil einer Software, der es Benutzern ermöglicht, unter Umgehung der normalen Zugriffssicherung aus der Ferne Zugang zum Computer oder einer sonst geschützten Funktion eines Computerprogramms zu erlangen. |
| Bitcoin | Bitcoin ist ein weltweit verwendbares dezentrales Zahlungssystem und der Name einer digitalen Geldeinheit. |
| Bot | Ursprung im slawischen Wort für Arbeit (Robota). Bezeichnet ein Programm, das bestimmte Aktionen nach dem Empfang eines Befehls selbstständig ausführt. So genannte Malicious Bots können kompromittierte Systeme fernsteuern und zur Durchführung beliebiger Aktionen veranlassen. |
| 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. |
| CEO-Fraud | CEO-Fraud oder CEO-Betrug ist die Rede, wenn Täter im Namen des Firmenchefs die Buchhaltung oder den Finanzdienst anweisen, eine Zahlung auf ein (typischerweise ausländisches) Konto der Betrüger vorzunehmen. |
| 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. |
| CPU / Prozessor | Die CPU (Central Processing Unit) ist eine andere Bezeichnung für Prozessor, der zentralen Einheit in einem Computer, und enthält die logischen Schaltungen um ein Computer-Programm auszuführen. |

| | |
|---|---|
| Cryptomining | Durch das Mining werden neue Blöcke erzeugt und anschließend zur Blockchain hinzugefügt. Der Vorgang ist sehr rechenintensiv und wird deshalb vergütet. |
| DDoS | Distributed-Denial-of-Service-Attacke. Mit einer DoS-Attacke wird der Dienst oder das System des Opfers von vielen verscheiden Systemen aus gleichzeitig angegriffen, so dass dieses zum Erliegen kommt und nicht mehr verfügbar ist. |
| Defacement | Verunstaltung von Webseiten. |
| Domain Name System | Domain Name System. Mit Hilfe von DNS lassen sich das Internet und deren Dienste benutzerfreundlich nutzen, da die Benutzer anstelle von IP-Adressen Namen verwenden können (z. B. www.melani.admin.ch). |
| Downloader | Ein Downloader ist ein Programm, das eine oder mehrere Instanzen von Schadsoftware herunterlädt und installiert. |
| Exploit-Kit | Baukasten, mit welchen Kriminelle Programme, Scripts oder Code-Zeilen generieren können, womit sich Schwachstellen in Computersystemen ausnutzen lassen. |
| Fernzugriffstool | Die Fernwartungs-Software (englisch: Remote Administration Tool) stellt eine Anwendung des Konzeptes Fernwartung für beliebige Rechner oder Rechnersysteme dar. |
| Finanzagent | Ein Finanzagent ist jemand, der sich als legaler Geldvermittler und damit auch im Finanz-Transfergeschäft betätigt. In jüngerer Zeit wird dieser Begriff in Zusammenhang mit illegalen Finanz-Transaktionen gebraucht. |
| Global Positioning System (GPS) | Global Positioning System (GPS), offiziell NAVSTAR GPS, ist ein globales Navigationssatellitensystem zur Positionsbestimmung und Zeitmessung. |
| Internet der Dinge | Der Begriff Internet der Dinge (Internet of things IoT) beschreibt die Vernetzung und das Zusammenarbeiten von physischen und virtuellen Gegenständen. |
| Javascript | Eine objektbasierte Scripting-Sprache zur Entwicklung von Applikationen. JavaScripts sind im HTML-Code integrierte Programmteile, die bestimmte Funktionen im Internet-Browser ermöglichen. Ein Beispiel kann das Kontrollieren von Benutzereingaben bei einem Webformular sein. So kann überprüft werden, ob alle eingegebenen |

