Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Informatiksteuerungsorgan des Bundes ISB
Nachrichtendienst des Bundes NDB

Melde- und Analysestelle Informationssicherung MELANI
https://www.melani.admin.ch/

INFORMATIONSSICHERUNG

LAGE IN DER SCHWEIZ UND INTERNATIONAL

Halbjahresbericht 2019/1 (Januar – Juni)

29. OKTOBER 2019

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

1 Übersicht / Inhalt

2 Editorial

Ransomware – Auch die Verwaltungen kann es treffen

Martin Müller ist ICT-Sicherheitsbeauftragter der Stadtverwaltung Bern, Mitglied in verschiedenen nationalen Arbeitsgruppen zum Thema ICT-Security und Swiss Certified ICT Leader.

Ransomware, Crypto-Trojaner, Verschlüsselungstrojaner oder Erpressungstrojaner, egal wie wir es nennen, solche Schadsoftware und die Lösegeldforderung, die nach der erfolgreichen Einnistung des Trojaners erscheint, sind seit WannaCry und der medialen Berichterstattung bekannt. Die Forderungen bewegen sich dabei zwischen wenigen hundert bis zu mehreren hunderttausend US-Dollars, die in Form von Bitcoins zu zahlen sind, damit die verschlüsselten Dateien wieder entschlüsselt werden. Eine Garantie, den Schlüssel zu den eigenen Daten zu erhalten, besteht jedoch nie.

Auch die Stadtverwaltung Bern war in den Jahren 2017 und 2019 von solchen Attacken betroffen. Die Angreifenden haben nicht gezielt die Stadtverwaltung angegriffen, sondern führten grossflächige Angriffe durch, um möglichst viel Geld zu generieren. Was vielen Sicherheitsbeauftragten schlaflose Nächte bereitet, ist die Tatsache, dass solche Angriffe heute mit sehr wenig Wissen und Mitteln ausgeführt werden können. Das sogenannte Ransomware-as-a-Service (RaaS) Modell ist bei verschiedenen Anbietern im Darknet bereits für eine geringe Summe erhältlich. Die Angriffsform steht somit nicht mehr nur professionellen Cyber-Kriminellen offen, sondern eigentlich jedem, egal ob Skriptkiddies mit Geltungsdrang oder Hacktivisten mit politischen Motiven.

Nebst allen möglichen technischen Sicherheitsvorkehrungen wie Firewalls, Angriffserkennungs- und Verhinderungssystemen, Antivirussystemen, Lösungen für die E-Mail-Sicherheit und das stetige Aktualisieren von Soft- und Hardware ist die regelmässige Erstellung von Sicherungskopien (Backups) eine wichtige technische Massnahme. Diese Backups sollten physisch oder logisch getrennt vom restlichen Unternehmensnetz aufbewahrt werden. So kann im Ereignisfall der Betrieb rasch wieder aufgenommen und der Datenverlust auf ein Minimum beschränkt werden. Das städtische Backup-Management hat sich bei den Angriffen auf die Verwaltung bisher sehr gut bewährt.

Nebst allen technischen Mitteln, die uns in der heutigen IKT-Welt zu Verfügung stehen, ist es aber der Mensch, der nach wie vor im Mittelpunkt steht und stehen muss. Deshalb erachten wir die Schulung und Sensibilisierung der Mitarbeitenden als die wichtigste Massnahme und tragenden Pfeiler der IKT-Sicherheit. Mit der digitalen Transformation im Verwaltungsumfeld muss die Grundlage geschaffen werden, damit die Mitarbeitenden die neuen Mittel sicher, verantwortungs- und vertrauensvoll nutzen können. Auch ein gesundes Mass an Misstrauen und gesundem Menschenverstand trägt zur Sicherheit bei. Die Stadtverwaltung Bern hat in ihrer Digitalstrategie 2021 und IKT-Sicherheitskampagne 2019-2020 daher bewusst die Befähigung des Menschen in den Mittelpunkt gestellt und wir empfehlen Ihnen, dies auch zu tun.

Martin Müller

3 Schwerpunktthema: Ransomware

Ransomware (dt. erpresserische Schadsoftware, Verschlüsselungstrojaner) ist ein etabliertes Angriffswerkzeug im Kosmos der Cyber-Kriminalität. Verschlüsselungstrojaner zielen auf die Verfügbarkeit von Daten ab, mit dem Ziel der Erpressung. Aber auch, wobei in geringerem Masse, kann ein Ziel sein, einem Unternehmen Schaden zuzufügen. Im Laufe der Jahre haben Verschlüsselungstrojaner technische und taktische Entwicklungen erlebt, die sie zu einer der gefährlichsten Bedrohungen für Unternehmen gemacht haben. Im ersten Halbjahr 2019 wurde weltweit eine Zunahme der gezielten Angriffe auf Organisationen und ein Anstieg der Lösegeldforderungen beobachtet.

3.1 Historische Entwicklung

Bereits vor acht Jahren beschrieb MELANI das Aufkommen von bösartiger Software, die Computer für Erpressungszwecke blockiert.[1] Es handelte sich damals um eine der ersten Versionen von Ransomware, die den Bildschirm blockierte und eine vermeintlich von der Bundespolizei stammende Meldung anzeigte. In dieser wurde behauptet, dass eine Geldstrafe zu bezahlen sei, da angeblich illegales Material auf dem betreffenden Gerät festgestellt wurde. Diese Art von *Malware* war relativ harmlos und konnte in den meisten Fällen, durch eine einfache Analyse des Computers mit einer Antiviren-Live-CD entfernt werden.

Zwei Jahre später machte mit «Cryptolocker» erstmals *Malware* mit Verschlüsselungsfunktion gross Schlagzeilen.[2] «Cryptolocker» verschlüsselte sowohl Daten auf der Festplatte als auch auf lokal angeschlossenen Datenträgern. Für jedes Opfer wurde auf einem *C2*-Server ein spezifischer Schlüssel generiert. Dies erschwerte die Datenwiederherstellung im Vergleich zu Verschlüsselungstrojanern, welche einen fest programmierten und somit extrahierbaren Schlüssel verwenden. «Cryptolocker» verbreitete sich über infizierte E-Mail-Anhänge (*Malspam*), über *Drive-by-Infektionen* (manipulierte Web-Seiten), oder wurden via bereits auf dem Gerät installierte *Dropper* (eigenständig ausführbare Programm-Datei) heruntergeladen. Die Ausbreitung via *Dropper* ist derzeit weit verbreitet.

Im Jahr 2014 wurde der Verschlüsselungstrojaner «Synolocker» durch die Ausnutzung einer Sicherheitslücke in den *NAS*-Geräten der Firma Synology propagiert.[3] Die ausgenützte Schwachstelle war bekannt und ein Sicherheits-Update wurde Monate zuvor veröffentlicht. Dieser Fall zeigte die Notwendigkeit, nicht nur Programme und Betriebssysteme von Computern, sondern auch Router, *NAS*-Geräte und ähnliche Komponenten regelmässig zu aktualisieren. 2014 begannen Ransomware-Programmierer Massnahmen zu ergreifen, um die Erkennung und Analyse von *C2*-Servern zu erschweren. Zum Beispiel der Verschlüsselungstrojaner «CTB-Locker», der über gehackte Websites von Online-Medien verbreitet wurde, kommunizierte verschlüsselt mit seinen *C2*-Servern und nutzte den Anonymisierungsdienst «Tor», um seine Spuren zu verwischen und damit die Erkennung und Analyse durch Sicherheitsakteure zu erschweren.

---

1 MELANI Halbjahresbericht 2/2011, Kap. 3.5.

2 MELANI Halbjahresbericht 2/2013, Kap. 3.1.

3 MELANI Halbjahresbericht 2/2014, Kap. 3.6.

Kriminelle suchten und suchen konstant nach neuen Zielen. So wurden auch Datenbanken von schlecht gesicherten Websites ins Visier genommen und verschlüsselt, um von den Administratoren der Websites Lösegeld zu fordern.[4] Im Jahr 2015 waren «Teslacrypt» und «Cryptowall» die aktivsten Ransomware-Familien.[5]

2016 erlebte das Phänomen Ransomware einen Boom.[6] Zum ersten Mal traf es publikumswirksam kritische Infrastrukturen, insbesondere Krankenhäuser in Deutschland und den USA. Der Gesundheitssektor steht nicht nur vor Herausforderungen, alle IKT-Systeme sowie zertifizierte Medizintechnik aktuell zu halten und Sicherheitsupdates einzuspielen, sondern muss auch bei Ausfällen schneller als andere Opfer zu reagieren, da eine funktionsunfähige IKT-Infrastruktur Menschenleben gefährden kann. Daher ist der Druck relativ hoch, Lösegeld zu bezahlen, um schnell wieder operativ werden zu können. Auf die Forderungen der Erpresser einzugehen ist jedoch nicht unbedingt eine zielführende Vorgehensweise, wie das Beispiel des Kansas Heart Hospital bewies. Das Spital erhielt von den Erpressern nur den Schlüssel für einen Teil der Daten und sah sich dann für die Entschlüsselung der restlichen Daten mit einer zweiten Lösegeldforderung konfrontiert.[7]

Eine technische Weiterentwicklung von Ransomware kam mit «Locky», die ab Februar 2016 auch in der Schweiz aktiv wurde.[8] Diese verschlüsselte Dateien, die auf verbundenen Netzwerkgeräten (Cloud-Laufwerke, Netzwerk-Shares, usw.) abgelegt waren. Die exponentielle Zunahme des Phänomens bewog Sicherheitsbehörden dazu, die präventiven Massnahmen zu verstärken. MELANI organisierte in Zusammenarbeit mit verschiedenen Bundesämtern, Schweizer Verbänden und Organisationen sowie Software-Herstellern einen Tag zur Sensibilisierung bezüglich Ransomware.[9] Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlichte ein Lagedossier zum Thema Ransomware.[10]

Im ersten Halbjahr 2017 zeigten zwei internationale Ransomware-Angriffe das Risikopotenzial solcher Angriffe deutlich auf: «WannaCry» befiel mindestens 200'000 Computer in 150 Ländern. Die namhaftesten Opfer waren das spanische Telekommunikationsunternehmen Telefonica, Krankenhäuser in Grossbritannien und die Deutsche Bahn. In der Schweiz wurden einige hundert Opfer gezählt, kritische Infrastrukturen befanden sich keine darunter. Kurz darauf wütete die *Malware* «NotPetya» zuerst in der Ukraine, wo sie unter anderem den Flughafen Kiew, die ukrainische Zentralbank und die Radioaktivitätsmessstelle in Tschernobyl erfolgreich angriff. Die *Malware* breitete sich dann via ukrainische Ableger von Multinationalen Unternehmen global aus. Nennenswerte Opfer waren die dänischen Maersk (die weltweit grösste Container-Reederei) und der US-Pharmariese Merck. «NotPetya» traf auch Opfer in der Schweiz,

---

4 MELANI Halbjahresbericht 2014/2, Kap. 5.3.

5 MELANI Halbjahresbericht 2015/1, Kap. 4.6.1.5 und 2/2015, Kap. 4.5.1.

6 MELANI Halbjahresbericht 2016/1, Kap. 5.4.3.

7 https://www.csoonline.com/article/3073495/kansas-heart-hospital-hit-with-ransomware-paid-but-attackers-demanded-2nd-ransom.html

8 MELANI Halbjahresbericht 2016/1, Kap. 4.6.3.

9 https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/ransomwareday.html; https://www.switch.ch/news/ransomware-day/; https://www.ebas.ch/de/securitynews/509-nationaler-ransomware-awareness-tag

10 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Lagedossier_Ransomware.pdf

zum Beispiel die Werbefirma Admeira.[11] Den Angriffen durch «WannaCry» und «NotPetya» ist gemein, dass die *Malware* sich wurmartig – also selbständig – durch die Ausnützung einer Lücke im *SMB-Protokoll* in Netzwerken verbreitete. Während bei «WannaCry» die Verbreitung zufällig erscheint, wird bei «NotPetya» davon ausgegangen, dass grundsätzlich ukrainische Unternehmen getroffen werden sollten. Sicherheitsexperten haben in beiden Fällen die Existenz einer rein kriminellen Motivation in Frage gestellt. Obwohl weder Angreifer noch Motivation endgültig geklärt sind, wird davon ausgegangen, dass in beiden Fällen Sabotage respektive das Auslösen von Panik das Ziel gewesen ist.

In der zweiten Jahreshälfte 2017 war die Ransomware «BadRabbit» Ursprung von geolokalisierten Angriffen, hauptsächlich in Russland, aber auch in der Ukraine, Deutschland und der Türkei. «BadRabbit» verbreitete sich mittels vorgetäuschten Updates von Adobe Flash und nutzte den «EternalRomance»-Exploit, um wie «Mimikatz» die Systeme der betroffenen Unternehmen zu infiltrieren und Zugangsdaten für die Weiterverbreitung zu erhalten.[12]

Der Produktivitätsverlust, welcher bis zur Wiederinstandstellung der durch Ransomware betroffenen Systeme verursacht werden kann, spürte 2018 der taiwanesische Hersteller von Mikrochips TSMC (Taiwan Semiconductor Manufacturing Company). Sie mussten die Produktion in mehreren Betriebsanlage wegen einer «WannaCry»-Variante anhalten.[13]

Bis 2018 waren Ransomware-Angriffe meist nicht zielgerichtet. Einzig die Gruppe «SamSam» war bekannt für gezielte Angriffe. Diese setzte Verschlüsselungstrojaner hautsächlich gegenüber US-Organisationen ein. Mit «Ryuk» erschien 2018 eine Ransomware, welche scheinbar spezifisch bei Organisationen platziert wurde, von welchen hohe Lösegelder verlangt werden konnten. «Ryuk» war im letzten Halbjahresbericht[14] Thema und ist auch 2019 sehr aktiv (siehe Kapitel 3.4.1). Daneben gibt es Ransomware, die sowohl gezielt als auch opportunistisch eingesetzt wird, wie beispielsweise «GandCrab» und «Dharma».[15]

3.2 Neuste Vorfälle

In der ersten Jahreshälfte 2019 nahm die Zahl der gezielten Ransomware-Angriffe zu. Zu den bereits erwähnten «Ryuk», «GandCrab» und «Dharma» sind «LockerGoga», «MegaCortex» und «RobbinHood» dazugekommen. Letzterer legte Ende Mai die Stadtverwaltung von Baltimore lahm.[16] Angriffe mit Ransomware stellt eine der gefährlichsten Cyber-Bedrohungen für Unternehmen, Organisationen und Verwaltungen dar. Ein erfolgreicher Angriff erfordert nicht nur den Einsatz von Zeit, Personal und Geld für die Bereinigung der Systeme und zur Wiederherstellung verlorener Daten, sondern kann auch den Ruf einer Unternehmung schädigen oder einen Produktivitätsverlust über einen gewissen Zeitraum beinhalten.[17] So musste beispiels-

11 MELANI Halbjahresbericht 2017/1, Kap. 3.
12 MELANI Halbjahresbericht 2017/2, Kap. 5.4.2.
13 MELANI Halbjahresbericht 2018/2, Kap. 5.3.5.
14 MELANI Halbjahresbericht 2018/2, Kap. 4.5.4.
15 https://www.symantec.com/blogs/threat-intelligence/targeted-ransomware-threat
16 https://www.tripwire.com/state-of-security/featured/ransomware-baltimore-network/
17 https://www.symantec.com/blogs/threat-intelligence/targeted-ransomware-threat

weise der Aluminiumproduzent Norsk Hydro aufgrund eines Ransomware-Angriffs die grundsätzlich automatisierte Produktion im manuellen Betrieb fortsetzen[18] oder die Polizisten von Jackson County im US-Bundesstaat Georgia mussten ihre Berichte wieder von Hand schreiben, nachdem die Systeme der Stadtverwaltung von «Ryuk» lahmgelegt worden waren.[19] In der Schweiz hat die Offix Holding AG, die Opfer von «Ryuk» wurde (siehe auch Kapitel 3.4.1), schlimmeres abgewendet, indem sie innerhalb weniger Stunden einen Notbetrieb einrichtete, der es ermöglichte, Kunden zu informieren und ihre tägliche Arbeit während der Lösung der Computerprobleme fortzusetzen. Die Firma ging nicht auf die Lösegeldforderung in der Höhe von 45 Bitcoins (circa 330'000 Franken) ein.[20]

Im Berichtszeitraum wurden auch Vorfälle verzeichnet, bei denen zwei Cyber-Bedrohungen gleichzeitig eingesetzt wurden: Ransomware und Phishing. Der dabei entdeckte Verschlüsselungstrojaner verschlüsselt nicht nur Dateien, sondern versucht gleichzeitig den Opfern sensible Daten zu entlocken. Die Opfer können wählen, ob sie das Lösegeld mit Bitcoin oder über PayPal bezahlen möchten. Wählen sie die Option PayPal, werden sie auf eine Phishing-Seite geleitet. Dort werden sie aufgefordert sowohl die Kreditkarteninformationen als auch die Zugangsdaten zu PayPal und weitere persönliche Angaben einzugeben.[21]

Da die Angreifer realisiert haben, dass ihre Pläne durch Backups vereitelt werden können, änderten sie ihre Vorgehensweise. Sie beschaffen nun zuerst die nötigen Zugänge und Passwörter, um auch die Backups zu löschen oder zu verschlüsseln, bevor sie mit der Verschlüsselung der operativen Systeme beginnen.

Es ist nicht verwunderlich, dass Unternehmen, die kein Backup haben oder deren Backup unbrauchbar gemacht wurde und sie sich deshalb in einer existenzbedrohender Lage befinden, beschliessen, das Lösegeld zu zahlen. Schon 2014 erklärte MELANI, dass Ransomware solange Erfolg haben würde, wie bei den Opfern Zahlungsbereitschaft vorhanden ist.[22] In der ersten Jahreshälfte 2019 sorgten die Fälle von zwei Städten in Florida für Aufsehen: Riviera City und Lake City. Sie erklärten sich bereit, die exorbitanten Lösegeldforderungen von 65 Bitcoins (ca. 600'000 Dollar) bzw. 42 Bitcoins (ca. 500'000 Dollar) zu zahlen. Im Fall von Lake City wurde die Lösegeldforderung durch Verhandlungen direkt mit der städtischen Versicherung vereinbart.[23] Diese Tendenz könnte sich auch in der Schweiz etablieren.[24] Langfristig handelt es sich bei der Bezahlung von Lösegeld aber nicht um eine «lohnende Investition». Denn je mehr Unternehmen bereit sind Lösegeld zu bezahlen, desto mehr, Cyber-Kriminelle werden anstiftet einen Wechsel zu diesem Geschäftsmodell zu unternehmen.[25]

---

18 https://www.bleepingcomputer.com/news/security/lockergoga-ransomware-sends-norsk-hydro-into-manual-mode/

19 https://statescoop.com/georgia-county-paid-400k-to-ransomware-hackers/

20 https://www.inside-it.ch/articles/54898

21 https://www.bleepingcomputer.com/news/security/new-ransomware-bundles-paypal-phishing-into-its-ransom-note/

22 MELANI Halbjahresbericht 2014/2, Kap. 5.3.

23 https://www.zdnet.com/article/second-florida-city-pays-giant-ransom-to-ransomware-gang-in-a-week/

24 https://www.nzz.ch/wirtschaft/ransomware-warum-zahlreiche-firmen-loesegeld-zahlen-duerften-ld.1489507

25 https://www.symantec.com/blogs/threat-intelligence/targeted-ransomware-threat

3.3 Ransomware-as-a-Service

Mit der zunehmenden Arbeitsteilung und Spezialisierung im cyber-kriminellen Milieu entwickelt sich auch der Untergrundmarkt weiter. Im Darknet werden schon seit geraumer Zeit vorkonfigurierte Cyber-Angriffe angeboten.[26] Dies wird als «Cybercrime-as-a-Service» (*CaaS*) oder im Fall von Ransomware als *RaaS* bezeichnet. Damit können auch Personen ohne spezielle Computerkenntnisse einen digitalen Angriff lancieren.[27] Diese Art von Service bietet zu einem bestimmten Preis die Elemente an, die für einen Angriff benötigt werden: Anleitung zur Erstellung der *Malware*, das Management Panel (Dashboard), welches alle notwendigen Informationen über die erfolgreichen Infektionen liefert, den Entschlüsselungsschlüssel und ggf. ein Tutorial zur Verwendung der bereitgestellten Tools. Ausgehend von diesem Basispaket kann der «Kunde» seine Ransomware und seinen Angriff an seine Bedürfnisse anpassen.[28]

3.4 Aktuell besonders aktive Ransomware

3.4.1 Ryuk

Die Ransomware «Ryuk» ist seit der zweiten Hälfte 2018 aktiv und wurde schon im letzten Halbjahresbericht thematisiert.[29] Im Dezember wurde mit «Ryuk» die Druckerei «Tribune Publishing» in Los Angeles angegriffen. Die Angreifer verschlüsselten den Server, der die Produktionsplattform für den Druck und die Verteilung mehrerer US-Zeitungen unterstützte. Der Ausfall verzögerte oder verhinderte in teilweise die Veröffentlichung der Samstagsausgaben der Los Angeles Times und der San Diego Union Tribune sowie der Westküsten-Publikationen des Wall Street Journal und der New York Times.[30]

Mit «Ryuk» werden gezielte Angriffe auf Computer und Unternehmensnetzwerkserver durchgeführt. Die Datenverschlüsselung ist oft die Endphase eines dreistufigen Angriffs, der mit einer «Emotet»-Trojaner-Infektion beginnt. «Emotet» wird häufig via E-Mail mit einem verseuchten Link oder Anhang verbreitet (*Malspam*). Wenn jemand im Unternehmen unbedarft klickt, installiert sich «Emotet» auf dessen Computer und sendet wiederum E-Mails an die dort vorhandenen Kontakte, um sich weiter zu verbreiten. «Emotet» kann als *Dropper* für andere bösartige Software fungieren. In einigen Fällen wird beispielsweise «Trickbot» heruntergeladen (siehe Kapitel 4.6), der eine Analyse des angegriffenen Netzwerks macht, um herauszufinden, ob es einer Privatperson oder einem Unternehmen gehört. Ist letzteres der Fall, versucht er sich im Netzwerk zu verbreiten, indem er die *SMB*-Sicherheitslücke ausnutzt. So werden weitere Informationen über das potenzielle Opfer gesammelt. «Ryuk» wird meist nur heruntergeladen, wenn das Opfer als ausreichend attraktiv angesehen wird.[31]

---

[26] Siehe MELANI Halbjahresbericht 2009/2, Kap. 4.7: "In der Cyberkriminalität ist im letzten Jahr das kommerzielle Modell Crimeware-as-a-Service (CaaS) entwickelt worden. Die Cyberkriminellen, welche sich in technischen Belangen nicht gut auskennen, können bei diesem Modell einen entsprechenden Dienst «mieten»."

[27] Siehe hierzu detailliert im MELANI Halbjahresbericht 2016/2, Kap. 6.1.

[28] https://securityaffairs.co/wordpress/84273/breaking-news/inpivx-ransomware-service.html

[29] MELANI Halbjahresbericht 2018/2, Kap. 4.5.4.

[30] https://www.heise.de/newsticker/meldung/Cyber-Attacke-verzoegert-Druck-grosser-Tageszeitungen-in-den-USA-4260103.html

[31] MELANI Halbjahresbericht 2018/2, Kap. 4.5.4.

Im laufenden Jahr wurden mit «Ryuk» gezielte Angriffe durchgeführt und dann exorbitante Beträge an Lösegeld gefordert. Unter den Opfern sind die Verwaltungen einiger Städte in den Vereinigten Staaten, die zwischen 130'000 Dollar und 600'000 Dollar Lösegeld gezahlt haben.[32]

In der Schweiz gab es Fälle im Baugewerbe, im öffentlichen Verkehr und in der Industrie. Zum Beispiel wurde Mitte Mai die Offix Holding AG, eine Firma für Büroartikel und Kanzleien, «durch einen gezielten, geplanten, massiven und durchorchestrierten Hacker-Angriff»[33] schwer getroffen.[34] Das Einfallstor war ein per E-Mail gesendetes Word-Dokument, welches via Makro die *Malware* «Emotet» installierte. Nachfolgend wurden «Trickbot» und «Ryuk» heruntergeladen. Zwei Tage später funktionierte ein grosser Teil der Systeme des Betriebes nicht mehr: Zeiterfassung, Saläradministration, Bilddatenbanken, Telefon-Server, Citrix-Server, Exchange Server und andere.[35] Verschont waren nur die Webshops, die auf Linux-Servern laufen, und das Warenbewirtschaftungssystem.

