Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Informatiksteuerungsorgan des Bundes ISB
Nachrichtendienst des Bundes NDB

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

INFORMATIONSSICHERUNG

LAGE IN DER SCHWEIZ UND INTERNATIONAL

Halbjahresbericht 2019/2 (Juli – Dezember)

30. APRIL 2020

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

1 Übersicht / Inhalt

2 Editorial

Delegierter des Bundes für Cybersicherheit

Florian Schütz ist Delegierter des Bundes für Cybersicherheit und Leiter des Nationalen Zentrums für Cybersicherheit.

Aus MELANI wird das «Nationale Zentrum für Cybersicherheit». So titelte ein Beitrag auf der MELANI Homepage Anfang 2020. Dabei handelt es sich um einen weiteren Schritt zur Etablierung der Zuständigkeiten im Bund, welche vom Bundesrat am 30. Januar 2019 festgelegt worden ist (siehe Abbildung 1). Wie das Nationale Zentrum für Cybersicherheit (NCSC) im Detail organisiert wird, ist Bestandteil laufender Arbeiten und noch nicht final verabschiedet. Was jetzt aber schon klar ist: MELANI ist ein wichtiger Teil des neuen Zentrums und soll weiter gestärkt und ausgebaut werden. Daher möchte ich in diesem Editorial auf meine Erfahrungen mit MELANI im zweiten Halbjahr 2019 zurückblicken und drei zukünftige Herausforderungen erörtern.

Seit der Gründung von MELANI am 1. Oktober 2004 hat die Informations- und Kommunikationstechnologie (IKT) Wirtschaft, Forschung und Gesellschaft weiter durchdrungen. IKT ist der Kern digitalisierter Prozesse und in fast allen Bereichen des Lebens anzutreffen. Eine allgemeine Lageanalyse wird der diversifizierten Bedrohung nicht mehr gerecht. Viel mehr braucht es spezifische Analysen für Wirtschaftssektoren, Bereiche der Politik, Forschung und Gesellschaft. Als erste Massnahme wird aktuell in einem Pilotprojekt eine spezifische Lagedarstellung für den Finanzsektor erprobt.

Eine weitere Herausforderung ist die Skalierung der Verarbeitung von Vorfällen. Im ersten operativen Jahr von MELANI vor 15 Jahren wurden gesamthaft weniger als 500 Meldungen verzeichnet. Demgegenüber wurden alleine im Januar dieses Jahres mehr als 500 Meldungen an uns gerichtet. Um dieses Volumen zu verarbeiten, wurde als erste Massnahme im zweiten Halbjahr 2019 eine nationale Anlaufstelle für Cybersicherheit geschaffen. Sie nimmt Meldungen entgegen, analysiert diese und stellt die Behandlung durch die richtigen Stellen sicher.

Weiter wird vor allem die Automatisierung der Analyse und Verarbeitung sowie die nahtlose Integration der beteiligten Stellen – zum Beispiel von Strafverfolgungsbehörden – eine wichtige Aufgabe sein.

«Du wurdest gewogen...du wurdest gemessen...und du wurdest für nicht gut genug befunden.» lautet ein Zitat aus dem Film «Ritter aus Leidenschaft». Obwohl MELANI international einen exzellenten Ruf geniesst, hören wir ab und zu in öffentlichen Diskussionen, dass MELANI für nicht gut genug befunden wird. Während es unbestritten Verbesserungspotential gibt, wird diese generische Kritik der guten Arbeit der Teams nicht gerecht. Wir sehen den Grund dieser Kritik darin, dass durch das Fehlen von öffentlichen Kennzahlen (Key Performance Indicators, KPI) eine differenzierte Betrachtung schwierig ist und so, je nach Situation, der eine oder andere falsche Schluss gezogen wird. Deshalb werden wir zukünftig KPIs etablieren, um differenzierte Kritik zu ermöglichen und den Erfolg besser zu messen.

Eine Kritik haben wir uns schon zu Herzen genommen: Der MELANI Halbjahresbericht war einigen zu wenig technisch. Um weiterhin die Zielgruppe der Politiker, Führungskräfte und interessierten Privatpersonen zu erreichen, aber auch den Fachpersonen etwas zu bieten, haben wir zum ersten Mal einen technischen Anhang erstellt. Über Anregungen diesbezüglich würden wir uns sehr freuen. Schreiben Sie uns dazu bitte, ob wir diesen in Zukunft ausbauen sollen oder nicht.[1]

MELANI hat in den vergangen 15 Jahren viel erreicht und geleistet, wie auch der vorliegende Halbjahresbericht zeigt. In den nächsten Jahren werden die Herausforderungen mit Sicherheit noch zunehmen. Ich bin aber überzeugt, dass wir diese meistern werden und mit der neuen Organisation im nationalen Zentrum für Cybersicherheit eine solide Grundlage für die Zukunft schaffen.

Florian Schütz

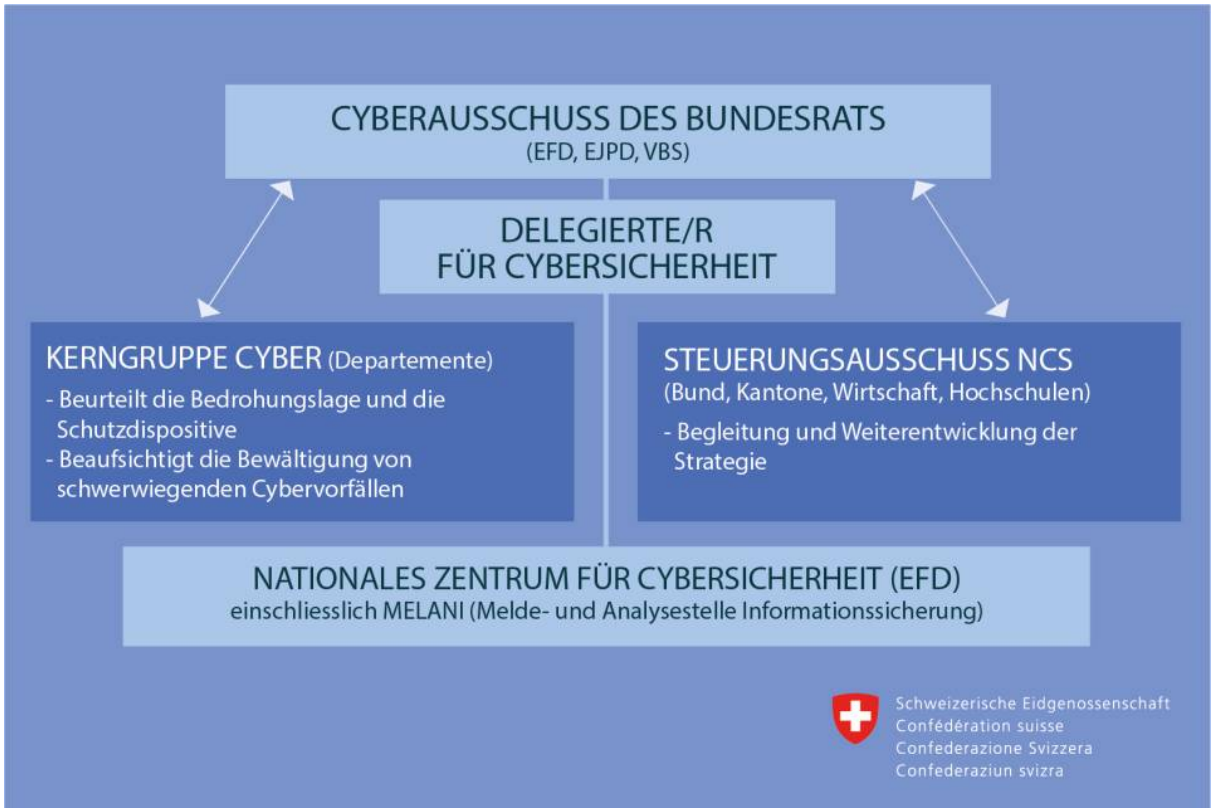

Abb. 1: Cyberorganisation im Bund

[1] Wir laden Sie ein, die Evaluation des Berichts auf unserer Webseite auszufüllen: https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/evaluation-halbjahresbericht.html

3 Schwerpunktthema: Personendaten im Netz

3.1 Einführung

Die allermeisten Datenbearbeitungen geschehen heutzutage elektronisch und auf Geräten, die mehr oder weniger direkt mit dem Internet verbunden sind. Vielfach sind Daten in einer beliebigen Cloud gespeichert und können dort abgerufen werden.

«Unsere Daten» oder präziser «Daten über uns» sind von verschiedensten Akteuren an einer Vielzahl von Orten gespeichert und kaum jemand hat einen vollständigen Überblick darüber, wer welche Daten über sie oder ihn hat und wo diese bearbeitet werden.

Daten werden gesammelt, gehandelt und aggregiert – vielfach auch gestohlen, wobei «stehlen» irreführend ist, denn Daten werden einfach kopiert und kommen dem Besitzer nicht abhanden. Gleiches gilt beim «Verkauf» von Daten. Oft werden Daten «verkauft», vervielfältigt und weiterverkauft. Das erschwert die Rückverfolgung erheblich, welchen Weg ein Datensatz genommen hat, bis er irgendwo wieder auftaucht.

Die Selbstbestimmung über die eigenen Daten ist fast unmöglich und die Verfolgung von Datenschutzverletzungen stellt betroffene Personen wie auch die zuständigen Stellen vor grosse Herausforderungen.

Fast täglich sorgen Datenabflüsse oder durch Fehlkonfigurationen offen zugängliche Daten für Schlagzeilen.[2] Bei den grössten Vorfällen ist mittlerweile die Rede von über einer Milliarde betroffener Datensätze.[3] MELANI hat im Halbjahresbericht 2017/2 Datenabflüsse als Schwerpunktthema aufgegriffen.[4]

3.2 Daten der Online-Welt

Wir leben im vernetzten Informationszeitalter. Das Internet ist aus unserem Alltag nicht mehr wegzudenken. Wir bestellen Waren, beziehen Dienstleistungen und Informationen, tauschen Meinungen, Bilder und vieles mehr über das weltweite Kommunikationsnetz. Dadurch gibt es von uns viele Online-Konten bei unzähligen Anbietern, die schnell erstellt und manchmal genauso schnell auch wieder vergessen sind. Bei diesen Konten sind typischerweise eine E-Mail-Adresse und ein Passwort hinterlegt. Einige Dienste verlangen auch die Angabe von Name, Adresse, Geburtsdatum, Telefonnummer, Fotos oder Kreditkartendaten. Vermutlich verfügen die Betreiber dieser Dienste über Informationen, was wir mit diesem Konto abgerufen oder was wir ins Netz hochgeladen haben. Insbesondere im Zusammenhang mit Social Media-Konten geben wir vieles preis: Mit wem wir befreundet sind und kommunizieren, wem wir folgen, was wir mögen oder teilen und wie lange wir uns mit welchen Themen beschäftigen. Aus diesen Angaben lassen sich sehr detaillierte Persönlichkeitsprofile erstellen.

---

2 https://www.helpnetsecurity.com/2019/11/14/breaches-2019/; https://www.immuniweb.com/blog/stolen-credentials-dark-web-fortune-500.html

3 https://securityaffairs.co/wordpress/94275/breaking-news/elasticsearch-social-information-1-2b-people.html; https://www.wired.com/story/billion-records-exposed-online/

4 MELANI Halbjahresbericht 2017/2, Kap. 3.

Auch beim blossen Surfen im Web generieren wir digitale Spuren in Form von Daten, die auf den Servern von Dienstanbietern, Werbenetzwerken und weiteren Inhaltsprovidern gespeichert werden. Oder auf unseren Geräten – z. B. in Form von *Cookies*. Auch einige Browser-Erweiterungen (*Add-Ons* respektive *Plug-Ins*) erheben Daten und speichern sie oder leiten sie weiter.[5] Diese sind zwar nicht unbedingt nach Personen mit Namen erschlossen, jedoch pseudonymisiert zugewiesen. Dies erlaubt die Erstellung eines Persönlichkeitsprofils und u. a. die Auslieferung von personalisierter Werbung oder das Anbieten von weiteren möglicherweise für uns interessanten Inhalten. Werden diese Daten mit einem Personenidentifikator – z. B. in Form einer E-Mail-Adresse oder eines Social Media-Kontos – verbunden, können sie auch ausserhalb des Erhebungskontextes transportiert und unabhängig davon personenbezogen bearbeitet und genutzt werden.

3.3 Daten aus der analogen Welt

Daten aus der analogen Welt werden seit dem Einzug der elektronischen Datenverarbeitung (EDV) digital gespeichert – am Anfang noch in alleinstehenden Computern oder rein internen Firmennetzwerken, mittlerweile auf Geräten, die alle mehr oder weniger direkt mit dem Internet verbunden sind. Korrespondenz, Planungen, Kundenkarteien, Buchhaltung und Mitarbeiteradministration sind grösstenteils digitalisiert. Beispielsweise führen wir unsere privaten Adressbücher häufig nur noch im Computer und auf dem Smartphone sowie in der Cloud.

Im Zuge der Digitalisierung werden Daten aus immer mehr Bereichen elektronisch bearbeitet. Sei dies im Gesundheitswesen mit dem digitalen Patientendossier oder bei Fitness-Apps, bei der Mobilität mit Online-Tickets für den öffentlichen Verkehr oder Velomieten per App, beim Wohnen durch SmartHome-Geräte, beim Lieferdienst für Essens- und andere Bestellungen, um nur einige davon zu nennen.

Auch Behörden führen Datenbanken seit längerem elektronisch, sind mittlerweile vernetzt und bauen Leistungen des E-Government aus. Wenn Unbefugte Zugriff auf Behördensysteme erlangen, können grosse Teile oder sogar die ganze Bevölkerung betroffen sein.[6]

3.4 Spezialfall öffentliche Register und Datenbanken

Auch bei traditionellen öffentlichen Registern, die mit der Digitalisierung online gestellt worden sind, müssen einige Aspekte berücksichtigt werden, die das Internet mit sich bringt. Was vorher einzeln auf Papier versendet wurde oder auf dem Amt eingesehen werden durfte, kann nun von überall auf der Welt abgefragt und dann lokal gespeichert werden. Zwar schreiben die entsprechenden Verordnungen vor, dass die Systeme «vor Serienabfragen geschützt»[7] werden oder gewisse Einträge «für Einzelabfragen im Internet unentgeltlich zur Verfügung»[8]

---

5 https://www.washingtonpost.com/technology/2019/07/18/i-found-your-data-its-sale/

6 Equador https://www.zdnet.com/article/database-leaks-data-on-most-of-ecuadors-citizens-including-6-7-million-children/; Chile https://www.zdnet.com/article/voter-records-for-80-of-chiles-population-left-exposed-online/; Bulgarien https://www.inside-it.ch/articles/55013

7 Artikel 27 Grundbuchverordnung (GBV), SR 211.432.1: https://www.admin.ch/opc/de/classified-compilation/20111142/index.html#a27

8 Artikel 12 Handelsregisterverordnung (HRegV), SR 221.411: https://www.admin.ch/opc/de/classified-compilation/20072056/index.html#a12

gestellt werden sollen. Je nach technischer Umsetzung kann dennoch mit etwas Geduld und Programmieraufwand ein ganzes Register ausgelesen werden. Entsprechend entsteht dadurch ein Spannungsfeld zwischen der gesetzlich vorgesehenen (auch elektronischen) Öffentlichkeit der Daten und dem Schutz vor deren missbräuchlicher Bearbeitung. Die gesetzlichen Grundlagen äussern sich nicht dazu, ob eine Abfrage anonym durchgeführt werden können muss. Um missbräuchliche Massenabfragen effektiv zu verhindern oder zumindest zu entdecken, müssten Abfragende identifiziert und ihre Abfragen in einer Form für gewisse Zeit gespeichert werden, was wiederum gesetzlicher Grundlagen bedarf.

Telefonbücher wurden bereits Ende der Achtzigerjahre digitalisiert und damals noch auf CD zum Kauf angeboten. Bald wurden diese Daten dann auch im Internet zugänglich gemacht, da sie ja bereits öffentlich verfügbar waren und dies deshalb erlaubt ist. Auch wenn die Telefonbücher kaum Mobil-Nummern oder E-Mail-Adressen enthalten, können Daten aus diesen Verzeichnissen als Stammdaten im Sinne einer Grundlage für Datensammlungen dienen – insbesondere für Akteure, die sich nicht um die rechtliche Zulässigkeit einer entsprechenden Bearbeitung scheren.

Ein besonderes Beispiel sind die früher öffentlich zugänglichen Informationen im Verzeichnis «Domain-Whois». In diesem Verzeichnis sind unter anderem Halter von Domainnamen publiziert. Diese Daten sind nun nicht mehr ohne weiteres einsehbar. Ursprünglich war das Whois dazu gedacht, dass Inhaber und Betreiber von Websites bekannt sind und einfach kontaktiert werden können. Transparenz war im frühen, von idealistischen Werten geprägten Internet eine Selbstverständlichkeit. Der über die Zeit aufgekommene Missbrauch der publizierten Daten führte jedoch bald zu Diskussionen über Form, Zweck und Notwendigkeit dieses Registers. Unter dem Druck der Europäischen Datenschutzgrundverordnung (DSGVO) wurde schliesslich gehandelt und Angaben zu Domainnamen sind nun vielfach anonymisiert.[9] Auch der Zugang zu Whois-Informationen bezüglich Schweizer Domainnamen sollen mit der anstehenden Revision des Fernmelderechts eingeschränkt werden.

3.5 Datenschutzgesetzgebung

Datenbearbeitungen und auch der Handel mit Personendaten sind je nach Umständen und anwendbarer Rechtsordnung erlaubt. Die Datenschutzvorgaben unterscheiden sich aber je nach Land erheblich. Die EU verordnet mit ihrer Datenschutzgrundverordnung (DSGVO) einen weltweit einheitlichen Schutz für die Daten ihrer Bürger. Auch wenn noch viele Fragen zur internationalen Durchsetzung dieser Vorgaben offen sind, hat die DSGVO bereits einige Wirkung erzielt. Seit ihrem Inkrafttreten im Mai 2018 werden Datenschutz und Datensicherheit von vielen Akteuren deutlich ernster genommen.

Mehrfach wird prognostiziert, dass Datenabflüsse in naher Zukunft grössere Schäden verursachen werden und mehr in Datensicherheit investiert wird.[10] Dies vor dem Hintergrund, dass seit dem Inkrafttreten der DSGVO Unternehmen bei Datenschutz-Verletzungen mit hohen

9 https://www.icann.org/resources/pages/gtld-registration-data-specs-en

10 https://securityintelligence.com/articles/11-stats-on-ciso-spending-to-inform-your-2020-cybersecurity-budget/; https://www.business2community.com/cybersecurity/10-cybersecurity-trends-in-2020-you-need-to-keep-an-eye-on-02275883; https://www.forbes.com/sites/gilpress/2019/12/03/141-cybersecurity-predictions-for-2020/; https://www.forbes.com/sites/gilpress/2019/12/12/42-more-cybersecurity-predictions-for-2020/

Bussen bestraft werden. Die Berechnung von Schäden berücksichtigt insbesondere die drohenden Bussen von bis zu 20 Millionen Euro oder 4% des Jahresumsatzes (je nachdem, welcher Wert höher ist), mit denen Unternehmen belegt werden können.

