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 2018/I (Januar – Juni)

8. NOVEMBER 2018

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

1 Übersicht / Inhalt

1 Übersicht / Inhalt 2
2 Editorial 5
3 Schwerpunktthema: Sicherheitslücke in der Hardware 6
3.1 Spectre und Meltdown 6
3.2 Warum dieser Design-Fehler? 6
3.3 Lösungsansatz 7
3.4 Mögliche Entwicklungen 8
4 Lage national 9
4.1 Spionage 9
4.1.1 Der Name des Labors Spiez als Absender für «Olympic Destroyer» missbraucht 9
4.2 Industrielle Kontrollsysteme 11
4.2.1 Offene Systeme am Netz – Bedrohung oder «Courant normal»? 11
4.3 Angriffe (DDoS, Defacements, Drive-By) 14
4.3.1 Aktivitäten von Apophis Squad in der Schweiz 14
4.4 Social Engineering und Phishing 15
4.4.1 Phishing 15
4.4.2 Anrufe im Namen von Banken 15
4.4.3 GDPR-Phishing 16
4.4.4 Betrugsversuche im Kalender 17
4.4.5 Vermeintlicher Gewinn – Kettenbriefe im Namen von IKEA, Milka und Co 18
4.4.6 Vom Internet in die reale Welt - Wenn Angreifer persönlich vorbeischauen 18
4.4.7 «Look alike»-Domain 19
4.4.8 E-Mail Adressen zu verkaufen 20
4.5 Datenabfluss 22
4.5.1 Kundendaten kommen bei Vertriebspartner von Swisscom abhanden 22
4.5.2 Die Verwendung von gestohlenen Daten 23
4.5.3 Passwörter für «Sextortion» 23
4.5.4 «Credential Stuffing» mit alten Passwörten 24
4.6 Crimeware 24
4.7 E-Banking Trojaner in der Schweiz 25
4.7.1 «Retefe» und Social Engineering 26
4.7.2 «Dridex» und Offline Zahlungs-Software 27
4.7.3 «Gozi ISFB» und die Drive-by-Verbreitung 28
5 Lage International 29
5.1 Spionage 29

5.1.1 «Sofacy» in Zusammenhang mit verschiedenen Vorfällen genannt 29
5.1.2 VPN-Filter – Mindestens 500'000 Geräte betroffen 30
5.1.3 Angriff auf Netzwerk der Deutschen Bundesregierung 31
5.1.4 Angriffe gegen Energieversorger 31
5.1.5 «Cisco's» «Smart Install» im Fokus von Angreifern 33
5.2 Industrielle Kontrollsysteme 35
5.2.1 Unerlaubter Zugriff auf das Infotainment-System von VW- und Audi-Fahrzeugen 35
5.2.2 Cryptominer bei europäischer Wasserwerksteuerung 36
5.2.3 «Hide'n Seek - IoT Botnet mit Peer-to-Peer Funktionalität 36
5.3 Angriffe (DDoS, Defacements, Drive-By) 37
5.3.1 «Memcached DDoS»-Angriff 37
5.3.2 Interne Bankensysteme immer noch im Visier der Cyber-Kriminellen 38
5.4 Datenabflüsse 39
5.4.1 DHS Privacy Leak 39
5.4.2 Datenabfluss bei «Exactis» 40
5.5 Präventive Massnahmen 40
5.5.1 Verhaftung von Mitglied im Zusammenhang mit den Carbanak/Cobalt Angriffen 40
5.5.2 Cyber Europe 2018 – Vorbereitung auf die nächste Cyber-Krise 41
5.5.3 Lazarus CC Server-Übernahme 42
6 Tendenzen und Ausblick 42
6.1 Die Verwendung von Daten bei Angriffen 42
6.2 Vernetzte medizinische Geräte, Gesundheitsdaten und Patientendossiers 44
6.3 Tempo vor Sicherheit? – Dem Mobilfunk kann auch in Zukunft nicht alles anvertraut werden. 45
6.3.1 Die bekannten Probleme mit dem SS7 Protokoll bei 2G und 3G 45
6.3.2 LTE macht einiges besser, aber noch lange nicht perfekt 46
6.3.3 Schliesst 5G endlich die Lücken? 46
6.3.4 Netzwerksicherheit alleine schützt nicht 47
7 Politik, Forschung, Policy 48
7.1 CH: Parlamentarische Vorstösse 48
7.2 Poltische Entwicklungen im Cyber-Bereich – Aktueller Stand 51
7.3 GDPR und Datenschutzgesetz 52
8 Publizierte MELANI Produkte 54
8.1 GovCERT.ch Blog 54
8.2 MELANI Newsletter 54
8.2.1 Datenabflüsse, Crimeware und Angriffe auf industrielle Kontrollsysteme - Themen im MELANI-Halbjahresbericht 54

8.2.2 Wieder vermehrt betrügerische Anrufe bei Firmen 54
8.3 Checklisten und Anleitungen..... 54
9 Glossar..... 55

2 Editorial

Dr. Bruce Nikkel
Leiter Cybercrime Intelligence & Forensic Investigation, UBS
Chairman European FI-ISAC
Professor für Digital Forensik, Berner Fachhochschule

Liebe Leserinnen und Leser,

Die Schweiz basiert historisch gesehen auf vertrauenswürdigen Beziehungen zwischen den einzelnen Kantonen, die zusammenarbeiten, um sich gegen gemeinsame Bedrohungen zu verteidigen. Dieses Beispiel von Vertrauen über verschiedene Interessensgruppen hinweg, resultiert aus einer langfristigen Entwicklung zu einer sicheren Gesellschaft. In unserer digitalen Welt spielt das Vertrauen weiterhin eine zentrale Rolle. Das Konzept der Zusammenarbeit von Gleichgesinnten in vertrauenswürdigen Gruppen ist mittlerweile in jedem Industriesektor ein wichtiger Faktor geworden. Diese Gruppen verfolgen das Ziel, gemeinsam Cyber-Bedrohungen und Cybercrime-Aktivitäten zu verhindern und zu bekämpfen.

Solche Gruppen von vertrauenswürdigen Gleichgesinnten können ad-hoc Charakter haben, wo man sich informell trifft und gemeinsam aktuelle technische Bedrohungen und mögliche Lösungen diskutiert. Regierungsstellen und Firmen organisieren aber auch formellere Vertrauensgruppen, wie sogenannte ISACs (Information Sharing and Analysis Centers) oder CERTs (Computer Emergency Response Teams). MELANI etablierte in der Schweiz die Koordination von solch vertrauenswürdigen Gruppen, zwischen verschiedenen Sektoren der kritischen Infrastrukturen wie Energie, Telekommunikation, Finanz und anderen Sektoren. In diesen Gruppen arbeiten konkurrierenden Firmen zusammen, um sich kooperierend für ein insgesamt grösseres Ziel einzusetzen, was letztendlich der Sicherheit der Gesellschaft dient.

Cyber-Bedrohungen wirken über nationale Grenzen hinweg. Deshalb muss die Zusammenarbeit auch auf Personen und Gemeinschaften ausserhalb der Schweiz ausgedehnt werden. So existieren zahlreiche internationale Initiativen, welche auf Vertrauen basieren und gemeinsam Bedrohungen gegen die Gesellschaft aus globaler Sicht analysieren. MELANI nimmt an diesen globalen Initiativen zusammen mit vielen anderen Schweizer Organisationen teil. Typischerweise bestehen solche Gruppen aus Mitgliedern der Industrie, von Regierungs-CERTs (wie MELANI), der Strafverfolgung und anderen Sicherheitsspezialisten.

Die Sicherheit unserer digitalen Gesellschaft basiert auf dieser nationalen und internationalen Zusammenarbeit - formell und informell. Dies muss weiterhin gefördert und ausgebaut werden. Cyberbedrohungen und Cyberkriminalität können nicht von einer einzelnen Organisation gestoppt werden. Die Kooperation zwischen im Wettbewerb stehenden Firmen und Organisationen und zwischen dem öffentlichen und dem privaten Sektor ist enorm wichtig. Vertrauen zwischen Individuen ist der Schlüssel zum Erfolg. Dieses Vertrauen kann nur erreicht werden, indem man die Beziehungen zwischen den Firmen und Organisationen sowohl national als auch international ständig pflegt und weiterentwickelt. Der Beitrag von MELANI zur Entwicklung und Koordination vertrauenswürdiger Gruppen bringt wertvolle Sicherheit in unsere Cyber-Welt.

Dr. Bruce Nikkel

3 Schwerpunktthema: Sicherheitslücke in der Hardware

3.1 Spectre und Meltdown

Der Umgang mit Sicherheitslücken gehört im IKT-Bereich mittlerweile zum Alltag. Wöchentlich werden Sicherheitslücken bekannt. Nicht jede Lücke ist aber gleich kritisch, viele haben nur geringe oder dann sehr spezifische Auswirkungen. Für Schlagzeilen sorgen vor allem diejenigen Schwachstellen, die von aussen und damit von jeder im Internet aktiven Person ausgenutzt werden können («Remote Code Execution»). Hier ist das Schadenspotential auch besonders hoch. Dies traf beispielsweise auf die Sicherheitslücke «Heartbleed» oder auf die Schadsoftware «Wannacry» zu, welche eine Schwachstelle im SMB-Protokoll ausnutzten. Glücklicherweise standen nach Bekanntwerden der Lücke die entsprechenden Software-Updates meist zeitnah zur Verfügung, denn die Software-Firmen haben sich darauf eingestellt und ihre Prozesse bezüglich Behebung von Sicherheitslücken optimiert. Doch was passiert, wenn eine Lücke nicht die Software, sondern die Hardware betrifft? Zwar gab es bereits Hardware-Lücken wie beispielsweise der Pentium-FDIV-Bug[1] im Jahre 1994 oder «Rowhammer» im Jahre 2014[2] bei der es möglich war in bestimmten Typen von RAM Speicherbausteinen einen Fehler zu erzeugen, wenn derselbe Bereich immer und immer wieder gelesen wird. Dies führte zu Interaktionen mit benachbarten Speicherbereichen. Die Hardware-Lücken «Spectre» und «Meltdown», die in der ersten Januarwoche 2018 bekannt wurden[3], waren im Ausmass allerdings erheblich gravierender. Ein Fehler im Design von Prozessoren ermöglicht es einem Angreifer, Daten auszulesen, die sich auf dem Prozessor befinden. Solche Fehler lassen sich nicht mit einem einfachen Software-Update aus der Welt schaffen.

3.2 Warum dieser Design-Fehler?

Um Anwendungen schneller zu machen, haben sich die Prozessorhersteller folgendes einfallen lassen: Prozessoren treffen Annahmen, welche Rechenoperation als nächstes benötigt werden, führen diese aus und speichern die Resultate («speculative execution» und «out of order execution»). Trifft die Annahme nicht zu, werden die Resultate verworfen, trifft die Annahme zu, steht das Resultat schneller bereit. Computer legen häufig benötigte Instruktionen und Daten im sogenannten Cache ab. Dieser Speicher ist direkt auf dem Prozessor implementiert, so dass darauf sehr schnell zugegriffen werden kann. Ein Angreifer kann nun aus der benötigten Rechenzeit eines Datenzugriffs auf die Speicheradresse der Daten schliessen. Ein Wert, der sich bereits im Cache befindet und vorausberechnet wurde, wird schneller ausgelesen, als wenn dieser neu berechnet werden muss.

Um auf geschützte Informationen zuzugreifen, nutzt ein Angreifer aus, dass auch Resultate in den Speicher geschrieben werden, für die er gar keine Rechte hat. Erst wenn das dazugehörige Resultat dann wirklich gebraucht wird, wird eine Überprüfung der Rechte durchgeführt. Fehlen diese Rechte, wird die Operation mit einer Fehlermeldung abgebrochen. Ungeachtet dessen verbleiben die Informationen aber für einen kurzen Augenblick im Speicher

---

1 https://de.wikipedia.org/wiki/Pentium-FDIV-Bug (Stand: 31. Juli 2018).

2 https://de.wikipedia.org/wiki/Rowhammer (Stand: 31. Juli 2018).

3 https://meltdownattack.com (Stand: 31. Juli 2018).

(Cache) und können ausgelesen werden, sofern der entsprechende Speicherbereich noch nicht überschrieben worden ist.

Das Verfahren wird seit 20 Jahren angewendet. Es führt zu schnelleren Rechnerleistung und somit zu einer Zeitersparnis. Vor zwanzig Jahren waren Computer meist abgeschlossene Systeme. Im Zeitalter von Cloud-Computing und virtuellen Systemen fällt die Entdeckung dieser Schwachstellen in eine Periode, bei denen mehrere Benutzer auf einen Prozessor zugreifen und ist deshalb besonders gravierend. Deshalb standen beim Finden von Lösungen vor allem Cloud-Anbieter im Zentrum des Interesses, denn dort teilen sich typischerweise mehrere virtuelle Systeme die gleiche Hardware.

Betroffen sind aber die meisten Computer, Server, Smartphones und Tablets. Praktisch alle Benutzer solcher Geräte dürften in irgendeiner Weise von dieser Lücke betroffen sein. Infizierte Systeme werden für die Angreifer auf Prozessorebene verfügbar und erlauben somit einen breiteren Zugriff auf die im System vorhandenen Informationen.

3.3 Lösungsansatz

Weist ein Gerät sicherheitsrelevante Mängel auf, wird es in der Regel vom Hersteller zurückgerufen. In der Automobilindustrie werden regelmässig Fahrzeuge zurückgerufen und fehlerhafte Teile ausgewechselt. In der Computerwelt ist ein solcher Ansatz kaum durchführbar, weil ein Austausch der betroffenen Hardware-Komponente, in diesem Fall der Prozessor, eine Herausforderung ist. Ein Austausch wurde zwar beim Pentium-FDIV-Fehler im Jahre 1994 unter dem Druck der Anwender erzwungen. Heutzutage wäre die Anzahl betroffener Geräte und der damit zusammenhängende logistische Aufwand um einiges grösser. Ausserdem bestünde die Gefahr von fehlerhaften Implementationen, da die Systeme nicht wie in der Autoindustrie genormt, sondern sehr unterschiedlich konfiguriert sind. Die Prozessorhersteller haben sich deshalb dazu entschieden, den Fehler mit Hilfe von Software- und Mikrocode-Updates (Code zum Steuern der Abläufe in einem Prozessor) zu beheben. Einen Hardware-Fehler mit einem Software-Update zu beheben, klingt zunächst paradox. Die Updates reduzieren beispielsweise die Genauigkeit der Zeitauflösung oder deaktivieren teilweise jene Bereiche, in denen die Prozessoren die Vorausberechnungen und die daraus resultierende Beschleunigung durchführen. Man erkauft sich die Behebung des Fehlers aus der Ferne so mit einem Leistungsabfall des Prozessors. Dieser Leistungsabfall muss wiederum durch mehr Rechenleistung kompensiert werden. Für eine langfristige Lösung wird deshalb ein anderer Ansatz gefunden werden müssen.

Die Mikroprozessoren müssen somit zukünftig neugestaltet und die Prozessorarchitektur überarbeitet werden. Dies dürfte wohl Jahre dauern. Bei den heutigen Systemen bildet der Prozessor das Zentrum und ist das am stärksten optimierte Element. Speicher und Kommunikation dienen dem Prozessor zu.[4] In einer neuen Architektur müssten Speicher und damit auch die Sicherheit mehr und besser in das System integriert werden (Security by Design). Es stellt sich die Frage mit welchen Methoden man generell eine erhöhte Sicherheit bei der Entwicklung von Hardware Elementen sicherstellt.

[4] https://www.netzwoche.ch/storys/2018-03-07/wie-meltdown-und-spectre-zukuenftige-computerarchitekturen-beeinflussen (Stand: 31. Juli 2018).

3.4 Mögliche Entwicklungen

«Spectre» und «Meltdown» haben eine Diskussion über Hardware-Lücken ausgelöst. Sicherheitsforscher weltweit arbeiten nun vermehrt an dieser Thematik, um weitere Lücken zu finden. So wurde «Spectre NG» (NG steht für «Next Generation») im Mai publik und beinhaltete insgesamt acht weitere Schwachstellen[5], die auf der Methodik von «Spectre» und «Meltdown» aufbauen, darunter «Foreshadow» alias «L1 Terminal Fault» mit welcher ein Angreifer aus einer virtuellen Maschine heraus den vermeintlich geschützten Speicher einer anderen virtuellen Maschine, die auf demselben Computer läuft, lesen kann. Im Juli 2018 wurden drei weitere CPU-Lücken ret2spec, SpectreRSB und NetSpectre bekannt gegeben.

Es ist davon auszugehen, dass weitere Hardware-Lücken entdeckt werden, weil die meisten Computersysteme immer noch auf Entwicklungen basieren, die 20 Jahre und älter sind. Aufgrund von Kompatibilitätsgründen wurde es verpasst, Systeme und Architekturen von Grund auf zu erneuern. Stattdessen versuchte man, Bestehendes weiterzuentwickeln, obwohl System und Architektur zum Teil nicht für diese neuen Funktionen entwickelt wurden. Gerade im dynamischen Umfeld der IKT ist dies bemerkenswert und wird künftig bei Lücken eine grössere Rolle spielen. Im Gegensatz zu Software ist ein weltweiter Austausch von Hardware unrealistisch. Entscheidend wird sein, wie sich das Risiko solcher Lücken minimieren lässt und inwiefern man damit zusammenhängende Leistungseinbussen verkraftet.

Empfehlungen:

Empfehlungen bezüglich Hardwarelücken finden Sie auf der MELANI-Website

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

[5] https://www.heise.de/ct/artikel/Super-GAU-fuer-Intel-Weitere-Spectre-Luecken-im-Anflug-4039134.html (Stand: 31. Juli 2018).

4 Lage national

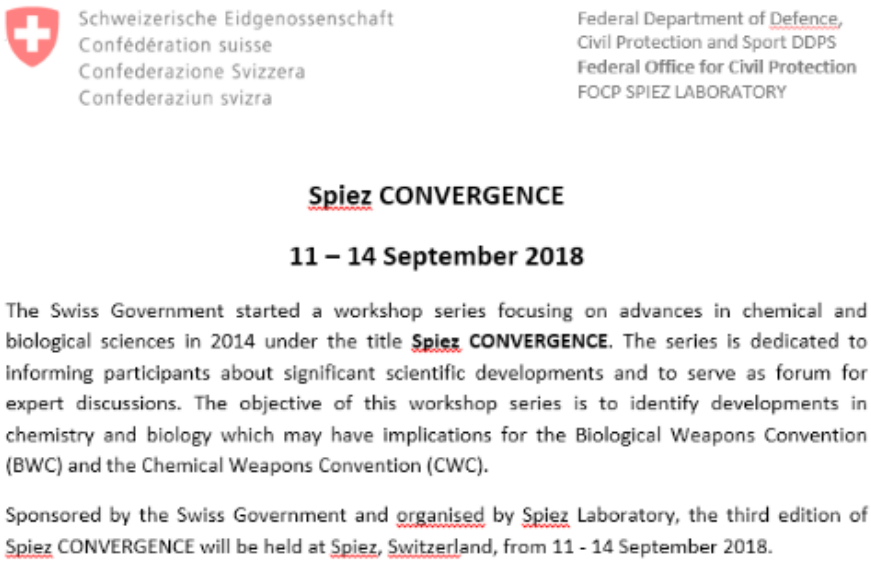
4.1 Spionage

4.1.1 Der Name des Labors Spiez als Absender für «Olympic Destroyer» missbraucht

Am 19. Juni 2018 publizierte der Sicherheitsdienstleister «Kaspersky» einen Bericht über den Einsatz der Malware «Olympic Destroyer». Die Schadsoftware trat erstmals an den Olympischen Winterspielen 2018 in Pyeongchang in Südkorea in Erscheinung. Damals hatte der Wurm mit Sabotagefunktionalitäten während der Eröffnungsfeier einen Angriff auf die Infrastruktur des Veranstalters verübt. Verschiedene Sicherheitsexperten gingen von einer sogenannten «False Flag»-Operation aus und verdächtigte den Angreifer, er versuche den Verdacht auf einen Dritten (in diesem Falle Nordkorea) zu lenken. So stellte sich denn auch diese auf den ersten Blick naheliegende Zuordnung beziehungsweise Attribution im Nachhinein als falsch heraus und zeigte einmal mehr, dass Attribution im Cyber-Bereich nicht einfach ist. Mittlerweile wird «Olympic Destroyer» vom Sicherheitsdienstleister «Kaspersky» mit der Hackergruppe «Sofacy» in Verbindung gebracht (siehe Kapitel 5.1.1).

Im Mai und Juni 2018 wurden gezielte Phishing-E-Mails, so genanntes «Spear Phishing» entdeckt. Die in der E-Mail angefügten Dokumente wurden mit Teilen der obgenannten «Olympic Destroyer»-Schadsoftware vom Februar 2018 in Verbindung gebracht. Ziele dieser Angriffe waren laut «Kaspersky» Finanzorganisationen in Russland sowie Biologie- und Chemie-Laboratorien im Bereich Gefahrenabwehr. Öffnet ein Empfänger die E-Mail, versucht die Schadsoftware den Computer zu infizieren und in eine «Botnetzl»-Infrastruktur einzubinden. Die Infektion ist komplex und basiert auf verschiedenen Technologien wie VBA, Powershell und MS HTA mit JavaScript. Technische Details hat «Kaspersky» in einem Blogeintrag publiziert.[6] Sabotageaktionen wurden bei diesem Angriff nicht beobachtet. Um einen gezielten Angriff durchzuführen und die Empfänger zu verleiten auf den Anhang zu klicken, nahmen die Angreifer in einem Fall eine öffentlich verfügbare Einladung des Labors Spiez für eine internationale Konferenz als Vorlage für ihr Mail. Die E-Mail wurde anschliessend mit gefälschtem Absender im Namen des Bundesamtes für Bevölkerungsschutz (BABS) und des Labors Spiez an diverse Empfänger gesendet. Server der Bundesverwaltung waren zu keinem Zeitpunkt involviert. Entgegen diverser Medienberichte wurde das Labor Spiez nicht angegriffen. Der Name des Labors wurde lediglich für den Angriff missbraucht, um diesem mehr Seriosität zu verleihen.

[6] https://securelist.com/olympic-destroyer-is-still-alive/86169/ (Stand: 31. Juli 2018).



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defence,
Civil Protection and Sport DDPS
Federal Office for Civil Protection
FOCP SPIEZ LABORATORY

Spiez CONVERGENCE

11 – 14 September 2018

The Swiss Government started a workshop series focusing on advances in chemical and biological sciences in 2014 under the title **Spiez CONVERGENCE**. The series is dedicated to informing participants about significant scientific developments and to serve as forum for expert discussions. The objective of this workshop series is to identify developments in chemistry and biology which may have implications for the Biological Weapons Convention (BWC) and the Chemical Weapons Convention (CWC).

Sponsored by the Swiss Government and organised by Spiez Laboratory, the third edition of Spiez CONVERGENCE will be held at Spiez, Switzerland, from 11 - 14 September 2018.

