Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Informatiksteuerungsorgan des Bundes ISB
Nachrichtendienst des Bundes NDB

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

INFORMATIONSSICHERUNG

LAGE IN DER SCHWEIZ UND INTERNATIONAL

Halbjahresbericht 2017/I (Januar – Juni)

2. NOVEMBER 2017

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

1 Übersicht / Inhalt

2 Editorial

Michel Buri
Stv. Leiter Informatik Service
Verantwortlicher Informatiksicherheit
Spital Wallis

Liebe Leserin, lieber Leser

Die massive, weltweite Malware-Infektion mit WannaCry vom 12. Mai 2017 werden wir so schnell nicht vergessen. Viele private oder öffentliche Unternehmen haben schwere Schäden erlitten. Auch der öffentliche britische Gesundheitsdienst (NHS) war stark betroffen. Jede und jeder von uns hat sich wahrscheinlich die Frage gestellt: «*Was, wenn…?* ». Wie wir alle wissen, hatten wir Glück im Unglück, denn die Folgen hätten noch viel verheerender sein können. Sicher hat sich jede und jeder von uns auch schon grundsätzlicher gefragt, ob zwischen den Nutzen und Risiken der Informationstechnologien stets gut abgewogen wird und ob das Restrisiko noch vertretbar ist.

Diese Frage treibt heute die Spitäler um. Die Medizin des 21. Jahrhunderts, die die Patientinnen und Patienten noch stärker in den Behandlungsprozess miteinbezieht, wird weitgehend auf diesen Technologien beruhen und in der medizinischen Behandlung immer mehr miteinander verbundene Medizinprodukte (Geräte) einsetzen. Dementsprechend sind wir im Falle eines Cyberangriffs vom Typ WannaCry mit riesigen institutionellen Herausforderungen konfrontiert (z.B. körperliche Unversehrtheit der Patientinnen und Patienten oder die Kontinuität der Tätigkeiten nicht mehr gewährleisten zu können).

Eine erste Antwort auf die Fragen nach der Vertretbarkeit des Risikos geben die Ärztinnen und Ärzte, die den Artikel vom 7. Juni 2017 in der Zeitschrift « *The New England Journal of Medicine* » und insbesondere folgende Schlussfolgerung verfasst haben: « *We wouldn't accept being told to use outdated equipment on our patients, and our now-critical IT should be no different* »[1]. Ebenso wenig wie man eine abgelaufene Spritze oder ein abgelaufenes Medikament verwenden darf, sollten miteinander verbundene medizinische Geräte, deren Betriebssystem veraltet oder nicht mit den aktuellsten Sicherheitsupdates ausgestattet ist, noch verwendet werden. Genau das ist aber heute der Fall!

Das ist im heutigen Gesundheitswesen eine der grössten Herausforderungen. Um die Betriebssicherheit miteinander verbundener Medizinprodukte (Geräte) während ihrer ganzen Lebensdauer angemessen sicherstellen zu können, muss ihre IT-Sicherheit anders konzipiert werden und dynamisch sowie ganzheitlich sein.

Um diese Herausforderung bewältigen zu können, müssen alle involvierten Akteure und Verantwortungsträger, wie Hersteller, Spitäler und die Regulierungsbehörde Swissmedic, eng zusammenarbeiten. MELANI spielt in diesem Gefüge, das die Sicherheit miteinander verbundener Medizinprodukte (Geräte) gewährleisten soll, eine zentrale Vermittlerrolle.

Ich wünsche Ihnen bei der Lektüre dieses jüngsten Berichts viel Vergnügen.

Michel Buri

---

[1] R. Clarke, T. Youngstein. Cyberattack on Britain's National Health Service – A wake-up Call for Modern Medicine. In NEJM, June 2017 (Stand: 31. Juli 2017).

3 Schwerpunktthema: WannaCry und NotPetya - Verschlüsselungssoftware oder mehr?

Im ersten Halbjahr 2017 haben im Cyber-Bereich zwei Ereignisse weltweit für grosse Schlagzeilen gesorgt: Am 12. Mai 2017 befiel der Verschlüsselungstrojaner «WannaCry» gemäss Informationen von Europol mindestens 200‘000 Rechner in 150 Ländern. Betroffen waren unter anderem der spanische Telekomanbieter Telefonica, Spitäler in Grossbritannien und die Deutsche Bahn. In der Schweiz konnte MELANI potentielle 204 Opfer identifizieren, wobei im Vergleich zum Ausland keine Betreiber von kritischen Infrastrukturen betroffen waren. Am 27. Juni 2017 verursachte die Schadsoftware «NotPetya» vor allem in der Ukraine grosse Schäden. Betroffen waren u.a. der Flughafen von Kiev, die Ukrainische Zentralbank und die Messstation für Radioaktivität in Tschernobyl. Aber auch andere Länder waren betroffen: Beispielsweise die dänische Reederei Maersk – die grösste Containerschiffsreederei der Welt – sowie der US-amerikanische Pharmakonzern Merck. In der Schweiz fiel unter anderem die Werbefirma Admeira «NotPetya» zum Opfer. Welche Besonderheiten diese beiden Angriffe aufweisen und welche Fragen sie aufwerfen, zeigen die nachfolgenden Kapitel.

Bei Angriffen mit erpresserischer Schadsoftware, so genannter Ransomware, werden Daten auf dem Computer des Opfers verschlüsselt. Anschliessend wird dieses zur Zahlung eines Lösegelds aufgefordert, um die Daten wieder herstellen zu können. Solche Verschlüsselungssoftware wird schon relativ lange eingesetzt. Jedoch scheinen seit einiger Zeit immer mehr Kriminelle auf diese Art von Schadsoftware zurückzugreifen. MELANI beobachtet die Entwicklung in diesem Bereich genau und hat in früheren Halbjahresberichten schon mehrfach auf die verschiedenen Typen und die Vorgehensweise hingewiesen.[2] Zudem hat MELANI zusammen mit zahlreichen Partnern am 19. Mai 2016 einen Awareness Tag zum Thema «Ransomware» durchgeführt.[3] Diese Vorfälle zeigen einmal mehr, wie verletzlich die moderne Gesellschaft mit ihren vernetzten Computersystemen ist.

Empfehlung:

MELANI-Infoseite bezüglich Verschlüsselungstrojanern
https://www.melani.admin.ch/melani/de/home/themen/Ransomware.html

3.1 Ablauf

In beiden Fällen wurde für die Verbreitung der Schadsoftware eine Schwachstelle im SMB-Protokoll missbraucht. SMB ist ein Netzwerkprotokoll für Datei-, Druck- und andere Serverdienste und ist der Kern der Netzwerkdienste von Microsoft. Weiter wird SMB vom frei

[2] https://www.melani.admin.ch/melani/de/home/themen/Ransomware.html (Stand: 31. Juli 2017).

[3] https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/ransomwareday.html (Stand: 31. Juli 2017).

verfügbaren Softwareprojekt «Samba» verwendet, um Windows-Systemen den Zugriff auf Ressourcen von Unix-basierten Systemen zu ermöglichen und umgekehrt.

Den Angriffen vorausgegangen war die Veröffentlichung eines Hacking-Werkzeugs mit dem Namen «DoublePulsar» durch die Gruppe «Shadow Broker» im April 2017. Dieses Hacking-Werkzeug nutzte unter anderem auch die oben genannte SMB-Schwachstelle «Eternal Blue» aus. «DoublePulsar» selbst ist eine Installationssoftware für Backdoor-Programme, die mutmasslich von der National Security Agency (NSA) entwickelt und eingesetzt wurde. Zusammen mit anderen Werkzeugen soll «DoublePulsar» den US-Behörden bereits im Jahr 2016 gestohlen worden sein.

Bei «WannaCry» hat die Infektion höchstwahrscheinlich nur über vom Internet sichtbare Laufwerke mit veralteter SMB-Software stattgefunden, denn bis heute gibt es keinen Hinweis auf andere Infektionswege wie beispielsweise E-Mail. Bei «NotPetya» hingegen wurde ein manipuliertes Update einer Buchhaltungssoftware mit Namen «MeDoc» als Initialvektor ausgemacht. In der Ukraine tätige Unternehmen müssen diese Software verwenden, um Steuern zu entrichten. War ein Computer in einem Firmennetzwerk infiziert, diente die SMB-Lücke dazu, dass sich «NotPetya» lateral im entsprechenden Firmennetz bewegen konnte. Zusätzlich haben die Angreifer noch alternative Möglichkeiten zur lateralen Verbreitung eingebaut. Die Fälle unterscheiden sich also insofern, dass die Angreifer bei «WannaCry» auf gut Glück versucht haben, ihre Software zu platzieren, währenddem bei «NotPetya» die Vermutung nahe liegt, dass gezielt ukrainische Firmen angegriffen werden sollten.

In Anbetracht des Potenzials der beiden Angriffe muss die Abwicklung der Lösegeldzahlungen als unprofessionell bezeichnet werden: Bei «NotPetya» setzten die Angreifer auf E-Mail-Kommunikation. Die entsprechende E-Mail Adresse wurde jedoch rasch gesperrt, was die Kommunikation mit den Opfern verunmöglichte und auch verhinderte, dass ein Entschlüsselungscode an die Opfer verschickt werden konnte. Diese Information wurde rasch über die Medien verbreitet, weshalb nur wenige Opfer bezahlt haben. Zudem war das geforderte Lösegeld in Höhe von etwas über 300 Dollar in beiden Fällen vergleichsweise gering.

3.2 Krimineller Hintergrund oder gezielte Sabotage?

Bei beiden Fällen stellten Sicherheitsexperten einen rein kriminellen Hintergrund in Frage. Die unprofessionelle Implementierung der Bezahlkomponente verdeutlicht die Zweifel, dass in beiden Fällen tatsächlich finanzielle Interessen im Vordergrund standen. Das Ziel rein pekuniär motivierter Akteure im Bereich Ransomware ist es, möglichst schnell und effizient einen hohen Gesamtbetrag von ihren Opfern zu erpressen. Daher ist gerade dieser Teil des Angriffsprozesses erfahrungsgemäss der ausgereifteste, was man von „WannaCry“ und „NotPetya“ nicht behaupten kann.

Der Schadcode von «WannaCry» wies laut Experten Ähnlichkeiten zur Schadsoftware «Lazarus» auf, die beim Angriff auf die Nationalbank von Bangladesch im März 2016 verwendet wurde. Bei «NotPetya» deutet der gezielte Verbreitungsvektor über das ukrainische Buchhaltungsprogramm «MeDoc» darauf hin, dass Sabotage die Hauptmotivation der Täterschaft gewesen sein dürfte. Dass auch Unternehmen ausserhalb der Ukraine betroffen waren, dürfte damit zusammenhängen, dass diese Firmen in der Ukraine tätig sind und dementsprechend diese Buchhaltungssoftware einsetzen müssen. Wer hinter beiden Angriffen steht, dürfte wohl nie ganz geklärt werden. Der Fall zeigt deshalb

exemplarisch die Vorteile eines Cyber-Angriffs: Wie in solchen Fällen üblich, bleibt es auch hier bei Indizien. Einen handfesten Beweis gibt es nicht. Während die Welt über Motivation und Herkunft des Angriffs spekuliert, kann sich der Angreifer in der Anonymität des Internets verstecken.

3.3 Das Problem nicht aktualisierter Systeme

Die Ausbreitung der Schadsoftware in beiden Fällen war deshalb erfolgreich, weil die dazugehörige Sicherheitslücke im SMB-Protokoll eine Verbreitung ohne Benutzerinteraktion ermöglichte. Die Lücke war allerdings zu diesem Zeitpunkt längst bekannt. Bereits Anfang März 2017 hatte Microsoft ein Update veröffentlicht. Dementsprechend hätte ein Vorfall wie «WannaCry» oder «NotPetya» nie zu Infektionen führen dürfen. Wieso waren trotzdem namhafte Unternehmen Opfer dieser Angriffe? Im privaten Bereich werden Updates oft mit einer automatischen Update-Funktion eingespielt. Wenn ein Hersteller die Updates am Dienstag veröffentlicht, sind diese am Mittwoch bereits auf einem Grossteil der Privatcomputer installiert. Im Businessbereich sieht dies allerdings anders aus. Hier können Updates nicht einfach über Nacht eingespielt werden. Ein fehlerhaftes Update kann dazu führen, dass eine geschäftskritische Applikation nicht mehr funktioniert und ein Unternehmen dadurch Verluste schreibt. Deshalb müssen zuerst Tests durchgeführt werden, die sicherstellen, dass die von den Softwarefirmen zur Verfügung gestellten Updates keine negativen Auswirkungen auf geschäftskritische Applikationen haben. Deshalb ist vor jedem Update eine Einschätzung vorzunehmen, ob das Risiko eines nicht eingespielten Updates dasjenige einer nicht funktionierenden Applikation übersteigt. Selbstverständlich können auch andere risikomindernde Massnahmen, wie beispielsweise das Abschotten gefährdeter Systeme, implementiert werden.

In bestimmten Bereichen ist ein Update oft sogar nahezu unmöglich, beispielsweise im Gesundheitsbereich. Bei jeder Veränderung wie dem Einspielen eines Updates würden medizinische Geräte ihre Zertifizierung und damit ihre Zulassung verlieren. Das Risiko würde somit vom Hersteller auf den Betreiber übergehen. Ein fehlerhaftes Update an einem Medizingerät kann möglicherweise lebensbedrohliche Folgen haben. Daher ist es verständlich, dass Spitäler, Arztpraxen, Labors usw. dieses Risiko nicht eingehen wollen. Eine Neuzertifizierung würde das Problem zwar beheben. Jedoch führt eine Neuzertifizierung zu hohen Kosten, braucht Zeit und ist auch nicht überall möglich. Dass im Falle von „WannaCry“ mit seiner wohl ungezielten, globalen Verteilung auch der Gesundheitsbereich in diesem Falle in Grossbritannien betroffen war, ist so gesehen nicht überraschend.

3.4 Die Verantwortung von Sicherheitsdiensten

Um den steigenden Herausforderungen im Bereich der Sicherheit adäquat begegnen zu können, müssen Sicherheitsdienste wie Polizei oder Nachrichtendienste immer öfter auch elektronische Methoden benutzen, um Zielpersonen zu überwachen. Da die Kommunikation über das Internet zunehmend verschlüsselt stattfindet, liegt deren Fokus vermehrt auf den Endgeräten der Zielpersonen, damit die gewünschte Information noch bevor diese verschlüsselt übermittelt wird, beschafft werden kann. Für Sicherheitsdienste sind somit unbekannte Sicherheitslücken («*ZeroDay*-Lücken») ein unumgängliches Mittel zum Zweck: Wenn Geräte auf dem neuesten Stand sind und Personen sich nicht mittels Social Engineering austricksen lassen, ist dies eine der einzigen Möglichkeiten, um trotzdem auf das Zielsystem zu gelangen. Das Ausnützen und Zurückhalten von Wissen um eine solche

Sicherheitslücke unterläuft allerdings in jedem Falle den Prozess des so genannten «Responsible Disclosures». Entsprechend ist dieses Wissen immer mit einer entsprechend grossen Verantwortung gekoppelt und bedingt speziell auf staatlicher Seite einer geregelten, nachvollziehbaren und kontrollierten Risikoabwägung.

Während beim Einsatz solcher ZeroDay-Lücken auf staatlicher Seite in erster Linie davon ausgegangen werden kann, dass ein bestimmtes Ziel oder eine Person im Vordergrund steht, ist dies bei anderen Akteuren nicht notgedrungen der Fall. Werden solche Sicherheitslücken dann plötzlich und unkontrolliert öffentlich und von Dritten verantwortungslos eingesetzt, kann der angerichtete Schaden höher sein als der Mehrwert, den sich ein Sicherheitsdienst ursprünglich versprochen hat. Dies zeigen die Fälle «WannaCry» und «NotPetya»: Angeblich stammte das Wissen um die Lücke im SMB-Protokoll, sowie die dazugehörigen Werkzeuge, die das Ausnützen der Lücke vereinfachen aus dem Portfolio der NSA. Diese Informationen wurde Mitte April 2017 von der Gruppe «Shadow Broker» veröffentlicht, welche bereits im August 2016 für sich reklamierte, Informationen zu ZeroDays von der NSA gestohlen zu haben.

Sollte die bei WannaCry und NotPetya eingesetzte Sicherheitslücke und der dazugehörige Exploit tatsächlich aus der Küche eines Nachrichtendienstes stammen, der sein Wissen bereits 2016 an Dritte verloren hat, hätte möglicherweise eine frühzeitige Information an Microsoft und die damit verbundene frühzeitige Bereitstellung eines Updates, schlimmeres verhindern können. Aufgrund der Zeitspanne bis zum Update im März 2017 scheint es fraglich, ob dies geschehen ist. In diesem Fall wäre demnach nicht nur das Wissen um eine heikle Sicherheitslücke seit längerer Zeit vorhanden gewesen, sondern es hätte selbst nach Abfluss dieser Informationen kein umgehendes «Responsible Disclosure» gegenüber Microsoft stattgefunden. Das Risiko einer unkontrollierten Veröffentlichung von kritischen Sicherheitslücken wäre somit in Kauf genommen worden.

Es gab bereits frühere Fälle, bei denen Informationen zu ZeroDay-Schwachstellen gestohlen und anschliessend für kriminelle Zwecke missbraucht wurden: Die Firma «Hacking Team» wurde 2015 Opfer eines Hackerangriffs. Die entwendeten Daten wurden anschliessend im Internet publiziert. «Vault 7» ist eine Serie von Dokumenten, die Wikileaks ab dem 7. März 2017 veröffentlichte. Sie weist unter anderem auf 24 ZeroDay-Lücken im Betriebssystem Android hin, welche die CIA angeblich im Jahre 2016 gekannt haben soll.

3.5 Datensicherung – Lebensversicherung für jede Firma

Ob und wieviel eine Versicherung in einem Vorfall schliesslich zahlen wird, wissen wohl die wenigsten, aber trotzdem hofft jeder, dass sie einen allfälligen Schaden vollumfänglich decken wird. Gross ist dann der Frust, wenn der Schaden nicht durch die Police abgedeckt, die Deckungssumme zu klein ist oder die Versicherungspolice nicht gezahlt wurde. Jeder tut also gut daran, von Zeit zu Zeit seine Policen zu überprüfen und gegebenenfalls den veränderten Lebensumständen anzupassen. Ähnlich verhält es sich im Bereich Datensicherung.