In der Revision des Schweizer Datenschutzgesetzes sind Strafbestimmungen vorgesehen, gemäss welcher nicht Unternehmen, sondern «private Personen» bestraft werden sollen, also Angestellte der Unternehmen. Nur wenn eine Busse unter CHF 50'000.- in Betracht fällt, kann ein Geschäftsbetrieb zu deren Bezahlung verurteilt werden, wenn die Ermittlung der strafbaren Person unverhältnismässigen Aufwand bedingt. Es wird sich zeigen, inwiefern dies zu Spannungen innerhalb von Unternehmen führt, wenn die Führungsetage Entscheide (nicht) trifft und Vorgaben (nicht) macht, deren Konsequenzen Datenschutzbeauftragte oder einfachen Mitarbeitende zu tragen haben.

3.6 Risiken und Nebenwirkungen

Über Folgeschäden von Datenschutzverletzungen, welche betroffene Personen erleiden können, spricht selten jemand. Sie sind auch schwierig zu beziffern. Daten wie Name, Adresse, Geburtsdatum, Telefonnummer, E-Mail-Adresse usw. sind zwar keine «besonders schützenswerten» Personendaten, in den falschen Händen kann mit solchen Angaben jedoch bereits Einiges angestellt werden. Ein erhöhtes Spam-Aufkommen ist dabei noch das geringste Problem. Abgeflossene Daten werden von Kriminellen für massgeschneiderte *Social Engineering*-Angriffe verwendet, welche die Installation von Schadsoftware, die Beschaffung weiterer (sensiblerer) Daten, das Auslösen ungerechtfertigter Zahlungen oder andere, sich auf die Betroffenen negativ auswirkende, Ziele verfolgen.[11] Angaben zu Personen können auch zur Identitätsanmassung missbraucht werden – jemand kann sich als diese Person ausgeben, indem sie deren Daten verwendet. So können mit dieser fremden Identität Social Media-Konten erstellt, Domainnamen registriert oder Bestellungen getätigt werden. Auch Betrug gegen Kontakte von Personen, deren E-Mail-Konto kompromittiert oder Daten anderweitig abgeflossen sind, kommt regelmässig vor.

Die Konsequenzen unbefugter Beschaffung und Weiterverarbeitung von Daten sind schwer abschätzbar. In Zeiten von Big Data und maschinellem Lernen wird automatisiertes Zusammenführen verschiedenster Datenquellen immer einfacher. Ob dies durch Unternehmen für legitime Zwecke, im rechtlichen Graubereich oder durch kriminelle Akteure erfolgt, ist nur oberflächlich relevant. Es ist davon auszugehen, dass jede Datenbank früher oder später gehackt wird und die Datensätze den Weg in den Untergrundmarkt finden.

3.7 Schlussfolgerung

«Unsere Daten» oder eben «Daten über uns» sind von vielen Akteuren an vielen Orten gespeichert. Das Erheben, Sammeln und Zusammenführen von Daten ist ein Geschäftsmodell in legalen und in illegalen Kreisen und führt zum Handel mit diesen Daten. Somit müssen wir damit rechnen, dass Gewerbe- oder Werbetreibende und kriminelle Akteure über mehr oder

[11] Siehe https://www.microsoft.com/security/blog/2019/12/02/spear-phishing-campaigns-sharper-than-you-think/ und MELANI Halbjahresberichte, jeweils in den Kapiteln "Social Engineering".

weniger grosse Datenbestände über uns verfügen und diese verwenden können, um uns gezielt anzugehen. Wenn aus den Daten zudem Persönlichkeitsprofile erstellt werden, eröffnet dies Möglichkeiten zur spezifischen psychologischen Einflussnahme, nicht nur bezüglich Konsum und der Empfänglichkeit für Betrugsmaschen, sondern auch bezüglich der Meinungsbildung und damit insofern schliesslich auch des Wahl- und Stimmverhaltens.

Werbung wird uns im Internet bereits heute vielfach individuell angezeigt. Diese Tendenz wird sich fortsetzen und dürfte zunehmend auch von politischen Akteuren genutzt werden, um gezielt Wahl- und Abstimmungspropaganda zu machen.

Kriminelle werden ihre Angriffsmethoden weiter verbessern und individueller auf potenzielle Opfer zuschneiden. Schon lange gilt eine personalisierte Anrede in einem E-Mail nicht mehr als taugliches Kriterium für dessen Seriosität. Kriminelle befüllen ihre Mails schon länger mit Name, Adresse, Telefonnummer und weiteren persönlichen Angaben über den Empfänger oder die Empfängerin. Auch gefälschte Absenderadressen werden regelmässig so gewählt, dass es scheint, als käme das E-Mail von einer bekannten Person – wenn das E-Mail oder die Social Media-Nachricht nicht sogar mit dem echten, aber kompromittierten, Konto des vermeintlichen Absenders gesendet wird.

Beurteilung / Empfehlungen:

Auch wenn das Internet viele Vorteile mit sich bringt und den Zugang zu wertvollen Informationen enorm vereinfacht hat: Glauben Sie nicht alles, was im Netz steht oder im elektronischen Posteingang landet. Vorsicht und eine gesunde Portion Skepsis sind beim Surfen und Kommunizieren im Internet angezeigt. Sprechen Sie im Zweifelsfall lieber einmal mehr mit Bekannten über Themen und Ereignisse und über sonderbare Nachrichten. Fragen Sie im Zweifelsfall beim vermeintlichen Absender nach, bevor Sie einen Link anklicken oder ein per E-Mail zugeschicktes Dokument öffnen.

Wer Personendaten bearbeitet und speichert, muss darum besorgt sein, diese angemessen vor unbefugtem Zugriff zu schützen. Öffentliche Register sollen eine grundsätzliche Abfrage zulassen, müssen jedoch Massenabfragen verhindern. Auch bei anderen Datensammlungen, auf welche in eingeschränkter Weise – z. B. mit Test- oder Demozugängen – zugegriffen werden darf, ist darauf zu achten, dass diese Einschränkungen nicht ausgehebelt werden können. Akteure, die sich auf das Sammeln von Daten spezialisiert haben, versuchen technische Einschränkungen zu umgehen, zum Beispiel durch automatische Generierung zahlreicher Test-Konten oder anderweitiger Vorspiegelung einer Vielzahl von Nutzenden.

4 Bedrohungslage

Über das Online-Meldeformular von MELANI[12] können uns Vorfälle zur Kenntnis gebracht und Fragen gestellt werden. Meldungen helfen uns, Trends zu Gefahren im Internet zu erkennen, darüber zu informieren und allfällige Gegenmassnahmen zu empfehlen oder selbst zu ergreifen. Die untenstehende Grafik über Art und Anzahl der Meldungen des zweiten Halbjahres 2019 gibt Hinweise darauf, was die Schweizer Bevölkerung in dieser Periode beschäftigt hat.

Im Internet wird viel gelogen und betrogen. Dies lässt sich aus den Meldungen zu Phishing, Betrug und «*Fake Sextortion*» ableiten. Bei diesen Phänomenen handelt es sich um Vorfälle, die typischerweise relativ leicht erkennbar sind und deshalb auch häufig zu Meldungen führen. Bei entsprechenden Meldungen kann mehrheitlich davon ausgegangen werden, dass betroffene Nutzerinnen und Nutzer die Machenschaften durchschaut haben und nicht Opfer wurden. Über die Erfolgsquote dieser Angriffe können wir keine fundierten Aussagen machen. Demgegenüber ist bei Meldungen zu Ransomware damit zu rechnen, dass der zugrundeliegende Vorfall zumindest manchmal einen gewissen Schaden angerichtet hat. Andere Malware-Ereignisse laufen unbemerkt im Hintergrund ab und werden deshalb weder erkannt noch von Betroffenen gemeldet (vgl. «Drive-By» Situation in der Schweiz, Kap. 4.3.2).

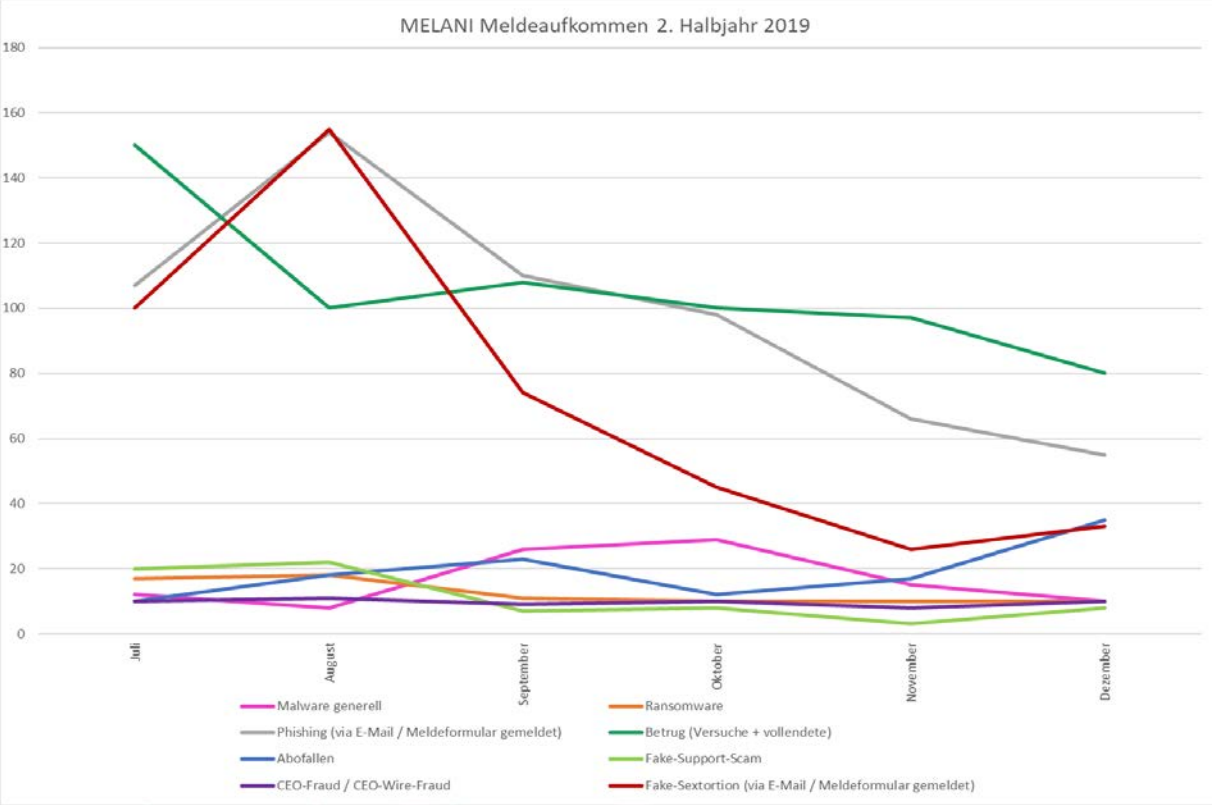

Abb. 2: Via Online-Meldeformular eingegangene Meldungen. Nicht enthalten sind Meldungen über andere Kanäle.

12 https://www.melani.admin.ch/melani/de/home/meldeformular/formular0.html

4.1 Spionage

Auch im zweiten Halbjahr 2019 war die Cyberspionage ein beliebtes Werkzeug von Staaten für das Sammeln von Informationen sowie den Diebstahl von geistigem Eigentum. Die «Threat Analysis Group» (TAG) von Google befasst sich mit der Erkennung und Abwehr von Cyberangriffen gegen ihre Nutzerinnen und Nutzer. Sie vermeldete beispielsweise allein für das dritte Quartal 2019 (Juli bis September) 12'000 *Spear-Phishing*-Versuche in 149 Staaten.[13] Verantwortlich dafür sollen über 270 mit Regierungsstellen verbundene Gruppen sein, die in mindestens 50 Ländern agieren. Abgesehen von der klassischen Spionage wurden auch Desinformationskampagnen erfasst, mit denen die Interessen eines bestimmten Staates gefördert oder politische Bewegungen diskriminiert werden sollen. Wie die Dissidenten und Aktivistinnen gehören auch die Politikerinnen und Politiker zur Gruppe mit hohem Risikopotenzial. Dies bezeugen Hunderte von Angriffsversuchen gegen politische Organisationen, die von «AccountGuard», dem Sicherheitsservice von Microsoft, registriert worden sind. Diese Plattform wurde für die Warnung von Wahlkampf betreibenden Kandidierenden und Ämtern eingerichtet, die ins Visier von Cyberangriffen geraten sind. Am stärksten sollen aber die Grossunternehmen von gezielten, staatlich gesponserten Versuchen der Cyberkompromittierung betroffen sein. Zahlenmässig sollen sie über drei Viertel der 10 000 Nutzerinnen und Nutzer ausmachen, über die Microsoft 2019 Meldung erstattete.[14] Der Software-Gigant erstellte eine Liste mit den fünf aktivsten Angriffsgruppen, sogenannten *Advanced Persistent Threat (APT),* des Jahres 2019. Von den aufgelisteten Gruppen soll «Holmium» alias «APT33» – laut Microsoft und anderen Sicherheitsfirmen[15] – von der iranischen Regierung gesponsert sein. Sie soll in erster Linie Organisationen anvisieren, die in den Sektoren Zivil- und Militärluftfahrt sowie in der petrochemischen Energie tätig sind. Die Kampagne geriet in die Schlagzeilen, weil unter anderem zwischen 2016 und 2017 ein in der Luftfahrt tätiges US-amerikanisches Unternehmen und eine im gleichen Bereich aktive saudi-arabische Organisation angegriffen worden waren.[16] Eine weitere besonders aktive Gruppe ist laut Microsoft «Strontium» alias «Fancy Bear» alias «APT28» oder «Sofacy». Gemäss offizieller Kommunikation einiger Staaten (namentlich die UK und die USA) sowie Sicherheitsfirmen (wie «CrowdStrike») soll die Gruppe mit dem russischen Militärnachrichtendienst (GRU) in Verbindung stehen. Die Gruppe wurde unter anderem mit den Angriffen gegen den deutschen Bundestag (2015), das US-amerikanische Democratic National Committee (2016) und die Welt-Anti-Doping-Agentur (2016) in Verbindung gebracht.

4.1.1 Cyberangriffe gegen Sport- und Anti-Doping Organisationen

Sport- und Anti-Doping-Organisationen sind bereits seit einigen Jahren das Ziel von Cyberspionage-Kampagnen. Wie im MELANI Halbjahresbericht 2018/1 (Kapitel 4.1.1) ausgeführt, wurde die IKT-Infrastruktur der olympischen Winterspiele von Pyeongchang (Südkorea) im

13 https://blog.google/technology/safety-security/threat-analysis-group/protecting-users-government-backed-hacking-and-disinformation/

14 https://blogs.microsoft.com/on-the-issues/2019/07/17/new-cyberthreats-require-new-ways-to-protect-democracy/; https://arstechnica.com/tech-policy/2019/07/microsoft-warns-10000-customers-theyre-targeted-by-nation-sponsored-hackers/

15 https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html

16 Siehe MELANI Halbjahresbericht 2017/2, Kapitel 5.1.2.

gleichen Jahr vom Wurm «Olympic Destroyer» angegriffen, bei dem der Sicherheitsdienstleister Kaspersky Lab Analogien mit «Sofacy» fand. Es scheint, dass auch die Gruppe «Fancy Bears» mit dieser Kampagne in Verbindung steht. Sie veröffentlichte am Anfang des gleichen Jahres Daten, die zwischen Ende 2016 und Anfang 2017 dem Internationalen Olympischen Komitee sowie dem Nationalen Olympischen Komitee der USA entwendet worden waren. Dazu gehörten neben E-Mails der Organisationen auch Krankengeschichten von Athleten.

Am 28. Oktober 2019 verkündete das «Threat Intelligence Center» von Microsoft die Identifikation zahlreicher Angriffe, die vermutlich von «Sofacy» gegen mindestens 16 Anti-Doping-Behörden und Sportorganisationen auf drei Kontinenten ausgeführt worden waren. Die Angriffe begannen vermutlich Mitte September, kurz vor der Veröffentlichung des Entscheids der Welt-Anti-Doping-Agentur (WADA), Russland von den Olympischen Spielen Tokio 2020 auszuschliessen.[17]

Diese Kampagne ist bei weitem nicht die einzige in Verbindung mit den Sommerspielen, welche im Jahr 2021 in Japan stattfinden werden, nachdem sie aufgrund der Coronavirus-Krise um ein Jahr verschoben wurden.. Die Organisatoren warnten vor E-Mail-Kampagnen, die den Namen des Organisationskomitees der Olympischen Spiele und der Paralympics missbrauchen, um die Empfängerinnen und Empfänger auf *Phishing*-Seiten weiterzuleiten oder ihre Geräte zu infizieren. Eine Phishing-Kampagne zielte spezifisch auf 170'000 Einzelpersonen in Japan und den USA ab. Einige Details dieses Angriffs, wie die Absicht und der Umfang, seien in einem Chat im Dark Web gefunden worden.[18] Die Hinweise scheinen in diesem Fall auf eine andere Urheberschaft hinzudeuten als diejenige der versuchten Infiltration von Sport- und Anti-Doping-Organisationen im vergangenen Oktober.[19]

Was macht diese Ziele so attraktiv? Vor den Wettkämpfen können die Angriffe dazu dienen, Informationen über Athleten aus anderen Ländern, ihre Fähigkeiten, Schwachpunkte und Pläne zu sammeln – in der Hoffnung, mit diesen Informationen mögliche Gewinnstrategien zu entwickeln. Ein weiterer Grund könnte die Verfälschung der Ergebnisse von Dopingtests sein. In einigen Ländern geht der Sport über einen Wettkampf zwischen Athleten hinaus. Er ist Teil des gesellschaftlichen Zusammenhalts und kann für politische Zwecke genutzt werden, zum Beispiel erlaubt es der Sport einigen politischen Führungskräften von der Popularität erfolgreicher Sportler zu profitieren. Zudem bieten grosse Sportveranstaltungen eine ideale Plattform, um die eigenen Informatikkenntnisse zur Schau zu stellen. Potenziell bieten solche Angriffe durch *False-Flag*-Techniken zudem die Gelegenheit, ein konkurrierendes Land zu diskreditieren und die Figuren auf dem Schachbrett der internationalen Politik neu anzuordnen. Schliesslich können die Angriffe in einem sanktionierten Land das Bedürfnis nach Genugtuung stillen.

4.1.2 «Winnti» Industriespionage-Kampagne

Laut neusten Enthüllungen steigt die Zahl der deutschen Weltkonzerne, die in den letzten Jahren Ziel von Cyberangriffen geworden sind. Der Kommunikationsriese Siemens beispielsweise bestätigte vor Kurzem, im Juni 2016 Opfer eines Cyberangriffs gewesen zu sein, bei dem es aber anscheinend zu keinem Datenabfluss gekommen war. Betroffen war auch «Covestro»,

17 https://blogs.microsoft.com/on-the-issues/2019/10/28/cyberattacks-sporting-anti-doping/

18 https://www.bleepingcomputer.com/news/security/tokyo-2020-staff-warns-of-phishing-disguised-as-official-emails/

19 https://english.kyodonews.net/news/2018/09/e2d8f3727275-phishing-scam-on-2020-olympics-tickets-spotted.html

ein Hersteller von Kunst- und Klebstoffen, der ebenfalls keinen Schaden davontrug. Der Pharmariese «Bayer» teilte im April mit, dass er bereits 2018 Opfer von Cyberspionage geworden war. All diese Angriffe sollen laut verschiedenen Sicherheitsexperten von «Winnti» ausgelöst worden sein. Mit diesem Namen wird sowohl eine Gruppe als auch die von ihr genutzte Malware bezeichnet, die unter anderem dafür bekannt ist, dass sie 2016 den Stahlkonzern «ThyssenKrupp» infiltriert hatte.[20] Die gleichen Experten sind der Meinung, dass diese Angriffe ihren Ursprung in China haben.