Abbildung 1: E-Mail, welche im Namen des Bundesamtes für Bevölkerungsschutz (BABS) an Empfänger versendet wurde (Quelle: Kaspersky)

Am 12. und 14. März 2018 wurden in einer ähnlichen Vorgehensweise Spear-Phishing-E-Mails mit einer angeblichen Einladung zu einer internationalen Konferenz an europäische Regierungsorganisationen versendet. Die E-Mail enthielt ein Word-Dokument mit dem Namen «Defence & Security 2018 Conference Agenda.docx». Auch hier kopierten Angreifer die Agenda direkt von der Webseite und sendeten diese an potenzielle Konferenzteilnehmer. In diesem Fall enthielt das Dokument ein Flash-Objekt mit einem Aktionskript, das versuchte, die eigentliche Schadsoftware (sog. «Payload») herunterzuladen. Speziell bei diesem Angriff war, dass die bösartige Komponente erst aktiviert wurde, nachdem das Opfer auf die dritte Seite des Dokumentes blätterte.[7] Diese Methode dürfte wohl gewählt worden sein, um die Detektion des Angriffs zu erschweren. Hinter diesem Angriff vermuteten Sicherheit-Spezialisten der Firma PaloAltoNetworks die «Sofacy»-Gruppe.[8]

Beurteilung

Einladungen zu Konferenzen sind bei Angreifern beliebt, um gezielte Attacken durchzuführen. Einerseits sind solche Daten typischerweise öffentlich und für den Angreifer somit frei verfügbar. Damit kann ein Angriff sehr gezielt durchgeführt werden, da nur diejenigen Personen sich für die Einladung interessieren werden, welche auch in dem Bereich arbeiten. Andererseits müssen die Angreifer keine grossen Recherchearbeiten durchführen. Die Geschichte ist authentisch und enthält in der Regel weder inhaltliche noch sprachliche Fehler.

7 https://www.zdnet.com/article/hackers-are-using-a-flash-flaw-in-fake-document-in-this-new-spying-campaign/ (Stand: 31. Juli 2018).

8 https://researchcenter.paloaltonetworks.com/2018/03/unit42-sofacy-uses-dealerschoice-target-european-government-agency/ (Stand: 31. Juli 2018).

4.2 Industrielle Kontrollsysteme

4.2.1 Offene Systeme am Netz – Bedrohung oder «Courant normal»?

Die zunehmende Vernetzung und Durchdringung praktisch aller Lebensbereiche mit Informatik eröffnet ökonomische wie gesellschaftliche Potenziale, auf die ein hochentwickeltes und industrialisiertes Land wie die Schweiz nicht verzichten kann. Gleichzeitig aber entstehen durch die zunehmende Digitalisierung neue Risiken.

Bisher isoliert betriebene industrielle Kontrollsysteme werden zunehmend mit dem Internet verbunden. Dadurch lassen sich die Vorteile nutzen, die eine solche Vernetzung mit sich bringt. Nicht alle diese Geräte wurden jedoch für die Vernetzung entwickelt und verfügen zu einem grossen Teil noch über ältere und nicht mehr unterstütze Betriebssysteme. Deshalb sind diverse Sicherheitsmassnahmen zu treffen, um den sicheren Betrieb zu gewährleisten.

Einige Systeme stützen sich auf zentrale und wichtige Funktionen ab, die allerdings historisch bedingte Schwachstellen aufweisen oder gar nicht für die Verwendung von kritischen Systemen konzipiert worden sind. Die Erkennung und Behebung allfälliger Lücken wird daher immer wichtiger. Kollaborative Ansätze helfen dabei, Fehlfunktionen anhand von Heuristiken zu entdecken. Eine solche Lösung wurde im Februar 2018 vom Bundesamt für Rüstung (armasuisse) vorgestellt: Viele Dienste basieren mittlerweile auf GPS-Signalen. So orientieren sich Drohnen, Helikopter und auch Flugzeuge mit Hilfe von GPS-Signalen. Stör- oder Täuschungssignale können Drohnen von ihrem Kurs abbringen. Um das zu verhindern, überwacht ein neuartiges System namens «Crowd-GPS-Sec»[9] kontinuierlich den Luftraum anhand digitaler Flugverkehrs-Signale von Flugzeugen und Drohnen. Mit neuartigen Algorithmen können die Forscher innerhalb von wenigen Sekunden falsche GPS-Signale detektieren. Nach einigen Minuten kann der Standort des Angreifers auf wenige Meter genau geortet werden.

Auch Alltagsgegenstände werden immer häufiger ans interne Netzwerk oder ans Internet angeschlossen. Beispielsweise verfügen Web-Cams, «intelligente Lichtschalter», Kühlschranke oder Smart-TVs immer häufiger über eine Netzwerkschnittstelle. Dadurch steigt nicht nur die Anzahl der Kommunikationsteilnehmer im Internet, sondern auch die Anzahl verwundbarer Geräte, welche von Hackern missbraucht werden können. Problematisch sind insbesondere Geräte, die offen und ungeschützt mit dem Internet verbunden sind oder deren Sicherheitslücken direkt via Internet ausnutzbar sind. Die Suchmaschine «Shodan», erfasst solche Systeme und ermöglicht es, sogenannte «Exposure Maps» für einzelne Länder zu erstellen. Gemäss «Shodan» sind in der Schweiz 478 industrielle Kontrollsysteme von aussen sichtbar und die häufigste von aussen ausnutzbare Sicherheitslücke ist immer noch «Heartbleed».[10] Ersichtlich ist ebenfalls, dass 405 «Cisco Smart Install Clients» (Tool zum Installieren neuer Switches unter Cisco) öffentlich zugänglich sein sollen (vgl. dazu auch Kapitel 5.1.5).

---

9 https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-69896.html (Stand: 31. Juli 2018).

10 Stichtag war der 31. August 2018

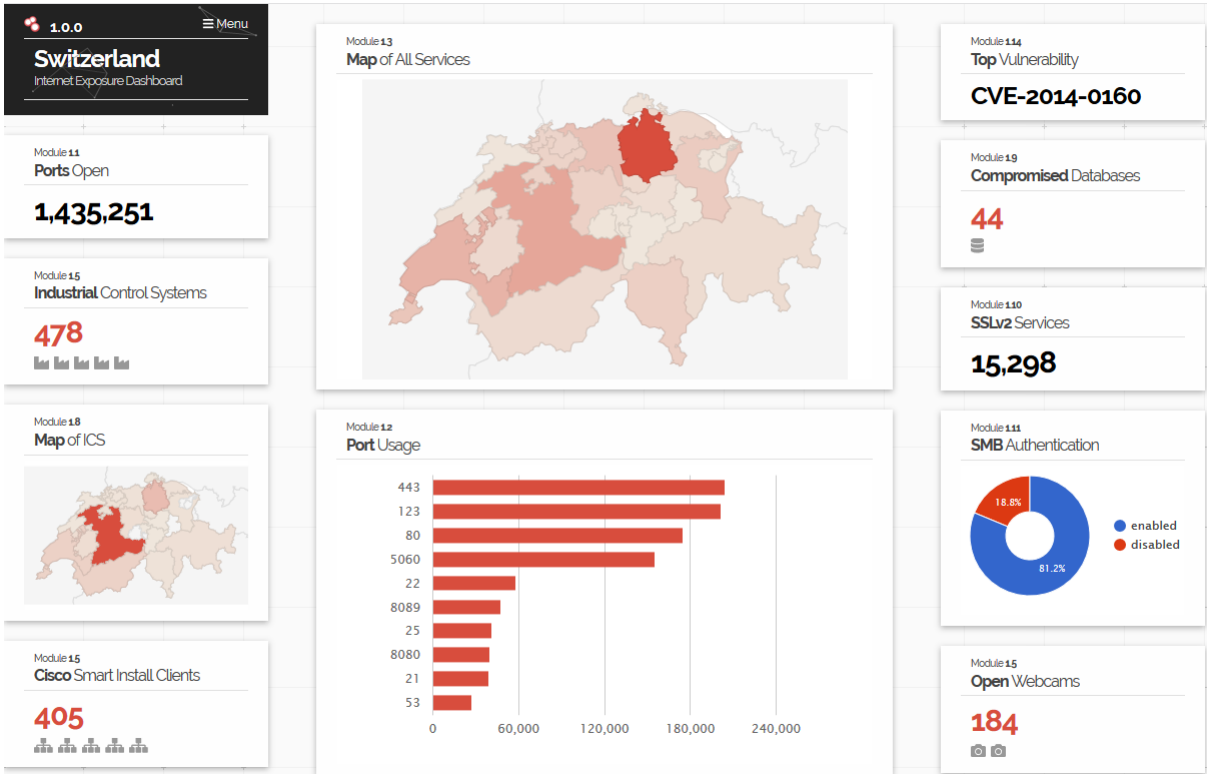


Abbildung 2: Übersicht über verwundbare und über das Internet zugängliche Systeme in der Schweiz (Quelle: https://www.shodan.io/. Stichtag war der 31. August 2018)

Für Angreifer werden stets bessere Werkzeuge verfügbar, um solche Lücken ohne grosse Fachkenntnisse auszunutzen. Ein neues Werkzeug mit dem Namen «Autosploit» machte diesbezüglich Anfang Jahr Schlagzeilen. Dieses Tool verbindet die Suchmaschine «Shodan» mit dem «Metasploit»-Framework. Das «Metasploit»-Framework ist ein Werkzeug zur Entwicklung und Ausführung von Exploits gegen einen Zielrechner. Mit der Kombination dieser beiden Dienste lassen sich Sicherheitslücken automatisch und ohne spezifisches Wissen ausnutzen. Das Programm beginnt mit einer «Shodan»-Suche nach einem speziellen Dienst wie beispielsweise einem «Apache»-Server oder dem «Internet Information Service» von Microsoft. Ein weiterer Befehl startet anschliessend die Angriffe. Dabei soll das Skript automatisch die richtigen Exploits aus der «Metasploit»-Bibliothek heraussuchen.

Bislang mussten Angreifer neben der kriminellen Energie auch das entsprechende Wissen besitzen. Mit solchen Werkzeugen entfällt letztere Anforderung und der Kreis der Täterschaft vergrössert sich erheblich.

Nicht immer ist einfach abzuschätzen, wie kritisch offene Systeme einzustufen sind, sowie ob und wie allenfalls sensible Systeme betroffen sind[11]. Vor zwei Jahren publizierten Hacker am «Chaos Communication Congress (CCC)» zahlreiche Screenshots von Systemen, in die sie angeblich eingedrungen waren. Darunter befand sich auch die Wasserversorgung einer kleinen Schweizer Gemeinde. Eine genauere Analyse und Nachfrage bei der Gemeinde ergab allerdings, dass der Zugang zwar nicht publiziert war, interessierte Bürger sich aber durchaus diese Daten ansehen dürfen. Auf den Grafiken sah man, wieviel Wasser aus den einzelnen

11 https://www.suedostschweiz.ch/zeitung/wasserwerk-wurde-gehackt (Stand: 31. Juli 2018).

Quellen in das Reservoir fliesst. Kritische Daten waren jedoch keine ersichtlich und auch Manipulationen waren über den Fernzugang nicht möglich.

Beurteilung / Empfehlung:

Mit dem Internet vernetzte Gegenstände und Geräte können grundsätzlich von jedem gefunden werden (beispielsweise mit einem Portscan oder einer Suchmaschine wie «Shodan») und bieten daher eine besonders grosse Angriffsfläche. Ans Internet angeschlossenen Geräte müssen sowohl abgesichert (individuelle Passwörter, eingeschränkter Zugang) als auch regelmässig aktualisiert werden. Eine Aktualisierung sollte immer rasch erfolgen, sobald entsprechende Updates verfügbar sind. Anders als beim Desktop-Computer oder Smartphone denkt beim intelligenten Lichtschalter oder Kühlschrank jedoch kaum jemand daran, dass auch bei diesen Geräten allenfalls Software-Updates durchgeführt werden müssen.

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

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

DOKU

Minimalstandard zur Stärkung der IKT-Resilienz

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

Empfehlung:

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

MELDEN

Meldeformular MELANI

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

DOKU

Checkliste mit Massnahmen zum Schutz industrieller Kontrollsysteme

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

4.3 Angriffe (DDoS, Defacements, Drive-By)

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

4.3.1 Aktivitäten von Apophis Squad in der Schweiz

Die Gruppe «Apophis Squad» erlangte anfänglich dadurch Berühmtheit, dass sie sich im März und April 2018 zu falschen Bombenalarmen an US-amerikanischen und englischen Schulen bekannte.

Im Juni 2018 machte die Gruppe mit einer anderen Art von Aktivität auf sich aufmerksam. Die Gruppe bekannte sich auf ihrem Twitter-Account zu zahlreichen DDoS-Attacken und bewarb damit ihren Booter/Stresser-Dienst. Die meisten dieser Attacken waren nur von kurzer Dauer, eine Ausnahme war allerdings diejenige gegen «Protonmail», einem Schweizer Secure E-Mail-Provider, welche sich über mehrere Tage erstreckte und die Verfügbarkeit des Dienstes über eine längere Dauer störte. Die mögliche Ursache dieser Hartnäckigkeit dürfte in der Reaktion eines Protonmail-Managers zu suchen sein, der die Angreifer auf seinem Twitter-Account als «Clowns» bezeichnet und diese damit wohl provoziert hatte. Diese verschiedenen Aktivitäten sind nicht ohne rechtliche Folgen geblieben und führten Ende August 2018 zu einer Verhaftung.

Diese Aktivitäten und das Echo in den Medien veranlasste offenbar andere Akteure, diese Gelegenheit zu ergreifen und quasi als Trittbrettfahrer unter dem Namen Apophis Squad eigene Erpressungsversuche zu unternehmen, ohne entsprechende DDoS-Fähigkeiten zu haben Im August wurden auf diese Art zahlreiche im Finanzsektor tätige Unternehmen erpresst. In der betreffenden Mail wurde explizit auf den Angriff gegen Protonmail angespielt und mit einer äusserst heftigen DDoS-Attacke gedroht, sollte der Empfänger vor Ablauf der gesetzten Frist nicht die merkwürdige Summe von 2.01 Bitcoin bezahlen. Danach wurde mit zahlreichen Mahnungen nachgedoppelt. Aufgrund der verschiedenster Indizien kam MELANI sehr schnell zum Schluss, dass es sich höchstwahrscheinlich um einen Akteur handelt, der bloss die Bekanntheit von Apophis Squad ausnützen wollte, ohne wirklich eine Attacke ausüben zu wollen respektive ohne Kapazität diese auch durchführen zu können. Erstens verwendete der Akteur häufig die gleichen Bitcoin-Adressen, was die Identifizierung des Ursprungs einer allfälligen Zahlung verunmöglicht. Ausserdem wurde auf dem von Apophis Squad verwendeten Twitter-Account berichtet, dass derzeit «Copycats» am Werk seien und dass ihre Vorgehensweise nicht der des ursprünglichen Akteurs entspreche.

Am vorgesehenen Datum, an dem die Attacke stattfinden sollte, wurde keine Aktivität gemeldet, was die Einschätzung von MELANI bestätigte. Unternehmen sollten sich jedoch trotzdem sehr gut auf mögliche DDoS-Attacken vorbereiten, denn es gibt viele andere Gruppen, die in der Lage sind, solche auszuführen.

Empfehlung:

Auf der Internetseite von MELANI ist eine Liste von Massnahmen gegen DDoS-Attacken publiziert

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

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.

4.4.1 Phishing

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

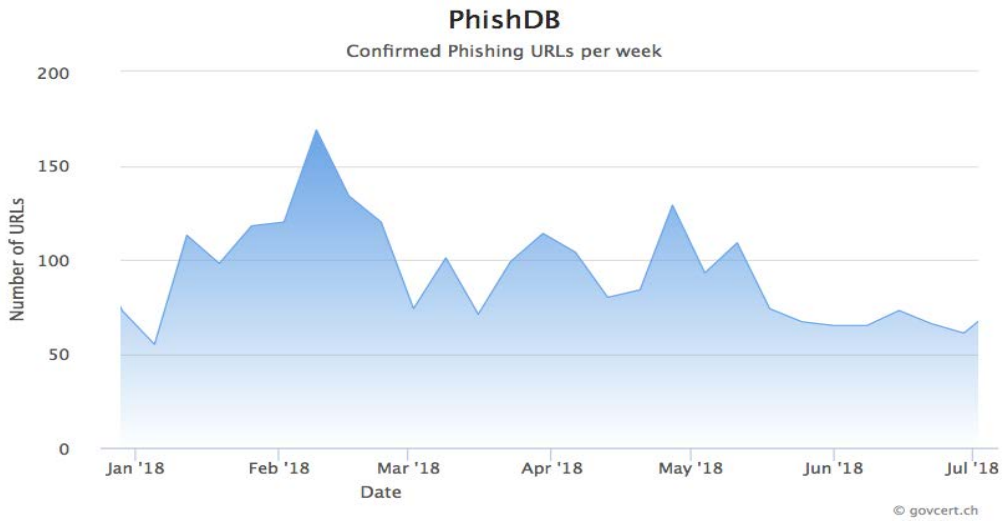


Abbildung 3: Gemeldete und bestätigte Phishing-Seiten pro Woche auf antiphishing.ch im ersten Halbjahr 2018

Insgesamt wurden im ersten Halbjahr 2018 2'501 verschiedene eindeutige Phishing-Seiten über das von MELANI betriebene Portal «antiphishing.ch» gemeldet. Auf Abbildung 3 sind die gemeldeten Phishing-Webseiten pro Woche dargestellt, wobei die Anzahl über das Jahr gesehen variiert. Die Gründe hierzu sind sehr verschieden: Zum einen gibt es ferienbedingte Schwankungen, da in der Ferienzeit weniger Phishing-Seiten gemeldet werden und zum anderen verschieben die Kriminellen ihre Angriffe regelmässig von Land zu Land.

4.4.2 Anrufe im Namen von Banken

Wieder wurden vermehrt betrügerische Anrufe bei Firmen festgestellt, bei welchen sich Angreifer als Bankmitarbeiter ausgaben. Die Anrufer bitten um die Ausführung von Zahlungen oder geben vor, ein Update beim E-Banking durchführen zu müssen, das anschliessend getestet werden soll.

Die Angreifer versuchen typischerweise die Mitarbeitenden der Firma zu überzeugen, eine Software für den Fernzugriff (zum Beispiel NTR-Cloud, Teamviewer) zu installieren, verbinden sich dann mit dem Computer des Opfers und täuschen vor, ein E-Banking-Update durchzuführen. Anschliessend geben die Täter vor, dass das Update getestet werden müsse und versuchen das Opfer zu überzeugen, seine Zugangsdaten für das E-Banking der Firma einzugeben. Die Angreifer geben vor, anhand einer Testzahlung die Funktionsweise des Systems überprüfen zu wollen. Ist die Zahlung durch eine Kollektivunterschrift geschützt, versuchen die Betrüger das Opfer zu überzeugen, alle Unterschriftsberechtigten zu organisieren, um die Zahlung freizugeben.

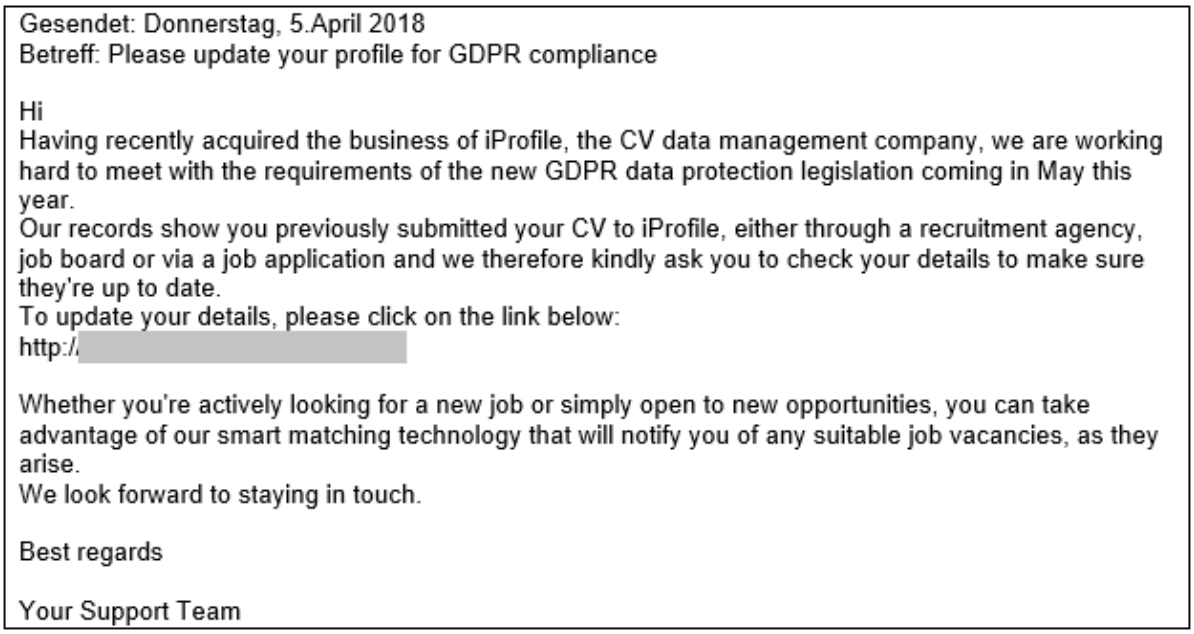
In einer anderen Variante werden die Opfer angewiesen, aufgrund von dringenden E-Banking Updates für einige Tage auf das E-Banking zu verzichten. Im Falle von dringenden Transaktionen soll das Opfer eine durch die Betrüger angegebene Rufnummer kontaktieren. Ruft das Opfer den vermeintlichen Bankmitarbeiter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

Beurteilung:

Die Beispiele zeigen, wie aktuell «Social Engineering»-Methoden weiterhin sind. Die Sensibilisierung innerhalb der Firmen, die Einhaltung der IKT-Prozesse, sowie die Überprüfung der online preisgegebenen Informationen über Mitarbeitende, Geschäftsleitung und Verwaltungsrat ist der Schlüssel, solchen Betrugsversuchen wirksam vorzubeugen.

4.4.3 GDPR-Phishing

Am 25. Mai 2018 lief die zweijährige Übergangsfrist aus, und die Datenschutz-Grundverordnung der Europäischen Union (EU DSGVO / EU GDPR) ist in Kraft getreten (siehe Kapitel 7.3). Wie erwartet, wurde das Ende der Übergangsfrist zur Einführung der GDPR zu Phishing-Zwecken für Missbräuche ausgenutzt: Im Zeitraum vor dem 25. Mai 2018 wurden sehr viele E-Mails mit Informationen bzgl. den bevorstehenden Massnahmen im Rahmen der Umsetzung der GDPR von Unternehmen an ihre Kunden verschickt. Solche Zeitfenster machten sich findige Betrüger zu nutzen und setzen darauf, dass die Empfänger über die Einführung der GDPR informiert sind und sich auch verpflichtet fühlen, ihre Profile entsprechend zu bearbeiten (siehe Beispiel Abbildung 4).


Gesendet: Donnerstag, 5.April 2018
Betreff: Please update your profile for GDPR compliance

Hi
Having recently acquired the business of iProfile, the CV data management company, we are working hard to meet with the requirements of the new GDPR data protection legislation coming in May this year.
Our records show you previously submitted your CV to iProfile, either through a recruitment agency, job board or via a job application and we therefore kindly ask you to check your details to make sure they're up to date.
To update your details, please click on the link below:
http:/

Whether you're actively looking for a new job or simply open to new opportunities, you can take advantage of our smart matching technology that will notify you of any suitable job vacancies, as they arise.
We look forward to staying in touch.

