Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Informatiksteuerungsorgan des Bundes ISB
Nachrichtendienst des Bundes NDB

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

INFORMATIONSSICHERUNG

LAGE IN DER SCHWEIZ UND INTERNATIONAL

Halbjahresbericht 2017/II (Juli – Dezember)

26. APRIL 2018

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

1 Übersicht / Inhalt

2 Editorial

Werner Meier
Delegierter Wirtschaftliche Landesversorgung

Liebe Leserin, lieber Leser

Die Digitalisierung bietet immense Chancen für unser Land – stellt es aber auch vor grosse Herausforderungen. Die Steuerung und Optimierung von Prozessen in der Wirtschaft durch Informations- und Kommunikationstechnologien (IKT) kann nur dann nachhaltig gelingen, wenn die IKT jederzeit verfügbar, zuverlässig und widerstandsfähig gegenüber Störungen und Angriffen ist. Kurz: Digitalisierung ohne IKT-Sicherheit ist undenkbar.

Dem Bundesrat ist die Digitalisierung ein wichtiges Anliegen. Dies hat er mit seiner Strategie «Digitale Schweiz» zum Ausdruck gebracht und gleichzeitig «Sicherheit» als eines von vier Kernzielen verankert. Der im Sommer 2017 von WBF und UVEK eingesetzte Beirat zur Strategieumsetzung setzte das Thema «Cybersecurity» ebenfalls oben auf die Traktandenliste.

Die Wirtschaftliche Landesversorgung (WL) hat den gesetzlichen Auftrag, die Versorgung der Schweiz mit lebenswichtigen Gütern und Dienstleistungen für den Krisenfall sicherzustellen. Die IKT ist für die WL nicht nur per se lebenswichtig, sondern beispielsweise als Ressource für das Funktionieren der Versorgung unseres Landes mit elektrischer Energie oder Logistikdienstleistungen von zentraler Bedeutung. Zur Zielerreichung verfügt die WL mit dem revidierten Landesversorgungsgesetz über eine moderne gesetzliche Grundlage sowie mit ihrer Kaderorganisation aus der Wirtschaft über das dazu notwendige Fachwissen.

In den letzten Monaten hat die WL einen Allgemeinen IKT-Minimalstandard erarbeitet, welcher im Rahmen der Nationalen Strategie zum Schutz vor Cyberangriffen (NCS) hilft, die Resilienz zu erhöhen. Basierend auf dem NIST Framework Core werden 106 Massnahmen beschrieben, wie Betreiber kritischer Versorgungsinfrastrukturen ihre IKT-Ressourcen schützen können. Der Allgemeine IKT-Minimalstandard wird demnächst der Öffentlichkeit vorgestellt und frei verfügbar sein. Bereits jetzt dient er dem Verband Schweizerischer Elektrizitätsunternehmen (VSE) als Grundlage zur Erstellung eines Pendants für die Strombranche. Dieser Branchenstandard, an dem die WL massgeblich mitgearbeitet hat, wird zur Selbstregulierung für diesen Wirtschaftssektor. Zurzeit sind ebenfalls IKT-Minimalstandards für Abwasser sowie die Wasser-, Gas- und Mineralölversorgung in Arbeit.

Die WL leistet damit nicht nur einen Beitrag zur Digitalisierung der Schweiz, sondern fördert die IKT-Resilienz der kritischen Versorgungsinfrastrukturen gegenüber Ausfällen, Störungen und Angriffen der IKT. Wie notwendig dies ist, wird Ihnen vorliegender Halbjahresbericht der Melde- und Analysestelle Informationssicherung MELANI eindrücklich vor Augen führen. Dabei wünsche ich Ihnen eine spannende Lektüre.

Werner Meier
Delegierter Wirtschaftliche Landesversorgung

3 Schwerpunktthema: Datenabflüsse

In der digitalen Welt werden pro Tag Millionen von Datensätzen mit persönlichen Angaben generiert und gespeichert. Sei es an der Kasse des Supermarktes beim Vorzeigen der Punktekarte, beim Bezahlen mit der Debit- oder Kreditkarte, beim Online Shopping, beim Checken der E-Mails oder beim Arztbesuch. Die Liste liesse sich beliebig fortsetzen. Auch beim Surfen im Internet hinterlässt jeder Einzelne täglich dutzende von Spuren.

Geraten diese Datensätze in falsche Hände, kann damit Missbrauch betrieben werden. Leider kommt es immer häufiger zu ungewolltem Datenabfluss, auch in der zweiten Jahreshälfte des vergangenen Jahres: Im Oktober 2017 teilte der Internetkonzern Yahoo! mit, dass der Datenabfluss aus dem Jahre 2013 mit über drei Milliarden Datensätzen offenbar alle Nutzenden betraf und nicht nur wie angenommen einen Teil davon.[1] Dies ist bislang der grösste Datenabfluss der Geschichte. Eine eindrückliche Zahl liefert auch das Portal «have I been pwned»[2]. Hier kann jeder überprüfen, ob seine E-Mail-Adresse jemals von einem Datenabfluss betroffen war. Als Gesamtzahl gestohlener Passwörter fungiert dort aktuell die unglaubliche Zahl von fast fünf Milliarden.

Auch in der Schweiz wurden in den vergangenen Monaten Datenabflüsse registriert. So gab die Swisscom bekannt, dass im Oktober 2017 Unbefugte Zugriff auf über 800'000 Kundendaten hatten. Galaxus/Digitec hatte im November 2017 den Verdacht, dass Betrüger in den Besitz von Kundendaten gekommen waren und auch der Krankenversicherer Groupe Mutuel informierte im Dezember 2017 die Öffentlichkeit über einen Datenabfluss. Ebenfalls im Dezember wurde MELANI auf 70'000 abgeflossene Zugangsdaten aufmerksam gemacht, die im Nachhinein der Schweizer Firma «DVD-Shop» zugeordnet werden konnten.

Mittlerweile regelmässig tauchen abgeflossene Datensätze mit Passwörtern, Kreditkartendaten oder anderen persönlichen Daten auf den einschlägigen Portalen auf. Allerdings ist es in vielen Fällen schwierig, die Herkunft, das Alter und die Qualität der Daten zu überprüfen. Bei einer Vielzahl von gestohlenen Datensätzen ist anzunehmen, dass deren Abfluss überhaupt nicht bemerkt worden ist.

3.1 Definition

Datenabflüsse sind Sicherheitsvorfälle, bei denen sich unbefugte Drittpersonen Personendaten, Geschäftsgeheimnisse oder andere Daten beschaffen, die nicht für sie bestimmt sind. Der Begriff «Datenabfluss» ist dabei sehr offen definiert und beinhaltet neben Datendiebstahl und Spionage auch Datenpannen, bei welchen Daten unabsichtlich zugänglich gemacht werden. So umfasst das Spektrum der betroffenen Daten dann auch nicht nur Passwörter und Kreditkartendaten, sondern auch Daten beispielsweise aus dem Gesundheits- und Finanzbereich.

---

1 http://www.sueddeutsche.de/digital/yahoo-hackerangriff-bei-yahoo-traf-alle-drei-milliarden-konten-1.3693671 (Stand: 31. Januar 2018).

2 https://haveibeenpwned.com/ (Stand: 31. Januar 2018).

3.2 Erpressen, sammeln und politische Motive

Eine häufige Vorgehensweise der Kriminellen, um mit Datenabflüssen Geld zu verdienen, dürfte sicherlich die Erpressung der Firma sein, bei der die Daten abgeflossen sind. Einer der ersten derartigen Fälle in der Schweiz geht auf das Jahr 2014 zurück. Damals hatte eine Gruppe mit dem Namen «Rex Mundi» ein Unternehmen in der Romandie mit der Veröffentlichung von Daten erpresst. Neben dem Unternehmen können aber auch die betroffenen Kunden Ziel einer solchen Erpressung sein.

Ein weiterer Verwendungszweck von Daten aus Datenabflüssen ist deren Einsatz für gezielte Angriffe. Im Untergrundmarkt haben sich Akteure darauf spezialisiert, möglichst viele Informationen über ein Opfer zusammenzutragen. Dazu nutzen sie neben frei verfügbaren Quellen auch Informationen, die aus Datendiebstählen stammen. Gelingt es den Angreifern, sich mithilfe der verschiedenen Daten ein genaues Bild des Opfers zu machen, sind auch sehr gezielte Angriffe möglich. In der Berichtsperiode wurde beispielswies die Verbreitung von E-Mails mit Schadsoftware beobachtet, bei welchen neben der Anrede mit Vor- und Nachnamen des Empfängers auch dessen Telefonnummer und/oder Postadresse aufgeführt war.

Datenabflüsse, die im Zusammenhang mit politischer Motivation stehen, sind speziell zu betrachten. Der bekannteste Fall ist die Veröffentlichung der sogenannten «Snowden-Files». Neben Snowden versuchen seither zahlreiche andere Akteure mit der gleichen Methode die Gesellschaft aufzurütteln oder zu verändern. Erinnert sei beispielsweise an die Veröffentlichung der «Panama-» und «Paradise-Papers». Mit diesen enthüllten die Akteure die weltweiten Geschäftspraktiken verschiedener Politiker und Prominenter im Finanzmarkt.

3.3 Auswirkungen

Doch was bewirken Datenpannen bei Betroffenen, welchen Schaden richten sie an? Diese Frage wird unterschiedlich beantwortet, weil jeder den Wert seiner Daten anders definiert. Bei Privatpersonen ist es den einen egal, ob und welche Daten erhoben werden und was mit diesen gemacht wird. Andere hingegen versuchen, das Datenaufkommen über die eigene Person möglichst kleinzuhalten. Dementsprechend schätzen Letztere den persönlichen Schaden viel höher ein.

Auch spielt die Art der abgeflossenen Daten eine Rolle und lässt sich systematisch in zwei Gruppen teilen: Daten, die problemlos zurückgesetzt werden können und solche, welche ein Leben lang bestehen bleiben. Passwörter und Kreditkartenangaben können rasch gewechselt werden und fügen dem Betroffenen nur kurzfristigen Schaden zu. Daten zur eigenen Gesundheit, zu persönlichen Vorlieben oder zur finanziellen Situation können nicht einfach «zurückgestellt» werden und fügen längerfristigen Schaden zu. So können Angreifer ein Opfer auch noch Jahre nach einem Datenabfluss in Schwierigkeiten bringen. Erschwerend kommt hinzu, dass ein Opfer in manchen Fällen von diesen Datenabflüssen gar nichts weiss und sich dementsprechend auch nicht dagegen wehren und schützen kann.

Bei Unternehmen führt unerwünschter Datenabfluss neben dem Aufwand und den Kosten vor allem zu Reputationsverlust. Dabei ist die Kundenkommunikation von entscheidender Bedeutung. Aus diesem Grund ist es für eine Firma äusserst wichtig, sich gut auf ein mögliches Datenleck vorzubereiten. Dies beinhaltet eine Notfallplanung, vorbereitete Kommunikation und klare Verantwortlichkeiten. MELANI empfiehlt im Fall von Datenabflüssen generell eine möglichst hohe Transparenz gegenüber den betroffenen Kunden. Es ist wichtig, diese so rasch wie

möglich zu informieren, um Folgeschäden möglichst klein zu halten. Dabei liegt die Kunst darin, nüchtern und unaufgeregt zu kommunizieren.

3.4 Benachrichtigung der Betroffenen

Wurden in einem Unternehmen Daten gestohlen, stellt sich schnell einmal die Frage nach der Benachrichtigung der Kunden. Die betroffene Firma hat die besten Möglichkeiten, diese Kommunikation durchzuführen. Nur sie hat den Überblick über die betroffenen Kunden, die Art und Menge der gestohlenen Daten und kann geeignete Massnahmen empfehlen, wie beispielsweise das Zurücksetzen der Passwörter. Dabei ist sicherzustellen, dass Unberechtigte nicht an Informationen über betroffene Personen gelangen können. So verlangte der Krankenversicherer «Groupe Mutuel» beispielsweise bei einer Auskunftsanfrage, ob man betroffen sei, eine Kopie des Personalausweises.

Eine noch grössere Herausforderung ist die Information der Betroffenen, wenn bei einem Datenabfluss die Herkunft der Daten nicht bekannt ist. Auf Portalen wie «Pastebin» tauchen immer wieder Kombinationen aus Benutzernamen und Passwort auf, deren Herkunft nicht eindeutig festgestellt werden kann. In der Vergangenheit hat MELANI schon mehrmals solche Listen mit abgeflossenen Datensätzen erhalten. In diesen Fällen hat MELANI jeweils ein Checktool zur Verfügung gestellt, damit Internetbenutzende selber herausfinden können, ob sie betroffen sind oder nicht. Vielfach kann auch anhand der Rückmeldungen aus der Bevölkerung die Herkunft der Daten im Nachhinein eruiert werden. Ist die Herkunft zugewiesen, ist es nach Ansicht von MELANI Aufgabe des Unternehmens, die Kunden wie auch die Öffentlichkeit über den Datenabfluss zu informieren.

3.5 Datenschutz

Der Schutz von Personendaten ist im Bundesgesetz über den Datenschutz (DSG) geregelt. Es bezweckt den Schutz der Persönlichkeit und der Grundrechte von natürlichen und juristischen Personen, über die Daten bearbeitet werden. Es wird zwischen Personendaten und besonders schützenswerten Personendaten unterschieden. Letztere Kategorie umfasst religiöse, weltanschauliche, politische oder gewerkschaftlichen Ansichten oder Tätigkeiten, die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, Massnahmen der sozialen Hilfe sowie administrative oder strafrechtliche Verfolgungen und Sanktionen. Bei deren Bearbeitung muss die Einwilligung der betroffenen Person ausdrücklich erfolgen. Das Datenschutzgesetz trägt auch dem Sicherheitsaspekt genügend Rechnung und definiert, dass Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden müssen.

Die Totalrevision des Schweizerischen Datenschutzgesetzes ist zurzeit im Gange. Es ist davon auszugehen, dass die Revision verschiedene Neuerungen der EU-Datenschutz-Grundverordnung aufgreifen wird, welche nach einer zweijährigen Übergangsfrist per 25. Mai 2018 durch alle EU-Mitgliedstaaten anzuwenden ist. So gilt die EU-Datenschutz-Grundverordnung auch für alle Schweizer Unternehmen mit oder ohne EU-Niederlassung, welche den 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. Die wichtigsten Änderungen durch die neuen Vorschriften sind im Überblick: das Recht auf vergessen werden; Datenverarbeitung ausschliesslich nach ausdrückli-

cher 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.

Besonders letztere Vorgabe wird den Umgang mit Datenpannen wohl grundlegend verändern und den Fokus verstärkt auf den Sicherheitsaspekt von Datenbanken und der Datenbearbeitung lenken. Allerdings wird diese Vorgabe die Cyber-Kriminellen wohl noch mehr motivieren, Profit aus Datenabflüssen zu erzielen. Ein Erpressungsangebot, das unter der Summe der Geldbusse liegt, würde vielleicht die eine oder andere Firma dazu verleiten, das billigere Angebot anzunehmen.

3.6 Ursachen und Schutz

Die Ursachen der Datenabflüsse sind vielfältig und reichen von Diebstahl durch Mitarbeitende über vergessene und schlecht gewartete Server bis hin zu Backups, die nicht ordnungsgemäss geschützt sind.[3]

3.6.1 Keine Datenleichen

Der Mensch neigt dazu, alle einmal erhobenen Daten irgendwo zu speichern, auch wenn diese schon lange keinen Nutzen oder keine Gültigkeit mehr haben. So finden sich wohl in jedem Adressbuch eines Mobiltelefons Kontakte, die schon lange nicht mehr gültig sind. Solch «vergessene» Daten vergrössern das Ausmass einer Datenpanne unnötig. Besonders bei einer Migration eines Servers ist darauf zu achten, dass die Daten auf den alten Systemen anschliessend gelöscht werden. Ebenfalls sollte jedem Datensatz eine Lebenszeit zugeordnet werden, damit dieser periodisch auf seine Gültigkeit überprüft wird. Auch sollten nur die Daten abgefragt und gespeichert werden, die wirklich notwendig sind. Dies ist einerseits eine Forderung des Datenschutzgesetzes (Art. 4 Abs. 2 DSG, Verhältnismässigkeit), andererseits reduziert es die Auswirkung eines Datenlecks sehr stark, wenn nur wenige Daten gespeichert worden sind.

3.6.2 Zugriff schützen / Verkehr reduzieren

Zugriffe von aussen sollten auf ein Minimum beschränkt werden und müssen besonders geschützt und überwacht werden. Jedes Unternehmen muss sich überlegen, wer Zugriff auf welche Daten benötigt und wie dieser Zugriff geschützt wird. Zum Beispiel sollten nicht verwendete Ports geschlossenen werden. Der Einsatz eines zweiten Faktors für die Authentisierung ist bei Zugriffen von aussen dringend empfohlen. Für den breiten Einsatz haben sich Verfahren mit «One Time Password (OTP)» bewährt, wie z. B. der weit verbreitete «Google Authenticator», der als App auf dem Smartphone installiert wird.

Auch ausgehender Verkehr sollte auf die nötigen Verbindungen reduziert werden. Viele Angriffe beruhen darauf, dass der infizierte Computer Code vom Internet nachlädt. Dies geschieht

[3] Die häufigsten Fallstricke werden in einer Top 10 Liste des OWASP Projekt dokumentiert (Open Web Application Security Project). Diese Liste wird regelmässig aktualisiert. https://www.owasp.org/

oft automatisiert. Das Verbieten von ausgehendem Verkehr erhöht somit die Hürde für einen Angreifer beträchtlich.

Generell und unabhängig davon, ob es ein unbedeutendes Kontaktformular oder eine wichtige Geschäftsanwendung ist, die vom Benutzer eingegebenen Daten sollten so rasch als möglich an ein Backend System weitergereicht werden, das nicht direkt vom Internet her erreichbar ist.

Jede Server-Software und Applikation muss stets auf dem neuesten Stand gehalten werden. Gibt es für eine Schwachstelle keinen Patch oder kann dieser nicht eingespielt werden, sind entsprechende risikomindernde Massnahmen zu treffen. Der Einsatz einer Web Application Firewall ist empfehlenswert: Es gibt eine Vielzahl von kommerziellen und Open Source-Produkten, welche eine Webanwendung zusätzliche schützen können. Die meisten dieser Produkte können auch Regeln gegen die häufigsten Verwundbarkeiten (OWASP Top 10) anbieten.