Bei einer Firma bilden die gespeicherten Daten die Grundlage für das tägliche Geschäft, ohne die kein Geld verdient werden kann. Es sind dies die Kundenkontakte, Kundenkorrespondenz, Aufträge, die Buchhaltung, die Webseite mit allfälligen Datenbanken und viele andere Daten, die für den täglichen Betrieb unabdingbar sind. Es ist deshalb keine Frage, dass diese Daten regelmässig gesichert werden müssen. Allerdings sollte man sich

nicht einfach darauf verlassen, dass das Backup funktioniert. Das Funktionieren der Backups muss regelmässig getestet werden. Ebenfalls muss regelmässig überprüft werden, ob wirklich alle relevanten Daten beim Backup-Prozess berücksichtigt werden.

Bei einem Datenverlust, beispielsweise im Zusammenhang mit Verschlüsselungstrojanern, kommt noch ein weiterer Aspekt dazu. Das Einspielen der Backupdateien dauert in der Regel mehrere Stunden. Während dieser Zeit können Angestellte nicht arbeiten. Das hat im besten Fall einen Gewinnausfall zur Folge, bei kritischen Infrastrukturen wie Spitälern kann dies aber weit gravierendere Auswirkungen haben. So mussten im Falle von «WannaCry» Spitäler in Grossbritannien ihren Notfalldienst einstellen und Patienten auf andere Spitäler ausweichen.

Empfehlung:

Definieren Sie eine Backup Strategie!

Überlegen Sie sich, welche Daten wie häufig gespeichert werden sollen und wie lange die einzelnen Backups gespeichert werden.

Die Sicherungskopie sollte offline gespeichert werden, das heisst auf einem externen Medium (wie beispielsweise einer externen Festplatte), welches nach dem Backupvorgang wieder vom Computer getrennt wird, damit ein Verschlüsselungstrojaner nicht auf dieses zugreifen kann. Ansonsten werden bei einem Befall durch Ransomware möglicherweise auch die Daten auf dem Backup-Medium verschlüsselt und unbrauchbar.

4 Lage national

4.1 Industrielle Kontrollsysteme (IKS)

Auch Betreiber kritischer Infrastrukturen können Opfer von Ransomware-Angriffen werden, wie in Kapitel 3 berichtet wurde. Die Ransomware nistet sich jedoch meist nicht direkt auf den industriellen Kontrollsystemen ein, sondern auf den «Administrationssystemen». Eine Beeinträchtigung dieser «Administrationssysteme» kann jedoch auch Einfluss auf die Produktion haben.

Ransomware, die spezifisch auf industrielle Kontrollsysteme zielt, ist bisher nur in Forschungsarbeiten aufgetaucht.[4] So hat das US-amerikanische Institute of Technology in Georgia ein Szenario beschrieben, in welchem mit dem experimentellen «LogicLocker» die installierte Steuerungslogik verschlüsselt und Lösegeld von den Betreibern erpresst werden könnte.

In einem anderen Fall hat die Firma «CRITIFENCE» eigens den Ransomware-Prototypen «ClearEnergy[5]» entwickelt, um die Massnahmen zur Schliessung der Lücke besser vermarkten zu können, welche «CRITIFENCE» zuvor in ICS-Produkten entdeckte. Die Malware blockiert den Zugang zur Steuerungslogik und droht damit, diese zu überschreiben

[4] http://www.cap.gatech.edu/plcransomware.pdf (Stand: 31. Juli 2017).

[5] http://securityaffairs.co/wordpress/57731/malware/clearenergy-ransomware-scada.html (Stand: 31. Juli 2017).

und damit unbrauchbar zu machen. Zum Glück haben diese Beispiele aber die Laborumgebungen noch nicht verlassen und es noch nicht auf produktive Umgebungen geschafft.

Klassische Ransomware-Angriffe auf Geräte, die zur Fernüberwachung von IKS-Systemen eingesetzt werden, sind hingegen auch in der Schweiz bereits aufgetaucht. So wurde ein System, welches eine Wasserversorgung steuerte, von einer Ransomware befallen. Die Schadsoftware verbreitete sich über die aus dem Internet erreichbare Fernüberwachung, wahrscheinlich mit einem Brute-Force-Angriff auf den entsprechenden Server. Das Ganze ging jedoch glimpflich aus: Das System konnte dank Backups wieder hergestellt werden und wurde zusätzlich abgesichert. Dieses Beispiel zeigt sehr schön, dass jede zusätzliche Funktionalität (hier die Fernüberwachung der Systeme) auch zusätzliche Sicherheitsmassnahmen erfordert.

Auch Teile zentraler Steuerungen von industriellen Kontrollsystemen werden vermehrt in die Cloud ausgelagert. Die Gornergratbahn[6] setzt beispielsweise ein in der Cloud virtualisiertes Bahnleitsystem ein. In Kombination mit dem Vorhaben, künftig führerlose Züge[7] einzusetzen, wächst auch die Kritikalität der eingesetzten Steueranlagen. Dementsprechend müssen diese Steuerungssysteme zwingend gut abgesichert sein.

Empfehlung:

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

Meldeformular MELANI

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

Checkliste mit Massnahmen zum Schutz industrieller Kontrollsysteme

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

4.2 Angriffe (DDoS, Defacements, Drive-By)

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

---

6 https://www.siemens.com/innovation/de/home/pictures-of-the-future/mobilitaet-uns-antriebe/urbane-mobilitaet-gornergratbahn.html (Stand: 31. Juli 2017).

7 https://www.sob.ch/medienmitteilung/news/2017/6/15/sob-treibt-automatisches-fahren-voran.html(Stand: 31. Juli 2017).

4.2.1 VENOM Linux Rootkit am CERN analysiert

Am 11. Januar 2017 veröffentlichte das Computer Security-Team des CERN in Genf eine weltweite Warnung vor dem «VENOM»-Rootkit[8]. Ein Rootkit ist ein Softwarewerkzeug, das auf dem kompromittierten System installiert wird, um Anmeldevorgänge des Angreifers zu verbergen und seine Prozesse und Dateien zu verstecken. Im Fall von VENOM hat der Angreifer die Schadsoftware dabei in automatisierter Form auf das Dateisystem geladen, und Veränderungen wurden innerhalb weniger Minuten durchgeführt. Während dieses Vorgangs wurde die Systemzeit in der Art manipuliert, dass die Dateien falsche Modifikationszeiten hatten und somit nicht so leicht entdeckt werden konnten. Wenn immer möglich wurde der Schadcode direkt auf der angegriffenen Maschine aus dem temporären Speicher RAM ausgeführt, um keine Spuren auf den Laufwerken zu hinterlassen. Die Malware zielt auf Linux Server und installiert eine *Backdoor* auf dem betroffenen Gerät, kann aus der Ferne Befehle ausführen und Dateien verändern. Das EGI-CSIRT[9] vermutete die Initialinfektion über gestohlene Zugangsdaten für den SSH-Fernzugriff. Der Angriff zeigt Ähnlichkeiten mit dem Eindringen in den «Freenode»[10] Chat-Server im Jahre 2014. Das Rootkit VENOM zielte auf die Gemeinschaft der Astrophysiker. Am CERN hatte dieses Rootkit im Übrigen keine Auswirkungen.

Empfehlung:

Da «Venom» seine Spuren auf dem infizierten Gerät verwischt, empfiehlt sich für Server ein externes Log-Speicher-System, damit auch solche Fälle nachträglich analysiert werden können.

4.2.2 Propaganda statt Wassertemperatur

Politische Spannungen entladen sich immer häufiger digital. Wo früher Häuserwände mit Graffiti besprüht wurden, verunstalten heute Hacktivisten Webseiten. Die digitale Verwüstung hat für die Angreifer den Vorteil, dass sie sich nicht physisch vor Ort begeben müssen, sondern ihre Propaganda von irgendeinem Punkt dieser Erde aus verbreiten können. Diese Abkoppelung der lokalen Präsenz führt dazu, dass sich internationale Ereignisse auch auf Schweizer Webauftritte auswirken können.

Ende März 2017 trugen Aktivisten bei einer Demonstration in Bern ein Transparent mit der Aufschrift «Kill Erdogan with his own weapons» durch die Strassen. In den folgenden Tagen verzeichnete MELANI mehrere so genannte Defacement-Angriffe auf Schweizer Webseiten[11]. So fanden beispielsweise Besucher der Website Badi Wülflingen anstelle der gesuchten Wassertemperaturen türkisch-nationalistische Botschaften.

---

8 https://cern.ch/security/venom.shtml (Stand: 31. Juli 2017).

9 https://wiki.egi.eu/w/images/c/ce/Report-venom.pdf (Stand: 31. Juli 2017).

10 https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2014/october/analysis-of-the-linux-backdoor-used-in-freenode-irc-network-compromise/ (Stand: 31. Juli 2017).

11 http://www.tagesanzeiger.ch/digital/internet/tuerkische-propaganda-auf-schweizer-badiwebsite/story/12947804 (Stand: 31. Juli 2017).

Abbildung 1: Verunstaltete Webseite der Badi Wülflingen

Dass eine und gerade diese Badeanstalt betroffen war, war reiner Zufall. Die Hacktivisten suchen sich Webseiten mit Schwachstellen. Die Angreifer würden ihre Botschaften sicherlich gerne auf vielbesuchten Seiten bekannter Firmen und Organisationen platzieren. Diese sind aber meistens gut geschützt, weshalb die Angreifer oft auf kleinere Websites ausweichen.

Doch nicht nur Schweizer Websites wurden für diese Propaganda missbraucht. Auch gehackte Twitterkonten[12] wurden für die Verbreitung eingesetzt. Zudem gehörten auch andere Angriffsarten zum Repertoire: Türkische Hacker bekannten sich zu DDoS-Angriffen gegen die österreichische Webseite «oe24.at» im März 2017[13].

Politische Propaganda muss nicht der einzige Grund für Defacements sein. Wie einschlägige Portale[14] belegen, geht es oft auch um die Suche nach Anerkennung oder um den Wettbewerb mit Gleichgesinnten.

Empfehlung:

Angriffe auf Content Management Systeme (CMS) zur Erstellung von Websites lassen sich durch das zeitnahe Einspielen von Sicherheitsaktualisierungen massiv reduzieren. Es gibt jedoch noch eine Reihe weiterer Massnahmen, welche zur Sicherheit des CMS beitragen:

DOKU

Massnahmen zum Schutz von Content Management Systemen (CMS)

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

12 https://www.theregister.co.uk/2017/03/15/twitter_app_hack/ (Stand: 31. Juli 2017).

13 http://www.oe24.at/oesterreich/politik/Attacke-auf-oe24-Tuerkische-Hacker-bekennen-sich/273401472 (Stand: 31. Juli 2017).

14 http://zone-h.com/ (Stand: 31. Juli 2017).

4.2.3 Online-Medien weiterhin als Infektionskanal missbraucht

Im Halbjahresbericht 2012/2[15] hat MELANI vor den Risiken, welche die zunehmende Einbindung von Drittinhalten auf Webseiten mit sich bringt, gewarnt. Medienportale sind häufig die Rekordhalter beim Einbinden von verlinkten Videos, Werbung und sozialen Netzwerken. MELANI hat an dieser Stelle bereits mehrfach[16/17] über Infektionen von Besuchern solcher Medienportale berichtet.

Im Frühjahr 2017 wurden Schweizer News-Portale zum wiederholten Male angegriffen. Im März berichtete 20min.ch[18], dass sich Unberechtigte Zugriff auf ihr Online-Portal verschafft hatten, um bösartige Skripte zu platzieren. Ein ähnlicher Vorfall wiederholte sich im April bei pctipp.ch[19]. Durch ein eingeschleustes Skript wurde versucht, Online-Leser auf Seiten umzuleiten, die Malware auslieferten.

Für Angreifer sind Medienportale interessant, da diese viele Besucher und damit eine grosse Reichweite haben. Exemplarisch zeigt sich dies bei der gross angelegten Malvertising-Kampagne der Gruppe «AdGholas»[20]. Unter Zuhilfenahme sogenannter *Exploit-Kits* wird durch gezieltes Einschleusen bösartiger Dateien auf das Opfer zugeschnittene Malware verteilt.

---

15 Siehe MELANI Halbjahresbericht 2/2012, Kapitel 5.5 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2012-2.html (Stand: 31. Juli 2017).

16 Siehe MELANI Halbjahresbericht 2/2015, Kapitel 4.3.1 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2-2015.html (Stand: 31. Juli 2017).

17 Siehe MELANI Halbjahresbericht 1/2016, Kapitel 4.4.2 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2016-1.html (Stand: 31. Juli 2017).

18 http://www.20min.ch/digital/news/story/Angriffsversuch-auf-20minuten-ch-vereitelt-27863282 (Stand: 31. Juli 2017).

19 http://www.pctipp.ch/in-eigener-sache/artikel/drive-by-angriff-auf-pctipp-87549/ (Stand: 31. Juli 2017).

20 https://www.proofpoint.com/us/threat-insight/post/massive-adgholas-malvertising-campaigns-use-steganography-and-file-whitelisting-to-hide-in-plain-sight (Stand: 31. Juli 2017). https://www.proofpoint.com/us/threat-insight/post/adgholas-malvertising-campaign-using-astrum-ek-deliver-mole-ransomware (Stand: 31. Juli 2017).

Die vollständige Anleitung und Checkliste ist auf der Website von www.melani.admin.ch abrufbar:

DOKU

Massnahmen zum Schutz von Content Management Systemen (CMS)

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

Zudem finden Sie dort eine Anleitung und Checkliste, was zu tun ist, wenn bereits ein Angriff erfolgt ist:

DOKU

Anleitung Webseitenbereinigung

https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/anleitung-webseitenbereinigung.html

4.2.4 Vielen Dank für Ihre Registrierung – Der Anmelde-Spam

Unerwünschte Werbemails, sogenannter Spam, wird weltweit täglich milliardenfach versandt. Die eingesetzten Spamfilter der E-Mail-Anbieter werden jedoch immer besser und mildern die Auswirkungen für die meisten Nutzer in den meisten Fällen auf ein erträgliches Mass. Zu Beginn des Jahres 2017 verzeichnete MELANI aber vermehrt Meldungen von unerwünschtem Mailversand, der sich gegen einzelne spezifische Empfänger richtete. So erhielten Organisationen und Privatpersonen eine Vielzahl unerwünschter Mails mit der Aufforderung, sich für verschiedene Newsletter, Forumsbeiträge und ähnliche Dienste, die eine Anmeldung erfordern, zu registrieren. Werden solche Dienste automatisch von einem Programm registriert, spricht man von einer sogenannten «Subscription Bomb[21]».

Wenn keine Rückbestätigung gefordert wird, erhalten die Opfer anschliessend auch noch alle Folgenachrichten dieser zahlreichen Dienste. Man kann sich zwar von solchen Diensten wieder abmelden und entsprechende Filter setzten. Bei mehreren zehntausend solcher Anmeldungen kann für die Betroffenen daraus aber ein hoher Aufwand resultieren.

4.3 Social Engineering und Phishing

Neben all den technischen Angriffen sind vor allem solche erfolgreich, welche versuchen, das Opfer mit einer glaubwürdigen Geschichte um den Finger zu wickeln. So genannte 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. Früher gaben sich die Angreifer

[21] http://www.forbes.com/sites/leemathews/2017/05/10/secure-email-provider-attacked-with-500k-newsletter-sign-ups/ (Stand: 31. Juli 2017).

beispielsweise mit der Kontaktliste eines E-Mail-Kontos zufrieden. Sie schrieben den potenziellen Opfern, der Absender sei im Ausland, habe Handy und Portemonnaie verloren und benötige dringend finanzielle Unterstützung. Heute nehmen sich die Kriminellen die Zeit, den E-Mail-Verkehr eines kompromittierten Kontos penibel nach brauchbarem Material zu durchforsten. So wird zum Beispiel nach elektronischen Rechnungen gesucht, welche anschliessend mit veränderter IBAN-Nummer wieder dem Opfer zugestellt werden. Auch Kommunikationen mit der Bank stehen bei den Angreifern hoch im Kurs. Dass auch scheinbar unbrauchbare Daten für Betrügereien genutzt werden, zeigt ein Fall, bei dem das Händlerverzeichnis einer Ausstellung als Informationsbasis diente. Firmen wurden gezielt angeschrieben und ihnen mitgeteilt, dass man sich von dieser Veranstaltung kenne und dort bereits über ein «grosses» Geschäft diskutiert habe, dass mit höchster Diskretion behandelt werden müsse. Eine entsprechende Vertrauensbasis war somit gelegt. Anschliessend wurden die Mitarbeitenden unter Druck gesetzt und zur Zahlung eines grossen Betrages aufgefordert.

4.3.1 Phishing

Auch im ersten Halbjahr 2017 wurden zahlreiche Phishing-E-Mails versendet. Der Inhalt der Mails ändert sich dabei nicht sehr: Die einen fragen nach Kreditkartendaten, damit diese «verifiziert» werden können, andere fordern auf der verlinkten Seite nach Login und Passwort zu Internetdiensten. Regelmässig werden in solchen Phishing-Mails auch Firmenlogos von bekannten Unternehmen respektive des betroffenen Dienstes missbraucht, um den E-Mails einen offiziellen Anstrich zu geben.

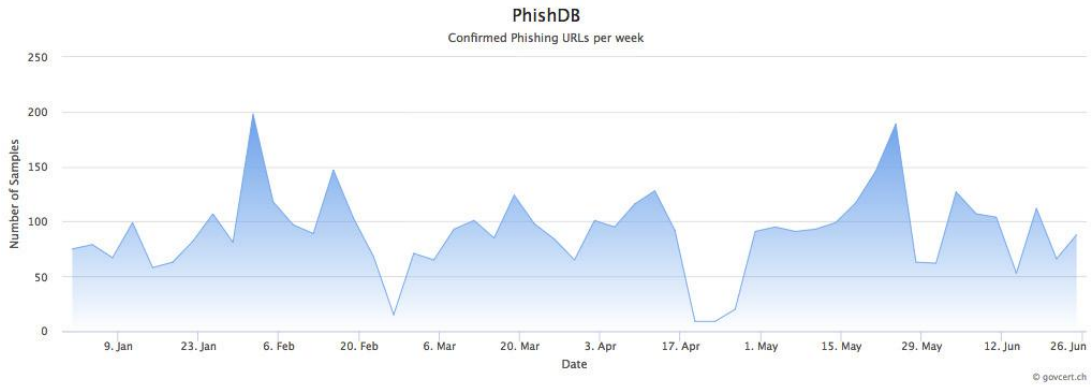


Abbildung 2: Gemeldete und bestätigte Phishing-Seiten pro Woche auf antiphishing.ch im ersten Halbjahr 2017

Insgesamt wurden im ersten Halbjahr 2017 2343 verschiedene eindeutige Phishing-Seiten über das von MELANI betriebene Portal antiphishing.ch gemeldet. Auf Abbildung 2 sind die gemeldeten Phishing-Webseiten pro Woche dargestellt, wobei die Anzahl über das Halbjahr 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.