Best regards

Your Support Team

Abbildung 4: Beispiel eines betrügerischen E-Mails, welches GDPR als Vorwand nimmt, um an Daten eines Opfers zu kommen.

Die konforme Umsetzung der Verordnung und die Statuierung hoher Geldbussen bei Verletzung des Datenschutzes wird nicht nur die Unternehmen weiterhin beschäftigen, sondern auch Kriminelle zu neuen erpresserischen Vorgehensweisen inspirieren. Ähnlich wie im Bereich «Social Engineering» werden öffentlich bekannte Informationen systematisch genutzt, um neue Opportunitäten zu schaffen.

4.4.4 Betrugsversuche im Kalender

Am Anfang jeder betrügerischen Vorgehensweise steht der Versuch der Angreifer, mit dem potenziellen Opfer unter einem beliebigen Vorwand in Kontakt zu treten. Am häufigsten ist der Versand einer E-Mail. Aber auch der Versand von SMS, Whatsapp-Nachrichten oder Meldungen in den sozialen Netzwerken wird immer beliebter. Doch es gibt noch eine weitere Taktik, die in der Berichtsperiode beobachtet wurde. Sie besteht darin, im elektronischen Kalender des Opfers manipulierte Einladungen zu platzieren. Je nach Einstellung wird eine solche Einladung auch angezeigt, wenn das Ereignis vom Empfänger nicht akzeptiert worden ist. Anschliessend werden automatisch Erinnerungen generiert. In einem aktuellen Fall sah das Opfer die Anzeige der Einladung in seinem Google-Kalender. Es handelte sich um ein Darlehensangebot und das Opfer wurde gebeten, per E-Mail oder Whatsapp-Nachricht über die in der Nachricht angegebenen Koordinaten Kontakt aufzunehmen. Der eigentliche Zweck der Attacke konnte nicht eruiert werden, doch man kann davon ausgehen, dass es sich um einen Phishing- oder Betrugsversuch handelte. Auf jeden Fall zeigt dieses Beispiel, dass Computernutzerinnen und -nutzer gut beraten sind, in allen Situationen Vorsicht walten zu lassen. Sogar Ereignisse im Kalender können Malware enthalten. Es ist nicht ausgeschlossen, dass einige sich täuschen lassen, da ihnen eine Anmeldung oder Benachrichtigung von ihrem persönlichen Kalender als unauffällig erscheint und sie deshalb zu einer unvorsichtigen Handlung verleitet werden. Es ist empfehlenswert, das E-Mail-Konto so einzustellen, dass nur akzeptierte Ereignisse im Kalender erscheinen.

4.4.5 Vermeintlicher Gewinn – Kettenbriefe im Namen von IKEA, Milka und Co

Ein Jahr lang Schokolade, ein Gutschein von «IKEA» oder ein neues iPhone. In regelmässigen Abständen sind Whatsapp-Nachrichten, SMS und E-Mails im Umlauf, die solche Gewinne versprechen. Am Ende gibt es allerdings nicht Schokolade, sondern nur Frust. Hinter solchen E-Mails stecken Datensammler. Die Fragen sind bei all diesen Gewinnspielen so gewählt, dass sie jedermann leicht beantworten kann. Die Autoren wollen nämlich, dass möglichst viele Mitspieler «gewinnen», und sie damit an möglichst viele Daten kommen. Um an den Gewinn zu kommen, muss man auf einer gefälschten Website persönliche Daten wie den Namen, das Alter, die E-Mail-Adresse oder Handy-Nummer und manchmal auch die Wohnadresse angeben. Bei dieser Vorgehensweise kommen auch internationale Domänen zum Einsatz (siehe Kapitel 4.4.7) So wurde bei einer Variante eines «Milka»-Gewinnspiels bei der Domäne von «Milka» ein «i» ohne Punkt, wie man es im Türkischen findet, verwendet. Nutzern fällt das auf den ersten Blick nicht auf und sie denken, dass sie sich auf der offiziellen Seite von «Milka» befinden.

Eine weitere Masche bei diesen Gewinnspielen ist die Forderung, dass man nur an den Gewinn kommt, wenn die Nachricht an 20 Kontakte weitergeleitet wird. Die Form des Kettenbriefes ermöglicht dabei dem Initiator, dass er sich nicht einmal um den Versand kümmern muss. Dieser wird vom Opfer gleich selbst erledigt. Dass die Nachricht von einer Person kommt, die der Empfänger kennt, ist ein weiterer Vorteil dieser Vorgehensweise. So steigt die Chance, dass ein Opfer dem Gewinnspiel vertraut und mitmacht.

Empfehlung:

Nachrichten mit verlockenden Gewinnversprechen müssen deshalb kritisch hinterfragt und dürfen schon gar nicht weitergeleitet werden. Am besten ignoriert man diese grundsätzlich.

4.4.6 Vom Internet in die reale Welt - Wenn Angreifer persönlich vorbeischauen

Straftaten im Internet bieten den Vorteil, dass sie aus der Ferne durchgeführt werden können. Die Täterschaft sitzt meistens im Ausland, fernab von den Zugriffsmöglichkeiten der lokalen Strafverfolgungsbehörden. Da die Betrüger die Straftaten aus ihrer gewohnten Umgebung heraus durchführen können, sinkt auch deren Hemmschwelle. So wird für einen Banküberfall bedeutend mehr kriminelle Energie benötigt, als für einen Versand von Phishing-E-Mails. In der Berichtsperiode gab es allerdings einige Vorfälle, die eine physische Präsenz vor Ort voraussetzten. Im Juni 2018 gab es Warnungen über Telefonbetrüger, die sich als Google Mitarbeiter ausgaben.[12] Anscheinend wurde in einigen Fällen auch versucht ein Kontakt vor Ort herzustellen. In einem Fall wurde Firmen beispielsweise mitgeteilt, «Google» wünsche einen persönlichen Termin, um von ihnen erhobene Daten zu verifizieren. Auch wenn diese Vorgehensweise auf den ersten Blick durchaus Sinn machen würde, scheint ein persönlicher Besuch von «Google»-Mitarbeitenden aber dann doch etwas übertrieben zu sein. Die tatsächliche Absicht der Betrüger liess sich nicht abschliessend klären.

---

12 https://www.itmagazine.ch/Artikel/67409/Polizei_warnt_vor_Anrufen_von_falschen_Google-Mitarbeitern.html (Stand: 31. Juli 2018).

In einem anderen Fall kam es zu Telefonanrufen im Namen des Bundesamtes für Energie (BFE). Die Anrufer gaben vor, einen Energiecheck vor Ort durchführen zu wollen. Ob die Anrufer das Opfer ausspähen, ihm etwas aufschwatzen oder auf den Computer zugreifen wollten, ist nicht bekannt.

Empfehlung:

In vielen Unternehmen mit Kundenkontakt stehen Computer im Kundenbereich. Wenn sich Mitarbeitende vom Computer entfernen müssen, wird aus Bequemlichkeit oft darauf verzichtet, diesen zu sperren. In dieser Zeit haben potenzielle Angreifer die Möglichkeit, Programme von USB-Sticks zu aktivieren oder irgendwelche bösartigen Seiten aufzurufen. Der Computer sollte auch bei kürzester Abwesenheit immer gesperrt werden. Zusätzlich kann auch der Schutz der USB-Schnittstellen einen Sicherheitsgewinn bringen, insbesondere dann, wenn diese nicht verwendet werden. Betriebssysteme sind mittlerweile so eingerichtet, dass sie Dateien auf einem USB-Stick nicht mehr automatisch ausführen. Der Benutzer muss bestätigen, dass er die Aktion durchführen möchte. Trotzdem gibt es immer wieder Sicherheitslücken, die dieses Sicherheitselement aushebeln können.

4.4.7 «Look alike»-Domain

Bereits 2005 warnte MELANI vor folgendem Phishing-Trick: Betrüger täuschten unter Zuhilfenahme von so genannt internationalisierten Domainnamen (IDN) dem surfenden Anwender URLs vor, die den echten zum Verwechseln ähnlich sehen. Die Domäne www.epic.com mit kyrillischen Zeichen ist beispielsweise quasi nicht zu unterscheiden von der Webseite www.epic.com des Software-Herstellers Epic. Wenn man zusätzlich das entsprechende Sicherheitszertifikat ausstellt, ist es auch möglich, eine mit «https://» geschützte Verbindung herzustellen. Dadurch erscheint die Internetseite für einen Besucher durch das Schloss im Browser als «sicher» und deshalb vertrauenswürdig. Sehr viele internationale Zeichen sehen praktisch identisch aus wie jene in unserem Alphabet, was zu Missbräuchen führt. Diese Vorgehensweise wird als homographischer Angriff oder homographisches Phishing bezeichnet. Nachdem diese Angriffsart in den letzten Jahren kaum aufgefallen ist, wurden in der aktuellen Berichtsperiode wieder Fälle in der Schweiz beobachtet.

Weil die kyrillischen Buchstaben a, c, e, o, p, x und y praktisch gleich aussehen wie die lateinischen Buchstaben a, c, e, o, p, x und y, werden kyrillische Schriftzeichen am häufigsten für homographische Angriffe verwendet. h, i, j und s können ebenfalls verwendet werden. Beim griechischen Alphabet ähnelt nur das Omikron «o» und das Ny «v» einem lateinischen Kleinbuchstaben. Eher selten werden armenische und hebräische Schriftzeichen verwendet.[13]

Die Abhilfe einzelner Browserhersteller bestand im Jahre 2005 darin, dass in der Adressleiste die Sonderzeichen als so genannter «Punycode» dargestellt wurde, so dass der Benutzer eine solche Domain leicht erkennen konnte. Der Domainname paypal.com mit einem kyrillischen a lautet dann xn—pypal-4ve.com. «Firefox» führte zudem eine «Whitelist» mit überprüften Domänen ein, bei denen kein «Punycode» eingeblendet wurde. Diese Strategie wurde 2012 geändert, da im Zuge der Verbreitung von IDN-Domains der Unterhalt und die Grösse der

[13] https://de.wikipedia.org/wiki/Homographischer_Angriff (Stand: 31. Juli 2018).

«Whitelist» zu gross wurde. IDNs werden seitdem dargestellt, wenn alle Zeichen dem gleichen Zeichensatz angehören oder die «Top Level»-Domäne (TLD) den Einsatz von IDNs einschränkt. Ähnlich wird es auch in «Internet Explorer» und «Opera» gemacht. «Safari» stellt problematische Zeichensätze ebenfalls in Punycode dar.

Betroffen sind vor allem länderübergreifende TLDs wie .com, .net oder .biz. Dabei achten die Angreifer darauf, dass alle Buchstaben aus einem Zeichensatz stammen und deshalb der Browser den Punycode nicht einblendet. Dies schränkt zwar ein. Aus den obgenannten Buchstaben lässt sich die eine oder andere Kombination homographer Phishing-Domains kreieren.

Bei länderspezifischen TLDs werden die Zeichensätze meist eingeschränkt, so auch bei der TLD .ch.[14] Hier sind nur 32 zusätzliche Zeichen erlaubt. Trotzdem können Angreifer auch hier Buchstaben nehmen die ähnlich aussehen. Ein î mit Accent ist nur schwer von einem normalen i zu unterscheide. Der Browser stellt bei eingeschränktem Zeichensatz kein Punycode dar.

Abbildung 5: Abbildung der 32 zusätzlichen Zeichen, welche in der Schweiz für Domainnamen erlaubt sind (Quelle:nic.ch)

Beurteilung/Empfehlung:

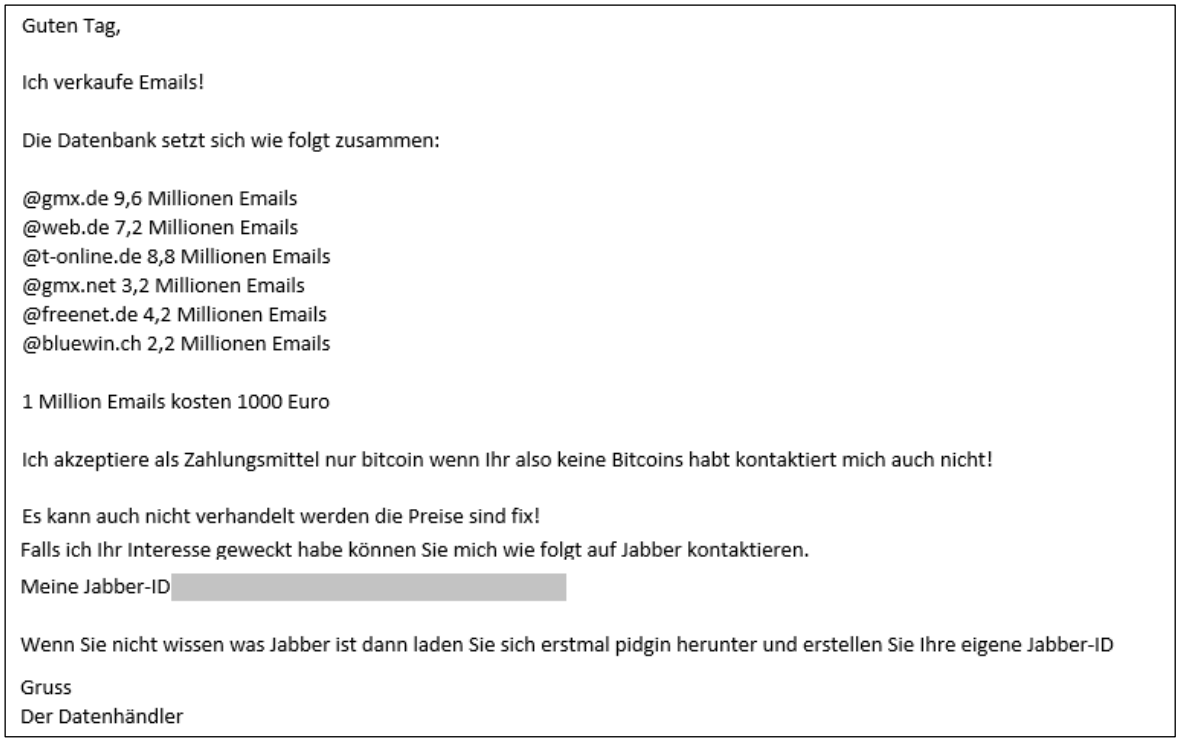
Die durch die Browserhersteller getroffenen Massnahmen lösen dieses Problem grösstenteils. Erfahrungsgemäss betreiben die Angreifer keinen allzu grossen Aufwand, um Phishing-Seiten zu generieren. Meist werden Websites gehackt, um anschliessend darauf betrügerische Seiten zu platzieren. Um eine korrekte URL bemüht sich kaum jemand. Anders sieht es bei sehr gezielten Angriffen aus. Diese Methode könnte durchaus ein Weg sein, um einen Spionage-Trojaner an das Opfer zu bringen.

Im «Firefox» kann man IDN komplett deaktivieren. Danach werden alle URLs in der Adresszeile in «Punycode» dargestellt. Dazu muss man auf der Konfigurationsseite (about:config) die Variable «network.IDN_show_punycode» von «false» auf «true» stellen.

4.4.8 E-Mail Adressen zu verkaufen

Bereits im Dezember 2017 wurde eine grosse Anzahl E-Mail-Adressen im Internet zum Kauf angeboten. Im Mai 2018 wurde ein weiteres Mal in grosser Zahl ein Verkaufsangebot von E-Mail-Adressen an Schweizer Empfängerinnen und Empfänger versendet. Es lässt sich nicht sagen, ob der Absender tatsächlich im Besitz der angegebenen Menge E-Mail-Adressen war.

[14] https://www.nic.ch/de/faqs/idn/ (Stand: 31. Juli 2018).



Guten Tag,

Ich verkaufe Emails!

Die Datenbank setzt sich wie folgt zusammen:

@gmx.de 9,6 Millionen Emails
@web.de 7,2 Millionen Emails
@t-online.de 8,8 Millionen Emails
@gmx.net 3,2 Millionen Emails
@freenet.de 4,2 Millionen Emails
@bluewin.ch 2,2 Millionen Emails

1 Million Emails kosten 1000 Euro

Ich akzeptiere als Zahlungsmittel nur bitcoin wenn Ihr also keine Bitcoins habt kontaktiert mich auch nicht!

Es kann auch nicht verhandelt werden die Preise sind fix!
Falls ich Ihr Interesse geweckt habe können Sie mich wie folgt auf Jabber kontaktieren.
Meine Jabber-ID

Wenn Sie nicht wissen was Jabber ist dann laden Sie sich erstmal pidgin herunter und erstellen Sie Ihre eigene Jabber-ID

Gruss
Der Datenhändler

Abbildung 6: Im Mai 2018 wurde ein weiteres Mal in grosser Zahl ein Verkaufsangebot von E-Mail-Adressen an Schweizer Empfängerinnen und Empfänger versendet.

Dass Erstellen von Sammlungen mit E-Mail-Adressen und deren Weiterverkauf stellt ein lukratives Geschäftsmodell von Internetkriminellen dar. Die Betrüger nutzen sowohl Informationen, die aus Datendiebstählen stammen, als auch frei verfügbare Quellen. Spammer lassen automatisiert das Internet nach gültigen E-Mail-Adressen durchforsten, die auf Webseiten (beispielsweise in Foren oder Gästebüchern usw.) publiziert sind. Auch kompromittierte E-Mail-Konten sind eine gute Quelle für E-Mail-Adressen. Hier werden sowohl Adressbücher als auch die E-Mails nach Adressen durchsucht. Eine weitere Methode ist das Durchprobieren gängiger Vor- und Nachnamen. Wird eine E-Mail an solche geratenen Adressen versendet, melden die meisten Mailserver, dass diese Adresse nicht existiert – bei allen anderen kann der Sender davon ausgehen, dass die Adresse tatsächlich existiert. Diese Versuche werden vollautomatisiert durchgeführt.

Sammlungen mit gültigen E-Mail-Adressen kursieren im Untergrundmarkt zuhauf. In der Regel spielt sich der Verkauf von solchen Daten auch innerhalb dieses Marktes ab. Es ist sehr untypisch, dass solche «Verkaufsangebote» in grosser Zahl ungezielt an «normale» Internetnutzer versendet werden. Die Motivation der Angreifer bei solchen Massenversänden ist unklar. Denkbar ist ein Versuch, die Empfänger zu verleiten, Geld im Voraus zu bezahlen, ohne dass die Täterschaft überhaupt im Besitz der E-Mail Adressen ist. Es kann sich auch um einen Versuch handeln, eine bestehende Spam-Datenbank auf ihre Aktualität zu überprüfen und zu schauen, welche E-Mail-Adressen von den Mail-Servern zurückgewiesen werden.

Beurteilung / Empfehlung:

Die E-Mail-Welle im Mai 18 führte zu zahlreichen Meldungen an MELANI und auch zu einiger Verwirrung, da in vielen Fällen vermutet wurde, dass auch das zur E-Mail-Adresse zugehörige Passwort gestohlen und verkauft würde. Dies war glücklicherweise nicht der Fall. Das Auftauchen der eigenen Adresse in einer solchen Datenbank ist zwar unschön, lässt sich aber kaum verhindern, da die E-Mail-Adresse der zentrale Dreh- und Angelpunkt aller Internetdienstleistungen ist und deshalb vielerorts verwendet wird. Eine Sicherheitseinbusse besteht dennoch nicht, sofern man sich an die gängigen Richtlinien im Umgang mit E-Mails hält:

Siehe Verhaltensregeln im Umgang mit E-Mails auf der MELANI-Website

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

MELANI empfiehlt in solchen Fällen, die E-Mail zu ignorieren und auf keinen Fall zu antworten. Eine Antwort bestätigt den Spammern, dass die gewählte E-Mail-Adresse funktioniert und die Nachrichten gelesen werden. Dies kann einen Anstieg an Spam-E-Mails zur Folge haben.

4.5 Datenabfluss

4.5.1 Kundendaten kommen bei Vertriebspartner von Swisscom abhanden

Im Herbst 2017 entwendeten Cyber-Kriminelle Kontaktdaten von rund 800'000 Swisscom-Kunden. Allerdings wurde das Swisscom-Netzwerk nicht direkt kompromittiert: Die Hacker beschafften sich die Zugangsdaten eines Vertriebspartners, der mit der Bearbeitung dieser Daten betraut war. Wie die Zugriffsdaten beim Vertriebspartner entwendet wurden, ist nicht bekannt. Swisscom hatte den Vorfall bei einer Routinekontrolle entdeckt.[15]

Bei den gestohlenen Daten handelt es sich um Informationen, die notwendig sind, um den Kunden zu identifizieren, wie etwa Name, Wohnadresse, Telefonnummer und Geburtsdatum. Es sind Informationen, die grösstenteils auch in Telefonbüchern oder auf Social Media zu finden sind. Gemäss Philippe Vuilleumier, Leiter «Group Security» von Swisscom, waren keine gemäss Datenschutz als «besonders schützenswert» eingestufte Personendaten wie Passwörter, Gesprächs- oder Zahlungsdaten betroffen. Solche sensiblen Daten werden mit entsprechend strengeren Schutzmechanismen gesichert.[16]

Als Sofortmassnahme hat Swisscom die betroffenen Zugänge der Partnerfirma gesperrt und in einer zweiten Phase die Sicherheitsmassahmen verschärft. Insbesondere wurden eine

[15] https://www.srf.ch/news/wirtschaft/massnahmen-eingeleitet-datendiebstahl-bei-swisscom (Stand: 31. Juli 2018).

[16] https://www.swisscom.ch/de/about/medien/aktuell/interview-philippe-vuillemier-leiter-group-security.html (Stand: 31. Juli 2018).

verstärkte Überwachung der Zugriffe durch Partnerfirmen, ein Alarmierungssystem bei verdächtigen Aktivitäten und eine Zwei-Faktoren-Authentifizierung eingeführt.[17]

Zu den Sofortmassnahmen gehörte auch die transparente Kommunikation. So wurde der eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) informiert, Festnetz- und Firmenkunden schriftlich benachrichtigt und ein kostenloser Infodienst via SMS eingerichtet. So konnten Mobilfunkkunden überprüfen, ob sie von diesem Datenabfluss betroffen waren.

4.5.2 Die Verwendung von gestohlenen Daten

Am 26. April 2018 meldete die schweizerische Firma «Epsitec», Herstellerin einer Verwaltungssoftware für kleine und mittlere Unternehmen, auf ihrer Website, Opfer eines Datendiebstahls gewesen zu sein. Der Angriff betraf E-Mail-Adressen, Telefonnummern und die Postdresse von etwa 35'000 Kunden. Gemäss Angaben von «Epsitec» wurden keine Kreditkartennummern und Passwörter gestohlen.[18] Bemerkenswert in diesem Fall war der Verwendungszweck der Daten durch die Kriminellen: Sie generierten draus personalisierte E-Mails, um den die Schadsoftware Retefe zu verbreiten. Da Nutzerinnen und Nutzer unerwarteten und unpersönlichen E-Mails immer misstrauischer begegnen, müssen sich Kriminelle einiges einfallen lassen. Eine persönliche Anrede oder der Bezug zu einem bestehenden Firmenkontakt können dabei helfen, das Opfer zum Öffnen einer angefügten Datei zu verleiten. Im aktuellen Fall wurden deshalb nicht nur Vorname und Name verwendet, sondern auch die Daten aus dem «Epsitec»-Datendiebstahl, um der E-Mail mehr Glaubwürdigkeit zu verleihen. Mit der E-Mail wurde entweder eine angeblichen DHL-Lieferung angekündigt oder eine Anfrage der Eidgenössischen Steuerverwaltung (ESTV) vorgetäuscht.