3.6.3 Schlecht geschützte Backups

Backups gehören zur Lebensversicherung jeder Firma, müssen jedoch den gleichen Sicherheitsanforderungen genügen, wie die produktiven Daten. Auch archivierte Daten auf externen Festplatten sollten verschlüsselt gespeichert werden.

3.6.4 Ungeschützte Passwörter

Befinden sich unter den abgeflossenen Daten Passwörter, sollten diese nicht auf einfache Weise entschlüsselt werden können. Dies bedingt den Einsatz einer Hashfunktion[4] sowie eines sogenannten Salts. Beim «Salzen» wird das Passwort mit einem weiteren, nur dem System bekannten Wert ergänzt und erst dann der Hashfunktion unterzogen. Es sollten dabei möglichst lange Salts verwendet werden, die pro Passworterstellung neu generiert werden. Ebenfalls wichtig ist die Verwendung einer langsamen Hash-Funktion. Die Berechnung des Passwort-Hashes wird dabei möglichst kompliziert und langsam durchgeführt. Den regulären Anwender stört es wenig, wenn das Anmeldeprozedere ein paar Millisekunden länger dauert. Für den Hacker, der die Berechnung millionenfach ausführen muss, verlängert sich die Rechenzeit so dagegen drastisch.

3.6.5 Diebstahl durch Insider

Daten werden manchmal auch durch noch aktive oder ehemalige Mitarbeitende entwendet, die aus Unzufriedenheit dem Unternehmen schaden oder sich einen persönlichen Vorteil verschaffen wollen. Dem entgegenwirken kann man, indem ein gutes und offenes Arbeitsklima geschaffen wird und indem über Probleme offen gesprochen werden darf. Wichtig ist aber auch dafür zu sorgen, dass die Mitarbeitenden nur auf Daten zugreifen dürfen, die sie für die Erledigung ihrer Arbeit benötigen. Ehemaligen Mitarbeitenden müssen umgehend alle Zugänge entzogen werden, was eine saubere Zugriffs-Policy voraussetzt.

---

[4] Eine Hashfunktion ist eine Abbildung, die effizient eine Zeichenfolge beliebiger Länge (hier Passwort) auf eine Zeichenfolge mit fester Länge (Hashwert) abbildet.

4 Lage national

4.1 Spionage

4.1.1 Neuer Angriff auf bundesinterne Systeme

Im Juli 2017 wurde die Spionagesoftware «Turla» auf einzelnen Servern des Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS) entdeckt. Die Malware ist in der Bundesverwaltung keine Unbekannte. Es war ebenfalls die Spionagesoftware «Turla», welche im Dezember 2015 den bundesnahen Technologiekonzern RUAG angegriffen hat, der u. a. für die Sicherstellung der Ausrüstung der Armee zuständig ist. Damals gelang es den Angreifern, mehr als 20 Gigabyte Daten zu entwenden. Im aktuellen Fall wurde die Malware bereits in der Frühphase entdeckt, bevor sie wichtige Daten stehlen oder sie im Netzwerk weitere angeschlossene Systeme befallen konnte. Dies, obwohl der Angreifer seine Infrastruktur und Werkzeuge ausgebaut und den Komplexitätsgrad des Vorgangs erhöht hat. Die zuständigen Bundesstellen konnten die notwendigen Überprüfungen rechtzeitig durchführen und geeignete Massnahmen treffen. Die Zusammenarbeit der einzelnen Bundesstellen war sehr gut und erlaubte es, Informationen zu den Angriffsmethoden und zu den technischen Indikatoren zusammenzutragen. Der Austausch solcher Indikatoren, sowohl national als auch international, ist ein zentrales Element, um laufende oder zukünftige Angriffe zu entdecken. Der Bundesrat, die Mitglieder des Sicherheitsausschusses des Bundesrats sowie die Präsidien der zuständigen Kommissionen wurden zeitnah informiert, wie es bei solchen Ereignissen üblich ist. Das VBS hat zudem wegen der Cyber-Angriffe auf seine Server bei der Bundesanwaltschaft Strafanzeige gegen Unbekannt eingereicht.[5]

4.2 Industrielle Kontrollsysteme

Regelmässig liest man in der Presse von gefährdeten, aus dem Internet erreichbaren industriellen Kontrollsystemen (Industrial control system ICS) wie Fabriksteuerungen, Pumpen von Wasserkraftwerken[6] oder medizintechnischen Geräten[7]. Diese Systeme sind deshalb in Gefahr, weil beispielsweise in einer der verwendeten Komponente eine Sicherheitslücke aufgetaucht ist oder weil diese nicht sicher genug konfiguriert worden sind.

Häufig wird nach Bekanntwerden solcher Fälle kritisiert, dass die Betreiber der betroffenen Infrastrukturen Updates nicht zeitnah einspielen. Es gibt aber durchaus Gründe, welche das Einspielen von Sicherheits-Patches herauszögern oder verunmöglichen. So kann beispielsweise das Update einer Komponente die Zertifizierung des Gesamtsystems gefährden. Viel wichtiger wäre es deshalb, dass die Systemlandschaft und das Netzwerk, in dem sich diese Geräte befinden, so robust gebaut und betrieben werden, dass Schwachstellen auftreten können, ohne die Kernfunktionen dadurch zu gefährden.[8] Auch In der Checkliste «Massnahmen

---

5 https://www.vbs.admin.ch/de/aktuell/medienmitteilungen.detail.nsb.html/68135.html (Stand: 31. Januar 2018).

6 http://www.spiegel.de/netzwelt/web/so-bedrohen-hacker-wasserversorgung-stromnetz-und-kliniken-a-1181325.html (Stand: 31. Januar 2018).

7 https://nakedsecurity.sophos.com/2018/02/01/hospital-mri-and-ct-scanners-at-risk-of-cyberattack/ (Stand: 31. Januar 2018).

8 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf (Stand: 31. Januar 2018).

zum Schutz von industriellen Kontrollsystemen» von MELANI fällt auf, dass das Patch-Management lediglich eine von elf Massnahmen darstellt. Die zehn anderen Massnahmen beinhalten andere risikomindernde Massnahmen: Eine robuste Netzwerkarchitektur garantiert beispielsweise, dass sich in der Netzwerkzone, in der das verwundbare Gerät eingebunden ist, im besten Fall nur Systeme befinden, die mit dem verwundbaren Gerät kommunizieren müssen. Zonenübergange sollten auf das unbedingt notwendige reduziert und gut überwacht werden. Mitarbeitende dürfen zu jedem Zeitpunkt nur diejenigen Rechte haben, die unbedingt nötig sind, um die vorgesehenen Aufgaben zu erledigen. Die zentrale Log-Auswertung ermöglicht zudem die Kontrolle, ob alle Systeme wie vorgegeben ablaufen. Sollte trotz allen Vorkehrungen dennoch ein Angriff registriert werden, hilft der Security Incident Management-Prozess. Ist die Reaktion auf einen Sicherheitsvorfall definiert und bei allen Involvierten eingeübt, lässt sich der potenzielle Schaden auf ein Minimum beschränken.

In der Fachliteratur wird der Ausgleich eines unvermeidbaren Risikos durch eine oder mehrere andere Verteidigungsstrategien als «Defense-in-Depth»[9] beschrieben. Ein grundsätzliches Beispiel einer ICS-Netzwerkarchitektur findet sich in Abbildung 1.

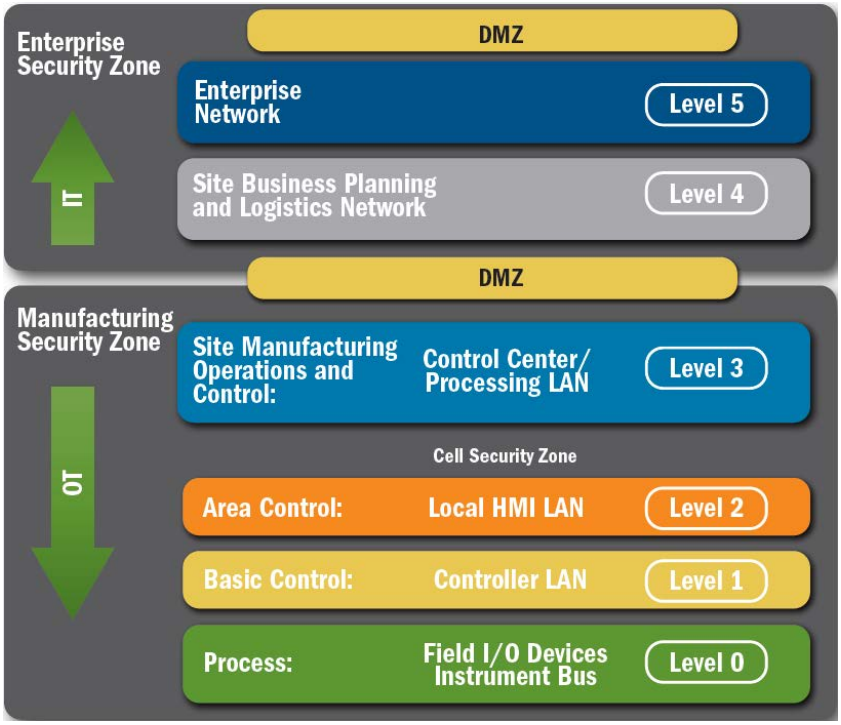

Abbildung 1: ICS Netzwerkzonenarchitektur des ICS-CERT[9]

Obwohl diese Empfehlungen für sich isoliert alle selbstverständlich und einfach in der Umsetzung sind, fehlen für die Durchführung in komplexen Systemlandschaften oft entsprechende Ressourcen. In vielen Fällen wird auch der termingerechte Abschluss des Projektes oder die betriebliche Einfachheit der Abläufe über die Sicherheit gestellt. Um die knappen Ressourcen dort einzusetzen, wo sie am meisten Wirkung erzielen, ist ein übergeordnetes Risikomanagement unabdingbar, bei dem Restrisiken erkannt und durch das Management getragen werden.

9 https://ics-cert.us-cert.gov/Abstract-Defense-Depth-RP (Stand: 31. Januar 2018).

Empfehlung:

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

Meldeformular MELANI

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

Checkliste mit Massnahmen zum Schutz industrieller Kontrollsysteme

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

4.2.1 Hacker, die den Takt vorgeben

Ein Herzschrittmacher ist ein batteriebetriebener Kleinstcomputer, der über die nötige Sensorik, Auswert-Elektronik und Aktor-Elemente in Form eines Impulsgebers verfügt. Damit kann dieser die Herzschläge überwachen und notfalls elektrisch stimulieren. Viele der kleinen Lebensretter verfügen zusätzlich über eine Funkschnittstelle, damit zur Analyse der Herzwerte und Anpassung der Konfiguration keine weiteren chirurgischen Eingriffe notwendig werden.

Das auf Kontrollsysteme fokussierte ICS-CERT des US-amerikanischen Department of Homeland Security (DHS) publizierte am 29. August 2017 Hinweise[10] zu Sicherheitslücken bei mehreren Herzschrittmachermodellen der Firma Abbott Laboratories. Die von MedSec Holdings Ltd entdeckten Schwachstellen ermöglichen die Manipulation von Daten, die über die Funkschnittstelle mit dem Implantat ausgetauscht werden. Der Sender des Angreifers müsste wohl zwar, wie bei einem Routine-Service beim Arzt, direkt auf den Körper aufgelegt werden, könnte dann aber sämtliche Lese- respektive Schreibvorgänge durchführen. Grund dafür ist, dass die Authentifizierung des Programmiergeräts vom vorgesehenen Standard abweicht. Gemäss einer Veröffentlichung[11] der amerikanischen Lebensmittel- und Arzneimittelbehörde FDA, die auch medizinische Geräte reguliert, hat ein solcher Angriff, der die Sicherheitslücken ausnutzt, noch nicht stattgefunden.

Die Herstellerfirma hat inzwischen Updates[12] für die betroffenen Geräte veröffentlicht. Diese lassen sich bei einem Besuch beim behandelnden Arzt einspielen. In der Schweiz mussten

10 https://ics-cert.us-cert.gov/advisories/ICSMA-17-241-01 (Stand: 31. Januar 2018).

11 https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm (Stand: 31. Januar 2018).

12 https://www.sjm.com/~/media/galaxy/patients/heart-vascular/arrhythmias/resources-support/cybersecurity/pacemaker-firmware-update-patient-guide-aug2017-us.pdf (Stand: 31. Januar 2018).

sich ca. 5000 betroffene Patienten[13] dem Prozedere unterziehen, was fast einem Siebtel der in der Schweiz eingesetzten Herzschrittmacher entspricht.

4.3 Angriffe (DDoS, Defacements, Drive-By)

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

4.3.1 DDoS-Erpressung mit berühmtem Namen

Erpressung ist derzeit eine beliebte Masche derjenigen Cyber-Kriminellen, die auf einen schnellen finanziellen Gewinn aus sind. Neben erpresserischer Software, genannt Ransomware und der Drohung, zuvor gestohlene Daten zu veröffentlichen, gehört auch die Drohung, einen DDoS-Angriff durchzuführen zum Repertoire der Angreifer – obwohl viele Angreifer gar nicht über die Kapazität verfügen, einen DDoS-Angriff zu tätigen. Sie nutzen dies nur als Drohgebärde, um den Opfern Angst einzujagen.

Oft übernehmen die Angreifer zudem Namen von Gruppierungen, die bereits aus früheren Angriffen bekannt sind. Sie begnügen sich damit, eine erpresserische E-Mail zu schicken, ohne sich dabei die Mühe zu machen, tatsächlich einen Angriff durchzuführen. Sie hoffen darauf, dass das Opfer den Namen in eine Suchmaschine eingibt und dann, beeindruckt von den Taten der implizierten Gruppe, die Lösegeldsumme zahlt.

Auch die DDoS-Erpressergruppe «Fancy Bear», welche im Sommer 2017 auftauchte und im November ebenfalls in der Schweiz aktiv war, bediente sich dieser Methode. Erstaunlicherweise wird dieser Name nicht durch eine Gruppe im DDoS-Bereich verwendet, sondern der Name gehört zu der wohl berühmtesten Spionagegruppe weltweit. Hinter «Fancy Bear» respektive dem bekannteren Aliasnamen «Sofacy» wird ein staatlicher Akteur vermutet, der auch Zero-Day-Exploits zu seinem Repertoire zählt. Da «Sofacy» bislang nicht in Zusammenhang mit DDoS-Erpressungen aufgefallen ist, liegt die Vermutung nahe, dass es sich hier um eine Gruppe handelt, die den Namen «Fancy Bear» verwendete, von der Bekanntheit der Gruppe profitieren wollte und sich dadurch einen höheren Ertrag versprach.

4.4 Social Engineering und Phishing

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

4.4.1 Phishing

Auch im zweiten Halbjahr 2017 wurden zahlreiche Phishing-E-Mails versendet. Der Inhalt der Mails ändert sich dabei nicht markant: Die einen fragen nach Kreditkartendaten, damit diese

[13] https://www.blick.ch/news/wirtschaft/sicherheitluecke-bei-herzschrittmachern-5000-schweizer-in-gefahr-id7255939.html (Stand: 31. Januar 2018).

«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.

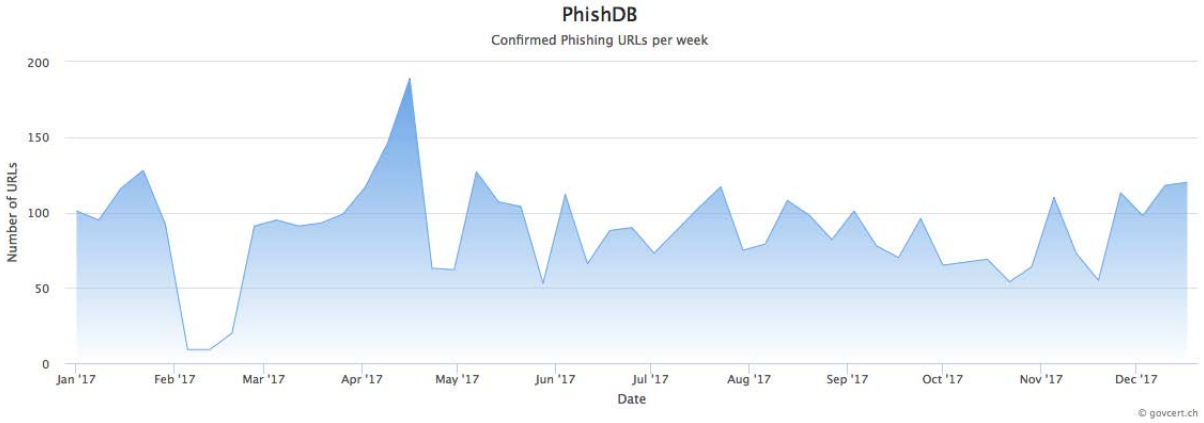

Abbildung 2: Gemeldete und bestätigte Phishing-Seiten pro Woche auf antiphishing.ch im Jahr 2017

Insgesamt wurden im Jahr 2017 4587 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 Jahr gesehen variiert. Die Gründe hierzu sind sehr verschieden: Zum einen gibt es ferienbedingte Schwankungen, da in der Ferienzeit weniger Phishing-Seiten gemeldet werden und zum anderen verschieben die Kriminellen ihre Angriffe regelmässig von Land zu Land.

4.4.2 Bill Swap Betrug – Austausch elektronischer Rechnungen im E-Mail Konto

Neben den Angriffen auf Kreditkartendaten haben Kriminelle vor allem Zugangsdaten zu E-Mail-Konten im Visier. Da jeder Online-Dienst eine Passwortrückstellung anbietet, mit der das Kennwort zurückgestellt werden kann, ist die eigene E-Mail-Adresse mittlerweile Dreh- und Angelpunkt für praktisch alle Internetdienstleistungen geworden. Allerdings bietet das E-Mail-Konto für Kriminelle weit mehr. Heute nehmen sich Kriminelle die Zeit, den E-Mail-Verkehr eines kompromittierten Kontos penibel nach brauchbarem Material zu durchforsten. Eine Methode, die MELANI im zweiten Halbjahr 2017 mehrfach gemeldet worden ist, ist das Durchsuchen des E-Mail-Kontos nach elektronischen Rechnungen. Finden die Betrüger eine solche aktuelle Rechnung wird diese aus dem E-Mail Eingang kopiert und anschliessend darin gelöscht. Der Angreifer hat nun genügend Zeit, die der Mail angefügte PDF-Rechnung zu manipulieren. Hierzu werden die Bankkontodaten des Rechnungsstellers geändert und die IBAN-Nummer des Betrügers eingesetzt. Das so veränderte Dokument wird dann anschliessend wieder dem E-Mail-Konto zugestellt. Der Betrüger braucht lediglich den Absender zu fälschen und wiederum die E-Mail-Adresse der rechnungsstellenden Firma einzutragen. Die Manipulation ist anschliessend kaum mehr zu erkennen.