4.3.2 Neue Angriffsmethode richtet sich gegen Firmen

Im ersten Halbjahr 2017 mehrten sich Anrufe bei potenziellen Opferfirmen, in denen sich Angreifer als Bankmitarbeiter ausgaben. Dies ist für die Angreifer einfach möglich, da viele Unternehmen die Bankverbindung auf ihrer Website publizieren. Die Information kann aber

auch im Vorfeld durch die Betrüger mittels Telefonanruf oder E-Mail-Anfrage beim Unternehmen eruiert werden.

Die Anrufer geben vor, ein Update beim E-Banking durchführen zu müssen, das anschliessend getestet werden soll. Um diesen Test durchführen zu können, müssten allerdings alle Mitarbeitenden der Finanzabteilung, insbesondere diejenigen, die Unterschriftsberechtigung beim E-Banking haben, anwesend sein. Um Vertrauen zu schaffen, erwähnen die Betrüger zum Teil die Namen von existierenden Mitarbeitenden.

Bei einem weiteren Anruf soll dann ein Fernzugriffstool installiert und dem Anrufer der Zugriff gewährt werden. Dieser gibt vor, anhand einer Testzahlung die Funktionsweise des Systems überprüfen zu wollen. Da in der Geschäftswelt Zahlungen ab einer gewissen Höhe nur durch eine Kollektivunterschrift freigegeben werden können, fordern die Betrüger die Unterschriftsberechtigten auf, ihre Zugangsdaten anzugeben. In Wirklichkeit geben sie allerdings so die Zahlung frei. In einigen Fällen wird dem Opfer während dieses Vorgangs durch die Angreifer ein schwarzer Bildschirm eingeblendet, damit das Opfer die betrügerische Zahlung nicht bemerken kann.

Empfehlung:

Das Beispiel zeigt, wie aktuell Social Engineering-Methoden weiterhin sind. Die Sensibilisierung innerhalb der einzelnen Firmen ist der Schlüssel, solchen Betrugsversuchen wirksam vorzubeugen:

- Verzichten Sie wenn möglich auf die Publikation Ihrer Bankverbindung im Internet
- Gewähren Sie niemals Unbefugten Zugriff auf Ihr System
- Installieren Sie niemals auf Anforderung unbefugter Drittpersonen so genannte Remote-Tools
- Keine Bank wird Sie auffordern, irgendwelche Tests durchzuführen. Banken verfügen über eigene IT-Abteilungen oder haben die IT ausgelagert. In jedem Fall werden Sicherheitsupdates geprüft, bevor diese öffentlich zugänglich gemacht werden.

4.3.3 CEO-Fraud – Low Tech Fraud

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

Dass diese Betrugsform eine enorme Zuwachsrate hat, bestätigen verschiedene Statistiken, die im ersten Halbjahr 2017 publiziert worden sind. Laut Deutschem Bundeskriminalamt

(BKA) sind durch CEO-Fraud in den letzten Monaten in Deutschland Schäden in Millionenhöhe entstanden.[22] Auch das FBI hat im Mai dieses Jahres Zahlen zu der enormen Entwicklung dieses Betrugstyps publiziert. So wurde bei CEO-Fraud zwischen Januar 2015 und Dezember 2016 eine Zunahme von 2370 Prozent festgestellt. Laut Bericht wurden Fälle in 132 Ländern mit einer Schadensumme in Milliardenhöhe registriert.[23] Die gestohlenen Gelder werden dabei meist zu Banken in China und Hong Kong gelenkt, aber auch auf Banken im Vereinigten Königreich werden vermehrt Gelder aus diesem Betrugstyp geleitet. Längst verantworten Social Engineering-Angriffe ohne grossen technischen Aufwand einen beachtlichen Teil der finanziellen Schäden im Internet.

Empfehlung:

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

Aktuelle Gefahren: CEO-Fraud

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

Aktuelle Gefahren: Social Engineering

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

4.3.4 Falscher Telefonsupport: Immer perfektere Methoden

Schon seit mehreren Jahren rufen Betrüger Schweizerinnen und Schweizer an. Sie geben sich meistens als Microsoft aus und behaupten, ein Informatikproblem erfordere eine Störungsbehebung via Telefonsupport. Die Betrüger versuchen das Opfer zu erschrecken, indem sie ihm vorgaukeln, sein Computer sei beschädigt. Dabei fordern sie das Opfer zum Beispiel auf, den «Event Viewer» zu öffnen, der alle Ereignisse und Aktivitäten auf dem Computer anzeigt. Je nach Alter und Konfiguration des Computers kann die Liste der im Ereignisprotokoll aufgeführten Fehlermeldungen sehr lang sein, ohne dass das System ein Problem hat. Anschliessend versuchen die Betrüger, mit einer Fernsteuerungssoftware auf den Computer zuzugreifen und nehmen Manipulationen vor, um dann für ihre angebliche Dienstleistung noch Geld zu verlangen. Wir haben dieses Vorgehen schon mehrfach beschrieben (zum ersten Mal im Halbjahresbericht 2011/2, Kapitel 3.1) [24].

---

[22] https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2017/CEO_Fraud_10072017.html (Stand: 31. Juli 2017).

[23] https://www.ic3.gov/media/2017/170504.aspx#fn3 (Stand: 31. Juli 2017).

[24] Siehe MELANI Halbjahresbericht 2/2011, Kapitel 3.1 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2011-2.html (Stand: 31. Juli 2017).

Diese Telefonanrufe bleiben zwar weiterhin aktuell, doch die Betrüger verwenden heute zusätzlich noch andere Methoden, um mit ihren Opfern in Kontakt zu treten. Bei einer Variante wird immer noch angerufen, bei Entgegennahme des Anrufs wird dem Opfer allerdings eine Nachricht abgespielt, in der es aufgefordert wird, auf eine bestimmte Nummer zurückzurufen, damit angeblich auf ihrem Computer festgestellte Informatikprobleme gelöst werden können.

Eine andere gefährlichere Variante treibt seit einiger Zeit im Ausland ihr Unwesen und taucht seit kurzem auch in der Schweiz auf. Hierbei erscheint beim Surfen im Internet plötzlich ein Pop-up, das von präparierten Internetseiten oder von einer auf dem Computer installierten Adware stammt. Auf dem Pop-up ist eine vermeintliche Nachricht von Microsoft zu lesen, der Computer sei durch eine Schadsoftware infiziert. Der Benutzer wird aufgefordert, eine bestimmte Nummer anzurufen, um den Diebstahl sensibler Daten zu vermeiden. Sobald er das tut, geht es mit dem klassischen Ablauf des falschen Telefonsupports weiter, wie er weiter oben beschrieben wurde. Interessanterweise verwenden die Betrüger manchmal Schweizer Nummern. Anrufe auf diese Nummern werden wahrscheinlich ins Ausland umgeleitet.

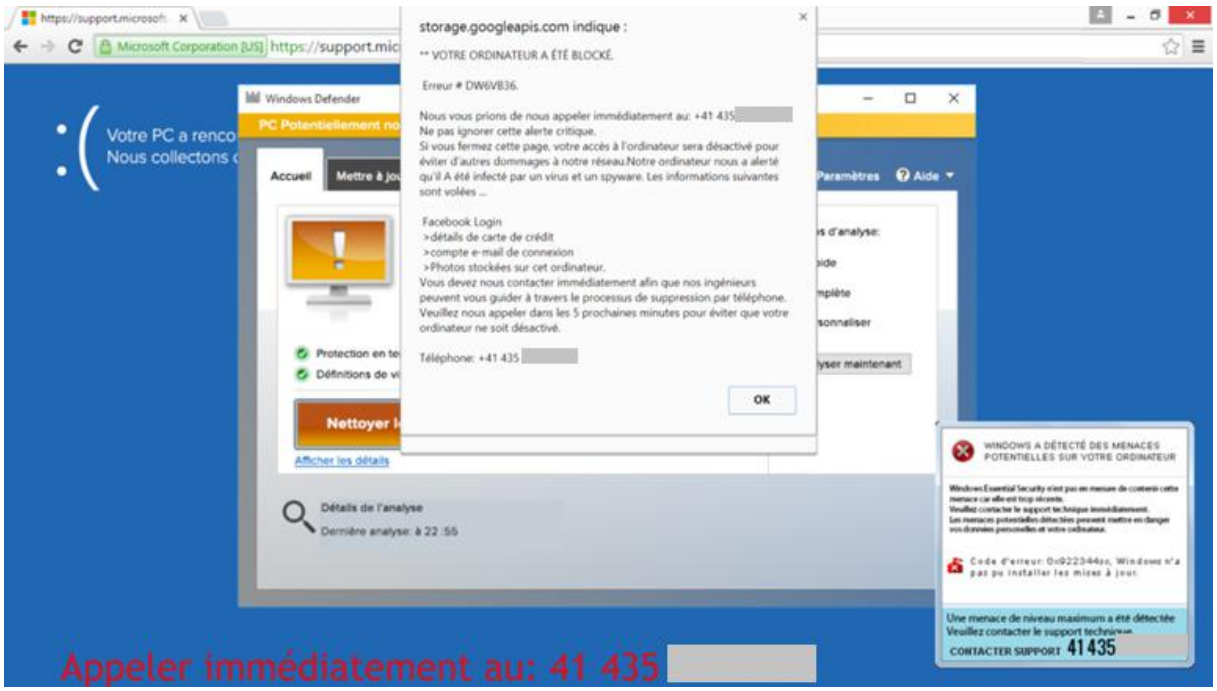


Abbildung 3: Beispiel eines Pop-ups auf dem Bildschirm. Es handelt sich nicht um die echte Navigationsleiste, sondern um ein Bild, das den Eindruck erweckt, man befinde sich tatsächlich auf der Microsoft-Webseite.

Die grundlegenden Tipps, wie man auf diese neue Vorgehensweise reagieren soll, sind immer noch dieselben: Microsoft und andere Unternehmen rufen niemals von sich aus an, um Informatikprobleme zu lösen. Es wird deshalb dringend empfohlen in einem solchen Fall sofort den Hörer aufzulegen. Falls den Betrügern ein Fernzugriff gewährt wurde, ist es empfehlenswert, das Betriebssystem neu zu installieren und alle auf diesem Computer verwendeten Passwörter durch neue zu ersetzen.

Tauchen Warnmeldungen in der Form von Pop-ups auf, verschwinden diese in der Regel mit dem Schliessen des Browsers. Sind die Pop-ups immer noch vorhanden, kann der Browser über den Task-Manager geschlossen werden. Da solche Pop-ups üblicherweise von

zweifelhaften Webseiten stammen, lässt sich das Risiko vermeiden, wenn diese möglichst nicht angesurft werden.

Empfehlung:

Mehr Informationen finden Sie auf den Seiten von Microsoft:

INFO

https://blogs.technet.microsoft.com/mmpc/2017/04/03/tech-support-scams-persist-with-increasingly-crafty-techniques/

https://www.microsoft.com/en-us/safety/online-privacy/avoid-phone-scams.aspx

4.3.5 Phishing über «Data URL»-Funktion

Angreifer suchen auf der einen Seite immer nach neuen Wegen, Internetbenutzer hinters Licht zu führen und auf der anderen Seite, es Sicherheitsdienstleistern auch möglichst schwer zu machen, die betrügerischen Seiten zu deaktivieren. Eine dieser Möglichkeiten ist der Missbrauch der so genannten «Data-URL»-Funktion des Browsers für Phishing-Angriffe. Diese Vorgehensweise ist zwar nicht neu, wurde aber im März 2017 erneut für Phishing-Angriffe verwendet. Eine «Data-URL» ermöglicht es, Daten direkt in einen Link einzubetten, als wären es externe Ressourcen. Der Vorteil liegt darin, dass so der ganze Inhalt einer Webseite direkt in den Link untergebracht werden kann, ohne diesen, wie sonst üblich, von einem Webserver herunterzuladen. Die Seite ist also nicht auf einem Webserver gespeichert und kann so auch nicht von Sicherheitsdienstleistern deaktiviert werden.

Eine solche in einen Link eingebettete Seite unterscheidet sich von einer normalen Webseite in der angezeigten URL, die nicht wie üblich mit «https://», sondern mit «data:text/html» beginnt und sehr lang ist. Durch geschicktes Wählen der ersten Zeile und damit dem Bereich, der in der Adresszeile des Browsers sichtbar ist, kann ein Betrüger aber dem Opfer vortäuschen, dass es auf einen Webserver eines E-Mail-Providers oder eines Kreditkarteninstituts geleitet wird. Hierzu gestaltet der Betrüger den Startbereich der «Data-URL» so, dass nur der Link der jeweiligen Firma sichtbar ist (siehe untenstehende Abbildung). Der Rest des sehr langen Links, der den ganzen Quelltext der Seite enthält, verschwindet in den weiteren nicht angezeigten Zeilen.[25]

Abbildung 4: «Data-URL» einer eingebetteten Webseite, der vermeintlich auf die Login-Seite von Yahoo führt, in Tat und Wahrheit allerdings eine von den Betrügern kreierte eingebettete Webseite ist

[25] https://thehackerblog.com/dataurization-of-urls-for-a-more-effective-phishing-campaign/index.html (Stand: 31. Juli 2017).

4.4 Crimeware

Crimeware ist eine Form von Schadsoftware, die kriminologisch zur Computerkriminalität zählt und rechtlich bei Datenbeschädigung sowie betrügerischem Missbrauch einer Datenverarbeitungsanlage anzusiedeln ist. Auch im ersten Halbjahr 2017 konnten zahlreiche Infektionen mit Crimeware festgestellt werden. Der grösste Teil ging wie bereits in den Vorjahren auf das Konto der Schadsoftware «Downadup» (auch bekannt als «Conficker»). Der Wurm existiert bereits seit über acht Jahren und verbreitet sich über eine im Jahr 2008 entdeckte und ebenso lange geschlossene Sicherheitslücke in Windows-Betriebssystemen. An zweiter und dritter Stelle folgen die Schadsoftware «spambot» und «cutwail», die sich auf das Versenden von Spam und Schadsoftware spezialisiert haben. An vierter Stelle ist das seit dem Angriff auf den Internetdienstleister «Dyn» bekannt gewordene *Bot*-Netzwerk «Mirai», welches Geräte im Internet der Dinge infiziert. Auf Platz 9 folgt der erste E-Banking Trojaner «Dyre».

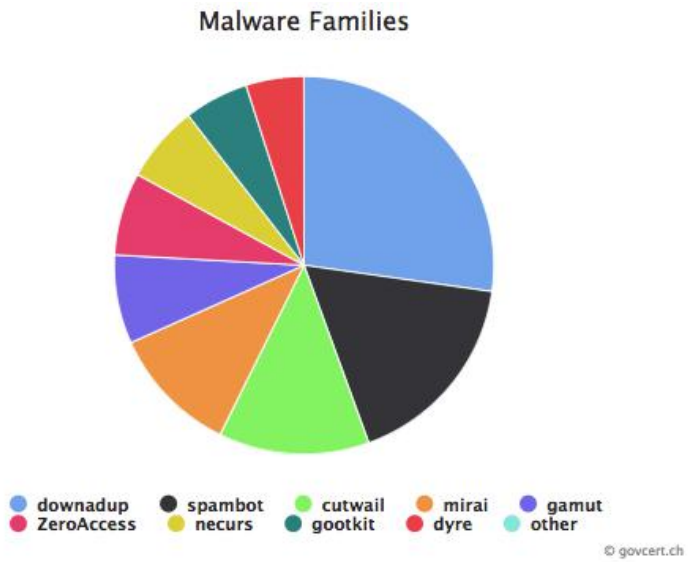
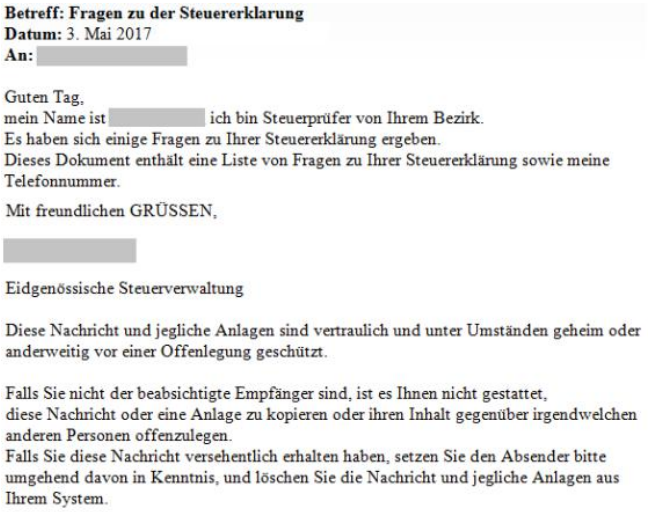


Abbildung 5: Verteilung der Schadsoftware in der Schweiz, welche MELANI bekannt ist. Stichtag ist der 30. Juni 2017. Aktuelle Daten finden Sie unter: http://www.govcert.admin.ch/statistics/dronemap/

4.4.1 Zunehmender Missbrauch von Bundesstellen und bekannten Unternehmen bei Versand von Schadsoftware

Betrüger versenden vermehrt E-Mails im Namen von Bundesstellen, um den E-Mails einen möglichst offiziellen Charakter zu geben und ihrem Betrugsversuch grössere Erfolgsaussichten zu geben. So waren beispielsweise E-Mails im Umlauf, die angeblich von der Eidgenössischen Steuerverwaltung (ESTV) stammen. Dabei wurde eine Steuerrückerstattung in Aussicht gestellt, wenn man das mit Schadsoftware angereicherte und angehängte Dokument ausfüllte. Die Absenderadressen sind in diesen Fällen gefälscht.