| | |
|---|---|
| | Zeichen bei geforderter Angabe einer Telefonnummer auch wirklich Zahlen sind. Wie ActiveX Controls werden JavaScripts auf dem Rechner des Webseitenbesuchers ausgeführt. Neben nützlichen, lassen sich leider auch schädliche Funktionen programmieren. Im Gegensatz zu ActiveX werden JavaScripts von allen Browsern unterstützt. |
| Kontroll- oder Steuerungssysteme (IKS) | Kontroll- oder Steuerungssysteme (IKS) bestehen aus einem oder mehreren Geräten, welche das Verhalten von anderen Geräten oder Systemen steuern, regeln und/oder überwachen. In der industriellen Produktion ist der Begriff «Industrielle Kontrollsysteme» (engl. Industrial Control Systems, ICS) geläufig. |
| Malware | Oberbegriff für Software, die schädliche Funktionen auf einem Rechner ausführt (wie beispielsweise Viren, Würmer, Trojanische Pferde). |
| Man-in-the-Middle Attacke | Attacke, bei der sich der Angreifer unbemerkt in den Kommunikationskanal zweier Partner hängt und dadurch deren Datenaustausch mitlesen oder verändern kann. |
| Metadaten | Metadaten oder Metainformationen sind Daten, die Informationen über andere Daten enthalten |
| Patch | Eine Software, die den fehlerhaften Teil eines Programms durch einen fehlerfreien ersetzt und dadurch z. B. eine Sicherheitslücke behebt. |
| Peer to Peer | Peer to Peer Eine Netzwerkarchitektur, bei der die beteiligten Systeme gleiche Funktionen übernehmen können (im Gegensatz zu Client-Server Architekturen). P2P wird häufig zum Austausch von Daten genutzt. |
| Phishing | Mittels Phishing versuchen Betrüger, an vertrauliche Daten von ahnungslosen Internet-Benutzern zu gelangen. Dabei kann es sich beispielsweise um Kontoinformationen von Online-Auktionsanbietern (z. B. eBay) oder Zugangsdaten für das Internet-Banking handeln. Die Betrüger nutzen die Gutgläubigkeit und Hilfsbereitschaft ihrer Opfer aus, indem sie ihnen beispielsweise E-Mails mit gefälschten Absenderadressen zustellen. |
| PowerShellScript | PowerShell ist ein plattformübergreifendes Framework von Microsoft zur Automatisierung, Konfiguration und Verwaltung von Systemen, bestehend aus einem Kommandozeileninterpreter sowie einer Skriptsprache. |
| Proxy | Ein Proxy ist eine Kommunikationsschnittstelle in einem Netzwerk. Er arbeitet als Vermittler, der auf der einen |

| | |
|---|---|
| | Seite Anfragen entgegennimmt, um dann über seine eigene Adresse eine Verbindung zur anderen Seite herzustellen. |
| Router | Geräte aus dem Bereich Computernetzwerke, Telekommunikation oder auch Internet, die mehrere Rechnernetze koppeln oder trennen. Router werden beispielsweise in Heimnetzwerken eingesetzt und machen die Verbindung zwischen internem Netz und dem Intranet. |
| Schadsoftware | Oberbegriff für Software, die schädliche Funktionen auf einem Rechner ausführt (wie beispielsweise Viren, Würmer, Trojanische Pferde). |
| Schwachstelle / Lücke | Schwachstelle in Hard- oder Software, über die Angreifer Zugriff auf ein System erlangen können. |
| Smartphone | Ein Smartphone ist ein Mobiltelefon, das mehr Computerfunktionalität und -konnektivität als ein herkömmliches fortschrittliches Mobiltelefon zur Verfügung stellt. |
| SMB-Protokoll | Server Message Block (SMB) ist ein Netzwerkprotokoll für Datei-, Druck- und andere Serverdienste in Rechnernetzen. |
| SMS | Short Message Service ist ein Dienst zum Versenden von Kurzmitteilungen (maximal 160 Zeichen) an Mobiltelefonbenutzer. |
| Social Engineering | Social Engineering-Angriffe nutzen die Hilfsbereitschaft, Gutgläubigkeit oder die Unsicherheit von Personen aus, um beispielsweise an vertrauliche Daten zu gelangen, oder die Opfer zu bestimmten Handlungen zu bewegen. Eine bekannte Form von Social Engineering ist Phishing. |
| Spam | Unaufgefordert und automatisiert zugesandte Massenwerbung, worunter auch Spam-E-Mails fallen. Als Spammer bezeichnet man den Absender dieser Mitteilungen, während das Versenden selbst als Spamming bezeichnet wird. |
| Spear-Phishing | Gezielte Phishing-Attacke. Dem Opfer wird zum Beispiel vorgegaukelt, mit einer ihr vertrauten Person via E-Mail zu kommunizieren. |
| Supply Chain-Angriffe | Angriff bei dem versucht wird, über die Infektion einer Firma in der Lieferkette das eigentliche Ziel zu infizieren. |