Zu Beginn konzentrierte sich die Gruppe mit rein finanziellen Absichten auf Angriffe gegen Online-Spielplattformen. Spätestens 2015 weitete sie jedoch ihre Aktivitäten auf Industriespionage aus. Sie scheint es insbesondere auf den Chemie- und Pharmasektor sowie auf Unternehmen, die auf Spitzentechnologien spezialisiert sind, abgesehen zu haben. In einer vertieften Analyse stellten der «Bayerische Rundfunk» und der «Norddeutsche Rundfunk» ältere Infektionen fest, die bis zu dem Zeitpunkt noch keine Schlagzeilen gemacht haben. Sie erwähnten beispielsweise das Unternehmen «Henkel», das wie «Covestro» unter anderem Klebstoffprodukte für die Industrie herstellt und 2014 infiltriert worden war. Ein weiteres bestätigtes Opfer sei «BASF» (Badische Anilin- und Soda-Fabrik), eines der grössten Chemieunternehmen der Welt, das seinen Sitz ebenfalls in Deutschland hat. Der 2015 erfolgte Angriff hatte keine schwerwiegenden Konsequenzen.[21]

Nach dem Eindringen in ein Unternehmensnetz erstellen die Hacker eine Abbildung des Netzwerks, um anschliessend nach den strategischen Punkten zu suchen, in denen das Schadprogramm versteckt werden kann. Auf diese Weise können sie möglichst lange unsichtbar im Hintergrund agieren und Informationen über das Unternehmen und seine Produkte sammeln, in der Hoffnung, Betriebsgeheimnisse zu finden. Ausdauer ist eines der Hauptmerkmale von «Winnti». Durch die Installation von Hintertüren verschafft sich die Täterschaft andauernden Zugriff auf ein Unternehmensnetz. Im Oktober 2019 meldete das IT-Sicherheitsunternehmen «ESET», bis dahin eine unbekannte Hintertür bemerkt zu haben, die auf Microsoft SQL (MSSQL) zielt und von «Winnti» benutzt wird.[22]

Obwohl «Winnti» nach dem Angriff auf «ThyssenKrupp» in Deutschland ins Rampenlicht geraten ist, ist die Kampagne auch in anderen Ländern Westeuropas, Asiens und in den USA aktiv. Eine Recherche von «ESET» hat ergeben, dass die Gruppe über «PortReuse», eine im März 2019 bekannt gewordene Hintertür, einen grossen Hersteller von mobiler Hard- und Software mit Sitz in Asien infiziert haben soll. Mit dieser Kompromittierung bereitete sich die Hackergruppe möglicherweise auf einen weitreichenden Angriff über die Zulieferungskette vor.[23]

Schliesslich wird die Malware auch für politische Spionage genutzt. Gemäss den Experten von Kaspersky Lab soll es derzeit mindestens zwei Gruppen geben, die dieses Angriffswerkzeug

---

20 https://www.waz.de/wirtschaft/spionage-mehrere-dax-konzerne-von-hackern-angegriffen-id226573145.html; siehe auch MELANI Halbjahresbericht 2016/2, Kapitel 5.1.3.

21 http://web.br.de/interaktiv/winnti/

22 https://www.zdnet.com/article/researchers-find-stealthy-mssql-server-backdoor-developed-by-chinese-cyberspies/; https://www.welivesecurity.com/deutsch/2019/10/29/winntis-skip-2-0-microsoft-sql-server-backdoor/

23 https://www.bleepingcomputer.com/news/security/winnti-group-uses-new-portreuse-malware-against-asian-manufacturer/

verwenden. Dies erschwert die abschliessende Feststellung, ob es sich bei den Verantwortlichen für die Industrie-Cyberspionage um die gleichen Akteure handelt wie bei jenen, welche eher politische Spionage betreiben – sei es gegen die Regierung von Hongkong oder den indischen Telekommunikationsanbieter in der Region, in der sich der Hauptsitz der tibetischen Exilregierung befindet.[24]

Schlussfolgerung / Empfehlungen:

Bereits seit mehreren Jahren sind Advanced Persistent Threats (APT) ein Problem, das nicht mehr ausschliesslich staatliche und militärische Stellen betrifft. Immer öfter sehen sich auch internationale Organisationen und private Unternehmen in diversen Sektoren mit hochkomplexen Angriffen konfrontiert. Man kann diese Ereignisse teilweise mit einer gewissen Demokratisierung der hochkomplexen Angriffe erklären, weil die dafür verwendeten Werkzeuge mittlerweile weitestgehend verfügbar sind (siehe Kapitel 5.1.1 des Halbjahresberichtes 2019/1). Dies führt zu einer grösseren Anzahl Angreifer, die verschiedenste Ziele verfolgen. Viele Unternehmen aus der Privatwirtschaft verfügen weder über die nötigen finanziellen Ressourcen, noch über das Fachwissen für die Bekämpfung einer solchen Bedrohung.

Eine mögliche Lösung ist die Auslagerung der eigenen Computersicherheit an IT-Experten wie Cloud-Dienstleister und Cloud-Sicherheitsanbieter. Dies entbindet die Unternehmen jedoch nicht von der Verantwortung, weitere interne Massnahmen zur Sensibilisierung und Schulung der Mitarbeitenden zu treffen. Nicht zu unterschätzen ist das Risiko, dass (ehemalige) Mitarbeitende Dritten Zugriff auf das firmeneigene System gewähren. Sie können sich so auf einfache Weise bereichern, aus einem persönlichen Ressentiment heraus handeln oder wollen den Arbeitgeber mutwillig schädigen.

Empfehlenswert ist, sich einem oder mehreren öffentlichen oder privaten Netzwerken anzuschliessen, die Informationen über aktuelle Bedrohungen austauschen und Tipps geben, wie Risiken zu erkennen sind und was man selber zum eigenen Schutz unternehmen kann.

[24] http://web.br.de/interaktiv/winnti/

Technische Massnahmen:

Zeigt eine interne Risikoanalyse eine konkrete Gefahr für Ihre Organisation oder Einrichtung auf, sollten Sie sich mit einigen technischen Massnahme schützen, um die Möglichkeit einer Infektion einzuschränken:

Auf Systemebene:

- Verwendung von «AppLocker» (oder einer vergleichbaren Funktion), um die Ausführung von unbekannten Binärdateien, namentlich aus den Ordnern der Nutzerprofile, zu verhindern;
- Einschränkung der nicht notwendigen Nutzerrechte;
- Verwendung eines Alarms für die Ausführung von Systemausführungswerkzeugen.

Für das Active Directory (AD):

- Sorgfältige Überwachung des AD für die Erkennung von ungewöhnlichen und grossen Anfragen;
- Einführung einer Mehrfach-Authentisierung für das AD und insbesondere für den Fernzugriff;
- zudem wird den Microsoft-Kunden empfohlen, regelmässig RAP as a Service zu verwenden (siehe https://services.premier.microsoft.com/assess/).

Auf Netzebene:

- Archivierung der Logdaten für eine Dauer von mindestens 2 Jahren für wichtige Gateway-Systeme wie Proxy DNS;
- Ausführung von Passive DNS für die Schnellprüfung von verdächtigen Domains;
- Einführung des signaturengestützten Intrusion Detection System (IDS) «Snort»;
- Verwendung einer internen Segmentierungspolitik (es ist im Allgemeinen besser, die Client-Client-Kommunikation zu vermeiden);
- Sammlung der Netflow-Daten an verschiedenen Stellen des internen Netzwerks;
- Wahl eines zentralen Kontrollpunkts für den Internetzugriff, der sorgfältig überwacht wird;
- Out-of-Band-Verwaltung der Server, die ein Management-LAN verwenden – keine Navigation und E-Mails von der Managementstation;
- Proxy Whitelisting für internationale Server, die extern kommunizieren müssen.

4.2 Industrielle Kontrollsysteme

Im ersten Halbjahresbericht im Jahre 2005 schrieb MELANI in einem Artikel zu neuen Richtlinien zur Informatik-Sicherheit von Nuklearanlagen in den USA: «Die Hauptprobleme in der Sicherheit der so genannten SCADA-Systeme in Kraftwerken (Supervisory Control and Data Acquisition) ist in den Bereichen der bisher weitgehend unverschlüsselten Daten- und Kommando-Transmissionen, der Anbindung an öffentliche Netzwerke und in der fehlenden Standardisierung der Technologien zu suchen».[25]

Seither hat das Sicherheitsbewusstsein im Bereich industrieller Kontrollsysteme (IKS) merklich zugenommen. Dazu beigetragen haben sicher auch die in den letzten 15 Jahren bekannt gewordenen Angriffe auf die Integrität von Prozessen, welche durch IKS gesteuert werden. Neben Angriffen auf die Systeme selbst, die diese natürlich beeinträchtigen können, lassen speziell Angriffe aufhorchen, die auf den durch die Systeme gesteuerten Prozess zielen. «Stuxnet»[26] im Jahr 2010, «Industroyer/CRASHOVERRIDE»[27] Ende 2016 und «Triton/Trisis»,[28] entdeckt im Jahr 2017, sind die namhaftesten Beispiele in dieser Kategorie. Zur Veranschaulichung beleuchten wir im Kapitel 4.2.1 die prozessual angestrebte Schadenswirkung von «CRASHOVERRIDE» auf die Stromversorgung der Ukraine.

Die ausgebaute Vernetzung der Steuerungssysteme sowie Aktoren und Sensoren haben zur gesteigerten Kritikalität der passenden Absicherung solcher Systemlandschaften beigetragen. Das «Industrial Internet of Things» (IIoT) ermöglicht erfolgsversprechende neue Automatisierungsprozesse, steigert aber gleichzeitig die Angriffsfläche auf eben diese Prozesse. Die Gewährleistung eines adäquaten Niveaus der Sicherheitsmassnahmen bleibt eine noch nicht flächendeckend gelöste Herausforderung.

4.2.1 Stromversorgung bleibt im Visier

Die Stromversorgung in der Ukraine wurde im Dezember 2016 Opfer einer Cyberattacke, welche zu einem Ausfall führte.[29] Den Technikern der «Ukrenergo» im Unterwerk «Nord» bei Kiew gelang es damals jedoch nach knapp einer Stunde, die Stromversorgung durch manuelle Schalthandlungen wieder herzustellen. Neue Auswertungen[30] dieses Angriffes mit der Schadsoftware «CRASHOVERRIDE» zeigen jedoch auf, dass die Angreifer bei erfolgreicher Ausführung (siehe Abbildung 3) eine physische Zerstörung von Netzelementen bei genau diesem Vorgang provozieren wollten. Ein Teil des Angriffs zielte auf die Schutz-Relays des Übertragungsnetzes. Das Ziel des Angriffs, die Schutzfunktion der Relays ausser Kraft zu setzen (Denial of Service), schlug jedoch fehl. Ohne den Schutz durch die Relays in Kombination mit der fehlenden Visibilität in die angegriffenen Kontrollsysteme hätte eine ungünstige Einschaltsequenz Teile des Netzes schädigen können, was neben den physischen Schäden zu bedeutend längeren Ausfallzeiten geführt hätte.

---

25 MELANI Halbjahresbericht 2005/1, Kapitel 7.1.

26 MELANI Halbjahresbericht 2010/2, Kapitel 4.1.

27 MELANI Halbjahresbericht 2017/1, Kapitel 5.3.

28 MELANI Halbjahresbericht 2017/2, Kapitel 5.3.2.

29 MELANI Halbjahresbericht 2016/2, Kapitel 5.3.1.

30 https://dragos.com/resource/crashoverride-reassessing-the-2016-ukraine-electric-power-event-as-a-protection-focused-attack/

Abb. 3: Beabsichtigter Angriffsverlauf (Quelle: dragos.com)

Das Wissen um solche Absichten von Angreifern zeigt die Wichtigkeit, Risiken in kritischen Bereichen so gering wie möglich zu halten. Ein Bericht der Eidgenössischen Elektriztitätskommission ElCom[31] machte im 2019 bekannt, dass in der Umsetzung der adäquaten Sicherheitsmassnahmen in der Schweizer Elektrizitätsversorgung noch Optimierungspotenzial besteht.[32] So verlangt die ElCom unter anderem, «OT-Systeme regelmässig auf Sicherheitslücken zu testen». In der Berichtsperiode wurde beispielsweise eine ganze Reihe von Schwachstellen[33] im Echtzeitbetriebssystem «VxWorks» publik, welches die Basis vieler anwendungsspezifischer Kontrollsysteme darstellt. Diese tiefe Integration bedingt die Mitwirkung einer ganzen Kette von Systemherstellern und Betreibern, um die Lücken in den operativen Prozessleitsystemen zu schliessen. Bekannte Sicherheitslücken im Bereich der Prozesssteuerung könnten künftig noch merklich zunehmen, da der Schwachstellen-Forschungswettbewerb «Pwn2Own»[34] neben klassischen IT-Systemen künftig auch IKS in seine Liste von zu untersuchenden Systemen aufnimmt. Neben den Systemen im Einsatz werden auch immer weitere Elemente mit den Netz verbunden,[35] was die koordinierte Umsetzung von Sicherheitsvorgaben unter Einbezug sämtlicher involvierter Zulieferer weiter erschwert.

Ausserdem nehmen laufend weitere Angreifer die Stromversorgungsbranche[36] sowie auch deren Zuliefererkette[37] ins Visier. Im Spätsommer 2019 wurden zwei *Spear-Phishing*-Wellen gegen Stromverteiler in den USA beobachtet, die versuchten, die «LookBack»-Malware bei den Empfängerunternehmen einzuschleusen. Dazu imitierten die Angreifer in der Branche anerkannte Lizenzierungsgremien, um die Empfänger zu verleiten, die mitgesandten Anhänge zu

31 https://www.elcom.admin.ch/dam/elcom/de/dokumente/2019/Cyber-Sicherheit%202019%20-%20Bericht%20der%20ElCom.pdf.download.pdf/Cyber-Sicherheit%202019%20-%20Bericht%20der%20ElCom.pdf

32 https://www.tagesanzeiger.ch/schweiz/standard/fuer-hacker-stehen-die-einfallstore-offen/story/20223699

33 https://www.armis.com/urgent11/

34 https://www.darkreading.com/vulnerabilities---threats/pwn2own-adds-industrial-control-systems-to-hacking-contest/d/d-id/1336191

35 https://www.zdnet.com/article/ameo-concerned-about-nation-state-attacks-on-power-grids/

36 https://www.proofpoint.com/us/threat-insight/post/lookback-malware-targets-united-states-utilities-sector-phishing-attacks

37 https://www.wired.com/story/iran-apt33-industrial-control-systems/

öffnen. Die Malware selbst amtet – einmal installiert – als *Remote Access Trojan (RAT)*, welche dem Angreifer per Fernzugriff umfangreiche Funktionalitäten auf den infizierten Systemen zur Verfügung stellt.

Im Zuge des Wandels von fossilen Treibstoffen hin zu Elektromobilität gewinnt die Stromversorgung auch für diesen gesellschaftlichen Aspekt an Bedeutung. Gleichzeitig verlagern die energiepolitischen Ziele die Elektrizitätsproduktion weiter von zentralen Grosskraftwerken hin zu dezentralen, kleineren Anlagen erneuerbarer Energiegewinnung. Damit einher geht die Informatisierung der Stromversorgung (SmartGrid). MELANI ist bestrebt, zusammen mit den Stromproduzenten und Netzbetreibern die Versorgung der Schweiz bestmöglich vor einem Eintritt von Informationssicherheitsrisiken zu bewahren. Die Zuverlässigkeit der Stromversorgung ist ein zentraler Faktor für das Funktionieren von Wirtschaft und Gesellschaft und den Erhalt unseres Wohlstandes.

Empfehlung:

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

Meldeformular MELANI
https://www.melani.admin.ch/melani/de/home/meldeformular.html

Checkliste mit Massnahmen zum Schutz industrieller Kontrollsysteme:
https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/massnahmen-zum-schutz-von-industriellen-kontrollsysteme--ics-.html

4.3 Angriffe (DDoS, Defacements, Drive-By)

4.3.1 DDoS zur Erpressung oder Beeinträchtigung eines Dienstes

In der Altjahrswoche 2019 gab es DDoS-Attacken gegen Schweizer Online-Medien,[38] wodurch einige Webseiten zwischenzeitlich nicht verfügbar waren. Die Motivation dahinter bleibt bis heute unklar.

Unter DDoS (Distributed Denail of Service = Verweigerung eines Dienstes) versteht man einen Angriff auf Computer-Systeme mit dem Ziel, deren Verfügbarkeit zu stören. Im letzten Halbjahr wurden wieder häufiger DDoS-Attacken in Zusammenhang mit Erpressung beobachtet.[39] Die

[38] https://www.20min.ch/digital/news/story/Technische-Probleme-auf-20minuten-ch-12858361; https://www.nzz.ch/wirtschaft/cyberattacke-gegen-schweizer-medien-ld.1530906

[39] Zu dieser Vorgehensweise siehe insbesondere MELANI Halbjahresbericht 2016/1, Kap. 4.4.1 sowie weitere Beiträge in den MELANI Halbjahresberichten 2018/1, Kap. 4.3.1, 2017/2, Kap. 4.3.1, 2016/2, Kap. 4.4.1, 2015/2, Kap. 4.3.4, 2015/1, Kap. 4.4.1.

Angreifer führen oft vorab einen Test-Angriff durch, um zu zeigen, dass sie diese Fähigkeiten besitzen. Sie verlangen vom Opfer die Bezahlung eines Lösegelds, um einen weiteren, heftigeren Angriff abzuwenden. Auch können solche Angriffe politisch motiviert sein, wie der DDoS-Angriff auf die Webseiten der Britischen «Labour Party» gezeigt hat.[40] Laut einigen Sicherheitsforschern ist die Tendenz jedoch bei Angriffen von niedriger Intensität, so dass die DDoS-Abwehrmassnahmen (noch) nicht eingeschaltet werden, die Performance von Webseiten oder Servern aber dennoch beeinträchtigt ist.[41]

Empfehlung:

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

Checkliste mit Massnahmen gegen DDoS-Attacken

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

4.3.2 «Drive-By»: Situation in der Schweiz

Es gibt verschiedene Varianten, wie ein Gerät mit Schadsoftware infiziert werden kann. Eine verbreitete Methode ist, Webseiten zu hacken und ein Skript zu platzieren. Dieses sucht durch das Ausprobieren von *Exploits* nach noch nicht geschlossenen Sicherheitslücken im Browser oder bei sonstigen Anwendungen wie z. B. FlashPlayer. Da das Aufrufen der manipulierten Webseite bereits ausreichen kann, um infiziert zu werden, spricht man von «Drive-By-Download».