Betreff: Fragen zu der Steuererklarung
Datum: 3. Mai 2017
An: [redacted]

Guten Tag,
mein Name ist [redacted] ich bin Steuerprüfer von Ihrem Bezirk.
Es haben sich einige Fragen zu Ihrer Steuererklärung ergeben.
Dieses Dokument enthält eine Liste von Fragen zu Ihrer Steuererklärung sowie meine Telefonnummer.

Mit freundlichen GRÜSSEN,

[redacted]

Eidgenössische Steuerverwaltung

Diese Nachricht und jegliche Anlagen sind vertraulich und unter Umständen geheim oder anderweitig vor einer Offenlegung geschützt.

Falls Sie nicht der beabsichtigte Empfänger sind, ist es Ihnen nicht gestattet, diese Nachricht oder eine Anlage zu kopieren oder ihren Inhalt gegenüber irgendwelchen anderen Personen offenzulegen.
Falls Sie diese Nachricht versehentlich erhalten haben, setzen Sie den Absender bitte umgehend davon in Kenntnis, und löschen Sie die Nachricht und jegliche Anlagen aus Ihrem System.

Abbildung 6: Beispiels eines betrügerischen E-Mails im Namen der Eidgenössischen Steuerverwaltung ESTV

Die Angreifer verwenden als Absender auch bekannte Firmennamen, um dem E-Mail ein seriöses Aussehen zu geben. Beliebt bei Angreifern sind angebliche Paketzustellversuche von DHL und der Schweizerischen Post oder Zahlungsanweisungen. Ein bekanntes Beispiel sind auch gefälschte Swisscom-Rechnungen, mit denen Angreifer im Februar 2017 versucht haben, die Schadsoftware «Dridex» zu verbreiten.

Auch gefälschte Vorladungen zu Gerichtsverhandlungen oder E-Mails, die angeblich von der Kantonspolizei stammen, benutzen die Angreifer, um den Empfänger zu verunsichern und diesen zum Klick auf einen Link zu verleiten oder einen Anhang zu öffnen.

Schlussfolgerung:

Die Angreifer wollen den Benutzer überrumpeln, seine Neugier wecken oder ihn verängstigen, um ihn dann zu einer unbedachten Aktion zu verleiten. In den meisten Fällen wird schnell klar, dass es sich um eine Fälschung handelt. So kommuniziert beispielsweise die Eidgenössische Steuerverwaltung nur auf dem Postweg und nie via E-Mail. Bei den missbrauchten Organisationen sorgen betrügerische E-Mails für ein grosses Meldeaufkommen und somit für einen grossen Arbeitsaufwand.

4.4.2 Schadsoftware: Vorsicht ist geboten – unabhängig vom Betriebssystem

Nutzer des Betriebssystems MacOS müssen sich ebenfalls auf Malware-Angriffe über Microsoft-Office-Dokumente einstellen: Sicherheitsforscher haben im Umlauf befindliche Word-Dokumente entdeckt, deren Makros speziell auf MacOS ausgelegt sind. Öffnet der Nutzer das manipulierte Dokument und erlaubt - trotz Warnhinweis - die Aktivierung der Makro-Funktion, prüft die enthaltene Schadsoftware, ob das Sicherheits-Tool «Little Snitch» aktiv ist. Ist dies nicht der Fall, wird Schadcode nachgeladen und eine Backdoor auf dem Mac eingerichtet.[26]

[26] https://www.digitaltrends.com/computing/macos-suffers-first-word-macro-virus/ (Stand: 31. Juli 2017).

Andere Angriffe gegen das MacOS enthielten einen Anhang in Form einer ZIP-Datei, welche eine detaillierte Rechnung einer angeblichen Bestellung hätte enthalten sollen. Ziel dieser Vorgehensweise war die Installation des Bankentrojaners «Retefe» auf diesen Rechnern. «Retefe» ist ein in der Schweiz gut bekanntes Schadprogramm, das aber bislang von den Angreifern nur gegen Windows-Betriebssysteme eingesetzt worden ist.

Um das Betriebssystem eines bestimmten Opfers zu eruieren und dieses mit der richtigen Schadsoftwareversion zu bedienen, versuchen die Kriminellen im Vorfeld ein unverdächtiges E-Mail zu senden, das dem Angreifer diese Information automatisch liefert. Das E-Mail enthält dabei ein kleines, für den Mail-Empfänger fast unsichtbares Bild (1x1 Pixel). Wenn dieses Bild heruntergeladen wird (was abhängig von der E-Mail Konfiguration auch automatisch geschehen kann), wird eine Verbindung mit dem Server des Angreifers aufgebaut, auf dem das Bild abgespeichert ist. Gleichzeitig werden automatisch verschiedenste Informationen der Computerkonfiguration, unter anderem auch Informationen zum verwendeten Betriebssystem, übermittelt. Die Kriminellen erhalten so die Möglichkeit, die E-Mail-Adresse mit der Computerkonfiguration in Verbindung zu bringen. In einem zweiten Schritt senden sie ein E-Mail, welches auf das entsprechende Betriebssystem ausgerichtet ist.

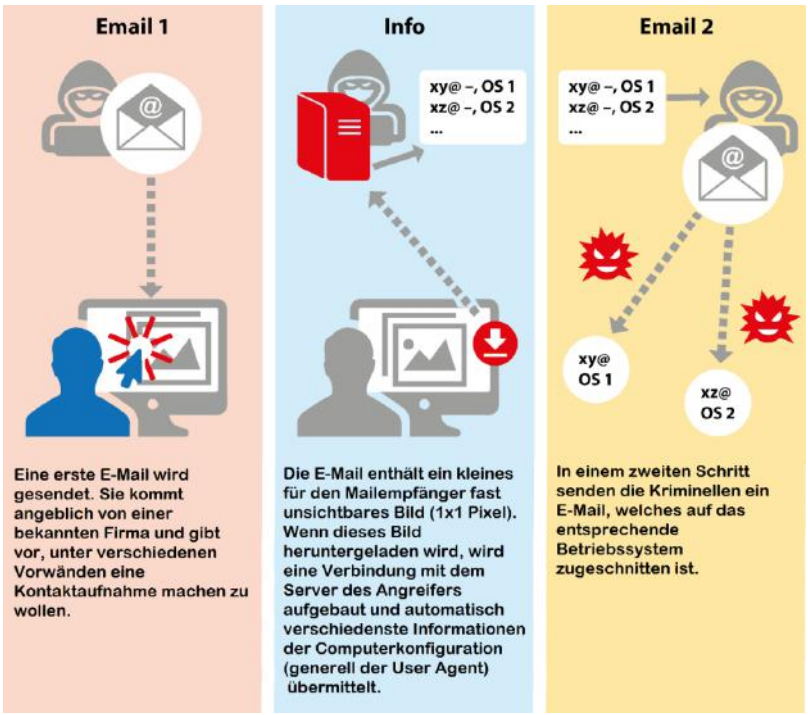


Abbildung 7: Schematischer Ablauf, wie die Betrüger das Betriebssystem eines bestimmten Opfers eruieren

5 Lage International

5.1 Spionage

5.1.1 Managed IT Service Provider im Visier von APT10

Die mutmasslich aus China stammende Cyber-Spionagekampagne «APT10», auch bekannt unter den Namen «menuPass», «CVNX», «StonePanda» und «POTASSIUM», hat seit 2009 sowohl diverse Industriesektoren als auch staatliche Einrichtungen im Visier. Vor allem scheinen es die Angreifer auf militärische Einrichtungen verschiedener Nationen und auf die Vereinigten Staaten abgesehen zu haben.

Der Sicherheitsdienstleister «BAE System» hat im April 2017 in Zusammenarbeit mit dem Prüfungs- und Beratungsunternehmen PwC und dem britischen National Cyber Security Center eine Untersuchung zu den jüngsten Aktivitäten von «APT10» veröffentlicht. Gemäss dieser führt «APT10» seit etwa der zweiten Hälfte 2016 zwei Angriffskampagnen durch: die erste gegen japanische Organisationen und eine zweite, die sich weltweit auf einige wichtige Managed IT Service Provider (MSP) konzentriert.

In der ersten Kampagne wurde der neue Trojaner «ChChes» eingesetzt. Dieser nutzt ein Zertifikat, das aus dem Daten-Leak des «Hacking Teams» vom Juli 2015 stammt[27]. Nach bisherigem Wissen ist «APT10» die einzige Hacker-Gruppe, die diese spezifische Malware einsetzt. Mit Hilfe von gezielten E-Mails wurden unter anderem die zwei bekannten Schadsoftwaretypen «PluX» und «Poison Ivy» verteilt. Die Mails enthielten als Worddokument getarnte Dateien mit einem Icon, das nach dem Anklicken die Schadsoftware herunterlud. Die E-Mails mit vorgetäuschten Absenderadressen und aktuellen Betreffzeilen wie beispielsweise «The impact of Trump's victory to Japan» wurden zwei Tage nach den US-amerikanischen Präsidentschaftswahlen gezielt an Mitarbeitende von japanischen Pharmaunternehmen sowie an die US-amerikanische Niederlassung einer japanischen Firma verschickt.[28]

Die in der zweiten Kampagne angegriffenen MSP unterstützen grosse Organisationen beim Betreuen ihrer IT-Infrastruktur. Sie sind ein attraktives Ziel, da sie direkte Zugriffsrechte auf Systeme und Daten ihrer Kunden haben. Vermutlich waren die MSP nicht das eigentliche Ziel, sondern dienten nur dazu, sich Zugang zu Netzwerken zahlreicher grosser Unternehmen zu verschaffen. Dies zeigt deutlich, dass man auch deshalb seine Partner sorgfältig auswählen sollte. Dies insbesondere, wenn die Sicherheit an ein externes Unternehmen ausgelagert wird.

MSPs wurden unter anderem mit dem Spionagetool «PlugX» angegriffen, das von diversen Gruppen eingesetzt wird. Ebenfalls verwendet wird der kürzlich entwickelte Backdoor-Virus «RedLeaves».

---

[27] vgl. Halbjahresbericht 2/2015, Kap. 5.1.1 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2-2015.html (Stand: 31. Juli 2017).

[28] https://researchcenter.paloaltonetworks.com/2017/02/unit42-menupass-returns-new-malware-new-attacks-japanese-academics-organizations/ (Stand: 31. Juli 2017).

«APT10» greift aber nicht nur mit neuen Tools an, auch die Command and Control-Infrastruktur wurde in der Berictsperiode erheblich erweitert. Das legt den Schluss nahe, dass diese Gruppe sehr professionell ist und ihr grosse finanzielle Mittel zur Verfügung stehen. Ausserdem ist auch das Zielspektrum stark erweitert worden: So werden nicht mehr nur der US-amerikanische Verteidigungssektor oder die Technologie- und Kommunikationsbranche angegriffen, sondern auch verschiedene andere Industriebranchen auf der ganzen Welt. Betroffen waren Systeme in Grossbritannien, den USA, in Indien, Japan und anderen Ländern.

5.1.2 Geschwisterpaar spioniert 16‘000 Personen aus

Cyber-Spionage und Diebstahl sensibler Daten hochrangiger Politiker sind seit dem Cyber-Angriff auf die Parteileitung der Demokraten in den USA populär geworden (vgl. Kapitel 6.2). So wurden auch italienische Politiker Opfer eines ähnlichen Angriffs. In diesem Fall war aber keine ausländische Regierung für den Angriff verantwortlich. Am 10. Januar 2017 wurde das italienische Geschwisterpaar Giulio und Francesca Maria Occhionero verhaftet.

Bei der eingesetzten Malware handelt es sich um eine Eigenkreation einer ausführbaren, portablen und versteckten Win32PE-Datei. Obwohl sie von unerfahrenen Kriminellen entwickelt wurde, die sich nicht um ihre eigene Sicherheit kümmerten, blieb sie ungefähr drei Jahre lang unentdeckt und spionierte 16‘000 Personen aus. Der Angriff flog auf, als der Sicherheitsverantwortliche der ENAV (Nationale Gesellschaft für Flugassistenz) sich aufgrund einer verdächtigen E-Mail, welche die Malware verbreitete, an die italienische Postpolizei wandte. Die mutmasslichen Täter und Entwickler der Malware hatten bei der Registrierung der IP-Adressen sowie beim Datendiebstahl Spuren hinterlassen. So konnte die Polizei die Namen der Verantwortlichen ausfindig machen. Da die Geschwister ausserdem ihre Kommunikation über WhatsApp führten, die zu diesem Zeitpunkt noch unverschlüsselt war, konnte der Verdacht bestätigt werden.

Die Kampagne richtete sich gegen Regierungs- und Wirtschaftsvertreter. Berühmte Opfer sind Italiens Ex-Premier Matteo Renzi, Mario Draghi, Präsident der Europäischen Zentralbank, sowie Persönlichkeiten aus dem Vatikan. Ebenfalls attackiert wurden Mitglieder einer Freimaurer-Loge. Das IT-Sicherheitsunternehmen Trendmicro schätzt, dass die Geschwister auf diese Weise rund 87 Gigabyte sensibler Daten entwenden konnten. Die aus dem Finanzbereich stammenden Daten hätten die Geschwister zu ihren Gunsten nutzen können, da sie Besitzer des Finanzberatungsunternehmens «Westland Securities» waren. Es bleibt noch zu klären, ob und an wen die Informationen hätten verkauft werden sollen.

5.1.3 Kaspersky-Topmanager in Russland wegen Landesverrats festgenommen

Online-Aktivitäten können gefährlich sein. Diese ziemlich allgemeine Behauptung gilt jedoch nicht nur für potenzielle Opfer oder Kriminelle. Auch Forscher im Bereich Informationssicherheit leben manchmal gefährlich, wenn sie sich mit Informationen über die Sicherheit bestimmter Staaten befassen. Ruslan Stoyanov kann dies bestätigen: Er war bei Kaspersky für die «Computer Incidents Investigation» verantwortlich und wurde Ende 2016 verhaftet und des Landesverrats angeklagt. Das bekannte Unternehmen für Cyber-Sicherheit distanzierte sich von diesem Vorfall und teilte mit, dass «unser Mitarbeiter aufgrund von

Vorfällen verhaftet wurde, die sich vor seiner Anstellung bei Kaspersky ereignet hatten.» [29]. Die russischen Behörden haben die Verhaftung nicht näher kommentiert. Offenbar wird Stoyanov aber vorgeworfen, US-amerikanischen Unternehmen geheime Informationen preisgegeben zu haben, unter anderem an den IT-Dienstleister «Verisign», welcher seinerseits die Informationen an die Geheimdienste der USA weitergegeben haben soll. Dasselbe Verbrechen wird auch dem Vizechef der Cyber-Division des russischen Geheimdienstes FSB, Sergei Mikhailov, und einem weiteren Mitarbeiter, Dmitry Dokuchayev, vorgeworfen. Der Vizedirektor von «Verisign» dementierte, dass die Berichte, die den Regierungsbehörden oder anderen Kunden übergeben wurden, Staatsgeheimnisse enthalten haben könnten, äusserte sich aber nicht konkret zum Fall Stoyanov.

5.1.4 APT32 – Spionage aus Vietnam?

Manchmal kommen Spionagekampagnen auch aus Regionen, die weniger im Fokus solcher Vorfälle stehen. Dies gilt beispielsweise für die Gruppe «OceanLotus», die 2014 von «SkyEye Labs» entdeckt worden ist. Bekannt wurde sie jedoch erst kürzlich durch eine Recherche der Sicherheitsfirma «FireEye» und trägt seither den Namen «APT32». Die Hacker sind wahrscheinlich schon seit 2013 aktiv und ihre Aktionen scheinen den Interessen Vietnams zu dienen. Ziel der Angriffe waren nicht nur diverse Unternehmen mit wirtschaftlichen Interessen in Vietnam, dem Gesundheitswesen, einige vietnamesische Medien und ausländische – vor allem die chinesische – Regierungen, sondern auch Dissidenten und Aktivisten. «FireEye» hat zwölf massive Angriffe festgestellt.

«APT32» arbeitet mit Schadsoftwarepaketen, die an handelsübliche Programme angehängt werden. Anhand der angegriffenen Ziele lässt sich vermuten, dass eine staatliche Organisation die Hand im Spiel hat. Die vietnamesische Regierung erklärte jedoch, keine Kenntnis von den Tätigkeiten von «OceanLotus» zu haben.

Für die jüngsten Angriffe hat die Gruppe «APT32» Microsoft-Dokumente mit schädlichen Makros verwendet, die via E-Mail an die Opfer versendet wurden. Die Angriffe richteten sich gegen die vietnamesische Niederlassung einer weltweit tätigen Beratungsfirma, gegen die Angehörigen der vietnamesischen Diaspora in Australien, gegen Angestellte der philippinischen Regierung sowie gegen die vietnamesischen Niederlassungen zweier Produzenten von Konsumgütern in den Philippinen und den USA. Die Angreifer verwendeten einfache Social-Engineering-Techniken, um die Opfer davon zu überzeugen, die Makros zu aktivieren.

5.1.5 Missbrauch von kommerzieller Überwachungssoftware

«Pegasus» ist ein ausgeklügeltes Spionageprogramm (Spyware), das spezifisch für Mobiltelefone entwickelt wurde und in der Lage ist, sowohl iOS- als auch Android-Systeme zu infiltrieren. Es wurde von der israelischen Überwachungsfirma NSO entwickelt und wird nur an staatliche Institutionen für die Bekämpfung von Terrorismus und Kriminalität verkauft. Mit «Pegasus» lassen sich sämtliche Aktivitäten eines mobilen Geräts überwachen. Der Verdacht hat sich allerdings erhärtet, dass die Spyware der NSO in einigen Fällen auch für wirtschaftliche Partikularinteressen und nicht für die dafür vorgesehenen Zwecke verwendet wurde.

---

[29] http://www.forbes.com/sites/thomasbrewster/2017/01/25/russia-kaspersky-treason-arrest/#1ce5f9174a68 (Stand: 31. Juli 2017).

Bereits im August 2016 berichteten die Sicherheitsunternehmen «Citizen Lab» und «Lookout Security»[30] über Ahmed Mansoor, einen bekannten Menschenrechtsaktivisten aus den Vereinigten Arabischen Emiraten. Er wurde Opfer dieser Spionagesoftware. In Mexiko soll die Software in zwei unterschiedlichen Operationen eingesetzt worden sein.