4.5.3 Passwörter für «Sextortion»

In der Berichtsperiode wurde ein weiterer Verwendungszweck von Daten aus Datenabflüssen beobachtet. Speziell ist dabei, dass es sich zwar um sensible Daten wie Passwörter handelt, diese Daten aber zum Teil mehrere Jahre alt sind. Auf den ersten Blick sind solche veralteten Daten nur von geringem Nutzen. Kriminelle haben sich aber auch für solche Daten einen Verwendungszweck einfallen lassen. MELANI hat im Sommer 2018 verschiedenste Wellen von erpresserischen E-Mails registriert. Den Empfängern wird mit der Veröffentlichung kompromittierende Materials gedroht, welches zuvor mittels Malware auf dem Computer des Opfers zusammengetragen worden sein soll.[19] Die Erpresser behaupten, auch die Webcam des Empfängers unter Kontrolle zu haben. Als vermeintlichen Beweis erwähnen die Kriminellen ein Passwort oder eine Mobilfunknummer, welche tatsächlich vom Opfer verwendet wird resp. früher verwendet worden ist. Die Angabe solch persönlicher Daten dient dazu, der Forderung mehr Glaubwürdigkeit zu verleihen und den Empfänger zu verunsichern. Genau hier kommen die Angaben aus alten Datenabflüssen ins Spiel. Bei allen gemeldeten Fällen stammten die Angaben aus älteren Datenbeständen.

---

17 https://www.swisscom.ch/de/about/medien/press-releases/2018/02/20180207-mm-swisscom-verschaerft-sicherheitsmassnahmen-fuer-kundenangaben.html (Stand: 31. Juli 2018).

18 https://www.watson.ch/digital/schweiz/581594688-hacker-klauen-35-000-kundendaten-bei-schweizer-software-firma-epsitec (Stand: 31. Juli 2018).

19 https://www.skppsc.ch/de/themen/internet/sextortion-erpressung/ (Stand: 31. Juli 2018).

Beurteilung:

Die Erpresser versandten die E-Mails auf gut Glück in der Hoffnung, dass sich unter den Empfängern Personen befinden, welche sich in letzter Zeit Pornoseiten angeschaut hatten. Die Empfänger lassen sich so durch die E-Mail einschüchtern. MELANI wurde kein einziger solcher Fall gemeldet, bei dem die Täterschaft tatsächlich im Besitz von kompromittierendem Bild- oder Videomaterial war, geschweige denn solches versendet oder publiziert hätte.

4.5.4 «Credential Stuffing» mit alten Passwörten

Zwar ändern viele Benutzende regelmässig ihre Passwörter. Kann ein Krimineller allerdings auf eine Vielzahl von Datensätzen zurückgreifen, sind darunter immer einige gültige Passwörter. Viele Nutzerinnen und Nutzer verwenden das gleiche Passwort bei verschiedenen Diensten und dies über längere Zeit. Dies ist eine willkommene Vereinfachung für Kriminelle und ermöglicht ihnen, die gesammelten Login-Daten aus den diversen Datenabflüssen bei den verschiedensten Internetdienstleistern systematisch durchzuprobieren. Hierbei spricht man von sogenanntem «Credential Stuffing». Wenn Nutzerinnen und Nutzer ein Passwort mehrfach verwenden, ermöglichen sie den Kriminellen, sich mit etwas Glück oder Ausdauer unter ihrer Identität einzuloggen und den Dienst zu missbrauchen. In einem Fall, der MELANI 2018 gemeldet wurde, wurden knapp eine Million solch gestohlener Login/Passwort-Kombinationen benutzt, um zu versuchen, sich in ein Online-Portal einzuloggen. Im besagten Fall stammten die missbräuchlich verwendeten Zugangsdaten aus teilweise sehr alten Abflüssen bei anderen Anbietern.

Beurteilung / Empfehlung:

Regelmässig werden Webshops und andere Internetdienste gehackt und die zugehörigen Kundendaten extrahiert. Wenn Passwörter nicht oder nur unzureichend verschlüsselt sind, können Kriminelle in den Besitz von Zugangsdaten gelangen. Mit diesen Daten versuchen die Kriminellen, sich bei einer Vielzahl anderer Internetplattformen anzumelden. Sie hoffen, dass Anwender dieselben Login-Daten bei mehreren Diensten einsetzen.

Dienste, die solche Login-Versuche feststellen, können sich bei MELANI melden. MELANI integriert diese Daten in das Checktool (www.checktool.ch). Anschliessend können Internetnutzende mittels Checktool überprüfen, ob ihre Daten betroffen sind.

Online verwendete Passwörter müssen ausreichend lang sein, damit sie nicht einfach zu erraten sind. Pro Shop/Dienst sollte ein separates Passwort gewählt werden. Wo dies verfügbar ist, sollte ein zweiter Faktor für das Login aktiviert werden.

4.6 Crimeware

Auch im ersten Halbjahr 2018 gab es zahlreiche Infektionen mit krimineller Software (Crimeware). Die Statistik in Abbildung 7 zeigt die Verteilung der wichtigsten Schadsoftware in der Schweiz auf. Es gibt auch Malware, die zwar ebenfalls eine hohe Bedeutung hat, aber nicht in der Statistik erscheint wie zum Beispiel die E-Banking-Malware «Retefe». «Retefe» ist keine Schadsoftware im eigentlichen Sinne, sondern verändert lediglich die Einstellungen des Browsers.

Der grösste Anteil ging wie bereits in den Vorjahren auf das Konto der Schadsoftware «Downadup» (auch bekannt als «Conficker»). Der Wurm existiert bereits seit über zehn Jahren und verbreitet sich über eine im Jahr 2008 entdeckte Sicherheitslücke in Windows-Betriebssystemen. Der entsprechende Patch ist ebenfalls seit 2008 verfügbar. Auf Platz zwei folgt neu «Gamut» - eine Spam-Malware, welche im letzten Quartal 2017 für 37% des internationalen Spam-Aufkommens verantwortlich sein soll. Das «Gamut Botnet» sendet vor allem Spam zu Jobangeboten zwecks «Money Mule»-Rekrutierung.[20] Auf Platz drei folgt «Gamarue»[21] - auch bekannt unter dem Namen «Andromeda». Dies ist ein Downloader, der weitere Schad-Software nachladen kann. An vierter und fünfter Stelle folgen die Schadsoftware «Spambot» und «Stealrat». Auch diese beiden sind für den Versand von Spam zuständig. «Stealrat» tut dies über infizierte Domänen oder IP-Adressen, unter denen «WordPress», «Joomla!» und «Drupal» laufen. Spam-Nachrichten werden dadurch über legitime Mail-Server versendet und sind schwieriger zu filtern. Auf Platz sechs folgt die erste Cryptominer-Schadsoftware «Monerominer» in der Liste, auf Platz neun der erste E-Banking-Trojaner «Gozi». Das seit dem Angriff auf den Internetdienstleister «Dyn» bekannt gewordene Bot-Netzwerk «Mirai» ist aus den Top Eleven verschwunden.

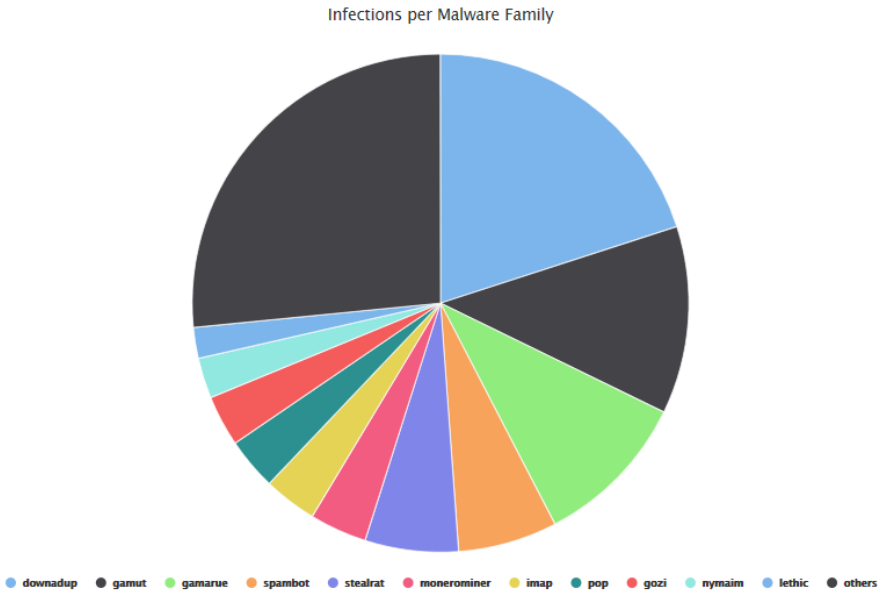


Abbildung 7: Verteilung der Schadsoftware in der Schweiz, welche MELANI bekannt ist. Stichtag ist der 30. Juni 2018. Aktuelle Daten finden Sie unter: http://www.govcert.admin.ch/statistics/dronemap/

4.7 E-Banking Trojaner in der Schweiz

Online-Zahlungssysteme sind attraktive Ziele für Cyber-Kriminelle, da man mit ihnen mit einem insgesamt kleinen Risiko grosse Gewinne machen kann. Die meisten heute beobachteten Cyber-Kampagnen verbinden Social Engineering-Methoden und die

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

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

Verwendung von Malware. Ausserdem werden verschiedene Tricks angewendet, um die Antivirenprogramme zu umgehen, die eigene Infrastruktur gegen Take-Down-Versuche zu schützen und Massnahmen der Strafverfolgungsbehörden zu erschweren. Auch in der untersuchten Berichtsperiode waren wieder verschiedene E-Banking-Trojaner im Umlauf.

4.7.1 «Retefe» und Social Engineering

«Retefe» gehört aktuell zu den verbreitetsten Trojanern in der Schweiz. Früher geschah die Verbreitung der Malware in erster Linie via gefälschte Rechnungen von Online-Shops wie z. B. Zalando oder Ricardo, doch in jüngerer Zeit hat «Retefe» seine Absender um viele bekannte Firmen erweitert. So verzeichnete MELANI im ersten Halbjahr 2018 mehrere Spam-Wellen im Namen von DHL, der SBB, der Polizei verschiedener Kantone, der Eidgenössischen Steuerverwaltung (ESTV) und der Fluggesellschaft Swiss. Zudem ist «Retefe» vom flächendeckenden Spam-Versand zum gezielten Versand mit personalisiertem Inhalt übergegangen. So wurden E-Mails mit richtigem Namen und Telefonnummer der Empfängerinnen und Empfänger versehen. Die Personalisierung setzt zwar grössere Vorbereitung des Angriffs voraus, die Anstrengungen scheinen sich aber zu lohnen, da sich die Opfer so besser täuschen lassen und sich die Erfolgschancen auf eine Infizierung dementsprechend erhöhen.

Die Schadsoftware zielt darauf ab, die Einstellungen des Webbrowsers (Internet Explorer, Firefox und Chrom) dahingehend zu verändern, dass das Opfer beim Aufruf einer E-Banking Seite auf eine von den Cyber-Kriminellen verwalteten Kopie umgeleitet wird. Beim Login-Vorgang auf das vermeintliche E-Banking-Portal ein, wird zuerst ein QR-Code eingeblendet, der, wird er mit einem Smartphone geöffnet, zu einem sogenannten SMS-Diebstahl-Trojaner führt. Nach der Installation dieser Android-App, werden alle von der Bank gesendeten SMS für die Zweifach-Authentifizierung an die Angreifer weitergeleitet. Betrüger können sich dann in das E-Banking des Opfers einloggen und Zahlungen vornehmen. In einem anderen Fall versuchten die Cyber-Kriminellen an Aktivierungsdaten für das E-Banking zu gelangen. Diese Daten werden den Bankkunden normalerweise mit einem Brief per Post zugestellt und enthalten einen QR-Code, der beim ersten Login im E-Banking mittels einer entsprechenden App eingescannt werden muss. Damit wird das Smartphone von der Bank als Kommunikationsmittel für die Zweifaktor-Authentifizierung anerkannt. Die Betrüger haben die Opfer via E-Mail aufgefordert, das Schreiben einzuscannen oder zu fotografieren.[22] Meist richtetet sich Retefe gegen Windows-Systeme. Im Jahre 2017 wurden aber auch verschiedene Angriffswellen beobachtet, welche sich gezielt gegen Schweizer Nutzende des Betriebssystems MacOS richteten.[23]

Seit September 2017 gehört auch die Sicherheitslücke «EternalBlue» zum Repertoire der Angreifer. Wenn ein Mitarbeiter in einer Firma versehentlich einen infizierten Anhang öffnet, kann die Malware mit Hilfe dieser Lücke auf den Computer springen, auf dem die Firma ihre E-Banking-Zahlungen tätigt. Das funktioniert allerdings nur, wenn die Sicherheitslücke, für die am 14. Mai 2017 ein Sicherheitspatch herausgegeben wurde, noch nicht geschlossen worden

---

22 https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/e-banking--angreifer-haben-es-auf-aktivierungsbriefe-abgesehen.html (Stand: 31. Juli 2018).

23 https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/malware---si-raccomanda-prudenza-indipendentemente-dal-sistema-o.html (Stand: 31. Juli 2018).

ist. Die Implementierung von «EternalBlue» deutet darauf hin, dass «Retefe» vor allem auf KMUs angesetzt wird.

4.7.2 «Dridex» und Offline Zahlungs-Software

In unseren Breitengraden ebenfalls weit verbreitet ist der E-Banking-Trojaner «Dridex». Dabei handelt es sich um einen Computerwurm, der erstmals im Jahr 2012 unter dem Namen «Cridex» auftauchte. Die wurmartige Verbreitung wies jedoch Nachteile auf, da offene Sicherheitslücken benötigt werden und auch die Verbreitung sehr auffällig ist. Jüngere Versionen werden deshalb fast ausschliesslich mit umfassendem Spam-Versand verbreitet. Dabei kommen infizierte Word-Dokumente zum Einsatz, welche als Rechnung, Bestätigung einer Online-Bestellung, Zahlungsaufforderung oder ähnliches getarnt werden. Als E-Mail-Absender werden scheinbar echte Firmen verwendet, die ihren Sitz oft im gleichen Land wie die Opfer haben. Die auf die Schweiz zugeschnittenen E-Mails sind hauptsächlich in Deutsch verfasst. Im ersten Halbjahr 2018 Jahr wurde in der Schweiz nur eine E-Mail-Welle zur Verbreitung von «Dridex» verzeichnet: E-Mails, welche im Namen von Swisscom versendet wurden, enthielten eine E-Rechnung, die der Rechnung des Telekommunikationsunternehmens sehr ähnlich waren. Hinter einem Feld mit dem Hinweis «Rechnung einsehen» versteckte sich ein Link zu einem schädlichen JavaScript, welches dann versuchte, den E-Banking-Trojaner «Dridex» zu installieren.

Einmal installiert wendet Dridex die so genannte Man in the Middle (MITM)-Methode an. Mit dieser Technik schaltet sich der Angreifer unbemerkt in einen Kommunikationskanal zwischen zwei Partnern – in diesem Falle der Bank und dem E-Banking Kunden - damit er den Austausch von Daten mitverfolgen und manipulieren kann. «Dridex» ist dezentral organisiert und dessen Netzarchitektur ist auf mehrere Ebenen und in untergeordnete Netze aufgeteilt, welche von unterschiedlichen kriminellen Gruppen unterhalten werden. Dies erschwert Gegenmassnahmen seitens der Behörden. Aus diesem Grund stellt «Dridex» weiterhin eine erhebliche Gefahr dar, obwohl im Oktober 2015 das US-Justizministerium und das FBI vermutlich den Kopf des Netzes verhaften konnten und seither weitere Angehörige des Netzwerks festgenommen werden konnten.[24]

Im Juli 2016 erweiterte «Dridex» den Modus Operandi auf «Offline Zahlungssysteme".[25] Nach der Infektion sucht die Schadsoftware Dridex nach Offline Zahlungs-Software auf dem infizierten Computer. Solche Software wird von vielen Unternehmen verwendet, um grössere Mengen an Zahlungen via Internet an eine oder mehrere Banken zu übermitteln. Findet Dridex eine solche Zahlungs-Software auf dem Computer, kann weitere Schadsoftware aus dem Internet nachgeladen werden, welche dann für das Erfassen von betrügerischen Zahlungen verwendet wird. In einigen Fällen wurde zum Beispiel das Schadprogramm «Cobalt Strike» eingesetzt, in anderen Fällen «Carbanak». Wurde auf dem infizierten Computer keine Offline Zahlungs-Software gefunden, griff «Dridex» seinen Möglichkeiten entsprechend die E-Banking-Sitzungen an.

Seit 2016 nimmt «Dridex» auch Geldbörsen von Kryptowährungen ins Visier. Dieses Jahr haben diesbezügliche Ziele in den Konfigurationsdateien zugenommen.

---

[24] https://www.fbi.gov/contact-us/field-offices/pittsburgh/news/press-releases/bugat-botnet-administrator-arrested-and-malware-disabled (Stand: 31. Juli 2018).

[25] https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/offline-payment-software.html (Stand: 31. Juli 2018).

Zurzeit ist sowohl national als auch international lediglich eine moderate Aktivität sichtbar. Das muss aber nicht heissen, dass die Gefahr abnimmt. Die gegenwärtige Ruhe kann auch als Aktualisierungs- und Vorbereitungsphase dienen. Zudem verwenden andere Organisationen wie die «Cobalt Gang», die wahrscheinlich mit «Dridex» zusammenarbeiten, die Ressourcen weiterhin.

4.7.3 «Gozi ISFB» und die Drive-by-Verbreitung

Die E-Banking Schadsoftware «Gozi» wurde in der Schweiz erstmals im Januar 2009 beobachtet. Es wird davon ausgegangen, dass «Gozi», vom Russen Nikita Kuzmin ins Leben gerufen worden ist, welcher im August 2011 vom FBI verhaftetet wurde.[26] Die Verbreitung von «Gozi» auf den Schwarzmärkten führte jedoch dazu, dass diese derzeit von verschiedenen Cyber-Kriminellen weiterhin eingesetzt wird. Die neue «ISFB» genannte Version nahm die Kunden von Schweizer Banken zum ersten Mal im Mai 2015 ins Visier. Auch «Gozi» verwendet die Man-in-the-Middle (MITM)-Methode für den E-Banking Betrug.

Die neue Variante von «Gozi» wird vor allem über Webseiteninfektionen verbreitet. Die Online Versionen von Tageszeitungen, die täglich von zahlreichen Leserinnen und Lesern besucht werden, sind ideale Angriffsziele für diese Art von Malware. Ihre Beliebtheit erlaubt es, eine grosse Anzahl von Opfern zu erreichen. So wurde beispielsweise im März 2017 die Webseite 20min.ch angegriffen, um den E-Banking-Trojaner zu verbreiten.[27] Ebenfalls werden Mail-Wellen mit infizierten .zip-Anhängen beobachtet. Anfang März 2018 beispielsweise als vermeintliche Paketankündigung der Firma Fedex.

2018 nutzte «Gozi» zum ersten Mal auch «Malvertising» um die Schadsoftware zu verbreiten. Diese Technik besteht darin, mithilfe von Werbeinseraten den Benutzer zu verleiten, eine manipulierte Software herunterzuladen. Bei Suchmaschinen werden die Anzeigen oft oberhalb der eigentlichen Suchresultate eingeblendet. Dies führt zu Verwechslungen bei den Nutzerinnen und Nutzern. Konkret warben die Cyber-Kriminellen auf google.ch für Java- und Firefox-Software, die neben dem gewünschten Programm auch noch gleich die Malware beinhaltete.

Aktuell scheint auch «Gozi» nicht nur E-Banking-Systeme ins Visier zu nehmen, sondern auch Offline Zahlungs-Software und Kryptowährungs-Geldbörsen. Das Interesse an diesen modernen Zielen scheint ein Haupttrend für die nahe Zukunft zu sein.

---

[26] https://www.justice.gov/usao-sdny/pr/nikita-kuzmin-creator-gozi-virus-sentenced-manhattan-federal-court (Stand: 31. Juli 2018).

[27] https://www.srf.ch/news/schweiz/nach-malware-attacke-auf-20-minuten-was-sie-jetzt-tun-koennen (Stand: 31. Juli 2018).

Beurteilung / Empfehlung:

Die drei Kampagnen beleuchten einige Trends auf dem Gebiet der Angriffe auf die Zahlungssysteme. Neben den klassischen Angriffsvektoren wie infizierte E-Mails und Webseiten, erweist sich auch der Missbrauch von Werbung zu kriminellen Zwecken als erfolgreiche Methode zur Verbreitung von E-Banking Schadsoftware. Für Nutzerinnen und Nutzer wird es immer schwieriger, solche Angriffe zu erkennen. In erster Linie sind deshalb die Betreiber von Webseiten gefordert, eine systematische Überprüfung der Werbeinserate und anderer dynamischer Inhalte - gerade von externen Drittfirmen – durchzuführen. Für Nutzerinnen und Nutzer gilt es weiterhin besonders beim Erhalt von E-Mails vorsichtig zu sein, auch wenn diese vermeintlich seriös und personalisiert daherkommen. Es ist deshalb empfehlenswert, lieber einmal zu wenig als zu viel auf einen Link oder einen Anhang zu klicken. Als weiter Trend ist erkennbar, dass KMUs bei E-Banking Angriffen vermehrt ins Visier geraten, weil sie tendenziell weniger gut geschützt sind als Grossfirmen, aber doch höhere Banktransaktionen generieren als eine Privatperson. Die Schweizer KMUs sind deshalb im Bereich der Informatiksicherheit mit wachsenden Herausforderungen konfrontiert. Hinsichtlich der intern zu treffenden Massnahmen hat MELANI vor kurzem eine Aktualisierung des «Merkblatts Informationssicherheit für KMUs» herausgegeben. Es enthält Ratschläge und Tipps, wie die Unternehmen ihre Widerstandsfähigkeit erhöhen können:

DOKU

Merkblatt Informationssicherheit für KMUs
https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/merkblatt-it-sicherheit-fuer-kmus.html

5 Lage International

5.1 Spionage

5.1.1 «Sofacy» in Zusammenhang mit verschiedenen Vorfällen genannt

«Sofacy», auch bekannt unter den Namen «APT28», «Fancy Bear» und «Tsar Team», bleibt weiterhin eine der aktivsten und bekanntesten Spionagegruppierung weltweit. «Sofacy» verwendet alle möglichen Arten von Infektionsvektoren: Gut gemachte und gezielte «Spear Phishing»-E-Mails mit präparierten Anhängen oder Links sowie auch Angriffe über «Watering Holes». Bei dieser Kampagne wird ein breites Arsenal an «Command-und Control»-Servern eingesetzt. Die Entwickler hinter «Sofacy» adaptieren die Malware nicht nur auf einzelne Opfer. Sie betreiben auch einen erheblichen Aufwand, um gezielte «Social Engineering»-Angriffe durchzuführen.[28] Neben den bislang sehr gezielten Angriffen wurden aber mittlerweile auch viel breiter gestreute Angriffe beobachtet, um möglichst viele potenzielle Opfer zu erreichen. Bei den Angriffen mit der Schadsoftware «Zebrocy», einem Downloader für die Backdoor, wurden die Ziele (E-Mail Adressen) nicht spezifisch, sondern eher zufällig

[28] https://securelist.com/a-slice-of-2017-sofacy-activity/83930/ (Stand: 31. Juli 2018).

ausgewählt und waren beispielsweise mittels Suchmaschine leicht auffindbar. Ein solches Vorgehen ist für eine APT-Kampagne eher untypisch und findet sich sonst eher bei Cyber-Kriminellen. Mit einer solchen Strategie ist zwar die Wahrscheinlichkeit einer erfolgreichen Infektion grösser, gleichzeitig steigt aber auch das Risiko, entdeckt zu werden.[29] Bemerkenswert ist auch die Ausweitung der Angriffe nach Fernost mit starkem Interesse an militärischen, Verteidigungs- und diplomatischen Organisationen.[30] Die Wahl von verschiedenen Zielen und Taktiken erschwert die Attribution. Dies könnte auch die Motivation der aktuellen Entwicklung von «Sofacy» sein.