Empfehlung:

Bei jeder Überweisung werden Informationen über das Empfängerkonto eingeblendet. Im besten Fall erscheint der Name oder zumindest das Bankinstitut des Empfängers. Diese Information sollten stets auf Plausibilität hin überprüft werden. Glücklicherweise haben Kriminelle nicht so viele Finanzagenten zur Verfügung, dass sie immer ein passendes Konto einblenden können. So passiert es mitunter, dass das Geld ins Ausland überwiesen werden soll, obwohl die Rechnung von einer Schweizer Firma ausgestellt wurde. Spätestens hier sollten Betroffene stutzig werden.

4.4.3 Phishing Office 365 - Der Schlüssel zum Büro

Seit Juni 2017 machen sogenannte «Office 365»-Phishing-E-Mails die Runde. Mit über 100 Millionen monatlichen Nutzern ist es nicht erstaunlich, dass das Office 365-Konto zu einem populären Ziel für Angreifer geworden ist.[14] Der Angriff startet mit einer gewöhnlichen Phishing-E-Mail, die beispielsweise vorgibt, dass die Grenze des Speicherplatzes überschritten sei und dass man sich zur Behebung des Problems einloggen soll. Es versteht sich von selbst, dass der angegebene Link auf eine betrügerische Webseite führt. Im Besitz der Office 365-Zugangsdaten können Angreifer verschiedene Dinge anstellen. Das häufigste Szenario ist das Setzen einer Weiterleitungsregel im betroffenen E-Mail-Konto. Danach wird der gesamte eingehende interne als auch externe E-Mail-Verkehr an ein von den Betrügern definiertes E-Mail-Konto gesendet und kann von den Betrügern mitgelesen werden. Wertvolle Ziele sind bei dieser Vorgehensweise die E-Mail-Konten von Firmen. So gewonnene Informationen können wiederum verwendet werden, um weitere Mitarbeitende anzugreifen. Da der Angreifer auch Zugriff auf das Adressbuch hat, kann er sehr gezielt einzelne Mitarbeitende innerhalb der Firma anschreiben. Angreifer versenden zuvor abgefangene E-Mails und manipulieren diese in der Weise, dass Mitarbeitende beispielsweise dazu aufgefordert werden, ein Dokument herunterzuladen. Um den Download zu starten, muss wiederum das Office 365-Passwort (auf einer manipulierten Webseite) eingeben werden. Betrüger arbeiten sich so in der anzugreifenden Firma Schritt für Schritt zu den für sie interessanten Personen vor.

Bei der gewünschten Zielperson angekommen, wird dann mit den zuvor gestohlenen Daten ein sehr gezielter CEO-Betrug durchgeführt. Denkbar ist auch, dass die Firma mit der gestohlenen E-Mail-Kommunikation erpresst wird oder dass die gestohlenen Daten an andere Betrüger weiterverkauft werden. Diese Methode kann auch für Wirtschaftsspionage verwendet werden.

[14] https://betanews.com/2017/08/30/office-365-phishing/ (Stand: 31. Januar 2018).

Empfehlung:

Arbeitet die Firma in der Office 365- Cloud, haben Angreifer mit den gestohlenen Zugangsdaten auch Zugriff auf sämtliche Dokumente der Firma. Solche Daten nur mit Benutzernamen und Passwort zu sichern, ist heutzutage äusserst fahrlässig. Aktivieren Sie deshalb wo immer möglich die 2-Faktor- Authentisierung.

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

4.5 Schwachstellen

4.5.1 Kundenaufträge auch am elektronischen Zahlschalter überprüfen

Das Zahlungsmanagementsystem «Smartvista» der Schweizer BPC Group wies im 2017 eine Sicherheitslücke auf, die für eine SQL-Injection ausgenutzt werden konnte[15]. Mit speziell formulierten und zeitlich richtig geplanten SQL-Abfragen auf der Transaktionsoberfläche des «Smart Vista» Front Ends (SFVE) wäre es einem Angreifer möglich gewesen, an eine Liste aller Benutzenden mit zugehörigen Passwörtern aus der dahinterliegenden Datenbank zu gelangen. Gemäss einer Mitteilung von BPC wurde das Unternehmen im Mai 2017 durch den Forscher Aaron Herndon der Sicherheitsfirma «Rapid7» auf die Lücke aufmerksam gemacht. Am 19. Juli desselben Jahres lieferte das Unternehmen einen Patch aus, der das Problem behebt.

4.6 Datenabfluss

Wie im Schwerpunktthema erläutert, kam es in der Schweiz auch im zweiten Halbjahr 2017 zu zahlreichen Datenabflüssen. In diesem Kapitel fassen wir bekannte Schweizer Vorfälle zusammen.

4.6.1 70'000 Zugangsdaten zum DVD-Shop aufgetaucht

Anfang Dezember 2017 wurde MELANI auf eine Liste mit Zugangsdaten bestehend aus Login und Passwort aufmerksam gemacht. Nach einer Prüfung wurde festgestellt, dass es sich um 70'000 Datensätze mit Bezug zur Schweiz handelte. Zu diesem Zeitpunkt war jedoch noch nicht klar, wo genau die Daten abgeflossen waren. MELANI entschloss sich dazu, die Daten in das MELANI-Checktool[16] zu integrieren, damit jede Person überprüfen konnte, ob ihr Benutzername betroffen war. Aufgrund von Rückmeldungen aus der Bevölkerung konnte MELANI anschliessend den betroffenen Webshop identifizieren. Es handelte sich um den «dvd-

[15] https://blog.rapid7.com/2017/10/11/r7-2017-08-bpc-smartvista-sql-injection-vulnerability/ (Stand: 31. Januar 2018).

[16] https://www.checktool.ch Für die Überprüfung ist nur die Eingabe der E-Mail-Adresse respektive des Benutzernamens notwendig. Diese Angaben werden nicht im Klartext an MELANI übermittelt und auch nicht gespeichert. (Stand: 31. Januar 2018).

shop.ch», welcher umgehend von MELANI informiert wurde. Der Betreiber des Shops hat daraufhin alle Passwörter zurückgesetzt und den Webshop deaktiviert. Gemäss Webseitenbetreiber handelte es sich um ältere Daten, die entwendet worden waren. Betroffene Kunden wurden durch ihn direkt informiert.

Empfehlung:

MELANI weist darauf hin, dass genügend lange Passwörter gewählt werden müssen, damit sie nicht einfach zu erraten sind. Pro Shop/Dienst sollte ein separates Passwort gewählt werden. Wo angeboten, sollte ein zweiter Faktor für das Login aktiviert werden.

4.6.2 Datenabfluss bei Schweizer Krankenversicherer

Die Krankenkasse Groupe Mutuel gab mittels Medienmitteilung bekannt, Hacker seien am 19. Dezember 2017 unter falscher Identität auf die 2012 lancierte externe IT-Plattform «ePremium Health» eingedrungen, um Daten zu stehlen. Diese Plattform ist für das Verkaufsnetz der Groupe Mutuel zur Erstellung von Offerten und Versicherungsanträgen bestimmt. Gemäss Angaben des Krankenversicherers wurden keine Versicherungspolicen, medizinische Berichte, Prämienrechnungen, Kostenbeteiligungsrechnungen und ähnliches gestohlen. Das interne IT-System der Groupe Mutuel, auf dem die Daten der rund 1,4 Millionen Kunden gespeichert sind, sei zu keinem Zeitpunkt in Gefahr gewesen. Nach dem Hackerangriff hat die Groupe Mutuel Anzeige gegen unbekannt eingereicht. Der Kantonspolizei Wallis gelang es anschliessend rasch, die mutmasslichen Täter zu identifizieren. Bereits am 28. Dezember 2017 wurde der erste Täter verhaftet. Einen Tag später konnte die Kantonspolizei Thurgau einen zweiten Verdächtigen fassen. Bei den mutmasslichen Tätern handelt es sich um einen 29-jährigen Schweizer und einen 30-jährigen Mazedonier. Beide wurden in Untersuchungshaft genommen. Die Untersuchung wird laut Polizei noch weitergeführt.[17]

Groupe Mutuel hat im Februar 2018 ein Formular für potenziell Betroffene publiziert, mit dem sie sich erkundigen können, ob sie vom Datenleck betroffen sind. Gefährdet sind vor allem Personen und Unternehmen, die im Zeitraum von 2012 bis heute eine Offerte von einem Vermittler oder Broker zu einer Versicherung der Groupe Mutuel verlangt haben.[18]

4.6.3 Krankheitsdaten bei Inkassofirma – Datenleck bei EOS

Ende Dezember 2017 berichtete die «Süddeutsche Zeitung»[19] über ein Datenleck beim schweizerischen Zweig der Inkassofirma EOS. Die EOS-Gruppe ist in insgesamt 26 Ländern aktiv und umfasst 55 Einzelunternehmen. Beim nun bekannt gewordenen Vorfall sind wahrscheinlich Daten in der Grössenordnung von rund drei Gigabyte abhandengekommen. Neben Angaben wie Namen, Adressen und die Höhe von geschuldeten Beträgen handelt es sich auch um weitere sensible Daten wie Krankenakten mit Angaben über Vorerkrankungen und

---

17 https://www.polizeiwallis.ch/medienmitteilungen/martinach-hackerangriff-auf-eine-versicherungsgesellschaft/ Stand: 31. Januar 2018).

18 https://www.groupemutuel.ch/de/clients-prives/page/cyberattaque.html (Stand: 31. Januar 2018).

19 http://www.sueddeutsche.de/digital/it-sicherheit-schwerwiegendes-datenleck-legt-zehntausende-schuldnerdaten-offen-1.3805589 (Stand: 31. Januar 2018).

Behandlungsdetails. Auch Ausweise und umfangreiche Kreditkartenabrechnungen sind Teil des Datenlecks. Die Datensätze reichen bis ins Jahr 2002 zurück.

Offenbar haben Ärzte auf einem Portal von EOS ganze Krankenakten hochgeladen, respektive hochladen können. Für welchen Zweck und unter welchen Auflagen dies geschah, ist nicht bekannt. Sensible Daten wie Krankendaten dürften für die Ausübung des Auftrags eines Inkassounternehmens nicht notwendig sein.

Auslöser des Datenabflusses soll bereits im April 2017 ein gezielter Angriff unter Ausnutzung der Sicherheitslücke «Apache Struts» gewesen sein. Laut EOS seien damals Anzeichen für einen Angriff entdeckt worden, allerdings habe dieser nie verifiziert werden können. Trotzdem sei der betroffene Server damals komplett neu aufgesetzt worden. Ob die Daten tatsächlich mit diesem Vorfall in Verbindung stehen oder ob es noch eine andere Lücke gegeben hat, ist nicht bekannt.

4.6.4 Datenabfluss auch bei Digitec

Am 6. November 2017 machte Digitec auf seiner Webseite publik, dass Daten aus einer alten Datenbank abhandengekommen sein könnten. Potenziell betroffen seien gemäss aktuellem Wissensstand Kundendaten von 2001 bis maximal Mitte 2014. Die mutmassliche Sicherheitslücke sei in der Zwischenzeit geschlossen worden und der neue Digitec-Shop nicht betroffen.[20] Wann genau der Datenabfluss stattgefunden hat, sei nicht bekannt.

4.7 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 zweiten Halbjahr 2017 gab es zahlreiche Infektionen mit Crimeware. Die Statistik in Figur 3 wiedergibt Daten von einzelnen Servern, auf welche sich infizierte Computer verbinden. Es gibt auch Malware, die ebenfalls eine hohe Bedeutung hat, aber nicht in der Statistik erscheint (wie zum Beispiel die e-Banking Malware Retefe).

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 zehn Jahren und verbreitet sich über eine im Jahr 2008 entdeckte und ebenso lange geschlossene Sicherheitslücke in Windows-Betriebssystemen. Auf Platz zwei folgt neu «gamarue»[21] – auch bekannt unter dem Namen «andromeda», ein Downloader, der weitere Schadsoftware nachladen kann. An dritter und vierter Stelle folgen die Schadsoftware «spambot» und «cutwail», die sich auf das Versenden von Spam und Schadsoftware spezialisiert haben. Das seit dem Angriff auf den Internetdienstleister «Dyn» bekannt gewordene *Bot*-Netzwerk «Mirai», welches Geräte im Internet der Dinge infiziert, fiel vom vierten auf den siebten Platz. Auf Platz neun folgt der erste E-Banking-Trojaner «Gozi».

---

20 https://www.digitec.ch/de/page/statement-zum-digitec-leck-6265 (Stand: 31. Januar 2018).

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

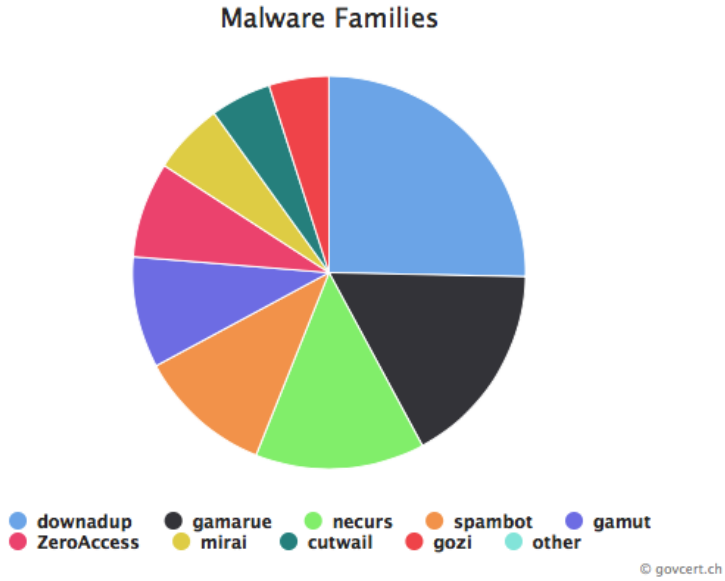

Abbildung 3: Verteilung der Schadsoftware in der Schweiz, welche MELANI bekannt ist. Stichtag ist der 31. Dezember 2017. Aktuelle Daten finden Sie unter: http://www.govcert.admin.ch/statistics/dronemap/

4.7.1 Ransomware

Auch in dieser Berichtsperiode wurden MELANI zahlreiche Fälle von Verschlüsselungstrojanern gemeldet. Ein funktionierendes Backup auf einem externen Medium, das durch die Verschlüsselungsschadsoftware nicht in Mitleidenschaft gezogen werden kann, ist dabei das A und O. Besser ist aber, es gar nicht so weit kommen zu lassen und entsprechende Vorkehrungen zu treffen. Die Verschlüsselung und somit der temporäre Verlust der Daten ist nämlich nur ein Teil des Problems. Ebenfalls ist zu berücksichtigen, dass in der Zeit des Zurückspielens des Backups allenfalls ein grosser Teil des Betriebes stillsteht. Da heute die meisten Firmen auf eine funktionierende IKT angewiesen sind, kann ein Stillstand je nach dem einen erheblichen finanziellen Verlust zur Folge haben. Hinzu kommt, dass gerade bei kritischen Infrastrukturen ein Nichtfunktionieren des Betriebes noch viel gravierendere Auswirkungen haben kann.

Empfehlung:

INFO

MELANI-Infoseite bezüglich Verschlüsselungstrojanern

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

4.7.2 E-Banking-Trojaner – «Retefe» immer noch weit verbreitet

Verschiedene E-Banking-Trojaner sind in der Schweiz mehr oder weniger aktiv. Darunter befindet sich beispielsweise die Malware «Dridex», welche die Fähigkeit hat, ihre Funktionen zu erweitern, um gezielt Geschäftskunden anzugreifen. Für diesen Zweck durchsucht «Dridex»

ein befallenes System nach Offline-Banking Software.[22] Der Trojaner «Gozi ISFB» verbreitet sich sowohl über Webseiteninfektionen als auch über verseuchte E-Mail-Anhänge. Der weltweit agierende «Trickbot» hat seine Zielliste im Jahr 2017 auch auf Schweizer Bankinstitute erweitert. «Trickbot» ist modular aufgebaut und wird laufend mit neuen Funktionen erweitert. «Emotet», ursprünglich ein e-Banking Trojaner, wird von den Angreifern auch für das Verbreiten anderer Malware z.B. Ransomware verwendet und bedient sich bei der Verbreitung vor allem gefälschter Rechnungen.

Eine der aggressivsten Schadsoftware in der Schweiz bleibt aber «Retefe». Sie hat in der Vergangenheit exklusiv die Länder Österreich, Schweden, Japan, Grossbritannien und die Schweiz angegriffen. MELANI hat «Retefe» bereits vor drei Jahren in ihrem Halbjahresbericht thematisiert. Im Gegensatz zu anderer Schadsoftware, welche sich auch über Webseiteninfektionen verbreiten, benutzt «Retefe» zur Verteilung ausschliesslich E-Mail. Dies geschah früher vor allem über gefälschte Rechnungen von Online Shops wie z. B. von Zalando oder Ricardo. Die neuesten Versionen imitieren vor allem Bundes- oder bundesnahe Stellen wie die Steuerverwaltung oder die Post.