Zwischen Juli und August 2016 nahm «Pegasus» einen wichtigen Wissenschaftler des Mexican National Institute for Public Health (INSP) sowie die Direktoren zweier mexikanischer NGOs ins Visier, die sich in der Bekämpfung des Übergewichts engagierten. Alle drei Zielpersonen unterstützten die sogenannte Soda Tax, eine Massnahme, die zur Einschränkung des Konsums gezuckerter Getränke führen soll und 2014 eingeführt worden war. Die Steuer führte wie erhofft zu einem Rückgang des Verkaufs solcher Produkte, was im Lebensmittelsektor erwartungsgemäss Unzufriedenheit auslöste. Im Juni 2017 machte «Citizen Lab» in einem Artikel publik, dass versucht werde, Journalisten, Anwälte und Aktivisten, die sich für die Menschenrechte einsetzten oder die Korruption der mexikanischen Regierungsbehörden untersuchten, mit Schadsoftware anzugreifen.[31] Der grösste Teil der Infizierungsversuche fand im August 2015 sowie zwischen April und Juli 2016 statt, als sich die oben erwähnten Vorwürfe an die Adresse des Präsidenten und der Regierung häuften. Beide Male handelte es sich um gezielte Angriffe, die über SMS verbreitet worden waren. Mit Social-Engineering-Techniken versuchten die Angreifer, die Empfängerinnen und Empfänger dazu zu bringen, auf einen Link zu klicken, hinter dem sich ein Spionageprogramm verbarg. Wenn die Zielperson nicht auf die Versuche hereinfiel, wurden die Familienmitglieder ins Visier genommen. So erhielt die Frau eines Anti-Korruptions-Aktivisten eine SMS mit einem Link auf vermeintliche fotografische Beweise, dass ihr Ehemann sie betrüge.

5.2 Datenabflüsse

Nach den rekordverdächtigen Datenabflüssen während des Jahres 2016, wie die halbe Milliarde Kundendatensätze bei «Yahoo»[32] oder die über 100 Millionen Zugangsdaten zum beruflichen Kontaktnetzwerk «LinkedIn»[33], wurden auch zu Beginn des neuen Jahres Meldungen zu abhanden gekommenen Personendaten publik. In Kapitel 6.3 beleuchten wir zudem die rechtlichen Änderungen in Europa im Rahmen der «EU general data protection regulation (GDPR)», welche auch Veränderungen im Umgang mit derartigen Vorfällen nach sich ziehen wird.

5.2.1 Ungewollte Transparenz bei Wählerprofilen der US-Republikaner

Von den Republikanern im US-Wahlkampf 2016 beauftragte Unternehmen sollten potenzielle Wähler ausforschen. Diese Firmen nahmen es mit der Absicherung der Server, auf denen

---

30 https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/ (Stand: 31. Juli 2017).

31 https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/ (Stand: 31. Juli 2017).

32 Siehe MELANI Halbjahresbericht 1/2016, Kapitel 5.2.1 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2016-1.html (Stand: 31. Juli 2017).

33 Siehe MELANI Halbjahresbericht 2/2015, Kapitel 5.2.2 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2-2015.html (Stand: 31. Juli 2017).

die Daten zu liegen kamen, anscheinend nicht so genau. Forscher der Firma «Upgard»[34] fanden die zusammengestellten Datensätze ungesichert auf einem Cloud-Server der Firma «Deep Root Analytics». 1.1 Terabytes an Daten, die von diesem und zwei weiteren Vertragspartnern gesammelt worden waren, lagerten für jedermann frei zugänglich in der «Amazon»-Cloud. Darunter persönliche Informationen wie Namen, Geburtsdaten, Adressen, Telefonnummern und Details der Wählerregistrierung sowie die durch die Firmen modellierten Ethnien- und Religionszugehörigkeiten von über 198 Millionen US-amerikanischen Wählerinnen und Wählern. Dies entspricht fast der kompletten Wählerbasis der USA. «Deep Root Analytics» nannte gegenüber der Zeitung «The Intercept[35]» einen Konfigurationsfehler in den Zugriffsrechten als Ursache des Datenlecks.

5.2.2 Vor DDoS geschützt, dafür vertrauliche Speicherinhalte verteilt

Die Firma «Cloudflare» hat sich mit ihrem Schutz gegen DDoS-Angriffe einen Namen gemacht. Infolge einer Fehlkonfiguration der Serversoftware wurden jedoch teilweise sensible Speicherinhalte von Drittseiten an die Besucher anderer Kunden verteilt. Tavis Ormandy, ein Sicherheitsforscher beim «Google Project Zero», bemerkte, dass während mehreren Monaten bei Aufrufen von Seiten, denen das «Content Delivery Network Cloudflare»[36] vorgeschaltet war, neben den angefragten Webseiten auch geheime Informationen von anderen Kunden publiziert wurden. Der Fehler wurde in Anlehnung an den SSL-Bug Heartbleed auf Social Media auch als Cloudbleed betitelt.

Ormandy ist bekannt dafür, dass er sich vor allem Firmen vornimmt, die selbst versprechen, vor Gefahren im Internet zu schützen. Cloudflare erklärte, es gebe keine Anzeichen, dass neben dem Google-Forscher weitere Personen den Fehler bemerkt hätten. Es bleibt das Risiko, dass Daten in Caches von Suchmaschinen und Webdiensten, welche die Seiten indiziert haben, weiterhin für Unberechtigte einsehbar sind.

5.2.3 Abgeflossene Personendaten dämpfen Vertrauen in Indische E-ID

Um die Geldflüsse im Land transparenter zu gestalten, möchte Indien Anreize schaffen, weniger Bargeld- und mehr Kartenzahlungen zu tätigen. Dazu dient das vor acht Jahren etablierte Online-Identitäts-Projekt «Aadhaar», welches die Basis für die Datenbank der eindeutigen Identitäten (UID) verwaltet, die zur Authentisierung und Autorisierung von Kartenzahlungen eingesetzt wird.

Das Indische «Center for Internet and Society (CIS)»[37] machte publik, dass 135 Millionen Karten-Datensätze abgeflossen sind, die mit 100 Millionen Bankkonten verknüpft sind. Für

---

34 https://www.upguard.com/breaches/the-rnc-files?utm_campaign=RNC%20Files&utm_source=upguard_home&utm_medium=breakingnewsbanner, (Stand: 31. Juli 2017).

35 https://theintercept.com/2017/06/19/republican-data-mining-firm-exposed-personal-information-for-virtually-every-american-voter/ (Stand: 31. Juli 2017).

36 Ein «Content Distribution Network» ist ein Netz regional verteilter und über das Internet verbundener Server, mit dem Inhalte, insbesondere grosse Mediendateien ausgeliefert werden

37 http://cis-india.org/internet-governance/information-security-practices-of-aadhaar-or-lack-thereof-a-documentation-of-public-availability-of-aadhaar-numbers-with-sensitive-personal-financial-information-1 (Stand: 31. Juli 2017).

den Datenabfluss verantwortlich ist nicht die eigentliche «Aadhaar»-Datenbank. Das Problem liegt bei mindestens vier Regierungsprojekten, die «Aadhaar»-Daten mit eigenen Informationen anreichern.

Der Vorfall zeigt exemplarisch die Risiken, die mit dem Einsatz von eindeutigen Online-Identitäten einhergehen und unbedingt grösstmöglich eingegrenzt werden müssen. Für die Nutzer kann eine kleine Fahrlässigkeit bei einem der Partner gravierende Schäden der Privatsphäre verursachen und das Vertrauen in dieses Projekt für lange Zeit schwächen.

5.3 Industrielle Kontrollsysteme (IKS)

Neue Erkenntnisse zur eingesetzten Malware, welche im Dezember 2016 zum zweiten Mal mitverantwortlich für einen Stromausfall in der Ukraine war[38], stehen im Zentrum dieses Kapitels. Aber auch Fernseher, Sirenen, Überwachungskameras und Hotelzimmertüren, welche man ebenfalls unter dem Begriff «Industrielle Kontrollsysteme» subsumieren kann, zählen im ersten Halbjahr 2017 zu den Opfern.

Auch bei Betreibern von industriellen Kontrollsystemen wird laufend Schadsoftware entdeckt. Eine Studie des Projektes «MIMICS (Malware in Modern Industrial Control Systems)»[39] der Cyber Security Firma «Dragos», welche im IKS Umfeld aktiv ist, kommt zum Schluss, dass Betreiber industrieller Kontrollsysteme mit denselben Schadsoftware-Typen zu kämpfen haben, wie die übrigen Unternehmen. Ein reiner E-Banking Trojaner kann zwar in einem Kontrollsystem wenig anrichten. Hingegen kann eine Ransomware, wenn für den Betrieb notwendige Dateien verschlüsselt werden, das Gerät oder ganze Systeme inoperabel machen. So waren aktuell beispielsweise Smart-Fernseher[40] oder Überwachungskameras[41] in Washington DC Opfer von Verschlüsselungstrojanern. Grossen Schaden richtete auch die Malware «Brickerbot»[42/43] an, die verwundbare Geräte im Internet der Dinge in zerstörerischer Manier lahmlegte. All diese Angriffe sind für die Betroffenen sicher gravierend, sind aber eigentlich keine expliziten Angriffe auf die Funktion der jeweiligen Kontrollsysteme.

5.3.1 Industroyer/CrashOverride – Malware kommuniziert selbstständig mit Unterwerk

Nach der intensiven Berichterstattung[44/45] zu Beginn dieses Jahres wurde es ruhiger um den mutmasslichen Cyber-Angriff auf die Stromversorgung im Norden Kiews im Dezember 2016.

---

38 Siehe MELANI Halbjahresbericht 2/2016, Kapitel 5.3.1 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2016-2.html (Stand: 31. Juli 2017).

39 https://dragos.com/blog/mimics/ (Stand: 31. Juli 2017).

40 https://www.heise.de/security/meldung/Erpresser-Botschaft-in-Dauerschleife-Smart-TV-von-LG-mit-Ransomware-infiziert-3584043.html (Stand: 31. Juli 2017).

41 www.theregister.co.uk/2017/01/30/ransomware_killed_70_of_washington_dc_cctv_ahead_of_inauguration/ (Stand: 31. Juli 2017).

42 https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-102-01A (Stand: 31. Juli 2017).

43 http://www.zdnet.com/article/homeland-security-warns-of-brickerbot-malware-that-destroys-unsecured-internet-connected-devices/ (Stand: 31. Juli 2017).

44 http://www.bbc.com/news/technology-38573074 (Stand: 31. Juli 2017).

Die involvierten Sicherheitsforscher waren aber in der Zwischenzeit intensiv daran, den Ursachen hinter dem Stromausfall auf die Spur zu kommen. Am 12. Juni publizierten der Security-Dienstleister «ESET» und die auf Informationssicherheit in industriellen Kontrollsystemen spezialisierte Firma «Dragos» koordiniert die Resultate der untersuchten Malwaresamples, denen sie die Namen «Industroyer»[46] respektive «Crashoverride»[47] gaben. «Crashoverride» ist das erste bekannte Malware-Framework, dass explizit zum Angriff auf Stromnetzwerke entworfen wurde. Nach «Stuxnet», «Havex» und «Blackenergy 2» ist es erst die vierte auf industrielle Kontrollsysteme massgeschneiderte Schadsoftware. Neben «Stuxnet» ist «Crashoverride» sogar erst die zweite Schadsoftware, die den physikalischen Prozess autonom beeinflussen kann. Wie Abbildung 8 zeigt, ist die Launcher-Komponente befähigt, vier verschiedene Module zur Beeinflussung industrieller Protokollkommunikation auszuführen, die häufig im Betrieb von Stromnetzen anzutreffen sind. Dabei ist das Framework modular aufgebaut, so dass mit vertretbarem Aufwand auch weitere Protokolle für künftige Ziele integriert werden können. «Dragos» nennt den Akteur hinter der Schadsoftware «ELECTRUM», der nach Aussagen von «Dragos»-Analysten Verbindungen zur Gruppe «Sandworm» aufweist. Diese wiederum wird von verschiedenen Sicherheitsdienstleistern[48] für die Angriffe auf die Stromversorgung in der Ukraine in den Jahren 2015 und 2016 verantwortlich gemacht.

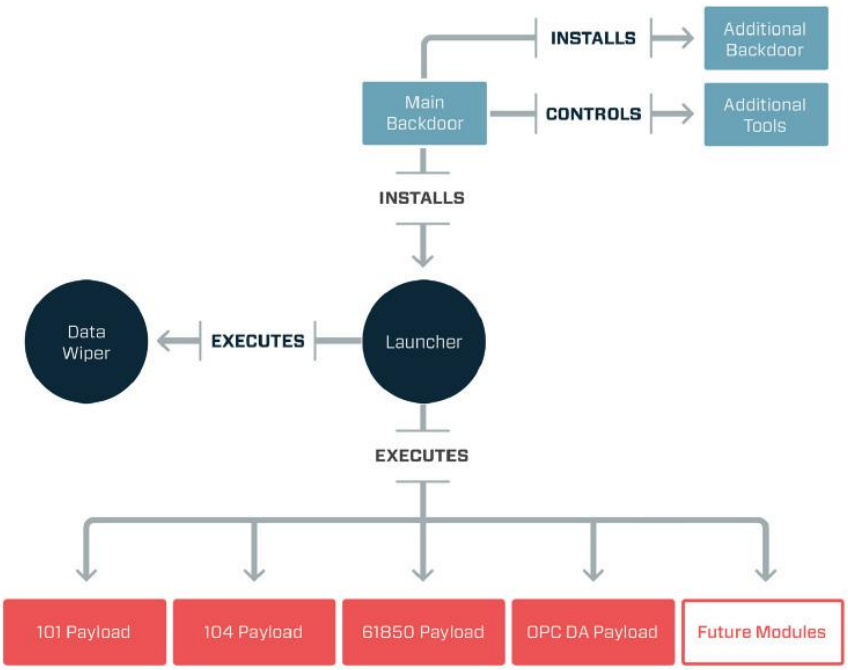


Abbildung 8: Schematischer Aufbau und Zusammenspiel der «Crashoverride» Module (Quelle: *https://dragos.com/blog/crashoverride/)*

---

45 https://nakedsecurity.sophos.com/2017/01/16/ukraine-power-outages-the-work-of-cyberattackers-warn-experts/ (Stand: 31. Juli 2017).

46 https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/ (Stand: 31. Juli 2017).

47 https://dragos.com/blog/crashoverride/ (Stand: 31. Juli 2017).

48 https://www.wired.com/story/russian-hackers-attack-ukraine/ (Stand: 31. Juli 2017).

5.3.2 Funkhacker lassen um Mitternacht die Alarmsirenen in Dallas ertönen

Jeweils am ersten Mittwoch im Februar findet am Mittag in der Schweiz der jährliche Sirenentest statt, damit die Alarmierung der Bevölkerung im Falle einer Katastrophe auch sicher funktioniert. Dass am 7. April 2017 kurz vor Mitternacht in der Stadt Dallas die Sirenen während 95 Minuten vor nicht existenten Tornados warnten, war keineswegs auf einen Test zurückzuführen. Zuerst ging man von einem Angriff auf die Systeme der Blaulichtorganisationen der texanischen Stadt aus. Die Behörden konnten jedoch bald mitteilen, dass niemand in die Netzwerke eingedrungen sei. Grund des Fehlalarms war, dass sich die Sirenen über Funksignale steuern lassen, die im Ereignisfall vom nationalen Wetterdienstes ausgesendet werden. Diese Funksignale sind jedoch bei älteren Sirenen nicht speziell gesichert oder gar verschlüsselt, sondern werden offen übermittelt. Geräte, die solche Funkwellen, so genannte «Software Defined Radios (SDR)», aussenden können, werden immer erschwinglicher. Praktisch jedermann kann diese Geräte einsetzen, weshalb es nur eine Frage der Zeit war, bis diese Systeme missbraucht werden. Der Angreifer musste nur sämtliche möglichen Befehle auf der entsprechenden Frequenz durchprobieren. Den Erfolg dieser Methode werden die geplagten Ohren der Anwesenden in Dallas bestätigen.

5.3.3 Das verschlüsselte Schloss

Viele Hotels haben keine klassischen Schlüssel mehr, sondern geben den Gästen eine Karte ab, auf welcher der Öffnungscode des entsprechenden Zimmers gespeichert ist. Der Vorteil liegt auf der Hand. Neben dem handlicheren Umgang für die Gäste können bei einem Verlust des Zimmerschlüssels einfach der alte Code revoziert und der Türe ein neuer Code zugewiesen werden. Dass dieser Fortschritt auch seine Schattenseiten hat, musste das Romantik Seehotel Jägerwirt in Österreich erfahren. Das vollausgebuchte Hotel konnte am Eröffnungswochenende plötzlich keine ihrer Zimmertüren mehr öffnen. Grund war eine Infektion mit einer Ransomware[49]. Neben den Buchungs- und Zahlungssystemen wurde auch der Server der Schlüsselkarten verschlüsselt. Somit konnten weder die Zimmertüren entsperrt, noch die Schlüsselkarten umprogrammiert werden. In der Verzweiflung zahlte das Hotel die knapp 1500 Euro Lösegeld in Bitcoin. Die Erpresser entschlüsselten daraufhin die infizierten Geräte, versuchten aber eine Backdoor in den Systemen offen zu halten. Das Hotel tauschte daraufhin einen Teil der Geräte aus und sicherte das Netzwerk zusätzlich ab, was eine weitere Infektion verhindern soll. Nach der unangenehmen Erfahrung mit dem digitalen Schliesssystem plant der Jägerwirt bei der nächsten Renovation, wieder auf herkömmliche Schlüssel umzustellen.

[49] https://www.thelocal.at/20170128/hotel-ransomed-by-hackers-as-guests-locked-in-rooms/ (Stand: 31. Juli 2017).

