Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Nationales Zentrum für Cybersicherheit NCSC
Nachrichtendienst des Bundes NDB

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

INFORMATIONSSICHERUNG

LAGE IN DER SCHWEIZ UND INTERNATIONAL

Halbjahresbericht 2020/I (Januar – Juni)

29. OKTOBER 2020

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

1 Übersicht / Inhalt

2 Editorial

Schweizer Cyberdiplomatie im Zeichen der digitalen Geopolitik

Sondergesandter und Chef des Büros für Cyber-Aussen- und -Sicherheitspolitik, Jon Fanzun

Jon Fanzun, Sondergesandter und Chef des Büros für Cyber-Aussen- und -Sicherheitspolitik

Noch vor wenigen Jahren war Cybersicherheit ein Nischenthema, das international fast ausschliesslich in technischen Expertenkreisen diskutiert wurde. Heute ist Cybersicherheit zu einem elementaren Bestandteil und zu einem heiss diskutierten Thema der internationalen Politik geworden. Das Thema ist überdies brisant, weil digitale Technologien eine zentrale Rolle in unserer hochentwickelten Informationsgesellschaft spielen. Schlüsseltechnologien rücken deshalb in den Mittelpunkt globaler Konflikte.

Der aktuelle Streit zwischen den USA und China zum Thema 5G ist beispielhaft, wie sich sicherheitspolitische, wirtschaftliche und gesellschaftliche Fragen zu einer neuen Form der Geopolitik vermischen. Man kann in diesem Zusammenhang von einer «digitalen Geopolitik» sprechen, bei welcher es nicht nur um einen Wettlauf der Technologien, sondern auch um einen ideologischen Wettlauf zwischen einem freiheitlichen und einem staatenzentrierten Modell geht.

Vor diesem Hintergrund ist die Schweiz gefordert, ihre Interessen auch im Cyberraum aktiv zu vertreten. Das Büro Cyber im EDA übernimmt diese Aufgabe in Zusammenarbeit mit den verschiedenen Partnern in der Bundesverwaltung – namentlich auch mit dem Nationalen Zentrum für Cybersicherheit (NCSC). Die aktuelle Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS 2.0) sowie die Aussenpolitische Strategie 2020-2023 bilden hierfür den strategischen Rahmen.

Die Schweiz setzt sich für einen freien, sicheren und offenen Cyberraum ein, der für friedliche Zwecke genutzt wird und auf klaren Regeln und gegenseitigem Vertrauen basiert. Sie vertritt dabei den Grundsatz, dass das Völkerrecht auch im Cyberraum anzuwenden und umzusetzen ist. Überdies setzen wir uns international für den Einbezug relevanter Akteure aus der Zivilgesellschaft und der Wirtschaft ein. Wir bringen unsere Interessen und Werte in den internationalen Foren wie der UNO, der OSZE oder der OECD ein. Ebenfalls wichtig sind bilaterale Cyberdialoge. In den kommenden Jahren wollen wir diese Dialoge – entsprechend der NCS 2.0 – mit ausgewählten Ländern intensivieren und ausbauen.

Angesichts der zunehmenden Blockbildung, des dramatisch abnehmenden Vertrauens zwischen Staaten und der daraus resultierenden Fragmentierung des Cyberraums, wird es aber schwierig sein, Fortschritte in der internationalen Cyberdiplomatie zu erreichen. Es wird schon schwierig genug werden, den bisher erreichten internationalen Konsens – der etwa im Bericht der «United Nations Group of Governmental Experts» (GGE) von 2015 festgehalten ist – zu konsolidieren.

Wenn das Vertrauen schwindet und die Debatten härter werden, wächst auch der Bedarf an Brückenbauern. Die Schweiz kann hier ihre diplomatischen Stärken und ihre Glaubwürdigkeit in die Waagschale werfen. Sie kann ihre Erfahrung aus der offline- in die online-Welt übertragen. Eine wichtige Rolle spielt hier das internationale Genf. Hier kann die Schweiz einen vertrauensvollen Rahmen bereitstellen, um über Cybersicherheit und neue Technologien zu diskutieren. Der «Geneva Dialogue on responsible Behaviour in Cyberspace» ist ein gutes Beispiel, wie die Schweiz auf pragmatische Art einen Beitrag zu mehr Cybersicherheit leistet, indem globale Firmen wie Microsoft, Kaspersky oder Huawei an den Diskussionen über Cybersicherheit beteiligt werden.