Nach erfolgreicher Infektion ändert «Retefe» die Einstellungen des Browsers so, dass bestimmte Websites (namentlich die E-Banking-Portale einiger Schweizer Finanzinstitute) über einen Proxy-Server umgeleitet werden. Zusätzlich installiert «Retefe» ein Zertifikat auf dem Computer mit dem es möglich ist, wiederum Zertifikate für beliebige Finanzinstitute auszustellen und sich als solches auszugeben. So vermeidet die Schadsoftware eine sonst auftretende Zertifikats-Fehlermeldung, die das Opfer misstrauisch machen würde. Meldet sich ein Opfer via einen mit «Retefe» infizierten Computer im vermeintlichen E-Banking-Portal an, wird diesem ein QR-Code angezeigt. Dieser QR-Code führt zu einer Website, auf welcher das Opfer aufgefordert wird, eine App «zur Erhöhung der Sicherheit» – in Wahrheit jedoch eine Android-Schadsoftware, einen sogenannten SMS-Trojaner – herunterzuladen und zu installieren. Installiert das Opfer die angepriesene Android App, werden sämtliche von der Bank gesendeten SMS zur 2-Faktor Authentifizierung an einen Webserver im Ausland und damit an die Hacker weitergeleitet. Somit sind diese nun in der Lage, sich im E-Banking des Opfers einzuloggen und auch Zahlungen zu tätigen.

Im letzten Halbjahr erweiterte sich diese Vorgehensweise, indem die Täterschaft versucht hat, an Briefe mit so genannten Aktivierungsdaten zu gelangen. Diese Briefe werden in der Regel von der Bank per Briefpost an die Kundinnen und Kunden versendet und enthalten ein Mosaikbild, welches beim erstmaligen Login eines Gerätes ins E-Banking mit einer App eingescannt werden muss. Anschliessend wird das entsprechende Gerät von der Bank für die mobile Authentifizierungsmethode zugelassen. Die Angreifer versuchten mittels Social Engineering, an die Aktivierungsdaten zu gelangen und forderten das Opfer auf, diesen Brief einzuscannen oder zu fotografieren und an die Betrüger zu übermitteln.

Im September wurde die Schadsoftware zudem mit dem Exploit von «EternalBlue» ergänzt. Dies ist diejenige Lücke, welche bei der Verschlüsselungswelle «WannaCry» im Mai ausge-

[22] Halbjahresbericht 2016/2, Kapitel 4.6.1 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2016-2.html (Stand: 31. Januar 2018).

nutzt worden ist und weltweit für Schaden gesorgt hat. Mit der Implementation von «EternalBlue» dürfte «Retefe» vor allem die Verbreitung in Firmennetzwerken im Visier haben. Öffnet ein Mitarbeiter versehentlich einen verseuchten Anhang, kann sich die Malware auf den Computer verschieben, wo die Firma ihre E-Banking-Zahlungen durchführt. Dies funktioniert natürlich nur, sofern die Lücke noch nicht geschlossen worden ist.

Im Verlauf der Berichtsperiode erreichten MELANI immer wieder Meldungen von E-Mails mit «Retefe», welche sowohl eine korrekte Anrede als auch eine korrekte Telefonnummer des Empfängers im Betreff hatte. Meist handelte es sich bei diesen E-Mails um eine vermeintliche Kontaktaufnahmen der Eidgenössischen Steuerverwaltung (ESTV), in denen vorgegeben wird, dass es noch Fragen zur Steuererklärung gebe. Es gab zwar genügend Anzeichen, die einen Empfänger hätten misstrauisch machen sollen. Die aufgeführte eigene Telefonnummer hat vermutlich dennoch dazu geführt, dass einige Empfänger den Anhang geöffnet haben.

Von: Eidgenossische Steuerverwaltung ESTV [redacted]
Gesendet: Mittwoch, 21. Februar 2018 11:32
An: [redacted]
Betreff: Fragen zu der Steuererklarung (die Nummer 043 [redacted] ist unzuganglich)

Sehr geehrte(r) Herr/Frau [redacted]

Mein Name ist [redacted], ich bin Finanzinspektor und bin zuständig für Ihren Bezirk.

Es gibt einige Fragen zu Ihrer Einkommensteuererklärung.

Dieses Dokument beinhaltet die Liste von Fragen über Ihre Steuererklärung, sowie auch meine Kontaktnummer.

Freundliche Grüsse

[redacted]

Das Gemeindesteueramt

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Abbildung 4: Beispiel eines betrügerischen E-Mails mit der Schadsoftware Retefe und der Telefonnummer im Betreff

Wie die Angreifer die Daten von E-Mail-Adresse, Vor- und Nachnamen und vor allem der Telefonnummer verbinden konnten, ist unklar. Es gibt Hinweise, dass die Daten unter anderem aus einem Datenabfluss stammen könnten.

5 Lage International

5.1 Spionage

5.1.1 Naher Osten im Visier

Cyber-Spionage-Kampagnen lassen sich grob in zwei Kategorien unterteilen: In wirtschaftlich motivierte oder in diejenigen mit Ziel auf strategische, militärische und/oder politische Informa-

tionen. Nachfolgend sind einige Kampagnen ausgeführt. So machen beispielsweise die politischen Spannungen im Nahen Osten und dessen Wichtigkeit in der Erdöl- und Erdgasproduktion die Länder in dieser Region zu attraktiven Zielen der Cyber-Spionage.

5.1.2 Beispiel APT33

«Nicht nur politische oder wirtschaftliche Gegner haben interessante Daten – auch Informationen von Partnern können wertvoll sein.» So könnte der Slogan der Cyber-Spionage-Kampagne «APT33»[23] lauten, welche die US-amerikanische Sicherheitsfirma FireEye einer iranischen Stelle zuschreibt. APT33 ist mindestens seit 2013 aktiv und hat es besonders auf saudi-arabische, US-amerikanische und südkoreanische Ziele in den Bereichen Militär-, Zivilluftfahrt sowie Energie abgesehen. Von Mitte 2016 bis Anfang 2017 soll APT33 ein amerikanisches Luft- und Raumfahrtunternehmen kompromittiert und eine saudi-arabische Organisation mit Aktivitäten ebenfalls im Luftfahrtbereich ins Visier genommen haben. APT33 verbreitet ihre Malware-Programme über E-Mails, die als Arbeitsangebote getarnt sind. Für die Absender-E-Mail-Adresse wurden ähnlich lautende Domainnamen von saudischen und westlichen Luftfahrtfirmen registriert, die sowohl im zivilen als auch militärischen Bereich mit Saudi-Arabien zusammenarbeiten. Die Sicherheitsfirma FireEye geht davon aus, dass die erwähnten Angriffe darauf abzielten, an militärische Informationen der saudi-arabischen Luftwaffe zu kommen, um den Wissensstand der iranischen Luftwaffe zu erhöhen und Erkenntnisse in die militärische und strategische Entscheidungsfindung Teherans einfliessen zu lassen.

Im gleichen Zeitraum war die Spionagekampagne ebenfalls bei einer südkoreanischen Raffinerie aktiv. Im Mai 2017 erhielten zudem Mitarbeitende einer saudi-arabischen Firma und eines weiteren südkoreanischen Unternehmens, beide ebenfalls im Ölgeschäft tätig, solche E-Mails. Die als Jobangebot getarnten E-Mails enthielten ein Spionageprogramm und wurden vermeintlich von einer saudi-arabischen Erdölgesellschaft versandt.

FireEye soll eine Person, wahrscheinlich ein ehemaliges Mitglied der iranischen Regierung, identifiziert haben, welche mit diesen Vorfällen in Verbindung steht. Einige der verwendeten Malware-Programme enthielten zudem Wörter auf Farsi, der Amtssprache des Iran. Auch die Uhrzeiten und Tage, an denen die Attacken verübt worden sind sowie der Einsatz von spezifischen Schadprogrammen, welche auf iranischen Hacker-Websites zu finden sind, scheinen den Verdacht einer iranischen Täterschaft zu bestätigen.

Auch die bislang bekannteste mutmasslich iranische Cyber-Spionage-Kampagne «Shamoon», die ab 2012 Organisationen im Persischen Golf ins Visier nahm, konzentrierte sich auf den petrochemischen Sektor.

5.1.3 «Copy Kittens» – technische und strategische Entwicklung[24]

Am 29. März 2017 erklärte das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI), dass die Website der Tageszeitung «Jerusalem Post» manipuliert und für die Verbreitung von Schadprogrammen missbraucht worden war. Die Webseiteninfektion stehe wahr-

---

23 https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html (Stand: 31. Januar 2018).

24 http://www.clearskysec.com/tulip/ (Stand: 31. Januar 2018).

scheinlich im Zusammenhang mit einigen, nicht näher beschriebenen Auffälligkeiten im Netzwerkverkehr des Bundestags seit Januar 2017.[25] Im gleichen Monat bestätigte die israelische Cyber-Intelligence-Firma ClearSky die Infektion auf «Jerusalem Post» und machte auch Infektionen auf anderen israelischen Websites und der des palästinensischen Gesundheitsministeriums publik. Die Verantwortung für die Attacke schrieb sie der Spionagegruppe «CopyKittens» zu.[26] Die kompromittierten Websites enthielten von Oktober 2016 bis Ende Januar 2017 ein Javascript, welches ein spezifisches Tool für Penetrationstests für Webbrowser von einer eigens von den Hackern registrierten Domain herunterlud. Dabei wurde das Javascript nicht an jeden Website-Besucher ausgeliefert, sondern nur bei bestimmten ausgewählten Opfern.

Bei «CopyKittens» handelt es sich um eine mindestens seit 2013 aktive Cyber-Spionage-Gruppe, deren Name auf die Praxis zurückgeht, Codefragmente aus Online-Foren zu kopieren und diese für ihre Cyber-Angriffe zu verwenden. Die Gruppe hat es hauptsächlich auf Israel, Saudi-Arabien, die Türkei, die Vereinigten Staaten, Jordanien und Deutschland, aber auch auf Bedienstete der UNO abgesehen. Staatliche und wissenschaftliche Institutionen, Unternehmen der Verteidigungsindustrie, Zulieferfirmen des Verteidigungsministeriums und grosse Informatikunternehmen gehören unter anderem zu den Zielen dieser Gruppe.

Die Kampagne verbreitet sich neben den oben beschriebenen Watering-Hole-Angriffen auch über gezielte E-Mails mit schädlichem Anhang oder schädlichem Link. Ein Beispiel für Letzteres ist ein E-Mail an Mitarbeitende zahlreicher Regierungsorganisationen. Verschickt wurde das E-Mail Ende April 2017 von einem kompromittierten E-Mail-Konto. Der Titel des angefügten infizierten Dokuments verwies auf internationale Beziehungen zwischen dem Iran, Nordkorea und Russland. In zwei weiteren Fällen brach die Gruppe in die E-Mail-Konten von Personen ein, die mit dem eigentlichen Angriffsziel in Verbindung standen. Dabei wurden bestehende Unterhaltungen des legitimen Inhabers missbräuchlich verwendet, um ein E-Mail mit einem Link zu einer eigens dafür registrierten schädlichen Website zu senden.

Bereits seit 2013 erstellt und verwaltet die Gruppe falsche Facebook-Profile. Auf diesem Weg baut sie Vertrauen zu potenziellen Opfern auf und sammelt Informationen über diese für weitere Angriffe. So wurden über diese falschen Profile auch Links auf eine infizierte Website versendet. Um glaubwürdiger zu wirken, veröffentlichten die Profile auch harmloses Material und haben eine unverdächtige Anzahl an Freunden.

Schlussfolgerung:

2015 galt «Copy Kittens» noch als Angreifer mit nur durchschnittlichem Schadenpotenzial. Doch die neuesten öffentlich bekannt gewordenen Angriffe zeigen, dass sich die Gruppe scheinbar technisch und strategisch weiterentwickelt hat und neben online beschafften Malware-Programmen auch selbst entwickelte Werkzeuge einsetzt.

---

25 https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2017/Cyber-Angriff_auf_den_Bundestag_Stellungnahme_29032017.html (Stand: 31. Januar 2018).

26 http://www.clearskysec.com/wp-content/uploads/2017/07/Operation_Wilted_Tulip.pdf (Stand: 31. Januar 2018).

5.1.4 Die Gruppe OilRig entwickelt neue Angriffssysteme[27]

In der Vergangenheit zielten die Spionagekampagnen der Gruppe «OilRig» auf öffentliche und private Unternehmen in Nordamerika und Europa, wobei ihr besonderes Interesse der Erdöl- und Erdgasproduktion und dem entsprechenden Handel im Nahen Osten galt. OilRig hat ihr Arsenal im Berichtshalbjahr um neue Trojaner ergänzt und nimmt den Nahen Osten weiter unter Beschuss. Zwischen Juli und August 2017 wurden in mehreren Angriffen zwei neue Instrumente eingesetzt: die Backdoor «ISMAgent» und einen Injector für deren Installation. Der Injector besitzt eine komplexe Struktur und enthält Techniken, die die Entdeckung auf den Zielcomputern zusätzlich erschweren.

Am 23. August 2017 attackierte OilRig eine regierungsinterne Stelle der Vereinigten Arabischen Emirate über ein gezieltes Phishing-E-Mail mit zwei ZIP-Anhängen und einem Bild im E-Mail-Text. Da das Bild von einem externen Server heruntergeladen wurde, diente es wahrscheinlich zur Verifikation, ob der Empfänger das E-Mail öffnete. Der Angriff wies auch einige andere interessante technische Kniffe auf. So war die Absenderadresse nicht gefälscht, obschon als Absender eine interne Adresse der Firma angegeben war. Wahrscheinlich war «OilRig» mittels Phishing an die Authentifizierungsdaten eines legitimen E-Mail-Kontos in der gleichen Domäne gelangt, von dessen Account aus sie dann die oben beschriebene E-Mail versenden konnte. Beide ZIP-Dateien enthielten ein Word-Dokument. Im ersten war ein schädliches Makro versteckt, über das der Injector die erwähnte Backdoor installierte. Dabei verwendeten die Angreifer Social Engineering-Techniken, um die Empfänger dazu zu bringen, das Ausführen des Makros zuzulassen. Das zweite Dokument versuchte, eine Sicherheitslücke in Microsoft Word[28] auszunutzen, für die das Update erst vor kurzem herausgegeben worden war. Die Gruppe versucht, das Ausnutzen von technischen und menschlichen Schwächen zu kombinieren.

Nachdem die Hacker ins System eingedrungen sind, verwenden sie auf dem Schwarzmarkt erhältliche Programme wie z. B. «Mimikatz», um sich innerhalb der Firma die notwendigen Authentifizierungsdaten zu beschaffen und um sich im Firmennetzwerk von Computer zu Computer zu bewegen. Gemäss Sicherheitsdienstleister «Palo Alto» soll die Gruppe auch sogenannte Supply-Chain-Angriffe[29] durchführen: Diese Methode besteht darin, nicht direkt das eigentliche Ziel anzugreifen, sondern den Umweg über einen Dienstleister der Firma zu gehen. Da dieser Zugänge zum Netz des Ziels hat oder Software und Hardware liefert, kann das Ziel indirekt angegriffen werden. Weil eine Firma in der Regel mehrere Dienstleister hat, hat der Angreifer mit dieser Methode eine grössere «Auswahl» an Möglichkeiten (und Schwachstellen), um den Angriff durchzuführen. Diese Methode wird immer häufiger verwendet, wie auch im Kapitel «Internationale Angriffe» des Halbjahresberichtes 1/2017[30] beschrieben wird: Laut

---

27 https://researchcenter.paloaltonetworks.com/2017/10/unit42-oilrig-group-steps-attacks-new-delivery-documents-new-injector-trojan/ (Stand: 31. Januar 2018).

28 CVE-2017-0199 Microsoft Word Office/WordPad Remote Code Execution Vulnerability

29 https://researchcenter.paloaltonetworks.com/2017/12/unit42-introducing-the-adversary-playbook-first-up-oilrig/ (Stand: 31. Januar 2018).

30 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2017-1.html (Stand: 31. Januar 2018).

den jährlichen Prognosen von Kaspersky zu den fortgeschrittenen Bedrohungen 2018 dürfte sich diese Bedrohung im laufenden Jahr noch verschärfen[31].

Schlussfolgerung:

Grundsätzlich gehört die Schweiz zwar nicht zu den Zielen der OilRig-Gruppe. Da es in der Schweiz aber zahlreiche Zulieferer von spezifischen Produkten und Dienstleistungen im petrochemischen Umfeld gibt, sind Angriffe auch in der Schweiz denkbar.

5.1.5 Werbeflächen auf Facebook von angeblich russischer Firma zu Propagandazwecken gekauft[32]

Im letzten Halbjahresbericht wurde die Einmischung von Drittländern in die US-amerikanischen Präsidentschaftswahlen mit Hilfe gezielter Cyber-Attacken thematisiert. Ziele waren nicht nur die Systeme zur Auszählung der Wahlzettel (diesbezüglich gibt es keine Hinweise auf erfolgreiche Manipulation) und E-Mail-Korrespondenz der demokratischen Partei. Die US-amerikanischen Nachrichtendienste erklärten, dass parallel auch Desinformationskampagnen insbesondere über die sozialen Netzwerke geführt worden waren. Vor kurzem wurde auch ein angeblich russisches Unternehmen mit einer während den US-amerikanischen Präsidentschaftswahlen auf Facebook durchgeführten Propagandakampagne in Verbindung gebracht. Die «Internet Research Agency» soll Werbeflächen auf Facebook gekauft haben, um politische Positionen der russischen Führung zu verbreiten. Mehr als 3300 Werbeanzeigen sind auf die russische Kampagne zurückzuführen.[33] Sie wurden von über 470 falschen Profilen verbreitet und beworben. Die Namen der beiden US-Präsidentschaftskandidaten wurden zwar in einigen Posts sporadisch genannt, aber in erster Linie wurden sozialpolitische Inhalte zu heiklen Themen wie beispielsweise der gleichgeschlechtlichen Partnerschaft, Immigration oder Recht auf Waffenbesitz verbreitet. Einige Posts sollten schliesslich gar keine ideologischen Kontroversen vermitteln, sondern lediglich im Netz Panik verbreiten und Chaos stiften. Die Zeitung «Washington Post» nennt beispielsweise eine Falschmeldung im Zusammenhang mit einem Chemikalien-Leck im Bundesstaat Louisiana. Die Propaganda wurde gezielt betrieben, d. h. dass diese Inhalte nur für Personen in bestimmten Regionen sichtbar waren.

Bereits im Januar 2017 haben die US-amerikanischen Nachrichtendienste Russland der Einmischung in die Präsidentschaftswahlen bezichtigt.[34] Russland soll auch sogenannte Trolls bezahlt haben, die in den sozialen Netzwerken falsche Nachrichten verbreiten und die öffentliche Meinung beeinflussen sollen. Nach diesen Vorwürfen versprach der Vorstandsvorsitzende von Facebook, Mark Zuckerberg, Falschinformationen auf seiner Plattform zu bekämpfen.