3.4.2 LockerGoga und MegaCortex

«LockerGoga» trat erstmals im Januar 2019 in Erscheinung, als der multinationale französische Ingenieur- und Industrieberater Altran Technologies damit angegriffen wurde.[36] «LockerGoga» ist typischerweise auch erst Teil der zweiten Phase einer Infektion und wird von einem «PsExec»-Tool auf einem zuvor infizierten Gerät ausgeführt. Angreifer verwenden Hacking-Tools, die im Netz verfügbar sind, um Zugang zum System zu erlangen und Administratorenrechte zu erhalten, mit denen Sicherheits-Software und Backups vor der Installation der Ransomware deaktiviert werden können. Diese Technik ermöglicht es, zusammen mit der Verwendung legitimer Zertifikate, dass *Malware* der Erkennung durch Schutzmassnahmen entgeht.[37] Nach der Installation ändert «LockerGoga» die Zugangsdaten zum System und versucht, die Sitzung der damit verbundenen Benutzer zu beenden. So versucht «LockerGoga» möglichst viele Geräte gleichzeitig zu verschlüsseln. Die Ransomware erzeugt aber für jede zu verschlüsselnde Datei einen eigenen Prozess, was recht ungewöhnlich ist, da dies die Verschlüsselung erheblich verlangsamt.[38]

Im März sollen mindestens drei namhafte Unternehmen «LockerGoga» zum Opfer gefallen sein: Hexion und Momentive, zwei im Besitz des Investmentfonds Apollo Global Management stehende US-Unternehmen, die Harze, Silikone und andere Materialien herstellen,[39] und der norwegische Aluminiumproduzent Norsk Hydro. Bei letzterem wurde anscheinend zuerst eine US-Filiale infiziert, wonach sich die *Malware* «seitwärts» durch das Netzwerk bewegte (lateral movement) und fast alle Arbeitsplätze infizierte. An einigen Stellen musste auf manuellen Be-

---

32 https://www.bleepingcomputer.com/news/security/la-porte-county-pays-130-000-ransom-to-ryuk-ransomware/

33 Kundenkommunikation von Offix Holding AG gemäss Inside-IT: https://www.inside-it.ch/articles/54898

34 https://www.nzz.ch/wirtschaft/cyber-angriff-auf-schweizer-firma-offix-ein-kampf-ums-ueberleben-ld.1492862

35 https://www.inside-it.ch/articles/54898

36 https://ml.globenewswire.com/Resource/Download/0663f8d4-0acf-4463-b0fd-bb05042d1373, https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware

37 https://www.symantec.com/blogs/threat-intelligence/targeted-ransomware-threat

38 https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware

39 https://www.chemistryworld.com/news/hexion-momentive-and-norsk-hydro-all-hit-by-ransomware-cyber-attacks/3010328.article

trieb umgestellt werden, da das Produktionssystem nicht mehr verfügbar war. Scheinbar haben die Kriminellen Passwörter für Active Directory-Konten geändert. Es ist möglich, dass die Angreifer mit «Mimikatz» oder einem ähnlichen Tool die sogenannten Kerberos-Tickets erhielten, mit denen sie ihre Identität als Benutzer vortäuschen respektive für das System nachweisen konnten.[40]

«MegaCortex» verwendet eine ähnliche Vorgehensweise wie «LockerGoga». Bei Angriffen mit dieser Ransomware werden Unternehmen und Organisationen gezielt angegriffen. Laut verschiedenen Quellen wurden in nur 48 Stunden fast 50 Unternehmen in den USA, Europa und Kanada durch «MegaCortex» infiziert.[41] Laut Sophos-Forschern gibt es keine Code-Ähnlichkeiten zwischen «MegaCortex» und «LockerGoga», jedoch verwenden die Betreiber in beiden Fällen einen kompromittierten *Domänencontroller*, um *Malware* an Geräte in einem Zielnetzwerk zu versenden. PowerShell-Befehle werden ausgeführt, um die kriminell kontrollierten *C2*-Server zu kontaktieren und die Verschlüsselung einzuleiten. Mindestens einer der *C2*-Server wurde sowohl für «MegaCortex» als auch für «LockerGoga» verwendet, erklären die Forscher.[42] Wie «Ryuk» wurde «MegaCortex» oft bei Unternehmen mit bereits bestehenden «Emotet»- und «Qbot»-Infektionen nachgewiesen.[43] Auch in der Schweiz wurden Aktivitäten von diesen Kryptotrojanern gemeldet.

3.4.3 GandCrab

In der zweiten Jahreshälfte 2018 machte «GandCrab» 50% des weltweiten Ransomware-Marktes aus. Dies war möglich, weil die *Malware*-Entwickler nach einem Ransomware-as-a-Service-Modell arbeiteten und ihre *Malware* im Darkweb anboten. Der Preis betrug 40% der Gewinne, welche durch die Angriffe mit diesem Tool erzielt werden.[44] Dies erklärt auch die Vielzahl der Vektoren, die zur Verbreitung der *Malware* verwendet wurden: Verschiedene Varianten von Massen-E-Mails (*Malspam*) wie auch vermeintliche Bewerbungsschreiben und von Kriminellen spezifisch aufgesetzte oder gehackte legitime Websites mit *Drive-by-Infektionen*.[45]

Seit ihrem Erscheinen im Januar 2018 kennt «GandCrab» verschiedene Versionen und Überarbeitungen des Codes, die die Angriffe immer effektiver machen und die Bekämpfung erschwert. Auch *Malware*-Autoren setzen auf Redundanz: Im laufenden Jahr wurde bei einigen Angriffen der Einsatz einer Kombination von «GandCrab» mit «BetaBot» oder «AzorUlt» beobachtet. «BetaBot» verfügt über Funktionen, um durch Deaktivierung von Antivirus und Firewall der Erkennung zu entgehen. Danach analysiert «BetaBot» das Gerät des Opfers, sammelt Informationen wie Zugangsdaten und E-Banking-Anmeldeinformationen. Währenddessen gewährleistet die zweite *Malware* (z. B. «GandCrab») die Redundanz der Infektion des betroffenen Systems, auch im Falle eines Systemabsturzes.[46]

---

40 https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware

41 https://www.darkreading.com/perimeter/lockergoga-megacortex-ransomware-share-unlikely-traits/d/d-id/1334696

42 https://news.sophos.com/en-us/2019/05/10/megacortex-deconstructed-mysteries-mount-as-analysis-continues/

43 https://www.darkreading.com/perimeter/lockergoga-megacortex-ransomware-share-unlikely-traits/d/d-id/1334696

44 https://www.europol.europa.eu/newsroom/news/just-released-fourth-decryption-tool-neutralises-latest-version-of-gandcrab-ransomware

45 MELANI Halbjahresbericht 2/2018, Kap. 4.5.4.

46 https://www.scmagazineuk.com/gandcrab-returns-trojans-redundency/article/1523389

Der Cloud-Dienstleister Meta10 mit Sitz in Zug erlitt am 22. Februar 2019, einen Angriff mit der Ransomware «GandCrab v5.2».[47] Betroffen waren einige Datenbank- und Applikationsserver sowie Backup-Server. Systembereinigung und Dokumentenwiederherstellung haben bei rund zehn Prozent der Kunden des Unternehmens zu spürbaren Leistungseinbussen geführt. Das Unternehmen entschied sich sofort für eine proaktive Kommunikation und informierte seine Kunden über den Vorfall. Diese konnten sich über die Seite «Service-Status» ständig über den aktuellen Stand informieren. Auch die Stadtverwaltung Bern wurde 2019 Opfer eines «GandCrab»-Angriffs, konnte sich jedoch dank ihrem vorbildlichen Backup-Management schnell vom Vorfall erholen.[48]

Ende Mai 2019 gaben die Betreiber von «GandCrab» bekannt, dass mit ihrer Ransomware 2 Milliarden Dollar Lösegeld generiert wurden und sie sich vom Geschäft zurückziehen wollten. Sie baten ihre Partner, die Verbreitung von «GandCrab» innerhalb von 20 Tagen einzustellen und ermutigten die Opfer, so schnell wie möglich Lösegeld zu zahlen, um zu vermeiden, dass ihre Daten für immer verloren gehen.[49]

Seit Mitte Juni 2019 steht unter nomoreransom.org ein Tool zur Verfügung, das die aktuell im Umlauf befindlichen Versionen (1, 4 und 5 bis 5.2) der Ransomware «GandCrab» entschlüsseln kann. Das Programm, das in Zusammenarbeit von Strafverfolgungsbehörden verschiedener Länder mit Unterstützung der Firma Bitdefender entwickelt worden ist, ermöglicht es Opfern, ihre verschlüsselten Dateien wiederherzustellen.[50] Eine Woche vor der Herausgabe dieses Werkzeuges kommunizierte ein syrischer Vater durch einen Tweet, dass er nicht genug Geld hätte, um das Lösegeld zu zahlen, und somit die Fotos seines toten Sohnes nicht wiederherstellen könne. Die Administratoren von «GandCrab» hatten Mitleid und entschieden sich dazu, einen Entschlüsselungsschlüssel für die syrischen Opfer der Ransomware zur Verfügung zu stellen.[51]

Es ist denkbar, dass die Ankündigung der «Pensionierung» ein Schritt war, um die Aufmerksamkeit von sich selbst abzulenken und sich neu zu organisieren. Laut einigen Sicherheitsexperten sind die Betreiber von «GandCrab» schon wieder im Geschäft und verwenden nun Verschlüsselungssoftware namens «REvil» und «Sodinokibi».[52] Die *Malware* «Sodinokibi» verzeichnete bereits ihre ersten Schweizer Opfer.

3.5 Ausblick

Im Zusammenhang mit Ransomware wird es in den nächsten Jahren weiterhin technische und methodische Entwicklungen geben. Es ist damit zu rechnen, dass Angriffe noch gezielter erfolgen und die Angriffsvektoren technisch noch ausgefeilter werden. Umso wichtiger wird es

47 https://www.computerworld.ch/security/hacking/cyberangriff-legt-zuger-cloud-provider-meta10-lahm-1684975.html

48 Siehe hierzu das Editorial des ICT-Sicherheitsbeauftragten der Stadtverwaltung Bern in Kapitel 2 oben.

49 https://securityaffairs.co/wordpress/86438/malware/gandcrab-shutdown-operations.html

50 https://www.europol.europa.eu/newsroom/news/just-released-fourth-decryption-tool-neutralises-latest-version-of-gandcrab-ransomware

51 https://krebsonsecurity.com/2019/07/is-revil-the-new-gandcrab-ransomware/

52 https://krebsonsecurity.com/2019/07/is-revil-the-new-gandcrab-ransomware/ und https://www.tesorion.nl/aconnection-between-the-sodinokibi-and-gandcrab-ransomware-families/

sein, Verwundbarkeiten zu beheben und den Grundschutz im Netzwerk hoch zu halten. Kriminelle sind typischerweise opportunistisch: Ist der Aufwand zu gross und stellt sich innert nützlicher Frist kein Erfolg ein, lohnt sich das Ziel nicht und sie ziehen weiter.

Wie sich bereits seit einigen Jahren abzeichnet, bietet das exponentielle Wachstum von mit dem Internet verbundenen Geräten (Internet der Dinge) Kriminellen ein immer grösseres Angriffsfeld.[53] Diese Entwicklung führt dazu, dass die meisten der von uns täglich verwendeten elektronischen Geräte mit dem heimischen Netzwerk oder gar direkt mit dem Internet verbunden und daher potentiell verwundbar sind. Es gibt verschiedenste Szenarien, in denen Kriminelle ein Gerät temporär unbrauchbar machen, um den Besitzer zu erpressen.

Aber auch die Strafverfolgung rüstet auf und arbeitet mit Sicherheitsbehörden und privaten Unternehmen auf verschiedenen Ebenen zusammen, um den Tätern Einhalt zu gebieten. Sie koordinieren sich national und international und können erste Erfolge vorweisen.[54]

3.6 Gastbeitrag: Gemeinsam gegen Cyber-Kriminelle

von Daniel Nussbaumer, Chef Cybercrime Kantonspolizei Zürich und Leiter NEDIK

Digital agile Kriminelle erfordern digital agile Strafverfolgungsbehörden. Im Kampf gegen Cyber-Kriminelle ist entscheidend, dass Bund und Kantone im stetigen Aus-tausch stehen und rasch reagieren können. Die Schweizer Polizeikorps haben sich deshalb im polizeilichen Netzwerk NEDIK zusammengeschlossen, um gemeinsam und in enger Zusammenarbeit mit MELANI repressiv und präventiv zu wirken.

Gezielte, professionelle Cyber-Angriffe gegen Unternehmen können diese in ihrer Existenz gefährden. Betroffenen Unternehmen geht es dann regelmässig ums Überleben. Entsprechend haben sie auch neue, veränderte Bedürfnisse an die Behörden. Wird ein Unternehmen angegriffen, ist es ihm wichtig zu wissen, wie die Täter in ein System eingedrungen sind, welche Systeme kompromittiert sind, wie das Unternehmen mit allfälligen Lösegeldforderungen umgehen soll und ob man das einzige geschädigte Unternehmen ist.

Hilfe bieten in solchen Situationen die Schweizer Polizeikorps und MELANI. Sämtliche Polizeikorps der Schweiz haben sich im interkantonalen Netzwerk für die Ermittlungsunterstützung in der digitalen Kriminalitätsbekämpfung NEDIK zusammengeschlossen, um bei Cyber-Angriffen rasch gemeinsam reagieren zu können. Dank eines regelmässigen operativen Austauschs in diesem Netzwerk und der unmittelbaren Verbreitung aktueller, neuer Fälle und Fallentwicklungen, erkennen wir Zusammenhänge heute sehr schnell und können – auch aufgrund des engen Austauschs mit MELANI im Ereignisfall – adäquat reagieren und entsprechende Empfehlungen abgeben. Aufgrund der Beteiligung des Bundesamts für Polizei (fedpol) in NEDIK und dessen Zusammenarbeit mit Europol können wir auch bei neuen Ereignissen unmittelbar über die Landesgrenzen hinaus agieren.

---

53 MELANI Halbjahresbericht 2014/2, Kap. 5.3.

54 https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public, https://www.maketecheasier.com/man-arrested-for-spreading-shame-driven-ransomware/

NEDIK bietet einen Mehrwert, aber nicht nur in der Ereignisbewältigung. Zusammen mit MELANI produzieren wir im Rahmen von NEDIK Bulletins zur Lage im Cyber-Bereich und entwickeln gemeinsam Präventionstipps und Strategien zur Verhinderung und Bekämpfung von Cyber-Kriminalität. Diese Best Practices lassen wir sämtlichen Polizeikorps zu-kommen, um allen Betroffenen in sämtlichen Kantonen den bestmöglichen Support zum Schutz vor Cyber-Risiken zu bieten, sei dies im präventiven oder im repressiven Bereich.

Empfehlungen:

MELANI empfiehlt zum Schutz vor Ransomware folgende Massnahmen:

- **Erstellen Sie regelmässig Sicherungskopien (Backups) Ihrer Daten zum Beispiel auf einer externen Festplatte. Nutzen Sie dabei das Generationenprinzip (täglich, wöchentlich, monatlich / mindestens 2 Generationen). Stellen Sie jeweils sicher, dass Sie das Medium, auf welchem Sie die Sicherungskopie erstellen, nach dem Backup-Vorgang vom Computer bzw. Netzwerk physisch trennen. Ansonsten besteht die Gefahr, dass die Angreifer auch auf die Daten des Backups Zugriff erhalten und verschlüsseln oder löschen können.**
- Bei Cloud-basierten Backup-Lösungen sollten Sie sicherstellen, dass der Provider analog zum klassischen Backup mindestens über zwei Generationen verfügt und dass diese für eine Ransomware nicht zugreifbar sind, indem man für kritische Operationen beispielsweise eine *Zweifaktor-Authentifizierung* verlangt.
- Sowohl Betriebssysteme als auch alle auf den Computern oder Servern installierte Applikationen (z. B. Adobe Reader, Adobe Flash, Java usw.) müssen konsequent und unverzüglich auf den neuesten Stand gebracht werden. Falls vorhanden, am besten mit der automatischen Update-Funktion.
- Schützen Sie auch alle vom Internet erreichbaren Ressourcen (insbesondere Terminal-Server, RAS- und VPN-Zugänge) mit einem zweiten Faktor. Stellen Sie Terminal-Server hinter ein VPN-Portal.
- Blockieren Sie den Empfang von gefährlichen E-Mail-Anhängen auf Ihrem E-Mail-Gateway. Dazu zählen auch Office-Dokumente mit Makros.
- Beobachten Sie die Logfiles Ihrer Antivirus-Lösung auf Unregelmässigkeiten.

4 Lage national

4.1 Spionage

4.1.1 Lazarus greift Schweizer Banken an

Im März 2019 hat der Sicherheits-Software-Hersteller McAfee ein Follow-up des Berichts vom Dezember 2018 über die «Sharpshooter»-Kampagne publiziert. Die Kampagne zielte im letzten Jahr auf 87 Unternehmen weltweit, vor allem aber auf Unternehmen in den USA. Die im

Fokus stehenden Firmen waren im Verteidigungs-, Energie-, Nuklear- und Finanzsektor tätig.[55] Im zweiten Bericht bestätigt McAfee den ersten Verdacht: Hinter den Angriffen steckt die «Lazarus»-Gruppe.

«Lazarus» ist dafür bekannt, Systeme von verschiedenen Banken angegriffen zu haben[56] und wird von vielen Experten mit dem nordkoreanischen Regime in Verbindung gebracht.

Bereits im ersten Report berichtete McAfee von Angriffsversuchen gegen schweizerische Finanzinstitute MELANI steht, wie bereits im letzten Halbjahresbericht erwähnt,[57] mit verschiedenen Banken in Kontakt. Es konnten weder damals noch heute Spuren von Infektionen bei potentiell betroffenen Firmen in der Schweiz gefunden werden.

4.1.2 APT40

Die Grundlage der aktuellen Strategie von China, um die geschäftlichen Beziehungen zwischen Asien und Europa zu verbessern, ist die Entwicklung von Logistik- und Verkehrsinfrastrukturen. Der IKT-Sicherheitsdienstleister FireEye hat eine Spionage-Operation entdeckt,[58] die seit mindestens 2013 läuft und gegen Länder gerichtet ist, die für die neue Seidenstrasse (Belt and Road Initiative, BRI) strategisch relevant sind, wozu auch die Schweiz zählt.[59] Hinter dieser Operation steckt die Gruppe «APT40» (auch bekannt als «Leviathan» und «TEMP.Periscope»), bei welcher FireEye eine Verbindung zur chinesischen Regierung vermutet. Die Operation hatte zum Ziel, Informationen zu beschaffen, um die Modernisierung des maritimen Sektors allgemein und der Schiffbaufähigkeiten im Besonderen zu unterstützen.

Die Gruppe verwendet Phishing-E-Mails mit schädlichen Anhängen und *Drive-by-Infektionen*, um den Verteidigungssektor, den Transportsektor und den Schiffstechnologiesektor anzugreifen. Bereits im Jahr 2017, wurde die Identität eines Herstellers von autonomen U-Booten missbraucht, um Universitäten zu infiltrieren, die Forschung im Bereich Schiffbau betreiben. Dieser Sektor ist von fundamentaler Wichtigkeit für die chinesische Regierung, sowohl aus kommerzieller als auch aus Verteidigungssicht.[60] Deshalb ist dieses Forschungsgebiet auch im Visier von anderen Spionagekampagnen, bei welchen ebenfalls Verbindungen zu Peking vermutet werden (siehe auch Kapitel 4.1.4).

Neben Spionagekampagnen im Forschungs- und Industriebereich, führt «APT40» Spionagekampagnen gegen Organisationen in Südostasien durch oder ist involviert in die Territorialkonflikte im Chinesischen Meer. Im Jahr 2018 wurden verschiedene kambodschanische

---

55 MELANI Halbjahresbericht 2/2018, Kap. 4.1.2.

56 https://www.symantec.com/connect/blogs/swift-attackers-malware-linked-more-financial-attacks

57 MELANI Halbjahresbericht 2/2018, Kap. 4.1.2; https://www.tagesanzeiger.ch/sonntagszeitung/nordkorea-greift-schweizer-banken-an/story/15090344

58 https://www.fireeye.com/blog/threat-research/2019/03/apt40-examining-a-china-nexus-espionage-actor.html

59 Zur Belt and Road Initiative siehe http://english.www.gov.cn/beltAndRoad/ und http://english.www.gov.cn/archive/publications/2015/03/30/content_281475080249035.htm

60 Vgl. die Strategie «Made in China 2025» auf http://english.www.gov.cn/2016special/madeinchina2025/; http://en.people.cn/n/2015/0522/c98649-8895998.html

Behörden kompromittiert, welche in die Durchführung der dortigen Wahlen involviert waren.[61] Kambodscha zählt zu den Ländern, die strategisch wichtig sind für die neue Seidenstrasse.

Es wurden bislang keine Spuren von Infektionen bei potentiell betroffenen Firmen in der Schweiz gefunden.

4.1.3 VPN-Filter

Im Mai letzten Jahres hat Talos, die Sicherheitsabteilung des Telekommunikationsunternehmens Cisco, über das Botnetz «VPN Filter» berichtet. Mindestens eine halbe Million Router und *NAS*-Geräte in 54 Staaten, vor allem in der Ukraine, soll das Botnetz umfassen.[62]

Die *Malware* «VPN Filter» verfügt über eine modulare Struktur mit verschiedenen Funktionalitäten. Die Schadsoftware kann beispielsweise ein betroffenes Gerät unbrauchbar machen, ist aber auch in der Lage, sich im Netzwerk auszubreiten und andere Systeme zu infizieren (lateral movement). Die Schadsoftware kann Informationen (insbesondere Zugangsdaten) stehlen und Internetverkehr zu einem anderen Empfänger umleiten. Ferner sucht und überwacht ein Modul allfälligen Modbus-Netzverkehr.[63] Modbus ist ein Kommunikationsprotokoll, dass oft von industriellen Kontrollsystemen verwendet wird.

Das Botnetz von «VPN Filter» hätte auch für Sabotageaktionen genutzt werden können. Das FBI hat jedoch praktisch gleichzeitig mit Bekanntwerden des Botnetzes die Kontrolle über einen Teil der *Command & Control* Infrastruktur übernommen. Aufgrund dieser Massnahme konnten nicht nur die infizierten Geräte identifiziert, sondern auch der Versand von Befehlen der Botnetz-Betreiber an die Geräte verhindert werden.

Obwohl Updates publiziert worden sind, die es Sicherheits-Software erlaubt, die *Malware* zu identifizieren und zu stoppen, hat MELANI Kenntnis von einigen hundert noch aktiven Infektionen in der Schweiz. Um die Schadsoftware zu eliminieren und die Sicherheitslücke zu schliessen, müssen die Geräte auf die Werkeinstellungen zurückgesetzt und danach aktualisiert werden.

Empfehlungen

Die Netzinfrastruktur wird immer häufiger von Cyber-Kriminellen angegriffen. Router und Switches sind lohnende Ziele, weil sie oft direkt mit dem Internet verbunden sind, aber nicht immer genügend geschützt werden. Sie können dementsprechend ein einfaches Einfallstor in ein Heim- oder Betriebsnetzwerk sein.

Jedes Gerät, das direkt mit dem Internet verbunden ist, benötigt einen spezifischen Schutz gegen unerlaubte Zugriffe. Dies beinhalt nicht nur die Verwendung eines starken Passworts sondern auch das schnellstmögliche Einspielen von Updates.

---

61 https://www.fireeye.com/blog/threat-research/2018/07/chinese-espionage-group-targets-cambodia-ahead-of-elections.html

62 MELANI Halbjahresbericht 1/2018, Kap. 5.1.2.

63 https://blog.talosintelligence.com/2019/05/one-year-later-vpnfilter-catastrophe.html

4.1.4 APT10

Im ersten Halbjahr 2019 wurden neue Opfer der Cyberspionagekampagne «APT10» bekannt. Die seit 2006 aktive Gruppe erlangte aufgrund ihrer Operation «Cloud Hopper» Bekanntheit, bei welcher ab 2015 weltweit *Managed Services Provider (MSP)* angegriffen wurden.[64] Das US-Justizdepartement (Department of Justice, DoJ) und die anderen vier Länder der «Five Eyes» haben offiziell Stellung genommen und eine Beteiligung der chinesische Regierung an dieser Spionage-Kampagne angeprangert.[65]

Am 20. Dezember 2018 hat das DoJ zwei chinesische Staatsbürger, welche verdächtigt werden an der Operation «Cloud Hopper» beteiligt gewesen zu sein, des Betruges und des Identitätsdiebstahls beschuldigt. Damals wurden die Namen von zwei grossen IT-Service Provider als Opfer der Spionage-Kampagne genannt: Hewlett Packard Enterprise (HPE) und IBM. Die Vermutung war, dass zumindest im Fall von HPE der Angreifer seit Jahren in deren Netzwerk gewesen war.

Im Juni 2019 hat die Nachrichtenagentur Reuters die Namen von sechs weiteren Opfern von «APT10» publiziert.[66] Es handelt sich um Fujitsu, Tata Consultancy Services, Dimension Data, NTT, Computer Sciences Corporation und DXC Technology. Diese neue Entdeckung erhöhte die Zahl der möglichen Opfer drastisch. Die MSPs sind nämlich nicht das eigentliche Ziel, sondern dienen als Einfallstor in die grossen Unternehmen, deren IKT-Infrastruktur sie betreiben oder unterstützen. Die HPE-Infektion ist zum Beispiel vom Ericsson IKT-Sicherheitsteam entdeckt worden. Der schwedische Telekomunikations-Riese war auf der Suche nach dem Eintrittsvektor verschiedener *Malware*-Infektionen, die sich zwischen 2014 und 2017 ereignet hatten. Es ist unmöglich zu sagen, wie viele Unternehmen durch diesen Vektor infiltriert worden sind. Die Service Provider sind ein sehr vorteilhaftes Ziel, da sie über direkte Zugriffsrechte für die Systeme ihrer Kunden verfügen und teilweise auch Daten für diese bearbeiten.