Cyberdiplomatie ist Teamsport. Der Einbezug der relevanten Akteure und ihres Know-hows ist essenziel, um die Schweizer Interessen auf dem internationalen Parkett wirksam einbringen zu können. Die Bündelung und die Koordination der Kräfte im Rahmen des NCSC schafft diesbezüglich auch für die internationale Cybersicherheit der Schweiz einen Mehrwert. Mein Dank geht darum an alle beteiligten Akteure aus den verschiedenen Departementen für ihren Einsatz für einen freien, sicheren und offenen Cyberraum.

Jon Fanzun

In eigener Sache:

Der Halbjahresbericht MELANI erscheint zum letzten Mal in diesem Kleid und wird neu unter dem Label des Nationalen Zentrums für Cybersicherheit (NSCS) erscheinen. Mit in Kraft treten der «Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung» am 1. Juli 2020 ist MELANI Teil des NCSC geworden.

Damit wir unsere Produkte laufend verbessern und auf die Bedürfnisse der Leserschaft eingehen können, laden wir Sie ein, uns **Ihre Meinung zu diesem Bericht** zukommen zu lassen:

https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/evaluation-halbjahresbericht1.html

3 Schwerpunktthema: COVID-19

3.1 Gelegenheit für Social Engineering

Cyberakteure passen Social-Engineering-Angriffe regelmässig an aktuelle Grossereignisse wie Naturkatastrophen und Sportanlässe an. Dies war auch bei der aktuellen Pandemie der Fall. Ein neuartiges Virus, über das wenig Wissen vorhanden ist und das potenziell alle Menschen betreffen kann, eignet sich hervorragend für solche Angriffe, die Gefühle wie Verunsicherung, Angst und Neugierde ausnutzen. So versuchten die Angreifer der Bevölkerung heimlich Schadsoftware auf den Computern zu installieren oder sie versuchten Einzelpersonen dazu zu bringen, persönliche Daten preiszugeben, indem sie versprachen, Informationen über das Virus zu geben. Diese Informationsversprechen gingen von den neuesten Erkenntnissen über Ansteckungsvektoren, die Infektionszahlen bis zu Informationen über die aktuelle Ausbreitung. Auch mit Schutzmassnahmen und Behandlungsmethoden wurde geworben. Die anfänglich beschränkte Verfügbarkeit von persönlicher Schutzausrüstung wie Gesichtsmasken und Desinfektionsmittel bot den Angreifern ebenfalls Gelegenheit, mit entsprechenden Angeboten Aufmerksamkeit zu erhalten.[1] Nachdem Regierungen Massnahmen zur Unterstützung der Bevölkerung und von Unternehmen beschlossen hatten, folgten auch diesbezüglich betrügerische E-Mails.[2] Dies insbesondere dort, wo ausserordentliche und damit ungewohnte Prozesse dafür geschaffen wurden. Das Nachverfolgen von Kontakten, so genanntes Contact-Tracing bietet ebenfalls Ansätze für Social Engineering. Schliesslich warben u. a. Freizeitparks und Attraktionen nach ihrer Wiedereröffnung mit Sonderangeboten, was von Kriminellen zum Anlass genommen wurde, gefälschte Angebote dieser Art zu verbreiten.[3] Die Entwicklung und Lancierung von Impfstoffen wird voraussichtlich ebenfalls von den Angreifern als Thema für diese Art von Angriffen verwendet werden.

Ein Szenario, das infolge der Ladenschliessungen und dem damit verbundenen Anstieg von Online-Bestellungen neuen Aufwind bekam, waren vermeintliche Lieferungen von Paketen, die nicht zugestellt werden konnten oder mit denen etwas nicht in Ordnung sei. Häufig waren diese Nachrichten verbunden mit der Aufforderung eine Aktion auszuführen.[4] So wurden die Empfänger solcher E-Mails oder SMS aufgefordert, fehlendes Porto oder eine Gebühr für die Zollabfertigung nachzuzahlen. Über solche E-Mails im Namen von Lieferdiensten wie DHL, FedEx und UPS, aber auch der Post oder des Zolls wird meist Schadsoftware verbreitet oder Phishing und Betrug betrieben sowie Abofallen gestellt (siehe dazu Kapitel 3.1.3 sowie auch Überblick Meldeeingang im Kapitel 4).