---

31 https://www.kaspersky.com/about/press-releases/2017_kaspersky-labs-threat-predictions-for-2018 (Stand: 31. Januar 2018).

32 https://www.washingtonpost.com/politics/facebook-says-it-sold-political-ads-to-russian-company-during-2016-election/2017/09/06/32f01fd2-931e-11e7-89fa-bb822a46da5b_story.html?utm_term=.936611ed98fb (Stand: 31. Januar 2018).

33 http://www.wired.co.uk/article/facebook-twitter-russia-congress-fake-ads-2016-election-trump (Stand: 31. Januar 2018).

34 http://www.zeit.de/politik/ausland/2017-01/hacker-angriff-us-wahl-russland-barack-obama-geheimdienste (Stand: 31. Januar 2018).

5.2 Datenabflüsse

Der Berichtszeitraum war einmal mehr geprägt durch mehrere Fälle von massivem Datendiebstahl, die in den Medien für Schlagzeilen sorgten.

5.2.1 Equifax

Zu den spektakulärsten gehörte zweifellos der Angriff auf Equifax: eines der grössten Kreditratingunternehmen der USA. Am 7. September 2017 meldete das Unternehmen, bereits im Juli einen unerlaubten Zugriff auf seine Netzwerke entdeckt zu haben. Der Eintrittspunkt war offenbar die Sicherheitslücke «Apache Struts», für die Equifax keinen Patch installiert hatte. Über diese Lücke wurden möglicherweise die persönlichen Daten von 143 Millionen Kundinnen und Kunden in den Vereinigten Staaten entwendet. Was diesen Fall abgesehen von der hohen Zahl von Betroffenen besonders heikel macht, ist die Menge an persönlichen Daten und Daten zur finanziellen Situation, auf die das Unternehmen Zugriff hat und mit denen es die Kreditrisiken berechnen kann. Dazu zählt unter anderem die Sozialversicherungsnummer («Social security number, SSN»[35]). Der Angriff auf Equifax machte die Sicherheitsrisiken in Zusammenhang mit dieser eindeutigen Identifikationsnummer deutlich. Ursprünglich diente die SSN zur Identifizierung von Einzelpersonen im Sozialversicherungswesen, hat sich aber im Laufe der Zeit zu einem eindeutigen Personenidentifikator in verschiedenen Bereichen wie etwa der medizinischen Versorgung, bei den Steuern oder auch der Kreditvergabe entwickelt. Der Diebstahl dieser Nummer eröffnet weitreichende Möglichkeiten für betrügerische Handlungen und Identitätsdiebstahl. Dies umso mehr, wenn gleichzeitig andere persönliche Daten ihrer Inhaberin oder ihres Inhabers erbeutet werden.

5.2.2 Wirtschaftsprüfungs- und Beratungsfirma

Der Medienrummel hatte sich kaum gelegt, als «The Guardian» am 25. September 2017 einen weiteren Vorfall publik machte, der wiederum ein grosses amerikanisches Unternehmen betraf.[36] Laut Informationen der englischen Zeitung war der E-Mail-Dienst von Deloitte, einer der vier grössten Wirtschaftsprüfungsgesellschaften der Welt («The Big Four»), seit Oktober oder November 2016 das Ziel von Cyber-Attacken. Über ein ungenügend gesichertes Administrator-Konto sei es möglich gewesen, auf den E-Mail-Verkehr zwischen Deloitte und seinen wichtigsten Kunden zuzugreifen, die in der Azure-Cloud von Microsoft gespeichert sind. Der Sicherheitsstandard des Unternehmens stand dabei ganz besonders im Fokus der Kritik, vor allem nachdem bekannt geworden war, dass potenziell kritische Elemente seiner Netzinfrastruktur auf dem Internet sichtbar waren (namentlich offenes RDP, VPN-Logindaten).[37] Zu den Tätigkeitsbereichen von Deloitte gehören auch Beratungen betreffend Cyber-Sicherheit für Unternehmen, die in vielen sensiblen Sektoren tätig sind. Im Juni 2017 wurde Deloitte von Gartner zum fünften Mal in Folge zum weltbesten Unternehmen im Bereich der Sicherheitsberatungen gewählt.

---

35 https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/statistik--register-und-forschung/ahv-nummer.html (Stand: 31. Januar 2018).

36 https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails (Stand: 31. Januar 2018).

37 https://www.theregister.co.uk/2017/09/26/deloitte_leak_github_and_google/ (Stand: 31. Januar 2018).

5.2.3 Erpressung mit Daten zu Fahrgewohnheiten

Das Silicon Valley blieb ebenfalls nicht von Datendiebstählen verschont. Im November bestätigte Uber, dem Unternehmen seien persönliche Daten von 57 Millionen Kundinnen, Kunden und Fahrern gestohlen worden. Das Unternehmen war bereits seit Ende 2016 über Einzelheiten dieses Vorfalls unterrichtet. Laut einem Bericht von Bloomberg[38] liess sich der Ursprung des Diebstahls auf eine private GitHub-Seite, die von Uber-Ingenieuren genutzt wird, zurückverfolgen. Die Täter konnten dort Login-Daten stehlen, die ihnen Zugang zu sensiblen Informationen verschafften, die Uber im Cloud-Service von Amazon hostet. Danach erpressten sie das Unternehmen mit Erfolg: Dieses bezahlte offenbar 100'000 Dollar im Austausch für die entwendeten Daten und dafür, dass Stillschweigen über den Diebstahl bewahrt wird. Mit der Zahlung dieses Lösegeldes und der versprochenen Vernichtung der Daten war diese Geschichte aber noch lange nicht abgeschlossen: Der Fall wurde schliesslich doch publik. Indem das Unternehmen, nachdem es vom Datendiebstahl erfahren hatte, sich dafür entschied, weder die Behörden noch die Opfer darüber zu unterrichten, ist es seinen rechtlichen Verpflichtungen nicht nachgekommen. Verschiedene Gerichtsverfahren sind momentan im Gang. Ob das Unternehmen nach der ersten Lösegeldzahlung weiter erpresst wurde, ist nicht bekannt.

5.2.4 Datenträger verloren

Dass Datenabflüsse nicht immer durch Sicherheitslücken oder schlecht konfigurierte Systeme verursacht werden, zeigt ein Fall aus Grossbritannien. Im Oktober 2017 hat ein Passant auf Londons Strassen einen USB-Stick mit unverschlüsselten Daten in der Grössenordnung von 2.5 Gigabyte gefunden. Darauf abgespeichert waren zum Teil sensible Informationen zum Flughafen Heathrow wie beispielsweise Informationen zu Standorten von Überwachungskameras, Fluchtwegen und Zeiten von Polizeipatrouillen. Der Finder hatte den USB-Stick einer Zeitung übergeben, die dann den Vorfall publik machte. Wie der USB-Stick auf die Strasse gelangte, ist unklar.

Schlussfolgerung:

Das Minimieren von Cyber-Risiken ist ein ganzheitlicher Prozess und muss auch physische Sicherheitsvorkehrungen umfassen. Dabei muss klar geregelt werden, welche Daten überhaupt auf externen Medien gespeichert werden dürfen und welche Sicherheitsmassnahmen (beispielsweise welche Verschlüsselungsstärke) anzuwenden sind.

Weitere Informationen finden Sie im Schwerpunktsthema in Kapitel 3.

5.3 Industrielle Kontrollsysteme

5.3.1 «Dragonfly» späht die Infrastruktur der Energieversorger aus

Im Juli berichtete die New York Times, dass ein Kernkraftwerk in Kansas seit Mai 2017 im Visier von Hackern sei[39]. Seither wurden mehrmals Cyber-Angriffe auf den Energiesektor in

[38] https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data (Stand: 31. Januar 2018).

[39] https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html (Stand: 31. Januar 2018).

den USA und in Europa bekannt[40,41]. Auch wenn die Medienberichte den Eindruck erwecken, dass Angriffe auf den Energiesektor zunehmen und eine neue Gruppe mit dem Namen «Palmetto Fusion» für Aufruhr sorge, dürften all diese Operationen auf einen einzigen seit 2011 aktiven Akteur mit Namen «Dragonfly» herunterzubrechen sein.[42] Seit 2013 greift «Dragonfly» alias «Havex», «Energetic Bear», «Crouching Yeti» usw. den Energiesektor in den USA und in Europa an. Ab 2017 erlebten diese Angriffe, die unter dem Namen «Dragonfly 2.0» subsumiert sind, eine auffallende Intensivierung und verbesserten sich auch technisch.

«Dragonfly 2.0» nutzt für die Angriffe Spearphishing-Mails[43] mit infizierten Anhängen oder Links sowie speziell präparierte Webseiten aus dem Umfeld der Opfer, sogenannte Watering Holes[44]. Die kompromittierten und für die Angriffe verwendeten Webseiten weisen auf das Zielpublikum von «Dragonfly» hin: im Energiesektor tätige Unternehmen, Händler im Energiesektor, auf den Energiesektor spezialisierte Anwälte sowie Produzenten von Informatiklösungen für die europäische und US-Industrie. Die Angreifer versuchen so an Zugangsdaten kritischer Netzwerke zu gelangen. Das US-amerikanische Softwareunternehmen Symantec bezeichnet in seinem Bericht zu «Dragonfly 2.0» neben den Opfern in den USA und der Türkei auch eine angegriffene Firma in der Schweiz. MELANI konnte diese Aussage nicht verifizieren. Diesbezüglich wurden noch keine Opfer in der Schweiz identifiziert.[45]

---

40 https://www.wired.com/story/russian-hacking-teams-infrastructure/ (Stand: 31. Januar 2018).

41 https://www.independent.ie/irish-news/news/exclusive-eirgrid-targeted-by-state-sponsored-hackers-leaving-networks-exposed-to-devious-attack-36003502.html (Stand: 31. Januar 2018).

42 https://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat-energetic-bear (Stand: 31. Januar 2018).

43 http://blog.talosintelligence.com/2017/07/template-injection.html (Stand: 31. Januar 2018).

44 https://www.riskiq.com/blog/labs/energetic-bear/ (Stand: 31. Januar 2018).

45 https://www.watson.ch/Digital/Schweiz/472496967-Droht-ein-Blackout--Hacker-attackieren-Schweizer-Energiesektor (Stand: 31. Januar 2018).

Schlussfolgerung:

Spionage gegen Informatiknetzwerke im Energiesektor kann mehreren Zwecken dienen. Einerseits kann sich der Angreifer zu den Netzwerken einen Zugang verschaffen und so Informationen stehlen, um sich einen strategischen und ökonomischen Vorteil zu verschaffen. Andererseits ermöglicht die Kontrolle über Rechner kritischer Netzwerke im Bedarfsfall, Prozesse zu manipulieren oder zu beeinträchtigen.

Derzeit ist kein Fall von Sabotage bekannt, der durch «Dragonfly» – in welcher Version auch immer – verübt worden ist. Es ist aber nicht auszuschliessen, dass «Dragonfly» in Zukunft ebenfalls beabsichtigt, solche Angriffe auszuführen, insbesondere wenn sich die politische Lage ändert. So könnten die aktuellen Spionageversuche auch dazu dienen, sich einen Überblick über Möglichkeiten zu verschaffen, um zukünftig für alle politischen Eventualitäten gewappnet zu sein. Angriffe der «Sandworm» Gruppe – ein anderer Akteur mit ähnlicher Ausprägung, der im Jahr 2015/2016 das Stromnetz der Ukraine sabotierte – haben gezeigt, dass es eine monatelange Vorbereitung braucht, um zu verstehen, wie die angegriffenen Kontrollsysteme konfiguriert sind und welche Befehlskombinationen zur angestrebten Sabotageaktion nötig sind. Problematisch ist, dass bereits Aufklärungsversuche bei fehlerhafter Ausführung zu unbeabsichtigten Kollateralschäden führen können. Die beobachteten Angriffsversuche zeigen die Wichtigkeit der Anwendung einer breiten Palette an Massnahmen wie in Kapitel 4.2 beschrieben.

5.3.2 Angriff gegen Sicherheitskontrollsysteme

Im Dezember 2017 veröffentlichten mehrere Sicherheitsfirmen Berichte über eine Schadsoftware mit dem Namen «Triton/Trisis», die Prozesssicherheitslösungen von Industriesteueranlagen im Visier hat. Die Schadsoftware, die Mitte November 2017 entdeckt worden und seit mindestens August 2017 aktiv ist, greift sehr spezifisch einzelne Konfigurationen des Systems «Triconex» der französischen Firma Schneider Electric an. Es wurde von mindestens einem Ziel gesprochen, das sich im Nahen Osten befinden soll.

Bislang fokussierten die Angriffe direkt auf die Steuerungen des Hauptprozesses. Eine Prozess-Sicherheitslösung hingegen überwacht und kontrolliert den Betrieb einer Anlage. Übersteigt beispielsweise der Druck oder die Temperatur des zu überwachenden Prozesses eine kritische Grösse, bei der die Anlage Schaden nehmen kann, werden automatisch Gegenmassnahmen (wie z. B. eine Abschaltung oder die Verhinderung einer Operation) eingeleitet. Gelingt es, ein solches Sicherheitssystem so zu manipulieren, dass bei einem Fehlverhalten die automatische Abschaltung verhindert wird, kann eine Anlage beschädigt oder sogar zerstört respektive Menschen geschädigt oder getötet werden. Mancherorts greift ein Operator manuell in ein System ein, um diese Massnahmen auszulösen.

Gezielte Angriffe auf industrielle Kontrollsysteme sind immer noch selten. «Triton/Trisis» ist erst die fünfte bekannte Schadsoftware, die spezifisch auf industrielle Steuerungen ausgerichtet ist. Die bekannteste Schadsoftware in diesem Zusammenhang ist «Stuxnet», eine 2010

entdeckte Schadsoftware zur Störung bzw. Zerstörung von Zentrifugen iranischer Urananreicherungsanlagen. Aktuellere Beispiele sind die Angriffe im Dezember 2015[46] und 2016[47] auf die Stromversorgung in der Ukraine unter Einbezug der Malware «Blackenergy» resp. «Industroyer/Crashoverride».

Schlussfolgerung:

Solche Angriffe wurden bislang sehr zurückhaltend eingesetzt. Dies dürfte damit zusammenhängen, dass eine solche Operation immer die Gefahr eines unkontrollierbaren Kollateralschadens birgt, was dann auch unkalkulierbare Konsequenzen für den Angreifer haben könnte. Im vorliegenden Fall wurde dieser Umstand den Angreifern zum Verhängnis. Ihre Manipulationsversuche mit der Malware verursachten eine automatische Notabschaltung des angegriffenen Systems. Die Untersuchung dieser Abschaltung führte zur Entdeckung der Malware. Deshalb richten sich solche Angriffe in der Regel sehr gezielt gegen eine spezifische Systemkonfiguration und sie sind entsprechend aufwändig. Ein solcher Aufwand ist für pekuniär orientierte Angreifer kaum zu rechtfertigen und wird typischerweise nur von Staaten betrieben. Das System «Triconex» ist zwar in der Industrie zahlreich im Einsatz, allerdings ist jede Implementierung einzigartig und ein Angriffsvektor kann ohne signifikant grösseren Aufwand nicht auf andere Systeme übertragen werden. Der Fokus auf Prozess-Sicherheitslösungen zeigt aber die Absicht der Angreifer, möglichst grossen physischen Schaden am System selbst oder dem gesteuerten analogen Prozess anzurichten.

5.3.3 Experimenteller Hackerangriff auf Flugzeug durch das DHS

An der Konferenz «CyberSat – Security in Aerospace» in den USA stehen Cyber-Angriffe in den Bereichen Satellit und Luftfahrt im Fokus. Ein Vertreter des US-Heimatschutzministeriums (DHS) gab an der CyberSat im November 2017 bekannt, dass es den DHS-Sicherheitsexperten anlässlich eines Experiments im September 2016 gelungen sei, ins Computersystem einer Boeing 757 am Flughafen Atlantic City einzudringen[48]. Das Flugzeug ist zuvor vom DHS gekauft worden, um mögliche Schwachstellen im Bereich von Cyber-Angriffen zu eruieren. Es handelt sich dabei um einen Flugzeugtyp, der u. a. bei vielen US-Fluggesellschaften zum Einsatz kommt. Der Angriff erfolgte aus der Ferne und ohne Mithilfe von Insidern. Für den Hackerangriff wurden die Funkverbindungen des Flugzeugs genutzt. Die Schwachstelle, die für den Cyber-Angriff ausgenutzt wurde, sei von der DHS innerhalb von zwei Tagen entdeckt worden. Grund für dieses Experiment dürfte ein Vorfall im April 2015 gewesen sein. Damals behauptete der IT-Sicherheitsexperte Chris Robert via Twitter, dass er Schwachstellen in den Passagier-Unterhaltungssystemen (IFE) der Flugzeugtypen Boeing 757-200, Boeing 737-800, Boeing 737-900 und Airbus A-320 entdeckt und ausgenutzt habe, die es zulassen, auf kritische Systeme der On-Board-Elektronik zuzugreifen.[49] Das Experiment zeigt die Wichtigkeit einer

---

46 MELANI Halbjahresbericht 2015-2, Kapitel 5.3.1, https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2-2015.html (Stand: 31. Januar 2018).

47 MELANI Halbjahresbericht 2016-2, Kapitel 5.3.1, https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2016-2.html (Stand: 31. Januar 2018).

48 https://www.bleepingcomputer.com/news/security/dhs-team-hacks-a-boeing-757/ (Stand: 31. Januar 2018).

49 MELANI Halbjahresbericht 2015/1, Kapitel 5.3.3, https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2015-1.html (Stand: 31. Januar 2018).

sauberen physischen Trennung der Avionik (Aviatik und Elektronik) von den extern erreichbaren Informations- und Kommunikationssystemen, sodass auch bei Fehlkonfigurationen keine Verbindung zwischen den beiden Netzwerken ermöglicht und ausgenutzt werden kann.