Im zweiten Halbjahr 2019 hat MELANI rund 500 infizierte Webseiten in der Schweiz festgestellt und deren Betreiber darüber informiert, damit diese ihre Webseiten bereinigen konnten.

Internetnutzer, welche solche infizierten Webseiten entdecken sind gebeten, diese MELANI zu melden und damit einen Beitrag zur allgemeinen Cybersicherheit zu leisten.

Empfehlungen:

1. Installieren Sie mindestens zwei verschiedene Browser, um bei Bekanntwerden einer schweren Sicherheitslücke bei einem Browser kurzfristig auf einen anderen umsteigen zu können.
2. Installieren Sie immer die neusten Updates für Ihre Browser, am besten mittels automatischen Sicherheitsupdates.
3. Verwenden Sie wenn möglich einen sogenannten «*Ad-Blocker*» und schränken Sie die Verwendung von «*JavaScript*» so stark wie möglich ein.
4. Wenn eine Webseite Sie unerwartet zum Herunterladen einer Datei auffordert, akzeptieren Sie dies auf keinen Fall.

---

40 https://www.theregister.co.uk/2019/11/12/labour_party_reports_cyber_attack/

41 https://www.zdnet.com/article/ddos-attacks-getting-smaller-sneakier-and-more-dangerous/#ftag=RSSbaffb68

4.3.3 Cyberangriff gegen die Kryptowährungsplattform «Upbit»

Kryptowährungsplattformen sind immer wieder ein lukratives Ziel für Angreifer, da bei einem erfolgreichen Angriff sehr viel Geld gestohlen werden kann. So erging es auch der südkoreanischen Plattform «Upbit», bei welcher Angreifer 342'000 «*Ethereum*» aus dem «*Exchange Hot Wallet*» gestohlen haben. Zum Zeitpunkt des Diebstahls waren diese «Ethereum» 48,5 Millionen US Dollar wert. Spekulationen zufolge könnte es sich um einen sogenannten «Exit Scam» handeln: Insider transferieren Geld der Nutzer der Plattform auf ein eigenes Konto und behaupten, ein Cyberangriff sei schuld dafür. Allerdings ist es schwierig, die gestohlenen «Ethereum» zu Bargeld zu machen, da diese mit relativ viel Aufwand «gewaschen»[42] werden müssten, um die Rückverfolgung ihrer Herkunft zu verhindern.[43]

4.4 Social Engineering und Phishing

4.4.1 Phishing

Im zweiten Halbjahr 2019 gab es sehr viele Phishing-Angriffe, besonders auch im Namen von verschiedenen Schweizer Marken. Der Inhalt der Mails ändert sich dabei nicht markant: Die einen fragen nach Kreditkartendaten, damit diese «verifiziert» werden können, andere fordern auf der verlinkten Seite nach Login und Passwort zu Internetdiensten. Regelmässig werden in solchen Phishing-Mails Firmenlogos von bekannten Unternehmen respektive des betroffenen Dienstes missbraucht, um den E-Mails einen offiziellen Anstrich zu geben. Nach wie vor ein häufiges Ziel sind E-Mail-Dienste, da mit den Zugangsdaten zu Mail-Konten eine Vielzahl von weiteren Angriffsmöglichkeiten offen stehen.

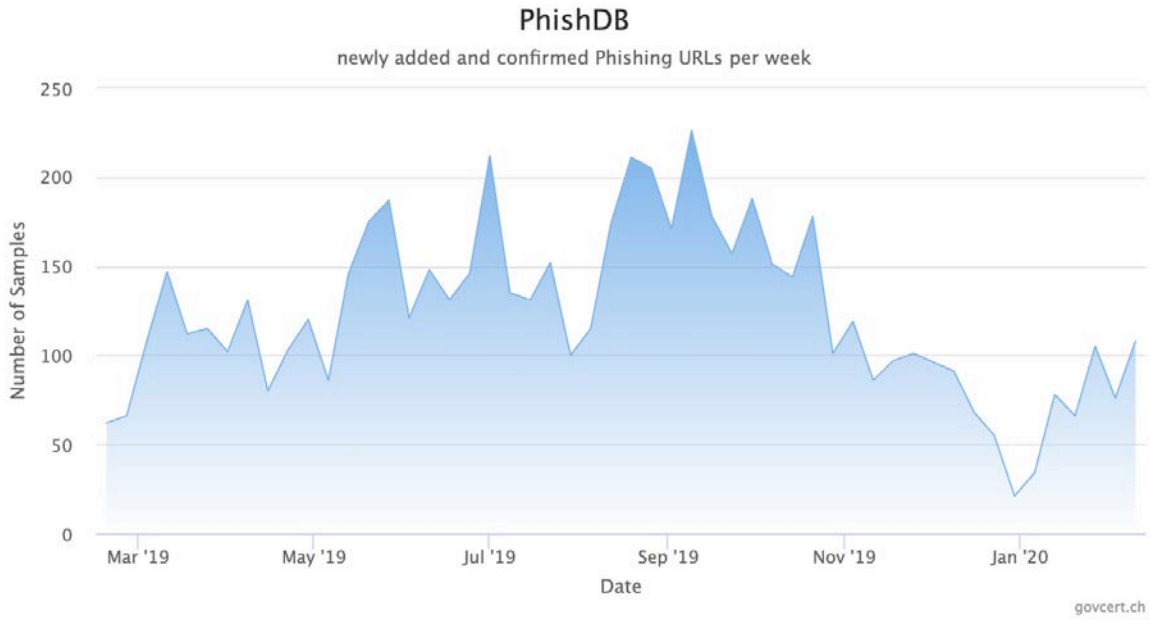

Abb. 4: Gemeldete und bestätigte Phishing-Seiten pro Woche auf antiphishing.ch im letzten Jahr, Stichtag 9.2.2020.

---

42 Siehe dazu auch Kap. 5.3

43 https://www.zdnet.com/article/upbit-cryptocurrency-exchange-loses-48-5-million-to-hackers/

4.4.2 Phishing-Webseiten mit 404-Fehlerseiten

Bei Webauftritten werden 404-Fehlerseiten verwendet, um einen Besucher darüber zu informieren, dass eine Unterseite, welche er auf einer Website besuchen möchte, unter der aufgerufenen Adresse nicht (mehr) existiert. Die meisten Betreiber von Websites erstellen für solche Situationen eine 404-Fehlerseite im Webseitendesign und hinterlegen diese als Standardfehlermeldung. So können sie Inhalte ihrer Wahl bei Auftreten des 404-Fehlers anzeigen lassen und dadurch den Website-Besucher gezielt informieren und gegebenenfalls weiterleiten. Wie auf jeder Webseite lassen sich leider auch hier bösartige Inhalte wie Phishing oder Drive-By-Downloads platzieren. Microsoft berichtete im vergangenen August, eine derartige Phishing-Kampagne gegen seine Benutzer entdeckt zu haben. Eine Phishing-Seite, die das Portal für die Anmeldung bei einem Microsoft-Konto perfekt nachahmt, wurde auf einer Website einer von Kriminellen registrierten Domain als 404-Fehlerseite hinterlegt. Das heisst, dass beim Aufruf jeder nicht existierenden URL auf der Website, die Besucher auf die manipulierte 404-Fehlerseite bzw. Phishing-Seite geleitet wurden.[44] Dank dieser Methode können die Angreifer eine unbegrenzte Anzahl von Phishing-URLs nach dem Zufallsprinzip erstellen und so die Erkennung und Blockierung anhand der Links in den E-Mails erschweren, da den URLs nur der Domainname gemeinsam ist.

Kriminelle hinter Phishing-Seiten sind ständig auf der Suche nach neuen Möglichkeiten, Benutzer dazu zu bringen, einem bösartigen Link zu folgen. Denken Sie also immer zweimal nach, bevor Sie einem Link in einem E-Mail oder einer Nachricht auf dem Smartphone folgen. Sie finden viele Empfehlungen auf unserer Website:

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

Sie können uns Phishing-Fälle unter folgender Adresse melden:

https://www.antiphishing.ch/

Ihre Meldungen helfen uns, Massnahmen zu ergreifen und somit andere Benutzer zu schützen.

4.4.3 Erpressung mit Behauptungen – neue Varianten

Weiterhin behaupten Kriminelle per E-Mail, dass sie Zugang zu Computer und Webcam hätten und drohen damit, kompromittierendes Bild- oder Videomaterial des Empfängers zu veröffentlichen, sollte kein Lösegeld innert einer bestimmten Frist in einer Kryptowährung bezahlt werden («*Fake Sextorsion*»). Oft enthalten diese Mails Passwörter und/oder Telefonnummern, die einen tatsächlichen Bezug zum potenziellen Opfer haben. MELANI kennt jüngste Beispiele, in denen bei den potenziellen Betrugsopfern vor Ablauf der Frist «nachgefasst» wurde, indem auf das Ende der Frist und die daraus entstehenden Konsequenzen nochmals per Mail hingewiesen wurde.

[44] https://www.bleepingcomputer.com/news/security/microsoft-warns-of-phishing-attacks-using-custom-404-pages/

Es wurden neuerdings auch Fälle verzeichnet, in denen der Absender behauptet, dass er im Besitz von Videodateien sei, die den Empfänger beim Konsumieren von illegaler Pornografie mit Kindern zeige. Um den Empfänger einzuschüchtern, sind Dateien im Anhang personalisiert benannt mit seinem Namen oder seiner E-Mail-Adresse. Diese Masche kann natürlich auch Nutzerinnen treffen.

Weiter gingen Beispiele ein, in denen andere Kryptowährungen als Bitcoin verwendet wurden. Dies wohl mit der Annahme, dass die Instrumente zur Nachverfolgung der Zahlung bei weniger gängigen Kryptowährungen noch nicht so gut funktionieren. Auch wurden *QR-Codes* anstelle von *Wallet*-Adressen im Klartext verwendet, da diese in E-Mails von Sicherheits-Software erkannt und die Mails häufig als betrügerisch geblockt werden. Dies zeigt erneut die Wichtigkeit der Kombination technischer Sicherheitsmassnahmen mit Sensibilisierungskampagnen, um die Prävention gegen Cyberangriffe effizient umzusetzen.

MELANI kennt auch Drohungen mit Säureangriffen und Engagement von Auftragskillern. Diese Art von erpresserischen E-Mails fanden jedoch nicht dieselbe Verbreitung wie die Masche der «Fake-Sextorsion». Dies ist sicher auf die Tatsache zurückzuführen, dass die Hemmung, sich bei Androhung physischer Gewalt bei den Behörden zu melden, weit geringer ist, als im Fall von «Fake-Sextorsion», wo auf allfällige intime Handlungen in der Vergangenheit Bezug genommen wird.

IT-Security-Forscher[45] haben entdeckt, weshalb die Sextorsion-Kampagnen in so grossen Wellen verzeichnet wurden. Mit Hilfe der Malware «Phorpiex» wurden inzwischen mehr als 450'000 Rechner infiziert und zu einem *Botnetz* zusammengeschlossen. Dieses Botnetz dient den Kriminellen dazu, ihre elektronischen Erpresserschreiben massenweise zu versenden. Die E-Mail-Adressen der Empfänger werden zufällig aus einer E-Mail-Datenbank gezogen. Die Inhalte der E-Mails werden aus Textbausteinen erstellt, was den Grad der Automation noch zusätzlich erhöht. Die Versand-Frequenz ist mit rund 30'000 Sextorsion-Mails pro Stunde relativ hoch. Die Reichweite der Kampagnen soll 27 Millionen potenzielle Opfer umfassen.

Lassen Sie sich von Behauptungen nicht einschüchtern, reagieren Sie nicht auf erpresserische E-Mails und kontaktieren Sie im Zweifelsfall die Behörden. Weiterführende Informationen zu Fake-Sextorsion-Mails finden Sie auf https://www.stop-sextortion.ch/, wo Sie solche E-Mails auch melden können. Falls Sie das im E-Mail genannte Passwort weiterhin verwenden, sollten Sie dieses unverzüglich ändern. Generell sollten Sie Passwörter regelmässig ändern und nicht das gleiche Passwort für mehrere Internetdienste zu verwenden. Kombinieren Sie für eine effiziente Prävention gegen Cyberangriffe technische Sicherheitsmassnahmen mit Sensibilisierungskampagnen.

45 https://m.pctipp.ch/news/artikel/user-pc-fuer-sextortion-spam-missbraucht-93135/

4.4.4 Geschäfts-E-Mail-Kompromittierung: eine widerstandsfähige und sich ständig weiterentwickelnde Vorgehensweise

Seit 2013 hat MELANI im Rahmen ihrer Halbjahresberichte die Masche Präsidenten- und Chef-Betrug («*CEO Fraud*») mehrfach aufgegriffen.[46] Dieses Phänomen hat mit der Zeit viele Veränderungen durchlaufen, und die Kriminellen verbessern ständig ihre Vorgehensweise, um neue Ziele und Opfer zu erreichen.

In den letzten Jahren haben Betrüger zunehmend die Identität von Lieferanten angenommen und Rechnungen mit abgeänderter IBAN an deren Kunden geschickt. Oftmals liefert das Hacken eines E-Mail-Kontos oder einer Online-Kollaborationsplattform Kriminellen die notwendigen Informationen auf dem Silbertablett, und die Original-Rechnungen können gefälscht werden.[47] Jüngste Statistiken des «Financial Crimes Enforcement Network» (FINCEN) in den Vereinigten Staaten bestätigen diesen Trend der zunehmenden Übernahme der Identitäten von externen Geschäftspartnern des Opferunternehmens.[48] Die Analyse des FINCEN liefert auch interessante Zahlen zu den betroffenen Tätigkeitsbereichen. Die verarbeitende Industrie (Manufaktur) und das Baugewerbe werden in den Vereinigten Staaten besonders ins Visier genommen. Dies lässt sich vielleicht damit erklären, dass diese Sektoren besonders von externen Lieferanten abhängig sind und mit vielen Subunternehmen arbeiten. Jedoch bleiben alle Sektoren potenzielle Ziele für Cyberangriffe aller Art.

Aber auch Betrugsversuche, bei denen sich der Angreifer als eine Person innerhalb des Zielunternehmens ausgibt, sind noch immer üblich. Kriminelle versuchen, die technologischen Fortschritte zu nutzen, um ihre Vorgehensweise zu verbessern. Das «Wall Street Journal» berichtete im September 2019 über einen Fall, bei dem sich Betrüger nicht nur per E-Mail als CEO ausgaben. Die Kriminellen waren mit Hilfe von Sprachsoftware und künstlicher Intelligenz in der Lage, die Stimme des Geschäftsführers zu imitieren und telefonisch betrügerische Geldüberweisungen zu veranlassen.[49]

Bei einer kürzlich auch in der Schweiz beobachteten Variante dieser Betrugsart geben sich die Kriminellen als Mitarbeitende eines Unternehmens aus. Sie schreiben an die Personen, die für die Auszahlung der Gehälter (in der Regel das Personalwesen) zuständig sind, und teilen ihnen mit, dass «ihr» Gehalt per sofort auf ein anderes Bankkonto überwiesen werden soll. Dieses Phänomen wurde bereits Anfang 2019 durch den Sicherheitsanbieter «Trustwave» genau dokumentiert[50]. In dem von «Trustwave» beschriebenen Fall legen Betrüger Adressen bei kostenlosen E-Mail-Diensten an. Zuvor werden die für den Angriff erforderlichen Informationen, wie z. B. die Identität der für die Lohnverwaltung zuständigen Personen, einfach aus offenen Quellen (Unternehmenswebsite, soziale Netzwerke usw.) entnommen.

---

46 MELANI Halbjahresberichte 2013/1, Kap. 3.4; 2016/1, Kap. 4.5.1; 2016/2, Kap. 4.5.1; 2017/1, Kap. 4.3.3; 2018/2, Kap. 4.4.3; 2019/1, Kap. 4.4.5.

47 Siehe MELANI Halbjahresbericht 2018/2, Kap. 4.4.3.

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

49 https://www.zdnet.com/article/forget-email-scammers-use-ceo-voice-deepfakes-to-con-workers-into-wiring-cash/

50 https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/bec-payroll-scam-your-salary-is-mine/

Schlussfolgerung / Empfehlung:

Angesichts der extremen Kreativität der Kriminellen und ihrer Fähigkeit, ihre Praktiken ständig anzupassen, bleibt die Abwehr von Betrugsversuchen eine Herausforderung für alle Unternehmen. Sensibilisieren Sie die Mitarbeitenden dahingehend, dass alle vom Unternehmen definierten Prozesse und Sicherheitsmassnahmen jederzeit einzuhalten sind. Insbesondere sollten alle Geldtransfers nach dem Vier-Augen-Prinzip mit Kollektivunterschriften erfolgen. Ankündigungen von Kontoänderungen ist besondere Aufmerksamkeit zu schenken.

Informationen und Empfehlungen zum Thema CEO-Betrug:

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

4.4.5 Online-Anlagebetrug

Im Berichtshalbjahr erhielt MELANI verschiedene Meldungen über falsche Online-Handelsplattformen und dafür werbende Websites, die mit Kryptowährungen schnelle und grosse Gewinne versprechen. Diese betrügerische Werbung wird oft über soziale Netzwerke verbreitet und missbraucht Prominente, um die Glaubwürdigkeit zu unterstreichen. In fiktiven Interviews erklären Prominente wie Roger Federer und DJ Bobo, einen Teil ihres Vermögens mit Bitcoins gemacht zu haben. Im Netz wird davor gewarnt, dass einmal investiertes Geld verloren sei.[51] «Fake News» sind ein derzeit verbreitetes Phänomen, vor dem man sich mit einer kritischen Haltung gegenüber bizarren oder aus zweifelhafter Quelle stammenden Meldungen schützen kann.

Börsenhandel ist grundsätzlich ein riskantes Geschäft. Unpersönliche Nachrichten von Handelsplattformen (beispielsweise in einem sozialen Netzwerk, per E-Mail, SMS oder WhatsApp) lassen darauf schliessen, dass es sich um eine unseriöse Massensendung handelt. Ein Aufklärungsvideo der Eidgenössischen Finanzmarktaufsicht (FINMA) stellt die Problematik ausführlich dar und erklärt, wie man sich vor Anlagebetrug schützen kann.[52] Ausserdem hat die FINMA eine Liste der anerkannten elektronischen Plattformen publiziert.[53] Zu berücksichtigen ist, dass auch (Massen-)Werbung für dubiose Angebote automatisiert mit Namen und weiteren individuellen Angaben versehen werden kann.