2018 machte die Schadsoftware «Olympic Destroyer» im Zusammenhang mit den Olympischen Spielen in Pyeongchang (Südkorea) Schlagzeilen. So wurde die IKT-Infrastruktur der Winterspiele und jene von einigen Partnern durch diesen Wurm angegriffen. Obschon eine eindeutige Attribution nicht möglich ist, hat der Sicherheitsdienstleister «Kaspersky» einige Ähnlichkeiten mit «Sofacy» ausmachen können (siehe auch Kapitel 4.1.1).

Am 10. Januar 2018 publizierte die Gruppe «Fancy Bears Hack Team» Daten, die zwischen Ende 2016 und Anfang 2017 dem Internationalen Olympischen Komitee sowie dem Nationalen olympischen Komitee der USA entwendet worden sein sollen. Auch hier werden Zusammenhänge mit der «Sofacy» Gruppe vermutet.[31]

5.1.2 VPN-Filter – Mindestens 500'000 Geräte betroffen

Am 23. Mai 2018 publizierte Cisco's Sicherheitsfirma «Talos» Daten zu einem Bot-Netzwerk namens «VPN-Filter», welches mindestens eine halbe Million Router und NAS-Geräte umfassen soll.[32] Bei einem entsprechenden Befehl durch den Angreifer überschreibt die Schadsoftware die ersten 5'000 Bytes des ersten Speicherblocks. Das Gerät kann danach nicht mehr starten. Die Auswirkungen eines gleichzeitigen Ausfalls von einer halben Million Geräte lässt sich in etwa erahnen. Die Geräte befinden sich in insgesamt 54 Ländern mit Schwerpunkt in der Ukraine. Dabei werden Erinnerungen an die Schadsoftware «NotPetya» wach. Auch damals befand sich das Zentrum des Angriffs in der Ukraine, die Auswirkungen waren aber rund um die Welt zu spüren.

Alle infizierten Geräte waren mit dem Internet verbunden und wiesen bekannte Sicherheitslücken auf oder waren nur durch Standardpasswörter geschützt. «VPN-Filter» wurde auf diversen Geräten entdeckt, unter anderem von den Router-Herstellern «MikroTik», «Linksys», «Netgear», «TP-Link» – aber auch NAS-Geräte des Herstellers «QNAP» waren betroffen. Die Schadsoftware ist dreistufig aufgebaut. Nur die erste Stufe ist permanent auf

---

29 https://researchcenter.paloaltonetworks.com/2018/06/unit42-sofacy-groups-parallel-attacks/ (Stand: 31. Juli 2018).

30 https://www.kaspersky.de/about/press-releases/2018_sofacy-erweitert-sein-operationsgebiet-in-richtung-fernost (Stand: 31. Juli 2018).

31 https://www.wired.com/story/russian-fancy-bears-hackers-release-apparent-ioc-emails/ https://www.mid-day.com/articles/russia-apparently-hacking-winter-olympics-emails-report/18923160 https://www.eclecticiq.com/resources/russian-hacking-group-fancy-bear-prepares-to-attack-winter-olympics-u-s-senate (Stand: 31. Juli 2018).

32 https://blog.talosintelligence.com/2018/05/VPNFilter.html (Stand: 31. Juli 2018).

dem Gerät installiert und lädt dann die eigentliche Schadsoftware und deren Funktionen in zwei weiteren Schritten nach.

Am Anfang war die Schadsoftware nur durch ein Rücksetzen auf die Werkseinstellungen zu eliminieren. Praktisch gleichzeitig mit der Veröffentlichung des Bot-Netzwerks konnte das FBI den Server übernehmen, der nach dem Neustart die Informationen für die zweite Stufe liefert, wo und wie die Schadsoftware wieder aufgespielt werden soll. Konkret liest die Malware die benötigten Informationen für eine Neuinstallation aus den Metadaten eines Bildes, welches auf der Foto-Plattform «Photobucket.com» abgespeichert war. Ein Neustart entfernt die Schadsoftware zwar nicht vom Gerät, allerdings kann diese die eigentlichen Funktionen aus Stufe zwei und drei nicht mehr nachladen. Durch die Massnahmen des FBI wird die schädliche Schadsoftware quasi neutralisiert und es können zudem auch infizierte Geräte identifiziert werden. Bei der Analyse ist «Cisco Talos» auf einen charakteristischen Fehler bei der Umsetzung der eingesetzten RC4-Verschlüsselung gestossen, der bereits bei der Malware «BlackEnergy» aufgefallen war.

5.1.3 Angriff auf Netzwerk der Deutschen Bundesregierung

Ende Februar 2018 wurde bekannt, dass das Deutsche Auswärtige Amt Opfer eines Hackerangriffs geworden sei. Der Hackerangriff soll bereits zum Jahreswechsel von 2016 auf 2017 erfolgt sein.[33] Die Angreifer hatten Zugriff auf das zentrale Datennetz der Bundesverwaltung, den sogenannten Informationsverbund Berlin-Bonn (IVBB). Der IVBB ist eine Art Intranet für Bundesrat, Bundeskanzleramt, Bundesministerien, den Bundesrechnungshof und diverse Sicherheitsbehörden. Nach dem Hack des Bundestags im Jahr 2015 ist dies der zweite grosse bekannt gewordene Angriff auf die IKT-Infrastruktur der deutschen Regierung.[34]

Der Angriff soll unter anderem über eine Lernplattform erfolgt sein, die an der Hochschule des Bundes zu Weiterbildungszwecken genutzt wird.[35] Genauere Informationen über möglicherweise verwendete Sicherheitslücken seien aber nicht bekannt.[36] Diverse Medien spekulierten, dass es sich um einen Angriff der «Sofacy»-Gruppe gehandelt haben könnte. Erst später fiel der Verdacht auf die «Snake/Turla»-Gruppe, die auch für Angriffe in der Schweiz verantwortlich gemacht wird. Der Rüstungskonzern «Ruag» wurde ebenfalls mit «Snake/Turla» angegriffen.

5.1.4 Angriffe gegen Energieversorger

Am 15. Mai 2018 machte die «Süddeutsche Zeitung» einen Angriff auf die Telekom- und «EnBW»-Tochterfirma «Netcom BW» publik, der bereits im Sommer 2017 stattgefunden

---

33 https://www.zeit.de/politik/2018-04/hackerangriff-bundesregierung-russland-verfassungsschutz-hans-georg-maassen (Stand: 31. Juli 2018).

34 https://www.zeit.de/digital/datenschutz/2018-03/hackerangriff-bundesregierung-outlook-auswaertiges-amt (Stand: 31. Juli 2018).

35 http://m.faz.net/aktuell/politik/inland/hacker-angriff-war-gezielter-angriff-auf-das-auswaertige-amt-15476826.html (Stand: 31. Juli 2018).

36 https://www.tagesschau.de/inland/hackerangriff-bundesregierung-101.html (Stand: 31. Juli 2018).

hatte.[37] Dieser konnte zwar bereits in einer frühen Phase abgewehrt werden, gemäss des Zeitungsberichts sei es aber während kurzer Zeit möglich gewesen, den Internetverkehr mitzulesen. Die Angreifer konnten über das Mitarbeiterkonto eines externen Dienstleisters auf den Router zugreifen. Unter anderem sollen auch Schwachstellen in der Router-Software von «Cisco» ausgenutzt worden sein. Details zu der Schwachstelle wurden allerdings nicht genannt. Nachdem die Angreifer die Kontrolle übernommen hatten, konnten sie Programme aufspielen und Daten ausleiten. Die Gefahr einer Sabotage habe nicht bestanden, da das Versorgungsnetz nicht über das Netzwerk von «Netcom» laufe. Zudem sei der Angriff in einer frühen Phase entdeckt worden. Wer hinter den Angriffen steckt, konnte nicht eindeutig ermittelt werden. Verdächtigt wird einerseits die Gruppe «Sandworm», welche für die Angriffe auf das ukrainische Stromnetz im Winter 2015/2016 verantwortlich sein soll. Andererseits wird auch die Gruppe «Dragonfly» vermutet, welche bereits im letzten Jahr mit Angriffen gegen westliche Stromversorger aufgefallen ist.[38]

Am 7. Juni 2018 wandte sich das Deutsche Bundesamt für Verfassungsschutz (BfV) in einer Publikation an deutsche Energieunternehmen. Es lägen Erkenntnisse über aktuelle Angriffe der APT-Gruppe «Dragonfly» vor. Im Visier würden die Energieversorgung, die Wasserversorgung/-entsorgung und die Informationstechnik/Telekommunikation stehen. Dabei habe sich gezeigt, dass Angriffe der letzten Monate insbesondere gegen Infrastrukturkomponenten wie Router gerichtet gewesen wären.[39] Die Angreifer verwenden vielfach öffentlich zugängliche Angriffswerkzeuge und versuchen, unzureichend gesicherte Systeme unter ihre Kontrolle zu bringen. Um Zugriff zu erlangen, scannen die Angreifer in der Regel in einem ersten Schritt den Netzbereich eines potenziellen Opfers mit einem Portscanner. Auch das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) warnte seinerseits am 13. Juni 2018 vor Angriffen gegen den Energiesektor – aber auch vor Angriffen gegen andere Sektoren.[40]

Im Juli 2018 hat das «Department of Homeland Security (DHS)» seinerseits bekannt gegeben, dass in den letzten Jahren Hunderte von Zielen in der Stromversorgung der USA angegriffen worden waren. Dabei hatten es Angreifer anscheinend bis in die Kontrollzentren geschafft und waren demnach schon derart tief in die Anlagen vorgedrungen, dass sie hätten «Schalter umlegen» und damit die Stromversorgung beschädigen oder unterbrechen können.[41] Meist suchten die Angreifer den Weg über Drittfirmen mit weniger gut gesichertem Netzwerk. Dazu wurden beispielsweise Phishing-E-Mails versendet, um an die Anmeldeinformationen der

---

37 https://www.sueddeutsche.de/digital/enbw-tochter-hacker-haben-deutschen-energieversorger-angegriffen-1.3980625 (Stand: 31. Juli 2018).

38 MELANI Halbjahresbericht 2/2017 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lagebreichte/halbjahresbericht-2017-2.html (Stand: 31. Juli 2018).

39 https://www.verfassungsschutz.de/de/oeffentlichkeitsarbeit/publikationen/pb-spionage-und-proliferationsabwehr/broschuere-2018-06-bfv-cyber-brief-2018-01 (Stand: 31. Juli 2018).

40 https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/Cyber_Angriffe_auf_deutsche_Energieversorger_13062018.html (Stand: 31. Juli 2018).

41 https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110 (Stand: 31. Juli 2018).

Anbieter zu kommen. Sobald sie einmal in diesem Netz waren, konzentrierten sich die Angreifer auf ihr eigentliches Ziel, die Stromversorger.[42]

5.1.5 «Cisco's» «Smart Install» im Fokus von Angreifern

Bereits seit 2016 gibt es regelmässig Berichte über Angriffe auf Switches von «Cisco» mittels der Fernwartungsfunktion «Smart Install (SMI)». Problematisch sind dabei Geräte, die direkt und ungeschützt mit dem Internet verbunden sind, da das Tool keine Authentifizierung vorsieht. Einen solchen Schutz muss ein Betreiber zusätzlich installieren[43]. Bereits im Februar 2017 veröffentlichte «Cisco» eine Information zu dieser Problematik.[44] Da die Geräte allerdings genauso funktionieren, wie sie sollen, sah «Cisco» darin keine Schwachstelle, sondern verwies vielmehr auf die Verantwortung der Benutzer, welche für den Schutz der Geräte zuständig seien. Das Problem besteht darin, dass Besitzer weder das Protokoll konfigurieren, noch dieses abschalten. Der Client wartet dann im Hintergrund konstant auf Konfigurations- oder Installationsbefehle. Ein Angreifer kann deshalb die Server-Einstellungen modifizieren, die Konfigurations-Dateien auslesen und modifizieren, das Betriebssystem ersetzen und Konten erstellen sowie beliebige Befehle ausführen.

Zwischenzeitlich waren über 200'000 gefährdete Geräte übers Internet erreichbar und liessen sich theoretisch neu konfigurieren oder komplett übernehmen. In der Schweiz waren ca. 1500 IP-Adressen über potentiell exponierte Systeme bekannt.[45] Seit Ende 2017 hat «Cisco» Hinweise darauf erhalten, dass Angreifer Geräte systematisch nach dieser Verwundbarkeit durchsuchen. Wie eine Grafik von Cisco zeigt, hat der Verkehr auf dem dazugehörigen Port 4786 seit dieser Zeit sehr stark zugenommen.

---

42 https://www.nzz.ch/international/russische-hacker-sitzen-schon-an-den-hebeln-der-amerikanischen-stromversorgung-ld.1406263 (Stand: 31. Juli 2018).

43 https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k17-0274_update_1.html (Stand: 31. Juli 2018).

44 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170214-smi (Stand: 31. Juli 2018).

45 Stand Mai 2018

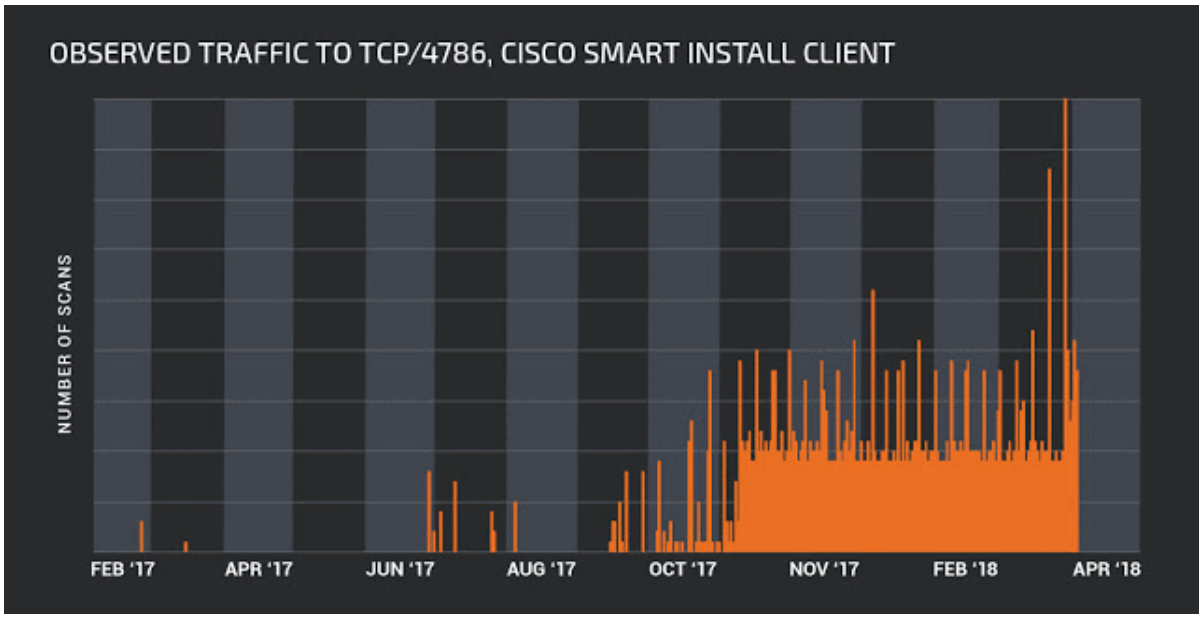


Abbildung 8: Anzahl Scans auf Cisco Smart Install Clients zwischen Februar 2017 und April 2018 (Quelle: Talos, https://www.talosintelligence.com/)

Anfang April 2018 schrieb «Cisco Talos» in einer weiteren Publikation, dass es Hinweise auf vermehrte Angriffe gegen kritische Infrastrukturen unter Zuhilfenahme des SMI-Protokolls gebe.[46] Konkret wurde dabei eine Verbindung zur Spionagegruppe «Dragonfly» vermutet. Zuvor hat das US-amerikanische CERT vor «Russischen Akteuren» gewarnt, welche Netzwerke von Firmen im Energiesektor, aber auch von anderen kritischen Sektoren angegriffen und infiltriert haben.[47]

Ebenfalls im April haben Experten des Sicherheitsunternehmens «Kaspersky» eine Hacker-Kampagne entdeckt, bei der vor allem «Cisco» Geräte im Iran und Russland betroffen waren. Verantwortlich für diese Angriffswelle zeichnete anscheinend ein Bot-Netz, das nach offenen und ungeschützten Ports 4786 sucht, um danach «Smart Install» zu übernehmen, die Konfiguration zu überschreiben und den Switch unbrauchbar zu machen. Schlussendlich wurde eine Nachricht mit einer US-amerikanischen Flagge und ein Text mit den Worten «Do not mess with our elections» hinterlassen.[48]

Dass Ende März zwei Schwachstellen publiziert wurden, welche es einem Angreifer ermöglichen, «Cisco»-Geräte lahmzulegen oder zu übernehmen, sorgte für zusätzliche Schlagzeilen. Der zeitliche Zusammenfall der Angriffe und der beiden Lücken führte zu zahlreichen Spekulationen über einen möglichen Zusammenhang. Dies veranlasste «Cisco» zu einer Klarstellung, dass bei den bislang beobachteten Angriffen keine Sicherheitslücke ausgenutzt wurde, sondern diese einzig und alleine durch schlecht oder nicht konfigurierte Geräte verursacht wurden.[49]

---

46 https://blog.talosintelligence.com/2018/04/critical-infrastructure-at-risk.html (Stand: 31. Juli 2018).

47 https://www.us-cert.gov/ncas/alerts/TA18-106A (Stand: 31. Juli 2018).

48 https://www.kaspersky.com/blog/cisco-apocalypse/21966/ (Stand: 31. Juli 2018).

49 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180409-smi (Stand: 31. Juli 2018).

Beurteilung/ Empfehlungen

Router stehen vermehrt im Visier von Angreifern. Dies hat zwei Hauptgründe. Erstens sind diese meist das schwächste Glied in der Kette, da Updates nicht immer zeitnah eingespielt werden. Zweitens sind Router zentrale Netzwerkgeräte, über welche die Kommunikation einer Firma läuft. Zudem sind Router oft direkt am Internet angeschlossen und demnach auch für einen Angreifer aus dem Internet direkt angreifbar.

Da das Cisco «Smart Install»-Protokoll keine Authentifikation verlangt, kann ein Angreifer jedes vom Internet her zugängliche und nicht zusätzlich geschützte Gerät angreifen. Diese Geräte sind dringend vor unbefugten Angriffen von aussen zu schützen. Ausserdem sind Updates jeweils zeitnah einzuspielen.

5.2 Industrielle Kontrollsysteme

5.2.1 Unerlaubter Zugriff auf das Infotainment-System von VW- und Audi-Fahrzeugen

Im April 2018 veröffentlichten niederländische Sicherheitsforscher die Ergebnisse ihrer Untersuchungen über die Ausnutzung einer Schwachstelle im Infotainment-System bestimmter VW- und Audi-Modelle. Als Angriffsvektor wurde von den Forschern die WIFI-Verbindung des Fahrzeugs verwendet, worüber die Angreifer das IVI-System (in-vehicle infotainment) des Fahrzeugs kompromittieren konnten. Hinter diesem ziemlich allgemeinen Begriff verstecken sich verschiedene interaktive Audio- und Videodienste, mit denen man zum Beispiel Musik hören, Informationen erhalten oder im Fahrzeug telefonieren kann. Die Forscher erklärten, dass sie auf diese Weise Gespräche mithören konnten, die über die Freisprechanlage geführt wurden, Zugriff auf das Adressbuch hatten und die Bewegungen des Fahrzeugs mitverfolgen konnten. Die Forscher beschlossen dann, ihre Arbeiten zu unterbrechen und keine Eindringversuche in kritische Systeme wie die Bremse oder das Gaspedal zu unternehmen.[50]

Es ist nicht das erste Mal, dass die Sicherheit vernetzter Fahrzeuge im Mittelpunkt steht. In der Forschung wird diese Frage regelmässig behandelt, seit der unerlaubte Zugriff auf einen Jeep Cherokee im Jahr 2015 Berühmtheit erlangte.[51] Die Trennung zwischen dem Infotainment-System, welches oft ins Visier von Hackern gerät, und den sensiblen Systemen des Fahrzeugs ist von zentraler Bedeutung. In diesem Fall ist es den Forschern nicht gelungen, eine Durchlässigkeit zwischen diesen beiden Systemen nachzuweisen. Als Massnahme gegen die Publikation einer Sicherheitslücke wäre es auf jeden Fall wünschenswert, die gesamte Fahrzeugflotte respektive deren Software aus der Ferne zu aktualisieren, doch das ist nicht immer möglich. Oftmals sind nur die Systeme neu produzierter Fahrzeuge auf dem neuesten Stand, obwohl es der Kunde in der Hand hätte, den Sicherheits-Patch durch seinen Händler einspielen zu lassen.

---

50 https://www.bleepingcomputer.com/news/security/volkswagen-and-audi-cars-vulnerable-to-remote-hacking/ (Stand: 31. Juli 2018).

51 https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (Stand: 31. Juli 2018).

5.2.2 Cryptominer bei europäischer Wasserwerksteuerung

Der Erfolg der Kryptowährungen bietet äusserst verlockende Perspektiven für Cyber-Kriminelle. Neben Bitcoin-Diebstählen im grossen Stil haben sich die Kriminellen auch an anderer Stelle breit gemacht, indem sie das für diese Art von Währung typische «Mining» missbrauchen. Mining oder auf Deutsch «Schürfen» bezeichnet den Prozess, über den die Transaktionen in einer Kryptowährung verifiziert und neue Währungseinheiten geschaffen werden. Für diese komplexen Berechnungen sind erhebliche IKT-Ressourcen notwendig. Die Bereitstellung dieser Ressourcen wird mit einer gewissen Menge von «geschürftem» Geld entschädigt, die dem Anteil der Beteiligung an der Berechnung entspricht. Letztlich trägt das Mining zur Geldschöpfung bei.