Schlussfolgerung / Empfehlung:

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

Checkliste mit Massnahmen zum Schutz industrieller Kontrollsysteme

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

5.4 Angriffe (DDoS, Defacements, Drive-By)

5.4.1 Netzwerke von Finanzinstituten während sieben Minuten umgeleitet

Ende April 2017 wurde der Netzwerkverkehr von mehreren Finanzdienstleistern, darunter auch jener der Kreditkartenfirmen «Visa» und «Mastercard», während knapp sieben Minuten über einen russischen Telekomanbieter umgeleitet. Anomalien im so genannten «Border Gateway Protokoll (BGP)» tauchen leider immer wieder auf. BGP regelt den Verkehr zwischen den verschiedenen Teilnetzen des Internet und gibt somit vor, welches Datenpaket über welchen Provider geleitet wird. Auffällig an diesem Fall ist allerdings, dass der fehlerhafte Befehl des russischen Telekomanbieters «Rostelecom» sich alleine auf Adress-Blöcke von Finanzdienstleistern und IT-Sicherheitsunternehmen konzentrierte. Es bestand die Möglichkeit, dass in der Zeit der Fehlleitung Netzwerkverkehr analysiert und schlimmstenfalls gar verändert wurde. Was die Fehlkonfiguration verursachte, ist bislang nicht bekannt. Insbesondere konnte bisher nicht geklärt werden, ob diese Fehlkonfiguration durch einen technischen oder menschlichen Fehler verursacht wurde oder gar auf einen Hackerangriff zurückzuführen ist.[50]

In einem anderen Fall, bei dem ein Grossteil des Netzwerkes einer brasilianischen Bank betroffen war, wurde der Netzwerkverkehr während fünf Stunden komplett übernommen. Den Angreifern gelang es, den DNS-Betreiber der Bank zu kompromittieren und somit gegenüber den meisten Netzwerkteilnehmern als Betreiber der Bankinfrastruktur aufzutreten. Auf diese Wiese könnten Transaktionen ausgespäht, Zugangsdaten abgegriffen und Kunden mit Malware infiziert werden.[51]

5.4.2 Gezielte Infektion über Webseite des polnischen Finanzregulators

Anfang Februar 2017 wurde bekannt, dass auf verschiedenen Computern mehrerer polnischer Banken Schadsoftware gefunden worden war. Als Infektionsvektor gilt die Website des polnischen Finanzregulators KNF, die von Angreifern mit einer so genannten

[50] https://arstechnica.com/information-technology/2017/04/russian-controlled-telecom-hijacks-financial-services-internet-traffic/ (Stand: 31. Juli 2017).

[51] https://www.wired.com/2017/04/hackers-hijacked-banks-entire-online-operation/ (Stand: 31. Juli 2017).

Drive-by-Infektion versehen wurde. Dazu wurde eine der lokalen JavaScript-Dateien so verändert, dass eine weitere externe JavaScript-Datei heruntergeladen wurde, die dann ihrerseits Schadsoftware nachgeladen hat.[52] Durch das alleinige Ansurfen dieser Webseite bestand so die Möglichkeit, dass die Computer der Besucher mit einer Schadsoftware infiziert wurden. Da auf den Finanzregulator mehrheitlich Personen im Finanzumfeld zugreifen, dürfte der Angreifer einen sehr gezielten Angriff geplant haben. Anschliessend versuchte die Schadsoftware Verbindung mit ausländischen Servern aufzunehmen. Gemäss dem Portal «BadCyber» gelang es den Angreifern in einigen Fällen, Zugriff auf Computer in Bankinfrastrukturen zu erhalten.[53]

Es stellte sich heraus, dass der gezielte Attacke auf polnische Finanzinstitute nur ein Teil des Angriffs war. So fand man auch auf der Website der mexikanischen Banken- und Börsenaufsicht eine Webseiteninfektion des gleichen Typs. Das Exploit-Kit war so konfiguriert, dass nur Besucher infiziert wurden, die die Seite mit einer von 150 vordefinierten IP-Adressen ansurften. Diese 150 IP-Adressen konnten zu 104 verschiedenen Organisationen in 31 Ländern zugeordnet werden. Der Grossteil dieser Firmen sind Banken, ein kleinerer Teil gehört zu Telekom- und Internetfirmen. Schweizer Organisationen waren gemäss aktuellem Kenntnisstand keine betroffen. Die Angriffe konnten dabei bis mindestens Oktober 2016 zurückverfolgt werden.

Die bislang unbekannte Schadsoftware «Ratankba»[54] lud – nachdem sie mit dem Steuerserver Kontakt aufgenommen hatte – ein Hacktool herunter, welches mit «Lazarus» in Verbindung gebracht wird. Die «Lazarus» Gruppe wird mit Angriffen gegen US-amerikanische und Südkoreanische Ziele in Verbindung gebracht, die seit 2009 stattfinden. Ebenfalls wird «Lazarus» für den Angriff auf die Nationalbank in Bangladesch im Jahre 2016 in Verbindung gebracht.[55] Weitere Analysen von «Kaspersky» belegen, dass die Gruppe «Lazarus» eine eigene Subgruppe unterhält, die speziell auf Angriffe gegen das Finanzsystem ausgerichtet ist. Die Gruppe tauchte in der Vergangenheit ebenfalls unter dem Namen «BlueNorof» auf. Die Hartnäckigkeit und Ausdauer des Akteurs wird den internationalen Finanzmarkt wohl auch in Zukunft nicht verschonen.

5.4.3 Botnetz streut Gerüchte zur Marktmanipulation

«Necurs» ist ein klassisches Botnetz zum Versand von Spam-Nachrichten und ist bekannt für die breite Verteilung der Ransomware «Locky» oder des E-Banking-Trojaners «Dridex». Gemäss MELANI-Statistik belegt «Necurs» den siebten Platz bei den meistverbreiteten Schadprogrammen in der Schweiz.[56] In der Berichtsperiode wurde beobachtet, wie Betrüger

---

52 https://badcyber.com/several-polish-banks-hacked-information-stolen-by-unknown-attackers/ (Stand: 31. Juli 2017).

53 https://www.theregister.co.uk/2017/02/06/polish_banks_hit_by_malware_sent_through_hacked_financial_regulator/ (Stand: 31. Juli 2017).

54 https://www.symantec.com/connect/blogs/attackers-target-dozens-global-banks-new-malware-0 (Stand: 31. Juli 2017).

55 Siehe MELANI Halbjahresbericht 1/2016, Kapitel 5.4.1 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2016-1.html

56 Siehe aktueller MELANI Halbjahresbericht 1/2017, Kapitel 4

den Spam-Versand zur Manipulation von Penny-Stock-Börsenkursen verwendet haben[57]. In einer von «Necurs» versendeten Spam-Welle wurde eine angebliche Übernahme im Drohnenmarkt angekündigt. Die Empfänger, welche der Versuchung eines schnellen Gewinns nicht wiederstehen konnten, kauften anschliessend Anteile der beworbenen Firma und trieben so deren Aktienkurs in die Höhe. Die Angreifer hatten bereits vor dem Spam-Versand Anteile der Firma gekauft und verkauften diese nach dem selbstverursachten Höhenflug der Aktie mit einem satten Gewinn. Das Beispiel dieses «Pump and Dump»-Angriffs zeigt auf, wie Internet-Kriminelle immer wieder neue Wege suchen, ihre Infrastruktur und Fähigkeiten finanziell gewinnbringend einzusetzen – dabei aber auch auf altbekannten Pfaden wandeln.

5.4.4 Patientendatenbank in den Händen von Erpressern

Nach den Schäden, die «WannaCry» bei Spitälern vor allem in Grossbritannien angerichtet hat, zeigt auch ein Vorfall in einer Klinik für plastische Chirurgie in Litauen, wie sensibel Patientendaten sind und wie wichtig es ist, diese entsprechend zu schützen. Die Angreifer, die sich selber «Tsar Team» nennen, erpressten die Kunden dieser Klinik in über 60 Ländern mit der Publikation von Patientenfotos, welche sie zuvor aus der Datenbank der Klinik kopiert hatten. Als Beweis wurden 25‘000 dieser Fotos im Internet publiziert[58]. Bevor die Erpresser die Kunden einzeln mit Forderungen zwischen 50 und 2‘000 Euro kontaktierten, versuchten sie, die gesamte Datenbank für eine halbe Million Pfund in Bitcoins an die Klinik zu verkaufen. Diese ging auf die Forderung der Erpresser nicht ein. Wieviele Kunden den Erpressern die Lösegeldsumme bezahlt haben, ist nicht bekannt. Der Name «Tsar Team» taucht auch in Zusammenhang «Sofacy». Eine Verbindung konnte allerdings bisher nicht bestätigt werden. Es ist auch denkbar, dass die Angreifer den bekannten Namen der Spionagegruppe lediglich nutzen, um überzeugender Druck auf die Opfer ausüben zu können.

5.4.5 SS7 – Alter Standard für E-Banking-Authentifizierung

Um sich bei einem Internetdienst wie E-Banking sicher anmelden zu können, wird neben dem Passwort mindestens ein weiterer Authentifizierungsmechanismus eingesetzt. Idealerweise läuft dieser über einen zweiten, unabhängigen Kommunikationskanal. Viele Anbieter setzen hier auf SMS via Mobiltelefon. Da die meisten Mobiltelefone heutzutage kleine Computer sind, können sie mit Schadsoftware infiziert werden, die unter anderem die Nachrichten abfangen und an die Betrüger weiterleiten können. Zudem werden Bankgeschäfte heute vielfach direkt mit dem Smartphone getätigt, so dass Login und Zweitauthentifizierung über das gleiche Gerät erfolgen. Damit fehlt die zusätzliche Sicherheit, die die SMS-Authentifizierung bieten sollte. MELANI behandelte bereits im letzten Halbjahresbericht die Problemfelder, welche durch den Einsatz von SMS als zweiten Faktor bei der Authentifizierung entstehen.[59]

---

57 http://blog.talosintelligence.com/2017/03/necurs-diversifies.html (Stand: 31. Juli 2017).

58 https://www.theguardian.com/technology/2017/may/31/hackers-publish-private-photos-cosmetic-surgery-clinic-bitcoin-ransom-payments?CMP=twt_gu (Stand: 31. Juli 2017).

59 Siehe 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 2017).

Anfang März 2017 wurde durch Kriminelle eine weitere Möglichkeit aktiv ausgenutzt, von der Bank zwecks Authentifizierung versendete SMS abzufangen. Wie der deutsche Mobilfunkanbieter «O_2» gegenüber der «Süddeutschen Zeitung» bestätigte, wurde eine seit Jahren bekannte Schwachstelle im SS7-Protokoll benutzt, um missbräuchliche Transaktionen von deutschen Bankkonten zu ermöglichen.[60] Die Kriminellen missbrauchten dazu eine Funktion in den Protokollen von SS7, welche eigentlich dazu da ist, das internationale Roaming zu ermöglichen. Mobiltelefone können sich im Ausland bei einem fremden Netz anmelden, der entsprechende ausländische Netzanbieter meldet diesen Vorgang ins Heimatnetz des Abonnenten und SMS-Nachrichten werden anschliessend ans fremde Netz übermittelt. Dieser Vorgang kann vorgetäuscht werden, ohne dass sich das Mobiltelefon im Ausland befindet: Die SMS werden dann zu Netzbetreibern im Ausland umgeleitet und können dort ausgelesen werden. Das funktioniert, weil das zugrunde liegende sogenannte SS7-Protokoll ursprünglich offen konzipiert wurde. Man ging von einem Grundvertrauen zwischen allen Mobilfunkprovidern aus. Mit der wachsenden Zahl an Anbietern in aller Welt besteht aber mittlerweile die Möglichkeit, dass sich einzelne Firmen nicht an die Regeln halten und unter Umständen betrügerische Aktivitäten zulassen oder mit Betrügern zusammenarbeiten.

Schlussfolgerung:

In einigen Ländern ist die Einstiegshürde für dubiose Netzteilnehmer deutlich gesunken. Gleichzeitig führen nicht alle Mobilfunkbetreiber Plausibilitätsprüfungen durch. Diese Problematik wird seit 2014 immer wieder thematisiert. Um die Authentifizierung per SMS auf Netzwerkebene auszuhebeln, bedarf es allerdings noch besonderer Fachkenntnisse. Gut organisierte kriminelle Gruppierungen und staatliche Akteure verfügen jedoch schon heute über die nötigen Fähigkeiten. Für Betrug im E-Banking bleibt die gleichzeitige Infektion von Computer und Smartphone eines Nutzers wohl die gängigere und lukrativere Methode. Alleine deshalb werden Anbieter von Online-Diensten mittelfristig zu alternativen Authentifizierungsmethoden wechseln.

5.5 Präventive Massnahmen

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

5.5.1 Deutsche Telekom-Ausfall durch «Mirai»: Verhaftung

Im letzten Halbjahresbericht wurde ausführlich über das «Mirai»-Botnetz berichtet.[61] «Mirai» ist eine Schadsoftware gegen das Betriebssystem «Linux», das in vielen Geräten des Internet of Things (IoT) verwendet wird. Ein Angriff mit dieser Schadsoftware führte am 27. November 2016 zum Ausfall des Internets bei 900‘000 Kunden der «Deutschen Telekom». Grund des Ausfalls war der Einsatz einer neuen Version der Schadsoftware, die aufgrund

[60] https://www.theregister.co.uk/2017/05/03/hackers_fire_up_ss7_flaw/ (Stand: 31. Juli 2017).

[61] Siehe MELANI Halbjahresbericht 2/2016, Kapitel 3 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2016-2.html (Stand: 31. Juli 2017).

einer fehlerhaften Programmierung Heimnetzwerkrouter der «Deutschen Telekom» zum Absturz gebracht hat, anstatt diese zu infizieren.

Ein Hacker aus Liberia, welcher hinter dieser einen Attacke stand, wurde mittlerweile in London verhaftet. Seine Erklärungen zeigen eindrücklich, wie mehrdimensional und komplex die Hintergründe einer solchen Tat sind. Der Verhaftete erklärte, er sei von einem liberianischen Telekommunikationsunternehmen angegangen worden, Konkurrenzfirmen zu sabotieren. Um einen DDoS-Angriff durchzuführen, hatte er danach den frei verfügbaren Schadcode des «Mirai»-Botnets adaptiert und diesen um eine neue Angriffsroutine ergänzt, welche die Fernwartungsfunktion bestimmter Router ausnutzen kann. Genau diese neu implementierte Funktion sorgte dann anscheinend für den Absturz der Router bei der «Deutschen Telekom». Auch pries der Angeklagte sein Botnetz im Internet zur Vermietung an. Vor Gericht sagte er jedoch, dass dies nur ein Ablenkungsmanöver seines effektiven Auftraggebers gewesen sei. Er selbst habe auf einen Job beim Auftraggeber gehofft. In der Tat wurde der liberianische Provider «Lonestar Cell» im Januar 2017 attackiert, was zu einem teilweisen Ausfall des Mobilfunkempfangs und zu einer Überlastung des Unterseekabels nach Afrika führte.

Das deutsche Gericht nahm ausschliesslich Bezug auf den Angriff auf die «Deutsche Telekom» und verurteilte den Angreifer deshalb nur zu einem Jahr und acht Monaten Freiheitsstrafe auf Bewährung. Allerdings kam er dennoch nicht auf freien Fuss, sondern landete in Auslieferungshaft. Die britischen Behörden werfen ihm nämlich ein Vielfaches vor. Neben dem bereits erwähnten Angriff auf «Lonestar Cell» soll er auch britische Grossbanken um fünfstellige Beträge erpresst haben.

5.5.2 Schwarzhändler von Apple-internen Kundendaten verhaftet

Die chinesische Polizei hat über zwanzig Mitarbeitende von Apple-Partnern verhaftet, die angeklagt werden, Kundendaten des iPhone-Herstellers gestohlen und dann auf dem Schwarzmarkt verkauft zu haben[62]. Die Angestellten, die hauptsächlich im Verkauf und Marketing tätig waren, griffen auf Datenbanken mit Informationen über iPhone- und iPad-Nutzer zu. Die Daten enthielten unter anderem Namen, Mobilfunknummern und AppleIDs. Die Täter boten diese Daten zu Preisen zwischen 1.50 und 26.50 US-Dollar pro Datensatz an interessierte Käufer im digitalen Untergrund an. Bis zu ihrer Verhaftung kamen über sieben Millionen US-Dollar aus dem Verkauf zusammen. Solche Insider-Angriffe zeigen deutlich auf, dass nicht nur präventive Schutzmassnahmen gegen Angreifer ausserhalb der eigenen Organisation, sondern auch interne Prozesse und Systeme zur Erkennung von laufenden Attacken implementiert werden müssen, um die eigenen Daten zu schützen.

62 https://www.tripwire.com/state-of-security/latest-security-news/apple-employees-detained-selling-user-data-chinese-black-market/ (Stand: 31. Juli 2017).

Ein guter Anfang, nicht Opfer solcher oder ähnlicher Angriffe zu werden, ist das MELANI-Merkblatt über IT-Sicherheit in KMUs:

Merkblatt IT-Sicherheit für KMUs

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

KMU-Portal des Bundes

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

6 Tendenzen und Ausblick

6.1 Die Rolle der Versicherungen im Cyber-Bereich

Wer sich in der Verordnung über die technischen Anforderungen an Strassenfahrzeuge (VST) etwas kundig macht, dem fällt auf, dass Türen zwar gegen «ungewolltes Öffnen» gesichert sein müssen, aber eine Abschliessvorrichtung explizit keine Anforderung für ein Strassenfahrzeug ist. Auch Fahrzeugalarmsysteme sind prinzipiell nicht nötig, aber falls sie zum Einsatz kommen, beschreibt die VST relativ genau, welchen Anforderungen diese entsprechen müssen.

Auch wenn ein Auto ohne Türschloss als Strassenfahrzeug durchgehen würde, käme es wohl kaum jemandem in den Sinn, am neu erstandenen Auto das serienmässig eingebaute Schloss wieder zu entfernen. Zum einen, weil wohl die wenigstens daran interessiert sind, Dieben die Arbeit zu erleichtern und zum anderen, weil hier die Versicherung im Falle eines Diebstahls nicht mehr zahlen würde.

Weitere Beispiele, in denen Versicherungen über Auflagen oder Prämienberechnungen de facto Sicherheitsstandards einfordern, gibt es dabei in mannigfacher Ausführung. So wird die Prämie für Kunstwerke bei einzelnen Versicherungen nicht einfach nur nach dem Wert des Gemäldes berechnet, sondern es fliessen weitere Faktoren mit ein, wie beispielsweise die vorhandenen Sicherheitsmassnahmen zum Schutz des Kunstwerks. Entsprechen diese den gegenwärtigen Best-Practices in diesem Bereich, bezahlt der Kunde weniger Prämien.