4.5 Datenabflüsse

4.5.1 Patientendaten zugänglich

Im Rahmen einer Untersuchung[54] wurden im Sommer 2019 mehrere Millionen von Patientendaten aus verschiedenen Ländern ungeschützt im Netz entdeckt. Dabei handelte es sich um

51 https://www.20min.ch/schweiz/news/story/Wieso-stoppt-niemand-die-Bitcoin-Betrueger--13654244
52 https://finma.ch/de/dokumentation/finma-videos/schutz-vor-anlagebetrug/
53 https://www.finma.ch/de/finma-public/bewilligte-institute-personen-und-produkte/
54 https://www.br.de/nachrichten/deutschland-welt/millionenfach-patientendaten-ungeschuetzt-imnetz,RcF09BW

hochsensible medizinische Daten auf ungesicherten Internetservern, die für jedermann während Jahren zugänglich gewesen waren. Die Röntgenbilder sind hochauflösend und mit personenbezogenen Daten versehen, darunter Vor- und Nachname, Geburtsdatum, Termin der Untersuchung und Informationen über den behandelnden Arzt oder die Behandlung selber. Die Untersuchungen mit bildgebenden Verfahren werden von den Geräten an spezielle Server geschickt, die für die Bildarchivierung verwendet werden (sog. «Picture Archiving and Communication System PACS»). In rund 50 Ländern sollen 16 Millionen Datensätze betroffen sein. Besonders betroffen sind Patienten aus den USA. In Deutschland sollen 13'000 Datensätze betroffen gewesen sein. Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) informierte 46 Länder und steht mit dem Betreiber des deutschen «PACS» Server in Kontakt. Es prüft zudem aufsichtsrechtliche Massnahmen von Empfehlungen für eine verbesserte IT-Sicherheit bis hin zur Verhängung einer Busse. Analysen von MELANI haben keinen Hinweis auf Schweizer Patientendaten geliefert, obwohl einige wenige PACS Server in der Schweiz standen.

Anhand des folgenden Beispiels lässt sich die weitreichende Verantwortung der Führungsorgane von Unternehmen aufzeigen:

Gewisse Hersteller von medizintechnischen Geräten vertreiben diese nicht nur, sondern sie betreuen diese nach dem Verkauf auch technisch. Als Dienstleister ist ein Unternehmen angehalten, gängige und branchenspezifische sowie allenfalls auch vertraglich vereinbarte Sicherheitsstandards einzuhalten. Dieses Wissen ist für das Risikomanagement in medizinischen Betrieben von zentraler Bedeutung: Der Empfänger der Dienstleistung eines Dritten ist dafür verantwortlich, sich über die tatsächlichen Sicherheitsmassnahmen des Dienstleisters zu informieren und diese dokumentieren zu lassen. So lässt sich sicherstellen, dass betriebsintern produzierte Daten beim externen Dienstleister auch entsprechend gesichert, gewartet und archiviert werden. Diese Sicherheitskonzepte sollten durch eine unabhängige externe Stelle überprüft werden.

Zwei weitere Datenabflüsse im Gesundheitssektor zeigen die Tragweite von Datenlecks und den Aufwand des Handlings solcher Vorfälle: Zwei in den USA ansässige Unternehmen – ein medizinisches Zentrum sowie ein medizinischer Zulieferer – berichteten über Datenabflüsse, von denen insgesamt rund 220'000 Personen betroffen gewesen waren.[55] Die Datenabflüsse ereigneten sich in Folge eines Phishing-Vorfalls und einer Ransomware-Attacke.

Hacker verschafften sich im Rahmen einer gezielten Phishing-Kampagne Zugang zu Office 365-Konten von Mitarbeitenden und konnten sich so rund zwei Monate unbemerkt in den E-Mail-Konten bewegen. Die Angreifer konnten möglicherweise auf aktuelle und ehemalige Patienten- und Mitarbeiterinformationen zugreifen und sich diese aneignen. Zu den potenziell abgeflossenen Informationen gehören Namen, Adressen, Geburtsdaten, Sozialversicherungsnummern, Mitarbeiter-Identifikationsnummern, medizinische Informationen, Krankenversicherungsinformationen, Finanzinformationen, Zahlungsmittelinformationen, Führerscheindaten,

[55] https://www.inforisktoday.com/2-health-data-breaches-affect-total-220000-a-13440

Reisepassinformationen, Passwort/PIN oder Kontoanmeldeinformationen und Rechnungsdaten[56].

Im Falle des Ransomware-Angriffs erlitt das medizinische Zentrum – ein Zusammenschluss verschiedener Dienstleistungserbringer im Gesundheitssektor – eine Verschlüsselung des Datenbestandes eines Mitglieds des medizinischen Zentrums. Dank Sicherungskopien (Backup) konnte der Zugang zu den medizinischen Daten wiederhergestellt werden. Allerdings waren die Verantwortlichen nicht in der Lage, den Zugang zu allen betroffenen Informationen wieder zu gewährleisten. Das Unternehmen geht davon aus, dass der Vorfall nicht zum Abfluss von Patienteninformationen an unbefugte Dritte geführt hat.

In beiden Fällen wurden die betroffenen Personen informiert und es wurden ihnen im Rahmen der Benachrichtigung kostenlose Kreditüberwachungsdienste während einer gewissen Zeit angeboten, um einen allfälligen Identitätsdiebstahl zu entdecken.

Empfehlungen:

Ein gesamtheitliches Risikomanagement ist in Unternehmen zentral. Bei grösseren Datenabflüssen sind regelmässig auch Drittanbieter beteiligt. Unternehmen sämtlicher Sektoren müssen Sicherheitsanforderungen an Drittanbieter präzise formulieren und diese in die Verträge einfliessen lassen. In diesem Rahmen sollten auch die Vorfallsbewältigung sowie das Krisen- und Business Continuity Management (BCM) zur Sprache kommen. Weiter sollten Sie überprüfen, dass die Deckung der Cyberversicherung des Drittanbieters ausreicht, um den finanziellen Schaden aus dem Datenverlust sämtlicher Kunden abzudecken.

4.5.2 Datenabfluss bei FSB Industriepartner «Sytech»

Am 13. Juli 2019 soll beim Unternehmen «Sytech» ein Kontaktmann für den russischen Geheimdienst FSB gehackt worden sein. BBC Russland berichtete, dass die Hacker 7,5 TB Daten aus dem Netzwerk des Auftragnehmers gestohlen hatten. Diese Daten umfassen Informationen über zahlreiche geheime Projekte, die von «Sytech» im Auftrag der russischen Regierung und ihres Geheimdienstes entwickelt worden sind. Die gestohlenen Daten wurden anschliessend an eine andere Hackergruppe weitergegeben, welche diese mit den russischen Medien teilte. Gemäss BBC Russland handelt es sich um das grösste Datenleck in der Geschichte der russischen Geheimdienste.[57]

Die Daten umfassen eine Vielzahl von Projekten, darunter:

1. «Mentor» wurde angeblich für die russische Militäreinheit Nr. 71330 entwickelt, bei der es sich um den radio-elektronischen Geheimdienst des FSB Russlands handle. Dieses Projekt würde ausgewählte E-Mail-Konten in bestimmten Zeitabständen überwachen, um Informationen zu bestimmten Phrasen zu sammeln.

---

[56] In einem ähnlich gelagerten Fall hatten die Hacker zusätzlich Zugang zu den Informationen wie Diagnose und medizinische Behandlung: https://www.bleepingcomputer.com/news/security/phishing-incident-exposes-medical-personal-info-of-60k-patients/

[57] https://www.bleepingcomputer.com/news/security/russian-fsb-intel-agency-contractor-hacked-secret-projects-exposed/

2. «Nadezhda / Hope» ist ein Projekt, das die Verbindung zwischen Russland und dem restlichen Internet visualisieren soll. Diese Forschung ist Teil der Versuche Russlands, ein «souveränes Internet» zu schaffen, mit dem sich Russland vom Rest des Internets isolieren kann.

3. «Nautilus» ist ein Projekt, das zwischen 2009 und 2010 entwickelt wurde, um Informationen über Benutzer in sozialen Netzwerken wie «Facebook», «LinkedIn» und «MySpace» zu sammeln.

4. «Nautilus-S» ist eine Forschung zur De-Anonymisierung von Benutzern im Tor-Netzwerk durch die Schaffung von Ausgangsknoten, die von der russischen Regierung kontrolliert wurden.

Die Website für «Sytech» (www.sytech.ru) ist inzwischen deaktiviert worden, und das Unternehmen hat auf Anfragen der BBC nicht reagiert.

4.6 Crimeware

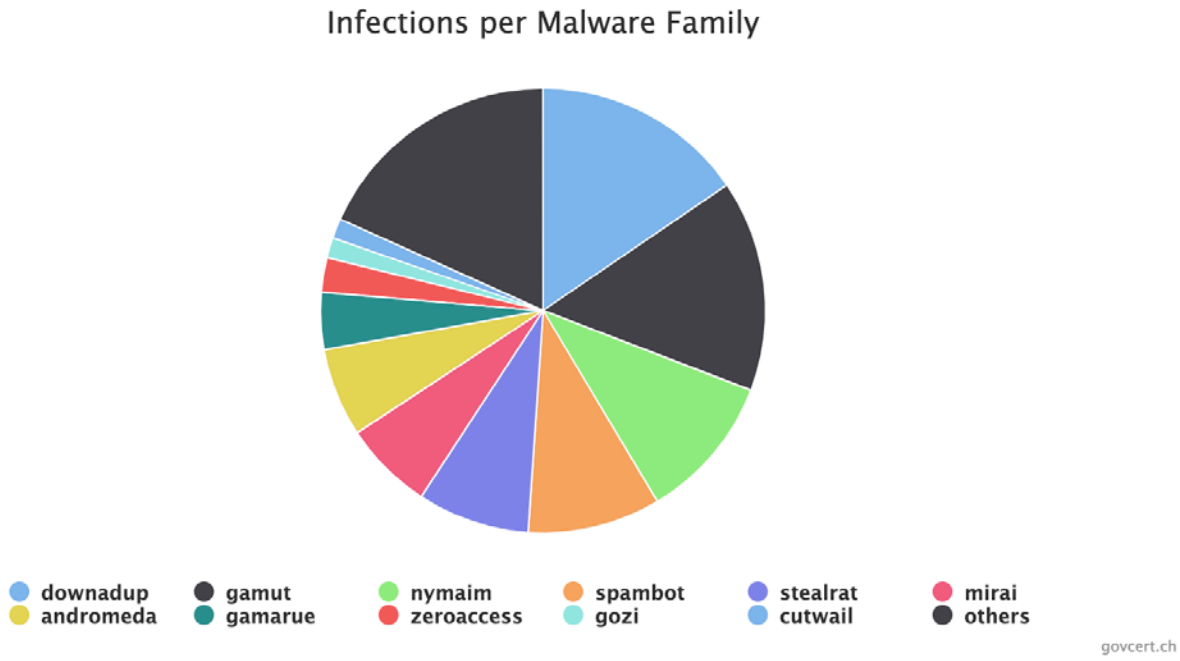

Abb. 5: Verteilung der Schadsoftware in der Schweiz, welche NCSC mit Hilfe von DNS Sinkholes bekannt ist. Stichtag 9. Februar 2020. Aktuelle Daten finden Sie unter: http://www.govcert.admin.ch/statistics/dronemap/

4.6.1 Ransomware: die jüngsten Entwicklungen

Stellen Sie sich vor, Sie wollen Tickets für das Spiel Ihrer Lieblingsmannschaft kaufen. Allerdings ist der Online-Vorverkauf gerade nicht verfügbar. Sie begeben sich deshalb guten Mutes an den Ticketschalter. Leider haben Sie kein Bargeld dabei, und das Kartenlesegerät funktioniert nicht. Der nächstgelegene Bankomat ist ein paar Kilometer entfernt, die Sie zu Fuss zurücklegen, weil auch keine Busse mehr fahren. All dies wegen einer Malware, die zu Erpressungszwecken verschiedene Computersysteme lahmgelegt hat.

Dieses Szenario ist nur teilweise erfunden: Tatsächlich ereignete sich im Berichtshalbjahr ein Angriff mit *Ransomware* auf einen Schweizer Fussballclub mit den oben ausgeführten Folgen auf das Ticket- und Zahlsystem.[58] Eine kleine Störung im öffentlichen Verkehr entstand ebenfalls infolge eines Hackerangriffs.[59] Das Szenario ist insoweit fiktiv, als die beiden Ereignisse nicht gleichzeitig und nicht in derselben Stadt stattgefunden haben.

Die starke und anhaltende Ransomware-Welle, die dazu führte, dass MELANI das Schwerpunktthema des letzten Halbjahresberichts dieser Bedrohung widmete, ist nicht abgeflacht. Auch in den letzten sechs Monaten waren sowohl auf nationaler wie auf internationaler Ebene zahlreiche Angriffe zu verzeichnen. Zudem waren neue Tendenzen erkennbar.

Der Gesundheitssektor war im zweiten Halbjahr 2019 international weiterhin stark betroffen. Im November waren die Offline-Computersysteme des Universitätsspitals Rouen in Frankreich von einer Ransomware betroffen, wodurch das Personal die Daten vorübergehend analog verarbeiten musste.[60] Einige Monate zuvor wurden in Deutschland die Server von 18 Spitälern verschlüsselt.[61] Der Blick nach Übersee enthüllt noch höhere Zahlen. Dort griff der Verschlüsselungstrojaner «Ryuk» das IT-Unternehmen «Virtual Care Provider Inc.» (VCPI) an, das Daten in der Cloud hostet und den Zugriff von über 100 Pflegeheimen in den USA sichert und verwaltet. Durch den Angriff wurde der Zugriff auf die Patientenakten verhindert.[62] «Ryuk» visiert vor allem Unternehmen und Organisationen mit grossem Umsatz an, um hohe Lösegelder zu erpressen. Unternehmen, die IT-Infrastrukturen von zahlreichen Kunden verwalten, sind ein strategisches Ziel, weil sie eine praktische Verbreitung der Infektion ermöglichen und sich als sehr lukrativ erweisen können. Im Oktober verschlüsselte «Ryuk» die Daten von 400 US-amerikanischen Tierspitälern der «National Veterinary Associates». Es scheint, dass die Infektion des *Active Directory* und eines *Exchange Server* bereits im Sommer stattgefunden hat. Da man die Infektion nicht vollständig beheben konnte, schlug sie wieder zu, nachdem sie Zeit gehabt hatte, sich erneut auszubreiten.[63] «Ryuk» wird oft nach einer vorangehenden Infektion durch die Trojaner «Emotet» oder «Trickbot» übertragen, was bei mindestens einem der erwähnten Angriffe der Fall war (zur Vertiefung der mehrstufigen Angriffsstruktur siehe MELANI-Halbjahresbericht 2019/1, Kapitel 3.4.1).

Aber nicht nur «Ryuk» verwendet eine Vorgehensweise mit mehreren Infektionsstufen. Diese anscheinend einträgliche Vorgehensweise häufte sich in jüngster Zeit. Ein in der Schweiz und international beobachteter *Dropper* ist «Ostap», der gewöhnlich den Trojaner «TrickBot» herunterlädt. Dieser verbreitet sich innerhalb eines Unternehmensnetzwerkes und platziert in ausgewählten Systemen eine Ransomware (zum Beispiel «Ryuk», «LockerGoga», «MegaCortex» usw.).

---

58 https://www.inside-it.ch/de/post/der-gehackte-fc-basel-und-die-konsequenzen-20191205

59 https://www.20min.ch/ro/news/romandie/story/Les-TPF-victimmes-d-une-attaque-informatique-23708264

60 https://www.silicon.co.uk/security/cyberwar/french-hospital-ransomware-attack-318031

61 https://www.spiegel.de/netzwelt/web/rheinland-pfalz-und-saarland-hackerangriff-auf-krankenhaeuser-a-1277759.html

62 https://krebsonsecurity.com/2019/11/110-nursing-homes-cut-off-from-health-records-in-ransomware-attack/

63 https://krebsonsecurity.com/2019/11/ransomware-bites-400-veterinary-hospitals/

Der Gesundheitssektor ist aber bei weitem nicht die einzige Zielscheibe. Es kann Unternehmen aller Branchen treffen. Ransomware-Angriffe erfolgen sowohl gezielt als auch zufällig.[64] Betroffen sind beispielsweise die Bereiche Industrie, Verkehr, öffentliche Verwaltung, Kommunikation und Sport. Kürzlich befiel die Ransomware «Ryuk» gezielt mindestens fünf Organisationen aus der Erdöl- und Gasindustrie. In mindestens einem Fall sollen die Angreifer über das *Remote Desktop Protocol (RDP)* in die *Active-Directory*-Server des Opfers eingedrungen sein.[65] Im zweiten Halbjahr 2019 stieg die Zahl der Ransomware-Angriffe, bei denen die Angreifer das Internet auf der Suche nach *VPN*-Servern und offenen *RDP-Ports* scannen und versuchen, mit *Brute-Force*-Angriffen Zugriff zu erhalten. Dieser Zugriff wird anschliessend als Initialvektor für die Infiltration eines Unternehmensnetzes verwendet. In der Schweiz wurden zum Beispiel die Malware «Dharma», «Phobos» und «Maze» beobachtet, wie sie offene oder schlecht gesicherte, im Internet sichtbare RDP-Zugänge ausnutzten.

Die Schwachstellen des RDP-Protokolls lassen sich nach erfolgter Infektion für die laterale Bewegung im System nutzen. Bereits im April 2018 identifizierte «FireEye» eine Verteilkampagne mit vorgetäuschten Aktualisierungen für verschiedene Browser (Chrome, Internet Explorer, Opera und Firefox), welche die Malware «Dridex», «NetSupport Manager RAT», «AZOrult» oder «Chthonic» übertrugen.[66] Nachdem diese Schadsoftware das Netzwerk ausspioniert, Anmeldeinformationen gestohlen und Rechte erworben hat, fungiert sie als Dropper für die Ransomware «BitPaymer» und «DoppelPaymer». Die Aktualisierungen tauchten auf infizierten Seiten auf, die potenzielle Opfer beispielsweise durch «http://»-Weiterleitungen erreichten. Im zweiten Halbjahr 2019 beobachtete MELANI für diesen Zweck kompromittierte Schweizer Websites.

Das Geschäftsmodell «Ransomware» basierte bis anhin rein auf dem Konzept «Datenentschlüsselung gegen Geld». Neuerdings exfiltrieren einige Angreifer-Gruppen[67] vor dem Verschlüsselungsangriff Daten, um dann durch deren teilweise Veröffentlichung ihre Täterschaft nachzuweisen, den Druck auf das Opfer zu erhöhen oder auch schlicht das Opfer mit der angedrohten Veröffentlichung zu erpressen – quasi als Rückfallebene, wenn die Erpressung mit der Datenverschlüsselung wegen erfolgreicher Datenwiederherstellung ins Leere läuft.[68] Im November 2019 beispielsweise hat die Maze-Gruppe fast 700 MB an Daten durchsickern lassen, die sie von einer Sicherheitsfirma gestohlen hatte.[69] Darauf folgten auch Daten weiterer Organisationen, die die Maze-Gruppe erpresst hatte, nämlich des medizinischen Diagnostiklabors «MDLab», des Draht- und Kabelhersteller «Southwire» und einer Kleinstadt in Florida.[70] Die hinter dieser Ransomware steckende Gruppe ist auch in der Schweiz aktiv.