---

1 https://securityintelligence.com/posts/german-task-force-for-covid-19-medical-equipment-targeted-in-ongoing-phishing-campaign/

2 https://www.cisa.gov/sites/default/files/publications/Avoid_Scams_Related_to_Economic_Payments_COVID-19.pdf; https://www.proofpoint.com/us/blog/threat-insight/ready-made-covid-19-themed-phishing-templates-copy-government-websites-worldwide

3 https://www.cybercrimepolice.ch/de/fall/wieder-betrug-mit-themenpark-tickets-zoo-zuerich-nein-abofalle/; https://www.srf.ch/news/schweiz/abzocke-mit-abofalle-betrug-im-namen-des-zueri-zoo

4 https://www.cybercrimepolice.ch/de/fall/sms-angeblich-im-namen-der-post-betrueger-verteilen-spionage-app/; https://www.cybercrimepolice.ch/de/fall/angebliche-paketlieferung-mit-code-per-sms-freischalten/; https://www.kaspersky.com/blog/covid-fake-delivery-service-spam-phishing/35125/

3.1.1 Verbreitung von Schadsoftware

Praktisch alle gängigen Schadsoftware-Familien wurden früher oder später mit einem Corona- oder COVID-19-Vorwand verbreitet. Der häufigste Verbreitungsvektor waren E-Mails mit verseuchtem Anhang oder einem Link auf eine infizierte Website. Daneben wurden in inoffiziellen App-Stores Apps angeboten, die vermeintlich die Ausbreitung des Virus auf einer Karte anzeigen und vor infizierten Personen in der Nähe warnen.[5] Ebenfalls wurden Kopien von offiziellen Tracing-Apps entdeckt, die mit Schadsoftware angereichert waren.[6] Zudem wurde das erhöhte Interesse an Videokonferenzlösungen ausgenützt: Über gefälschte Websites auf Typo-Domainnamen, d. h. zum Verwechseln ähnlichen Domainnamen, wurden mit Schadsoftware angereicherte Installationsdateien für Konferenzsoftware angeboten.[7]

Am 13. März gab es eine spezifisch auf die Schweiz ausgerichtete E-Mail-Welle mit Schadsoftware.[8] Bei dieser wurde das Bundesamt für Gesundheit (BAG) respektive die englische Abkürzung FOPH (Federal Office of Public Health) als vermeintlicher Absender verwendet. Die E-Mails wurden über die kenianische Botschaft in Paris versendet, deren IT-Infrastruktur gehackt worden war. In der angehängten Excel-Datei war der Trojaner «AgentTesla» versteckt, der Tastatureingaben mitschneidet und Bildschirmfotos erstellen kann.

Abb. 1: E-Mail im Namen des BAG mit schädlichem Anhang.

---

5 https://www.cybercrimepolice.ch/de/fall/vorsicht-vor-falscher-corona-virus-mapping-app/; https://symantec-blogs.broadcom.com/blogs/threat-intelligence/android-apps-coronavirus-covid19-malicious; https://research.checkpoint.com/2020/covid-19-goes-mobile-coronavirus-malicious-applications-discovered/

6 https://www.anomali.com/blog/anomali-threat-research-identifies-fake-covid-19-contact-tracing-apps-used-to-monitor-devices-steal-personal-data; https://www.bleepingcomputer.com/news/security/new-f-unicorn-ransomware-hits-italy-via-fake-covid-19-infection-map/; https://cert-agid.gov.it/news/campagna-ransomware-fuckunicorn-sfrutta-emergenza-covid-19/

7 https://blog.checkpoint.com/2020/03/30/covid-19-impact-cyber-criminals-target-zoom-domains/; https://blog.trendmicro.com/trendlabs-security-intelligence/zoomed-in-a-look-into-a-coinminer-bundled-with-zoom-installer/

8 https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/gefaelschte-emails-im-namen-des-bag.html

Mit solchen Corona- und COVID-19-Ködern wurde in den meisten Fällen Schadsoftware verbreitet, die Informationen stehlen können (*Infostealer* oder *Spyware*).[9] Diese Spyware beinhalten häufig auch Module, mit welchen beliebige weitere Schadsoftware platziert werden kann. In einigen Fällen wurde erpresserische Schadsoftware (Ransomware) direkt über solche E-Mails verbreitet.