Da dieser Prozess Geld einbringt, suchen gewisse Akteure bereits seit geraumer Zeit nach Möglichkeiten, um diesen zu missbrauchen (derartige Fälle wurden bereits in unserem Halbjahresbericht 2013/2[52] erwähnt). Unterdessen haben sich Angriffe, mit denen Rechnerkapazität für das Mining missbraucht werden, vervielfacht. Laut einem Artikel des Cyber-Sicherheitsunternehmen «PaloAltoNetworks» wurden bislang über 470'000 Malware-Versionen entdeckt, deren Ziel es ist, die Rechenleistung der Geräte ihrer Opfer anzuzapfen[53]. Es sind aber nicht immer nur private Computer, Büroautomation oder Webserver betroffen. Das Newsportal «SecurityWeek» berichtete über einen Cryptominer im Produktionsnetzwerk («Operational Technology network») eines europäischen Wasseraufbereitungsbetreibers.[54] Im betreffenden Fall bewirkte die Malware eine Verlangsamung des Netzwerks, weil die Schadsoftware die Rechenleistung und Internet-Bandbreite anzapfte.[55] Obschon die Infizierung keine schädliche Auswirkung auf die Funktionsweise des Systems hatte, musste das Unternehmen die zusätzlich entstandenen Kosten für Strom und Internet-Bandbreite bezahlen. Gut möglich, dass die Infizierung längerfristig auch das reibungslose Funktionieren der Infrastruktur hätte beeinträchtigen können, mit allen Folgen, die dies für die Nutzerinnen und Nutzer gehabt hätte.

5.2.3 «Hide'n Seek - IoT Botnet mit Peer-to-Peer Funktionalität

Seit der Schadsoftware «Mirai» sind Bot-Netzwerke, welche Geräte im Internet der Dinge für ihre Zwecke missbrauchen, einer breiten Öffentlichkeit bekannt. Anfang Januar 2018 wurde von Sicherheitsforschern ein neues IoT-Botnet mit Namen «Hide'n Seek» entdeckt, welches zur Verbreitung einen wurmartigen Mechanismus verwendet. Dazu erstellt die Schadsoftware eine zufällige Liste von IP-Adressen mit potenziellen Opfern, die anschliessend angesprochen werden. Sind bestimmte Ports bei dem Gerät offen, versucht die Schadsoftware sich mit Standardpasswörter oder Wörterbuchbegriffen einzuloggen; es werden auch unterschiedliche Sicherheitslücken durchprobiert. Das Bot-Netzwerk basiert auf einer für IoT untypischen

---

52 Siehe Halbjahresbericht 2013/2 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2013-2.html (Stand: 31. Januar 2018).

53 https://researchcenter.paloaltonetworks.com/2018/06/unit42-rise-cryptocurrency-miners/ (Stand: 31. Juli 2018).

54 https://www.securityweek.com/cryptocurrency-mining-malware-hits-monitoring-systems-european-water-utility (Stand: 31. Juli 2018).

55 https://radiflow.com/case-studies/detection-of-a-crypto-mining-malware-attack-at-a-water-utility/ (Stand: 31. Juli 2018).

dezentralen Peer-to-Peer-Struktur. Einzelnen Geräte tauschen dabei Informationen zu geglückten Login-Versuchen untereinander aus und lernen voneinander. Im Gegensatz zu «Mirai» legt «Hide'n Seek» den Fokus nicht auf Distributed Denial of Service (DDoS)-Funktion, sondern eher auf Spionage und anschliessenden Erpressungsversuchen. Der Funktionsumfang umfasst die Daten-Exfiltration, Codeausführung, sowie Gerätestörung. Da sich der Schadcode bisher nicht dauerhaft einnisten kann, lassen sich infizierte Geräte mittels Reboot wieder säubern.

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 in Verkehrsmitteln wie Auto und Flugzeug. Dabei dürfen jedoch die damit verbundenen Risiken nicht unbeachtet bleiben. Neue Möglichkeiten bergen immer auch neue Gefahren, die bereits bei der Entwicklung berücksichtigt werden müssen (Security by Design).

DOKU

Checkliste mit Massnahmen zum Schutz industrieller Kontrollsysteme

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

5.3 Angriffe (DDoS, Defacements, Drive-By)

5.3.1 «Memcached DDoS»-Angriff

Der Angriff auf den Online-Dienstleister «Github» am 28. Februar 2018 war mit einer Bandbreite von ca. 1.35 Tb/s einer der stärksten bisher aufgezeichneten DDoS-Angriffe. Mit Hilfe des Providers «Akamai» konnte der Angriff allerdings recht schnell abgewehrt werden.[56,57] Bei diesem Angriff handelte es sich um einen DDoS-Angriff unter Zuhilfenahme der sogenannten «Memcached»-Funktion, die bei Servern zum Einsatz kommt. «Memcached» ist eine Open-Source Software, welche für das Zwischenspeichern (caching) von Daten verwendet wird. Da die Daten im Arbeitsspeicher abgelegt sind, lässt sich schnell auf diese zugreifen, womit im Allgemeinen eine bessere Leistung von beispielsweise Internetanwendungen erreicht wird, siehe auch Kapitel 3. Der Server horcht dabei standardmässig auf Port 11211 TCP und/oder UDP und ist somit für alle Internet-Teilnehmer erreichbar. Nebst TCP wird auch das verbindungslose Protokoll UDP eingesetzt. Dadurch ist es Angreifern möglich, «Memcached»-Dienste, welche nicht durch entsprechende Massnahmen wie beispielsweise eine Firewall geschützt sind, für DDoS-Verstärkungsangriffe auf andere Internet-Teilnehmer zu verwenden. Besonders kritisch dabei ist, dass Angreifer mit einem einzigen UDP-Paket an einen solchen Server einen Verstärkungsfaktor von bis zu 51'000 und dadurch problemlos ein DDoS-Volumen von 1Tb/s und mehr erreichen können.

---

56 https://githubengineering.com/ddos-incident-report/ (Stand: 31. Juli 2018).

57 https://blog.apnic.net/2018/03/26/understanding-the-facts-of-memcached-amplification-attacks/ (Stand: 31. Juli 2018).

Weltweit gab es zum Zeitpunkt des Angriffes ca. 95'000 verwundbare Systeme[58]. Nach dem Angriff wurden viele Betreiber von verwundbaren Systemen angeschrieben und um eine Absicherung gebeten. Dies war durchaus erfolgreich, denn die Zahl ist seither stark gesunken. MELANI hat in der Schweiz ebenfalls verschiedentlich Betreiber über verwundbare Systeme informiert und auch hier konnte die Anzahl reduziert werden.

Empfehlung:

Üblicherweise wird der UDP-Port von «Memcached» (11211 UDP) für den regulären Betrieb nicht benötigt. Wir empfehlen deshalb, beim Einsatz von «Memcached» UDP komplett zu deaktivieren. Dazu muss die Konfigurationsdatei (/etc/memcached.conf) von «Memcached» lediglich mit folgender Zeile ergänzt werden:

-U 0

Beschränken Sie den Zugriff auf den «Memcached»-Server mittels einer Firewall. Es sollten nur diejenigen Systeme Zugriff auf den «Memcached»-Server haben, welche diesen auch benötigen.

Darüber hinaus empfehlen wir die allgemein bekannten Massnahmen zur Sicherung von Online-Diensten, wie z. B.:

- Stellen Sie sicher, dass Sie Updates zeitnah einspielen und somit stets die aktuellste Version von «Memcached» einsetzen.
- Konfigurieren Sie «Memcached»so, dass der «Memcached»-Dienst auf einem alternativen Port als 11211 TCP/UDP horcht. Beachten Sie aber, dass diese Massnahme alleine nicht ausreichend ist, da sie das Problem nur versteckt, anstelle es zu lösen.
- Überwachen Sie den Server, um einen allfälligen Missbrauch rasch zu erkennen.

Weitere Informationen zum Absichern von «Memcached» finden Sie unter.

https://www.digitalocean.com/community/tutorials/how-to-secure-memcached-by-reducing-exposure

https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/CERT-Bund/CERT-Reports/HOWTOs/Offene-Memcached-Server/Offene-Memcached-Server_node.html

5.3.2 Interne Bankensysteme immer noch im Visier der Cyber-Kriminellen

Die internen Systeme von Banken standen im untersuchten Zeitraum erneut im Interesse von Cyber-Kriminellen. Im Februar 2018 meldete beispielsweise die russische Zentralbank, dass bei einer Attacke gegen ein russisches Geldinstitut im letzten Jahr 339,5 Millionen Rubel erbeutet worden waren (was damals rund 6 Millionen US-Dollar entsprach). Um ihr Ziel zu erreichen, griffen die Cyber-Kriminellen erfolgreich einen Computer an, auf dem

[58] https://blog.apnic.net/2018/03/26/understanding-the-facts-of-memcached-amplification-attacks/ (Stand: 31. Juli 2018).

Geldüberweisungen über das Interbanken-Kommunikationssystem SWIFT durchgeführt wurden. Weder die genaue Identität des Opfers, noch die detaillierte Vorgehensweise der Angreifer wurden veröffentlicht.

Im August 2018 wurde ein noch spektakulärerer Angriff publik, bei dem 13,5 Millionen US-Dollar bei der indischen Bank Cosmos erbeutet worden waren. Gemäss den öffentlich verfügbaren Informationen haben die Angreifer gleichzeitig sowohl die Bankomaten als auch die SWIFT-Infrastruktur der Bank kompromittiert. Die Cyber-Kriminellen konnten in der Folge an Geldautomaten in 28 verschiedenen Ländern insgesamt 11,5 Millionen US-Dollar abheben und Transaktionen für 2 Millionen US-Dollar via das SWIFT-System tätigen. Nach der Anfangsinfektion arbeiteten sich die Cyber-Kriminellen mittels lateraler Bewegung zu den kritischen Systemen der Bank vor. Die Komplexität der angewandten Methoden und das Koordinationsniveau des Angriffs, welcher in mehreren Staaten gleichzeitig stattfand, deuten auf einen erfahrenen Akteur hin. Die Firma Securonix, die den Vorfall untersucht hat, schreibt den Angriff der Gruppe «Lazarus» zu. Lazarus ist dafür bekannt, in der Vergangenheit verschiedene Bankensysteme angegriffen zu haben.[59]

5.4 Datenabflüsse

5.4.1 DHS Privacy Leak

Das «US Department of Homeland Security (DHS)» meldete im Januar 2018, Opfer eines internen Datenabflusses geworden zu sein. Dabei waren persönliche Daten von mehr als 240'000 Mitarbeitenden des DHS, insbesondere aus dem Jahre 2014, betroffen. Zusätzlich waren auch Daten von Personen betroffen, die zwischen 2002 und 2014 in eine Untersuchung der DHS Aufsichtsbehörde – «Office of Inspector General» - involviert gewesen waren. Zu den vom Datenabfluss betroffenen gehörten auch Zeugen und Kläger. Gestohlen wurden unter anderem Name, Sozialversicherungsnummer, Wohn- und Mailadresse, Telefonnummer und Geburtstagsdatum.

Der Datenabfluss war in diesem Fall nicht auf einen externen Cyber-Angriff zurückzuführen; es handelte sich vielmehr um einen internen Vorfall. Im Mai 2017 wurde im Rahmen einer laufenden Strafuntersuchung festgestellt, dass ein ehemaliger DHS-Mitarbeiter eine unerlaubte Kopie des Fallmanagement-Systems der Behörde angelegt hatte.

Das DHS informierte seine Mitarbeitenden per Post und stellte eine telefonische Support-Hotline für betroffene Personen zur Verfügung. Ebenfalls offerierte es den Betroffenen einen 18 Monate dauernden Dienst, der sie vor Identitäts- und Kreditmissbrauch schützt. Ferner hat das DHS Sicherheitsmassnamen implementiert, um den Zutritt zu Systemen mit persönlichen Daten einzuschränken.[60]

---

59 https://www.securonix.com/securonix-threat-research-cosmos-bank-swift-atm-us13-5-million-cyber-attack-detection-using-security-analytics/ (Stand: 31. Juli 2018).

60 https://www.dhs.gov/news/2018/01/18/privacy-incident-involving-dhs-oig-case-management-system-update (Stand: 31. Juli 2018).

5.4.2 Datenabfluss bei «Exactis»

Auf eine Datenbank der US-amerikanischen Firma «Exactis» mit persönlichen Angaben von mehreren Millionen Personen konnte über längere Zeit ohne Schutz von aussen zugegriffen werden. «Exactis» ist eine Marketingfirma mit Sitz in Florida, die Daten über die Vorlieben und das Verhalten von Millionen von Personen sammelt. Das genaue Ausmass des Datenabflusses ist unklar. Schätzungsweise waren 200 Millionen Personen- und 110 Millionen Firmendaten betroffen. Unter den Daten befinden sich Geschäftsinformationen, Telefonnummern, Post- und E-Mail-Adressen. Glücklicherweise sollen keine Finanzinformationen, Sozialversicherungsnummern oder andere sensible Daten in der Datenbank gespeichert gewesen sein. Auch wenn nicht erwartet wird, dass betroffene Personen direkt geschädigt werden, könnten die Daten dennoch verwendet werden, um zukünftig gezielte und personalisierte Angriffe gegen sie durchzuführen (siehe Kapitel 6.1).

Speziell an diesem Vorfall ist, dass es sich nicht um einen eigentlichen Hackangriff handelt. Der Sicherheitsforscher Vinny Troia hatte mit dem Suchtool «Shodan» das Internet nach ElasticSearch»-Datenbanken abgesucht.[61] Die Datenbank von «Exactis» erschien dabei in den Resultaten und war weder durch eine Firewall noch durch andere Sicherheitsmassnahmen geschützt und somit für jedermann zugänglich. Ob Troia der erste war, der die Datenbank entdeckte, oder ob die Daten bereits vorher durch andere Akteure entdeckt und kopiert worden sind, ist nicht bekannt. «Exactis» hat nach der Benachrichtigung von Troia die Datenbank gesichert.

5.5 Präventive Massnahmen

5.5.1 Verhaftung von Mitglied im Zusammenhang mit den Carbanak/Cobalt Angriffen

Am 26. März 2018 verhaftete die spanische Polizei zusammen mit Europol und der Polizei weiterer Staaten ein Mitglied der kriminellen Gruppe die hinter den «Carbanak/Cobalt» Angriffen steckt.[62] Diese Splittergruppe machte sich ab 2013 einen Namen mit Angriffen auf Banken und da vor allem mit Manipulationen von Bankomaten, in der Weise, dass diese zu einem bestimmten Zeitpunkt Banknoten ausgaben (MELANI-Halbjahresbericht 2016/I[63]). Die Initialinfektion startete in diesen Fällen jeweils mit manipulierten E-Mails, welche manipulierte Anhänge enthielten. Nachdem die Opfer das Dokument heruntergeladen und ausgeführt hatten, konnten die Bandenmitglieder mittels lateraler Bewegung das restliche Bankennetzwerk infizieren. Die Gruppe wird verdächtigt, weltweit über 100 Finanzinstitute geschädigt und Verluste in Höhe von über einer Milliarde Euro verursacht zu haben.

---

61 http://www.vinnytroia.com/ (Stand: 31. Juli 2018).

62 https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain (Stand: 31. Juli 2018).

63 MELANI Halbjahresbericht 2016/1 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2016-1.html (Stand: 31. Juli 2018).

5.5.2 Cyber Europe 2018 – Vorbereitung auf die nächste Cyber-Krise

Stellen Sie sich folgende Situation vor: Es ist ein normaler Tag am Flughafen. Plötzlich zeigen die Check-in-Automaten einen Systemfehler an. Die Reise-Apps auf den Smartphones funktionieren nicht mehr. Die Mitarbeitenden an den Check-in-Schaltern können ihre Computer nicht mehr verwenden. Die Reisenden können weder ihr Gepäck aufgeben noch die Sicherheitskontrollen passieren. Überall bilden sich lange Schlangen. Auf den Anzeigetafeln werden alle Flüge als gestrichen angezeigt. Aus unbekannten Gründen funktioniert die Gepäckausgabe nicht mehr und über die Hälfte der Flugzeuge muss am Boden bleiben. Berichten zufolge hat eine radikale Gruppierung durch digitale und hybride Angriffe die Steuerung der kritischen Flughafensysteme übernommen. Sie hat sich bereits zu dem Angriff bekannt und nutzt ihre Propagandakanäle, um einen Aktionsaufruf zu verbreiten und mehr Anhänger für ihre radikale Ideologie zu gewinnen.

Diesem extremen Szenario standen am 6. und 7. Juni 2018 über 900 europäische Experten für Netz- und Informationssicherheit aus 30 Ländern bei der diesjährigen Übung «Cyber Europe 2018 (CE2018)» gegenüber, der bisher umfangreichsten EU/EFTA-Übung zur Netz- und Informationssicherheit. «Cyber Europe 2018» wurde von der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) in Zusammenarbeit mit Behörden und Ämtern für Netz- und Informationssicherheit aus ganz Europa organisiert. Auch die Schweiz nahm mit diversen Teilnehmern aus Verwaltung und Privatwirtschaft an dieser Übung teil. Das Hauptziel der Übung bestand darin, Organisationen darin zu unterstützen, ihre internen Notfallpläne zur Aufrechterhaltung des Geschäftsbetriebs und die entsprechenden Krisenmanagementpläne zu testen und gleichzeitig die Zusammenarbeit zwischen öffentlichen und privaten Einrichtungen zu fördern. «Cyber Europe» stärkt diese Zusammenarbeit und ist die Antwort auf grenzüberschreitende Bedrohungen. Sie besteht in einer nahtlosen Zusammenarbeit der europäischen Länder und Organisationen.

Eckwerte der diesjährigen Übung «Cyber Europe 2018»:

- Teilnehmende Länder: 30
  (Österreich, Belgien, Bulgarien, Kroatien, Zypern, Tschechische Republik, Dänemark, Estland, Finnland, Frankreich, Deutschland, Griechenland, Ungarn, Irland, Italien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Polen, Portugal, Rumänien, Slowakei, Slowenien, Spanien, Schweden, Schweiz, Vereinigtes Königreich)
- Teilnehmende Organisationen: 300
- Teilnehmeranzahl: über 900 Experten für Cyber-Sicherheit
- Anzahl der Angriffe: 23'222

«Cyber Europe» wurde vor acht Jahren geschaffen und hat sich zu einer wichtigen Übung zur Netz- und Informationssicherheit entwickelt, bei der Hunderte von Cyber-Sicherheitsexperten aus ganz Europa zusammen arbeiten. Sie ermöglicht eine flexible Lernerfahrung, da die Teilnehmenden die Übung auf die jeweiligen Anforderungen abstimmen können, unabhängig davon, ob es sich um einzelne Analysten oder ganze Organisationen handelt. Die internationale Zusammenarbeit aller teilnehmenden Organisationen gehört zu den Hauptanliegen. Die Schweiz war von Anfang an dabei und ist seit 2010 stolze Teilnehmerin der alle zwei Jahre stattfindenden Übung «Cyber Europe»

5.5.3 Lazarus CC Server-Übernahme

Am 25. April teilte das «ThaiCERT» mit, einen Command- und Control-Server an einer thailändischen Universität entdeckt und übernommen zu haben.[64] Laut ThaiCERT wurde der Server von der Gruppe «Hidden Cobra», die auch unter dem Namen «Lazarus Group» bekannt ist, benutzt. Lazarus wird insbesondere verdächtigt, 2014 gegen Sony Pictures und 2016 gegen die Nationalbank von Bangladesch Angriffe verübt zu haben[65] (MELANI-Halbjahresbericht 2016/I).[66] Sie hatte auf diese Weise 81 Millionen US-Dollar erbeuten können.

Laut McAfee zielte die Operation mit dem Namen «Operation GhostSecret» auf kritische Infrastrukturen in über 17 Ländern, darunter Finanzinstitute, Gesundheitseinrichtungen und Firmen aus der Unterhaltsbranche, eine davon in der Schweiz. Gemäss McAfee ist der Server Teil einer Kampagne, die im Februar 2018 gegen Finanzinstitute in der Türkei startete.[67]

Der Angreifer verfügt über mehrere Schadprogramme. Das US-CERT hat verschiedene Analysen über die Malware veröffentlicht und glaubt, dass diese Aktivitäten nord-koreanischen Angreifern zuzuschreiben sind.[68] Gemäss McAfee befand sich die Kampagne zum Zeitpunkt der Aufdeckung noch im Erkundungsstadium und war auf der Suche nach Informationen über zukünftige Ziele.

6 Tendenzen und Ausblick

6.1 Die Verwendung von Daten bei Angriffen

Wie im letzten MELANI Halbjahresbericht[69] erwähnt, kommt es immer häufiger zu ungewollten Datenabflüssen. Davor bleibt auch die Schweiz nicht verschont, wie die Vorfälle von Swisscom, DVD-Shop und Epsitec zeigen.

Cyber-Kriminelle sind bezüglich Verwendung solcher Daten sehr vielfältig und innovativ. Eine unmittelbare Vorgehensweise, um Datenabflüsse direkt in Geld umzumünzen, ist die direkte Erpressung der Firma, bei der die Daten abgeflossen sind. Dabei spielt es nicht so sehr eine Rolle, wie wertvoll die Daten sind. Der alleinige Umstand, dass Daten bei einer Firma abhandengekommen sind, setzen diese im Zeitalter der Datenschutz-Grundverordnung der Europäischen Union (EU DSGVO / EU GDPR) noch mehr unter Druck. Das bekannteste

---

64 https://www.thaicert.or.th/alerts/admin/2018/al2018ad001.html (Stand: 31. Juli 2018).

65 https://threatpost.com/thaicert-seizes-hidden-cobra-server-linked-to-ghostsecret-sony-attacks/131498/ (Stand: 31. Juli 2018).

66 MELANI Halbjahresbericht 2016/1 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2016-1.html (Stand: 31. Juli 2018).

67 https://securingtomorrow.mcafee.com/mcafee-labs/analyzing-operation-ghostsecret-attack-seeks-to-steal-data-worldwide/ (Stand: 31. Juli 2018).

68 https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity (Stand: 31. Juli 2018).

69 MELANI Halbjahresbericht 2017/2 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2017-2.html (Stand: 31. Juli 2018).

Beispiel in der Schweiz für diese Vorgehensweise ist die Hackergruppe «Rex Mundi». Diese Variante ist aber nur eine von vielen Möglichkeiten für Kriminelle. Generell ist der Trend feststellbar, dass Kriminelle zusehends den Wert von Daten erkennen und auch aus scheinbar wertlosen Datensätzen noch Profit schlagen.[70]

Den Kriminellen hilft dabei, dass die Ressourcen von gestohlenen Datensätzen im Untergrundmarkt schier unerschöpflich sind. Allein das Portal https://haveibeenpwned.com/, auf dem jedermann überprüfen kann, ob seine Zugangsdaten von einem Datendiebstahl betroffen sind, enthält über fünf Milliarden Kombinationen aus Benutzernamen und Passwörtern. Dazu kommt eine Vielzahl von anderen Daten aus Datenabflüssen, Daten aus gehackten E-Mail-Konten oder Computern. So ist im Untergrund ein ganzer Geschäftszweig entstanden, welcher Daten sichtet, wichtige Daten extrahiert und zu neuen Datenbanken zusammenfügt. Diese werden anschliessend an andere Kriminelle weiterverkauft. In Kapitel 4.5 sind diverse Beispiele aufgeführt, wie sich solche Daten verwenden lassen. Dabei lässt sich ein Trend zur Personalisierung bei den verschiedensten Vorgehensweisen feststellen.