Schlussfolgerung / Empfehlung:

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

Checkliste mit Massnahmen zum Schutz industrieller Kontrollsysteme

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

5.4 Angriffe (DDoS, Defacements, Drive-By)

5.4.1 DDOS

DDoS-Angriffe waren auch in dieser Berichtsperiode ein rege genutztes Instrument für Angreifer mit verschiedenen Motivationen. Der Schaden, der durch eine solche Attacke ausgelöst wird, hängt massgeblich von der Notwendigkeit ab, um jeden Preis einen Online-Service aufrechtzuerhalten. Die Angreifer sind sich dieser Tatsache absolut bewusst, weshalb sie sich immer systematischer auf ganz bestimmte Branchen konzentrieren – vor allem auf solche, für die eine Online-Präsenz aus ökonomischer Sicht zwingend ist. So war im zweiten Halbjahr 2017 die Spielbranche Ziel mehrerer Attacken. Einer dieser Angriffe, der besonders viel Aufsehen erregte, richtete sich gegen die nationale Lotterie Grossbritanniens. Am 30. September war es während 90 Minuten nicht möglich, online oder über die mobile App Tipps abzugeben. Der Zeitpunkt der Attacke war geschickt gewählt, weil die Störung am Samstagabend vor der Ziehung der Lottozahlen erfolgte: in einer Zeit also, in der üblicherweise Hochbetrieb herrscht. Der Grund für diesen Angriff ist nicht bekannt und es wurde auch keine erpresserische Forderung publik gemacht.

Mit dem Hype rund um die Kryptowährungen sind die verschiedenen Plattformen, über die solche Währungen gekauft oder umgetauscht werden können, ebenfalls zu einer beliebten Zielscheibe für DDoS-Angriffe geworden. Ein Beispiel für diesen Trend ist die Attacke gegen die Kryptowährung «Electroneum», die speziell für Smartphones entwickelt wurde. Dieser Vorfall hat das Unternehmen dazu gezwungen, die Lancierung ihrer mobilen App zu verschieben.

Während die Urheber von DDoS-Angriffen ständig auf der Suche nach neuen Opfern sind, fügen sie ihrem Arsenal auch immer neue Waffen hinzu. Schlecht gesicherte vernetzte Geräte

werden zunehmend breit ausgenutzt.[50] 2017 machte die «Pulse Wave»-Taktik von sich reden, die vom Anbieter für Sicherheitslösungen «Imperva Incapsula»[51] beschrieben wurde. Im Gegensatz zu herkömmlichen Angriffen, deren Intensität kontinuierlich zunimmt, bevor sie ihren Höhepunkt erreichen, umfasst eine «Pulse Wave»-Attacke eine Reihe von Angriffswellen, die jede sofort ihre maximale Stärke von bis zu 350 Gbit/s erreicht. Diese Wellen wiederholen sich manchmal während mehrerer Tage. Der Erfolg solcher Angriffe beruht teilweise auf den Besonderheiten einer hybriden DDoS-Abwehr, was bedeutet, dass erst dann eine Cloud-basierte Lösung eingesetzt wird, wenn die Attacke ein gewisses Niveau erreicht und auf Anwendungsebene nicht mehr bewältigt werden kann. «Pulse Wave»-Angriffe richten besonders grosse Schäden an, weil die Überlastgrenze sofort erreicht wird. «Imperva Incapsula» geht davon aus, dass diese Angriffstaktik in Zukunft regelmässig eingesetzt wird.

5.4.2 Ransomware: Bad Rabbit

Ende Oktober wurden die Ängste, die «WannaCry» und «NotPetya» ausgelöst hatten, durch eine neue Ransomware erneut geschürt. Diese Verschlüsselungssoftware mit dem Namen «Bad Rabbit» hatte sich über gefälschte Updates von Adobe Flash verbreitet. Offenbar wurde auch der Exploit «Eternal Romance» genutzt, um in das System der Opfer-Unternehmen einzudringen, ebenso wie «Mimikatz» zum Erschleichen von Login-Daten. Gemäss der Sicherheitsdienstleisters «Group IB» ist der Schadcode eine modifizierte Version von «NotPetya»[52], mit einem anderen Verschlüsselungsalgorithmus. Die meisten Opfer von «Bad Rabbit» befinden sich in Russland, aber einige Fälle wurden auch aus anderen Ländern gemeldet, namentlich aus der Ukraine, Deutschland und der Türkei.

5.4.3 Kryptowährungen

Im vergangenen Jahr standen Kryptowährungen nicht nur im Zentrum des Interesses der Bevölkerung und der Medien. Auch Kriminelle suchen nach Möglichkeiten, um vom rasanten Preisanstieg zu profitieren. Bei einigen Angriffen wurden die Plattformen selbst unter Beschuss genommen. Mit Hilfe von oft höchst ausgeklügelten Methoden können Kriminelle so auf einen Schlag enorm hohe Geldsummen stehlen. So wurde beispielsweise der Mining-Marktplatz «NiceHash» im Dezember 2017 um mehr als 70 Millionen Dollar erleichtert, und der Börsenplattform «Coincheck» wurde im Januar 2018 Kryptowährung im Wert von über einer halben Milliarde Dollar entwendet. Diese Vorfälle sind zwar im Einzelnen noch nicht ganz geklärt, aber sie machen die Risiken im Zusammenhang mit der Zentralisierung einer grossen Anzahl von Währungen auf ein und denselben Plattformen deutlich. Die Plattformen waren allerdings nicht die einzigen Ziele: Massgeschneiderte Angriffe richteten sich auch gegen einzelne Besitzerinnen und Besitzer von virtuellen Währungen. Die «New York Times» berichtete über eine besonders heimtückische Vorgehensweise[53], mit der mehrere Kryptoanleger in den Vereinigten Staaten ins Visier genommen wurden. In diesen Fällen gelang es den Angreifern, sich die Telefonnummern von Einzelpersonen zu beschaffen. Diese wurden gezielt ausgewählt, weil

---

50 Siehe Halbjahresbericht 2016/2 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2016-2.html (Stand: 31. Januar 2018).

51 https://www.incapsula.com/blog/pulse-wave-ddos-pins-down-multiple-targets.html (Stand: 31. Januar 2018).

52 https://www.group-ib.com/blog/badrabbit (Stand: 31. Januar 2018).

53 https://www.nytimes.com/2017/08/21/business/dealbook/phone-hack-bitcoin-virtual-currency.html (Stand: 31. Januar 2018).

sie potenziell über grosse Mengen von virtuellen Währungen verfügen. Dazu riefen sie die Mobilnetzbetreiber ihrer Opfer an und überredeten diese mit Hilfe von Social Engineering dazu, die Mobiltelefonnummer dieser Personen neu an ein Gerät in ihrer Kontrolle zu vergeben. Danach war es für die Täterschaft ein Leichtes, mithilfe der Mobilnummer die Passwörter zurückzusetzen und so auf die mit dieser Nummer verbundenen Konten zuzugreifen.

Eine weitere Methode besteht darin, Computerrechenleistung der Internet-Nutzerinnen und Nutzer zu kapern und so Kryptogeld zu schürfen. Spezielle Scripts, welche in Webseiten eingebaut werden, damit direkt über den Browser geschürft werden kann, wurden 2017 mehrfach beobachtet. Dieser Trend wird in Kapitel 6.2 des vorliegenden Berichts behandelt.

5.5 Schwachstellen

Zahlreiche schwerwiegende Schwachstellen machten in der Berichtsperiode Schlagzeilen. Höhepunkt war die Veröffentlichung der Schwachstelle «Spectre/Meltdown» in Prozessoren verschiedener Hersteller. Diese Art von Lücken, welche nicht mit einem einfachen Update geflickt werden können, zwingt die Sicherheitsverantwortlichen, neue Strategien zu definieren, um die Auswirkungen möglichst klein zu halten. Die «Spectre/Meltdown»-Lücke wird im nächsten Halbjahresbericht detailliert behandelt.

5.5.1 Lücke in bislang als sicher geltenden Verschlüsselungsstandard WPA2

Im Oktober 2017 publizierten zwei Forscher der Universität Leuven eine Schwachstelle im Verschlüsselungsstandard WPA2. Mit dieser Schwachstelle namens «KRACK», kurz für «Key Reinstallation AttaCK», ist es möglich, verschlüsselte Daten mitzulesen und auch Verbindungen zwischen zwei Geräten – etwa einem Browser und einem Web-Server – nachzuweisen. Dies hört sich zunächst sehr kritisch an. Es müssen aber spezielle Voraussetzungen erfüllt sein, damit diese Lücke ausgenutzt werden kann. Insbesondere muss sich ein Angreifer in unmittelbarer Nähe des WLAN-Gerätes aufhalten und die Funksignale empfangen können. Die Lücke kann also nicht breit aus dem Internet ausgenutzt werden. Ebenfalls ist es nicht möglich, Zugriff auf das WLAN-Passwort oder auf den Router zu erhalten, beispielsweise um später direkt auf das Gerät zuzugreifen. Geknackt werden ausschliesslich einzelne bestehende Verbindungen.

Diese Lücke basiert nicht auf einem Programmierfehler, sondern auf einem Designfehler des WPA2-Standards.

Einschätzung:

Sicherheitsrelevante Internetdienste wie zum Beispiel das Online-Banking werden bereits im Browser verschlüsselt, was in der Adresszeile mit https:// angezeigt wird. Die Verschlüsselung dieser https-Verbindungen ist durch die vorliegende Sicherheitslücke nicht gefährdet. Betroffen ist die darüber liegende Verschlüsselung der WLAN-Funkverbindung.

Trotzdem ist es empfehlenswert, die durch die Firmen für diese Lücke bereitgestellten Updates so rasch wie möglich zu installieren.

5.5.2 ROBOT – Die Rückkehr einer Schwachstelle

Erneut für Schlagzeilen sorgte der sogenannte «Bleichenbacher Angriff». Dies erstaunt, da dieser bereits vor 20 Jahren entdeckt worden ist. Eine systematische Überprüfung ergab, dass 27 der 100 populärsten Domänen immer noch verwundbar gegen diese Art des Angriffs sind. Darunter befinden sich beispielsweise auch Facebook und Paypal. So wurde die Lücke «The Return of Bleichenbacher's Oracle Threat» (Die Rückkehr von Bleichenbachers Oracle Bedrohung) oder kurz ROBOT genannt.

Der Schweizer Kryptograph Daniel Bleichenbacher erkannte 1998, dass die Fehlermeldungen eines SSL-Servers Informationen über die zu entschlüsselnden Daten preisgeben. Durch geschickt gewählte und mehrfach wiederholte Anfragen, kann man nach und nach eine Nachricht entschlüsseln. Der aktuelle TLS-Standard 1.2 verwendet weiterhin die fehlerbehaftete Version RSA im Standard PKCS #1 v1.5. Damit die Angriffe dennoch ins Leere laufen, sollte ein Server bei einem nicht korrekt formatierten Datenblock anstatt der entschlüsselten Daten Zufallsdaten zurückmelden und damit den Handshake weiter durchführen. Um mögliche Timing-Angriffe zu verhindern, müssen die zurückgegebenen Zufallsdaten schon vor der Entschlüsselung erzeugt werden. Das gesamte Verfahren ist extrem komplex. Dass diverse Server über keine korrekte Implementation verfügen, ist deshalb nicht erstaunlich.[54]

Beim aktuellen ROBOT-Angriff werden neben den obgenannten Fehlermeldungen auch andere Möglichkeiten wie beispielsweise TCP-Verbindungsabbrüche, Timeouts oder Protokollfehler genutzt, um einen verwundbaren Server zu erkennen. Insgesamt sind Produkte von verschiedenen Herstellern betroffen. Besonders problematisch sind dabei Geräte, deren «End of Life Cycle» bereits erreicht ist und bei denen demzufolge keine Updates mehr bereitgestellt werden.

5.5.3 Lücke in Sicherheitschip des Herstellers Infineon

Forscher haben im Oktober 2017 eine Schwachstelle bei der Erzeugung des RSA-Schlüssels in den Sicherheitschips von Infineon entdeckt. Dadurch ist es möglich, mithilfe des öffentlichen Schlüssels den privaten Schlüssel zu berechnen. Die Lücke für den als ROCA bezeichneten Angriff, steckt in einer Softwarebibliothek auf dem Chip. Diese wird benutzt, um die RSA-Primzahlen zu generieren. Diese sind nun offenbar zu schwach. Ein öffentlicher RSA-Schlüssel besteht aus zwei Zahlenwerten. Einer davon ist das Produkt aus zwei grossen, zufällig erzeugten Primzahlen. Wer nun die beiden Primzahlen kennt, kann den privaten Schlüssel berechnen. Der Aufwand zur Berechnung ist allerdings erheblich, was das Ausmass der Lücke relativiert. So würde man bei einer Schlüssellänge von 2048 Bit 141 CPU Jahre benötigen. Trotzdem ist es möglich, die Lücke mit ausreichend Rechenleistung auszunutzen. Die betroffenen Chips von Infineon werden in diversen Produkten eingebaut, beispielsweise in Smartcards, mobilen Endgeräten und in Notebooks. Estland als Vorreiter der Digitalisierung im Alltag – oder genauer gesagt die estnische eID – war ebenfalls betroffen. Dies hat die Regierung dazu bewogen, sämtliche der betroffenen 760.000 Zertifikate dauerhaft in ihren Systemen zurückzuziehen und zu blockieren.

---

54 https://www.golem.de/news/robot-angriff-19-jahre-alter-angriff-auf-tls-funktioniert-immer-noch-1712-131607-2.html (Stand: 31. Januar 2018).

5.5.4 Lücke noch vor Veröffentlichung des Betriebssystems

Wie jedes Betriebssystem ist auch MacOS regelmässig von Schwachstellen betroffen. Der Zeitpunkt, wann Drittparteien die Schwachstellen publik machen, ist für ein betroffenes Unternehmen immer ungünstig. In vorliegenden Fall gab es aber wohl keinen schlechteren Zeitpunkt: Kurz vor der Veröffentlichung des Betriebssystems «MacOS 10.13 High Sierra» Ende September 2017 veröffentlichte der Sicherheitsforscher und ehemalige NSA-Mitarbeiter Patrick Wardle eine Zero-Day-Lücke in diesem System. Auch ältere Versionen des Systems sind betroffen. Mit dieser Lücke ist es möglich, alle auf dem Computer gespeicherten Passwörter, den sogenannten Passwortmanager, auszulesen. Darin können beliebige sensitive Daten wie Kreditkartennummern, Passwörter für E-Mail-Konten oder Webshops gespeichert werden. Mit einem entsprechenden Schadprogramm, das per E-Mail-Anhang auf den Computer gelangt oder auch in eine legitime App verpackt wird, kann die entdeckte Lücke ausgenutzt und auf die sensiblen Daten zugegriffen werden. Der Fehler wurde bereits Anfang September 2017 an Apple gemeldet. Apple konnte aber nicht mehr rechtzeitig ein Update bereitstellen und High-Sierra wurde mit der Schwachstelle ausgeliefert.[55]

Anfang September 2017 hat Wardle bereits Details zu einer Methode publiziert, mit der sich eine Sicherheitsfunktion von «High Sierra» ohne grossen Aufwand umgehen lässt. Die betroffene Funktion «Secure Kernel Extension Loading» soll das Laden von Drittanbieter Kernel-Erweiterungen ohne Zustimmung des Nutzers verhindern.

5.6 Präventive Massnahmen

5.6.1 Trainings-Malware beschäftigt Antivirenhersteller

Über drei Jahre hinweg fiel den Sicherheitsforschern des japanischen Software- und Dienstleistungsanbieter Trendmicro[56] immer wieder dieselbe Malware auf, die sich gegen Personen in einflussreichen Positionen des südkoreanischen Energie- und Transportsektors richtete. Die Angriffe wurden unter dem Pseudonym «OnionDog» zusammengefasst. Auch weitere Firmen stiessen auf die Malware, analysierten sie und veröffentlichten Berichte[57]. Bei genauerer Untersuchung hat sich jedoch herausgestellt, dass «OnionDog» Teil einer gross angelegten Übungsanlage ist.

Die infizierten Geräte kommunizierten zwar mit einem Command and Control System, erhielten von diesem allerdings nie Befehle. Das System registrierte lediglich die Infektion. Die dahinterliegenden Adressen konnten dem südkoreanischen National Cyber Security Center (NCSC) zugeordnet werden. Es stellte sich heraus, dass die Malware Teil der «Ulchi Freedom Guard»-Übung war, die von Südkorea und den Vereinigten Staaten organisiert worden war.

---

55 http://www.zdnet.de/88313439/macos-high-sierra-sicherheitsforscher-macht-zero-day-luecke-oeffentlich/?inf_by=5a91d408671db898358b4e40 (Stand: 31. Januar 2018).

56 https://blog.trendmicro.com/trendlabs-security-intelligence/oniondog-not-targeted-attack-cyber-drill/ (Stand: 31. Januar 2018).

57 http://zhuiri.360.cn/upload/APT-C-03-en.pdf (Stand: 31. Januar 2018).

Empfehlung:

Realitätsnahe Übungen sind zwar zu begrüssen, doch sollte die Malware nicht aus dem Übungsszenario ausbrechen. So gewinnen Akteure mit bösartigen Absichten neue Erkenntnisse und benutzen diese für künftige Angriffe. Im schlimmsten Fall wird einem solchen Angriff weniger Priorität beigemessen, da man die Schadsoftware im Zusammenhang mit der vergangenen Übung kennt und als gefahrlos einstuft. Ein weiterer Aspekt sind voreilige Schlussfolgerung bezüglich der Attribution. Die über 200 öffentlich gefundenen Malware-Instanzen im aktuellen Fall liessen die Spekulationen über Ursprung und Absicht des Angreifers nur so sprudeln. Schuldzuweisungen können allerdings schnell zu ungewollter Eskalation führen. Wird Malware im Rahmen einer Übung eingesetzt, muss sichergestellt sein, dass diese die Übungsanlage nicht verlässt oder zumindest ausserhalb der Übungsanlage nicht funktioniert.

Eine gute und wiederholte Sensibilisierung der Mitarbeitenden ist einer der Hauptpfeiler, wenn es um Sicherheit im Internet geht. Übungen sind eine Möglichkeit, eine solche Sensibilisierung zu erreichen. Um einen reibungslosen Ablauf zu garantieren, sollten vor der Durchführung eines solchen Tests zumindest alle an der Infrastruktur beteiligten Akteure informiert werden: Es sind dies insbesondere die Registrierungsstelle der Top-Level-Domain (für .ch-Domänen ist dies SWITCH), Registrar und Hosting-Provider sowie gegebenenfalls der (externe) E-Mail-Anbieter. Schliesslich ist auch eine Ankündigung an MELANI sinnvoll, damit allfällige Meldungen im Sinne der Veranstalter der Awareness-Kampagne beantwortet werden können und durch MELANI keine Massnahmen gegen die Website eingeleitet werden.