Empfehlungen:

Wenn Sie in verdächtigen Mails auf Links geklickt oder Anhänge geöffnet haben, kann Ihr Gerät mit Schadsoftware infiziert sein. Sie sollten das Gerät untersuchen und gegebenenfalls säubern oder besser komplett neu installieren. Wenn Sie dies nicht selber durchführen können, wenden Sie sich an eine Fachperson. Antivirenprogramme bieten keine Garantie, alle Infektionen zu erkennen und sie vollständig zu entfernen. Ändern Sie nach der Neuinstallation alle mit dem betroffenen Gerät verwendeten Passwörter.

3.1.2 Phishing

Aktuelle Ereignisse und ungewohnte Situationen werden sehr gerne von Cyberkriminellen als Vorwand genutzt, um Personen mithilfe von Social Engineering dazu zu bringen, aus Neugierde, Angst oder Unwissenheit eine Aktion auszuführen. Dabei wird das eigentliche Ereignis häufig referenziert, um dem Szenario Glaubwürdigkeit zu verleihen. Zum Beispiel wurden kurz nach der Verhängung der Ausgangssperren E-Mails im Namen von Netflix verschickt, in denen ein Gratiszugänge während der Corona-Krise versprochen wurden.[10] Für eine Registrierung zu diesem Angebot mussten die Kreditkartendaten angegeben werden. Ein weiteres Beispiel, wie die ausserordentliche Situation für Angriffe ausgenutzt wurde, zeigte sich beim Phishing via vermeintliche Konferenzplattformen. Viele Nutzende verwendeten zum ersten Mal solche Konferenz- und Kollaborationssoftware. Somit war es für viele Benutzende nicht einfach zu erkennen, ob eine Nachricht von der Plattform stammte oder ob es sich um eine entsprechende Fälschung handelte.[11] Diese Unsicherheiten wurden von den Angreifern so ausgenutzt, dass die Nutzenden auf manipulierte Anmeldemasken geleitet wurden, wo sie zur Eingabe von Passwörtern aufgefordert wurden.

---

9 https://blog.checkpoint.com/2020/05/11/april-2020s-most-wanted-malware-agent-tesla-remote-access-trojan-spreading-widely-in-covid-19-related-spam-campaigns/; https://www.lastline.com/labsblog/infostealers-weaponizing-covid-19/; https://www.bleepingcomputer.com/news/security/microsoft-warns-of-covid-19-phishing-spreading-info-stealing-malware/;

10 https://www.cybercrimepolice.ch/de/fall/corona-phishing-mail-im-namen-von-netflix/

11 https://www.darkreading.com/cloud/fake-microsoft-teams-emails-phish-for-credentials/d/d-id/1337717; https://abnormalsecurity.com/blog/abnormal-attack-stories-microsoft-teams-impersonation/; https://abnormalsecurity.com/blog/abnormal-attack-stores-zoom-phishing-campaign/;

Empfehlungen:

Beim Empfang von neuartigen oder ungewöhnlichen Nachrichten gilt es immer, eine gesunde Portion Skepsis an den Tag zu legen. Statt Links in solchen Nachrichten zu folgen, sollten Sie sich wenn möglich über den gewohnten Weg in Ihr Nutzerkonto einloggen. Verifizieren Sie vor der Eingabe von persönlichen Daten, Passwörtern oder Kreditkarteninformationen immer, ob Sie sich tatsächlich auf der gewünschten Seite befinden.

3.1.3 Abofallen

Während des Lockdowns im März wurden über WhatsApp in der Schweiz Nachrichten verbreitet, welche die Verlosung von Lebensmittelgutscheinen versprachen. Als vermeintliche Absender wurden Detailhändler angegeben, die «die Nation während der Corona-Pandemie unterstützen» wollten. Dafür missbrauchten die Täter bekannte Marken wie Migros, Coop und Denner.[12] Auf der verlinkten Webseite wurde jeweils nach Kreditkarteninformationen gefragt – angeblich zur Verifizierung der Identität und damit jede Person nur einen Gutschein beanspruchen könne. Im Kleingedruckten auf der Seite war jedoch ein teures Abonnement versteckt, für welches von der Kreditkarte monatlich eine Gebühr abgebucht wurde.

Empfehlungen:

Kreditkartenabrechnungen sollten immer genau kontrolliert werden, um bei Unregelmässigkeiten oder ungerechtfertigten Abbuchungen die Kreditkarten nach Absprache mit der Herausgeberin gegebenenfalls zu sperren. An Betrüger bekanntgegebene Daten können von diesen nicht nur selbst für Abbuchungen genutzt, sondern auch weiterverkauft werden.