Die Angriffe zielen darauf ab, geistiges Eigentum zu stehlen. Opfer sind beispielsweise in den Bereichen militärischer Schiffsbau oder nukleare U-Boottechnik tätig. Die Modernisierung der See- und Schiffstechnologie ist von grundlegender Bedeutung für China.[67] Ein weiteres Ziel von Angriffen ist die Überwachung der Konkurrenz: Ericsson konkurriert zum Beispiel mit chinesischen Herstellern im Bereich Mobiltelefonie. Darüber hinaus ermöglicht der Diebstahl vertraulicher, umsatzrelevanter Informationen die Beurteilung, ob ein Unternehmen ein guter Akquisitionskandidat ist.

---

64 MELANI Halbjahresbericht 2/2018, Kap. 5.1.1 und 1/2017, Kap. 5.1.1.

65 https://www.securityweek.com/five-eyes-nations-blame-china-apt10-attacks;
USA: https://www.justice.gov/opa/press-release/file/1121706/download;
UK: https://www.gov.uk/government/news/uk-and-allies-reveal-global-scale-of-chinese-cyber-campaign;
Kanada: https://cse-cst.gc.ca/en/media/media-2018-12-20;
Australien: https://foreignminister.gov.au/releases/Pages/2018/mp_mr_181221.aspx;
Neuseeland: https://www.ncsc.govt.nz/newsroom/cyber-campaign-attributed-to-china/

66 https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/

67 Vgl. die Strategie «Made in China 2025» auf http://english.www.gov.cn/2016special/madeinchina2025/;
http://en.people.cn/n/2015/0522/c98649-8895998.html

Die Spionagekampagne könnte aber mehr als rein kommerzielle Ziele haben. Zwischen den bestätigten Opfern sticht die Firma «Sabre Corp.» hervor. Diese verwaltet die Reservationssysteme für tausende Hotels in der ganzen Welt, wie auch die Flugtickets von hunderten Fluggesellschaften. Obwohl es keinen Datenabfluss von Reiseinformationen gegeben haben soll, hätten die Angreifer über diesen Kanal Informationen zu Reisebewegungen von sehr vielen Personen beschaffen können.

In dem vom DoJ herausgegebenen Dokument wurde unter den Staaten, in denen Organisationen angegriffen wurden, auch die Schweiz genannt. Obwohl es keine konkreten Beweise von Infektionen bei Organisation mit Sitz in der Schweiz gab, sind Akquisitionskandidaten grundsätzlich immer als mögliche Ziele von Cyberspionage zu betrachten.

4.2 Industrielle Kontrollsysteme

Die Annehmlichkeiten des modernen Lebens werden in vielen Fällen erst durch industrielle Kontrollsysteme ermöglicht. Dafür, dass der Strom der Turbinen der Staudämme zuverlässig an unserer heimischen Steckdose zur Verfügung steht, sind unter anderem die Kontrollsysteme der lokalen Stromverteiler zuständig. Wie diese kleinen und mittleren Elektrizitätsversorgungsunternehmen (EVU) in Sachen Informationssicherheit gerüstet sind, wird anhand einer Studie in Kapitel 4.2.1. beleuchtet. Auch auf Reisen unterstützen überall Kontrollsysteme die schnelle und komfortable Ankunft am Zielort. Die Herausforderungen, die es z. B. bei der instrumentenunterstützten Landung zu bewältigen gilt, wird in Kapitel 4.2.2. erörtet.

4.2.1 Hausaufgaben für kleine und mittlere EVU

In der Stromversorgung machen meist Vorkommnisse mit Kraftwerken, Staudämmen oder Hochspannungsleitungen Schlagzeilen. Für den Endkunden ist jedoch der lokale Verteiler meist entscheidender für die Zuverlässigkeit der eigenen Stromversorgung. Wie es um die Cyber-Sicherheit dieser kleinen und mittleren Elektrizitätsversorgungsunternehmen (EVU) steht, hat der Fachverband Electrosuisse in einer Studie[68] untersucht.

Die Untersuchungen zeigen, dass Cyber-Sicherheit zwar bei allen Unternehmen Beachtung findet, jedoch der Umsetzungsstand und die systematische Herangehensweise von Massnahmen zur Gewährleistung der Informationssicherheit, speziell bei kleineren Werken, noch Ausbaupotential bietet. Angelehnt an das NIST Cybersecurity Framework[69] erkannte die Studie einen Fokus auf präventive Schutzmassnahmen, jedoch eine Vernachlässigung der weiteren Elemente des Frameworks.

Vielerorts wurde eine unvollständige Inventarisierung (Asset Management), wie auch mangelnde Visibilität im Netzwerk festgestellt. Zusammen mit der niedrigen Reaktionsbereitschaft und den fehlenden Notfallübungen stellen sich grosse Herausforderung in der Detektion und Bewältigung von Vorfällen. In übergeordneten organisatorischen Belangen wurde eine zu geringe Berücksichtigung der Risiken in der Priorisierung von Massnahmen und Budgetierung attestiert. Dabei spielen vernachlässigte Lieferantenrisiken und der Umgang mit dem Faktor

68 https://www.electrosuisse.ch/wp-content/uploads/2019/03/Electrosuisse_Cybersecurity-Erhebung-EVU_.pdf

69 https://www.nist.gov/cyberframework

Mensch als Schwachstelle eine Rolle. Bedingt werden diese Schwachstellen häufig durch fehlende Fachkompetenz und Ressourcen, vor allem bei den kleinen Studienteilnehmern, was auch darin resultiert, dass die Cyber-Sicherheit nicht aktiv als Prozess geführt wird.

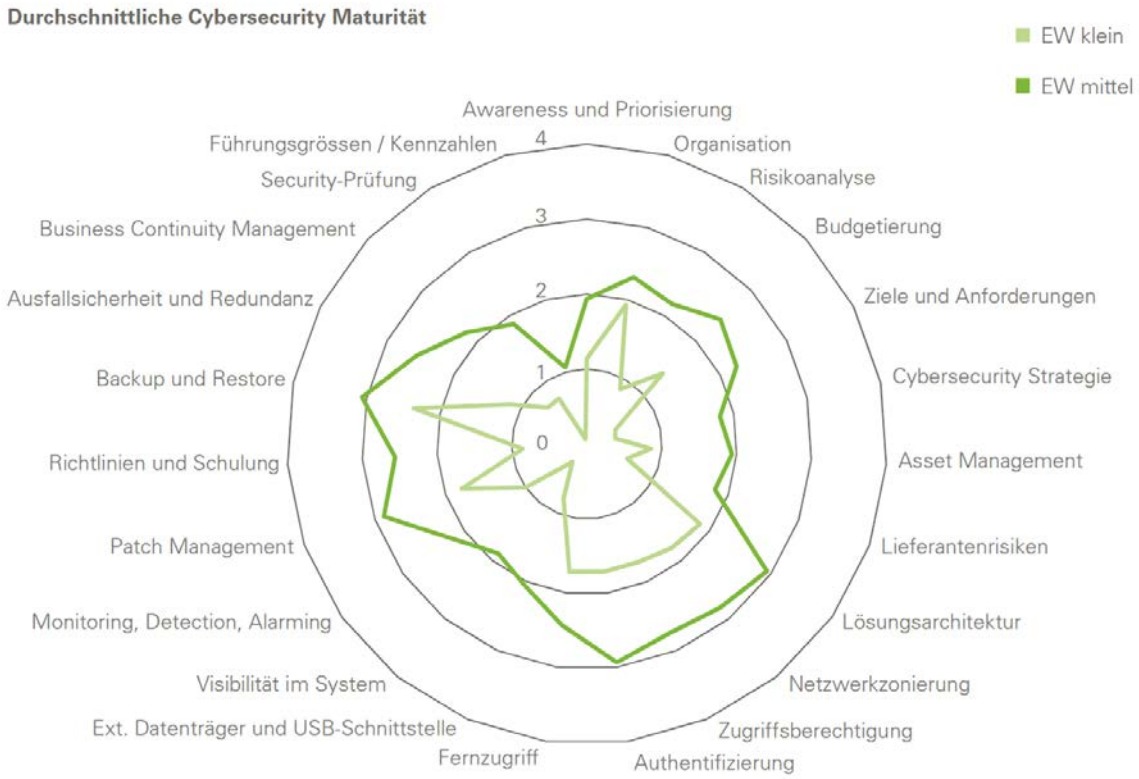

Abbildung 1: Übersicht der Studienresultate in den untersuchten Bereichen der Cyber-Sicherheit.

Ein Ansatz, wie kleine und mittlere EVU diese Lücken schliessen können, ist Kooperation in den Bereichen, die für alle Unternehmen identisch sind. Ein begrüssenswertes Projekt in dieser Hinsicht ist die firmenübergreifende Initiative zur Kooperation in der Cyber-Sicherheit einer Allianz von Stadtwerken.[70] Dank dem Netzwerk können alle Kooperationspartner von den Erfahrungen der anderen profitieren und gemeinsam das Niveau der Informationssicherheit ständig anheben.

4.2.2 Steiler als angezeigt – Störung des Instrumentenlandesystems möglich

Beim Landeanflug auf die meisten zivilen Flughäfen der Welt wird der Pilot durch ein Instrumentenlandesystem (engl. instrument landing system, ILS) unterstützt. Diese Systeme wurden in einer Zeit entworfen, in der die verwendete Funktechnologie nur für einen kleinen Anwenderkeis verfügbar oder erschwinglich war. Unter diesen, früher isolierten, Rahmenbedingungen waren kryptografische Sicherungs- und Authentisierungsmassnahmen nicht prioritär. An der vergangenen Usenix[71]-Konferenz demonstrierten Forscher der Northeastern Universität aus Boston eine kostengünstige Methode, um Funksignale eines ILS zu fälschen und so einem

[70] https://swisspower.ch/medien/medienmitteilungen/swisspower-lanciert-kooperation-für-cybersecurity-in-stadt-werken

[71] https://www.usenix.org/

Flugzeug eine falsche Ausrichtung anzuzeigen.[72] Das im Forschungspapier[73] beschriebene Gerät verwendet kommerziell erhältliche Komponenten, um ILS-Signale vorzutäuschen. Für einen erfolgreichen Angriff wird es entweder im Flugzeug oder in einem Umkreis von drei Meilen der angesteuerten Landebahn platziert. Voraussetzung ist, dass das gefälschte Signal beim Flugzeug die höhere Signalstärke als die legitime Kommunikation des Flughafens aufweist, damit das Flugzeug den Empfänger auf das Angriffssignal ausrichtet.

Ähnlich gelagerte Probleme sind auch bei weiteren funkbasierten Navigationshilfen wie GPS bekannt (siehe auch Kapitel 5.2.2). Da Piloten auch den Ausfall oder Fehlfunktionen des ILS trainieren, sollten sie auf einen solchen Angriff adäquat reagieren können. Wird dieser Ansatz jedoch künftig weiter ausgefeilt und angewandt, könnten solche Angriffe Beeinträchtigungen bei Flügen und Flughäfen verursachen, ähnlich den Konsequenzen, als unerlaubt operierende Drohnen im Dezember 2018 den Londoner Flughafen Gatwick lahmlegten.[74]

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 Distributed Denial of Service – DDoS

In der Berichtsperiode wurden MELANI wiederum mehrere *DDoS*-Angriffe gemeldet. Dies zeigt, dass verschiedene Akteure diese Methode weiterhin anwenden, um die Systeme ihrer Ziele unzugänglich zu machen. Es kann sich dabei um rein kriminelle Erpressungsversuche

[72] https://arstechnica.com/information-technology/2019/05/the-radio-navigation-planes-use-to-land-safely-is-insecure-and-can-be-hacked/

[73] https://aanjhan.com/assets/ils_usenix2019.pdf

[74] MELANI Halbjahresbericht 2018/2, Kap. 5.2.3.

handeln oder um Aktivisten, welche Unternehmen oder Organisationen schaden wollen. Daneben gibt es auch Fälle, in welchen die Motivation nicht geklärt werden konnte. Es kann angenommen werden, dass die Angreifer manchmal ihre Infrastruktur an zufällig ausgewählten Opfern testen.

Empfehlung:

MELANI empfiehlt verschiedene präventive und reaktive Massnahmen, um mit *DDoS*-Angriffen umzugehen.

Checkliste mit Massnahmen gegen DDoS-Attacken

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

4.3.2 Website-Hacks

Weiterhin werden regelmässig legitime Websites kompromittiert und für kriminelle Zwecke mitverwendet. Hacker erlangen meistens durch eine veraltete Version eines Content Management Systems (CMS) oder durch gestohlene FTP-Zugangsdaten Zugriff auf die Websites und platzieren dann Schadsoftware oder eine Phishing-Seite. Wenn MELANI solche Fälle feststellt, werden die Betreiber der Seite informiert, damit sie das Problem anhand unserer Anleitung[75] beheben können.

Empfehlung:

Prävention ist besser als Reaktion: Wenn Sie ein CMS wie z. B. Typo3, Wordpress oder Joomla verwenden, empfiehlt MELANI einen Blick auf die Checkliste «Massnahmen zum Schutz von Content Management Systemen (CMS)» zu werfen, damit Sie Ihre Website angemessen schützen können.

Checkliste mit Massnahmen zum Schutz von Content Management Systemen (CMS)

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

75 https://www.melani.admin.ch/webseitenbereinigung

4.3.3 Domain-Grabbing – Wenn ein Schützenverein plötzlich Schuhe verkauft oder eine politische Kampagne gefälschte Accessoires bewirbt

Nicht wirklich ein Angriff sondern eine Ausnützung des Systems stellen Übernahmen von nicht mehr verlängerten Domainnamen dar. So genannte Domain-Grabber beobachten, welche Domainnamen ausgelaufen sind und registrieren diese nach dem Ablauf der Karenzfrist für sich. Vielfach werden dann betrügerische Webshops auf diesen Domains platziert[76] – es werden jedoch verschiedene Geschäftsmodelle mit diesen frisch «abgelaufenen» Domains verfolgt. Die Domains profitieren, zumindest kurzfristig, von der guten Reputation, die durch die ehemaligen Domainbesitzer über Jahre aufgebaut wurde. Da meistens noch Links von Drittseiten auf die Domain bestehen, sind die Domains teilweise bei Internet-Suchmaschinen weiterhin sehr weit oben auf der Resultatliste zu finden.

Empfehlung:

Domainnamenregistrierungen müssen regelmässig erneuert werden. Wenn Sie eine Website haben, sollten Sie die entsprechenden Fristen im Auge behalten, damit Sie Ihren Domainnamen nicht unverhofft verlieren. Auch das beabsichtigte Stilllegen einer Website sollte geplant werden. Es ist nicht teuer und kann sinnvoll sein, eine Domain kontrolliert herunterzufahren. Das heisst, sie noch eine gewisse Zeit weiter zu betreiben, um alle möglichen Besucher darauf hinzuweisen, dass die Web-Päsenz eingestellt wurde. Zudem kann eine Auswertung der *Referrer* dabei helfen, andere Website-Betreiber zu informieren, die auf die Domain verlinken. Schliesslich geht es darum, den Ruf wie auch die Kunden und Sympathisanten der mit der Website assoziierten Entität zu schützen, sei dies ein Unternehmen, ein Verein, eine Privatperson oder sonst eine Interessensgemeinschaft.

4.4 Social Engineering und Phishing

Basis für einen guten Angriff ist eine glaubwürdige Geschichte, die das potenzielle Opfer veranlasst, etwas zu tun. Sogenannte *Social Engineering*-Angriffe funktionieren am besten, wenn der Angreifer viele Informationen über das potenzielle Opfer zusammentragen kann. Die Betrüger nutzen dabei sowohl frei verfügbare Quellen, als auch Informationen, die aus Datendiebstählen stammen. Gestohlene Daten werden gesichtet, mit anderen gestohlenen oder öffentlichen Daten verknüpft, aufbereitet und dann an andere Kriminelle weiterverkauft. Aus diesen Daten können Einzelangriffe massgeschneidert oder auch automatisiert personalisierte Massen-E-Mails (*Malspam*) erstellt werden.

4.4.1 Phishing

Die bei MELANI gemeldete Zahl von Phishing-Versuchen hat im ersten Halbjahr 2019 zugenommen. Es wurden 2'521 verschiedene als Phishing einzustufende URLs gemeldet und an die verschiedenen Organisationen weitergegeben, die Phishing bekämpfen (Browser-Hersteller, Anti-Phishing-Organisationen, betroffene Hosting-Provider). Die Ziele der Angreifer blie-

[76] In der Schweiz wird dieses Phänomen seit 2016 vermehrt beobachtet. SWITCH, die Registerbetreiberin für «.ch»-Domains, geht seither sehr effektiv dagegen vor. Andere Länderdomains hinken klar hinterher: https://www.nzz.ch/digital/kampf-gegen-fake-shops-im-netz-ld.1484852

ben sich im Wesentlichen gleich: Einerseits wurde versucht, Kreditkartendaten zu stehlen, andererseits Benutzername/Passwörter von Internetdiensten wie Paypal, Spotify oder Apple zu erhalten. Immer häufiger richten sich Phishing-Versuche gegen E-Mail-Konten, da diese für weitere Angriffe genutzt werden können. Als relativ neue Angriffsmethode ist das sogenannte «Real Time Phishing» (Phishing in Echtzeit, siehe Kapitel 4.4.2) dazu gekommen.

Abbildung 2: Gemeldete und bestätigte Phishing-Seiten pro Woche auf antiphishing.ch im ersten Halbjahr 2019

Einen Teil der Zunahme lässt sich erklären durch grosse Phishing-Wellen mit dem Ziel, Kreditkarteninformationen zu stehlen.

4.4.2 Real Time Phishing gegen PostFinance und UBS

Die häufigste Vorgehensweise bei Phishing ist, dass Angreifer Zugangsdaten in grossem Stil sammeln und erst einige Stunden oder Tage später dazu verwenden, sich im Konto des Opfers anzumelden. Häufig werden die gestohlenen Zugangsdaten auch weiterverkauft. Dieses Vorgehen funktioniert jedoch nicht, wenn der Benutzer einen zweiten Faktor für die Authentisierung verwendet (z. B. ein Einmalpasswort, engl. One Time Password, OTP). Die Antwort der Angreifer auf den häufigeren Einsatz von OTPs ist das «Real Time Phishing» (dt. Phishing in Echtzeit). Dies bedingt, dass der Angreifer sofort aktiv wird, wenn das Opfer auf den Phishing-Link im Mail klickt und so auf den Webserver des Angreifers geleitet wird.

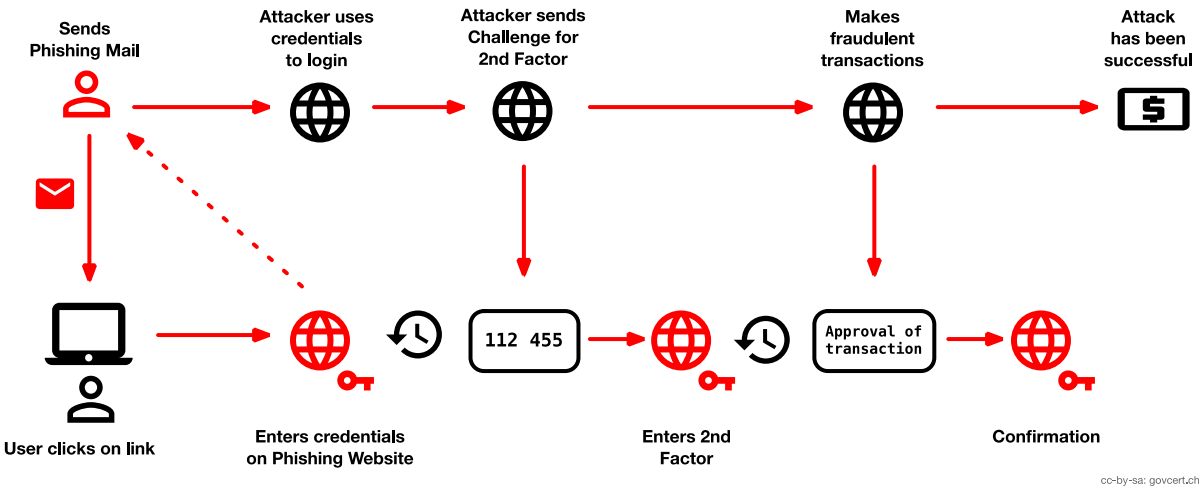

Abbildung 3: Ablaufschema eines Real Time Phishing Angriffs

Der Angreifer präsentiert eine perfekt gefälschte Login-Seite, bei welchem sich das Opfer zu authentisieren versucht. Der Angreifer zeichnet diese Daten auf und verwendet sie, um sich selbst bei der echten E-Banking-Plattform anzumelden. Nun wird der Angreifer von dieser aufgefordert, sich mit einem zweiten Faktor auszuweisen. Er zeigt nun dem Benutzer dieselbe Aufforderung auf dem gefälschten Webserver. Sobald der Benutzer auch den 2. Faktor eingegeben hat, erhält der Angreifer Zugang zum E-Banking-Portal, während er den Benutzer mit einer Fehlermeldung vertröstet.

Im Berichtszeitraum wurden zwei solche Kampagnen beobachtet, welche sich gegen Kunden von Schweizer Finanzinstituten gerichtet haben.

4.4.3 Social Media-Konten sind wertvoll

Nicht nur E-Mail-Konten und Kreditkarteninformationen werden gephisht. Jegliche Online-Konten sind gefährdet. Während mit einem gekaperten Twitter-Konto eine Desinformationskampagne gefahren werden kann, die den rechtmässigen Nutzer in schlechtem Licht dastehen lässt, können gehackte Instagram-Profile[77] oder Youtube-Konten für die betroffenen Personen auch finanzielle Einbussen bedeuten. Die «gesammelten» Abonnenten und Follower sind das Kapital von Influencern. Wenn sie die Kontrolle über ihren Online-Auftritt verlieren, müssen sie von vorne beginnen und ihre Community neu aufbauen. Zudem können sie in der Zwischenzeit keine Inhalte online stellen und somit entgehen ihnen Einnahmen. Der Verlust der Kontrolle über ein Online-Konto hat nicht nur für prominente Persönlichkeiten Konsequenzen. Das Leben von immer mehr Menschen findet zumindest teilweise auf den Social Media-Plattformen statt. Wer den Zugang beispielsweise zum Facebook-Konto verliert, hat vielleicht kurzfristig tatsächlich Probleme, Kontakte zu pflegen.

Empfehlung:

Es ist wichtig, Online-Konten so gut wie möglich zu schützen, z. B. mit einer *Zwei-Faktor-Authentisierung*. Verwenden Sie komplexe und verschiedene Passwörter für jedes Konto.

Beschäftigen Sie sich schon vorgängig mit den Sicherheitsmassnahmen der Anbieter sowie allfälligen Prozessen, mit welchen die Kontrolle über ein gehacktes Konto zurückerlangt werden kann.

4.4.4 Kleine Bildschirme erhöhen Täuschungsrisiko

Smartphones sind kleine Computer. Viele Menschen erledigen einen grossen Teil ihrer Kommunikation damit. Das Organisieren von Terminen läuft häufig über die Kalender-App des Smartphones. Eine grosse Herausforderung für App-Programmierer besteht darin, möglichst alle relevanten Informationen auf dem relativ kleinen Bildschirm auf ansprechende Weise darzustellen. Dies führt häufig dazu, dass Hintergrundinformationen wie die vollständige Adresse eines Links oder die hinter einem (notabene vom Absender frei wählbaren) Anzeigenamen verborgene E-Mail-Adresse nicht einfach erkennbar oder schwer zugänglich sind. Die Reduktion auf das Wesentliche ist im normalen Umgang mit dem Smartphone sinnvoll und nützlich. Jedoch bietet dies Kriminellen auch viele Möglichkeiten, Empfänger von E-Mails und anderen

[77] https://blog.trendmicro.com/trendlabs-security-intelligence/how-a-hacking-group-is-stealing-popular-instagram-profiles/

Nachrichten zu täuschen. Neben dem Versand von betrügerischen E-Mails, SMS und anderen Kurznachrichten, können je nach Einstellungen des Smartphones und der Apps auch Terminanfragen[78] automatisch eingefügt, sowie Notifikationen und weitere Kommunikation auf dem Bildschirm zum aufpoppen gebracht werden.

Empfehlung:

Lassen Sie sich in der Smartphone-Umgebung nicht von unerwarteten Nachrichten überlisten, auch wenn diese auf einem regulären Kanal und in einem vertrauten Format daherkommen. Überlegen Sie sich immer zuerst, ob eine Mitteilung nicht auch von jemandem kommen könnte, der Sie bloss zu unbedachtem Klicken verleiten will. Verdächtige Nachrichten sollten unbesehen gelöscht werden. Prüfen Sie die Einstellungen Ihres Smartphones und der Apps, dass z. B. nur akzeptierte Terminanfragen in den Kalender eingefügt werden und Ihre Privatsphäre angemessen geschützt ist.

4.4.5 CEO-Betrug hält sich hartnäckig

Über *CEO-Betrug* (CEO Fraud) hat MELANI erstmals 2013 berichtet.[79] Die Masche ist nicht neu, hält sich aber hartnäckig. Verschiedene Organisationsarten sind weiterhin systematisch Ziel solcher Angriffe. Derzeit sind dies neben Privatunternehmen vor allem Sport- und andere Vereine sowie Gemeinden. Auf ihren Websites sind häufig alle Informationen vorhanden, die die Betrüger für ihren Angriff benötigen. Organigramme enthalten die Namen und E-Mail-Adressen der Personen in den verschiedenen Funktionen wie z. B. Vereins- oder Gemeindepräsidenten, Kassiere und Finanzverantwortliche. Das klassische Vorgehen beim *CEO-Betrug* besteht aus einem Mail, in dem sich die Betrüger als Präsident ausgeben und den Finanzverantwortlichen mit unterschiedlicher Begründung auffordern eine Überweisung vorzunehmen.