Ein eindrückliches Beispiel sind dabei gefälschte «Sextortion»-Angriffe. Dabei wird dem Opfer weisgemacht, dass die Täter über pornographische Aufnahmen des Opfers verfügen. Um diesem Bluff mehr Überzeugungskraft zu verleihen, verwenden die Erpresser persönliche Daten über das Opfer, welche aus einem Datenabfluss stammen (z. B. Vor- und Nachname, IP-Adresse oder verwendeter Provider, Passwörter oder Mobilfunk-Nummern).

Auch die Verbreitung von Schadsoftware wird immer häufiger personalisiert vorgenommen. Manchmal ist es auch möglich, dass ein gestohlener Datensatz direkte Auswirkungen auf die Geschäftstätigkeiten einer Malware-Gruppe hat. Eine Hypothese ist beispielsweise, dass die abgeflossenen Daten der in der Romandie ansässigen Firma «Epsitec» zur Folge hatten, dass nach der Fokussierung der E-Banking Malware «Retefe» auf die Deutschschweiz nun auch Opfer in der Romandie schadhafte E-Mails erhielten.

Eine andere Betrugsart, bei welcher die Datenbasis über das Opfer eine zentrale Rolle spielt, ist der so genannte «CEO-Fraud» oder «President Scam». Der Grossteil der Betrüger sucht momentan noch spezifisch auf der Firmenwebseite oder auf den Social Media-Konten nach Informationen, um ein passendes Szenario auszuarbeiten. Aber auch hier ist davon auszugehen, dass Datenlecks einen immer grösseren Stellenwert erhalten werden. Gerade Informationsabflüsse wie bei der Firma «Exactis», bei welchem ein Drittel der Daten von Firmen stammt, könnten zukünftig für solche Angriffe verwendet werden.

Im Allgemeinen helfen Informationen aus Datenabflüssen Kriminellen, gezieltere Angriffe durchzuführen. Die Personalisierung scheint die Erfolgsrate im Vergleich mit Massen-Spam signifikant zu erhöhen. Es ist deshalb zu erwarten, dass zukünftig viel mehr Kriminelle diese Vorgehensweise wählen werden.

---

[70] MELANI Halbjahresbericht 2015/1 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2015-1.html (Stand: 31. Juli 2018).

6.2 Vernetzte medizinische Geräte, Gesundheitsdaten und Patientendossiers

Die Digitalisierung macht auch vor dem Gesundheitswesen nicht Halt. Unter dem Begriff «eHealth» werden alle elektronischen Gesundheitsdienste zusammengefasst: Mit elektronischen Mitteln werden im Gesundheitswesen die Abläufe verbessert und die Beteiligten vernetzt. Zentrales Element hierbei ist die digitale Gesundheitsakte, das so genannte «Elektronische Patientendossier (EPD)». In diesem sind alle medizinischen Daten einer Person gespeichert. Auf diese Weise sollen die Qualität der medizinischen Behandlung gestärkt, die Behandlungsprozesse verbessert, die Patientensicherheit erhöht und die Effizienz des Gesundheitssystems gesteigert sowie die Gesundheitskompetenz der Patientinnen und Patienten gefördert werden. Über eine sichere Internetverbindung sind die Gesundheitsdaten sowohl für Sie als auch Ihre Gesundheitsfachpersonen jederzeit abrufbar. Sie selbst bestimmen, wer welche Dokumente wann einsehen darf. Jede Bearbeitung des EPD wird protokolliert. Im Zugriffsprotokoll wird namentlich festgehalten, wer zu welchem Zeitpunkt Dokumente abgerufen oder neue Dokumente abgelegt hat. Diese umfassende Protokollierung bildet eine Vertrauenskette, die über mehrere Arbeitsschritte hinweg verlässlich überprüfen kann, dass die Informationen korrekt und unverändert übermittelt wurden.

Vertraulichkeit, Integrität und Verfügbarkeit der Daten sowie die Nachvollziehbarkeit ihrer Bearbeitung sind beim EPD unbedingt sicherzustellen. Gesundheitsdaten sind nicht nur aufgrund ihrer privaten Natur besonders schützenswerte Personendaten, sondern auch weil sie sich nicht verändern können. Daten unseres Körpers und die Krankengeschichte sind gegeben und lassen sich nicht austauschen.

Wenn eine Gesundheitsakte in falsche Hände gerät, sind die Daten (z. B. eine besondere Krankheit, verschriebene Medikamente usw.) bekannt und behalten inhärent Gültigkeit. Dies können sich verschiedene Akteure zu Nutze machen. Neben der naheliegenden Verwendung für sofortige Erpressung von betroffenen Personen können Patientendaten auch auf Vorrat beschafft werden, um sie allenfalls später zu nutzen, da sie sich ja nicht ändern können. Eine Person könnte zu einem späteren Zeitpunkt ein lukrativeres Ziel darstellen – sei dies, weil sie dann in Politik oder Wirtschaft eine führende Position einnimmt oder aus anderen Gründen eher (oder für eine grössere Summe) erpressbar wird. Gesundheitsdaten sind jedoch nicht nur für Kriminelle zwecks direkter Nutzung interessant, sondern können auch an wirtschaftliche und staatliche Akteure verkauft werden. So könnte beispielsweise personalisierte Werbung für Potenzmittel geschaltet oder entsprechende Informationen zur gezielten öffentlichen Denunzierung genutzt werden.

Da auch das bestgesicherte System nicht unfehlbar ist, sollte bei Gesundheitsdaten darauf geachtet werden, dass Daten nicht ohne Weiteres einer konkreten Person zugeordnet werden können. Bei der Pseudonymisierung muss darauf geachtet werden, dass eine angemessene Balance zwischen der Patientensicherheit vor falscher Zuordnung durch berechtigte Gesundheitsfachpersonen und richtiger Zuordnung durch unberechtigte Dritte gefunden wird.

Das EPD wird in der Schweiz in einem dezentralen System umgesetzt. Der dezentrale Ansatz hat Vorteile für die Informationssicherung, denn es gibt nicht einen einzigen Ort, an dem alle EPD-Dokumente der Schweizer Bevölkerung gespeichert sind. So wird ein Klumpenrisiko vermieden. Der geplante Einführungstermin für das EPD ist Frühjahr 2020. Bis dahin werden noch viele Tests durchgeführt, damit die Sicherheit und Vertraulichkeit des Systems bei dessen Einführung gewährleistet werden kann.

6.3 Tempo vor Sicherheit? – Dem Mobilfunk kann auch in Zukunft nicht alles anvertraut werden.

6.3.1 Die bekannten Probleme mit dem SS7 Protokoll bei 2G und 3G

Risiken in Zusammenhang mit der Nutzung öffentlicher WLAN[71]-Netze sind den meisten Anwendern inzwischen ein Begriff. Die Mobilfunknetze hingegen geniessen bei den meisten Besitzern von mobilen Geräten ein grösseres Vertrauen in Sachen Sicherheit. Wie in der Vergangenheit bereits mehrfach berichtet[72,73], gilt es auch in den Mobilfunknetzen gewisse Risiken zu beachten. Speziell, wenn sie als vertrauenswürdiger Zweitkanal, beispielsweise in Form eines SMS-Code bei der Zwei-Faktor Authentisierung, eingesetzt werden. Das technische Einfallstor der Angreifer gegen Mobilfunknetze der 2. und 3. Generation birgt das SS7-Protokoll in sich, das die Koordination zwischen Mobilfunkprovidern, beispielsweise beim Roaming, regelt. Inzwischen bieten dubiose Anbieter[74] im Darknet die Ausnutzung dieser Schwachstellen als Service für andere Kriminelle an. Auch legitime Firmen[75] offerieren darauf basierende Dienste an Sicherheitsbehörden[76]. Durch Einsatz entsprechender Firewall-Technologie auf Seiten der Mobilfunkanbieter kann solcher Missbrauch im eigenen Netz unterbunden werden. Sobald man jedoch in einem Fremdnetz roamt, ist man derartigen Angriffen allenfalls wieder schutzlos ausgeliefert, wenn der auswärtige Anbieter die Schutzmassnahmen nicht implementiert hat.

So liegen die Hoffnungen vor allem auf den modernen Netzen der 4. und speziell der 5. Generation, die Sicherheit für die Mobilfunkkunden zu erhöhen. Noch sind keine Endgeräte mit 5G-Technologie verfügbar, doch die Diskussionen um die Versteigerung der benötigten Frequenzen und Resultate erster Bandbreiten-Tests heizen die Diskussion um die Vorteile der neuesten Mobilfunkgeneration weiter an. Dem 5G-Standard wird zugetraut, durch die hohen Bandbreiten und schnellen Reaktionszeiten Wegbereiter des Internet der Dinge (IoT) sowie Industrie 4.0 (IIoT) zu werden. Erste Pilotversuche[77] zeigen bereits den erfolgreichen Einsatz der Technologie der nächsten Generation.

---

71 https://www.melani.admin.ch/melani/de/home/schuetzen/sekundaere-grundschutz.html (Stand: 31. Juli 2018).

72 MELANI Halbjahresbericht 2017/1, Kapitel 5.4.5, https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2017-1.html (Stand: 31. Juli 2018).

73 MELANI Halbjahresbericht 2/2016, Kapitel 6.2 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2016-2.html (Stand: 31. Juli 2018).

74 https://www.theverge.com/2017/6/13/15794292/ss7-hack-dark-web-tap-phone-texts-cyber-crime (Stand: 31. Juli 2018).

75 https://www.forbes.com/sites/thomasbrewster/2017/09/27/ability-inc-ss7-hackers-fail-to-sell-surveillance/#13d65f0d734c (Stand: 31. Juli 2018).

76 https://www.techrepublic.com/article/ss7-flaws-used-by-surveillance-firms-highlight-need-for-better-vendor-due-diligence/#ftag=RSS56d97e7 (Stand: 31. Juli 2018).

77 https://www.inside-it.ch/articles/50396 (Stand: 31. Juli 2018).

6.3.2 LTE macht einiges besser, aber noch lange nicht perfekt

Aktuell stellt Long Term Evolution (LTE), der Mobilfunkstandard der 4. Generation, den Endgeräten die schnellste und häufig genutzte Verbindungsmöglichkeit zur Verfügung. Statt SS7 setzt LTE auf das «Diameter»-Protokoll. Viele der bekannten Angriffe lassen sich aber infolge ungenügend sicherer Konfiguration und Rückwärtskompatibilität zu den alten Standards mit etwas mehr Aufwand weiter durchführen. Dr. Silke Holtmanns von «Nokia Bell Labs» präsentierte am «34. Chaos Computer Kongress» ihre Erkenntnisse[78] dazu. Wie bereits bei Angriffen gegen die älteren Standards, gibt es durchaus mögliche Massnahmen[79], die Lücken seitens der Mobilfunkbetreiber zu schliessen, was aber nicht von allen mit der gleichen Konsequenz umgesetzt wird.

Im letzten Halbjahr wurden zusätzliche Angriffsvarianten[80] gegen LTE bekannt. Durch sogenannte «Authentication Relay»-Attacken konnten Sicherheitsforscher der «Purdue University» und der Universität von Iowa Textnachrichten abfangen oder Standortdaten von Nutzern bei allen grossen US-Netzbetreibern auslesen. Mithilfe von Gerätschaften mit Anschaffungskosten von unter 4'000 US Dollar könnten auf diese Weise sogar gefälschte Katastrophenwarnungen an sämtliche Netzteilnehmer einer Region versandt werden.

Mit etwas mehr Aufwand konnte ein Forschungsteam der Ruhr-Universität Bochum und der New York Universität Abu Dhabi drei neue Angriffsszenarien[81] auf LTE-Netze aufzeigen. Die zwei passiven Varianten erlauben es, Nutzende im Netzwerk zu identifizieren und nachzuvollziehen, welche Webseiten sie besucht haben. Die aktive Variante nutzt eine Schwäche der eingesetzten Verschlüsselungsmethode, um durch manipulierte DNS-Antworten Netzwerkteilnehmer auf gefälschte Webseiten umzuleiten. Auch in diesem Fall reagierten Netzwerkausrüster und zeigten[82], wie sich solche Angriffe abwenden lassen.

6.3.3 Schliesst 5G endlich die Lücken?

Neben den vielgelobten Fortschritten in der Datenübertragung, verspricht die fünfte Generation des Mobilfunkstandards auch eine erhöhte Sicherheit für die Betreiber und Teilnehmer des Netzes. Verbesserungen sind zwar vorgesehen, es werden aber leider auch einige Unzulänglichkeiten aus den Vorgängerstandards übernommen. So findet die «Evolved Packet Core»-Architektur (EPC) auch Eingang in den neuen Standard. EPC führt Sprach- und Datenströme im Netzwerk zusammen. Das Fehlen eingebauter

78 https://www.heise.de/newsticker/meldung/34C3-Auch-4G-Mobilfunk-ist-einfach-abzuhoeren-und-zu-ueberwachen-3928496.html (Stand: 31. Juli 2018).

79 https://researchcenter.paloaltonetworks.com/2018/02/sp-prevent-bad-signals-harming-network-availability/, (Stand: 31. Juli 2018).

80 https://www.zdnet.com/article/new-lte-attacks-eavesdrop-on-messages-track-locations-spoof-alerts/ (Stand: 31. Juli 2018).

81 https://alter-attack.net/media/breaking_lte_on_layer_two.pdf (Stand: 31. Juli 2018).

82 https://blogs.cisco.com/security/protecting-against-the-latest-lte-network-attacks (Stand: 31. Juli 2018).

Verschlüsselungsmechanismen im darin enthaltenen GTPv2-Protokoll erlaubt die Überwachung mobiler Datenströme und ermöglicht DoS-Angriffe auf Netzkomponenten[83].

Als Rückfallebene bei 5G kommen auch Telekommunikationssatelliten zum Einsatz. Was hinsichtlich der Resilienz des Netzwerkes bei Ausfällen am Boden zu begrüssen ist, öffnet neue Angriffsvektoren[84] auf die Mobilfunkkommunikation. Sind Satelliten Teil des Einsatzszenarios, sollten die zugehörigen Risiken in den Sicherheitsüberlegungen berücksichtigt werden.

Auch der neueste Standard wird nicht alle Sicherheitsrisiken der Telekommunikation beseitigen können. Eine grosse Verantwortung bleibt bei den Mobilfunkbetreibern, die zu entscheiden haben, welche Priorität sie der Sicherheit in der Umsetzung des Standards einräumen. Die Hilfsmittel wie die Modellierung der Bedrohung[85] des eigenen Netzes wie auch Erfahrungen aus der klassischen IKT-Netzwerksicherheit stehen bereit, deren Einsatz ist aber mit Aufwand verbunden, den die Betreiber zu investieren gewillt sein müssen.

6.3.4 Netzwerksicherheit alleine schützt nicht

Auch bei der neuesten Mobilfunkgeneration können Anwender also nicht davon ausgehen, dass der Standard oder der Betreiber die Risiken der Informationssicherheit beseitigt. Auch beim Mobilfunk gilt es, die risikoadäquaten Schutzmassnahmen der eigenen Infrastruktur und Applikationen umzusetzen.

Die Vergangenheit hat gezeigt: Angreifer gehen nicht nur den Weg über das Netzwerk, sondern versuchen ihr Glück auch über die Geschäftsprozesse und die daran beteiligten Mitarbeiter. Häufig sind Mehrfaktor-Authentisierung oder Passwort-Rücksetzungsprozesse an die Mobilnummer des Kontoinhabers geknüpft. So haben es Angreifer bereits mehrfach erfolgreich durch Anrufe beim Kundendienst des Mobilfunkbetreibers geschafft[86], sich die Nummer auf ein eigenes Gerät portieren, oder sich Ersatz-SIM-Karten zuschicken zu lassen.

Eine eher unerwartete Herausforderung an die Netzwerkverfügbarkeit bereitete den europäischen Mobilfunkbetreibern die Regeländerung der EU zu Roaming-Tarifen in den Mitgliedsstaaten. Die Nutzer konnten durch die Anpassung auch im europäischen Ausland von den gleichen Konditionen profitieren wie im Heimnetz. Das veranlasste die Reisenden, nicht mehr nach WLANs zu suchen, sondern auch unterwegs das Mobilnetz zur Datenübertragung zu nutzen, was einen Anstieg um das sechs- bis achtfache des Roaming-Datenverkehrs mit sich brachte[87]. Dieser plötzliche Anstieg brachte einige der Anbieter in Feriendestinationen an ihre Kapazitätsgrenzen.

---

83 https://www.darkreading.com/perimeter/new-4g-5g-network-flaw-worrisome-/d/d-id/1330062 (Stand: 31. Juli 2018).

84 https://blog.trendmicro.com/trendlabs-security-intelligence/attack-vectors-in-orbit-need-for-satellite-security-in-5g-iot/ (Stand: 31. Juli 2018).

85 https://www.nccgroup.trust/us/about-us/newsroom-and-events/blog/2018/march/tackling-5g-security-with-threat-modelling/ (Stand: 31. Juli 2018).

86 https://krebsonsecurity.com/2018/02/how-to-fight-mobile-number-port-out-scams/ (Stand: 31. Juli 2018).

87 https://www.lightreading.com/regulation/roam-like-at-home-the-impact-after-one-year/a/d-id/744836 (Stand: 31. Juli 2018).

7 Politik, Forschung, Policy

7.1 CH: Parlamentarische Vorstösse

Geschäft	Nummer	Titel	Eingereicht von	Datum	Rat	Amt	Stand Beratung & Link
Po	18.3003	Eine klare Cyber-Gesamtstrategie für den Bund	Sicherheitspolitische Kommission	22.01.2018	NR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183003
Mo	18.3249	Zentrale Stelle für den Kampf gegen Cyberstalking	Marchand-Balet Géraldine	15.03.2018	NR	EJPD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183249
Ip	18.3335	Wie reguliert das Völkerrecht den Cyberraum?	Dobler Marcel	16.03.2018	NR	EDA	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183335
Ip	18.3511	Nutzen der strategischen Vorteile der Schweiz bei der Entwicklung eines sicheren digitalen Hardware-Markts	Vonlanthen Beat	13.06.2018	SR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183511
Pl	18.434	Cyber-Grooming mit Minderjährigen endlich unter Strafe stellen	Amherd Viola	14.06.2018	NR	Parlament	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20180434
Ip	18.3556	Cyberrisiken durch die Sensibilisierung der Bevölkerung und der Wirtschaft minimieren	Glanzmann-Hunkeler Ida	14.06.2018	NR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183556
Ip	18.3562	Cyberkriminalität. MELANI-Meldepflicht	CVP-Fraktion	14.06.2018	NR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183562
Po	18.3565	Schadensdeckung. Ereignislimite bei Cyberangriffen	CVP-Fraktion	14.06.2018	NR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183565
Mo	18.3006	Den Kollagps der Mobilfunknetze verhindern und den Anschluss an die Digitalisierung sicherstellen	Kommission für Verkehr und Fernmeldewesen	29.01.2018	SR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183006
Ip	18.3013	Amazon und andere Online-Händler. Beachtet die Post den Grundsatz der Gleichbehandlung?	Feller Olivier	26.02.2018	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183013
Fr	18.5111	WLAN in Bundesasylzentren?	Keller Peter	28.02.2018	NR	EJPD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185111
Pl	18.407	Netzneutralität in der Verfassung verankern	Reynard Mathias	01.03.2018	NR	Parlament	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20180407
Ip	18.3057	Zerstörung der direkten Demokratie durch E-Voting	Zanetti Claudio	01.03.2018	NR	BK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183057
Mo	18.3062	Stärkung der Volksrechte. Unterschriftensammlung für Initiativen und Referenden im Internet	Grüter Franz	05.03.2018	NR	BK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183062

Ip	18.3197	Gesetzliche Vertretung von Dienstleistern in der Schweiz	Marchand-Balet Géraldine	14.03.2018	NR	EJPD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183197
Ip	18.3222	Marktverzerrung zulasten der Schweiz	Amherd Viola	15.03.2018	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183222
Mo	18.3306	Rechtsdurchsetzung im Internet stärken durch ein obligatorisches Zustellungsdomizil für grosse kommerzielle Internetplattformen	Glättli Balthasar	15.03.2018	NR	EJPD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183306
Mo	18.3349	Gewährleistung der Netzneutralität	Flach Beat	16.01.2018	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183349
Ip	18.3367	Wissenschaften. Ein Trumpf der Schweiz in den internationalen Beziehungen	Béglé Claude	16.03.2018	NR	EDA	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183367
Mo	18.3379	Zugriff der Strafverfolgungsbehörden auf Daten im Ausland	Kommission für Rechtsfragen	23.03.2018	SR	EJPD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183379
Fr	18.5258	Wann wird die Internet-Mindestgeschwindigkeit auf 10 Megabit pro Sekunde erhöht?	Candinas Martin	30.05.2018	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185258
GBr	18.049	Bundesgesetz über elektronische Identifizierungsdienste	Botschaft des Bundesrates	01.06.2018		EJPD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20180049
Ip	18.3443	Kurse für ältere Menschen zum Umgang mit neuen Technologien anbieten	Marchand-Balet Géraldine	04.06.2018	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183443
Ip	18.3448	Fake News und die Schweizer Demokratie	Marchand-Balet Géraldine	04.06.2018	NR	BK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183448
Fr	18.5321	SBB. Kostenloser Internetzugang	Derder Fathi	04.06.2018	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185321
Mo	18.3507	Umsetzung des Büpf gemäss Abstimmungsdispositiv	Molina Fabian	13.06.2018	NR	EJPD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183507
Po	18.3590	Web 3.0 - Welche Rolle soll die Schweiz in einem dezentralisierten Netz spielen?	Béglé Claude	14.06.2018	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183590
Ip	18.3591	Webseite ch.ch - wie steht es um die Nutzung, und wie soll es damit weitergehen?	Wehrli Laurent	14.06.2018	NR	BK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183591
Mo	18.3617	Schaffung einer digitalen Identität 3.0. Für eine führende Rolle der Schweiz im Blockchain-Bereich und maximale Sicherheit von Personendaten	Béglé Claude	14.06.2018	NR	EJPD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183617
Ip	18.3670	WLAN-Verbindungen in SBB-Zügen	Ammann Thomas	15.06.2018	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183670