3.2 Angriffe auf Websites und –dienste

In mehreren Ländern waren Websites von Spitälern und Behörden, die Informationen zur Pandemie bereitstellten oder Leistungen anboten, kurzzeitig nicht mehr erreichbar.[13] Einige der Websiteverantwortlichen begründeten diese Ausfälle mit DDoS-Angriffen. Während dies sicher eine plausible Erklärung und meist auch zutreffend ist, dürfte in einigen Fällen durchaus das erhöhte Interesse der Bevölkerung an Inhalten und Dienstleistungen zur Überlastung der Server geführt haben.

12 https://www.cybercrimepolice.ch/de/fall/whatsapp-fake-kettenbrief-im-umlauf-migros-verlost-kostenlose-lebensmittel-im-wert-von-250-euro-um-die-nation-waehrend-der-corona-pandemie-zu-unterstuetzen/; https://www.cybercrimepolice.ch/de/fall/weiterer-whatsapp-fake-kettenbrief-angeblich-von-denner-im-umlauf/; https://www.cybercrimepolice.ch/de/fall/wieder-whatsapp-fake-kettenbrief-diesmal-im-namen-von-coop/; https://www.cybercrimepolice.ch/de/fall/neuer-whatsapp-kettenbrief-migros-verlost-gutscheine-in-hoehe-von-chf-180-/

13 https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response; https://hungarytoday.hu/coronavirus-govt-website-attack-shutdown/; https://www.lesechos.fr/tech-medias/high-tech/laphp-victimes-dune-cyberattaque-1188022; https://news.trust.org/item/20200401133925-o6wx4/

Empfehlungen:

In Unternehmen, die stark von der Verfügbarkeit von IT-Systemen abhängig sind, muss der Sicherung der entsprechenden Kanäle absolute Priorität eingeräumt werden. Eruieren Sie, welche Dienste so wichtig sind, dass deren Ausfall weitreichende Auswirkungen auf Ihre Organisation haben könnte. Denken Sie dabei auch an Basissysteme, ohne die Ihre kritischen Geschäftsanwendungen nicht funktionieren. Entwickeln Sie eine Strategie bezüglich DDoS-Attacken. Die zuständigen internen und externen Stellen sowie weitere Personen, die im Falle eines Angriffs agieren können, müssen bekannt sein. Idealerweise befasst sich ein Unternehmen im Rahmen des allgemeinen Risikomanagements schon vor einem Angriff auf Stufe der Geschäftsleitung mit der DDoS-Problematik und etabliert auf Betriebsebene eine gewisse DDoS-Abwehrbereitschaft. Ein DDoS-Angriff kann jede Organisation treffen. Sprechen Sie mit Ihrem Internet-Anbieter über Ihre Bedürfnisse und angemessene Vorkehrungen.

Checkliste mit Massnahmen gegen DDoS-Attacken:

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

3.3 Angriffe gegen Spitäler

Spitäler waren bereits vor der Pandemie auf der Zielliste von Cyberkriminellen und dabei insbesondere auch von Ransomware betroffen.[14] Durch die befürchtete pandemiebedingte Überlastung der Institutionen im Gesundheitswesen, erhielt jeder Zwischenfall in dieser Branche grosse Beachtung. Als am 16. März bekannt wurde, dass ein Spital in der Tschechischen Republik, welches auch ein wichtiges Corona-Testzentrum ist, infolge eines Ransomware-Vorfalls in seiner Funktion eingeschränkt wurde, war der internationale Aufschrei gross. Verschiedene Regierungen verurteilten solche Angriffe auf das Gesundheitswesen vehement und riefen zu internationaler Kooperation auf, um diesem Treiben Einhalt zu gebieten. Einige Ransomware-Akteure versprachen daraufhin von Angriffen auf Spitäler abzusehen. Dennoch hatten auch nachher noch verschiedene Spitäler Vorfälle mit Ransomware zu beklagen.[15] Mehrere Sicherheitsdienstleister boten an, betroffenen Institutionen des Gesundheitswesens kostenlos zu helfen.[16]

3.4 Cyber-Spionage

In der normalen Lage beschaffen Spione Informationen – gemäss den von ihren Regierungen vorgegebenen Prioritäten – die je nach Kontinent und Land sehr unterschiedlich sein können. Während der Pandemie hatten die Regierungen Interesse an den gleichen Informationen über das Virus und die dadurch verursachte Krankheit. Obwohl es sich um ein globales Problem