Von: [gefälschte Adresse des Vereinspräsidenten]
Gesendet: Dienstag, 19. März 2019 14:00
An: [Kassierin des Vereins]
Betreff: ANFRAGE

Hallo Corinna,
Ich möchte, dass du eine Überweisung machst. Lass mich wissen, ob du es sofort tun kannst, damit ich dir die Bankverbindung schicken kann.
Warten auf Ihre Antwort

Grüß
[Name des Präsidenten]

Von meinem iPhone gesendet

Mail 1: Der Betrüger gibt sich als Präsident aus und fordert die Kassierin zu einer dringenden Überweisung auf.

[78] MELANI Halbjahresbericht 2018/1, Kap. 4.4.4.
[79] MELANI Halbjahresbericht 2013/1, Kap. 3.4.

Hallo Corinna,

[Bankverbindung eines ausländischen Kontos]

Informieren Sie mich, wenn es erledigt ist.

Grüß
[Name des Präsidenten]

Von meinem iPhone gesendet

Mail 2: Nach der Antwort schickt der «Präsident» die Kontonummer für die Überweisung ins Ausland.

Dank der online leicht zugänglichen Informationen haben die Betrüger die Sendungen automatisiert und dabei offenbar die Qualitätskontrolle etwas vernachlässigt – teils mit kuriosen Folgen. In kleinen Vereinen oder Gemeinden kann der Vereins- respektive der Gemeindepräsident auch für die Finanzen zuständig sein. Beide Funktionen haben somit die gleiche Mail-Adresse. So wurde MELANI ein Fall gemeldet, bei dem die Kassierin einer Gemeinde, die gleichzeitig Gemeindepräsidentin ist, ein Mail - angeblich vom Gemeindepräsidenten - von ihrer eigenen Mail-Adresse erhalten hat. Dieses Beispiel zeigt, dass die Betrüger die nötigen Informationen für einen Angriff von frei zugänglichen Quellen (Firmenwebsite, soziale Netzwerke) beziehen.

Empfehlung:

MELANI empfiehlt, immer wieder zu prüfen, was für Informationen über Personen, Vereine, Unternehmen, usw. online zugänglich sind und ob sie dies auch sein sollen. Weitere Schutzmassnahmen sind die Sensibilisierung des Personals und genaue Prozessvorgaben, insbesondere bezüglich Zahlungen.

INFO

Informationen und Empfehlungen bezüglich CEO-Betrug:

https://www.melani.admin.ch/melani/de/home/themen/CEO-Fraud.html

4.4.6 Malspam: Einschüchterungen und Neugierde wecken zwecks Malware-Verbreitung

Internetkriminelle erfinden immer wieder neue Szenarien, um E-Mail-Empfänger zu verleiten auf einen Link zu klicken oder eine angehängte Datei zu öffnen. Der Fantasie sind keine Grenzen gesetzt. Im ersten Halbjahr 2019 wurde mit teilweise haarsträubenden Geschichten versucht, Nutzer dazu zu bringen, sich eine Schadsoftware zu installieren:

Kostenpflichtiges Abonnement: In einem sehr kurz gehaltenen E-Mail wurde den Empfängern gedankt, dass sie ein kostenpflichtiges Abonnement bei einer bestimmten Zeitung oder Zeitschrift abgeschlossen hätten. Die Zahlungsdetails und Nutzungsbedingungen seien im angehängten Dokument ersichtlich. Um die Empfänger zu überlisten, waren Vor- und Nachname in die Betreffzeile des E-Mails eingefügt.

Klagen gegen ehemalige Kunden: Nachdem bei einer kleinen Firma die Kundendatenbank gehackt worden war, erhielten alle darin verzeichneten Adressaten ein Mail mit persönlicher Anrede, dass sie gegen Vertragsbedingungen verstossen hätten und eine Schadenersatzklage eingereicht werde. Für Details wurde auf das angehängte Dokument verwiesen. Die Absenderadresse war nicht gefälscht, jedoch wurde als Anzeigename für die Absenderadresse derjenige der Firma gewählt, um unachtsame Empfänger zu täuschen.

Klagen gegen Gastronomiebetriebe: In einem E-Mail wurde behauptet, dass eine Familienangehörige nach einem Restaurantbesuch eine Lebensmittelvergiftung erlitten habe und das Lokal eingeklagt werde. In diesen Fällen diente das E-Mail nur als erste Kontaktaufnahme. Wer antwortete, erhielt ein E-Mail mit einem Link, hinter welchem sich *Malware* verbarg. Auf diese Weise verbreiten die Kriminellen ihre schädlichen Programme nicht breit, sondern sehr gezielt bei Personen, die auf die initiale Kontaktaufnahme reagiert haben. Dies hat zwei Vorteile: Zum einen wird die *Malware* nicht breit gestreut und fällt somit Sicherheitsakteuren wie Antiviren-Herstellern weniger schnell auf. Zum anderen ist die Wahrscheinlichkeit, dass die Empfänger auf den Link klicken grösser, da sie bereits mit dem Absender in Kontakt waren und das E-Mail entsprechend erwartet wurde.[80]

Hilfe für ein eingesperrtes Mädchen: In einem E-Mail bat ein vermeintlich in einem Keller von einem Peiniger angekettetes Mädchen die Empfänger, ihre Eltern zu informieren, damit sie gerettet würde. Alle Angaben seien im angehängten Dokument ersichtlich.

Bestellte und bezahlte Sterbehilfe: Bei einer ganz pietätslosen Masche wurden die Empfänger informiert, dass die Sterbehilfe-Prozedur auf ihren Namen bestellt und bezahlt worden sei. In drei Tagen würden sie von den Krankenpflegern an ihrer Heimadresse abgeholt. Die Begleitdokumente seien im Attachment zum E-Mail. Auch hier wurden die Empfänger persönlich mit Namen angeschrieben und zudem wurde ihre korrekte Postadresse angegeben.

Schlussfolgerung / Empfehlung:

All diesen Vorgehensweisen gemein ist, dass die Empfänger durch mehr oder weniger glaubwürdige Behauptungen dazu gebracht werden sollten, vorschnell einen Link anzuklicken oder eine Datei zu öffnen um «mehr Informationen» zu erhalten. Die E-Mails waren fast durchwegs personalisiert, d. h. die Empfänger wurden mit Namen angesprochen und teilweise war auch die Wohnadresse oder die Telefonnummer angegeben. Die entsprechenden Daten stammten typischerweise aus Datenabflüssen bei Webshops oder aus gehackten Adressbüchern von Nutzerinnen und Nutzern.

Eine persönliche Anrede wie auch die Nennung des Wohnortes oder der Telefonnummer sind kein verlässlicher Hinweis, dass eine Nachricht von einem legitimen Absender stammt. Seien Sie skeptisch, wenn Sie E-Mails erhalten, die eine Aktion von Ihnen verlangen und ansonsten mit Konsequenzen drohen (Geldverlust, Strafanzeige oder Gerichtsverfahren, Konto- oder Kartensperrung, verpasste Chance, Unglück), insbesondere wenn Dringlich-

[80] In der Fachpresse wurden Restaurants vor dieser Masche gewarnt: https://www.hotellerie-gastronomie.ch/de/artikel/achtung-ein-gastro-schreck-geistert-herum/ (vom 19.3.19); https://www.baizer.ch/aktuell?artID=6788&lvl=2 (vom 9.4.19); https://www.onlinewarnungen.de/warnungsticker/e-mail-lebensmittelvergiftung-trojaner-im-anhang-enthalten/ (vom 21.5.19).

keit geltend gemacht wird. Klicken Sie in verdächtigen E-Mails auf keine Anhänge und folgen Sie keinen Links – auch nicht aus reiner Neugier. Sie riskieren sonst Ihr Gerät mit Schadsoftware zu infizieren oder auf dubiosen Websites zu landen. Fragen Sie im Zweifelsfall beim vermeintlichen Absender über eine auf seiner Website angegebene oder anderweitig bereits bekannte Kontaktmöglichkeit nach, worum es sich genau handelt und ob das Mail tatsächlich von ihm stammt.

4.4.7 Wieder einmal Erpressungsversuche in Namen des EJPD

In den Jahren 2011 und 2012 trieben Online-Erpresser erstmals im grossen Stil ihr Unwesen. Damals wurde meist entweder der Browser oder der ganze Computer gesperrt und im Namen von Strafverfolgungsbehörden oder Urheberrechtsverwertungsgesellschaften behauptet, dass der Nutzer illegales pornographisches Material verbreitet oder unberechtigt Musik und Filme geteilt habe.[81] Diese Masche wurde mehrheitlich von Verschlüsselungstrojanern abgelöst,[82] jedoch noch nicht vollständig aufgegeben, wie das folgende Beispiel zeigt. Die Kriminellen haben zwar das neue Layout der Bundes-Website adaptiert, die sprachliche Ausdrucksweise erinnert jedoch eher an die früheren Phishing-Nachrichten und Betrugsversuche, welche durch ihre Grammatikfehler und Inkonsistenzen bei der Mehrsprachigkeit klare Hinweise darauf geben, dass die angezeigte Seite nicht von einer Schweizer Behörde stammen kann. Im aktuellen Fall wurde der Computer nicht mit *Malware* infiziert. Die Kriminellen versuchten durch blosse Einschüchterung, die betroffenen Personen zur Zahlung zu bewegen. Die Polizei würde jedoch niemals einen Computer sperren, um auf diese Weise Bussen oder Geldstrafen einzutreiben.

Abbildung 4: Sperr-Webseite mit Bundeslogo

[81] Siehe Halbjahresbericht 2011/2, Kap. 3.5 und 2015/2, Kap. 4.5.2.

[82] Siehe dazu das Schwerpunktthema Ransomware in Kapitel 3 oben.

4.4.8 Fake-Sextortion: Immer noch tappen viele in die Falle

Im ersten Halbjahr 2019 gab es wiederum Fake-Sextortion-E-Mails, in welchen die Absender behaupten, den Computer des Empfängers gehackt und den Empfänger beim Masturbieren gefilmt zu haben. MELANI hat im Februar 2019 dazu einen Newsletter[83] publiziert und zusammen mit den Kantonspolizeien und weiteren Partnern eine Website[84] lanciert, um die Bevölkerung bezüglich diesem Thema zu sensibilisieren. Leider bezahlen immer noch viele Leute das Lösegeld und wissen nicht, dass die Behauptungen in den E-Mails haltlos sind. Auf der Website stop-sextortion.ch wird auch kurz beschrieben, wie vorgegangen werden soll, sollten die Erpresser tatsächlich kompromittierendes Material besitzen (wenn z. B. vorgängig ein Video-Chat stattgefunden oder das Opfer selbst Nacktbilder versendet hat).

Es wurden diverse Wellen von Fake-Sextortion-E-Mails auf Englisch, Deutsch, Französisch und sogar einige auf Italienisch beobachtet. Die meisten waren sprachlich ziemlich korrekt geschrieben. Einige schienen weiterhin nur rudimentär übersetzt und die Behauptungen wenig stichhaltig.

Insgesamt wurden MELANI im Zeitraum von 6 Monaten 4'565 verschiedene Bitcoin-Adressen gemeldet. Die beobachteten Einzahlungen beschränkten sich auf wenige Adressen; auf den meisten erfolgte keine Transaktion. Insgesamt gingen 283 Bitcoins ein (Gegenwert Ende Juni 2019 circa 2.8 Millionen Franken). Es handelt sich dabei nicht nur um Zahlungen aus der Schweiz da es sehr schwierig ist nachzuweisen, wer die Einzahlungen von wo aus getätigt hat. Nichtsdestotrotz zeigen diese Zahlen, dass immer noch Geld überwiesen wird, auch wenn das Phänomen schon längere Zeit bekannt ist.

Im internationalen Kontext publizierte das Internet Storm Center von SANS Analysen der ihnen gemeldeten Bitcoin-Adressen, welche für Fake-Sextortion verwendet wurden.[85] Sie haben 434 Bitcoin-Adressen analysiert. Nur auf 56 Adressen wurde jemals eingezahlt. Für einige Zeit lag das Geld still. Bevor es ausbezahlt wird, legen die Angreifer das Geld auf konsolidierten Konten an. SANS identifizierte zwei dieser konsolidierten Bitcoin-Adressen, eine mit 6'190 Bitcoin (Gegenwert Ende Juni 2019 circa 62 Millionen Franken) und die andere mit 5'312 Bitcoin (Gegenwert Ende Juni 2019 circa 53 Millionen Franken) darauf. Der Autor des SANS-Artikels vermutet allerdings, dass es nur der Beginn des sogenannten Cash-Outs ist und dass der tatsächliche Betrag die oben genannten um ein Vielfaches übersteigt. Um das Cash-Out erfolgreich durchzuführen, werden die Bitcoins in kleinere Beträge aufgeteilt, um das Geld effektiver in einem Bitcoin-Mixer mischen zu lassen, und so die Nachvollziehbarkeit zu verunmöglichen.

---

83 https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/fake-sextortion.html

84 https://www.stop-sextortion.ch/de/index.html

85 https://isc.sans.edu/forums/diary/Sextortion+Follow+the+Money+Part+3+The+cashout+begins/24592/; https://isc.sans.edu/forums/diary/Sextortion+Follow+the+Money+The+Final+Chapter/25204/

Empfehlung:

Sofern Sie den Absender des Erpressungs-E-Mails nicht persönlich kennen und keine vorherige Chat-Beziehung stattgefunden hat, empfehlen wir Ihnen das E-Mail zu ignorieren und zu löschen. Bezahlen Sie auf keinen Fall Lösegeld.

Falls Sie ein solches E-Mail erhalten haben, können Sie zur Prävention beitragen, indem Sie dies in Ihrem beruflichen und persönlichen Umfeld thematisieren. So sensibilisieren Sie Mitarbeitende, Bekannte und Verwandte, damit diese nicht auf diese Betrüger hereinfallen.

Sollte ein vorgängiger Kontakt mit dem Erpresser stattgefunden haben und hat dieser effektiv kompromittierendes Material, so melden Sie sich beim nächsten Kantonspolizeiposten (https://polizei.ch/).

4.5 Datenabflüsse

4.5.1 Swisscom Traffic über China Telecom umgeleitet

Am 6. Juni 2019 wurde während mehr als zwei Stunden ein beachtlicher Teil des europäischen Mobilfunkverkehrs über die Infrastruktur von China Telecom umgeleitet. Der Vorfall ereignete sich aufgrund eines *BGP*-Routen-Lecks[86] beim Schweizerischen Rechenzentrum Safe Host, welches versehentlich über 70'000 Routen aus der Routingtabelle an den chinesischen Internet Service Providern *(ISP)* leitete.

Routen-Lecks führen zu einer Umleitung des Datenverkehr über einen unbeabsichtigten Weg, was eine Überbelastung oder ein «schwarzes Loch»[87] zur Folge haben kann. Daten können entsprechend manchmal nicht übertragen werden und werden fallen gelassen – also gelöscht, ohne ihr Ziel zu erreichen. Auch Verkehrsanalysen und Lauschangriffe sind möglich. Routen-Lecks entstehen meist durch versehentliche Fehlkonfigurationen.

Anstatt das BGP-Leck zu ignorieren, hat China Telecom die Routen umgehend übernommen und den Verkehr einer grossen Zahl von europäischen Mobilfunknetzen über das Netz von China Telecom umgeleitet. Dies erfolgte entgegen der Filterpraxis des Border Gateway Protocols (BGP), das auf ISP-Ebene verwendet wird, um die Leitung von Datenverkehr zu regeln und die Verbreitung von BGP-Lecks zu verhindern.

Zu den am stärksten betroffenen europäischen Netzwerken gehörten Mobilfunkbetreiber in der Schweiz (Swisscom), in Frankreich (Bouygues Telecom, Numericable-SFR) und in Holland (KPN). Die Dauer der Umleitung von über zwei Stunden wird von Experten als relativ lange bewertet. Die globale Kommunikation war dadurch auch erheblich beeinträchtigt, was sich für die Nutzer der betroffenen Mobilfunknetze durch die langsamen Verbindungen zeigte. Einige Server waren während dieser Zeit für die Nutzer gar nicht erreichbar. Nicht geklärt ist, ob die Umleitung des Datenverkehrs beabsichtigt oder ein technisches respektive menschliches Versagen war.

86 https://www.thousandeyes.com/learning/glossary/bgp-route-leak

87 https://de.wikipedia.org/wiki/Black_Hole_Router

Generell wird den Internet Service Providern empfohlen, sich an die BGP-Sicherheitsstandards zu halten, um zu verhindern, dass solche Fehlleitungen des Internetverkehrs überhaupt stattfinden.

4.5.2 IKT-Dienstleister CityComp nach Datendiebstahl erpresst

Im April 2019 drangen Cyber-Kriminelle in das Netzwerk des IKT-Infrastruktur Dienstleisters Citycomp ein.[88] Sie kopierten interne Daten und erpressten die Firma mit der Drohung, die abgefassten Dateien zu veröffentlichen. Die Firma ging nicht auf die Erpressung ein und so publizierten die Angreifer die 516 GB grosse Datensammlung auf extra dafür angelegten Websites. Unter den betroffenen Kunden befinden sich Ableger grosser Namen wie Oracle, Volkswagen oder Airbus. Auch Dateien mit Bezug zu Schweizer Firmen fanden sich im Leck.

Die Cyber-Kriminellen erpressten einzig den Dienstleister und nicht dessen Kunden, da diese nicht für das «schreckliche Sicherheitssystem» der Firma verantwortlich seien. In einer Stellungnahme[89] betonte Citycomp, auf keine Forderungen der Erpresser eingegangen zu sein und für die Vorfallbewältigung mit externen Spezialisten zusammenzuarbeiten. Kunden sowie die relevanten Datenschutzbehörden wurden transparent informiert und Ermittlungen des Landeskriminalamtes Baden-Württemberg sind im Gange.

Empfehlung:

Daten können nicht nur auf eigenen Systemen verloren gehen. Auch bei Zulieferern, Dienstleistern und Kunden lagern teilweise sensible Daten der eigenen Firma. Es lohnt sich vertraglich sicherzustellen, dass auch Ihre Partner ebenbürtige Sicherheitsmassnahmen und Vorgehensweisen in der Vorfalls-Bewältigung umsetzen, wie sie es in Ihrem eigenen Betrieb handhaben. Dies kann einen zusätzlichen Kontrollaufwand nach sich ziehen, hilft jedoch Überraschungen vorzubeugen.

4.6 Crimeware

Crimeware setzt sich aus den Begriffen Crime oder Criminal und Software zusammen. Es bezeichnet eine Gruppe von Schadsoftware, die für kriminelle Zwecke eingesetzt wird. Die folgenden Grafiken geben keinen vollständigen Überblick über *Malware* in der Schweiz, sondern zeigen die Tendenz im Bereich Crimeware, einerseits durch *Malspam*-Wellen, die MELANI zusammen mit den Security Teams der kritischen Infrastrukturen beobachten, andererseits durch *DNS*-Sinkhole[90] Daten.

Besonders besorgniserregend waren im ersten Halbjahr 2019 die grossen Schäden, welche durch gezielte Ransomware-Angriffe entstanden sind (siehe Schwerpunktthema in Kapitel 3). Dabei wurden Zugangsdaten in Firmen, welche mit Hilfe von «Emotet» gestohlen wurden,

88 https://www.vice.com/en_us/article/d3np4y/hackers-steal-ransom-citycomp-airbus-volkswagen-oracle-valuable-companies

89 https://www.citycomp.de/unternehmen/stellungnahme.html

90 Mit Hilfe von DNS-Sinkholing kann Traffic zu Domains, die für kriminelle Zwecke verwendet werden, auf die Infrastruktur von Sicherheitsorganisationen umgeleitet werden, indem die Domains entsprechend umregistriert werden.

weiterverkauft und von den Angreifern dazu verwendet, einen ersten Zugang ins Firmennetzwerk zu schaffen, von dem aus dann eine laterale Bewegung stattfand.

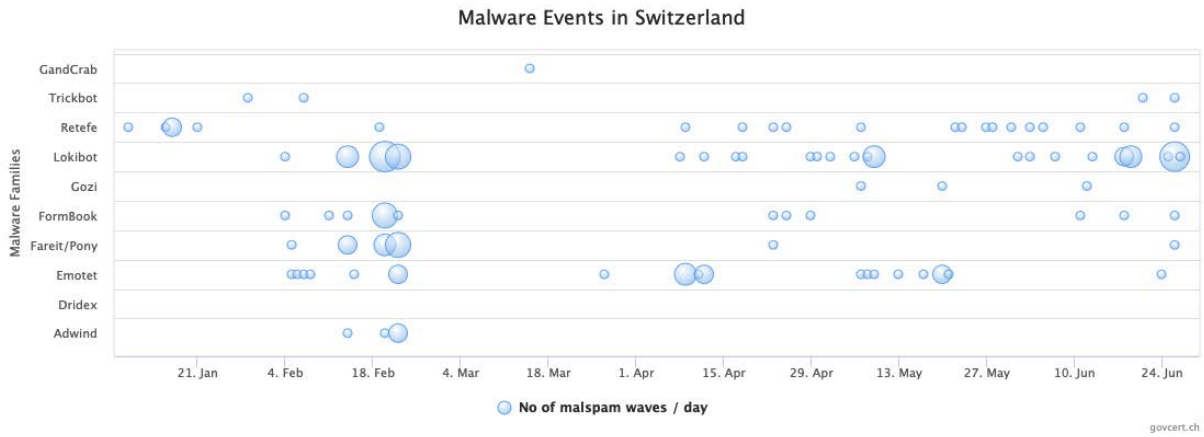

Abbildung 5: Beobachtete Malspam-Wellen

Gut sichtbar ist die grosse Menge an «LokiBot»-Wellen, ebenso die andauernde Aktivität von «Retefe». «Emotet» ist auf der Grafik etwas untervertreten, da MELANI die verschiedenen Wellen nicht einzeln, sondern summarisch nachverfolgt.

«Emotet» wurde im Berichtszeitraum zu einer sehr grossen Bedrohung, da die Angreifer bereits letztes Jahr damit begonnen haben, infizierte Bots in Firmen weiterzuverkaufen. Somit dient «Emotet» als Einfallstor für gezielte Ransomware-Attacken (s. auch Kapitel 3.4.1). «Trickbot» hat zwar keine Schweizer Banken in seinen Konfigurationsdateien, wird aber häufig in einem zweiten Schritt nach der initialen Infektion durch «Emotet» eingesetzt. Dabei kommt dem Angreifer die Modularität von «Trickbot» zu Gute. «Trickbot» verfügt über diverse Module, so z. B. zum Diebstahl von Zugangsdaten oder zur Ausbreitung mit Hilfe der «EternalBlue»-Lücke (Lücke im *SMB-Protokoll*).

Im Berichtszeitraum gab es nebst den gezielten Ransomware-Attacken auch viele Fälle von nicht gezielten Angriffen, welche oft mit «GandCrab» durchgeführt worden sind. Dabei wurden Dateien auf dem Gerät direkt nach dem Ausführen des jeweiligen Attachments verschlüsselt.

«Retefe» war ebenfalls ziemlich aktiv und wurde von den Angreifern über *Malspam*-Wellen mit unterschiedlichen Themen verteilt. Teils richteten sich die Wellen von der Form her eher gegen Unternehmen, teils gegen Endbenutzer.[91] Technisch wurde «Retefe» meist via E-Mail mit einem angehängten Word-Dokument verteilt. Die E-Mails verwendeten oft eine bekannte Marke, um glaubwürdig zu erscheinen. Durch das Einbetten von aktivem Code in den Word-Dokumenten wurden verschiedene Komponenten auf dem Gerät des Opfers installiert, so ein Root-Zertifikat, damit bei dem «*Man-in-the-Middle*»-Angriff keine Zertifikatswarnungen erscheinen, ein *SOCKS* zur Nutzung von Proxy-Diensten und ein Tor-Client zur Umleitung des Verkehrs zu E-Banking-Plattformen. Zusätzlich veränderte «Retefe» auch die Einstellungen im Browser (*Proxy* Settings), damit der Traffic, umgeleitet werden kann. Beim ersten Login-Versuch auf der E-Banking-Plattform versuchte «Retefe» den Benutzer dahingehend zu überlisten, dass dieser sich auf seinem Mobilgerät eine zusätzliche App installierte, welche dazu diente, den zweiten Authentisierungs-Faktor abzufangen.

---

[91] Malwareverbreitung durch Social Engineering, siehe Kapitel 4.4.6 oben.