Meldeformular MELANI

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

5.6.2 Umregistrierung von APT-Domänen

Die Gruppe «Fancy Bear» (auch bekannt als «APT28», «Sofacy» oder «Strontium») nutzt Domainnamen, die den Namen bekannter Firmen oder Produkte ähnlich sind, um Links oder Absender vertrauenswürdig erscheinen zu lassen. Bei den Angreifern sehr beliebt waren aufgrund der weiten Verbreitung auch Bezeichnungen mit einer offensichtlichen Anspielung auf Microsoft Produkte wie livemicrosoft[.]net oder rsshotmail[.]com.

Vor Gericht konnte Microsoft die Hintermänner der Kampagne zwar nicht zur Verantwortung ziehen. Den Anwälten des Software-Riesen gelang es jedoch, den Richter in Bezug auf die Markenrechte davon zu überzeugen, die Domänen auf Microsoft umschreiben zu lassen[58]. Somit verbanden sich Opfer ab dem Zeitpunkt der Umregistrierung nicht mehr mit Servern unter der Kontrolle der Angreifer, sondern mit solchen unter der Hoheit von Microsoft. Dadurch

[58] http://www.zdnet.com/article/us-election-hack-microsoft-wins-latest-round-in-court-against-fancy-bear-phishers/ (Stand: 31. Januar 2018).

wurde es möglich, die Opfer zu identifizieren und zu informieren, damit diese ihre Geräte bereinigen konnten.

5.6.3 Rescam-Bot – Mittels künstlicher Intelligenz gegen Vorschussbetrüger

Bei Vorschussbetrügereien werden den potenziellen Opfern seit Jahren haarsträubende Geschichten aufgetischt mit dem Ziel, diese zu einer Zahlung zu bewegen.[59] Die bekanntesten davon sind wohl die nigerianischen Prinzen, die behaupten, gegen eine vorgeschossene Gebühr das Erbe des Monarchen antreten zu können.

Die neuseeländische Non-Profit-Organisation Netsafe[60] schätzt den Schaden durch diese Betrugsart auf 12 Milliarden Dollar jährlich. Da sich Netsafe bewusst war, dass das Versenden solcher Betrugsversuche kaum verhindert werden kann, hat die Organisation einen anderen Lösungsansatz gewählt. Sie versuchte mittels eines mit künstlicher Intelligenz ausgestatteten Chatbots[61], die Betrüger möglichst lange zu beschäftigen. Über eine E-Mail-Adresse können dem Bot die betrügerischen E-Mails weitergeleitet werden. Der Chatbot analysiert den Inhalt der E-Mail, generiert sinnvolle Antworten und verstrickt die Angreifer so in lange Diskussionen. Indem der Chatbot den Angreifer möglichst lange beschäftigt, hält er diesen hoffentlich von anderen realen Angriffen fern. Beispielhafte Kommunikationsverläufe können auf dem Twitter-Konto[62] von rescam mitverfolgt werden. Die so erzeugte Kommunikation sorgt manchmal auch für ein Schmunzeln und zeigt die Unbeholfenheit der Betrüger, wenn sie mit ihren eigenen Maschen hingehalten werden.

6 Tendenzen und Ausblick

6.1 Netzneutralität

Netzneutralität bezeichnet das Prinzip, wonach alle Daten beim Transport durch das Internet gleichbehandelt werden, unabhängig von Senderin und Sender, Empfängerin und Empfänger, Dienst, Anwendung, Gerät oder Inhalt. Sie will also vor diskriminierenden Eingriffen in den Datenverkehr schützen. Verhaltensweisen, welche unter dem Thema Netzneutralität diskutiert werden, sind insbesondere die Blockierung, Priorisierung und Verlangsamung von Diensten sowie Produktdifferenzierung beim Internetzugang. Die Netzneutralität soll also zum Beispiel sicherstellen, dass Mobilfunkanbieter VoIP-Dienste nicht blockieren, Anschlussanbieter ihr gebündeltes IP-TV-Angebot nicht gegenüber Streaming-Diensten bevorzugen, Peer-to-Peer-Protokolle und Videoübertragungen nicht gedrosselt und Messenger- und Streaming-Dienste bezüglich Abrechnung des verbrauchten Datenvolumens gleichbehandelt werden.

---

59 https://www.skppsc.ch/de/faq/was-versteht-man-unter-vorschussbetrug/#was-versteht-man-unter-vorschuss-betrug (Stand: 31. Januar 2018).

60 https://www.netsafe.org.nz/ (Stand: 31. Januar 2018).

61 https://www.rescam.org/ (Stand: 31. Januar 2018).

62 https://twitter.com/rescambot/ (Stand: 31. Januar 2018).

In den USA hat die Telekommunikations-Aufsichtsbehörde (Federal Communications Commission FCC) am 14. Dezember 2017 eine Regulierung[63] erlassen, mit welcher von der FCC im Jahr 2015 erlassene Bestimmungen[64] zur Netzneutralität wieder rückgängig gemacht wurden. Konkret wurden Internet-Anbieter juristisch umklassifiziert und sind nun nicht mehr Telekommunikationsdienste und «Grundversorger» (common carriers), sondern wieder lediglich Informationsdienste und unterstehen deshalb nicht mehr der Regulierung und Aufsicht durch die FCC, welche bislang über die Einhaltung der Netzneutralität wachte.

Von Seiten mehrerer Bundesstaaten und auch aus dem Parlament gibt es Versuche, gegen den Entscheid der FCC vorzugehen.

In der EU wurde die Netzneutralität 2015 als «Regeln zur Wahrung der gleichberechtigten und nichtdiskriminierenden Behandlung des Verkehrs bei der Bereitstellung von Internetzugangsdiensten» in einer Verordnung festgeschrieben.[65] Dabei wurden jedoch verschiedene Ausnahmen definiert. So dürfen «Spezialisierte Dienste» wie zum Beispiel Telemedizin, für die ein spezifisches Qualitätsniveau objektiv notwendig ist, bevorzugt behandelt werden. Dies jedoch nur, wenn der spezialisierte Dienst nicht für einen allgemeinen Zugang zum Internet benutzt werden kann. Zudem sind Verkehrsmanagementmassnahmen zulässig, bei denen zwischen objektiv verschiedenen Verkehrskategorien unterschieden wird. Jede derartige Differenzierung soll jedoch nur auf der Grundlage objektiv verschiedener Anforderungen an die technische Qualität der Dienste (beispielsweise in Bezug auf Verzögerung, Verzögerungsschwankung, Paketverlust und Bandbreite), nicht aber auf Grundlage kommerzieller Erwägungen zulässig sein. Weiter ist erlaubt, für ausgewählte Dienste verwendete Datenvolumen von einer Anrechnung auf beschränkte monatliche Transfervolumen auszunehmen oder unterschiedlich abzurechnen (sogenanntes Zero-Rating). Den Mitgliedsstaaten ist vorbehalten, strengere Regeln bezüglich Netzneutralität zu erlassen.

In der Schweiz gibt es keine gesetzlich verankerte Netzneutralität. Im Rahmen der aktuellen Teilrevision des Fernmeldegesetzes (FMG)[66] liess das Bundesamt für Kommunikation (BAKOM) 2014 einen Bericht zur Netzneutralität[67] erstellen, um den Regelungsbedarf zu analysieren. Im Gesetzesentwurf beschränkte man sich dann jedoch auf umfassende Pflichten zur Bekanntgabe von Einschränkungen. Die Schweiz wird also auch in absehbarer Zukunft vermutlich keine verordnete Netzneutralität kennen. Verschiedene Exponenten haben allerdings bereits angekündigt, dass sie das Thema Netzneutralität in die Debatte zur FMG-Revision im Parlament tragen werden.

Ob sich die Internetanbieter aufgrund der Transparenzvorschriften und dem damit einhergehenden Risiko der öffentlichen Kritik von Verletzungen der Netzneutralität abhalten lassen, wird sich zeigen. Es ist auch denkbar, dass sich die Problematik in der Schweiz aufgrund des

---

63 Restoring Internet Freedom Order: https://apps.fcc.gov/edocs_public/attachmatch/FCC-17-166A1.pdf (Stand: 31. Januar 2018).

64 Open Internet Order: https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf (Stand: 31. Januar 2018).

65 VERORDNUNG (EU) 2015/2120, http://eur-lex.europa.eu/eli/reg/2015/2120/oj (Stand: 31. Januar 2018).

66 Übersicht auf der Webseite des BAKOM: https://www.bakom.admin.ch/bakom/de/home/das-bakom/organisation/rechtliche-grundlagen/bundesgesetze/fmg-revision-2017.html; Botschaft zur FMG-Revision: https://www.admin.ch/opc/de/federal-gazette/2017/6559.pdf; Gesetzesentwurf: https://www.admin.ch/opc/de/federal-gazette/2017/6705.pdf (Stand: 31. Januar 2018).

67 https://www.bakom.admin.ch/bakom/de/home/digital-und-internet/internet/netzneutralitaet.html (Stand: 31. Januar 2018).

guten Ausbaustandards der Netzinfrastruktur und der Angebotsgestaltung der Anbieter nicht im gleichen Masse auswirkt wie in anderen Ländern.

In den USA und auch in der EU besteht eine grundsätzliche Pflicht zur transparenten Bekanntgabe von einschränkenden Massnahmen. Es ist somit Aufgabe der jeweiligen Zivilgesellschaft, die Entwicklungen im Bereich der Netzneutralität zu beobachten und bei Bedarf einzugreifen.

6.2 Cyber-Parasiten: Wenn Malware Ihre CPU kapert

Der Erfolg der Kryptowährungen bietet äusserst verlockende Perspektiven für Cyber-Kriminelle. In Kapitel 5.4.3 dieses Berichts wird beispielsweise über Bitcoin-Diebstähle im grossen Stil berichtet. Aber die Kriminellen haben sich auch an anderer Stelle breit gemacht, indem sie das für diese Art von Währung typische Mining missbrauchen. Mining oder auf Deutsch Schürfen bezeichnet den Prozess, über den die Transaktionen in einer Kryptowährung verifiziert und neue Währungseinheiten geschaffen werden. Für diese komplexen Berechnungen sind erhebliche IT-Ressourcen notwendig. Die Bereitstellung dieser Ressourcen wird mit einer gewissen Menge von «geschürftem» Geld entschädigt, die dem Anteil der Beteiligung an der Berechnung entspricht. Letztlich trägt das Mining zur Geldschöpfung bei.

Da dieser Prozess Geld einbringt, suchen gewisse Akteure bereits seit geraumer Zeit nach Möglichkeiten, um diesen zu missbrauchen (derartige Fälle wurden bereits in unserem Halbjahresbericht 2013/2[68] erwähnt). Unterdessen haben sich Angriffe, mit denen Rechnerkapazität für das Mining missbraucht werden, vervielfacht. 2017 war diesbezüglich besonders ereignisreich – so sehr, dass manche sich fragen, ob es sich dabei nicht um einen der lukrativsten Businessmodelle für Cyber-Kriminelle handelt. Ausserdem wurden gewisse Schadcodes für das Mining genutzt, obwohl auch andere kriminelle Optionen möglich gewesen wären. Ein Beispiel dafür ist «WannaMine»: eine ausgeklügelte Schadsoftware, die sich insbesondere über den Exploit «EternalBlue» verbreitet. Der Exploit wurde bereits von der Ransomware «WannaCry» und «NotPetya» genutzt. Im Unterschied zu Letzteren nutzen die Kriminellen «WannaMine» aber in der Weise, dass es nach der Installation virtuelle Währung schürft, statt dass es die Daten der Nutzerinnen und Nutzer verschlüsselt.

Die Installation einer Schadsoftware ist nicht die einzige Möglichkeit, wie ein Computer ohne Wissen seines Nutzers zum Schürfen von Kryptowährung verwendet werden kann. Gewisse Webseiten enthalten auch Scripts, die dazu dienen, Kryptowährung über den Browser des Webseiten-Besuchers zu schürfen. Einige Webseitenbetreiber verlangen die Zustimmung des Besuchers, der dann seinen Computer bewusst zur Verfügung stellt, um sich an der Finanzierung einer Webseite zu beteiligen. Andere foutieren sich um diesen Hinweis. In zahlreichen Fällen wurden auch Webseiten manipuliert, um solche Scripts ohne Wissen des Betreibers zu platzieren.

---

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

Zwar mag das Ausnutzen der Ressourcen eines Computers harmloser erscheinen als andere Angriffsformen wie etwa die Verschlüsselung von Daten. Aber das Schadenspotenzial solcher Attacken darf dennoch nicht unterschätzt werden. Der Preis des heimlichen Minings ist zunächst der Strom, der durch die beanspruchte Rechnerleistung verbraucht wird. Zudem können Stabilitätsprobleme oder Abstürze die Folge sein, wenn die Rechnerleistung, die eigentlich für andere Prozesse zur Verfügung stehen sollte, von einer Malware in Anspruch genommen wird. Dies ist umso beunruhigender, wenn sensible Systeme betroffen sind. Bei der Entfernung einer solchen Software besteht zudem das Risiko von Unterbrüchen.

Die Entwicklung dieser Art von Attacken deutet darauf hin, dass gegenwärtig ein sehr interessantes Kosten-Nutzen-Verhältnis vorliegt. Für die Kriminellen müssen solche Methoden zwar im grossen Massstab umgesetzt werden, damit sie profitabel sind; die Rechnerleistung von einigen wenigen Maschinen reicht dazu nicht aus. Im Gegenzug bieten solche Angriffe aber den Vorteil eines regelmässigen Einkommens. Eine infizierte Maschine beginnt ganz einfach automatisch, Geld einzubringen. Letztlich handelt es sich dabei um die direkteste Verbindung zwischen der Infizierung eines Computers und der Generierung von Einkommen. Überdies bietet diese Art von Manipulation den Vorteil, dass sie oft nur schwer zu entdecken ist. Das Ziel besteht somit darin, über eine grosse Anzahl von Computern zu verfügen, die in aller Diskretion, regelmässig und mit möglichst wenigen Unterbrüchen einen kleinen Geldbetrag einbringen. Die grösste Sorge dürfte die Frage bereiten, was mit diesen verseuchten Maschinen geschehen wird, wenn das Verfahren eines Tages finanziell weniger attraktiv wird. Dann droht die Gefahr, dass die Malware umfunktioniert wird und für Aktionen verwendet wird, die möglicherweise zerstörerischer sind. Es wäre deshalb naiv, das heimliche Mining einfach als harmloses Parasitentum zu betrachten.

6.3 Outsourcing? Aber sicher!

In der globalisierten und spezialisierten Welt kann es sich heute praktisch keine Firma mehr leisten, alle Geschäftsabläufe «in house» zu betreiben. Will man konkurrenzfähig sein, müssen Abläufe möglichst effizient gestaltet und die Kosten niedrig gehalten werden. Ein Auslagern von gewissen Dienstleistungen (Outsourcing) kann zur Optimierung beitragen. Es ist jedoch wichtig, dass bei der Wahl eines externen Partners die Sicherheit ein entscheidendes Kriterium ist. Der günstigste Anbieter muss nicht zwingend der sicherste sein. Es kann zwar eine Dienstleistung, nie aber die Verantwortung und das Risiko ausgelagert werden. Beim Outsourcing muss sich jede Firma stets vor Augen führen, welche Daten sie in andere Hände geben will und was die Auswirkung auf die Firma wäre, wenn diese Daten kompromittiert würden. Daten, deren Verlust zu einer existenziellen Bedrohung der Firma führen würden, gehören nicht in fremde Hände.

Der Schwedische Premierminister Stefan Löfven musste das am eigenen Leib erfahren. Im Juli 2017 musste er vor der Presse eingestehen, dass für Daten des schwedischen Militärs, der Führerscheinbehörde und sogar des Zeugenschutzprogrammes die Möglichkeit des unautorisierten Zugriffs bestand. Die Behörde hatte zuvor ihre IT-Verwaltung an den Computerkonzern IBM ausgelagert. IBM beauftragte seinerseits Subunternehmen in Tschechien und Rumänien. Alle betroffenen Daten wurden zwar in Schweden gespeichert, Techniker der beiden Subunternehmen hatten jedoch ohne Sicherheitsüberprüfung Zugriff darauf. Die Behörde betonte, dass nichts auf einen Datenmissbrauch hindeute.

Empfehlung:

Um sich vor solch unliebsamen Überraschungen zu schützen, müssen im Vorfeld solcher Projekte genaue Anforderungen definiert und ein IT-Sicherheitskonzept für die ausgelagerten Bereiche erstellt werden. Dabei muss genau geklärt werden, welche Risiken eine Auslagerung der Daten beinhaltet und welche Massnahmen ergriffen werden müssen, um diese Risiken zu minimieren. Es ist wichtig, ein ehrliches Risikomanagement zu betreiben, die Risiken nicht kleinzureden und sich nicht von der Kostenersparnis blenden zu lassen. Zu ergreifende Massnahmen sind beispielsweise eine klare Definition von Zugriffsrechten, der Einbezug von ausschliesslich autorisierten Personen sowohl in den Installations- wie auch in den Wartungsprozess und die Verschlüsselung der Daten beim Transport und der Speicherung. Neben einer regelmässigen Datensicherung gehören auch gesicherte physische Zugangskontrollen zu den Anforderungen. Firmen sollten nicht einfach auf die Versprechen der Dienstleister vertrauen, sondern müssen diese regelmässig (beispielsweise in Form von Sicherheitszertifikaten) einfordern und überprüfen. Ebenfalls sind Massnahmen für den Fall zu definieren, falls es trotz aller Vorkehrungen zu einem Zwischenfall kommt.