| | |
|---|---|
| Take-Down | Ausdruck, der verwendet wird, wenn ein Provider eine Website aufgrund betrügerischen Inhalts vom Netz nimmt. |
| Top-Level-Domains | Jeder Name einer Domain im Internet besteht aus einer Folge von durch Punkte getrennten Zeichenfolgen. Die Bezeichnung Top-Level-Domain bezeichnet dabei den letzten Namen dieser Folge und stellt die höchste Ebene der Namensauflösung dar. Ist der vollständige Domain-Name eines Rechners bzw. einer Website beispielsweise de.example.com, so entspricht das rechte Glied (com) der Top-Level-Domain dieses Namens. |
| Transmission Control Protocol / Internet Protocol (TCP/IP) | Transmission Control Protocol / Internet Protocol (TCP/IP) ist eine Familie von Netzwerkprotokollen und wird wegen ihrer großen Bedeutung für das Internet auch als Internetprotokollfamilie bezeichnet. |
| UDP | Das User Datagram Protocol, kurz UDP, ist ein minimales, verbindungsloses Netzwerkprotokoll, das zur Transportschicht der Internetprotokollfamilie gehört. |
| USB | Universal Serial Bus. Serielle Kommunikationsschnittstelle, welche 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. |
| Watering-Hole-Angriffe | Gezielte Infektion durch Schadsoftware über Webseiten, welche bevorzugt nur von einer spezifischen Benutzergruppe besucht werden. |
| Webseiteninfektion | Infektion eines Computers mit Malware allein durch den Besuch einer Web-Seite. Vielfach beinhalten die betroffenen Web-Seiten seriöse Angebote und sind zwecks Verteilung der Malware zuvor kompromittiert worden. Die Infektion erfolgt meistens durch das Ausprobieren von Exploits für vom Besucher noch nicht geschlossene Sicherheitslücken. |
| WLAN | WLAN (Wireless Local Area Network) steht für drahtloses lokales Netzwerk. |
| Wurm | Im Gegensatz zu Viren benötigen Würmer zur Verbreitung kein Wirtprogramm. Vielmehr nutzen sie Sicherheitslücken oder Konfigurationsfehler in Betriebssystemen bzw. Anwendungen, um sich selbständig von Rechner zu Rechner auszubreiten. |

| | |
|---|---|
| ZeroDay-Lücken | Sicherheitslücke, für welche noch kein Patch existiert. |
| ZIP-Datei | ZIP ist ein Algorithmus und Dateiformat zur Datenkompression, um den Speicherbedarf von Dateien für die Archivierung und Übertragung zu verringern. |
| Zweifaktorauthentifizierung | Um die Sicherheit zu erhöhen wird die Zweifaktorauthentifizierung verwendet. Dafür sind mindestens zwei der drei Authentifikationsfaktoren notwendig: 1. Etwas, das man weiss (z. B. Passwort, PIN, usw.) 2. Etwas, das man besitzt (z. B. Zertifikat, Token, Streichliste, usw.) 3. Ein einmaliges Körpermerkmal (z. B. Fingerabdruck, Retina-Scan, Stimmerkennung usw.). |