MELANI sammelt und verteilt Informationen über infizierte Geräte in der Schweiz an Internet Service Provider und kritische Infrastrukturen. Die untenstehende Grafik zeigt die aktuelle Zahl an infizierter Geräten pro *Malware* Familie, welche via *DNS*-Sinkholing unschädlich gemacht worden sind:

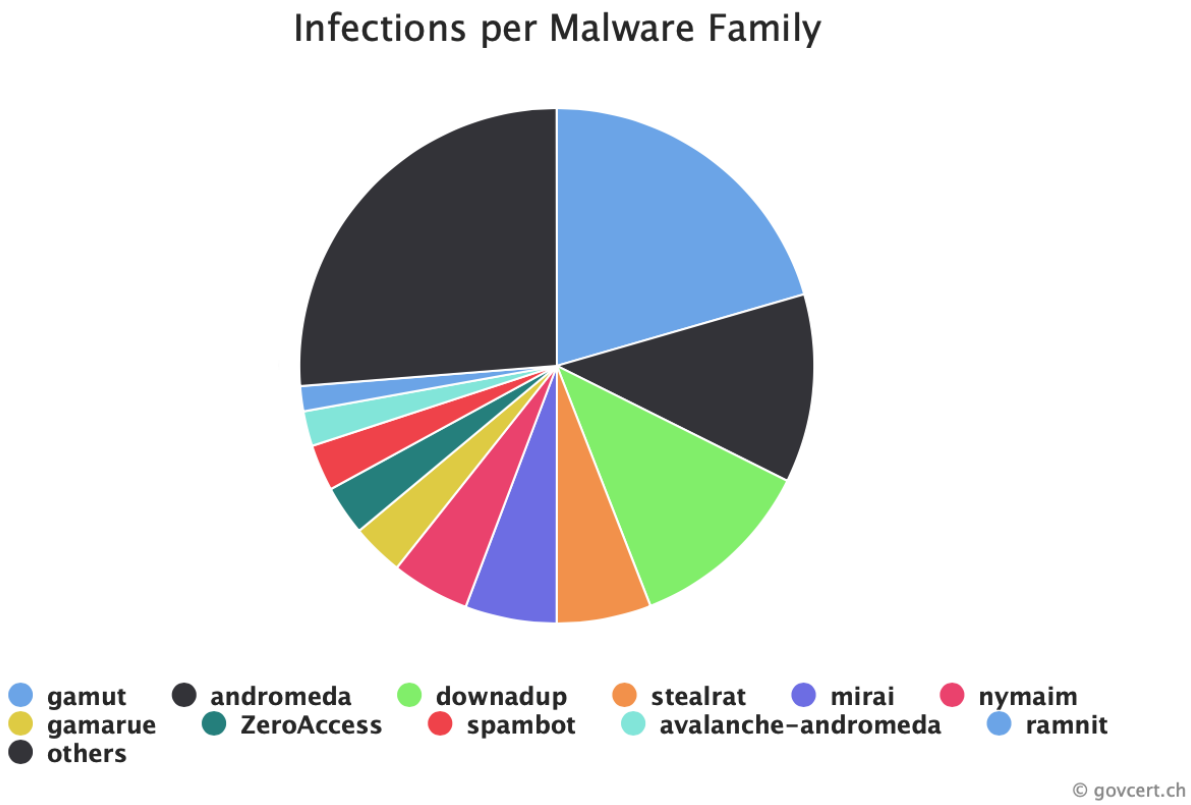

Abbildung 6: Verteilung der Schadsoftware in der Schweiz, welche MELANI bekannt ist. Stichtag ist der 30. Juni 2019. Aktuelle Daten finden Sie unter: http://www.govcert.admin.ch/statistics/malware/

Interessant ist die Tatsache, dass ca. 20% der Infektionen auf den Spambot «Gamut» zurückgehen. Auf dem zweiten Platz ist «Andromeda» zu finden, ein *Malware Dropper* mit Hilfe dessen weitere Schadsoftware installiert werden kann. Nach wie vor ein beträchtlicher Anteil von Infektionen geht auf das Konto von «Downadup» (auch «Conficker» genannt), einem *Wurm*, der seit 2008 aktiv ist.

5 Lage International

5.1 Spionage

5.1.1 Bemerkenswerte Entwicklungen

Im Berichtshalbjahr wurden zahlreiche Cyber-Spionageangriffe aufgedeckt, meist durch Berichte oder Analysen von Sicherheitsfirmen. Angesichts der vielen Meldungen, den unterschiedlichen Zielen, den erfinderischen Angreifern und neuen Techniken ist es nicht leicht den Überblick zu haben.

Deshalb wird häufig versucht, die Angriffe bestimmten Angreifergruppen oder Regionen zuzuschreiben. Diese Attribution[92] ist mit Schwierigkeiten verbunden, da oft Überschneidungen zwischen Gruppen oder Kampagnen beobachet werden. So zeigen neuere Kaspersky-Analysen, dass die für separate Angriffe bekannten Gruppen «Sofacy» und «Sandworm» zahlreiche Ähnlichkeiten aufweisen und teils von der gleichen Infrastruktur aus arbeiten.[93] Um die Sache noch komplizierter zu machen, werden «False Flags» (falsche Flaggen) verwendet, mit denen die Angreifer ihre Spuren verwischen und die Zuordnung fehlleiten wollen. So sollen z. B. bei den Aktivitäten von «Muddy Water» False Flags wie auf Chinesisch verfasste Code-Teile entdeckt worden sein. Bei den Verantwortlichen handelte es sich jedoch vermutlich um eine iranische Gruppe. Diese war in der Berichtsperiode sehr aktiv und hat sich neben den üblichen Zielen im Nahen Osten für Organisationen in Asien und Europa interessiert.[94]

Letztlich stellt sich bei der Zuordnung die Frage nach der Eigenart eines Angreifers: Welches Element ist so spezifisch für den Angreifer, dass es eine Zuschreibung ermöglicht? Die vom Angreifer eingesetzten technischen Mittel erfüllen das Kriterium immer weniger. Viele Gruppen verwenden heute – sei es beim Zugriff auf ein Netzwerk oder um sich in diesem zu bewegen – eine Vielzahl verschiedener, offen verfügbarer Tools. Dazu gehören Open-Source-Produkte wie «Metasploit» und der ID-Collector «Mimikatz» oder geleakte Tools wie der «EternalBlue»-Exploit. Durch die Vielzahl der verwendeten Instrumente bei einem Angriff bleiben die Gruppen agil und können ihre Techniken nach Bedarf zu bestimmten Zeitpunkten einsetzen. Ein Beispiel dafür ist das Arsenal, das die Gruppe «Emissary Panda»[95] 2019 bei verschiedenen Angriffen auf Regierungen im Nahen Osten eingesetzt hatte. Eigene Tools kamen nur noch situativ zum Einsatz. Die Identifikation einer Gruppe anhand der verwendeten Tools ist schwierig, wenn alle die gleichen Techniken einsetzen.[96] Hinzu kommt, dass sich der Kreis der potenziellen Angreifer durch die Verfügbarkeit der Tools erheblich erweitert hat.

Es mag überraschen, dass die öffentliche Attribution insbesondere der Regierungen so verbreitet ist,[97] wo doch die Zuschreibung anhand technischer Elemente immer unsicherer ist. Es gibt aber noch andere Elemente, an der sich die Zuschreibung orientieren kann, wie vor allem die Antwort auf die Frage «Cui bono – wer profitiert». Die politischen und wirtschaftlichen Ziele der Grossmächte sind meist bekannt (manchmal sogar Teil öffentlicher Strategien) und die Interessen hinter einem Angriff oft erkennbar.

So faszinierend und komplex diese Attributionen auch sind – sie helfen denjenigen wenig, die zum Ziel eines Angriffs geworden sind. Diese Unternehmen und Nutzer können angesichts der bekannten oder vermuteten Interessen der Staaten, die solche Angriffe durchführen, höchstens ihre Risikobeurteilung anpassen. Aber für das Opfer ist letztlich unwichtig, wer es angreift. Wichtig ist, die eigenen Schwachstellen zu erkennen und sich bewusst zu werden, wie ein Angreifer diese ausnutzen kann. In dieser Hinsicht ist die Anzahl und Vielfalt der verfügbaren Werkzeuge keine gute Nachricht. Jedem Angreifer steht ein riesiges Arsenal von Tools zur Verfügung.

---

92 Gemeint ist hier die öffentliche Attribution mit offizieller Benennung eines Angreifers.

93 https://securelist.com/zebrocys-multilanguage-malware-salad/90680/

94 https://documents.trendmicro.com/assets/white_papers/wp_new_muddywater_findings_uncovered.pdf

95 https://unit42.paloaltonetworks.com/emissary-panda-attacks-middle-east-government-sharepoint-servers/

96 Andere technische Elemente wie verwendete Infrastruktur (IP, Domains) können die Attribution ergänzen.

97 In den letzten Jahren wurden von den USA oder Verbündeten beispielsweise NotyPetya Russland, Wannacry Nordkorea oder APT10 offiziell China zugeschrieben. Siehe auch Kap. 4.1.4.

Schutz und Verteidigung der Ziele werden dadurch erschwert, dass die Angriffe auch über kompromittierte zielexterne Elemente erfolgen. Die Zulieferungskette (Supply Chain) ist schon seit einiger Zeit im Fokus.[98] Ein Beispiel dafür sind die Aktivitäten der China zugeschriebenen Cyber-Spionagegruppe «APT10», die es auf grosse Managed Service Provider (MSP) abgesehen hat[99] In der Berichtsperiode sind weitere Presseartikel erschienen, die meist über bereits Bekanntes berichteten[100] Es kann auch die von Unternehmen verwendete Software betroffen sein, wie dies bei der deutschen Fernwartungssoftware TeamViewer der Fall war. Im Mai 2019 räumte die Firma einen Angriff aus dem Jahr 2016 ein, dessen Auswirkungen schwer einzuschätzen sind.[101] Ein weiteres Beispiel für einen Angriff auf die Supply Chain ist der im März 2019 entdeckte Angriff, der Nutzerinnen und Nutzer von ASUS-Geräten betraf.[102] Der Schadcode soll über die automatische Update-Funktion von ASUS verbreitet worden sein. Betroffen war eine (unbekannte) Zahl von über ihre MAC-Adresse identifizierter Geräte. In solchen Fällen sind die Nutzer machtlos. Zu Updates des Geräteherstellers wird ja gerade aus Sicherheitsüberlegungen dringend geraten. Weitere Angriffe über externe Infrastruktur erfolgten in der Berichtsperiode durch Kompromittierung des *DNS*. Darüber wird im nachfolgenden Kapitel ausführlich berichtet.

5.1.2 DNS-Hijacking – Wegweiser in den Hinterhalt

Das *Domain Name System (DNS)* stellt sicher, dass Internetnutzende beim Aufruf einer Internet-Domäne wie www.melani.admin.ch an die IP-Adresse des zugehörigen Servers (bspw. 162.23.128.232) geleitet werden. Das US-CERT[103] warnte im Januar 2019 vor Versuchen, in die *DNS*-Infrastruktur einzudringen und *DNS*-Einträge so zu ändern, dass der Verkehr von Domain-Besuchern über Systeme unter Kontrolle der Angreifer umgeleitet wurde.

Über eine erste Variante berichtete Talos, die Sicherheitsabteilung von Cisco, unter der Bezeichung «DNSpionage»[104]. Dabei wurde einerseits die gleichnamige *Malware* gegen Anwender von Windows-Computern und andererseits Umleitungen auf Netzwerkebene gegen Ziele im Libanon und den Vereinigten Arabischen Emiraten beobachtet. Durch die Kontrolle über die *DNS*-Einträge waren die Angreifer auch befähigt, gültige SSL-Zertifikate für ihre Server auszustellen, um so auch verschlüsselten Verkehr umzuleiten.

Eine weitreichendere Übersicht der *DNS*-Hijacking Aktivitäten präsentierte der Sicherheitsdienstleister Fireeye[105] im Januar 2019. Die Bedrohungsforscher nennen drei verschiedene Varianten, wie die *DNS*-Abfragen aus Zielen im mittleren Osten, Nordafrika, Europa und Nord-

98 MELANI-Halbjahresbericht 2018/2, Kap. 3, sowie im vorliegenden Bericht Kap. 5.3.1.

99 MELANI-Halbjahresbericht 2017/1, Kap. 5.1.1 und 2018/2, Kap. 5.1.1.

100 https://uk.reuters.com/article/uk-china-cyber-cloudhopper-special-repor/special-report-inside-the-wests-failed-fight-against-chinas-cloud-hopper-hackers-idUKKCN1TR1DC

101 https://www.zdnet.com/article/chinese-cyberspies-breached-teamviewer-in-2016/

102 https://www.vice.com/en_us/article/pan9wn/hackers-hijacked-asus-software-updates-to-install-backdoors-on-thousands-of-computers

103 https://www.us-cert.gov/ncas/current-activity/2019/01/10/DNS-Infrastructure-Hijacking-Campaign

104 https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html

105 https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html

amerika manipuliert worden sind. Hauptsächlich versuchten die Angreifer aus dem umgeleiteten Datenstrom weitere Zugangsdaten für Systeme wie E-Mail und Dateiserver abzugreifen, um anschliessend als scheinbar legitime Nutzer in diese eindringen zu können.

Ende Januar 2019 bestätigte das Cyber-Sicherheitsunternehmen Crowdstrike[106] die beschriebenen Angriffsmethoden und benannte die Sektoren öffentliche Verwaltung, zivile Luftfahrt, sowie Internetdienstanbieter und Netzinfrastrukturdienstleister als Ziele der Angriffs-Kampagnen, die bis ins Jahr 2017 zurückreichen.

Im April 2019 berichtete Talos über einen weiteren Akteur, den sie unter der Bezeichnung «Sea Turtle» [107] bei ähnlichen Aktivitäten gegen die *DNS*-Infrastruktur beobachteten. Die Opfer waren Nationale Sicherheitsorganisationen, Aussenministerien und bekannte Energieorganisationen, sowie deren Dienstleister im *DNS*-Umfeld wie Registrare oder Telekommunikationsanbieter, die als Sprungbrett für die Angriffe gegen ihre Kunden dienten. In einem Folgebericht erwähnt Talos[108] unter anderem die Registry Griechenlands, welche die Vergabe von «.gr»-Domänen verwaltet, als Opfer. Die Angriffe weiteten sich gegen Energiefirmen, Think-Tanks, Nichtregierungsorganisationen und mindestens einen Flughafen aus. Auch Dienstleister und Organisationen in der Schweiz müssen mit Angriffen von «Sea Turtle» rechnen – sei dies als Mittel zum Zweck oder als direktes Ziel.

In der Folge dieser Angriffe rief die oberste Internetregulierungsstelle ICANN zur allgemeinen Implementierung der Domain Name System Security Extensions (DNSSEC) auf.[109] Es handelt sich dabei um eine Reihe von Internetstandards, die das *DNS* um Sicherheitsmechanismen zur Gewährleistung der Authentizität und Integrität der Daten erweitern. Mit diesen könnten solche Angriffe abgewehrt werden.

Die Bundesverwaltung unterstützt dies und hat für all ihre Websites DNSSEC eingeführt.

5.2 Industrielle Kontrollsysteme

5.2.1 Energieversorgungs-Kontrollsysteme bei bewaffnetem Konflikt immer im Blick

Am 14. Juni 2019 veröffentlichte die auf industrielle Kontrollsysteme spezialisierte Sicherheitsfirma Dragos einen Blog-Artikel zu den Aktivitäten einer Gruppe namens «Xenotime» und ihrer Schadsoftware «Triton/Trisis», die industrielle Sicherheitssysteme im Visier hat.[110] Laut einem Bericht von FireEye vom 23. Oktober 2018 sollen hinter der *Malware* russische Akteure stecken.[111]

---

106 https://www.crowdstrike.com/blog/widespread-dns-hijacking-activity-targets-multiple-sectors/

107 https://blog.talosintelligence.com/2019/04/seaturtle.html

108 https://blog.talosintelligence.com/2019/07/sea-turtle-keeps-on-swimming.html

109 https://www.icann.org/news/announcement-2019-02-22-en

110 https://dragos.com/blog/industry-news/threat-proliferation-in-ics-cybersecurity-xenotime-now-targeting-electric-sector-in-addition-to-oil-and-gas/; siehe auch MELANI Halbjahresbericht 2017/2, Kap. 5.3.2.

111 https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html

Dem Dragos-Bericht zufolge waren seit Mitte 2018 verstärkte Aktivitäten der Gruppe in europäischen Ländern sowie vor allem in den USA zu beobachten. Es sollen zwar keine Anlagen kompromittiert worden sein, die Gruppe hat aber ihre Auskundschaftung kontinuierlich weiterentwickelt. Insbesondere hat «Xenotime» den Zielbereich erweitert.[112] So wurde die Schadsoftware «Triton/Trisis» sowohl im Bereich Stromversorgung und –produktion als auch bei einer Gas- und Ölraffinerie eingesetzt.

Am 15. Juni 2019 veröffentlichte die New York Times einen Artikel über mögliche *Malware*-Einschleusung des US-Cyber Command (USCYBERCOM) in das russische Stromversorgungsnetz.[113] Diese in den letzten Jahren entwickelten Operationen sollen nicht nur den USA im Konfliktfall einen Vorsprung verschaffen, sondern vor allem als Abschreckung von russischen Cyber-Operationen gegen die USA dienen.

Die referenzierten Artikel zeigen, dass das staatliche Interesse an kritischen Infrastrukturen vor allem im Energiebereich anhält[114] und die Betreiber ihre Netze weiter profilieren und ihre Reaktionsfähigkeit bei Cyber-Angriffen ausbauen müssen.[115] Auf der Website des Bundesamtes für wirtschaftliche Landesversorgung (BWL) finden Sie den Mindeststandard für die Gewährleistung der IKT-Sicherheit bei der Stromversorgung.[116]

5.2.2 GPS-Spoofing belästigt Piloten im israelischen Luftraum

Seit in den allermeisten Smartphones ein GPS-Sensor verbaut ist, verlassen sich die meisten Menschen bei ihrer Navigation zu Fuss, im Auto oder anderweitig auf die satellitengestützte Orientierung im Raum. Wie in Kapitel 4.2.2 angedeutet, sind auch für Flugzeug-Piloten die GPS-Koordinaten zentral für ihre Flugroute. Im Verlaufe des Juni 2019 beschwerten sich mehrere Piloten beim Anflug auf den Ben Gurion Flughafen nahe Tel Aviv über unzuverlässige GPS-Signale.[117] Der israelische Pilotenverband sah eine *Spoofing*-Attacke als Ursache der Probleme mit falsch angezeigten Positionen.

Israelische Sicherheitsbehörden orteten die Signalquelle auf der syrischen Flugbasis Khmeimim und beschuldigten russische Systeme der elektronischen Kriegsführung (EKF) als Verursacher. Die Basis liegt ungefähr 350 km nördlich von Ben Gurion und wird intensiv von der russischen Luftwaffe zur Unterstützung des syrischen Regimes genutzt. Wenn die Anschuldigungen stimmen, zeigt sich, mit welcher Leistung die russischen EKF-Systeme bestückt sein müssen, um über eine solche Distanz die beschriebene Wirkung zu erzielen.

Der russische Botschafter in Israel dementierte die Vorwürfe umgehend und taxierte sie als unseriös und «Fake News».[118]

---

112 https://www.wired.com/story/triton-hackers-scan-us-power-grid

113 https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html

114 Siehe auch MELANI Halbjahresbericht 2015/2, Kap. 5.3.1 und 2016/2, Kap. 5.3.1.

115 Vgl. die in Kap. 4.2.1 erwähnte Studie von Electrosuisse.

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

117 https://www.gpsworld.com/israel-accuses-russia-of-spoofing-in-its-airspace/

118 https://www.bbc.com/news/technology-48786085

5.2.3 Die fremdgesteuerte Fernsteuerung

Wer hat nicht schon einmal gebannt zugeschaut, wie die Kranführerin auf der Baustelle vom Boden aus den riesigen Baukran mit den schweren Lasten über den kleinen Steuerknüppel dirigiert. Solche Funksteuerungen kommen an vielen Orten im Bau, der Logistik oder Produktionsbetrieben zum Einsatz.

Das japanische Sicherheitsunternehmen TrendMicro konnte in einer Analyse[119] demonstrieren, dass Angriffe über diese Funkschnittstelle möglich sind und beispielsweise Steuerbefehle manipuliert werden können. Voraussetzung für einen erfolgreichen Angriff ist in diesem Falle, dass der Angreifer sich physisch in der Nähe des Zieles befindet, damit die Signale das angegriffene Gerät auch erreichen. Um sich nicht in der Nähe aufhalten zu müssen, können Angreifer einen kleinen Transmitter im Umfeld des ferngesteuerten Systems platzieren und dieses über Wi-Fi oder Mobilfunk aus der Ferne ansprechen. Um die Plausibilität der Bedrohung aufzuzeigen, entwickelten die Forscher eine eigene batteriebetriebene Funkhardware «RFQuack» (siehe nachfolgende Abbildung), die in einer Hosentasche Platz findet.

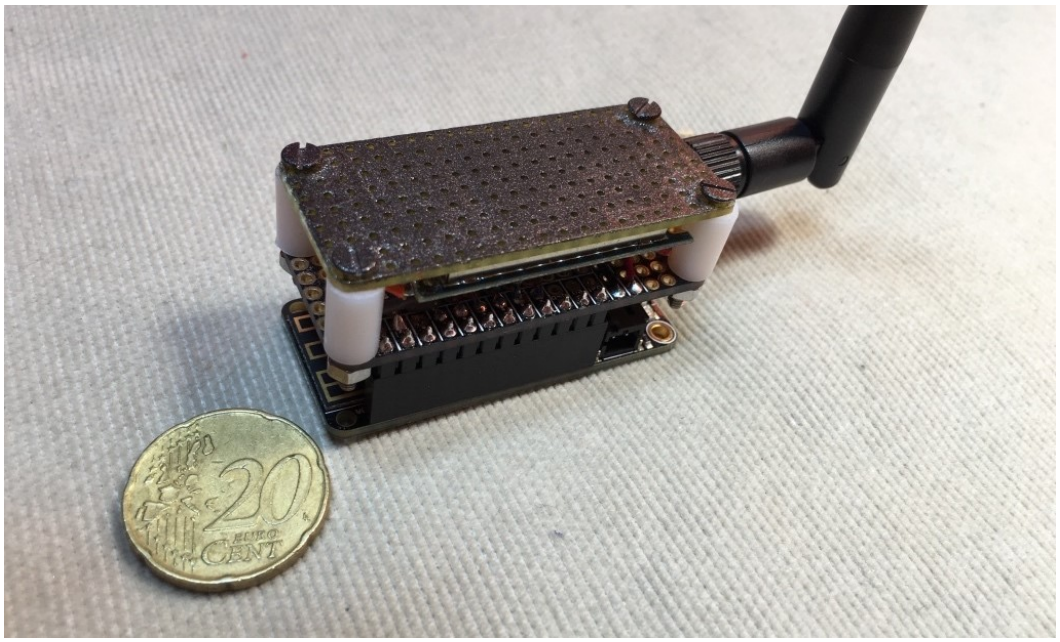

Abbildung 7: Grössenvergleich des RFQuack-Funkmoduls

Empfehlung:

Um sich bestmöglich vor solchen Angriffsszenarien zu schützen, empfehlen die Analysten, die Dokumentationen der anzuschaffenden Fernsteuerung genau zu studieren. Dabei soll darauf geachtet werden, dass die Geräte einen konfigurierbaren Verbindungsmechanismus «Pairing» anbieten. Weitere Massnahmen sind: Den Computer, mit welchem die Fernsteuerung programmiert wird, vom Netz getrennt zu betreiben und wo möglich gut erforschte Standardprotokolle wie «Bluetooth Low Energy» einzusetzen.

119 https://blog.trendmicro.com/trendlabs-security-intelligence/demonstrating-command-injection-and-e-stop-abuse-against-industrial-radio-remote-controllers/

Schlussfolgerung / Empfehlung:

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

Checkliste mit Massnahmen zum Schutz industrieller Kontrollsysteme

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

5.3 Angriffe (DDoS, Defacements, Drive-By)

5.3.1 Informatikdienstleister WIPRO gehackt

Im April 2019 berichtete der Investigativjournalist Brian Krebs, der multinationale Informatikdienstleister WIPRO sei Opfer eines Angriffs geworden.[120] Angesichts der Aktivitäten von Gruppen wie «APT10», die Managed Service Provider (MSP) meist zum Ausspionieren ihrer Kunden angreifen, haben die Experten Schlimmes befürchtet. Eine neue Analyse von Flashpoint[121] geht ebenfalls von einem Angriff auf die Kunden des Unternehmens aus, aber von einer anderen Motivation. Der Angreifer scheint eher auf einen finanziellen Gewinn als auf Spionage abzuzielen. Die Gruppe soll seit 2015 oder 2016 aktiv sein und es zur Finanzierung ihrer Tätigkeiten vor allem auf Geschenkgutscheine (Gift Cards) der Firmen abgesehen haben.

Ins Netzwerk ihres Ziels gelangten die Angreifer weitgehend über Phishing. Laut dem Bericht eines Sicherheitsunternehmens nutzten sie Templates eines Unternehmens, das in der Sensibilisierung tätig und in der Schweiz angesiedelt ist. Das muss nicht heissen, dass dieses Unternehmen selbst kompromittiert war. Die Angreifer haben auch frei zugängliche Angriffs-Tools eingesetzt oder nach einer ersten Kompromittierung im Netzwerk des Ziels vorhandene Dual-Use-Tools ausgenutzt.

Dieser Angriff zeigt einmal mehr, wie real das Risiko von Angriffen über die Zulieferungskette (Supply Chain) ist. Nicht nur bei Spionageangriffen wird versucht, über die Kompromittierung von Zulieferern in das Zielsystem zu gelangen. Auch andere Tätergruppen scheinen sich diesen Ansatz zunutze zu machen.