Schlussfolgerung:

Die Komplexität des Risikomanagements gerade bei ausgelagerten Dienstleistungen wird in den nächsten Jahren weiter zunehmen. Exemplarisch zeigte sich dies an den über den Jahreswechsel bekannt gewordenen Hardwareschwachstellen «Spectre» und «Meltdown». Auch Hardware kann Schwachstellen enthalten und kein Element in einem Informatiksystem kann als absolut sicher angesehen werden. Eine Sicherheitspolitik muss dementsprechend aus verschiedensten Massnahmen (organisatorische und technische Massnahmen) bestehen, um das Risiko beim Auftreten einer Lücke in einer Komponente möglichst gering zu halten. Bei diesen Schwachstellen waren virtualisierte Umgebungen und damit ausgelagerte Dienstleistungen besonders betroffen. Firmen, welche Daten in Rechenzentren Dritter bearbeiten, müssen sich deshalb versichern lassen, dass die Betreiber des Rechenzentrums alle nötigen Vorkehrungen getroffen haben, um die Risiken der entsprechenden Lücke zu minimieren. Garantien zu getroffenen Massnahmen können in einem solchen Fall innerhalb eines Vertrages gefordert werden.

7 Politik, Forschung, Policy

7.1 CH: Parlamentarische Vorstösse

Geschäft	Nummer	Titel	Eingereicht von	Datum Einreichung	Rat	Amt	Stand Beratung & Link
Ip	17.4285	Die Rolle der Akteure im Bereich Cyberabwehr und Cybersicherheit in der Schweiz klar definieren	Fathi Derder	15.12.2017	NR	VBS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174285
Ip	17.4100	Digitalisierung der Aussen- und Sicherheitspolitik. Risiken und Chancen für die Schweiz?	Damian Müller	13.12.201	NR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174100
Ip	17.4004	Übersicht tut Not - Koordination auch?	Sylvia Flückiger-Bäni	30.11.201	NR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174004
Ip	17.3905	Cyber-Risk-Gesetz	Sibel Arslan	29.09.2017	NR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173905
Po	17.3875	Armee. Wissenschaftliche Forschung stärken, Zusammenarbeit mit Forschungseinrichtungen vertiefen	Fathi Derder	29.09.2017	NR	VBS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173875
Mo	17.3849	Schweizer Armee. Wie können unsere Souveränität und unsere Unabhängigkeit sichergestellt werden, wenn mit der Digitalisierung die gegenseitige Abhängigkeiten immer mehr zunehmen?	Claude Béglé	28.09.2017	NR	VBS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173849
Ip	17.3731	Umfassende Cybersicherheit für alle statt Cyberwar nur für das VBS	Edith Graf-Litscher	27.09.2017	NR	VBS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173731
Ip	17.4296	Faire Besteuerung der Internet-Giganten. Für eine Ausgleichssteuer auf dem online erzielten Umsatz	Balthasar Glättli	15.12.2017	NR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174296
Ip	17.4090	Massnahmen gegen diskriminierende Tendenzen	Nadine Masshardt	13.12.2017	NR	EDI	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174090
Ip	17.3864	Illegale Angebote im Internet. Schäden und Risiken vermindern	Raphaël Comte	28.09.2017	SR	EJPD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173864
Ip	17.4314	Was war die Rolle der Post beim Markteintritt von Amazon in der Schweiz?	Regula Rytz	15.12.2017	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174314
Po	17.4249	Das Berggebiet zum Daten- und Digitalisierungs-Hub ausbauen	Martin Candinas	15.12.2017	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174249
Po	17.4041	Weniger Verkehrsunfälle dank Fahrassistenten? Mehr Daten über Fahrassistenzsysteme und deren Auswirkungen auf die Sicherheit	Jürg Grossen / Grünliberale Fraktion	07.12.2017	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174041
Fr	17.5619	Sollen Social Media dem Radio- und Fernsehgesetz unterstellt werden?	Edith Graf-Litscher	06.12.2017	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20175619

Fr	17.5614	Reicht die rechtliche Basis gegen die Verbreitung von Fake News über Social Media?	Edith Graf-Litscher	06.12.2017	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20175614
Fr	17.5592	Cyberdefence. Fähigkeiten zur strategischen Kommunikation und Führung von Informationsoperationen	Priska Seiler Graf	05.12.2017	NR	VBS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20175592
Ip	17.3896	Wie kann eine verkehrsträgerübergreifende digitale Plattform für den öffentlichen Verkehr geschaffen werden?	Claude Béglé	29.09.2017	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173896
Ip	17.3870	Ausbau des Mobilfunknetzes	Susanne Leutenegger Oberholzer	29.09.2017	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173870
Mo	17.3847	Internet der Dinge. Gestaltung der Rahmenbedingungen für ein nationales und internationales Ökosystem	Claude Béglé	28.09.2017	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173847
Ip	17.3733	Zivile Drohnen. Können die Gefahren ignoriert werden?	Manuel Tornare	27.09.2017	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173733
Ip	17.3734	Hassreden auf sozialen Netzwerken. Einfach gewähren lassen?	Manuel Tornare	27.09.2017	NR	EJPD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173734
Ip	17.3723	Mobilfunknetz der Swisscom. Wie sollen die Zahlen der Mobilfunkabdeckung und die Netzabdeckungskarte interpretiert werden?	Jacques Nicolet	25.09.2017	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173723
Fr	17.5397	Standortvorteil der Schweiz mit einem leistungsfähigen 5G-Mobilnetz sichern	Karl Vogler	13.09.2017	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20175397
Po	17.4017	Die Chancen von «Civic Tech» nutzen	Damian Müller	04.12.2017	SR	BK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174017
Po	17.4295	Sicherheitsstandards für Internet of Things-Geräte (IoT) prüfen, weil diese eine der grössten Bedrohungen der Cybersicherheit sind	Balthasar Glättli	15.12.2017	NR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174295
Po	17.4273	Regtech-Lösungen: Deren Verbreitung bei Wirtschaftsakteuren und Behörden ist zu fördern	Claude Béglé	15.12.2017	NR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174273
Ip	17.4062	Validierungs-Service «Validator.ch» optimieren	Marcel Dobler	12.12.2017	NR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174062
Ip	17.3854	Eine zweite Chance für eine Digitalsteuer	Géraldine Savary	28.09.2017	SR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173854
Ip	17.3717	Konsequenzen und Herausforderungen der digitalen Transformation für das Bundesamt für Kultur	Kathy Riklin	25.09.2017	NR	EDI	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173717
Fr	17.5415	Kryptowährungen. Produktion, Verwendung, staatliche Kontrolle, Schadenpotenzial	Maximilian Reimann	18.09.2017	NR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20175415

7.2 Der Ruf der «Global Commission on the Stability of Cyberspace» den öffentlichen Teil des Internets zu schützen

Die «Global Commission on the Stability of Cyberspace (GCSC)» wurde im Februar 2017 an der Münchner Sicherheitskonferenz ins Leben gerufen und vereint herausragende Personen von Regierungen, Unternehmen, Technischer- und Zivilgesellschaft je aus verschiedensten geographischen Regionen. Ihre Mission ist das Fördern von Frieden, Sicherheit und Stabilität im internationalen Raum, indem Normen und Initiativen zum verantwortungsvollen Verhalten der staatlichen und nichtstaatlichen Akteure im Cyberspace vorgeschlagen werden.

Im November 2017 initiierten GCSC Repräsentanten einen «Call to Protect the Public Core of the Internet», in welchem alle Beteiligten aufgefordert werden die folgende Norm einzuhalten, welche die grundsätzliche Verfügbarkeit und Integrität des Internets gewährleisten soll:

> Non-Interference with the public core
>
> Without prejudice to their rights and obligations, state and non-state actors should not conduct or knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace.

Gemäss der Kommission beinhalten die Teile des «öffentlichen Kerns» des Internets unter anderem das Internet Routing, das Domain Name System, Zertifikate und Vertrauen und die Kommunikation über Kabel.

> Schlussfolgerung:
>
> Moderne Gesellschaften hängen mehr und mehr von mit dem Internet verbundenen Informationstechnologien ab und werden zusehends abhängiger von dessen Stabilität und Berechenbarkeit. Mit Blick auf den vernetzten globalen Cyberraum können Massnahmen, welche den «öffentlichen Kern» des Internets betreffen, weltweite Auswirkungen und unbeabsichtigte Konsequenzen sowie Kollateralschaden nach sich ziehen, die sehr schwierig vorauszusagen sind. Es ist deshalb im Interesse aller Beteiligten, welche das Gemeinwohl im Blick haben, allen Aktivitäten abzuschwören, welche das generelle Funktionieren des Internets in Gefahr bringen und gleichzeitig helfen, solche Aktivitäten zu verhindern oder abzuschwächen.

8 Publizierte MELANI Produkte

8.1 GovCERT.ch Blog

8.1.1 The Retefe Saga

03.08.2017 - Surprisingly, there is a lot of media attention going on at the moment on a macOS malware called OSX/Dok. In the recent weeks, various anti-virus vendors and security researchers published blog posts on this threat, presenting their analysis and findings. While some findings where very interesting, others were misleading or simply wrong.

➔ https://www.govcert.admin.ch/blog/33/the-retefe-saga

8.1.2 Leaked Accounts

29.08.2017 – MELANI/GovCERT has been informed about potentially leaked accounts that are in danger of being abused. MELANI/GovCERT provides a tool for checking whether your account might be affected: https://checktool.ch

➔ https://www.govcert.admin.ch/blog/34/leaked-accounts

8.2 MELANI Newsletter

8.2.1 E-Banking: Angreifer haben es auf Aktivierungsbriefe abgesehen

17.08.2017 – Ende 2016 hat MELANI in einem Newsletter darauf hingewiesen, dass Kriminelle vermehrt mobile Authentifizierungsmethoden beim E-Banking im Visier haben. Nun gehen die Angreifer einen Schritt weiter und versuchen Opfer dazu zu bringen, eine Kopie des von der Bank erhaltenen Briefes, welcher Aktivierungsdaten für die die Zwei-Faktor Authentifizierung (2FA) des E-Bankings enthält, an die Betrüger zu senden.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/e-banking--angreifer-haben-es-auf-aktivierungsbriefe-abgesehen.html

8.2.2 21'000 Zugangsdaten zu Internet-Diensten gestohlen

29.08.2017 - Die Melde- und Analysestelle Informationssicherung MELANI hat rund 21'000 Zugangsdaten bestehend aus Login und Passwort erhalten, die offensichtlich gestohlen wurden und nun für illegale Zwecke missbraucht werden.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/passwoerter-von-21000-e-mail-konten-im-umlauf.html

8.2.3 Verschlüsselungstrojaner und missbräuchliche Mails im Namen von Behörden im Vormarsch

02.11.2017 - Der am 2. November 2017 veröffentlichte 25. Halbjahresbericht der Melde- und Analysestelle Informationssicherung (MELANI) befasst sich mit den wichtigsten Cyber-Vorfällen der ersten Jahreshälfte 2017 im In- und Ausland. Im Schwerpunktthema widmet sich

der Bericht den Verschlüsselungstrojanern «Wanna Cry» und «NotPetya», die im Frühjahr 2017 weltweit für Schlagzeilen gesorgt haben.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/melani-halbjahresbericht-1-2017.html

8.2.4 70'000 Zugangsdaten zu Internet-Diensten gestohlen

05.12.2017 - Der Melde- und Analysestelle Informationssicherung MELANI wurde wiederum eine Liste mit Zugangsdaten bestehend aus Login und Passwort gemeldet. Diesmal handelt es sich um 70'000 Datensätze.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/passwoerter-von-70000-e-mail-konten-im-umlauf.html

8.3 Checklisten und Anleitungen

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

9 Glossar

Begriff	Beschreibung
Advanced Persistent Threats (APT)	Bei diese Angriffsweise kommen verschiedene Techniken und Taktiken zum Einsatz und wird sehr gezielt auf eine einzelne Organisation oder auf ein Land durchgeführt. Meist kann damit sehr hohen Schaden angerichtet werden. Deshalb ist der Angreifer bereit, sehr viel Zeit, Geld und Wissen in den Angriff zu investieren und verfügt dazu in der Regel über grosse Ressourcen.
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 Smartphones und Tablet-Computer gemeint.
Backdoor	Backdoor (deutsch: Hintertür) bezeichnet einen oftmals absichtlich eingebauten Teil einer Software, der es Benutzern ermöglicht, unter Umgehung der normalen Zugriffssicherung aus der Ferne Zugang zum Computer oder einer sonst geschützten Funktion eines Computerprogramms zu erlangen.
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.
Bot	Ursprung im slawischen Wort für Arbeit (Robota). Bezeichnet ein Programm, das bestimmte Aktionen nach dem Empfang eines Befehls selbstständig ausführt. So genannte Malicious Bots können kompromittierte Systeme fernsteuern und zur Durchführung beliebiger Aktionen veranlassen.
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.
DDoS	Distributed-Denial-of-Service Attacke. Mit einer DoS-Attacke wird der Dienst oder das System des Opfers von vielen verscheiden Systemen aus gleichzeitig angegriffen, sodass dieses zum Erliegen kommt und nicht mehr verfügbar ist.
Defacement	Verunstaltung von Webseiten.
Domain Name System	Domain Name System (DNS). 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).
Ethernet	Ethernet ist eine Technologie für kabelgebundene Datennetze.
Exploit-Kit	Baukasten, mit welchen Kriminelle Programme, Scripts oder Codezeilen generieren können, womit 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.
Hashfunktion	Eine Hashfunktion ist eine Abbildung, die eine grosse Eingabemenge (die Schlüssel) auf eine kleinere Zielmenge (die Hashwerte) abbildet.
Internet der Dinge	Der Begriff Internet der Dinge beschreibt die Vernetzung und das Zusammenarbeiten von physischen und virtuellen Gegenständen.
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 eingege-

	benen 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» (englisch: Industrial Control Systems, ICS) geläufig.
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.
Patch	Eine Software, die den fehlerhaften Teil eines Programms durch einen fehlerfreien ersetzt und dadurch z.B. eine Sicherheitslücke behebt.
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.

Port	Ein Port ist ein Teil einer Adresse, der Datensegmente einem Netzwerkprotokoll zuordnet. Dieses Konzept ist beispielsweise in TCP, UDP und SCTP vorgesehen, um Protokolle auf den höheren Schichten des OSI-Modells zu adressieren.
PowerShellScript	PowerShell ist ein plattformübergreifendes Framework von Microsoft zur Automatisierung, Konfiguration und Verwaltung von Systemen, bestehend aus einem Kommandozeileninterpreter sowie einer Skriptsprache.
Proxy	Ein Proxy ist eine Kommunikationsschnittstelle in einem Netzwerk. Er arbeitet als Vermittler, der auf der einen Seite Anfragen entgegennimmt, um dann über seine eigene Adresse eine Verbindung zur anderen Seite herzustellen.
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.
RSA-Verschlüsselung	Abkürzung für Rivest-Shamir-Adleman Verschlüsselung. Verschlüsselungsverfahren mit öffentlichen Schlüsseln, das 1978 eingeführt wurde. RSA ist ein asymmetrisches Verfahren.
Salts	Salt bezeichnet in der Kryptographie eine zufällig gewählte Zeichenfolge, die an einen gegebenen Klartext vor der Verwendung als Eingabe einer Hashfunktion angehängt wird, um die Entropie der Eingabe zu erhöhen.
Schadsoftware	Oberbegriff für Software, die schädliche Funktionen auf einem Rechner ausführt (wie beispielsweise Viren, Würmer, Trojanische Pferde).
Schwachstelle / Lücke	Schwachstelle in Hard- oder Software, über die Angreifer Zugriff auf ein System erlangen können.

Smartphone	Ein Smartphone ist ein Mobiltelefon, das mehr Computerfunktionalität und -konnektivität als ein herkömmliches fortschrittliches Mobiltelefon zur Verfügung stellt.
SMB-Protokoll	Server Message Block (SMB) ist ein Netzwerkprotokoll für Datei-, Druck- und andere Serverdienste in Rechnernetzen.
SMS	Short Message Service ist ein Dienst zum Versenden von Kurzmitteilungen (maximal 160 Zeichen) an Mobiltelefonbenutzer.
Social Engineering	Social-Engineering-Angriffe nutzen die Hilfsbereitschaft, Gutgläubigkeit oder die Unsicherheit von Personen aus, um beispielsweise an vertrauliche Daten zu gelangen, oder die Opfer zu bestimmten Handlungen zu bewegen. Eine bekannte Form von Social Engineering ist Phishing.
Spearphishing-Mails	Gezielte Phishing Attacke. Dem Opfer wird zum Beispiel vorgegaukelt, mit einer ihr vertrauten Person via E-Mail zu kommunizieren.
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.
Supply Chain-Angriffe	Angriff bei dem versucht wird über die Infektion einer Firma in der Lieferkette das eigentliche Ziel zu infizieren.

Take-Down	Ausdruck, der verwendet wird, wenn ein Provider eine Website aufgrund betrügerischen Inhalts vom Netz nimmt.
Troll	Als Troll bezeichnet man im Netzjargon eine Person, die ihre Kommunikation im Internet auf Beiträge beschränkt, die auf emotionale Provokation anderer Gesprächsteilnehmer zielt.
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.
Watering-Hole-Angriffe	Gezielte Infektion durch Schadsoftware über Webseiten, welche bevorzugt nur von einer spezifischen Benutzergruppe besucht werden.
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.
WLAN	WLAN (Wireless Local Area Network) steht für drahtloses lokales Netzwerk.
ZeroDay-Lücken	Sicherheitslücke, für welche noch kein Patch exisitiert.

Zertifikat	Ein digitales Zertifikat ist gewissermassen das Cyberspaceäquivalent eines Personalausweises und dient dazu, einen bestimmten öffentlichen Schlüssel einer Person oder Organisation zuzuordnen. Diese Zuordnung wird von der Zertifizierungsstelle beglaubigt, indem sie diese mit ihrer eigenen digitalen Unterschrift versieht.
ZIP-Datei	ZIP ist ein Algorithmus und Dateiformat zur Datenkompression, um den Speicherbedarf von Dateien für die Archivierung und Übertragung zu verringern.
Zweifaktorauthentifizierung	Um die Sicherheit zu erhöhen wird die Zweifaktorauthentifizierung verwendet. Dafür sind mindestens zwei der drei Authentifikationsfaktoren notwendig: 1. Etwas, das man weiss (z. B. Passwort, PIN, usw.) 2. Etwas, das man besitzt (z. B. Zertifikat, Token, Streichliste, usw.) 3. Ein einmaliges Körpermerkmal (z. B. Fingerabdruck, Retina-Scan, Stimmerkennung usw.).