---

64 Siehe Schwerpunktthema im MELANI Halbjahresbericht 2019/1, Kap. 3.

65 https://www.darkreading.com/threat-intelligence/ryuk-ransomware-hit-multiple-oil-and-gas-facilities-ics-security-expert-says-/d/d-id/1336865

66 https://www.fireeye.com/blog/threat-research/2019/10/head-fake-tackling-disruptive-ransomware-attacks.html

67 Z. B. «Maze», «Sodinokibi» und «Doppel Paymer».

68 https://www.bleepingcomputer.com/news/security/new-megacortex-ransomware-changes-windows-passwords-threatens-to-publish-data/; https://www.bleepingcomputer.com/news/security/maze-ransomware-not-getting-paid-leaks-data-left-and-right/

69 https://www.bleepingcomputer.com/news/security/allied-universal-breached-by-maze-ransomware-stolen-data-leaked/

70 https://www.bleepingcomputer.com/tag/maze/

Ein Ransomware-Angriff, der zum Datenabfluss wird, wenn das Lösegeld nicht bezahlt wird, scheint ein profitables Geschäftsmodell zu sein. Die Betreiber des Verschlüsselungstrojaners «REvil», der auch unter dem Namen «Sodinokibi» bekannt ist, haben angekündigt, auf dieses Geschäftsmodell umzusteigen.[71]

Aufgrund dieser Entwicklung birgt jeder Ransomware-Vorfall das Risiko eines potenziellen Datenlecks. Dieses Risiko bleibt auch nach der Bewältigung des Vorfalls bestehen. Je nach Wert der Daten und Informationen ist damit zu rechnen, dass die Kriminellen diese in Zukunft ebenfalls zu ihren Gunsten verwerten werden. Somit dürften auch Unternehmen, welche relevante personenbezogenen Daten bearbeiten, vermehrt in den Fokus der Hacker gelangen.

Empfehlungen:

Innerhalb des Unternehmens haben sich folgende Massnahmen bewährt: Achten Sie auf vollständige Datensicherungspraktiken, um die Sicherheit zu erhöhen, nach einer Ransomware-Attacke sämtliche Daten wieder herstellen zu können. Dazu gehört auch das Testen des Wiederherstellungsprozesses von Daten. Dokumentieren Sie Ihre IT-Infrastruktur, spielen Sie Software-Updates zeitnah nach Erscheinen ein und halten Sie die Sicherheitsrichtlinien auf dem neusten Stand. Erstellen Sie Konzepte für die Vorfallsbewältigung, für die Kommunikation sowie für das Business Continuity Management. Ermitteln Sie anhand regelmässiger Übungen die Wirksamkeit dieser Konzepte. Für eine effektive Prävention gegen Cyberangriffe sollten technische Sicherheitsmassnahmen mit regelmässiger Sensibilisierung der Mitarbeitenden einhergehen. Es ist eine nicht delegierbare Aufgabe der Führungsorgane eines Unternehmens, über die Umsetzung dieser Massnahmen zu wachen.

Kaum ein Unternehmen ist in der Lage, jeden Cyberangriff mit Sicherheit abzuwehren. Bauen Sie deshalb Reaktions- und Wiederherstellungsfähigkeiten auf, um die Auswirkungen eines nicht vermeidbaren Vorfalls zu mildern.

INFO

Im zweiten Halbjahr 2019 veröffentlichte MELANI aktualisierte Sicherheitsmassnahmen für den Schutz gegen die neue Vorgehensweise bei Ransomware-Angriffen:

https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/update-ransomware-neue-vorgehensweise.html

Achtung: Im Fall von Mehrphaseninfektionen genügt die Wiederherstellung der Daten aus dem Backup nicht! Lassen Sie das Netzwerk bereinigen und nehmen Sie eine Neuinstallation der infizierten Systeme vor, um den Dropper sicher zu beseitigen.

4.6.2 «Emotet» bleibt grösste Infektions-Bedrohung

Auch im zweiten Halbjahr 2019 war «Emotet» in der Schweiz sehr aktiv. Nach einer leichten Entspannung im Juni meldete sich die Gruppe im August in voller Stärke mit zahlreichen Verbreitungsaktivitäten und entsprechend vielen Opfern in der Schweiz zurück.

Die Vorgehensweise ist in diesem Halbjahr ähnlich geblieben: Der Trojaner greift weiterhin Inhalte aus vorgängigen E-Mail-Konversationen ab, generiert daraus neue Nachrichten und

71 https://www.bleepingcomputer.com/news/security/another-ransomware-will-now-publish-victims-data-if-not-paid/

schickt diese an die in den Verteilerlisten aufgeführten Empfänger. Die Mails enthalten einen schädlichen Anhang – oft ein Word-Dokument, das mit einem Makro versehen ist. Sobald das Opfer das Dokument öffnet und in den Bearbeitungsmodus wechselt, wird die Malware ausgeführt. Ohne zusätzliche Schutzmassnahmen lädt «Emotet» weitere Module herunter und stellt im Rechner des Opfers Persistenz her.[72]

Die Gruppe hat ihre Vorgehensweise perfektioniert und verkauft Zugänge zu Netzwerken und Systemen an andere Akteure weiter. Damit ist «Emotet» zu einem Schlüsselakteur der organisierten Cyberkriminalität geworden. Auch staatsnahe Gruppen tummeln sich auf dem Untergrundmarkt und sind am Erwerb von Zugängen zu kompromittierten Systemen interessiert, die sie zu Spionagezwecken oder für finanziellen Gewinn nutzen können.

Empfehlungen:

Es gilt nicht mehr nur bei E-Mails von unbekannten Personen kritisch zu sein, sondern auch bei bekannten Absendern Vorsicht walten zu lassen, insbesondere wenn ein unerwartetes E-Mail auf eine alte Konversation zurückgreift. Besonders vertrauenswürdige Firmen werden gerne als gefälschte Absenderadressen missbraucht. Fragen Sie im Zweifelsfall beim vermeintlichen Absender über eine bereits bekannte oder z. B. auf seiner Webseite angegebene Kontaktmöglichkeit nach, worum es sich genau handelt und ob das Mail tatsächlich von ihm stammt.

Seien Sie besonders vorsichtig, wenn Sie Word-Dokumente erhalten. Normalerweise versenden Firmen und Organisationen im Geschäftsverkehr (beispielsweise Rechnungen, Of-

Unternehmen sollten jene Webseiten, welche aktiv für die Verbreitung von Emotet verwendet werden, am Netzwerkperimeter wie beispielsweise auf dem Web-Proxy oder DNS sperren. Eine Liste von solchen Webseiten wird u. a. von abuse.ch zur Verfügung gestellt.

4.7 Schwachstellen

Fehler bei der Software-Entwicklung lassen Schwachstellen entstehen. Deshalb sind «Life Cycle-» und «Patch-Management» von zentraler Bedeutung. Jede Firma (unabhängig davon, ob KMU oder Grosskonzern), muss für all ihre Systeme und Anwendungen ein Inventar führen und mit einem Plan festlegen, was wann gepatched werden muss und welche Software zu welchem Zeitpunkt das Ende ihres Lebenszyklus erreicht. Dies gilt auch für hardwarenahe Komponenten wie z. B. Firmware oder Management Boards. Ausserdem sollte bei der Software-Entwicklung ein Augenmerk auf Verwundbarkeiten der verwendeten *Frameworks* und deren Abhängigkeiten gelegt werden.

Besonders heikel sind Lücken, welche von Remote über das Netz ohne Authentisierung ausgenützt werden können, wie z. B. die Lücke in *SMB* («EternalBlue»[73]), *RDP* («BlueKeep»[74],

[72] Siehe MELANI Halbjahresbericht 2019/1, Kap. 3.4.1 und 4.6 sowie technischer Anhang anbei.

[73] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144

[74] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0708

«BlueGate»[75, 76]), in «Citrix Netscaler»[77] und «Oracle Weblogic»[78]. Solange eine Lücke nicht bekannt ist («0-Day Exploit»), hat sie einen hohen Wert und wird meist nur bei gezielten Angriffen eingesetzt. Sobald die Lücke bekannt wird und Patches vorhanden sind, werden die Patches analysiert und so die Lücke bestimmt, welche bei ungepatchten Systemen noch offensteht. Mit dieser Information werden dann «Exploit Codes» geschrieben. Sobald ein öffentlich verfügbarer «Exploit Code» vorliegt, wird dieser in den Werkzeugkasten von den meisten kriminellen und/oder staatlichen Akteuren einfliessen und entsprechend häufig verwendet. Spätestens zu diesem Zeitpunkt sind Systeme, welche von aussen erreichbar sind und die Lücke enthalten, als kompromittiert zu betrachten. Webanwendungen und *CMS* mit ihren verschiedenen *Plugins* werden besonders häufig angegriffen und benötigen entsprechende Sicherungsmassnahmen (siehe auch «Massnahmen zum Schutz von Content Management Systemen CMS»[79]). Während das Patching von üblichen Informatiksystemen und -anwendungen relativ einfach möglich ist, gestaltet sich dies im Bereich von Steuerungssystemen, IoT-Geräten oder medizinischen Ausrüstungen als wesentlich schwieriger. Eine Lücke in «VxWorks», einem Echtzeit Betriebssystem, welches sehr oft in Steuerungssystemen, aber auch in Medizinalgeräten zum Einsatz kommt, wurde im September 2019 entdeckt[80] und exponiert eine Vielzahl von teilweise sehr schwierig zu aktualisierenden Geräten.

Das Ausnutzen von Lücken kann verschiedenen Zwecken dienen:

1. Datendiebstahl mit dem Ziel der Industriespionage oder der Erpressung
2. Verteilung von Ransomware
3. Übernahme eines Systems mit dem Ziel, Kryptowährungen zu schürfen
4. Versand von Malware oder Spam
5. Angriffspunkt für das weitere Vordringen in ein Netzwerk

75 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0610
76 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0609
77 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19781
78 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-2546
79 https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/massnahmen-zum-schutz-von-content-management-systemen--cms-.html
80 https://go.armis.com/urgent11

Empfehlungen:

Um eine gleichbleibende Sicherheit zu haben, benötigt eine Firma ein gutes «Life Cycle-» und «Patch-Management» über alle eingesetzten Komponenten hinweg. Dies betrifft nicht nur die üblichen Büroautomationssysteme, sondern auch Webanwendungen, mobile Geräte, IoT-Devices oder Steuerungskomponenten. Ein grosses Augenmerk ist dabei auch auf verwendete Frameworks und Software-Bibliotheken zu werfen.

Für den Fall kritischer Verwundbarkeiten, welche nicht sofort geschlossen werden, braucht es Ausweichlösungen (z. B. einen zweiten Webbrowser) oder Möglichkeiten zur Isolierung oder temporären Beseitigung der Schwachstelle (z. B. bei Webanwendungen eine Web Application Firewall).

Remote Access-Lösungen wie *VPN Gateways*, *Web Application Gateways*, E-Mail Webaccess oder exponierte Terminalservices gehören zu den interessantesten Zielen für Angreifer, da sie einen direkten Zugriff auf interne Ressourcen ermöglichen. Diese benötigen nebst dem Life Cycle- und Patch-Management in jedem Fall zusätzliche Sicherheitsmassnahmen wie z. B. eine Zwei-Faktor-Authentisierung, ein *Hardening* und eine zentralisierte Logauswertung.

Wer selbst Anwendungen, Systeme, Steuerungen oder IoT-Devices entwickelt, benötigt ebenfalls ein klar kommuniziertes Life Cycle- und Patch-Management sowie entsprechende Informationskanäle zu den Kunden. Es ist auch wichtig, einen einfach zu findenden Kontaktkanal bereitzustellen, über den *Security Researcher* Lücken melden können. Ein *«Bug Bounty»*-Programm ist eine prüfenswerte Ergänzung und kann dabei helfen, dass Lücken frühzeitig gemeldet und koordiniert behoben werden.

4.8 Präventive Massnahmen

4.8.1 Neuer Minimalstandard in der Lebensmittelversorgung

Das Bundesamt für Wirtschaftliche Landesversorgung (BWL) hat in den letzten Monaten einige Minimalstandards zur Sicherheit von Informatik- und Telekommunikationssystemen (IKT) für verschiedene Branchen veröffentlicht, da die Produktions- und Geschäftsprozesse in zunehmendem Masse abhängig von der IKT sind. Ein Ausfall dieser Systeme gefährdet die Geschäftstätigkeit von Unternehmen und die Versorgung der Schweiz mit kritischen Gütern und Dienstleistungen. Zum Schutz gegen Risiken in Zusammenhang mit der IKT und zur Sicherstellung der Versorgung der Bevölkerung mit Nahrungsmitteln hat das BWL vor Kurzem einen Minimalstandard für die IKT-Sicherheit in der Lebensmittelversorgung herausgegeben. Er soll Unternehmen aus der Lebensmittelbranche dabei unterstützen, IKT-Störungen zu vermeiden beziehungsweise diese rasch beheben zu können.

Diese Empfehlung folgt auf die bereits publizierten Minimalstandards für die IKT-Sicherheit in der Wasserversorgung und dem Handbuch für den Grundschutz von «Operational Technology» in der Stromversorgung. Diese Branchenstandards werden ergänzt durch den allgemeinen IKT-Minimalstandard, welcher aus den Verwundbarkeitsanalysen zu Cyberrisiken in ver-

schiedenen, für das Funktionieren der Schweiz wichtigen, Branchen resultierte. Diese Verwundbarkeitsanalysen hat das BWL im Rahmen der «Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken» (NCS) durchgeführt.[81]

4.8.2 Schweizer Polizei sperrt fiktive Onlineshops

Der Einkauf im Internet ist bequem – aber nicht frei von Risiken. Die Käuferinnen und Käufer laufen Gefahr, scheinbar gekaufte Artikel nach der Zahlung nicht zu erhalten oder gefälschte Ware zu bekommen. Zusätzlich zum Diebstahl besteht die Gefahr, dass die von den Käufern kommunizierten Daten für weitere Delikte verwendet werden.

Fiktive Onlineshops haben auch die Schweiz erfasst: Cyberkriminelle registrieren auch betrügerische Seiten mit der Domainendung «.ch». Zu bestimmten Jahreszeiten, beispielsweise vor Weihnachten, steigt diese Aktivität exponentiell.

Die «Abteilung Cybercrime» der Kantonspolizei Zürich verfolgt in Zusammenarbeit mit SWITCH, der Schweizer Registrierungsstelle von «.ch»-Internet-Online-Adressen (Domains), betrügerische Onlineshops mit Schweizer Internet-Domains. Im Dezember 2019 führte diese Zusammenarbeit zu einer Aktion, bei der 450 fiktive Onlineshops kurz nach ihrer Aufschaltung gesperrt wurden. Seit Anfang 2018 identifizierte und sperrte die Kantonspolizei Zürich insgesamt über 6'500 solcher Onlineshops.

Diese Massnahme reduzierte nicht nur die Zahl dieser fiktiven Shops, sondern führte auch zum drastischen Rückgang neu entstehender betrügerischer Shops mit Schweizer Internet-Domains. Dies bestätigt die Zürcher Kantonspolizei auf ihrer Website.[82] Ausserdem erklärt die Abteilung Cybercrime auf ihrer Website, welche Aspekte zu beachten sind, um solche Fallen zu vermeiden. Dazu gehören namentlich Domainnamen, die nichts mit der angebotenen Ware zu tun haben, das Fehlen des Schlosssymbols, das eine verschlüsselte Verbindung zur Website anzeigt, und das Fehlen des gesetzlich vorgeschriebenen Impressums.[83]

4.8.3 Internationale Operation zerschlägt die Infrastruktur eines «RAT as a Service»

MELANI hat wiederholt auf die nunmehr weit verbreitete Praktik des Anbietens von Cyberangriffen oder von Hilfsmitteln zu deren Ausführung hingewiesen.[84] Die Verfolgung solcher Vergehen ist alles andere als einfach. Zur Schwierigkeit der Identifizierung eines Cyberkriminellen kommt ein weiteres Hindernis: Der Grat zwischen Legalität und Illegalität ist schmal und nicht immer eindeutig erkennbar. Dies mag erklären, wie es möglich war, dass der Softwareentwickler «Shockwave™» seit 2012 ungestört das Fernzugriffstool (*Remote Administration Tool, RAT*) «Imminent Monitor» online verkaufen konnte, bevor im November 2019 eine internationale Operation mehrerer Strafverfolgungsbehörden die Infrastruktur unschädlich machte.

Der Autor distanzierte sich auf der Website, auf der er sein Produkt verkaufte, von Personen, die dieses für illegale Zwecke verwenden wollten und lehnte jegliche Verantwortung ab. Beim

---

81 https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-75891.html

82 https://www.kapo.zh.ch/internet/sicherheitsdirektion/kapo/de/aktuell/medienmitteilungen/2019_12/1912161f.html

83 https://www.cybercrimepolice.ch/de/fall/betruegerische-internetshops-vorsicht-bei-der-online-schnaeppchenjagd/

84 MELANI Halbjahresberichte 2009/2, Kap. 4.7; 2016/2, Kap. 6.1 und 2019/1, Kap. 3.3.

Kauf musste eine Erklärung abgegeben werden, dass die Dienstleistung nicht für das Verteilen von Malware genutzt wird. Das Produkt verfügte jedoch über eine Reihe von Funktionen, die für ein legales Fernzugriffsprodukt atypisch und überflüssig sind. Es ermöglichte beispielsweise die Deaktivierung der Antivirus-Software, verfügte über Eigenschaften, die eine Erkennung erschwerten, bot Zugriff auf den Remote Desktop, der dem Opfer verborgen blieb und ermöglichte sogar das Schürfen von Kryptowährungen auf dem Rechner des Opfers.

Das Basisprodukt kostete nur 25 US-Dollar und war so für alle zugänglich. Laut den Behörden wurde das Produkt tatsächlich von über 14'500 Kriminellen gekauft, die es in 124 Ländern gegen zehntausendende Opfer verwendeten.

Die Operation wurde gemeinsam von der australischen Bundespolizei (AFP), Europol, Eurojust, dem FBI und zahlreichen weiteren Strafverfolgungs- und Polizeibehörden durchgeführt und mündete in der Sicherstellung von 430 Geräten sowie der Verhaftung von 13 Nutzerinnen und Nutzern, die das Produkt illegal verwendeten.[85]

4.8.4 «Bug Bounty» Programme – Kopfgeldjagd im Internet

Um Hackern Anreize und eine Möglichkeit zu bieten, entdeckte Schwachstellen zu melden, haben sich in der Vergangenheit immer mehr «*Bug Bounty*»-Programme etabliert. Dabei handelt es sich um Plattformen, die Prämien für verifizierbare Schwachstellen vergeben. Dabei gibt es verschiedene Ansätze für ein «Bug Bounty»-Programm. Kommerzielle Plattformen vermitteln zwischen dem Hacker und dem Unternehmen und geben für beide Seiten die Regeln vor. Einigen Plattformen liegt auch ein nicht-kommerzieller Ansatz zu Grunde. Diese sind typischerweise kostenlos und Community-basiert, jedoch findet keine institutionalisierte Mittler-Funktion zwischen den Parteien statt. Solche Projekte bieten Sicherheitsexperten eine Plattform, Schwachstellen in beliebigen Webseiten zu melden. Aus Sicht der Unternehmen besteht die Möglichkeit, ein «Bug Bounty»-Programm für neu einzuführende Software zu starten, also nur punktuell, oder ein ständiges Bug Bounty-Programm einzuführen. Dazu kann die Dienstleistung eines kommerziellen Anbieters in Anspruch genommen oder ein firmeneigenes «Bug Bounty»-Programm aufgebaut werden. Auch einzelne Staaten[86] haben Regeln im Umgang mit Schwachstellen entwickelt.