120 https://krebsonsecurity.com/2019/04/experts-breach-at-it-outsourcing-giant-wipro/

121 https://www.flashpoint-intel.com/blog/wipro-threat-actors-active-since-2015/

5.3.2 Botnetz versucht RDP-Server via Brute-Force-Angriffe zu knacken

Seit Jahren scannen Angreifer das Internet auf offene oder schlecht gesicherte Ports, welche dann als Einfallstor in Netzwerke verwendet werden. Diese Ports sind meist einem Internetservice oder -Protokoll zugeteilt und zum Teil standardmässig definiert. Es gibt dafür mittlerweile sogar Suchmaschinen, welche kein grosses technisches Verständnis verlangen, um solche «offene Türen» zu finden. Einiger dieser Einfallstüren sind beliebter als andere. Im letzten halben Jahr hat MELANI wieder vermehrt Scan-Aktivitäten von *RDP*[122]-Ports festgestellt. Per Standardeinstellungen ist der *RDP*-Port 3389.

Das Botnetz «GoldBrute», welches über einen einzigen *Command & Control Server* kontrolliert wird, scannte zum Zeitpunkt des Artikels von SANS[123] 1.5 Millionen *RDP*-Server, welche im Internet exponiert zu finden sind. Dabei wächst das Botnetz ständig weiter. Das infizierte System lädt den Botcode herunter und beginnt dann zufällige weitere IP-Adressen auf *RDP*-Ports zu scannen. Wenn der Bot 80 weitere IP-Adressen gefunden hat, bei welchen ein *RDP*-Port zugänglich ist, meldet er diese an den Kommandoserver. Dieser leitet dann jedem Bot ein Set an IP-Adressen weiter, welche er *bruteforcen* soll. Jedoch wird untypischerweise immer nur ein zugeteilter Username und EIN dazugehöriges Passwort versucht, um unter dem Radar zu bleiben und somit von gängigen Sicherheitsprogrammen nicht erkannt zu werden. Via *RDP* kompromittierte Systeme werden ihrerseits zu einem Bot. Theoretisch könnten die Angreifer auch eine andere Schadsoftware, wie zum Beispiel Ransomware oder eine Datenbeschaffungssoftware installieren, was dann für die Eigentümer des gehackten Systems schwerwiegende Folgen haben könnte.

5.3.3 Neues von Anonymous

Aktionen, zu denen sich Anonymous bekennt, sind in letzter Zeit selten geworden. Ein Grund dafür könnten die publikumswirksamen Verhaftungen von Teilnehmern im Nachgang von früheren Aktionen sein. Verschiedene Ereignisse insbesondere zum Thema Informationsfreiheit vermochten Aktivisten der Bewegung aber weiterhin zu mobilisieren. So die Verhaftung von Julian Assange in London, die Anlass zu Aktionen gegen englische und ecuadorianische Interessen auslöste. Der Gründer von Wikileaks hielt sich seit 2012 im Asyl in der ecuadorianischen Botschaft in London auf. Als Gegenschlag gegen die Aufhebung des Asyls und die Verhaftung im April 2019 hat eine Gruppe, die sich zu Anonymous bekannte, kurz nach der Verhaftung bei verschiedenen englischen Polizeidiensten gestohlene Daten veröffentlicht. Personendaten waren jedoch scheinbar nicht darunter. Eine andere Gruppe hat sich im Namen von Anonymous zu *DDoS*-Angriffen auf Websites britischer Behörden bekannt. Auch die ecuadorianischen Behörden berichteten von *DDoS*-Angriffen insbesondere auf die Website der Zentralbank und des Premierministers.

5.3.4 DDoS-Angriffe für Bitcoins

Seit einiger Zeit ist bekannt, dass der Erfolg virtueller Währungen zu virtuellen Raubzügen verleitet. MELANI hat schon mehrfach über Angriffe auf Nutzer oder Plattformen solcher Währungen berichtet.[124] Je beliebter eine Währung respektive ein Dienst ist, desto grösser das

---

[122] Remote Desktop Protocol: Ein Netzwerkprotokoll von Microsoft für den Fernzugriff auf Windows-Computer.

[123] https://isc.sans.edu/forums/diary/GoldBrute+Botnet+Brute+Forcing+15+Million+RDP+Servers/25002/

[124] Siehe insbesondere MELANI Halbjahresbericht 2017/2, Kap. 5.4.3.

Risiko eines Angriffs. Dieses Jahr hat es den Bitcoin-Walletdienst «Electrum» getroffen. Die Nutzer des Dienstes wurden verleitet, eine manipulierte Version der App herunterladen. Zu diesem Zweck haben die Angreifer eine Reihe von schädlichen «Knoten» im Peer-to-Peer-Netz positioniert, das zur Freigabe der Transaktionen verwendet wird. Kam der Nutzer zu einem dieser Knoten (der als Server im Peer-to-Peer-Netzwerk fungiert), erhielt er eine Fehlermeldung mit einem Link auf ein vermeintliches Update der App, das er herunterladen müsse. Es handelte sich dabei jedoch um ein Schadprogramm, mit dem das Wallet dann geleert wurde.

Das war noch nicht alles. Als Reaktion auf die Gegenmassnahmen der «Electrum»-Betreiber wurden *DDoS*-Angriffe auf die nicht kompromittierten Netzknoten durchgeführt. Bei Unerreichbarkeit der «echten» Knoten konnten die Nutzer leichter auf die «falschen» Knoten mit dem schädlichen Update weitergeleitet werden. Im April schätzte die Sicherheitsfirma Malwarebytes, dass auf diese Weise 771 Bitcoins gestohlen wurden (was im April etwa 4 Millionen Dollar entsprach).[125]

5.4 Datenabflüsse

5.4.1 Citrix-Hack

Das Software-Unternehmen Citrix wurde am 6. März 2019 vom FBI informiert, dass sich internationale Cyber-Kriminelle Zugang zum internen Citrix-Netzwerk verschafft hatten.[126] Citrix informierte in der Folge seine Kunden, dass ausländische Hacker in ihr internes Firmennetzwerk eingedrungen sind und Daten abgezogen haben. Auf welche Daten die Eindringlinge Zugriff hatten, ist Gegenstand laufender Untersuchungen. Gemäss Citrix gibt es jedoch keine Hinweise, dass die Hacker an der offiziellen Citrix-Software oder an anderen Produkten Manipulationen vorgenommen haben.

Der Vorfall ist möglicherweise Teil einer ausgeklügelten Kampagne, welche sich stark auf Regierungen, militärisch-industrielle Firmen, Energieunternehmen, Finanzunternehmen und Betreiber kritischer Infrastrukturen konzentriert.[127]

5.4.2 Magento: Sicherheit von Online-Shops

Anfällige Erweiterungsmodule von Drittanbietern sind heute die Hauptquelle für Hacks der Online-Shop-Software Magento. So führt unter anderem eine Schwachstelle im Datenbank-Protokoll MySQL, welche seit Jahren dokumentiert ist, dazu, dass Kriminelle Schadcode in E-Commerce Shops einbauen können. Dieses Beispiel zeigt, dass es für Online-Händler anspruchsvoll ist, ihre Webseiten von schädlichen Codes sauber zu halten, da auch die verwendeten Module von Drittanbietern ständig auf dem neuesten Stand sein sollten. Dies führt zu einem Interessenkonflikt zwischen der Stabilität des E-Shops und einer kontinuierlichen Update-Politik, nicht zuletzt, weil Magento keine standardisierte Möglichkeit anbietet, bei kritischen Releases von Drittanbietern informiert zu werden.

---

125 https://blog.malwarebytes.com/cybercrime/2019/04/electrum-bitcoin-wallets-under-siege/

126 https://www.citrix.com/blogs/2019/03/08/citrix-investigating-unauthorized-access-to-internal-network/

127 https://www.forbes.com/sites/kateoflahertyuk/2019/03/15/who-is-resecurity-the-mysterious-firm-that-blamed-iran-for-the-citrix-hack/; https://www.theregister.co.uk/2019/03/08/citrix_hacked_data_stolen/

5.4.3 Data Leak in Panama

Sicherheitsforscher entdeckten einen ungeschützten Elasticsearch-Server, auf dem personenbezogene Daten von fast 90 Prozent der Einwohner von Panama gespeichert sind. Zu den exponierten Daten gehören vollständige Namen, Geburtsdaten, Ausweisnummern, Krankenversicherungsnummern und andere persönliche Daten. Die Datenbank enthielt weiter 3.4 Millionen Datensätze über panamaische Bürger, die als «Patienten» bezeichnet wurden. Das CERT-Panama hat die Datenbank nach Erhalt der Meldung umgehend gesichert. Ob jemand während der Zeit, in der die Daten ungeschützt abrufbar waren, auf die Daten zugegriffen hat, kann allerdings nicht mehr festgestellt werden.

5.4.4 Millionen von Facebook Daten auf Amazon Cloud-Server gefunden

Sicherheitsforscher fanden erneut unzählige Facebook-Benutzerdaten, welche öffentlich auf den Cloud Computing-Servern von Amazon einsehbar waren.[128] Die jüngste Entdeckung zeigt, dass Facebook-Benutzerdaten auch ein Jahr nach dem Cambridge Analytica-Skandal immer noch unsicher abgelegt und weit verbreitet online zu finden sind. Fakt ist, dass Facebook-Daten vertraglich über Jahre relativ frei jedem zur Verfügung gestellt hat, der das Soziale Netzwerk in seinen Dienst integriert hat. Diese Praxis wurde erst kürzlich beendet. Die Entdeckungen zeigen jedoch, dass Firmen, welche durch Verträge Zugang zu Daten von Facebook erhalten, im Bereich Datenschutz viel zu wenig aktiv sind. Nach etlichen Skandalen ist weiterhin fraglich, ob Benutzerdaten auf Facebook sicher sind und die Nachvollziehbarkeit der Datenhandhabung für den einzelnen Nutzer transparent genug ist. Dies allerdings ist nicht nur ein Facebook-spezifisches Problem. In Zeiten von BigData und Automation ist dieses Thema zudem relevant wie nie zuvor, denn die Analyse der Datensätze lassen beachtliche Rückschlüsse zu. Nutzer tun gut daran, sich über ihren digitalen Auftritt und die Herausgabe von persönlichen Daten Gedanken zu machen. Das jüngste Beispiel zeigt weiter eindrücklich, wie sich die Probleme der Datensicherheit und die Kontrolle der Daten durch einen weiteren Trend verstärken: den Übergang vom Betrieb und der Datenhaltung überwiegend in eigenen Rechenzentren zu Cloud Computing-Diensten von Technologie-Giganten.

5.5 Schwachstellen

5.5.1 «BlueKeep» – Wurmartige Schwachstelle im RDP-Protokoll

Im Mai 2019 wurde im Microsoft Remote Desktop Protocol (*RDP*) eine Schwachstelle bekannt («BlueKeep» aka CVE-2019-0708). Kurz nach Bekanntgabe der Schwachstelle und der Veröffentlichung des Sicherheits-Patches durch Microsoft starteten Angreifer automatisierte Scanning-Aktivitäten, um offene *RDP*-Ports zu finden.[129] Sie versuchten dann per *Brute Force-Angriff* (ausprobieren einfacher, schwacher oder bereits bekannter Passwörter) Zugang zu den Systemen zu erhalten, um dann anschliessend die Schwachstelle ausnutzen zu können.

Die Schwachstelle erlaubt das Ausführen von Code via Fernzugriff. Da die Schwachstelle in allen Windows-Versionen ab Windows 2000 bis Windows 7 inklusive Windows Server 2008 R2 zu finden ist, wurde sie als sehr kritisch eingestuft. Neuere Versionen (Windows 8 und 10)

128 https://www.upguard.com/breaches/facebook-user-data-leak

129 https://www.zdnet.com/article/intense-scanning-activity-detected-for-bluekeep-rdp-flaw/

sind davon nicht betroffen. Microsoft hat am 14. Mai 2019 einen Patch veröffentlicht, mit welchem alle Versionen bedient werden, sogar die Versionen, welche von Microsoft eigentlich nicht mehr unterstützt werden, da sie ihr Lebensende erreicht haben.

Die Spezialität dieser Schwachstelle ist es, dass sie «*Wurmcharakte*r» hat. Das heisst eine Schadsoftware kann sich ohne Interaktion eines Menschen «automatisch» auf ungepatchte Systeme weiterverbreiten. Dies könnte verheerende Auswirkungen haben, da viele Systeme verwundbar sind und diese nicht in jedem Fall zeitnah gepatcht werden.

Zurzeit gibt es einige Beweise, dass es möglich ist, diese Schwachstelle auszunutzen, jedoch haben die Forscher das «How to» nicht öffentlich publiziert und die Schwachstelle wird bislang nicht aktiv von Kriminellen ausgenutzt. Jedoch werden seit geraumer Zeit erhöhte Aktivitäten zu *RDP*-Port-Scanning beobachtet. Ein solches Port Scanning kann benutzt werden, um eine Liste von verwundbaren Systemen anzufertigen, sodass potenzielle Ziele bereits bekannt sind, wenn ein funktionierender Exploit verfügbar wird. Es handelt sich nur um eine Frage der Zeit, bis jemand einen Exploit schreibt, der dann «in the wild» ausgenutzt wird.[130]

Empfehlung:

Um sich vor «BlueKeep» zu schützen, sollten Sie unbedingt den entsprechenden Sicherheitspatch einspielen. Zudem rät MELANI, Remote Desktop Services und die zugehörigen Ports zu deaktivieren, sofern diese nicht zwingend gebraucht werden.

Erhöhtes *RDP*-Port-Scanning ist beunruhigend, da es sehr viele Ports gibt, welche mehr oder weniger frei vom Internet aus erreichbar sind. Es gibt Studien, welche besagen, dass im ersten Quartal 2019 bei Ransomware das häufigste Einfallstor offene oder schlecht konfigurierte *RDP*-Ports gewesen seien.[131] Dies auch oftmals, weil weder Nutzer noch Administratoren wissen, dass der Service in ihrem Netzwerk überhaupt aktiviert ist. Das heisst, die Nutzer werden über einen Vektor angegriffen, dessen Existenz sie sich nicht bewusst sind und somit auch keine diesbezüglichen Schutzmassnahmen ergreifen. Insofern ist es unabdingbar, dass die Nutzer und Administratoren ihre Netzwerke kennen und wissen, was für Services und Geräte vorhanden sind, um diese effektiv absichern zu können.

Die Auswirkungen von Ransomware sind, wie weiter oben im Kapitel 3 beschrieben, gravierend und können eine Firma für mehrere Tage komplett lahmlegen. Ebenfalls können Angreifer über das *RDP*-Einfallstor sich lateral im Firmennetzwerk bewegen und somit zu interessanteren Zielen vorstossen. Sie können somit auch wichtige Daten stehlen, löschen oder eben verschlüsseln und unbrauchbar machen. Sofern keine gute, getestete Backup-Lösung vorhanden ist, sind solche Daten meist verloren – bis jemand ein sogenanntes Entschlüsselungstool kreiert, womit zumindest ein Teil der Daten wiederhergestellt werden kann.

---

130 In der Zeit zwischen Redaktion und Publikation dieses Berichts hat sich diese Vorhersage schon realisiert und BlueKeep wurde in das Open Source Penetrationstesting-Tool «Metasploit» integriert.

131 https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/rdp-security-explained/

Um einen solchen Angriff zu vermeiden, gibt McAfee folgende Tipps:[132]

Empfehlungen:

- Keine *RDP*-Verbindungen über das offene Internet zulassen; *RDP* sollte NIE offen zum Internet sein, da es kontinuierliche Scanning-Aktivitäten gibt und Nutzer bezüglich Denial of Service-Attacken oder Benutzerkonto-Übernahmen verwundbar sind.
- Komplexe Passwörter verwenden, denn es werden viele *Brute-Force-Attacken* auf *RDP*-Ports versucht.
- Verwenden von Multifaktorauthentifizierung (z. B. Security Token, Code erhalten via Benachrichtigung oder biometrische Verifizierung).
- *RDP* Gateway verwenden, um mehr Kontrolle zu haben (z. B. um Logging zu ermöglichen).
- Blockierung von Benutzernamen oder IP-Adressen, welche zu viele erfolglose Login-Versuche verzeichnen.
- Benützen eines Firewalls, um den Zugriff einzuschränken.
- Verschlüsselung benützen.
- Network Level Authentication (NLA) aktivieren. Diese Massnahme schützt zu einem grossen Teil vor der «BlueKeep»-Schwachstelle, da ein Angreifer sich erst mit einem gültigen Konto einloggen müsste, bevor er die Schwachstelle ausnutzen kann.
- Beschränkung der Zugriffsrechte der Benutzer, welche sich via *RDP* einloggen können (meist brauchen nicht alle Administratoren einen Zugang).

Sofern diese Massnahmen korrekt umgesetzt sind, haben Sie Ihr Risiko bezüglich Ransomware- und anderen Angriffen über RDP schon erheblich verringert.

5.5.2 EXIM-Schwachstelle bei Millionen von Mailservern

«Exim» ist ein sogenannter MTA (Mail Transfer Agent), also ein Bestandteil eines Mailservers. Es handelt sich um die Software, welche E-Mails entgegennimmt und diese sendet. Die meisten Unix-basierten Systeme benutzen «Exim»-Komponenten, bei Debian-Systemen sind diese als Standardsoftware installiert.[133, 134]

Die Schwachstelle hat zwei Komponenten: Einerseits können lokale Angreifer (Insider) Systembefehle mit Root-Zugriff ausführen lassen, andererseits können auch Angreifer, welche nur Fernzugriff haben, bei bestimmten nicht standardmässigen Konfigurationen, ähnliches bewirken.

---

[132] https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/rdp-security-explained/

[133] https://meterpreter.org/cve-2019-10149-exim-remote-code-execution/

[134] https://blog.skyboxsecurity.com/exim-vulnerability/

Diese Schwachstelle wurde bereits eine Woche nach der Veröffentlichung von Angreifern aktiv missbraucht. In den Publikationen ist man sich uneinig, wie viele verwundbare Systeme zur Zeit der Veröffentlichung der Schwachstelle weltweit vorhanden waren: Laut skyboxSecurity handelt es sich um mehr als 3.5 Millionen Server. SecureZoo[135] geht von mehr als 4 Millionen Geräten aus (circa 90% aller Installationen weltweit), welche die verwundbare Version von «Exim» benutzen.[136] Die neueste Version von «Exim» ist von der Schwachstelle nicht mehr betroffen. Alle Systeme sollten dringend auf die «Exim»-Version 4.92 aktualisiert werden. Auf 57% aller E-Mail-Server läuft die «Exim»-Software. Sicherheitsforscher schätzen das Schadenspotenzial deshalb als immens ein.[137]

Einschätzung:

Es werden täglich viele Schwachstellen publiziert. Für einige gibt es zum Zeitpunkt der Veröffentlichung bereits einen Sicherheits-Patch – für andere nicht. Da in einem Unternehmen in der Regel verschiedene Systeme und Software eingesetzt werden, kann es schwierig sein, alle Schwachstellen betreffend der benützten Hard- und Software manuell nachzuverfolgen. Updates sollten daher sofern möglich automatisch installiert werden. Nicht alle publizierten Schwachstellen werden auch effektiv von Angreifern ausgenutzt. Es gibt jedoch Schwachstellen, welche relativ einfach ausgenutzt werden können, nach kurzer Zeit bereits in *Exploit-Kits* integriert werden und dann auch dementsprechendes Schadenspotenzial haben.

5.5.3 Wie aus einem Smartphone eine Wanze wird

In der ersten Hälfte von 2019 wurden zwei Schwachstellen veröffentlicht, welche es Angreifern erlaubt hätten, ein Smartphone in eine Wanze zu verwandeln. Die eine wurde bei der Applikation «Facetime» und die andere bei «WhatsApp» entdeckt.

Bei der «WhatsApp» Schwachstelle handelte es sich um eine sogenannte «Buffer Overflow»-Schwachstelle im VoIP-(Voice-over-IP)Modul von «WhatsApp», welches zum Telefonieren mit der App benutzt wird. Sie konnte ausgenutzt werden, indem speziell angefertigte SRTCP[138]-Pakete an das Ziel-Smartphone versendet wurden. Genauer gesagt reichte es aus, wenn ein manipulierter «WhatsApp»-Anruf auf das Ziel-Smartphone getätigt wurde. Die angerufene Person musste weder den Anruf entgegennehmen, noch war eine Spur eines Anrufs in Abwesenheit zu sehen. Somit war die Kompromittierung des Smartphones schwierig zu entdecken. Die Schwachstelle wurde entdeckt, als angeblich ein Anwalt in Grossbritannien Ziel eines solchen Angriffs wurde[139].

Die «FaceTime»-Schwachstelle wurde von einem Jugendlichen zufällig entdeckt. Es handelt sich um einen Software-Fehler in der iPhone-App «FaceTime».[140] Sie erlaubte es einem nach

135 https://www.securezoo.com/2019/06/critical-exim-vulnerability-discovered-and-patched/
136 https://www.cisecurity.org/advisory/a-vulnerability-in-exim-could-allow-for-remote-command-execution_2019-061/
137 https://www.securezoo.com/2019/06/critical-exim-vulnerability-discovered-and-patched/
138 Secure Real Time Control Transport Protocol: https://tools.ietf.org/html/rfc3711
139 https://securityaffairs.co/wordpress/85477/breaking-news/whatsapp-zero-day.html
140 https://www.buzzfeednews.com/article/nicolenguyen/facetime-bug-iphone

wenigen Handlungsschritten, Audiomitschnitte aus der Umgebung der angerufenen Person zu hören und Bilder von der Frontkamera zu sehen, noch bevor diese den Anruf überhaupt angenommen hat. Damit dies funktionierte, musste der Anrufende sich selbst wie eine weitere Person zum Anruf hinzufügen. Apple hat für diesen Fehler kurz darauf einen Sicherheits-Patch veröffentlicht, mit dem das Problem behoben wurde.[141]

5.5.4 Internet Explorer Zero-Day-Verwundbarkeit: Irresponsible disclosure

Es kommt immer wieder vor, dass Sicherheitsforscher Exploits für Schwachstellen publizieren, um Software-Hersteller dazu zu zwingen, sofort Patches für Schwachstellen herzustellen, welche ihnen zuvor gemeldet wurden.

Dies war auch der Fall bei einem Internet Explorer *Zero-Day Exploit*.[142] Ein Sicherheitsforscher hat Microsoft darüber in Kenntnis gesetzt und als diese zu verstehen gaben, dass sie zurzeit keinen Patch dafür geplant haben, hat er den Exploit zusammen mit einem sogenannten Proof-of-Concept publiziert. Darin zeigte er, dass es möglich ist, lokale Dateien zu stehlen und somit aus der Ferne die Programmversionen auszukundschaften, wenn ein Nutzer eine präparierte MHT-Datei[143] öffnet (welche auf Windowssystemen standardmässig mit Internet Explorer geöffnet werden).

Cybercrime-Gruppen verwenden öfters MHT-Dateien für *Spear-Phishing* oder zur Schadsoftware-Verbreitung. Der Wettlauf zwischen den Kriminellen, diese Methode zu implementieren und Microsoft, einen entsprechenden Patch herauszugeben, ist eröffnet.

Ob bei solchen «irresponsible disclosure» jeweils die Forscher einfach ungeduldig sind oder ein Problem auf Seite des Herstellers besteht, lässt sich nicht generell sagen. Software-Hersteller sollten auf jeden Fall alle eingehenden Meldungen zu Schwachstellen ernsthaft prüfen und Sicherheitsforschern anständige Rückmeldungen geben, in welchen auch ein Zeithorizont für die Behebung der Schwachstelle angegeben ist.

5.6 Präventive Massnahmen und Strafverfolgung

5.6.1 Zerschlagung des kriminellen Netzwerks hinter «GozNym»

Der E-Banking Trojaner «GozNym» wurde von einem kriminellen Netzwerk betrieben, welches eine klare Arbeitsteilung aufwies und dessen Mitglieder über mehrere Staaten verteilt waren (darunter Georgien, Bulgarien, Ukraine, Moldawien, Kasachstan und Russland). Eine komplexe polizeiliche Operation, an welcher verschiedene Länder und internationale Organisationen teilnahmen, ermöglichte die Verhaftung von mehreren Bandenmitgliedern. Darunter waren *Malware*-Entwickler, ein Spezialist für Massendistribution von E-Mails, einige mit dem eigentlichen Online-Bankraub beauftragte Hacker, Geldwäsche-Agenten und weitere in unterstützender Funktion tätige Personen. Im Mai 2019 wurden zehn Mitglieder der Gruppe in Pittsburgh angeklagt und weitere Verfahren sind in Georgien, Moldawien und in der Ukraine hängig. Auch gegen den Provider des «Bulletproof Hosting Service» wird zur Zeit in der Ukraine

141 https://9to5mac.com/2019/01/28/facetime-bug-hear-audio/

142 https://www.zdnet.com/article/internet-explorer-zero-day-lets-hackers-steal-files-from-windows-pcs/

143 In MHT-Dateien werden Webseiten inklusive Grafiken und anderer eingebetteter Elemente gespeichert.

gerichtlich vorgegangen. Seine Dienste wurden neben «GozNym» für mehr als 20 weitere *Malware*-Kampagnen genutzt.[144]

5.6.2 Weiterer Erfolg gegen Microsoft Fake Support

Bereits im letzten Halbjahresbericht konnte MELANI von einer Polizeiaktion gegen Computer-Support-Betrüger berichten. Damals intervenierte die indische Polizei in 26 Callcentern, von wo die englischsprachigen Anrufe ausegangen waren.[145] Mittlerweile konnte auch die französische Polizei einen Erfolg vermelden.[146] Sie konnte drei als Drahtzieher verdächtigte Franzosen festnehmen. Im untersuchten Fall wurde den Opfern jeweils mit nur schwer entfernbaren Einblendungen auf dem Computer suggeriert, dass dieser infiziert sei und sie den «Microsoft Support» auf die angezeigte Nummer anrufen sollen. Die Spuren führten zuerst in den Maghreb, wo die vermeintlichen Support-Agenten stationiert waren. Durch Ermittlungen des Geldflusses konnten schliesslich die französischen Auftraggeber identifiziert werden.