Der Cyber-Bereich ist hoch dynamisch und was gestern noch als state-of-the-art galt, ist heute bereits kalter Kaffee. Dies macht die Formulierung von Mindestsicherheitsstandards zu einer kontinuierlichen und dynamischen Aufgabe. Mit Blick auf den breiten Einsatz von Informations- und Kommunikationstechnologien müssen Sicherheitsstandards im Cyber-Bereich zusätzlich noch flexibel und auf den eigentlichen Bestimmungszweck angepasst sein. Staatliche Regulatorien zu erlassen ist jedoch in vielen Fällen ein langsamer Prozess.

Auf der anderen Seite sind Versicherung im Rahmen ihres Geschäftes relativ frei, sich schnell an Entwicklungen und Veränderungen anzupassen und basierend auf den jeweiligen best-practices von ihren Kunden Sicherheitsmassnahmen einzufordern. So decken

Versicherer auch jene Massnahmen ab, die typischerweise gar keinen Regulatorien unterstehen. Somit bietet das wachsende Geschäft mit Cyber-Versicherungen nicht nur eine wirtschaftliche Gelegenheit, sondern auch die Chance generell, die Sicherheitskultur und somit die Grundsicherheit im Cyber-Bereich nachhaltig zu erhöhen.

Ganz darauf zu setzen, dass die Versicherungsbranche über kurz oder lang die Problematik der Sicherheitsstandards im Cyber-Bereich löst, ist allerdings keine Option. Zum einen können Fachbehörden hier unterstützend agieren, indem sie beispielsweise in ihrem Geltungsbereich Prinzipien basierte Vorgaben machen, die der Versicherungsbranche als Richtschnur dienen können. Auch mit Blick auf die eigentliche Risikokalkulation können staatliche Einheiten im Cyber-Bereich mit ihrem Wissen zu Bedrohung und Entwicklung einen Beitrag leisten. Und zu guter Letzt existiert auch im Cyber-Bereich die hypothetische Möglichkeit eines «Jahrhundertbebens», welches mit Blick auf die theoretisch exorbitanten Verluste jede Versicherung in den Abgrund reissen würde und damit das Versichern einiger Cyber-Risiken schlicht verunmöglicht. Eine Lösung für diese Problematik zu finden, beispielsweise analog zur staatlichen Garantie bei Erdbebenschäden ab einer gewissen Schadenssumme, ist eine Herausforderung für Staat und Versicherungsbranche. Falls dies aber gelingt, erhalten Versicherungen Planungssicherheit und somit auch die Möglichkeit, das Geschäft mit Cyber-Policen proaktiver zu gestalten. Am Ende gewinnt dabei nicht nur die Versicherungsbranche, sondern mit der Übernahme von Risiken und den dazu gehörenden Risikominimierenden Auflagen auch die Wirtschaft, Gesellschaft und der Staat.

6.2 Politikerinnen und Politiker - ein beliebtes Ziel von Cyber-Manipulatoren

Die Cyber-Attacke gegen die Parteileitung der Demokraten in den Vereinigten Staaten (DNC), welche die Sicherheitsfirma «Crowdstrike» den Spionageoperationen «Cozy Bear» und «Fancy Bear» zuschrieb[63], war die erste einer langen Serie von Cyber-Angriffen, bei denen politische Exponentinnen und Exponenten im Fokus waren. Die Angriffe haben gezeigt, dass die Veröffentlichung privater Nachrichten durchaus auch die öffentliche Meinung zu beeinflussen vermag. Gemäss einem Blog von «The Intercept»[64] gewinnt die Hypothese, dass die tatsächliche Absicht der Cyber-Kriminellen die Manipulation der Ergebnisse der US-amerikanischen Präsidentschaftswahlen gewesen sei, zunehmend an Boden. Die Absicht, den eigenen Kandidaten zu favorisieren, indem man der Konkurrenz schadet, zeigt sich ebenfalls im Phänomen der sogenannten «Fake News», die während Wahlkampagnen vermehrt auftauchen.

Für den Schutz von Staat, Gesellschaft und den demokratischen Institutionen reichen technische Schutzmassnahmen bei Regierungs- und Firmennetzwerken für sich alleine nicht aus. Man stellt nämlich fest, dass immer mehr private Online-Konten von Prominenten, politisch aktiven Personen und insbesondere von gewählten Volksvertretern zur Zielscheibe von Angriffen werden, sei dies um kompromittierendes Material zu suchen oder das Konto für rufschädigende oder manipulierende Äusserungen zu verwenden.

---

63 Siehe MELANI Halbjahresbericht 2/2016 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2016-2.html (Stand: 31. Juli 2017).

64 https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/ (Stand: 31. Juli 2017).

Dem Beispiel anderer Länder wie Deutschland und Grossbritannien folgend hat MELANI deshalb eine Liste von Sicherheitsmassnahmen in Form einer Infokarte entwickelt, die den Schweizer Parlamentarierinnen und Parlamentariern helfen soll, sich zu schützen. Natürlich sind die Empfehlungen auch für nicht-Politiker geeignet.

6.2.1 Angriffe auf Wahlprogramme

Die Cyber-Angriffe anlässlich der amerikanischen Präsidentschaftswahlen richteten sich nicht nur gegen die E-Mail-Konten von Vertretern der demokratischen Parteileitung. Gemäss der Website «The Intercept»[65] wurde auch ein Unternehmen angegriffen, das Geräte zur Überprüfung der Wahlzettel herstellt.

Ebenfalls sollen gezielte Mails an über 100 Beamte geschickt worden sein, die für die Beobachtung der Wahlresultate zuständig waren. Die Mails, versehen mit einer Malware, waren gut durchdacht: Sie richteten sich an nichts ahnende Mitarbeitende lokaler Regierungsorganisationen. Die Mails stammten angeblich von einem Mitarbeiter einer Firma, die Dienstleistungen im Bereich E-Voting und Wahlsoftware anbietet. Der Account der Firma war zuvor zu diesem Zweck kompromittiert worden. Zwischen dem 31. Oktober und dem 1. November 2016 wurde an 122 Adressaten ein E-Mail mit einem schädlichen Word-Dokument verschickt, das einen Trojaner enthielt. Die NSA gab sich jedoch sowohl zum Ergebnis dieser Angriffe wie zum eventuellen Erfolg der bösartigen Mails und allfällig extrahierter oder gar manipulierter Daten bedeckt.

Es stellt sich deshalb die Frage, wie sicher elektronische Wahlprogramme tatsächlich sind. Staaten, die solche Programme einsetzen, sollten sich bewusst sein, dass es sich um kritische Infrastrukturen handelt. Sie sollten sich überlegen, mit welchen Prozessen diese am besten abgesichert werden können. Wird das Risiko als zu hoch erachtet, müssen auch extreme Lösungen in Betracht gezogen werden. Beispielsweise der Verzicht auf solche Programme, wie dies in Deutschland und Grossbritannien der Fall ist.

6.2.2 Honeypot-Accounts: Strategie gegen Infiltrierungsangriffe

E-Mails von Mitarbeitenden der Kampagne «En Marche» kamen während des französischen Wahlkampfs ins Visier einer Spear-Phishing-Kampagne. Zusätzlich hat die NSA einen Infiltrierungsversuch in die französische Infrastruktur entdeckt und am 5. Mai 2017 die zuständigen Behörden gewarnt. Es überraschte nicht, dass sich Angriffe gegen Ende der Wahlkampagne intensivierten. Die Ereignisse rund um den US-amerikanischen Präsidentschaftswahlkampf und das Wissen, keinen umfassenden Schutz bieten zu können, veranlasste das technische Team von «En Marche!» dazu, präventiv zu handeln. Mit einer «Cyber-Blurring-Strategie» wurden falsche E-Mail-Konten eingerichtet, die als Honeypot oder Lockvogel für die Angreifer dienen sollten. Jedes falsche Konto wurde mit Ad-hoc-Dokumenten gefüllt, um die Arbeit der Hacker zu stören, weil sie im Falle einer Datenextraktion zuerst verifizieren mussten, ob die Dokumente echt waren oder nicht. Diese Arbeit nahmen die Angreifer allerdings nicht auf sich. Sie publizierten sämtliche ca. 9 Gigabyte an Daten, also auch die Ad-hoc-Dokumente. Die Daten wurden anfänglich über die US-amerikanische Website «Pastebin» verteilt und darauf von «4Chan» und «WikiLeaks

[65] https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/ (Stand: 31. Juli 2017).

geteilt». Trotz des Versuches, den Präsidentschaftskandidaten Macron mit Meldungen zu diskreditieren, dass er beispielsweise ein geheimes Konto auf den Bahamas besitzen soll, war die Strategie erfolgreich. Die Tatsache, dass die veröffentlichten Daten teilweise falsch und auch nicht sonderlich pikant waren, hatte dazu geführt, dass die Kampagne von Macron nicht wesentlich beeinflusst wurde.

Die Qualität der E-Mails, die für den Angriff verwendet wurden, wurde allgemein als gut bezeichnet. Kurz vor Ende der Kampagne tauchten beispielsweise E-Mails auf, die angeblich vom «Digital Director» Emmanuel Macrons stammten. Die Mails forderten die Empfängerinnen und Empfänger auf, eine angehängte Datei herunterzuladen, um sich so vor Cyber-Angriffen zu schützen. Der Angriff war jedoch nicht sehr professionell. Zudem hinterliessen die Angreifer Spuren. Beispielsweise fanden sich russische Benutzernamen in den erstellten oder veränderten Dokumenten, oder diese wurden mit einer Microsoft-Version bearbeitet, welche nur in Russland erhältlich ist. Auch in der C&C-Infrastruktur tauchten Indizien auf, dass hinter den Angriffen die Hackerkampagne «Sofacy» steckt[66], die auch für die Angriffe auf die Clinton-Kampagne verantwortlich gemacht wird.

6.2.3 Auch Deutschland und Grossbritannien im Visier

Wie das Deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) erklärte, wurden Ende Juni 2017 die privaten E-Mail-Accounts von Wirtschaftsvertretern und von Angestellten öffentlicher Verwaltungen von Phishing-Wellen nahezu überhäuft.[67] Die Angriffsversuche konzentrierten sich auf Yahoo- und Gmail-Konten. Die Untersuchung der Infrastruktur der Angreifer zeigte Ähnlichkeiten mit den in Kapitel 6.2.1 und 6.2.2 beschriebenen Kampagnen gegen die Parteileitung der Demokraten in den USA und Frankreich.

Am Freitag, 23. Juni 2017, wurde auch das englische Parlament Opfer einer Cyber-Attacke. Gehackt wurden offenbar die E-Mail-Konten von rund 90 Parlamentarierinnen und Parlamentariern. Grund dafür seien viel zu einfache Passwörter gewesen, die nicht den Vorgaben entsprachen. Nachdem die Cyber-Kriminellen die E-Mail-Accounts gehackt hatten, sperrten sie die Fernzugriffe, um die rechtmässigen Kontoinhaberinnen und -inhaber daran zu hindern, sichere Passwörter einzurichten.

---

66 https://www.nytimes.com/2017/04/24/world/europe/macron-russian-hacking.html?mcubz=0 (Stand: 31. Juli 2017).

67 http://www.zdnet.de/88302365/bsi-warnt-vor-phishing-angriffen-auf-funktionstraeger/?inf_by=59a97d93681db8d9688b45bf (Stand: 31. Juli 2017).

Empfehlung:

Jede Verwaltung und Firma kann nur ihre eigenen Netzwerke und Infrastrukturen schützen. Mobile Geräte, E-Mail-Adressen und andere IT-Infrastrukturen, die Mitarbeitende privat nutzen, sind ausserhalb deren Einflussbereichs. Angriffe auf private Netzwerke haben also potenziell mehr Chancen auf Erfolg, und es lässt sich nicht ausschliessen, dass in der Folge indirekt auch Regierungsnetze infiziert werden. Das BSI hat deshalb eine Reihe von Leitfäden publiziert, die der Prävention dienen. Sie richten sich an die Angestellten öffentlicher Verwaltungen oder an Spitzenangestellte von Finanzunternehmen, können aber auch für Privatpersonen hilfreich sein. MELANI empfiehlt insbesondere folgende Massnahmen, welche auf den Leitfäden des BSI beruhen:

- geschäftliche Nachrichten nicht über private E-Mail-Konten versenden;
- als vertraulich eingestufte Nachrichten verschlüsseln;
- Zwei-Faktor-Authentifizierung einrichten;
- Beim geringsten Verdacht, das E-Mail-Konto könnte gehackt worden sein, sollte das Passwort unverzüglich geändert werden.

MELANI hat eine Liste von Sicherheitsmassnahmen für Schweizer Parlamentarierinnen und Parlamentariern in Form einer Infokarte entwickelt.

Die Infokarte für Parlamentarierinnen und Parlamentarier kann auf der Webseite von MELANI heruntergeladen werden

https://www.melani.admin.ch/melani/de/home/dokumentation/Infokarten.html

6.3 Die neue EU-Datenschutz-Grundverordnung und die Auswirkungen auf die Schweiz

Die Datenschutz-Grundverordnung der Europäischen Union (EU DSGVO /EU GDPR) ist eine Verordnung, mit der die Normen für die Verarbeitung von personenbezogenen Daten durch private Unternehmen und öffentliche Stellen EU-weit vereinheitlicht werden. Die Verordnung ersetzt die Richtlinie 95/46/EG aus dem Jahr 1995, ist am 24. Mai 2016 in Kraft getreten und nach einer zweijährigen Übergangsfrist per 25. Mai 2018 durch alle Mitgliedstaaten anzuwenden.

Überzeugt, dass die digitale Zukunft Europas nur auf Vertrauen gegründet werden kann, verfolgt die EU mit der Datenschutz-Grundverordnung drei Ziele: Das Datenschutzrecht europaweit vereinheitlichen, den Binnenmarkt durch Gewährleistung der gleichen wirtschaftlichen Bedingungen in der Union stärken sowie den Datenschutz in Folge der technischen Entwicklung unter Wahrung des Grundrechtsschutzes zu modernisieren.

Die wichtigsten Änderungen durch die neuen Vorschriften sind im Überblick: das Recht auf Vergessenwerden; Datenverarbeitung ausschliesslich nach ausdrücklicher Einwilligung der betroffenen Person; das Recht auf Datenübertragbarkeit (an einen anderen Dienstleister); das Recht der Betroffenen, bei Verletzung des Schutzes der eigenen Daten darüber informiert zu werden und schliesslich ein härterer Durchgriff bei Verstössen gegen die

Verordnung. Letzteres bedeutet, dass im Falle eines Unternehmens Geldbussen von bis zu 4% seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden können.

Im Gegensatz zur Richtlinie 95/46/EG, welche von den Mitgliedstaaten in nationales Recht umgesetzt werden musste, gilt die Datenschutz-Grundverordnung ab Mai 2018 unmittelbar in allen Mitgliedstaaten. Dies bedeutet, dass es den Mitgliedstaaten grundsätzlich nicht erlaubt ist, den von der Verordnung festgeschriebenen Datenschutz durch nationale Regelungen abzuschwächen oder zu verstärken. Allerdings enthält die Verordnung über 70 Öffnungsklauseln, welche es den Mitgliedstaaten ermöglichen, gewisse Aspekte des Datenschutzes auf nationaler Ebene zu regeln.

Die zahlreichen Ausnahmen und die damit einhergehende Rechtsunsicherheit bringen denn der Datenschutz-Grundverordnung Kritik aus verschiedenen Kreisen. Die Verordnung verfehle die ursprüngliche Zielsetzung der Vereinheitlichung, sei zu abstrakt, mache zu viele Ausnahmen und führe so zwangsläufig zu Auslegeschwierigkeiten und Widersprüchen in Bezug zu national nach wie vor gültigem Recht. Insbesondere Deutschland warnt vor einer Ausdünnung des deutschen Datenschutzrechts. Schliesslich seien die Normen so technikneutral gehalten, dass die Risiken der Informationstechnik nicht ausreichend erfasst werden.

Die Datenschutz-Grundverordnung ist nicht nur in der EU sondern auch in Drittstaaten wie der Schweiz anwendbar. So gilt die EU-Datenschutz-Grundverordnung auch für alle Schweizer Unternehmen mit oder ohne EU-Niederlassung, die Personen in der EU Waren- oder Dienstleistungen anbieten (was mit entsprechenden Angeboten auf einer Webseite oder eines Webshops bereits erfüllt sein dürfte), persönliche Daten bearbeiten, die von Staatsangehörigen der EU-Mitgliedstaaten stammen oder das Verhalten von Personen in der EU analysieren.

Empfehlung:

MELANI empfiehlt daher, die entsprechenden Informationsverarbeitungsprozesse, die Datenhaltung und die Informationssicherung rechtzeitig an die neuen gesetzlichen Anforderungen anzupassen. Weiter ist davon auszugehen, dass die Einführung der Verordnung und die Statuierung hoher Geldbussen bei Verletzung des Datenschutzes nicht nur die Unternehmen beschäftigt, sondern auch Kriminelle zu neuen erpresserischen Vorgehensweisen inspirieren wird.

Die Totalrevision des Schweizerischen Datenschutzgesetzes ist zurzeit noch im Gange. Es ist davon auszugehen, dass die Revision verschiedene Neuerungen der EU-Datenschutz-Grundverordnung aufgreifen wird.