Seit Jahren wird debattiert, wie Hacker mit entdeckten Lücken umgehen sollten, um der Öffentlichkeit zu nutzen und Unternehmen nicht zu schaden. Zwei Wege haben sich mittlerweile etabliert: «full disclosure» und «responsible disclosure». Beim «full disclosure», also der kompletten Offenlegung, informiert der Hacker das Unternehmen und die Öffentlichkeit gleichzeitig. Das Unternehmen wird so unter Druck gesetzt, da die Lücke ab Bekanntwerden von jedem missbraucht werden kann. Und dies ist denn auch der Kritikpunkt an diesem Weg. Beim «responsible disclosure», also der verantwortungsvollen Enthüllung, informiert der Hacker zuerst nur das Unternehmen, das so Zeit bekommt (üblich sind 60 bis 120 Tage), das Problem zu beheben. Erst danach publiziert der Hacker die Schwachstelle.[87]

---

85 https://securityaffairs.co/wordpress/94525/cyber-crime/imminent-monitor-rat-shutdown.html
https://unit42.paloaltonetworks.com/imminent-monitor-a-rat-down-under/

86 Z.B. die Niederlande: https://www.government.nl/topics/cybercrime/fighting-cybercrime-in-the-netherlands/responsible-disclosure

87 https://www.zeit.de/digital/datenschutz/2013-09/bug-bounty-hack/seite-2

Grundsätzlich gilt für die Teilnahme an «Bug Bounty»-Programmen das Prinzip des «responsible disclosure». Dazu gehören folgende Elemente:

1. Das Unternehmen hat ausreichend Zeit (üblich sind 60 bis 120 Tage), die Schwachstelle zu verifizieren und zu beheben.
2. Drittparteien dürfen nicht über die Schwachstelle informiert werden.
3. Tests zu den Schwachstellen dürfen die Dienstleistungen, Produkte und den Regelbetrieb des Unternehmens nicht beeinträchtigen.
4. Daten dürfen weder ausgespäht noch weitergegeben werden.
5. Forderungen (vor allem finanzieller Art) im Zusammenhang mit der Meldung einer Schwachstelle werden nicht berücksichtigt.

Künftig wird diese Praxis wohl vermehrt von Firmen angewendet werden, so dass für qualifizierte Kopfgeldjäger und Security-Forscher im Internet die Zukunft rosig aussieht.[88] Bestehende «Bug Bounty»-Programme wie jenes der Swisscom beeindrucken mit beachtlichen Zahlen: Das Telekommunikationsunternehmen erhielt und bearbeitete 844 Schwachstellenberichte. Davon führten 427 Berichte zu einer Korrektur, und die Swisscom zahlte Prämien in der Höhe von CHF 350'000.- aus. Die Art der gemeldeten Schwachstellen reichen von *Low-Level-Cross-Site-Scripting* (XSS) bis hin zu hochkritischen *0-Days* in bekannten und weit verbreiteten Produkten.[89]

Jüngst haben Hacktivisten eine neue Form eines «Bug Bounty»-Programms lanciert, um Selbstjustiz-Hacker und Hacktivisten zu belohnen, die im Namen des öffentlichen Interesses Hacks und Datenlecks durchführen. Dies hat nur den Namen gemeinsam mit den traditionellen Programmen, bei denen es darum geht, einen wichtigen Beitrag zur Sicherheit zu leisten sowie Lücken in Sicherheitssystemen zu identifizieren und zu beheben, bevor diese ausgenutzt werden.

Das Nationale Zentrum für Cybersicherheit (NCSC) ist dabei, eine «Responsible Disclosure Policy» für die Schweiz zu erarbeiten.

MELDEN

Erkenntnisse zu Schwachstellen können bereits jetzt an

incidents@ncsc.ch

gemeldet werden.

88 https://www.swisscyberstorm.com/2019/11/26/some-background-on-switzerlands-biggest-bug-bounty-program/

89 Zahlen ab 2018, https://www.swisscyberstorm.com/2019/11/26/some-background-on-switzerlands-biggest-bug-bounty-program/

5 Forschung und Entwicklung

5.1 Wenn nichts mehr geht – Ransomware und jetzt?

Über das Vorgehen krimineller Gruppen, mit verschlüsselten Daten Geld zu erpressen, wurde in den MELANI-Halbjahresberichten schon einige Male berichtet.[90] Entsprechende technische Hilfsdokumente, wie man sich am besten vor solchen Ransomware-Angriffen schützen kann, sind auf der MELANI-Website verfügbar.[91]

Aber selbst die besten technischen Vorkehrungen schützen nicht zu hundert Prozent vor einer Infektion. Das Jahr 2019 sah eine Professionalisierung, speziell bei Gruppen, die sich auf das Geschäftsmodell «Ransomware» konzentrieren. Es wird nicht mehr einfach eine Verschlüsselung der lokal und über Netzwerkzugriffe gerade verfügbaren Daten ausgeführt, nachdem man die vermeintliche Telefonrechnung oder Bewerbungsunterlagen geöffnet hat. Vielmehr bewegen sich die Angreifer nach einer Erstinfektion mit einem *Trojaner* zuerst über längere Zeit innerhalb des Opfernetzwerkes, um sich möglichst Zugriff auf alle neuralgischen Systeme und Punkte zu verschaffen, inklusive der Online-Backups. Dies garantiert eine Maximierung des Schadens zum Zeitpunkt, wenn die eigentliche Verschlüsselungs-Software zuschlägt.

Dieses mehrstufige Vorgehen erlaubt es auf Seiten der IKT-Sicherheit unter Umständen die Angreifer zu entdecken und abzuwehren, bevor grösserer Schaden entsteht. MELANI wird immer wieder von Sicherheitsunternehmen und Partnerorganisationen über Infektionen von Unternehmensnetzen informiert und leitet diese auch an die betroffenen Netzbetreiber weiter. Auf der anderen Seite hat das mehrstufige Vorgehen verheerende Folgen, wenn die eigentliche Ransomware vom Angreifer aktiviert wird und neben neuralgischen Systemen beim primär infizierten Betrieb selbst produzierende Einheiten im Ausland auf einen Schlag stillstehen, weil sie über die Unternehmenszentrale netzwerktechnisch verbunden waren.

5.1.1 Erfolgreiche Ransomware ist kein IKT-Problem

Das Geschäftsmodell von Ransomware-Gruppen besteht darin, den grösstmöglichen Druck auf betroffene Unternehmen und Organisationen aufzubauen, um ihren Forderungen nach Bezahlung Nachdruck zu verleihen. Entsprechend zielen diese Gruppen auf einen Stillstand der IKT-gestützten Geschäftsprozesse ab. Auch wenn damit die IKT Ursache des Problems ist, sind ihr typischerweise die Hände gebunden, was die schnelle Lösung des eigentlichen Problems betrifft: Die Wiederinstandsetzung der kritischsten Geschäftsprozesse und -abläufe und die Aktivierung eines hoffentlich vorgängig durch das Management erstellten Business Continuity-Planes.

Nach einem erfolgreichen Ransomware-Angriff sind möglichst rasch jene Systeme und Prozesse zu identifizieren, die nicht vom Angriff betroffen waren, respektive jene, die auch ohne IKT-Unterstützung betrieben werden können.

---

90 MELANI Halbjahresberichte 2011/2, Kap. 3.5; 2013/2, Kap. 3.1; 2014/2, Kap. 3.6 und 5.3; 2015/1, Kap. 4.6.1.5; 2015/2, Kap. 4.5.1, 2016/1, Kap. 4.6.3 und 5.4.3; 2016/2, Kap. 6.1; 2017/1, Kap. 3; 2017/2, Kap. 5.4.2; 2018/2, Kap. 4.5.4 und 5.3.5; 2019/1, Kap. 3.

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

Der Einbezug von Juristen ist dabei von Beginn an notwendig, da in jedem Falle die Angreifer zumindest für einen kurzen Zeitraum Zugriff auf Daten hatten. Dementsprechend greifen die Regeln des Datenschutzgesetzes sowie der Datenschutz-Grundverordnung (DSGVO), sofern das Unternehmen auch in der EU Geschäfte tätigt. In einem zeitnahen zweiten Schritt ist festzustellen, was sich an IKT-Systemen auf Grund noch vorhandener Backups und Snapshots überhaupt wiederherstellen lässt. Typischerweise ist hier der Einbezug eines externen IKT-Sicherheitsdienstleisters ratsam, da diese mit ihrer Erfahrung bei Ransomware-Vorfällen relativ effizient eine Einschätzung zum eigentlichen Ausmass und verbleibende Handlungsoptionen machen können.

Liegen nach den ersten beiden Schritten die benötigten Fakten vor, wird sich jedes Management als dritten Schritt aufgrund des Ausmasses und den damit involvierten Kosten die Frage stellen müssen, ob auf die Forderungen der kriminellen Gruppen einzutreten ist. MELANI rät dringend davon ab, Lösegelder zu bezahlen, da dadurch das Geschäftsmodell der Ransomware-Gruppe bestätigt und finanziell unterstützt wird. Zudem ist nicht garantiert, dass die Kriminellen ihren Teil der Abmachung einhalten. Wichtig ist, dass betroffene Unternehmen unverzüglich mit der Kantonspolizei Kontakt aufnehmen, um Anzeige zu erstatten und das weitere Vorgehen zu besprechen.

5.1.2 Strafverfolgung – Mehr als nur Handschellen

Die Vorfallbewältigung führt nach den internen Sofortmassnahmen dann zu einem gerne unterschätzten, aber unabdingbaren vierten Schritt, unabhängig davon ob sich das Opfer zu einer Zahlung entscheidet oder nicht: Der Einbezug der Strafverfolgung.

Landläufig sehen Unternehmen davon ab, die Strafverfolgung bei Ransomware-Fällen einzubeziehen. Die Volksmeinung ist, dass die Polizei nichts gegen ausländische kriminelle Cybergruppen ausrichten kann. Die Strafverfolgung verfügt sehr wohl über Erfahrung mit solchen Vorfällen und ermittelt auf internationaler Ebene gegen Ransomware-Gruppen. Sollte sich ein Unternehmen dennoch zur Zahlung von Lösegeld entschliessen, verfügt die Polizei über entsprechend geschulte Mitarbeitende, um mit der Täterschaft in Kontakt zu treten.

Ein Gang zur Strafverfolgungsbehörde zahlt sich daher mehrfach aus. Er erlaubt ihr, Beweismittel zu erheben, um nicht nur den vorliegenden Fall zu bearbeiten, sondern auch bereits angestossene Verfahren aus anderen Fällen zu unterstützen und Ermittlungen zusammenzuführen. Sie fungiert dabei auch als de facto eigenes Kompetenzzentrum im Umgang mit Ransomware-Fällen. Sie kann beratend zur Seite stehen. Je nach Ransomware-Gruppe verfügt sie auch über Wissen, das den für die Wiederinstandsetzung verantwortlichen Mitarbeitenden und externen Leistungserbringern zu Gute kommen kann.

5.1.3 Plan B wie BCM

Im Jahr 2019 wurde speziell der Werkplatz Schweiz Ziel von Ransomware-Angriffen. Die Logik dahinter ist einfach. Wer nicht produzieren kann, ist zur Bezahlung eines hohen Lösegelds bereit, um nicht tagelange Betriebsausfälle zu riskieren. Dies ist nachvollziehbar. Der initiale Effekt der Nachricht, es stehe infolge einer Ransomware-Attacke alles still, wurde von einem Unternehmer auch schon als «*Near Death Experience*» beschrieben.

Ransomware greift die Verfügbarkeit von Prozessen an und unterscheidet sich so gesehen nur unwesentlich von Angriffen auf die Verfügbarkeit von Webshops (DDoS-Angriffe). Im Idealfall soll das Unternehmen still stehen und zur Zahlung bereit sein, um den Betrieb wieder

aufnehmen zu können. Stark von der IKT abhängige Betriebe werden somit hart getroffen. Deshalb zielen diese Angriffe entsprechend darauf ab, als erstes die IKT auszuschalten.

Eine Aufgabe der Geschäftsleitung jedes Unternehmens und jeder Organisation ist es, dafür zu sorgen, dass notfalls die kritischen Geschäftsprozesse auch unabhängig von der IKT-Abteilung weitergeführt werden können. Das so genannten Business Continuity Management (BCM) muss zwingend vor einem Cyberangriff etabliert sein.

5.2 Eskalierende Konflikte im Nahen Osten bedrohen auch Geschäftspartner in der Schweiz

Organisationen mit Geschäftsbeziehungen in den Nahen Osten können Gefahr laufen, als Sprungbrett für Angriffe gegen Ziele mit Bezug zu den andauernden Konflikten missbraucht zu werden.

Neben den offen ausgetragenen Konflikten in Syrien und in Jemen ist der nahe Osten aus Sicht der Informationssicherheit seit längerem eine risikobehaftete Region. So ist das Überwachungsregime der regionalen Regierungen einiges rigoroser, als es die meisten europäischen Staaten handhaben. Im vergangenen Jahr berichtete «Reuters»[92] über das «Project Raven», in welchem Veteranen der amerikanischen Nachrichtendienste den Vereinigten Arabischen Emiraten beim Aufbau ihrer offensiven Cyberkapazitäten halfen. «Project Raven» wurde später gemäss der Nachrichtenagentur in die Firma «DarkMatter» überführt. Das Königreich Saudi-Arabien machte Schlagzeilen mit dem Einsatz von GovWare im Vorfeld der Ermordung des Journalisten Khashoggi[93] sowie mutmasslich gegen den «Amazon»-Gründer und «Washington Post» Eigentümer Jeff Bezos.[94] Anderweitig antworteten die israelischen Streitkräfte mit einem Luftangriff gegen ein Gebäude, von welchem aus die palästinensische Hamas gemäss israelischer Mitteilung Cyberangriffe gegen sie durchführten.[95]

In diesem aufgeladenen Umfeld haben involvierte Regierungen und privatwirtschaftliche Unternehmen, speziell Betreiber kritischer Infrastrukturen, in den vergangenen Jahren laufend in ihr Informationssicherheitsdispositiv investiert. Diese gehärteten Organisationen stellen ein immer schwerer einnehmbares Ziel dar, weshalb die Angreifer begannen, nach Gelegenheiten entlang der Zuliefererkette in Europa[96, 97] und Nordamerika[98] zu suchen. Neben Zulieferern im industriellen Umfeld[99] sind speziell auch IKT-Dienstleister[100] ein lohnendes Zwischenziel, um von dort den eigentlichen Angriff gegen die feindliche Institution zu starten.

---

92 https://www.reuters.com/investigates/special-report/usa-spying-raven/

93 https://citizenlab.ca/2019/04/dubious-denials-scripted-spin-spyware-company-nso-group-goes-on-60-minutes/

94 https://techcrunch.com/2020/01/22/bezos-nso-group-hack/

95 https://www.zdnet.com/article/in-a-first-israel-responds-to-hamas-hackers-with-an-air-strike/

96 MELANI Halbjahresbericht 2018/2, Kap. 5.2.2.

97 https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/shamoon-attackers-employ-new-tool-kit-to-wipe-infected-systems/

98 https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage

99 https://www.wired.com/story/iran-apt33-industrial-control-systems/

100 https://www.symantec.com/blogs/threat-intelligence/tortoiseshell-apt-supply-chain

Weil in naher Zukunft keine Beruhigung im Nahen Osten zu erwarten ist, sollten sich Schweizer Organisationen mit Beziehungen in den Nahen Osten mit dem Risiko eines Cyberangriffs aus dieser Region auseinandersetzen. Dabei spielt es keine Rolle ob man als Lieferant, Dienstleister oder nur schon als Geschäftspartner einer Organisation, die daneben auch einen Bezug in die Konfliktregionen hat, auf den Radar der Angreifer gerät. Gruppierungen wie «APT33»[101], «Oilrig»[102], «Muddywater»[103], «Leafminer»[104] oder «APT39/Chafer»[105] usw. scheuen keinen Aufwand, ein passendes Einfallstor für ihre Operationen zu finden.

In den referenzierten Beschreibungen der Gruppierungen im «MITRE ATT&CK»[106] Wissenskatalog zu Methoden und Techniken der Angreifer finden sich sowohl eingesetzte Angriffsmethoden, wie auch passende Mitigations-Massnahmen. Eine saubere Implementierung und konsequente Anwendung von Mehr-Faktor-Authentisierung verhindert viele Angriffe dieser Art oder erschwert sie zumindest erheblich.

5.3 Neue Geschäftsmodelle, um noch weisser zu waschen

Cyberkriminalität ist ein typisches Beispiel für eine hoch entwickelte Arbeitsteilung. Jede Art von Cyberangriff kann als eine Abfolge klar definierter Aufgaben gesehen werden, auf die sich oft bestimmte Akteure spezialisiert haben. Diese Akteure streben ständig nach grösstmöglicher Effizienz und tragen damit zur Wirtschaftlichkeit des Phänomens insgesamt bei. Unter diesen verschiedenen spezifischen Aufgaben nimmt das Waschen von illegal erworbenem Geld einen besonderen Platz ein. In der Tat wäre die gesamte kriminelle Kette sinnlos, wenn es am Ende nicht möglich wäre, das Geld für den Gebrauch auf dem legalen Markt zu bereinigen. Diese Aktivität blüht: Laut einer 2018 von «Bromium» veröffentlichten Studie werden jedes Jahr zwischen 80 und 200 Milliarden Dollar von Cyberkriminellen gewaschen.[107]

Die Entwicklung virtueller Währungen war eine Revolution bei Transaktionen, die aus cyberkriminellen Aktivitäten resultieren. Heute wird eine ganze Reihe von kriminellen Aktivitäten mit virtuellen Währungen wie z. B. Bitcoin finanziert. Eine virtuelle Währung kann trotz Transaktionsdokumentationen mittels Blockchain auf eine Weise verarbeitet werden, die eine Rückverfolgung schwierig macht, z. B. durch die Verwendung von «Mixer/Tumblern».[108] Die Früchte von anderen cyberkriminellen Aktivitäten materialisieren sich jedoch immer noch in Form von traditionellen Währungen. Dies ist zum Beispiel der Fall beim Computerbetrug mit Hilfe von E-Banking-Trojanern oder bei Zahlungen mit einer gestohlenen Kreditkarte. Für diese Art von Aktivitäten muss eine eher traditionelle Geldwäscheaktivität durchgeführt werden. Schon seit langem ist dokumentiert, dass Privatpersonen angeheuert werden, um ihre Bankkonten zur Verfügung zu stellen, Gelder zu empfangen und dann für die Weiterleitung an ein anderes

101 https://attack.mitre.org/groups/G0064/
102 https://attack.mitre.org/groups/G0049/
103 https://attack.mitre.org/groups/G0021/
104 https://attack.mitre.org/groups/G0077/
105 https://attack.mitre.org/groups/G0087/
106 https://attack.mitre.org/
107 https://www.bromium.com/press-release/up-to-200-billion-in-illegal-cybercrime-profits-is-laundered-each-year-comprehensive-research-study-reveals/
108 Dienst, der es erlaubt, Transaktionen grösserer Beträge in Kryptowährungen zu verschleiern, indem sie über einzelne, sehr aktive Wallets geschleust und dort in viele kleine Transaktionen zerstückelt werden.

Konto eine Provision zu kassieren. Solche rekrutierten Privatpersonen werden «Money Mules» oder Finanzagenten genannt. Getreu ihrem opportunistischen Ansatz versuchen die Kriminellen auch, von bestehenden Plattformen zu profitieren. Bekannte Geldwäschemethoden basieren beispielsweise auf Mikrozahlungen über «PayPal» oder überteuerten eBay-Verkäufen.