Mo	18.3701	Freiwillige digitale Vignette	Candinas Martin	15.06.2018	NR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183701
Mo	18.3702	Smart Data. Die Schweiz soll bei der nachhaltigen Digitalisierung mit hoher Wertschöpfung eine führende Rolle spielen	Béglé Claude	15.06.2018	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183702
Fr	18.1044	Drohnen	Leutenegger Oberholzer Susanne	15.06.2018	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20181044
Po	18.3601	Die Gesetzgebung für Drohnen muss angepasst werden	Marchand-Balet Géraldine	14.06.2018	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183601
Po	18.3478	Bericht des Bundesrates über die Massnahmen, die es im Bereich der Drohnen zu ergreifen gilt	Brélaz Daniel	11.06.2018	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183478
Ip	18.3397	Regelung für den Privatgebrauch von Drohnen	Jositsch Daniel	28.05.2018	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183397
Fr	18.5399	Drohnen in der Schweiz	Leutenegger Oberholzer Susanne	06.06.2018	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185399
Mo	18.3371	Sicherheit und Ordnung beim Betrieb von Drohnen	Candinas Martin	16.03.2018	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183371
Po	18.3245	Identifikation von Drohnen und ähnlichen Flugkörpern	Guhl Bernhard	15.03.2018	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183245
Ip	18.3463	Von Smart Cities zu Smart Vilages	Egger Thomas	07.06.2018	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183463
Ip	18.3445	Automatisierte Fahrzeuge und Haftung. Wann wird die Gesetzgebung in der Schweiz angepasst?	Marchand-Balet Géraldine	04.06.2018	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183445
Fr	18.5220	Wird der Internetgigant Amazon in Bezug auf die Zustellpreise für Pakete gleich behandelt wie die anderen Kundinnen und Kunden der Post?	Feller Olivier	28.05.2018	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185220
Fr	18.1021	Warum gewichtet der Bund als Eigner der Swisscom eine umfassende, kundennahe Datenschutzpolitik nicht höher?	Glättli Balthasar	16.03.2018	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20181021
Fr	18.5209	5G-Netz in der Schweiz. Der Bundesrat kann den Ausbau auf dem Verordnungsweg ermöglichen	Derder Fathi	07.03.2018	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185209
Fr	18.5167	5G-Netz ohne höhere Grenzwerte beim Mobilfunk	Leutenegger Oberholzer Susanne	07.03.2018	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185167
Ip	18.3044	Partnerschaft zwischen der Post und Amazon	Reynard Mathias	28.02.2018	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183044

Ip	18.3575	Von Kinderarbeit freie IT-Geräte in der Bundesverwaltung	Masshardt Nadine	14.06.2018	NR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183575
Ip	18.3374	Neue BIT-Lösung für die Krebs-Registrierungssoftware. Wird durch eine fragwürdige Vergabe Geld verschwendet?	Weibel Thomas	16.03.2018	NR	EDI	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183374
Mo	18.3219	Weiterbildungsoffensive im Bereich der Digitalisierung für ältere Arbeitnehmende	Kälin Irène	15.03.2018	NR	WBF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183219
Mo	18.3008	Bundesverwaltungsinterne Dokumente standardmässig digital signieren	Dobler Marcel	26.02.2018	NR	BK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183008
Mo	18.3517	Impulsprogramm Digitalisierung an den Schulen	CVP-Fraktion	13.06.2018	NR	WBF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183517
Mo	18.3664	Digitalisierung auch im Gesundheitswesen. Sämtliche Rechnungen sollen elektronisch zu den Krankenversicherern	Grossen Jürg	15.06.2018	NR	EDI	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183664
Mo	18.365o	Erhöhung der Patientensicherheit mit elektronischer Dokumentation und elektronischem Austausch von medizinischen Daten	Humbel Ruth	15.06.2018	NR	EDI	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183650
Po	18.3502	E-Signatur für verwaltungsinterne Dokumente	Dobler Marcel	12.06.2018	NR	BK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183502

7.2 Poltische Entwicklungen im Cyber-Bereich – Aktueller Stand

Mit den Motionen Eder (SR FDP-17.3508)[88], Dittli (SR FDP-17.3507)[89] und Grüter (NR SVP-17.3199)[90] wurden letztes Jahr vom Parlament drei weitreichende Geschäfte im Bereich Cyber beantragt. Inzwischen wurde die Motion Eder von beiden Räten mit grosser Mehrheit angenommen, die Motion Dittli mit geringen Anpassungen ebenfalls von beiden Räten angenommen und die Motion Grüter mit 134 gegen 47 Stimmen bei 9 Enthaltungen im Nationalrat angenommen, jedoch im Ständerat unlängst verworfen. Somit wurde der Bundesrat mit der Schaffung eines Cybersecurity-Kompetenzzentrums sowie dem Aufbau einer Cyber-Truppe mit 100 IT-/Cyber-Spezialisten in der Schweizer Armee beauftragt. Während die erste Cyber-Rekrutenschule im August 2018 gestartet ist, braucht die Umsetzung der Aufträge im zivilen Bereich mehr Zeit.

88 https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173508 (Stand: 31. Juli 2018).

89 https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173507 (Stand: 31. Juli 2018).

90 https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173199 (Stand: 31. Juli 2018).

Mit der erneuerten «Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS II) für die Jahre 2018-2022[91] will der Bundesrat den Cyber-Risiken aktiv entgegentreten und die nötigen Massnahmen ergreifen, um die Sicherheit des Landes vor Bedrohungen aus dem Cyber-Raum zu wahren. Die NCS II wurde entsprechend vom Bundesrat am 18. April 2018 verabschiedet. Die Umsetzung und Zuteilung der Massnahmen der NCS II erfolgt gemeinsam mit den Kantonen, der Wirtschaft und den Hochschulen. Der zusätzliche Auftrag zur Schaffung eines Cybersecurity-Kompetenzzentrums soll denn ebenfalls im Rahmen der Umsetzung der NCS II eingeplant und vorangetrieben werden.

Vor der Sommerpause fällte der Bundesrat mit Hinblick auf den Aufbau des Cybersecurity-Kompetenzzentrums erste Grundsatzentscheide, um seine Anstrengungen bei der Prävention und der Bekämpfung von Cyber-Risiken zu intensivieren. Gemäss den ersten Grundsatzentscheiden soll das Kompetenzzentrum im Eidgenössischen Finanzdepartement (EFD) angegliedert werden und im Kampf gegen Cyber-Risiken die bundesinterne Koordination übernehmen, die Prävention fördern und als zentrale Ansprechstelle für die Anliegen der Wirtschaft und der Kantone dienen. Gleichzeitig soll die die Zusammenarbeit mit der Forschung und Wissenschaft gefördert werden. Das Kompetenzzentrum soll schliesslich von einem hochrangig angesiedelten «Mr./Mrs. Cyber» geleitet werden, jedoch ohne die in der Mo Eder geforderten Weisungsbefugnis. Der Grad der Zentralisierung sämtlicher Cyber-Stellen in einem Zentrum ist indes zu diesem Zeitpunkt noch unklar.

Der Entscheid, einen hochrangig angesiedelten Mr./Mrs. Cyber mit koordinativer Funktion, jedoch ohne Weisungsbefugnis auszustatten, wurde weitreichend kritisiert und der Bundesrat in einem offenen Brief seitens der Wirtschaftsverbände[92] und in einem offenen Brief der Sicherheitspolitischen Kommission des Nationalrates[93] aufgefordert, die Funktion des Mr./Mrs. Cyber mit Weisungsbefugnissen auszustatten. Schliesslich fordert die Sicherheitspolitische Kommission des Nationalrates für die Übergangszeit als Sofortmassnahme rasch personelle und finanzielle Ressourcen, u. a. zum Ausbau der Melde- und Analysestelle Informationssicherung (MELANI) sowie zur Verbesserung der Cyber-Resilienz von kritischen Infrastrukturen.

Definitive Entscheidungen des Bundesrates zur Schaffung des Kompetenzzentrums sind frühestens Ende 2018 zu erwarten[94].

7.3 GDPR und Datenschutzgesetz

Am 25. Mai 2018 ist die neue Datenschutz-Grundverordnung der Europäischen Union (EU DSGVO / EU GDPR) in Kraft getreten. Seit diesem Zeitpunkt sind die wichtigsten Änderungen wie das Recht auf Vergessen werden, Datenverarbeitung ausschliesslich nach ausdrücklicher Einwilligung der betroffenen Person, das Recht auf Datenübertragbarkeit an einen anderen Dienstleister, das Recht der Betroffenen, bei Verletzungen des Schutzes der eigenen Daten darüber informiert zu werden, sowie die Androhung von Geldbussen bei Zuwiderhandlung von bis zu 4% des weltweiten Jahresumsatzes des vorjährigen Geschäftsjahres, durchsetzbar.

---

91 https://www.isb.admin.ch/isb/de/home/themen/cyber_risiken_ncs/ncs_strategie.html (Stand: 31. Juli 2018).

92 https://www.satw.ch/cybersecurity/detail/publication/zu-den-grundsatzentscheiden-des-bundesrates-zur-cybersecurity/ (Stand: 31. Juli 2018).

93 https://www.parlament.ch/press-releases/Pages/mm-sik-n-2018-08-21.aspx (Stand: 31. Juli 2018).

94 https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-71458.html (Stand: 31. Juli 2018).

Allerdings besteht nach wie vor Unklarheit über die rechtskonforme Umsetzung der DSGVO / GDPR im Einzelfall. Obwohl die im Vorfeld befürchteten Abmahnwellen bei den Unternehmen im EU Raum ausblieben, war es für viele Firmen eine Herausforderung, die Verordnung konkret umzusetzen, da nicht zuletzt auch keine gängige Praxis dazu besteht. So gingen denn nicht wenige europäische Internetauftritte nach Inkrafttreten der DSGVO offline, aber auch amerikanische Zeitungen waren vorübergehend für europäische Kunden nicht mehr erreichbar. Besonders verunsichert fühlten sich kleinere Unternehmen, Vereine und Selbständigerwerbende sowie kleinere Unternehmen aus dem digitalen Sektor wie Online-Shops und Blogger. Viele sahen sich aus finanziellen und organisatorischen Gründen nicht im Stande, die Anforderungen der DSGVO zu erfüllen und fürchteten aufgrund der angedrohten Bussgelder um ihre Existenz, so dass die Webpräsenzen erstmal eingeschränkt oder abgestellt wurden.

Empfehlung:

Die Europäische DSGVO gilt grundsätzlich in der Schweiz nicht. In welchen Fällen Schweizer Unternehmen jedoch von der direkten Anwendung der DSGVO betroffen sind, kann überprüft werden unter:

INFO

https://www.edoeb.admin.ch/edoeb/de/home/aktuell/rgpd-last-minute.html

https://www.kmu.admin.ch/kmu/de/home/praktisches-wissen/kmu-betreiben/e-commerce/eu-regelung-zum-datenschutz.html

https://www.economiesuisse.ch/de/datenschutz-online-check

Die Schweiz richtet sich nach wie vor nach dem bestehenden Datenschutzgesetz aus dem Jahr 1993. Die Totalrevision des Datenschutzgesetzes wurde vom Parlament noch nicht an die Hand genommen. Vorgezogen werden dringende Anpassungen, die im Rahmen des Schengen Abkommens notwendig werden. Für die Totalrevision will sich das Parlament jedoch mehr Zeit geben. Daraus ergibt sich zwangsläufig eine Übergangsphase, welche nicht unproblematisch ist für die Schweizer Wirtschaft und die Schweizer Online-Welt. Diese muss sich auf das neue Recht einstellen und bedarf entsprechender Rechtssicherheit. Bis jedoch der zweite Teil mit der Totalrevision des Datenschutzgesetzes abgeschlossen ist, wird der juristische Rahmen relativ unübersichtlich sein.

8 Publizierte MELANI Produkte

8.1 GovCERT.ch Blog

Im ersten Halbjahr 2018 hat MELANI keine neuen GovCERT.ch Blogs publiziert.

8.2 MELANI Newsletter

8.2.1 Datenabflüsse, Crimeware und Angriffe auf industrielle Kontrollsysteme - Themen im MELANI-Halbjahresbericht

26.04.18 - Der am 26. April 2018 veröffentlichte 26. Halbjahresbericht der Melde- und Analysestelle Informationssicherung (MELANI) befasst sich mit den wichtigsten Cyber-Vorfällen der zweiten Jahreshälfte 2017 im In- und Ausland. Im Fokus stehen unter anderem der verbreitete Einsatz von Crimeware sowie Angriffe auf industrielle Kontrollsysteme im medizintechnischen Bereich. Die Häufung von Datenabflüssen und deren Auswirkungen werden im Schwerpunktthema beleuchtet.

https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/halbjahresbericht-2-2017.html

8.2.2 Wieder vermehrt betrügerische Anrufe bei Firmen

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

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

8.3 Checklisten und Anleitungen

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

9 Glossar

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

	einem Computer, und enthält die logischen Schaltungen um ein Computer-Programm auszuführen.
Cryptomining	Durch das Mining werden neue Blöcke erzeugt und anschließend zur Blockchain hinzugefügt. Der Vorgang ist sehr rechenintensiv und wird deshalb vergütet.
DDoS	Distributed-Denial-of-Service-Attacke. Mit einer DoS-Attacke wird der Dienst oder das System des Opfers von vielen verscheiden Systemen aus gleichzeitig angegriffen, so dass dieses zum Erliegen kommt und nicht mehr verfügbar ist.
Defacement	Verunstaltung von Webseiten.
Domain Name System	Domain Name System. Mit Hilfe von DNS lassen sich das Internet und deren Dienste benutzerfreundlich nutzen, da die Benutzer anstelle von IP-Adressen Namen verwenden können (z. B. www.melani.admin.ch).
Downloader	Ein Downloader ist ein Programm, das eine oder mehrere Instanzen von Schadsoftware herunterlädt und installiert.
Elastic Search	Elasticsearch ist eine in Java geschriebene Suchmaschine auf Basis von Apache Lucene.
Exploit-Kit	Baukasten, mit welchen Kriminelle Programme, Scripts oder Code-Zeilen generieren können, womit sich Schwachstellen in Computersystemen ausnutzen lassen.
Fernzugriffstool	Die Fernwartungs-Software (englisch: Remote Administration Tool) stellt eine Anwendung des Konzeptes Fernwartung für beliebige Rechner oder Rechnersysteme dar.
Finanzagent	Ein Finanzagent ist jemand, der sich als legaler Geldvermittler und damit auch im Finanz-Transfergeschäft betätigt. In jüngerer Zeit wird dieser Begriff in Zusammenhang mit illegalen Finanz-Transaktionen gebraucht.
Global Positioning System (GPS)	Global Positioning System (GPS), offiziell NAVSTAR GPS, ist ein globales Navigationssatellitensystem zur Positionsbestimmung und Zeitmessung.
Internet der Dinge	Der Begriff Internet der Dinge (Internet of things IoT) beschreibt die Vernetzung und das Zusammenarbeiten von physischen und virtuellen Gegenständen.

Javascript	Eine objektbasierte Scripting-Sprache zur Entwicklung von Applikationen. JavaScripts sind im HTML-Code integrierte Programmteile, die bestimmte Funktionen im Internet-Browser ermöglichen. Ein Beispiel kann das Kontrollieren von Benutzereingaben bei einem Webformular sein. So kann überprüft werden, ob alle eingegebenen Zeichen bei geforderter Angabe einer Telefonnummer auch wirklich Zahlen sind. Wie ActiveX Controls werden JavaScripts auf dem Rechner des Webseitenbesuchers ausgeführt. Neben nützlichen, lassen sich leider auch schädliche Funktionen programmieren. Im Gegensatz zu ActiveX werden JavaScripts von allen Browsern unterstützt.
Kontroll- oder Steuerungssysteme (IKS)	Kontroll- oder Steuerungssysteme (IKS) bestehen aus einem oder mehreren Geräten, welche das Verhalten von anderen Geräten oder Systemen steuern, regeln und/oder überwachen. In der industriellen Produktion ist der Begriff «Industrielle Kontrollsysteme» (engl. Industrial Control Systems, ICS) geläufig.
LTE	Long Term Evolution (kurz LTE, auch 3.9G) ist eine Bezeichnung für den Mobilfunkstandard der dritten Generation. Eine Erweiterung heisst LTE-Advanced bzw. 4G und ist abwärtskompatibel
Malware	Oberbegriff für Software, die schädliche Funktionen auf einem Rechner ausführt (wie beispielsweise Viren, Würmer, Trojanische Pferde).
Man-in-the-Middle Attacke	Attacke, bei der sich der Angreifer unbemerkt in den Kommunikationskanal zweier Partner hängt und dadurch deren Datenaustausch mitlesen oder verändern kann.
Metadaten	Metadaten oder Metainformationen sind Daten, die Informationen über andere Daten enthalten
mobileTAN	Mobile TAN besteht aus der Einbindung des Übertragungskanals SMS. Dabei wird dem Onlinebanking-Kunden nach Übersendung der ausgefüllten Überweisung im Internet seitens der Bank per SMS eine nur für diesen Vorgang verwendbare TAN auf sein Mobiltelefon gesendet.
MS HTA	HTML-Applikation (kurz: HTA) ist ein Begriff von Microsoft für Computerprogramme, die den Internet Explorer zur Ausführung nutzen.
NAS Geräte	Network Attached Storage (NAS) bezeichnet einfach zu verwaltende Dateiserver. Allgemein wird ein NAS

	eingesetzt, um ohne hohen Aufwand unabhängige Speicherkapazität in einem Rechnernetz bereitzustellen.
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.
Port	Ein Port ist ein Teil einer Adresse, der Datensegmente einem Netzwerkprotokoll zuordnet. Dieses Konzept ist beispielsweise in TCP, UDP und SCTP vorgesehen, um Protokolle auf den höheren Schichten des OSI-Modells zu adressieren.
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.
Public Key Infrastructure Infrastruktur	Public Key Infrastructure Infrastruktur zur Verwaltung und zum Einsatz von digitalen Zertifikaten.
RC4-Verschlüsselung	RC4 (Ron’s Code 4) wurde 1987 von Ronald L. Rivest entwickelt, ist eine Marke von RSA Security und ist offiziell geheim (Security by Obscurity).
Router	Geräte aus dem Bereich Computernetzwerke, Telekommunikation oder auch Internet, die mehrere Rechnernetze koppeln oder trennen. Router werden beispielsweise in Heimnetzwerken eingesetzt und

	machen die Verbindung zwischen internem Netz und dem Intranet.
Schadsoftware	Oberbegriff für Software, die schädliche Funktionen auf einem Rechner ausführt (wie beispielsweise Viren, Würmer, Trojanische Pferde).
Schwachstelle / Lücke	Schwachstelle in Hard- oder Software, über die Angreifer Zugriff auf ein System erlangen können.
Smartphone	Ein Smartphone ist ein Mobiltelefon, das mehr Computerfunktionalität und -konnektivität als ein herkömmliches fortschrittliches Mobiltelefon zur Verfügung stellt.
SMB-Protokoll	Server Message Block (SMB) ist ein Netzwerkprotokoll für Datei-, Druck- und andere Serverdienste in Rechnernetzen.
SMS	Short Message Service ist ein Dienst zum Versenden von Kurzmitteilungen (maximal 160 Zeichen) an Mobiltelefonbenutzer.
Social Engineering	Social-Engineering-Angriffe nutzen die Hilfsbereitschaft, Gutgläubigkeit oder die Unsicherheit von Personen aus, um beispielsweise an vertrauliche Daten zu gelangen, oder die Opfer zu bestimmten Handlungen zu bewegen. Eine bekannte Form von Social Engineering ist Phishing.
Spam	Unaufgefordert und automatisiert zugesandte Massenwerbung, worunter auch Spam-E-Mails fallen. Als Spammer bezeichnet man den Absender dieser Mitteilungen, während das Versenden selbst als Spamming bezeichnet wird.
Spear-Phishing	Gezielte Phishing-Attacke. Dem Opfer wird zum Beispiel vorgegaukelt, mit einer ihr vertrauten Person via E-Mail zu kommunizieren.
SS7	Das Signalling System #7 (SS7) ist eine Sammlung von Protokollen und Verfahren für die Signalisierung in Telekommunikationsnetzen. Es kommt im öffentlichen Telefonnetz, in Zusammenhang mit ISDN, Fest- und Mobilfunknetz und seit etwa 2000 auch verstärkt in VoIP-Netzen zum Einsatz.
SSH	Secure Shell Protokoll, mit dem dank Datenverschlüsselung u. a. das sichere Anmelden

	(Login) an einem über ein Netzwerk (z. B. Internet) zugänglichen Computersystem möglich ist.
Supply Chain-Angriffe	Angriff bei dem versucht wird über die Infektion einer Firma in der Lieferkette das eigentliche Ziel zu infizieren.
Take-Down	Ausdruck, der verwendet wird, wenn ein Provider eine Website aufgrund betrügerischen Inhalts vom Netz nimmt.
Top-Level-Domains	Jeder Name einer Domain im Internet besteht aus einer Folge von durch Punkte getrennten Zeichenfolgen. Die Bezeichnung Top-Level-Domain bezeichnet dabei den letzten Namen dieser Folge und stellt die höchste Ebene der Namensauflösung dar. Ist der vollständige Domain-Name eines Rechners bzw. einer Website beispielsweise de.example.com, so entspricht das rechte Glied (com) der Top-Level-Domain dieses Namens.
Transmission Control Protocol / Internet Protocol (TCP/IP)	Transmission Control Protocol / Internet Protocol (TCP/IP) ist eine Familie von Netzwerkprotokollen und wird wegen ihrer großen Bedeutung für das Internet auch als Internetprotokollfamilie bezeichnet.
UDP	Das User Datagram Protocol, kurz UDP, ist ein minimales, verbindungsloses Netzwerkprotokoll, das zur Transportschicht der Internetprotokollfamilie gehört.
USB	Universal Serial Bus. Serielle Kommunikationsschnittstelle, welche den Anschluss von Peripheriegeräten wie Tastatur, Maus, externe Datenträger, Drucker usw. erlaubt. Der Rechner muss beim Ein- beziehungsweise Ausstecken eines USB-Gerätes nicht heruntergefahren werden. Die neuen Geräte werden meist (allerdings abhängig vom Betriebssystem) automatisch erkannt und konfiguriert.
Watering-Hole-Angriffe	Gezielte Infektion durch Schadsoftware über Webseiten, welche bevorzugt nur von einer spezifischen Benutzergruppe besucht werden.
Webseiteninfektion	Infektion eines Computers mit Malware allein durch den Besuch einer Web-Seite. Vielfach beinhalten die betroffenen Web-Seiten seriöse Angebote und sind zwecks Verteilung der Malware zuvor kompromittiert worden. Die Infektion erfolgt meistens durch das Ausprobieren von Exploits für vom Besucher noch nicht geschlossene Sicherheitslücken.

WLAN	WLAN (Wireless Local Area Network) steht für drahtloses lokales Netzwerk.
Wurm	Im Gegensatz zu Viren benötigen Würmer zur Verbreitung kein Wirtprogramm. Vielmehr nutzen sie Sicherheitslücken oder Konfigurationsfehler in Betriebssystemen bzw. Anwendungen, um sich selbständig von Rechner zu Rechner auszubreiten.
ZeroDay-Lücken	Sicherheitslücke, für welche noch kein Patch existiert.
ZIP-Datei	ZIP ist ein Algorithmus und Dateiformat zur Datenkompression, um den Speicherbedarf von Dateien für die Archivierung und Übertragung zu verringern.
Zweifaktorauthentifizierung	Um die Sicherheit zu erhöhen wird die Zweifaktorauthentifizierung verwendet. Dafür sind mindestens zwei der drei Authentifikationsfaktoren notwendig: 1. Etwas, das man weiss (z. B. Passwort, PIN, usw.) 2. Etwas, das man besitzt (z. B. Zertifikat, Token, Streichliste, usw.) 3. Ein einmaliges Körpermerkmal (z. B. Fingerabdruck, Retina-Scan, Stimmerkennung usw.).