Die Masche mit dem gefälschten Microsoft Support gibt es mittlerweile seit fast zehn Jahren. MELANI berichtet und warnt immer wieder vor diesem Phänomen.[147] Dennoch erhält MELANI weiterhin regelmässig entsprechende Meldungen. Es ist davon auszugehen, dass diese Masche weiterhin erfolgreich angewendet und wohl so schnell nicht verschwinden wird. Gleichzeitig darf aber auch erwartet werden, dass die Strafverfolgung immer mehr solche Betrüger dingfest machen kann.

6 Tendenzen und Ausblick

6.1 Kosten der Cyber-Kriminalität

Die Experten sind sich einig: Cyber-Kriminalität nimmt laufend zu. Die Gründe dafür sind weitgehend bekannt: Die zunehmende Digitalisierung all unserer Tätigkeiten öffnet ein weites Feld an kriminellen Möglichkeiten. Darüber herrscht Einigkeit. Schwieriger ist es, diese Entwicklung zu beziffern, und noch schwieriger, die Schäden für die einzelnen Länder oder weltweit abzuschätzen. Die grösste Schwierigkeit, verlässliche Zahlen zu erhalten, liegt in der grossen Dunkelziffer im Bereich der Cyber-Kriminalität. Sei es einerseits, weil die Delikte nicht immer angezeigt beziehungsweise gemeldet werden oder andererseits, weil die Opfer die Delikte gar nicht erkennen. Statistiken zu Kosten der Cyber-Kriminalität sind daher immer mit Vorsicht zu geniessen, da es sich oft um reine Schätzungen oder Hochrechnungen handelt.

---

144 https://www.europol.europa.eu/newsroom/news/goznym-malware-cybercriminal-network-dismantled-in-international-operation

145 MELANI Halbjahresbericht 2018/2, Kap. 5.5.1.

146 http://www.leparisien.fr/faits-divers/cybercriminalite-trois-chefs-d-entreprise-soupconnes-d-avoir-pirate-8-000-francais-31-01-2019-8001474.php

147 https://www.melani.admin.ch/melani/de/home/meldeformular/formular0/meldeformularhaeufigefragen/mich-hat-eine-firma-angerufen-und-gesagt--dass-mein-computer-mit.html; https://www.melani.admin.ch/melani/de/home/themen/fake_support.html

Trotz dieser Schwierigkeiten: Quantitative Daten sind für die Akteure im Bereich Bekämpfung der Cyber-Kriminalität und die zuständigen politischen Behörden wichtig, vor allem für die Planung angemessener Massnahmen. In diesem Kapitel sind einige im ersten Halbjahr 2019 veröffentlichte Studien zur Cyber-Kriminalität zusammengefasst. Die Zahlen können über das Ausmass der beobachteten Phänomene Auskunft geben. Mithilfe des Vergleichs der Ergebnisse, die mit der gleichen Methode in verschiedenen Zeiträumen erzielt wurden, lassen sich auch Entwicklungen erkennen.

In der Studie «Measuring the Changing Cost of Cybercrime»,[148] welche am «Workshop on the Economics of Information Security» im Juni 2019 in Boston vorgestellt wurde, vergleichen die Autoren die aktuellen Zahlen und Schätzungen mit denjenigen der Erststudie, welche sie im Jahr 2012 durchgeführt hatten. Die Autoren machten systematische Auswertungen der Kosten durch Cyber-Kriminalität mit einem Fokus auf Betrug. In den sieben Jahren zwischen den Studien habe es einen Paradigmen-Wechsel bei der IKT-Nutzung gegeben: Daten werden vermehrt in der Cloud gespeichert, der Laptop wurde durch das Smartphone ersetzt, Android ersetzte Windows und die Menschen führen ihr Leben vermehrt (auch) online und in den Sozialen Medien. Dies führe dazu, dass mittlerweile die Hälfte aller Vermögensdelikte (in Anzahl und Deliktsumme) online geschehe. Die Autoren erwähnten ebenfalls, dass die Kompromittierung von Geschäfts-E-Mails (Business E-Mail Compromise, BEC) und Delikte, welche Kryptowährungen betreffen, stark zugenommen haben. Die Studienautoren stellten ausserdem fest, dass die Strafverfolgung in Bezug auf Cyber-Betrug nicht die gleiche Effizienz habe wie bei den klassischen Vermögensdelikten und regten an, dass doch mehr Geld für die Strafverfolgung aufgewendet werden solle, als für die Prävention und Antizipation. Denn auch wenn Prävention und Antizipation sehr wichtig seien, gebe es finanzwirtschaftlich gesehen noch eine zu grosse Gesamtschadenssumme.[149]

Bezüglich Ransomware besagt die Studie, dass die Kriminellen während einer Zweijahresperiode (2015-2017) ungefähr 16 Millionen Dollar Gewinn erzielt haben. Der effektive Schaden (inklusive verlorene Daten, Produktionsausfall, Erholungszeit usw.) wird jedoch um ein Vielfaches höher geschätzt.

Nach der OTA (Online Trust Alliance) der Internet Society[150] haben die Cyber-Kriminellen ihre Aktivitäten angepasst, um immer besser Geld verdienen zu können. Laut OTA haben alleine Ransomware-Angriffe letztes Jahr 8 Milliarden Dollar Schaden verursacht. Sie vermuten, dass die Kosten von Ransomware-Angriffen bis 2021 auf 20 Milliarden Dollar ansteigen werden und schätzen, dass Cyber-Angriffe im Jahr 2018 insgesamt mehr als 45 Milliarden Dollar Kosten verursacht hätten.[151,152]

148 https://www.repository.cam.ac.uk/handle/1810/294492

149 https://www.inside-it.ch/articles/54646

150 https://www.internetsociety.org/news/press-releases/2019/internet-societys-online-trust-alliance-reports-cyber-incidents-cost-45b-in-2018/

151 https://www.hackread.com/cloud-hosting-provider-insynq-hit-by-megacortex-ransomware/

152 https://www.finanzen.ch/nachrichten/aktien/internet-societys-online-trust-alliance-reports-cyber-incidents-cost-$45b-in-2018-1028337623

Gemäss einer Studie von Crowdstrike soll die Ransomware «Ryuk» innert vier Monaten über 3 Millionen Euro für ihre kriminellen Nutzer eingebracht haben. Und dies, obwohl «Ryuk» keine massenhaft versendete Ransomware ist, sondern eine, welche gezielt eingesetzt wird.[153]

Ein anderes Phänomen, welches für die Angreifer ziemlich viel Geld generiert hat, ist der sogenannte Business-E-Mail Compromise (BEC), auf Deutsch: Kompromittierung des Geschäfts-E-Mails. Darunter fallen gegen Firmen gerichtete Cyber-Angriffe, welche mit Rechnungen und Zahlungsanweisungen per E-Mail agieren. Meist werden dabei gefälschte Absender-E-Mail-Adressen oder aber kompromittierte E-Mail-Accounts der Finanzabteilung von Lieferanten und Geschäftspartnern verwendet. In den USA wurden in dreiviertel der Fälle Überweisungsversuche auf US-Konten versucht. In der Schweiz handelt es sich bei den beobachteten Fällen mehrheitlich um ausländische Konten, auf welche überwiesen werden soll. Die ans FBI gemeldeten, versuchten und erfolgreichen Überweisungsbetrügereien waren im Jahr 2018 bei einem Durchschnitt von 301 Millionen Dollar pro Monat. Wenn nur ein Bruchteil der Empfänger die falschen Rechnungen bezahlt oder die fiktiven Überweisungsaufträge ausführt, dann machen die Angreifer ein gutes Geschäft. Die Studie hält fest, dass der klassische CEO-Betrug (angeblicher CEO gibt dringende Zahlungsanweisung an die Finanzabteilung)[154] rückläufig ist und gefälschte Zahlungsanweisungen zunehmend im Namen von externen Personen (Kunden, Lieferanten, usw.) gemacht werden. Manchmal sind die E-Mail-Konten der externen Personen gehackt, manchmal wird aber auch einfach ihre Adresse *gespooft*, also als gefälschter Absender verwendet. BEC ist ein lukratives Geschäft, da die Gewinne ziemlich hoch sind, das Risiko und der Aufwand aber verhältnismässig gering.[155]

Eine weitere spannende Studie stammt von der Sicherheitsfirma Positive Technology.[156] Diese versucht zu beschreiben, wie viel eine *APT*-Attacke für die Angreifer kostet. *APT*s sind staatlich gesponserte Akteure, welche auch im Dienst von finanziell eher schwachen Staaten stehen können. Anhand der verwendeten Angriffswerkzeuge versuchen die Forscher die Kosten abzuschätzen, welche für das Beschaffen oder Herstellen der Tools aufgewendet werden müssen. Sie kommen zum Schluss, dass ein Tool für den *Spear-Phishing*-Versand (gezieltes Phishing) ungefähr 2'000 Dollar kosten würde. Hinzu kommt Penetration-Testing-Software für zwischen 8'000 und 40'000 Dollar. Die Werkzeuge für eine Bank-Attacke würden somit mindestens 55'000 Dollar kosten. Eine Cyber-Spionagekampagne hingegen kostet von Beginn weg mindestens 500’000 Dollar Diese Zahlen sind aber mit Vorsicht zu geniessen, da die Preise für Angriffswerkzeuge ziemlich variieren. Wenn eigene Werkzeuge entwickelt werden, sind die Kosten in der Regel höher einzuschätzen, da dazu das entsprechende Fachwissen von Hackern und Software-Entwicklern bezahlt werden muss. Andererseits gibt es Angriffswerkzeuge, welche legal kommerziell erhältlich sind und auch von angeheuerten Penetration-Testern verwendet werden. Diese sind meistens günstiger und machen es auch schwieriger, die Angriffe spezifischen *APT*s zuzuweisen, da die gleichen Werkzeuge von verschiedenen Gruppen oder Nationen verwendet werden.

---

153 https://www.lemonde.fr/pixels/article/2019/01/14/le-rancongiciel-ryuk-a-rapporte-plus-de-3-millions-d-euros-a-ses-auteurs_5408807_4408996.html

154 Siehe oben Kap. 4.4.5.

155 https://www.fincen.gov/sites/default/files/shared/FinCEN_Financial_Trend_Analysis_FINAL_508.pdf

156 https://www.ptsecurity.com/ww-en/analytics/advanced-persistent-threat-apt-attack-cost-report/

Auf Grund der Vorfälle der letzten Jahre und der erhöhten Sensibilisierung erhöhen immer mehr Unternehmen ihr Budget für die Cyber-Sicherheit. Eine Studie von ESI ThoughtLab[157] besagt, dass sich der mittlere Schaden von Cyber-Attacken im letzten Fiskaljahr auf 4.7 Millionen Dollar pro Opfer belief, wobei mehr als 1 von 10 Firmen über 10 Millionen Dollar verlor. Die Studienautoren machten eine Umfragen bei verschiedenen Firmen, ob diese Opfer eines Angriffs geworden sind und ob sie vorhätten, in Zukunft mehr Geld in die Cyber-Sicherheit zu investieren. Anscheinend werden Firmen in den meisten Sektoren ihre Investitionen in die Cyber-Sicherheit deutlich erhöhen.

Beurteilung:

Cyber-Kriminalität boomt, da vielfach mit relativ einfachen Mitteln sehr viel Geld verdient werden kann. Das Einsteiger-Kapital für Cyber-Kriminelle hält sich in Grenzen und auch das Fachwissen muss nicht immens sein, da es immer mehr Angriffsmethoden gibt, welche *aaS («as-a-Service») verkauft werden. Das heisst, eine Hackergruppe stellt zum Beispiel Ransomware-as-a-Service zu Verfügung, welche von Kriminellen gekauft und mit relativ we-nig Fachwissen verwendet werden kann, um grosse Gewinne zu erzielen respektive grossen Schaden anzurichten.

Eines der Ziele im Kampf gegen Cyber-Kriminalität ist es, das Business Modell der Cyber-Kriminellen zu durchbrechen. Das heisst den Aufwand erhöhen und das Geldverdienen schwieriger machen, sodass die Gewinne kleiner ausfallen. Opportunistische Cyber-Kriminelle versuchen mit einfach zur Verfügung stehenden Mitteln in Netzwerke einzudringen. Ist die Firma einigermassen gut geschützt und der Einsatz von Standard-Angriffswerkzeugen nicht auf Anhieb erfolgreich, suchen sie sich bald ein anderes, schlechter geschütztes Ziel. Diese Aussage gilt natürlich nicht für staatlich gesponserte Angreifer, da diese meist gezielt in ein bestimmtes Netzwerk eindringen sollen und daher auch viel Zeit und Geld in einen Angriff auf ein bestimmtes Ziel investieren können.

6.2 Persönlicher Datenschutz und gesellschaftliche Schutzmassnahmen – Wo liegt die Balance?

Im persönlichen wie auch im geschäftlichen Alltag verwenden wir immer selbstverständlicher Verschlüsselungstechnologien, wie es vor einigen Jahren noch kaum vorstellbar war. Viele nutzen zur Kommunikation beispielsweise «WhatsApp», dass in der aktuellen Version das Signal-Protokoll zur End-to-End Verschlüsselung der Chats einsetzt. Das bedeutet, dass die geschriebenen Nachrichten nur auf dem Sender- und Empfängergerät als Klartext vorliegen. Auf dem Transport durchs Internet werden die Texte verschlüsselt übertragen. Neben der zwischenmenschlichen Kommunikation geschieht auch das Aufrufen von Websites immer häufiger verschlüsselt. Auswertungen der Telemetriedaten der Browser Chrome[158] und Firefox[159] zeigen, dass über diese Browser aufgebaute Verbindungen inzwischen in rund 4/5 der Fälle

157 https://www.helpnetsecurity.com/2019/07/15/boost-cybersecurity-investments/

158 https://transparencyreport.google.com/https/overview?hl=de

159 https://letsencrypt.org/stats/

durch TLS-Zertifikate gesichert sind. Dazu beigetragen hat sicherlich, dass sich Website-Betreiber über die Initiative «Let's Encrypt»[160] der Non-Profit Organisation Internet Security Research Group (ISRG), kostenlos Zertifikate ausstellen lassen können.

Die Entwicklung hin zu mehr und besser verschlüsselten Verbindungen wird sich weiter akzentuieren. So wurde letztes Jahr von der Internet Engineering Task Force (IETF) das Transport Layer Security-Protokoll in der Version 1.3 (TLS 1.3) freigegeben.[161] *DNS*-Abfragen werden ebenfalls vermehrt verschlüsselt übertragen. So plant Mozilla für seinen Browser Mozilla Firefox «DNS-over-https (DoH)» standarmässig zu aktivieren.[162] In der aktuellen Android Version 9 wird «DNS-over-TLS (DoT)» falls verfügbar vom System forciert[163] und die neue Mobilfunkgeneration 5G bietet besseren Schutz vor falschen Mobilfunkantennen.[164]

All diese Weiterentwicklungen verbessern die Vertraulichkeit der Verbindungen für Nutzer von Endgeräten, schränkt aber teilweise etablierte Schutzmechanismen vor kriminellen Inhalten oder Überwachungsmöglichkeiten der Strafverfolgung ein. So verhindern die verschlüsselten *DNS*-Abfragen, dass diese von Angreifern auf dem Netzwerkpfad verändert werden können, verunmöglichen aber je nach angefragtem Server, Warnungen der Internetanbieter vor Phishing-Seiten oder Seiten, die versuchen, *Malware* auszuliefern. Auch MELANI unterstützt beispielsweise Blacklist-Betreiber, damit Internetnutzer nicht auf Phishing-Seiten landen[165] und ungewollt ihre Zugangsdaten beispielsweise zum E-Banking preisgeben. Eine ähnliche Problematik stellt sich auch bei der SSL-Terminierung, wo verschlüsselte Verbindungen auf einem *Proxy* aufgebrochen werden, um schädliche Inhalte wie *Malware* herauszufiltern. Die etablierten Methoden, die von vielen Firmen eingesetzt werden, werden durch TLS1.3 massiv erschwert bis verunmöglicht.

Speziell im Umfeld der Strafverfolgung wurde die Entwicklung hin zu mehr Verschlüsselung mehrfach heftig diskutiert,[166] da die eingespielten Mechanismen zum Schutz vor kriminellen Inhalten und zur Überwachung von Kriminellen auf gewisse Schwachstellen im Aufbau der Infrastruktur angewiesen waren. Problematisch ist, dass anstatt Wege zu suchen, wie der Schutz und die legale Überwachung ohne Sicherheitsverlust in der persönlichen Anwendung der Technologie umgesetzt werden könnte, einige staatliche Akteure mit Verboten neuer Technologie oder Vorschriften zum Einbau von Hintertüren agierten. Dabei wurde häufig fahrlässig argumentiert, dass diese Massnahmen die Sicherheit der Anwender nicht beinträchtige. Erst kürzlich hat die Argumentationslinie beim amerikanischen Justizminister insofern geändert, dass eingestanden wird, dass die vorgeschlagenen Massnahmen zum staatlichen Schutz der Gesellschaft nicht ohne Sicherheitsverlust der Endanwender möglich ist.[167]

---

160 https://letsencrypt.org/about/

161 https://www.ietf.org/blog/tls13/

162 https://blog.mozilla.org/futurereleases/2019/04/02/dns-over-https-doh-update-recent-testing-results-and-next-steps/

163 https://android-developers.googleblog.com/2018/04/dns-over-tls-support-in-android-p.html

164 https://www.zdnet.com/article/stingray-spying-5g-will-protect-you-against-surveillance-attacks-say-standards-setters/

165 https://www.antiphishing.ch/de/informationen/

166 https://www.theregister.co.uk/2019/06/25/andrew_sullivan_internet_society_interview/

167 https://www.schneier.com/blog/archives/2019/07/attorney_genera_1.html

Auf einer transparenten Grundlage kann so in einer Firma wie auch in einem Staat als Ganzes diskutiert werden, welche persönlichen Einschränkung zur Minderung der übergeordneten Risiken toleriert werden können. Ein Beispiel, wie die SSL-Terminierung unter Einhaltung des persönlichen Datenschutzes umsetzen werden kann, gibt die Checkliste des Zürcher Datenschützers zur Entschlüsselung von Web-Verbindungen.[168]

Sämtliche Organisationen sollten in ihrem Umfeld die neuen Technologien zur Steigerung der Sicherheit der Infrastruktur der beteiligten Personen gewinnbringend nutzen und nur sehr wohlüberlegt Einschränkungen dieser Massnahmen zum Schutz vor kriminellen Inhalten einführen. Auf Maximalpositionen zu verharren wird Beteiligte, die damit nicht einverstanden sind, zu Umgehungsmassnahmen verleiten. Nur mit der richtigen Balance kann im Internet der Zukunft die gewünschte optimale Sicherheit für alle erzielt werden.

6.3 Drohende Deglobalisierung der Lieferketten?

Stellen Sie sich folgendes Szenario vor: Ein Software-Fehler in einer Fahrzeugsteuerungskomponente eines Zulieferers führt in seltenen Fällen zu Fehlfunktionen beim Bremsverhalten der betroffenen Autos. Das mag unschön klingen, aber durch einen raschen Rückruf der betroffenen Modelle verschiedenster Autohersteller, welche diese Komponente einsetzen, lässt sich das Problem bei der Garage des Vertrauens mit einem Software-Update in 15 Minuten beheben. Nur das neue, vermeintlich europäische Auto, das man nach eingehenden Überlegungen insbesondere wegen seiner Verkehrssicherheit gekauft hat, bleibt vom Update ausgeschlossen. Grund dafür ist, dass wegen angeblicher nationaler Sicherheitsinteressen der Fahrzeugzulieferer in seinem Heimatland unter ein Exportkontrollregime gestellt wurde und leider keinen Technologietransfer mehr mit Unternehmen tätigen darf, deren Mutterkonzern ihren Hauptsitz in China haben.

Was als arg konstruiert daherkommen mag, hat sich im ersten Halbjahr 2019 in der Kommunikationsindustrie tatsächlich in ähnlicher Art abgespielt. Per 16. Mai 2019 erliess das US-Commerce Department's Bureau of Industry and Security (BIS) eine so genannte «Final Rule», welche den chinesischen IKT-Hersteller Huawei und damit verbundene Tochterunternehmen auf eine Liste mit Organisationen setzte, welche den Transfer von Gütern und Know-How an diese Geschäftseinheiten unter ein Exportkontrollregime stellen. Damit ist US-Unternehmen ohne spezielle Bewilligung untersagt, Geschäfte mit diesen Organisationen zu tätigen. Als Resultat verkündete Google einige Tage später, dass es in absehbarer Zukunft keine Android Updates mehr an Huawei liefern wird und die Mobiltelefone des Unternehmens über kurz oder lang aus dem Google-Ökosystem verbannt werden. Kurz darauf machten die Chip-Hersteller Intel, Qualcomm und Broadcomm ähnliche Aussagen.

Huaweis Reaktion auf die Äusserungen der Chip-Hersteller war in erster Linie darauf fokussiert, Kunden dahingehend zu versichern, dass im Vorfeld genügend Hardware gehortet wurde und man für diese Umstände auch über von US-Herstellern unabhängige Alternativen verfüge, um die geplanten Lieferungen zu erfüllen, wie beispielsweise für Sunrise mit Blick auf den

[168] https://dsb.zh.ch/internet/datenschutzbeauftragter/de/publikationen/anleitungen/_jcr_content/contentPar/form/formitems/kein_titel_gesetzt__0/download.spooler.download.1562593220478.pdf/Checkliste-Entschluesselung-Webverbindungen.pdf

Aufbau der 5G-Netzwerkinfrastruktur. In Anbetracht des drohenden Ausschluss aus der Android-Familie verkündete der chinesischen Handyhersteller beispielsweise die Möglichkeit, ein eigenes Betriebssystem und damit ein eigenes Ökosystem zu schaffen.

Mit ihrem unterdessen temporär verschobenen und leicht abgeschwächtem Durchgriff auf die heimische IKT-Industrie[169] eskalierten die US-Behörden einen grundsätzlich bilateralen Handelsstreit endgültig auf die globale Ebene und legten damit auch die Verwundbarkeit der höchst globalisierten Lieferketten dar, gerade mit Blick auf die Kommunikationsindustrie. Waren höhere Kosten auf Grund der gegenseitigen Sanktionen zwischen China und den USA die grösste Bedrohung für nicht US und chinesische Unternehmen sowie Kunden, stellt sich jetzt auch für Schweizer Nutzer von Huawei-Produkten und Komponenten die Frage nach deren Besitzstandwahrung, Lebensdauer, Unterhalt und Interoperabilität in der Zukunft. Und ganz generell die Frage, ob mit diesem Ausspielen der de facto vorherrschenden Marktmacht eines Staates ein Präjudiz geschaffen wurde, welches gleichgeartete Aktionen in anderem Kontext nach sich zieht. Der wirtschaftspolitische Unterton der Unterstellung Huaweis unter das US-Sanktionsregime ist dabei kaum zu überhören. Entsprechend steht zumindest hypothetisch die Frage im Raum, ob Ähnliches gegen einen ungeliebten, nicht chinesischen Hersteller nicht auch möglich wäre, abgesehen von Planungsunsicherheiten und Kosten, die die jetzige Situation bereits mit sich bringen.

Lieferketten sind heute ein globales Phänomen und das nicht nur im Bereich der IKT sondern in praktisch allen industriellen Fertigungen. Zulieferer sind denn auch nicht auf nur eine Handvoll Länder beschränkt. Der in Thalwil ansässige ETH-Spin-Off U-Blox spielt beispielsweise als Lieferant von hochpräzisen Ortungskomponenten bei der Entwicklung und Herstellung von autonomen Fahrzeugen international führend mit. Im Kern dieser globalisierten Lieferketten liegt der Grundsatz, dass Technologie und Know-How nach marktwirtschaftlichen Grundsätzen gehandelt, verbaut und eingesetzt werden können, um eine breite Auswahl von Endprodukten herstellen zu können, über deren Erfolg oder Misserfolg am Ende der Markt entscheidet.

Störungen dieses Systems treffen als erstes kleine, offene Volkswirtschaften wie die Schweiz, die mangels inländischer Alternativen auf ausländische Anbieter und mit Blick auf die eigene Zuliefererindustrie auf ausländische Kunden angewiesen sind, in einem möglichst offenen, global interoperablen Angebots- und Nachfragemarkt. Sei es mit Blick auf Planbarkeit, Investitionssicherheit oder der Möglichkeit, sich im Rahmen des Risikomanagements für eine Mischung von (Infrastruktur-) Komponenten aus unterschiedlichen staatlichen Einflusssphären zu entscheiden.

Die im Mai angestossene Dynamik birgt allerdings die Gefahr einer mittel- bis langfristigen Regionalisierung der Lieferketten und kann in extremis dazu führen, dass die Grundsicherheit gewisser Produkte temporär nicht mehr gewährleistet ist. Oder in Anlehnung an das einleitende Beispiel: Die Bremsen des Neuwagens zu Hause werden bis zur Verfügbarkeit eines Workaround des Autoherstellers in 1:100'000 Fällen weiterhin versagen, weil der staatliche Eingriff in die Lieferkette eine zeitnahe Lösung nicht zulässt.