Gegenwärtig hat der Erfolg von Plattformen wie «AirBnB» oder «Uber» das Interesse von Kriminellen geweckt. Diese Plattformen ermöglichen es einem Dienstleistungsanbieter, dank des Einsatzes neuer Technologien direkt mit seinen Kunden in Kontakt zu treten. Ein typisches Beispiel für diese neuen Geldwäschemethoden sind «Geisterfahrten» vor Uber. Die Kriminellen rekrutieren in erster Linie Uber-Fahrer, die möglicherweise wegschauen und versuchen, ihr monatliches Gehalt aufzurunden. Zu diesem Zweck werden Ankündigungen in Untergrundforen veröffentlicht. Der Kriminelle bestellt eine Fahrt und bezahlt dann den Fahrer in der vorgeschriebenen Form. Diese Fahrt ist jedoch rein fiktiv, und der Fahrer verlässt zu keiner Zeit sein Haus. Er zahlt das Geld an den Kriminellen zurück, wobei er einen Prozentsatz davon als Belohnung behalten darf. Ein sehr ähnliches Muster wurde auf der «AirBnB»-Immobilienuntervermietungsplattform beobachtet. In diesem Fall bezahlt der Kriminelle für eine Wohnung, die er niemals bewohnen wird. Auch hier zahlt der Vermieter ihm das Geld zurück und nimmt dabei eine Provision ein.

Der Kampf gegen die Cyberkriminalität zielt darauf ab, eine hochprofitable Kette von Aktivitäten zu unterbrechen, indem eines der Glieder angegriffen wird. Diese Methoden der Geldwäsche sind daher regelmässig im Visier von polizeilichen Aktionen. So gab Europol im Dezember 2019 bekannt, dass eine Operation, an der 31 Länder beteiligt waren, zur Verhaftung von 228 Money Mules-Rekrutierern geführt hatte.[109] Bereits im Mai gab dieselbe Behörde bekannt, dass sie zusammen mit den Behörden in Luxemburg und den Niederlanden «Bestmixer.io» geschlossen hat. Mit diesem Dienst war es möglich, in einem Jahr rund 200 Millionen Dollar zu waschen[110]. Wie die Beispiele der Missbräuche der Plattformen von «Uber» und «Airbnb» zeigen, fehlt es den Kriminellen nicht an Ideen und Wissen, wie sie ihre Geldwäsche-Modelle diversifizieren können. Neben der Arbeit der Polizei und den Sensibilisierungsmassnahmen gegen potenzielle «Money Mules» liegt ein Teil der Lösung zweifellos in den Massnahmen, die von den missbrauchten Online-Diensten eingeführt wurden, und in ihrer Fähigkeit, den Missbrauch der Dienste zur Geldwäsche zu erkennen.

109 https://www.europol.europa.eu/newsroom/news/228-arrests-and-over-3800-money-mules-identified-in-global-action-against-money-laundering

110 https://www.europol.europa.eu/newsroom/news/multi-million-euro-cryptocurrency-laundering-service-bestmixerio-taken-down

6 Publizierte MELANI Produkte

6.1 Blog GovCERT.ch

6.1.1 Trickbot - An analysis of data collected from the botnet

We are monitoring various threats and in that context we have collected quite some data about the Trickbot botnet in the past few years. This paper is based on an analysis of selected aspects of our Trickbot data collection. Our analysis consists of two main parts. In the first part we consider the PE timestamps of Trickbot droppers (i.e., the binaries being distributed by the Trickbot operators) and of the respective payloads (i.e., the PE binaries which are unpacked and then executed once a dropper is executed). The analysis is based on a collection of approximately 2100 droppers and corresponding payloads which were collected between July 2016 and February 2019.

https://www.govcert.admin.ch/blog/37/trickbot-an-analysis-of-data-collected-from-the-botnet

6.2 MELANI Newsletter

6.2.1 Update Verschlüsselungs-Trojaner: Neue Vorgehensweise

30.07.2019 – In den vergangenen Wochen wurden Schweizer Unternehmen Ziel einer neuen Art von Angriffen, mit der unbekannte Angreifer Unternehmensnetzwerke erfolgreich infiltrieren und deren Daten mittels einem Verschlüsselungstrojaner grossflächig verschlüsseln. Auch diverse namhafte Schweizer Unternehmen sind von den Angriffen betroffen.

https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/update-ransomware-neue-vorgehensweise.html

6.2.2 Microsoft stellt für ältere Produkte den Support ein: Gefahr droht

16.12.2019 - Gemäss einer Mitteilung von Microsoft werden am 14. Januar 2020 für verschiedene ältere Produkte der Support und somit die Updates eingestellt. Betroffen sind folgende Produkte: Betriebssystem «Windows 7», «Windows Server 2008» und «Windows Server 2008 R2».

https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/microsoft-end-of-life.html

7 Glossar

Begriff	Beschreibung
APT Advanced Persistent Threat	Bei dieser Angriffsweise kommen verschiedene Techniken und Taktiken zum Einsatz. Sie wird sehr gezielt auf eine einzelne Organisation oder auf ein Land durchgeführt. Meist kann damit sehr hoher Schaden angerichtet werden. Deshalb ist der Angreifer bereit, sehr viel Zeit, Geld und Wissen in den Angriff zu investieren und verfügt dazu in der Regel über grosse Ressourcen.
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.
BGP Border Gateway Protocol	Das Border Gateway Protocol ist das im Internet eingesetzte Routingprotokoll, welches den Weg von Datenpaketen zwischen Netzwerken bestimmt.
Bitcoin	Bitcoin ist ein weltweit verwendbares dezentrales Zahlungssystem und der Name einer digitalen Geldeinheit.
Bot	Ursprung im slawischen Wort für Arbeit (Robota). Bezeichnet ein Programm, das bestimmte Aktionen nach dem Empfang eines Befehls selbstständig ausführt. So genannte Malicious Bots können kompromittierte Systeme fernsteuern und zur Durchführung beliebiger Aktionen veranlassen.
Botnetz	Mehrere Bots können ein Netzwerk bilden. Dieses wird über eine Command & Control-Infrastruktur gesteuert.
Brute Force	Die Brute-Force-Methode ist eine Lösungsmethode für Probleme aus den Bereichen Informatik, Kryptologie und Spieltheorie, die auf dem Ausprobieren aller möglichen Fälle beruht.

Begriff	Beschreibung
C2 Command & Control	Befehls- und Steuerungsinfrastruktur von Botnetzen. Die meisten Bots können über einen Kommunikationskanal überwacht werden und Befehle empfangen.
CaaS Cybercrime-as-a-Service	Cyber-Kriminalität als einkaufbare Dienstleistung ermöglicht technisch wenig versierten Kriminellen durch einfach zu bedienende Werkzeuge, illegale Aktivitäten auch im Internet durchzuführen.
CEO-Betrug / CEO-Fraud	Von CEO-Betrug ist die Rede, wenn Täter im Namen des Firmenchefs die Buchhaltung oder den Finanzdienst anweisen, eine Zahlung auf ein (typischerweise ausländisches) Konto der Betrüger vorzunehmen.
CPU / Prozessor	Die CPU (Central Processing Unit) ist eine andere Bezeichnung für Prozessor, der zentralen Einheit in einem Computer, und enthält die logischen Schaltungen um ein Computer-Programm auszuführen.
Cryptomining	Durch das Mining werden neue Blöcke erzeugt und anschliessend zur Blockchain hinzugefügt. Der Vorgang ist sehr rechenintensiv und wird deshalb vergütet.
DDoS	Distributed-Denial-of-Service-Attacke. Mit einer DoS-Attacke wird der Dienst oder das System des Opfers von vielen verscheiden Systemen aus gleichzeitig angegriffen, so dass dieses zum Erliegen kommt und nicht mehr verfügbar ist.
Defacement	Verunstaltung von Webseiten.
DNS Domain Name System	Mit Hilfe des DNS lassen sich das Internet und deren Dienste benutzerfreundlich nutzen, da die Benutzer anstelle von IP-Adressen Namen verwenden können (z. B. www.melani.admin.ch).
Drive-by-Infektion	Infektion eines Computers mit Malware allein durch Besuch einer Webseite. Die Infektion erfolgt meistens durch das Ausprobieren von Exploits für vom Besucher noch nicht geschlossene Sicherheitslücken.
Dropper / Downloader	Ein Dropper oder Downloader ist ein Programm, das eine oder mehrere Instanzen von Schadsoftware herunterlädt und installiert.
Exploit-Kit	Baukasten, mit welchen Kriminelle Programme, Scripts oder Code-Zeilen generieren können, womit sich

Begriff	Beschreibung
	Schwachstellen in Computersystemen ausnutzen lassen.
Fernzugriffstool	Die Fernwartungs-Software (englisch: Remote Administration Tool) stellt eine Anwendung des Konzeptes Fernwartung für beliebige Rechner oder Rechnersysteme dar.
Finanzagent	Ein Finanzagent ist jemand, der sich als legaler Geldvermittler und damit auch im Finanz-Transfergeschäft betätigt. In jüngerer Zeit wird dieser Begriff in Zusammenhang mit illegalen Finanz-Transaktionen gebraucht.
GPS Global Positioning System	Global Positioning System (GPS), offiziell NAVSTAR GPS, ist ein globales Navigationssatellitensystem zur Positionsbestimmung und Zeitmessung.
Internet der Dinge	Der Begriff Internet der Dinge (Internet of Things, IoT) beschreibt die Vernetzung und das Zusammenarbeiten von physischen und virtuellen Gegenständen.
ISP Internet Service Provider	Internetdienstanbieter oder Internetdienstleister sind Anbieter von Diensten, Inhalten oder technischen Leistungen, die für die Nutzung oder den Betrieb von Inhalten und Diensten im Internet erforderlich sind.
Javascript	Eine objektbasierte Scripting-Sprache zur Entwicklung von Applikationen. JavaScripts sind im HTML-Code integrierte Programmteile, die bestimmte Funktionen im Internet-Browser ermöglichen. Ein Beispiel kann das Kontrollieren von Benutzereingaben bei einem Web-Formular sein. So kann überprüft werden, ob alle eingegebenen Zeichen bei geforderter Angabe einer Telefonnummer auch wirklich Zahlen sind. Wie ActiveX Controls werden JavaScripts auf dem Rechner des Website-Besuchers ausgeführt. Neben nützlichen, lassen sich leider auch schädliche Funktionen programmieren. Im Gegensatz zu ActiveX werden JavaScripts von allen Browsern unterstützt.
Kontroll- oder Steuerungssysteme (IKS)	Kontroll- oder Steuerungssysteme (IKS) bestehen aus einem oder mehreren Geräten, welche das Verhalten von anderen Geräten oder Systemen steuern, regeln und/oder überwachen. In der industriellen Produktion ist der Begriff «Industrielle Kontrollsysteme» (engl. Industrial Control Systems, ICS) geläufig.

Begriff	Beschreibung
Malspam	Massenhaft versendete E-Mails, mit welchen Schadsoftware verbreitet wird.
Malware / Schadsoftware	Oberbegriff für Software, die schädliche Funktionen auf einem Rechner ausführt (wie beispielsweise Viren, Würmer, Trojanische Pferde).
Man-in-the-Middle Attacke	Attacke, bei der sich der Angreifer unbemerkt in den Kommunikationskanal zweier Partner hängt und dadurch deren Datenaustausch mitlesen oder verändern kann.
Metadaten	Metadaten oder Metainformationen sind Daten, die Informationen über andere Daten enthalten
MSP Managed Services Provider	Ein Betreibermodellanbieter oder Betreiberlösungsanbieter ist ein IT-Dienstleister, der eine definierte Reihe von Dienstleistungen für seine Kunden übernimmt und verwaltet.
NAS Network Attached Storage	Netzgebundener Speicher: Direkt an einem Netzwerk angeschlossener Festplattenspeicher oder Dateiserver.
Patch	Eine Software, die den fehlerhaften Teil eines Programms durch einen fehlerfreien ersetzt und dadurch z. B. eine Sicherheitslücke behebt.
Peer to Peer	Peer to Peer Eine Netzwerkarchitektur, bei der die beteiligten Systeme gleiche Funktionen übernehmen können (im Gegensatz zu Client-Server Architekturen). P2P wird häufig zum Austausch von Daten genutzt.
Phishing	Mittels Phishing versuchen Betrüger, an vertrauliche Daten von ahnungslosen Internet-Benutzern zu gelangen. Dabei kann es sich beispielsweise um Kontoinformationen von Online-Auktionsanbietern (z. B. eBay) oder Zugangsdaten für das Internet-Banking handeln. Die Betrüger nutzen die Gutgläubigkeit und Hilfsbereitschaft ihrer Opfer aus, indem sie ihnen beispielsweise E-Mails mit gefälschten Absenderadressen zustellen.
PowerShellScript	PowerShell ist ein plattformübergreifendes Framework von Microsoft zur Automatisierung, Konfiguration und Verwaltung von Systemen, bestehend aus einem Kommandozeileninterpreter sowie einer Skriptsprache.
Proxy	Ein Proxy ist eine Kommunikationsschnittstelle in einem Netzwerk. Er arbeitet als Vermittler, der auf der einen

Begriff	Beschreibung
	Seite Anfragen entgegennimmt, um dann über seine eigene Adresse eine Verbindung zur anderen Seite herzustellen.
RaaS Ransomware-as-a-Service	Ransomware als einkaufbare Dienstleistung ermöglicht technisch wenig versierten Kriminellen durch einfach zu bedienende Werkzeuge Angriffe durchzuführen.
Ransomware	Schadsoftware, die ihre Opfer typischerweise durch Verschlüsselung von Daten zur Bezahlung von Lösegeld bewegen will.
RDP Remote Desktop Protocol	Ein Netzwerkprotokoll von Microsoft für den Fernzugriff auf Windows-Computer.
Router	Geräte aus dem Bereich Computernetzwerke, Telekommunikation oder auch Internet, die mehrere Rechnernetze koppeln oder trennen. Router werden beispielsweise in Heimnetzwerken eingesetzt und machen die Verbindung zwischen internem Netz und dem Intranet.
Schadsoftware / Malware	Oberbegriff für Software, die schädliche Funktionen auf einem Rechner ausführt (wie beispielsweise Viren, Würmer, Trojanische Pferde).
Schwachstelle / Lücke	Schwachstelle in Hard- oder Software, über die Angreifer Zugriff auf ein System erlangen können.
Smartphone	Ein Smartphone ist ein Mobiltelefon, das mehr Computerfunktionalität und -konnektivität als ein herkömmliches fortschrittliches Mobiltelefon zur Verfügung stellt.
SMB-Protokoll	Server Message Block (SMB) ist ein Netzwerkprotokoll für Datei-, Druck- und andere Serverdienste in Rechnernetzen.
SMS	Short Message Service ist ein Dienst zum Versenden von Kurzmitteilungen (maximal 160 Zeichen) an Mobiltelefonbenutzer.
Social Engineering	Social Engineering-Angriffe nutzen die Hilfsbereitschaft, Gutgläubigkeit oder die Unsicherheit von Personen aus, um beispielsweise an vertrauliche Daten zu gelangen, oder die Opfer zu bestimmten Handlungen zu bewegen. Eine bekannte Form von Social Engineering ist Phishing.

Begriff	Beschreibung
Spam	Unaufgefordert und automatisiert zugesandte Massenwerbung, worunter auch Spam-E-Mails fallen. Als Spammer bezeichnet man den Absender dieser Mitteilungen, während das Versenden selbst als Spamming bezeichnet wird.
Spear-Phishing	Gezielte Phishing-Attacke. Dem Opfer wird zum Beispiel vorgegaukelt, mit einer ihr vertrauten Person via E-Mail zu kommunizieren.
Spoofing	Fälschen von Adressierungselementen oder Signalen zwecks Täuschung der empfangenden Person oder des empfangenden Gerätes.
Supply Chain-Angriffe	Angriff bei dem versucht wird, über die Infektion einer Firma in der Lieferkette das eigentliche Ziel zu infizieren.
Take-Down	Ausdruck, der verwendet wird, wenn ein Provider eine Website aufgrund betrügerischen Inhalts vom Netz nimmt.
TCP/IP	Transmission Control Protocol / Internet Protocol ist eine Familie von Netzwerkprotokollen und wird wegen ihrer grossen Bedeutung für das Internet auch als Internetprotokollfamilie bezeichnet.
TLD Top-Level-Domain	Jeder Name einer Domain im Internet besteht aus einer Folge von durch Punkte getrennten Zeichenfolgen. Die Bezeichnung Top-Level-Domain bezeichnet dabei den letzten Namen dieser Folge und stellt die höchste Ebene der Namensauflösung dar. Ist der vollständige Domain-Name eines Rechners bzw. einer Website beispielsweise de.example.com, so entspricht das rechte Glied (com) der Top-Level-Domain dieses Namens.
UDP	Das User Datagram Protocol, kurz UDP, ist ein minimales, verbindungsloses Netzwerkprotokoll, das zur Transportschicht der Internetprotokollfamilie gehört.
USB	Universal Serial Bus. Serielle Kommunikationsschnittstelle, welche den Anschluss von Peripheriegeräten wie Tastatur, Maus, externe Datenträger, Drucker usw. erlaubt. Der Rechner muss beim Ein- beziehungsweise Ausstecken eines USB-Gerätes nicht heruntergefahren werden. Die neuen Geräte werden meist (allerdings abhängig vom Betriebssystem) automatisch erkannt und konfiguriert.

Begriff	Beschreibung
Watering-Hole-Angriffe	Gezielte Infektion durch Schadsoftware über Websites, welche bevorzugt nur von einer spezifischen Benutzergruppe besucht werden.
Webseiteninfektion	Infektion eines Computers mit Malware allein durch den Besuch einer Web-Seite. Vielfach beinhalten die betroffenen Web-Seiten seriöse Angebote und sind zwecks Verteilung der Malware zuvor kompromittiert worden. Die Infektion erfolgt meistens durch das Ausprobieren von Exploits für vom Besucher noch nicht geschlossene Sicherheitslücken.
WLAN	WLAN (Wireless Local Area Network) steht für drahtloses lokales Netzwerk.
Wurm	Im Gegensatz zu Viren benötigen Würmer zur Verbreitung kein Wirtprogramm. Vielmehr nutzen sie Sicherheitslücken oder Konfigurationsfehler in Betriebssystemen bzw. Anwendungen, um sich selbständig von Rechner zu Rechner auszubreiten.
ZeroDay-Lücken	Sicherheitslücke, für welche noch kein Patch existiert.
ZIP-Datei	ZIP ist ein Algorithmus und Dateiformat zur Datenkompression, um den Speicherbedarf von Dateien für die Archivierung und Übertragung zu verringern.
Zweifaktorauthentifizierung	Um die Sicherheit zu erhöhen wird die Zweifaktorauthentifizierung verwendet. Dafür sind mindestens zwei der drei Authentifikationsfaktoren notwendig: 1. Etwas, das man weiss (z. B. Passwort, PIN, usw.) 2. Etwas, das man besitzt (z. B. Zertifikat, Token, Streichliste, usw.) 3. Ein einmaliges Körpermerkmal (z. B. Fingerabdruck, Retina-Scan, Stimmerkennung usw.).