7 Politik, Forschung, Policy

7.1 CH: Parlamentarische Vorstösse

Geschäft	Nummer	Titel	Eingereicht von	Datum Einreichung	Rat	Amt	Stand Beratung & Link
Mo	17.3508	Schaffung eines Cyber Security Kompetenzzentrums auf Stufe Bund	Joachim Eder	15.06.2017	SR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173508
Mo	17.3507	Ein Cyber Defence Kommando mit Cybertruppen für die Schweizer Armee	Josef Dittli	15.06.2017	SR	VBS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173507
Mo	17.3497	Zentrale Anlauf- und Koordinationsstelle zur Bekämpfung der organisierten und international tätigen Computer-Kriminalität	Marcel Dobler	15.06.2017	NR	EJPD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173497
Mo	17.3496	Verpflichtender Grundschutz für kritische Strominfrastrukturen	Edith Graf-Litscher	15.06.2017	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173496
Mo	17.3475	Meldepflicht bei schwerwiegenden Sicherheitsvorfällen bei kritischen Infrastrukturen	Edith Graf-Litscher	15.06.2017	NR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173475
Po	17.3433	Cybersicherheit im Gesundheitswesen	Bea Heim	13.06.2017	NR	EDI	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173433
Mo	17.3199	Ausbau der Cyberabwehrkompetenz	Franz Grüter	16.03.2017	NR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173199
Ip	17.3136	Cybersicherheit im Gesundheitswesen	Bea Heim	15.03.2017	NR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173136
Ip	17.3103	Herausforderungen im Cyberbereich. Wie weiter in unserem Land?	Joachim Eder	13.03.2017	SR	VBS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173103
Mo	17.3591	Netzneutralität. Bewahren der ursprünglichen Lebendigkeit des Internets	Claude Béglé	16.06.2017	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173591
Ip	17.3452	Wie kann man die Medien beim Übergang in die digitale Welt unterstützen?	Adèle Thorens Goumaz	14.06.2017	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173452
Ip	17.3277	Lassen sich die Internetgiganten mit den heutigen rechtlichen Sanktionen bändigen?	Jean Christophe Schwaab	02.05.2017	NR	EJPD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173277
Ip	17.3276	Wie steht es um die Verantwortlichkeit für Werbung im Internet, die gesetzeswidrig ist, Hassbotschaften verbreitet	Jean Christophe Schwaab	02.05.2017	NR	EJPD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173276

		oder der Finanzierung krimineller Aktivitäten dient?					
Ip	17.3254	Die Vorteile moderner technologien für Menschen mit Behinderung nutzen. Beispiel HbbTV	Pascale Bruderer Wyss	17.03.2017	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173254
Ip	17.313	Internethandel mit lebenden Tieren und Tierschutz	Daniel Brélaz	15.03.2017	NR	EDI	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173130
Fr	17.5206	Cybersicherheit. Missbrauch von gehackten Geräten des Internet of Things für Botnetze durch Sicherheitsstandards unterbinden	Balthasar Glättli	08.03.2017	NR	WBF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20175206
Ip	17.3069	Erfassen die heutigen Statistiken das Potenzial der Digitalisierung?	Ruedi Noser	07.03.2017	SR	EDI	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173069
Ip	17.3075	Digital Gender Gap. Was sind Herausforderung und Chancen der Digitalisierung in der Arbeitswelt aus der Geschlechterperspektive?	Sibel Arslan	08.03.2017	NR	WBF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173075
Mo	17.3592	Die Steuerung der Digitalisierung so weiterentwickeln, dass sie sich von der Digitalisierung selbst inspirieren lässt	Claude Béglé	16.06.2017	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173592
Ip	17.3533	Stärkung der Informatikausbildung in der Schweiz	Franz Grüter	15.06.2017	NR	WBF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173533
Ip	17.3341	Ist das BIT ein Bundesamt für In- und Outsourcing?	Stefan Müller-Altermatt	04.05.2017	NR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173341
Fr	17.104 0	Ausbau der Mobilfunknetze für die Digitalisierung der Schweiz	Christian Wasserfallen FDP-Liberale Fraktion	06.06.2017	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20171040
Mo	17.3498	Mobiltelefonie: Geben wir der Schweiz ihre Wettbewerbsfähigkeit zurück!	Yannick Buttet	16.06.2017	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173498
Fr	17.5303	Gefährden Drohnen die Sicherheit der Landesflughäfen?	Priska Seiler Graf	07.06.2017	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20175303
Fr	17.5221	Alpbetriebe vom Telefonnetz abgehängt	Erich von Siebenthal	30.05.2017	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20175221

8 Publizierte MELANI Produkte

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

8.1 GovCERT.ch Blog

8.1.1 Notes About The «NotPetya» Ransomware

28.06.2017 - A new ransomware, currently named «NotPetya», has begun spreading yesterday. There are many victims, especially in Ukraine, but also large companies have been hit hard such as «Maersk» or «Merck». There are infections in Switzerland as well. As many others we have analyzed the malware and tried to harden evidence about its functioning. As there are many good papers already published, we do not want to repeat all these things but to highlight a few important facts that now can be considered being hardened evidence.

➔ https://www.govcert.admin.ch/blog/32/notes-about-the-notpetya-ransomware

8.1.2 «WannaCry»? It is not worth it!

15.05.2017 - On Friday, May 12th 2017, a ransomware called «WannaCry» hit the cyber space. Among the victims are hospitals in UK, the national telecom provider in Spain and U.S delivery service «FedEx». But WannaCry did not only hit the internet, the ransomware was also very present in newspapers worldwide. It also kept us and our partners from abroad very busy during the last weekend, analyzing the malware, reevaluating the current situation in Switzerland and world-wide, communicating with National Critical Infrastructure, and talking to the press. While we analyzed the threat as well, there are already many good papers on «WannaCry». For this reason we do for once not focus on the exact technical implementation, but try to give a comprehensive overview of this threat and the impact «WannaCry» has, with a focus on the situation in Switzerland.

➔ https://www.govcert.admin.ch/blog/31/wannacry-it-is-not-worth-it

8.1.3 When «Gozi» Lost its Head

04.04.2017 - After our automated unpacking procedure recently failed on a «Gozi» binary (MD5 c1a73ff8fb2836fe47bc095b622c6c50), we were forced to perform a manual analysis - and indeed we found some interesting new features in the first layer of the packer…

➔ https://www.govcert.admin.ch/blog/30/when-gozi-lost-its-head

8.1.4 Taking a Look at «Nymaim»

03.03.2017 - «Nymaim» is active worldwide since at least 2013 and is also responsible for many infections in Switzerland. Sinkhole Data shows that «Nymaim» is responsible for about 2% of infected devices in Switzerland that hit sinkholes the last few days. When we looked at the «Nymaim» trojan in January, we were stunned by their powerful code obfuscation

techniques and wrote an «IDAPython» script to deobfuscate the code using the debugger engine. Later we found similar tools already available in the public to do this using code emulation. Nevertheless, we decided to publish a paper about our approach, as it is a very nice case study to demonstrate how debugger orchestration works in «IDAPython», and to explain different disassembly strategies that can be used. Instrumenting the debugger means to set breakpoints in scripts and to run the code in pieces, which has a very dynamic and fascinating impact on the IDA GUI.

➔ https://www.govcert.admin.ch/blog/29/taking-a-look-at-nymaim

8.1.5 The Rise of «Dridex» and the Role of ESPs

20.02.2017 - Last week, we have warned Swiss citizens about a new malspam run targeting exclusively Swiss internet users. The attack aimed to infect them with «Dridex». «Dridex» is a sophisticated eBanking Trojan that emerged from the code base of «Bugat» / «Cridex» in 2014. Despite takedown attempts by the security industry and several arrests conducted by the FBI in 2015, the botnet is still very active. In 2016, MELANI / GovCERT.ch became aware of a handful of highly sophisticated attacks against small and medium businesses (SMB) in Switzerland aiming to steal large amounts of money by targeting offline payment software. During our incident response in 2016, we could identify «Dridex» to be the initial infection vector, which had arrived in the victim's mailbox by malicious Office Word documents, and uncovered the installation of a sophisticated malware called «Carbanak», used by the attacker for lateral movement and conducting the actual fraud. Between 2013 and 2015, the «Carbanak» malware was used to steal approximately 1 billion USD from banks worldwide.

➔ https://www.govcert.admin.ch/blog/28/the-rise-of-dridex-and-the-role-of-esps

8.1.6 «Sage 2.0» comes with IP Generation Algorithm (IPGA)

30.01.2017 - On Jan 20, 2017, we came across a malware that appeared to be a new Ransomware family called «Sage 2.0». Within a couple of days we were able to collect more than 200 malware binaries across our sensors associated with this new Ransomware. Last week, Brad Duncan also wrote a SANS InfoSec Diary entry on «Sage 2.0», noticing some strange UDP packets sent to over 7'000 different Ips.

➔ https://www.govcert.admin.ch/blog/27/sage-2.0-comes-with-ip-generation-algorithm-ipga

8.2 MELANI Newsletter

8.2.1 Schadsoftware: Vorsicht ist geboten - unabhängig vom Betriebssystem

15.06.2017 - Bei der Verbreitung von Schadsoftware via E-Mail versuchen Kriminelle vermehrt, ihre Opfer gezielt anzugreifen. Dabei sind nicht mehr nur ausschliesslich Windows Benutzer im Visier. In den vergangenen Wochen hat die Melde- und Analysestelle Informationssicherung MELANI verschiedene Schadsoftware-Wellen beobachtet, welche sich gezielt gegen Schweizer Nutzende des Betriebssystems MacOS, das von Apple entwickelte Betriebssystem, richteten. Es ist deshalb wichtig in Erinnerung zu rufen, dass unabhängig vom verwendeten Betriebssystem und für alle Nutzenden Vorsicht geboten ist.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/malware---si-raccomanda-prudenza-indipendentemente-dal-sistema-o.html

8.2.2 Zunehmender Missbrauch der Namen von Bundesstellen und Firmen

04.05.2017 - In den letzten Monaten hat der Missbrauch der Namen von Bundestellen und bekannten Firmen als Absenderadresse zugenommen. MELANI gibt Tipps, wie man sich verhalten soll.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/zunehmender-missbrauch-der-namen-von-bundesstellen-und-firmen.html

8.2.3 Für einen sicheren Umgang mit dem Internet der Dinge

20.04.2017 - Der am 20. April veröffentlichte 24. Halbjahresbericht der Melde- und Analysestelle Informationssicherung (MELANI) befasst sich mit den wichtigsten Cyber-Vorfällen der zweiten Jahreshälfte 2016 im In- und Ausland. Im Schwerpunktthema widmet sich der Bericht dem immer bedeutender werdenden Internet der Dinge.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/halbjahresbericht-2016-2.html

8.2.4 Social Engineering: Neue Angriffsmethode richtet sich gegen Firmen

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

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

8.3 Checklisten und Anleitungen

Im ersten Halbjahr 2017 hat MELANI keine neuen Checklisten und Anleitungen publiziert.

9 Glossar

Begriff	Beschreibung
Advanced Persistent Threats (APT)	Diese Angriffsweise führt zu einem sehr hohen Schaden, der auf eine einzelne Organisation oder auf ein Land wirkt. Der Angreifer ist bereit, sehr viel Zeit, Geld und Wissen in den Angriff zu investieren und verfügt in der Regel über grosse Ressourcen.
App	Der Begriff App (von der englischen Kurzform für Application) bezeichnet im Allgemeinen jede Form von Anwendungsprogrammen. Im Sprachgebrauch sind damit mittlerweile jedoch meist Anwendungen für moderne Smartphones und Tablet-Computer gemeint.
Backdoor	Backdoor (deutsch: Hintertür) bezeichnet einen Teil einer Software, der es Benutzern ermöglicht, unter Umgehung der normalen Zugriffssicherung Zugang zum Computer oder einer sonst geschützten Funktion eines Computerprogramms zu erlangen.
Backup	Backup (deutsch Datensicherung) bezeichnet das Kopieren von Daten in der Absicht, diese im Fall eines Datenverlustes zurückkopieren zu können.
Bitcoin	Bitcoin ist ein weltweit verwendbares dezentrales Zahlungssystem und der Name einer digitalen Geldeinheit.
Booter / Stresser	Werkzeuge, welche gegen Bezahlung DDoS Angriffe auslösen («DDoS as a service»).
Border Gateway Protokoll	Das Border Gateway Protocol ist das im Internet eingesetzte Routingprotokoll und verbindet autonome Systeme miteinander.
Browser	Computerprogramme, die vorwiegend dazu verwendet werden, verschiedene Inhalte im World Wide Web anzuzeigen. Die bekanntesten Browser sind Internet Explorer, Opera, Firefox und Safari.
Brute Force	Die Brute-Force-Methode ist eine Lösungsmethode für Probleme aus den Bereichen Informatik, Kryptologie und Spieltheorie, die auf dem Ausprobieren aller möglichen Fälle beruht.
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.
Content Delivery Network	Ein Content Delivery Network ist ein Netz regional verteilter und über das Internet verbundener Server, mit dem Inhalte – insbesondere grosse Mediendateien – ausgeliefert werden.
Cyber-Blurring-Strategie	Cyber-Blurring (zu Deutsch verwischen) beschreibt die Methode in einem Datensatz gezielt fehlerhafte Daten zu platzieren, um die Arbeit der Angreifer zu erschweren.
Data-URL	Ein Data-URL ist ein URI-Schema, das es ermöglicht, Daten in (HTML-)Quelltext so einzubetten, als wären es externe Ressourcen.
DDoS	Distributed-Denial-of-Service Attacke. Eine DoS-Attacke, bei der das Opfer von vielen verscheiden Systemen aus gleichzeitig angegriffen wird.
Defacement	Verunstaltung von Webseiten.
Domain 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).
e-Currency Dienste	Ein monetärer Wert in Form einer Forderung gegen die ausgebende Stelle, der auf einem Datenträger gespeichert ist, gegen Entgegennahme eines Geldbetrags ausgegeben wird, dessen Wert nicht geringer ist als der ausgegebene monetäre Wert, von anderen Unternehmen als der ausgebenden Stelle als Zahlungsmittel akzeptiert wird
Ethernet	Ethernet ist eine Technologie für kabelgebundene Datennetze.
Exploit-Kit	Baukasten, mit denen Kriminelle Programme, Scripts oder Codezeilen generieren können, mit denen sich Schwachstellen in Computersystemen ausnutzen lassen.
Fernzugriffstool	Die Fernwartungssoftware (englisch: Remote Administration Tool) stellt eine Anwendung des Konzeptes Fernwartung für beliebige Rechner oder Rechnersysteme dar.
Internet der Dinge	Der Begriff Internet der Dinge beschreibt, dass der Computer in der digitalen Welt zunehmend von «intelligenten Gegenständen» bis hin zu «KI», künstlicher Intelligenz, ergänzt wird.

IP-Adressen	Adresse, welche einen Computer im Internet (oder einem TCP/IP-Netzwerk) identifiziert (Beispiel: 172.16.54.87).
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.
Launcher	Computerprogramm, welches dabei hilft ein Programm zu lokalisieren und zu starten.
Makro-Malware	Schadsoftware, die mittels Makro installiert wird. Ein Makro ist eine Folge von Anweisungen, die mit nur einem einfachen Aufruf ausgeführt werden können.
Malware	Oberbegriff für Software, die schädliche Funktionen auf einem Rechner ausführt (wie beispielsweise Viren, Würmer, Trojanische Pferde).
Managed Service Providers (MSP)	Ein Managed Services Provider (MSP) ist ein Informations-Technologie-Dienstleister, der die Verantwortung für die Bereitstellung einer definierten Reihe von Dienstleistungen für seine Kunden übernimmt und verwaltet.
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.
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.
Plug-Ins	Ein Plug-in ist ein optionales Software-Modul, das eine bestehende Software erweitert bzw. verändert.
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.
RAM	Random-Access Memory (RAM) ist ein Datenspeicher, der besonders bei Computern als Arbeitsspeicher Verwendung findet, meist in Form von Speichermodulen.
Rootkit	Auswahl an Programmen und Technologien, welche den unbemerkten Zugang und die unbemerkte Kontrolle eines Computers ermöglichen.
Router	Geräte aus dem Bereich Computernetzwerke, Telekommunikation oder auch Internet, die mehrere Rechnernetze koppeln oder trennen. Router werden beispielsweise in Heimnetzwerken eingesetzt und machen die Verbindung zwischen internem Netz und dem Intranet.
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 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.
Software Defined Radios	Unter Software Defined Radio (SDR) fasst man Konzepte für Hochfrequenz-Sender und -Empfänger zusammen, bei denen kleinere oder grössere Anteile der Signalverarbeitung mit Software verwirklicht werden.
SQL-Injection	SQL-Injection (SQL-Einschleusung) bezeichnet das Ausnutzen einer Sicherheitslücke in Zusammenhang mit SQL-Datenbanken, die durch mangelnde Überprüfung von zu übermittelnden Variablen entsteht. Der Angreifer versucht dabei eigene Datenbankbefehle einzuschleusen, um Daten in seinem Sinne zu verändern oder Kontrolle über den Server zu erhalten.
SS7	Das Signalling System #7 (SS7) ist eine Sammlung von Protokollen und Verfahren für die Signalisierung in Telekommunikationsnetzen. Es kommt im öffentlichen Telefonnetz, in Zusammenhang mit ISDN, Fest- und Mobilfunknetz und seit etwa 2000 auch verstärkt in VoIP-Netzen zum Einsatz.
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.
Subscription Bomb	Als Subscription Bomb bezeichnet man das organisierte Einschreiben von E-Mail-Adressen bei mehreren Newsletter-Anbietern, um das Postfach oder die Kommunikationseinrichtungen des Empfängers zu blockieren.
Take-Down	Ausdruck, der verwendet wird, wenn ein Provider eine Seite aufgrund betrügerischen Inhalts vom Netz nimmt.
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.
Verschlüsselungstrojaner / Ransomware	Malware, mit der die Besitzer der infizierten Rechner erpresst werden sollen (ransom: englisch für Lösegeld). Typischerweise werden Daten verschlüsselt oder gelöscht und erst nach Lösegeldzahlungen der zur Rettung nötige Schlüssel vom Angreifer zur Verfügung gestellt.
Webbrowser	Computerprogramme, die vorwiegend dazu verwendet werden, verschiedene Inhalte im World Wide Web anzuzeigen. Die bekanntesten Browser sind Internet Explorer, Firefox und Safari.
Webseiteninfektion	Infektion eines Computers mit Malware allein durch 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.
Win32PE-Datei	Portable Executable (PE) beschreibt ein Binärformat ausführbarer Programme. Es ist das Dateiformat, das bei Win32- und Win64-Systemen für ausführbare Dateien verwendet wird.
WLAN	WLAN (Wireless Local Area Network) steht für drahtloses lokales Netzwerk.
ZeroDay-Lücken	Sicherheitslücke, für welche noch kein Patch exisitiert.
ZIP-Datei	ZIP ist ein Algorithmus und Dateiformat zur Datenkompression, um den Speicherbedarf von Dateien für die Archivierung und Übertragung zu verringern.
Zweifaktorauthentifizierung	Dafür sind mindestens zwei der drei Authentifikationsfaktoren notwendig: 1. Etwas, das man weiss (z.B. Passwort, PIN, usw.) 2. Etwas, das man besitzt (z.B. Zertifikat, Token, Streichliste, usw.) 3. Etwas, das man ist (z. B. Fingerabdruck, Retina-Scan, Stimmerkennung usw.).