[169] Vergleiche auch MELANI Halbjahresbericht 2018/2, Kap. 3.

7 Politik, Forschung, Policy

7.1 CH: Parlamentarische Vorstösse

Geschäft	Nummer	Titel	Eingereicht von	Datum Einreichung	Rat	Amt	Stand Beratung & Link
Mo	19.3009	Impulsprogramm zur Verbreitung innovativer Digitalisierungsprojekte im Bildungsbereich	WBK-NR	21.02.2019	NR	WBK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193009
Mo	19.3010	Lancierung eines Digitalisierungs-Impulsprogramms für eidgenössische und kantonale Universitäten, Fachhochschulen, Berufsbildung und Weiterbildung	Kommission für Wissenschaft, Bildung und Kultur (WBK-NR)	21.02.2019	NR	WBF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193010
Ip	19.3051	Huawei und die Herausforderungen von 5G. Risiken und Chancen für die Schweiz	Regazzi Fabio	06.03.2019	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193051
Mo	19.3121	Nationale Vorgehensweise bei Datenlecks	Buffat Michaël	14.03.2019	NR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193121
Po	19.3135	Haben wir die Cybersicherheit bei Beschaffungen der Armee im Griff?	Dobler Marcel	18.03.2019	NR	VBS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193135
Po	19.3136	Haben wir die Hard- und Softwarekomponenten bei unseren kritischen Infrastrukturen im Griff?	Dobler Marcel	18.03.2019	NR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193136
Ip	19.3139	Cyberbedrohungen mit Attachés minimieren	Müller Damian	18.03.2019	SR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193139
Ip	19.3185	Keine digitalen Hintertüren bei Beschaffungen des Bundes	Vogler Karl	20.03.2019	NR	VBS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193185
Po	19.3199	Verbesserung der Sicherheit von mit dem Internet verbundenen Produkten	Reynard Mathias	21.03.2019	NR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193199
Ip	19.3205	Abnehmende Dynamik bei der Digitalisierung. Was unternimmt der Bundesrat?	Burkart Thierry	21.03.2019	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193205
Ip	19.3255	Die liberale Demokratie gegen das Erstarken von Antisemitismus und rechtsextremem Gedankengut verteidigen.	Wermuth Cédric	21.03.2019	NR	EDI	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193255
Ip	19.3267	Entspricht die Praxis des Dienstes ÜPF hinsichtlich der Pflichten der Anbieterinnen abgeleiteter Kommunikationsdienste dem Gesetz?	Flach Beat	21.03.2019	NR	EJPD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193267

Geschäft	Nummer	Titel	Eingereicht von	Datum Einreichung	Rat	Amt	Stand Beratung & Link
Ip	19.3321	Die Einführung der neuen 5G-Mobilfunktechnologie in der Schweiz erfordert eine gute Aufklärung der Bevölkerung durch den Bund	Amman Thomas	22.03.2019	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193321
Ip	19.3330	Sollen Patientendaten an den Meistbietenden verkauft werden?	Reynard Mathias	22.03.2019	NR	EDI	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193330
Po	19.3342	Zulassungssystem für Open Government Data	Badran Jacqueline	22.03.2019	NR	EDI	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193342
Ip	19.3377	Kantonale Unterschiede beim Strafverfahren wegen Kinderpornografie. Noch immer kein Handlungsbedarf?	Guhl Bernhard	22.03.2019	NR	EJPD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193377
Mo	19.3428	Notwendige Erweiterung des Beirats "Digitale Transformation"	Kälin Irène	07.05.2019	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193428
Ip	19.3431	Wirtschaftliche Vorteile und gesundheitliche Folgen von 5G?	Fiala Doris	07.05.2019	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193431
Mo	19.3448	Provisorische Rechtsöffnung - Anpassung an die gewandelte Geschäftspraxis (Digitalisierung)	Dobler Marcel	08.05.2019	NR	EJPD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193448
Ip	19.3461	Cybersicherheit. Die Zukunft allein oder gemeinsam meistern?	Béglé Claude	08.05.2019	NR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193461
Ip	19.3505	Vergabe von Mobilfunkkonzessionen für 5G ohne entsprechende Grundlagen für die Bewilligungsbehörden	Töngi Michael	09.05.2019	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193505
Ip	19.3534	5G: Wenn eine Arbeitsgruppe die Auswirkungen der Strahlung in der Schweiz untersucht, ist die Unabhängigkeit der Gruppenmitglieder mindestens ebenso wichtig wie deren Kompetenzen	Borloz Frédéric	03.06.2019	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193534
Ip	19.3535	Einführung der 5G-Technologie in der Schweiz: Welche Kompensation vom Bund angesichts des Mehraufwands für die Kantone?	Gschwind Jean-Paul	03.06.2019	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193535
Po	19.3574	Offensive für einen digitalen Service public	Marti Min Li	11.06.2019	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193574
Po	19.3593	Digitalisierung naturwissenschaftlicher Sammlungen zu Gunsten der Schweizer Forschung	Germann Hannes	12.06.2019	SR	WBF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193593

Geschäft	Nummer	Titel	Eingereicht von	Datum Einreichung	Rat	Amt	Stand Beratung & Link
Mo	19.3649	Rechtliche Grundlage für einen Digitalisierungsfonds	Savary Géraldine	18.06.2019	SR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193649
Ip	19.3659	Swisscom lanciert Datenkraken Beem: Wie ist das mit der Eignerstrategie des Bundes vereinbar?	Marti Samira	19.06.2019	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193659
Mo	19.3663	Ein Digitalrat - im Namen des Volkes!	Pardini Corrado	19.06.2019	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193663
Ip	19.3686	Tallinn Deklaration zu eGovernment: Wo steht die Schweiz heute und was ist zu tun?	FDP-Liberale Fraktion	19.06.2019	NR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193686
Ip	19.3693	Digitale Transformation - eine grosse Herausforderung	Fiala Doris	19.06.2019	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193693
Po	19.3759	Digital taugliche Formerfordernisse im Konsumkreditgesetz	Dobler Marcel	20.06.2019	NR	EJPD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193759
Po	19.3785	Der digitale Analphabetismus führt zu sozialer Ausgrenzung	Reynard Mathias	20.06.2019	NR	EDI	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193785
Ip	19.3787	Was unternimmt der Bund gegen Hassreden ("hate speech") im Internet?	Seiler Graf Priska	20.06.2019	NR	EJPD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193787
Po	19.3850	Wie kann man eine effiziente Beteiligung des Privatsektors an Entwicklungsprojekten gewährleisten und neue Technologien fördern?	Béglé Claude	21.06.2019	NR	EDA	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193850
Ip	19.3865	Internationales Genf: wie kann die Schweiz internationale Organisationen und NGO im Prozess der Digitalisierung unterstützen und dabei gleichzeitig den Schutz der Daten von Kriegsopfern gewährleisten?	Derder Fathi	21.06.2019	NR	EDA	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193865
Ip	19.3866	Ein Cyberkommando für die Schweizer Armee?	Candinas Martin	21.06.2019	NR	VBS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193866
Po	19.3878	5G darf die Netzneutralität nicht gefährden	Béglé Claude	21.06.2019	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193878
Mo	19.3884	Eine Strategie für die digitale Souveränität der Schweiz	Derder Fathi	21.06.2019	NR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193884

Geschäft	Nummer	Titel	Eingereicht von	Datum Einreichung	Rat	Amt	Stand Beratung & Link
Ip	19.3919	Künstliche Intelligenz (KI) und Digitale Transformation - Wir brauchen eine holistische Strategie	Ricklin Kathy	21.06.2019	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193919
Pl	19.417	Schaffung einer Medienförderabage auf digitalen Prattfomren	Töngi Michael	21.03.2019	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20190417
Pl	19.418	Für ein Fördermodell zugunsten der elektronischen Medien	Töngi Michael	22.03.2019	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20190418
Fr	19.5274	5G-Technologie.Informieren und erklären, um einige verbreitete Vorurteile zu entkräften	Regazzi Fabio	05.06.2019	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20195274
Fr	19.5286	5G-Antennen - welche Grenzwerte gelten?	Schneider Schüttel Ursula	05.06.2019	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20195286
Fr	19.5296	5G-Technologie - Alternativen?	Schneider Schüttel Ursula	05.06.2019	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20195296
Fr	19.5315	Ist 5G schon in Betrieb?	Hardegger Thomas	11.06.2019	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20195315
Fr	19.5349	5G - wie weiter?	Bigler Hans-Ulrich	12.06.2019	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20195349
Fr	19.5355	5G: Verspätung und Kosten für die Wirtschaft?	Brunner Hansjörg	12.06.2019	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20195355
Fr	19.5370	Beem	Masshardt Nadine	12.06.2019	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20195370

7.2 CSS-Studie vergleicht Nationale Cyber-Sicherheitsstrategien – Herausforderungen für die Schweiz

Das Center for Security Studies (CSS) der ETH Zürich hat im März 2019 eine Vergleichsstudie über nationale Cyber-Sicherheitsstrategien der Länder Deutschland, Finnland, Frankreich, Holland, Israel, Italien und der Schweiz veröffentlicht und kommt zu folgenden Erkenntnissen.[170] Die Cyber-Sicherheitsstrategien weisen generell viele konzeptionelle Gemeinsamkeiten auf. Speziell erwähnt seien zentrale Aspekte wie der holistische Ansatz, welcher sowohl die nationale Sicherheit als auch sozioökonomische Anliegen umfasst; der hohe Stellenwert der internationalen Kooperation, die Betonung der notwendigen Zusammenarbeit mit dem Privatsektor sowie die Notwendigkeit umfassender Sensibilisierung, Bildung und Information. Die wichtigsten Unterschiede liegen in der Ansiedelung der Cyber-Sicherheit im Rahmen der staatlichen Strukturen sowie die Zuteilung der Verantwortlichkeiten. Dies betrifft insbesondere das Ausmass der Zentralisierung und die Beziehung zwischen zivilen und militärischen Kräften. Die Gründe für die Unterschiede sind grösstenteils auf die politische Kultur und die Organisation der politischen Systeme zurückzuführen.

Im Rahmen der Entwicklung und Umsetzung der nationalen Strategien hat das CSS verschiedene Herausforderungen erkannt. So zum Beispiel die vertikale Integration der nationalen Cyber-Sicherheit in den Rahmen der nationalen Sicherheit und die horizontale Koordination der verschiedenen Stellen, welche mit Cyber-Sicherheit beauftragt sind. Weiter werden sich die Länder künftig vermehrt mit der Förderung internationaler Zusammenarbeit und der Ausbildung internationaler Verhaltensnormen im Cyber-Raum auseinandersetzen müssen. Die Notwendigkeit von adäquaten Lagebildern und effizientes Krisenmanagement runden die künftigen Anforderungen ab.

7.3 Die Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)

In den letzten zwei Jahren hat der Bundesrat grundlegende Entscheide für den Schutz der Schweiz vor Cyber-Risiken getroffen. Im April 2018 hat er die «Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)»[171] für die Jahre 2018–2022 verabschiedet. Das übergeordnete Ziel der NCS ist, dass die Schweiz bei der Nutzung der Chancen der Digitalisierung angemessen vor Cyber-Risiken geschützt und ihnen gegenüber resilient ist. Aus dieser Vision abgeleitet, identifiziert die NCS sieben strategische Ziele, welche über 29 Massnahmen in insgesamt zehn Handlungsfeldern erreicht werden sollen.

Im Unterschied zur ersten NCS von 2012-2017 ist der Bereich der Cyber-Verteidigung, welcher sich auf die Rolle der Armee und des Nachrichtendienstes bei der Attribution, der Unterbindung von Cyber-Angriffen und der Gewährleistung der militärischen Einsatzbereitschaft bezieht, integraler Bestandteil der Strategie. Weitere Neuerungen betreffen die Ausweitung der Zielgruppe auf die gesamte Wirtschaft und Gesellschaft (die erste Strategie fokussierte auf den Schutz kritischer Infrastrukturen) und den stärkeren Fokus auf Standardisierung und Regulierung, wozu auch die Prüfung einer Meldepflicht gehört. Mit diesen Anpassungen wird die NCS ihrer Funktion als Gesamtstrategie gerecht, berücksichtigt die zunehmende Bedeutung

170 https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/MELANI%20Studie_final_AW_18März2019.pdf

171 https://www.isb.admin.ch/isb/de/home/themen/cyber_risiken_ncs/ncs_strategie.html

von Cyber-Risiken für alle Unternehmen und bietet die Grundlage für die Erarbeitung von Standards und regulativen Massnahmen.

7.3.1 Umsetzungsplan und Organisation des Bundes im Bereich Cyber-Risiken

Es ist klar, dass das ambitionierte Portfolio der NCS nur dann erfolgreich umgesetzt werden kann, wenn die Arbeiten der verschiedenen beteiligten Akteure optimal aufeinander abgestimmt und alle vorhandenen Kompetenzen genutzt werden. Alle beteiligten Stellen von Bund, Kantonen, Wirtschaft und Hochschulen haben deshalb gemeinsam den Umsetzungsplan[172] zur NCS erarbeitet, welcher vom Bundesrat am 15. Mai 2019 beschlossen wurde.[173] Der Umsetzungsplan legt für jede Massnahme fest, welche Organisation bis wann welche Projekte umsetzt und bildet so die Basis für das strategische Controlling mit welchem der Umsetzungsfortschritt der NCS überprüft werden wird.

Gleichzeitig mit der Erarbeitung des Umsetzungsplans hat der Bund seine eigene Organisation überprüft und angepasst.[174] Die wesentlichen Elemente dieser Organisation mit Bezug auf die Umsetzung der NCS sind in der nachfolgenden Abbildung veranschaulicht.

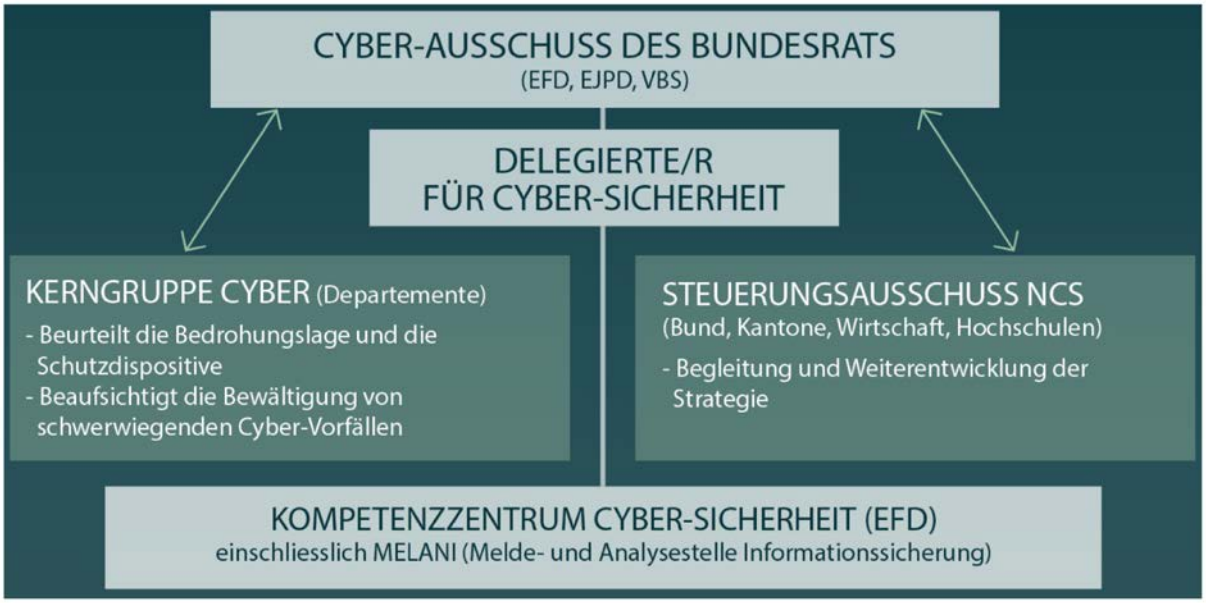

Abbildung 8: Organisation des Bundes im Bereich Cyber-Risiken

Wichtige Elemente der neuen Organisation sind die Stärkung der überdepartementalen Koordination und der Zusammenarbeit mit der Wirtschaft, den Kantonen und den Hochschulen. Folgende Gremien sind für diese Aufgaben neu geschaffen worden:

- Der **Cyber-Ausschuss des Bundesrats,** welcher sich aus den Vorstehenden des Eidgenössischen Finanzdepartements (EFD), des Eidgenössisches Justiz- und Polizeide-

172 https://www.isb.admin.ch/isb/de/home/themen/cyber_risiken_ncs/umsetzungsplan.html
173 https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-75046.html
174 https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-73839.html

partements (EJPD) und des Eidgenössische Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS) zusammensetzt, hat die Aufgabe, die Umsetzung der NCS zu beaufsichtigen.

- Die **Kerngruppe Cyber-Sicherheit** stärkt die Koordination zwischen den drei Bereichen Sicherheit, Verteidigung und Strafverfolgung, sorgt für eine gemeinsame Beurteilung der Bedrohungslage und beaufsichtigt die Bewältigung von schwerwiegenden und departementsübergreifenden Vorfällen durch die Bundesstellen.
- Der **Steuerungsausschuss NCS (StA NCS)** stellt die koordinierte und zielgerichtete Umsetzung der NCS-Massnahmen sicher und erarbeitet Vorschläge zur Weiterentwicklung der NCS.

7.3.2 Der Delegierte für Cyber-Sicherheit und das Kompetenzzentrum Cyber-Sicherheit

Neben den koordinierenden Gremien wurden mit dem Delegierten für Cyber-Sicherheit und dem Kompetenzzentrum Cyber-Sicherheit zentrale Strukturen geschaffen. Der Delegierte für Cyber-Sicherheit übernimmt die strategische Leitung der Cyber-Sicherheit im Bund, leitet das Kompetenzzentrum ebenso wie die vom Bund eingesetzten überdepartementalen Gremien (mit Ausnahmen des Cyber-Ausschusses) und vertritt den Bund in weiteren Gremien. Diese zentrale Position konnte mit der Person von Florian Schütz besetzt werden.[175] Er hat seine Aufgaben im August 2019 übernommen und ist direkt dem Vorsteher des Finanzdepartements unterstellt.

Das Kompetenzzentrums des Bundes für die Cyber-Sicherheit im EFD wird die nationale Anlaufstelle für alle Fragen mit Bezug zur Cyber-Sicherheit. Es baut dabei auf der bestehenden Organisation von MELANI auf und baut diese so aus, dass sie Dienstleistungen für die gesamte Wirtschaft anbieten und für die Bevölkerung Warnungen und Informationen zu Cyber-Risiken herausgeben kann. Innerhalb des Bundes unterstützt es die Ämter mit Cyber-Fachwissen bei Prävention, Standardisierung und Regulierung. Es erhält bei der Bewältigung von Cyber-Vorfällen Weisungskompetenzen gegenüber den Bundesstellen.

Der Bundesrat hat mit der Verabschiedung des Umsetzungsplans zur NCS auch Ressourcen für das Kompetenzzentrum Cyber-Sicherheit gesprochen, so dass dieses ab dem 1. Januar 2020 die bestehenden operativen Tätigkeiten von MELANI entsprechend ausweiten kann.

Eine detailliertere Beschreibung des Kompetenzzentrums des Bundes für Cyber-Sicherheit und seiner Aufgaben erscheint im nächsten MELANI Halbjahresbericht.

[175] https://www.efd.admin.ch/efd/de/home/dokumentation/nsb-news_list.msg-id-75421.html

8 Publizierte MELANI Produkte

8.1 GovCERT.ch Blog

8.1.1 Severe Ransomware Attacks Against Swiss SMEs

09.05.2019 - As we have seen an ever-increasing number of ransomware cases that show a rather sophisticated modus operandi, we are publishing a warning via MELANI Newsletter along with this blog post, documenting technical details about the recent ransomware attacks against Swiss small and medium enterprises (SMEs). The goal of this blog post is to give you a better understanding of the various modus operandi of the most common ransomware families we have encountered hitting Swiss targets in the past months.

➔ https://www.govcert.admin.ch/blog/36/severe-ransomware-attacks-against-swiss-smes

8.2 MELANI Newsletter

8.2.1 Sextortion: Zahlreiche Schweizerinnen und Schweizer betroffen – Behörden lancieren «stop-sextortion.ch»

24.04.2019 - Erpresser behaupten in einer Mail, Zugang zu Computer und Webcam zu haben und drohen damit, Bilder und Videos mit sexuellem Inhalt zu veröffentlichen, sollte kein Lösegeld bezahlt werden. Diese Betrugsmasche wird Fake-Sextortion genannt und dabei wird typischerweise eine Bezahlung in Bitcoins gefordert. Mit dieser Betrugsmethode haben Kriminelle in den letzten sechs Monaten trotz der kleinen geforderten Summen Bitcoins im Wert von ca. 360'000 Franken erbeutet. Solange die betroffenen E-Mail-Empfänger Lösegeld bezahlen, wird dieses Vorgehen befeuert und weiterhin eingesetzt. Helfen Sie mit, diese Masche zu stoppen und zahlen Sie kein Lösegeld. Auf der Website «stop-sextortion.ch», die von den Behörden heute lanciert wurde, finden Sie Informationen und können Fake-Sextortion E-Mails melden.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/fake-sextortion.html

8.2.2 Verschlüsselungstrojaner greifen vermehrt gezielt Unternehmensnetzwerke an

09.05.2019 - Seit Anfang 2019 häufen sich die Meldungen von KMUs und Grossunternehmen im In- und Ausland, dass deren Daten von Verschlüsselungstrojanern, sogenannter «Ransomware», verschlüsselt und somit unlesbar gemacht wurden. Bei diesen Angriffen wurden teilweise auch die Backups verschlüsselt. Dadurch wird die Wiederherstellung der Geschäftstätigkeit der betroffenen Unternehmen unmöglich.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/verschluesselungstrojaner-greifen-vermehrt-gezielt-unternehmensn.html

9 Glossar

Begriff	Beschreibung
APT Advanced Persistent Threat	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.
BGP Border Gateway Protocol	Das Border Gateway Protocol ist das im Internet eingesetzte Routingprotokoll, welches den Weg von Datenpaketen zwischen Netzwerken bestimmt.
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.
Botnetz	Mehrere Bots können ein Netzwerk bilden. Dieses wird über eine Command & Control-Infrastruktur gesteuert.
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.
C2 Command & Control	Befehls- und Steuerungsinfrastruktur von Botnetzen. Die meisten Bots können über einen Kommunikationskanal überwacht werden und Befehle empfangen.
CaaS Cybercrime-as-a-Service	Cyber-Kriminalität als einkaufbare Dienstleistung ermöglicht technisch wenig versierten Kriminellen durch einfach zu bedienende Werkzeuge, illegale Aktivitäten auch im Internet durchzuführen.

Begriff	Beschreibung
CEO-Betrug / CEO-Fraud	Von 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.
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.
DNS Domain Name System	Mit Hilfe des 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).
Drive-by-Infektion	Infektion eines Computers mit Malware allein durch Besuch einer Webseite. Die Infektion erfolgt meistens durch das Ausprobieren von Exploits für vom Besucher noch nicht geschlossene Sicherheitslücken.
Dropper / Downloader	Ein Dropper oder 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.

Begriff	Beschreibung
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.
GPS Global Positioning System	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.
ISP Internet Service Provider	Internetdienstanbieter oder Internetdienstleister sind Anbieter von Diensten, Inhalten oder technischen Leistungen, die für die Nutzung oder den Betrieb von Inhalten und Diensten im Internet erforderlich sind.
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 Web-Formular 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 Website-Besuchers 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.
Malspam	Massenhaft versendete E-Mails, mit welchen Schadsoftware verbreitet wird.
Malware / Schadsoftware	Oberbegriff für Software, die schädliche Funktionen auf einem Rechner ausführt (wie beispielsweise Viren, Würmer, Trojanische Pferde).

Begriff	Beschreibung
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
MSP Managed Services Provider	Ein Betreibermodellanbieter oder Betreiberlösungsanbieter ist ein IT-Dienstleister, der eine definierte Reihe von Dienstleistungen für seine Kunden übernimmt und verwaltet.
NAS Network Attached Storage	Netzgebundener Speicher: Direkt an einem Netzwerk angeschlossener Festplattenspeicher oder Dateiserver.
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.
RaaS Ransomware-as-a-Service	Ransomware als einkaufbare Dienstleistung ermöglicht technisch wenig versierten Kriminellen durch einfach zu bedienende Werkzeuge Angriffe durchzuführen.

Begriff	Beschreibung
Ransomware	Schadsoftware, die ihre Opfer typischerweise durch Verschlüsselung von Daten zur Bezahlung von Lösegeld bewegen will.
RDP Remote Desktop Protocol	Ein Netzwerkprotokoll von Microsoft für den Fernzugriff auf Windows-Computer.
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 / Malware	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.

Begriff	Beschreibung
Spoofing	Fälschen von Adressierungselementen oder Signalen zwecks Täuschung der empfangenden Person oder des empfangenden Gerätes.
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.
TCP/IP	Transmission Control Protocol / Internet Protocol ist eine Familie von Netzwerkprotokollen und wird wegen ihrer grossen Bedeutung für das Internet auch als Internetprotokollfamilie bezeichnet.
TLD Top-Level-Domain	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.
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 Websites, 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

Begriff	Beschreibung
	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.).