---

14 Siehe MELANI Halbjahresberichte 2016/1, Kap. 5.4.3; 2017/1, Kap. 3; 2019/1, Kap. 3; 2019/2, Kap. 4.6.1.

15 https://www.bleepingcomputer.com/news/security/ryuk-ransomware-keeps-targeting-hospitals-during-the-pandemic/; https://securityaffairs.co/wordpress/100548/malware/ryuk-ransomware-hospitals-covid19.html;

16 https://www.coveware.com/blog/free-ransomware-assistance-to-healthcare-coronavirus; https://cybersecurity.att.com/blogs/labs-research/a-surge-in-threat-activity-related-to-covid-19; https://coronahelp.isss.ch/

handelt, das die ganze Menschheit betrifft, arbeiten nicht alle Akteure bedingungslos zusammen. Verschiedene Länder vertrauen sich weder gegenseitig noch der Weltgesundheitsorganisation (WHO) und glauben, dass ihnen Informationen vorenthalten würden. Entsprechend schicken sie ihre Spione los, um solche Informationen zu beschaffen. Während die Aufklärung allenfalls geschönter Fallzahlen in einem Land für bessere Risikoeinschätzungen oder politische Propaganda genutzt werden kann, sind Informationen über die Tauglichkeit von Schutzmassnahmen, Behandlungsmethoden und Heilmittel unmittelbar hilfreich für die eigenen Massnahmen. Wenn es um potenzielle Impfstoffe geht, wird die Angelegenheit etwas komplizierter: Zwar forschen viele akademische Institutionen und andere Organisationen in diesem Bereich und tauschen sich gegenseitig aus. Es sind jedoch auch verschiedene private Unternehmen in diesem Bereich aktiv und erhoffen sich grosse Gewinne durch die Produktion von Eigenentwicklungen oder Patenten darauf. Die Herausforderung, ein wirksames Mittel zu finden und die Bevölkerung des eigenen Landes oder gar der ganzen Welt damit zu versorgen, ist eine wissenschaftliche und logistische, aber auch wirtschaftliche und politische Angelegenheit. Zu Spionage in Zeiten von COVID-19 siehe auch Kapitel 4.6.1.

Schlussfolgerung:

Alle in Forschung und Entwicklung im Bereich Pandemie tätigen Akteure müssen mit Spionageangriffen diversen Ursprungs rechnen. Sowohl staatliche, als auch private Organisationen sind an entsprechenden Daten, Forschungsergebnissen und Geschäftsgeheimnissen interessiert.

3.5 Homeoffice – aber sicher!

Die Digitalisierung im Arbeitsalltag hat durch die Pandemie einen grossen Schub erhalten. In vielen Unternehmen wurde Homeoffice eingeführt oder ausgebaut. Sitzungen fanden vermehrt per Telefon- oder Videokonferenz statt. Zum Teil haben Organisationen die kurzfristige Umstellung ihrer IT-Infrastruktur auf Homeoffice jedoch ohne adäquate Implementierung von Sicherheitsmassnahmen vollzogen und dadurch ihre Netzwerke exponiert.[17] Angreifer intensivierten ihre Scanning-Aktivitäten, um verwundbare Fernzugriffslösungen zu identifizieren und vorhandene Schwachstellen oder ungenügend geschützte Implementationen von *Remote Desktop Protocol (RDP)*-Lösungen und *Virtual Private Network (VPN)*-Server zu finden, um über diese in Firmennetzwerke einzudringen. Auch Phishing-Angriffe wurden gezielt auf die veränderte Arbeitssituation ausgerichtet. Viele Nutzende verwendeten zum ersten Mal Konferenz- und Kollaborationssoftware und von solchen Plattformen versendete Nachrichten waren ihnen nicht geläufig, weshalb entsprechende Fälschungen[18] für sie nicht einfach zu erkennen waren. Zu Homeoffice siehe auch Kapitel 6.1.

17 https://blog.shodan.io/trends-in-internet-exposure/

18 https://www.darkreading.com/cloud/fake-microsoft-teams-emails-phish-for-credentials/d/d-id/1337717; https://abnormalsecurity.com/blog/abnormal-attack-stories-microsoft-teams-impersonation/; https://abnormalsecurity.com/blog/abnormal-attack-stores-zoom-phishing-campaign/

Empfehlungen:

Die Nutzung von privater IT-Infrastruktur für das Homeoffice, insbesondere von privaten Computern, vergrössert die Angriffsfläche für Cyberangriffe, da private Netzwerke und persönliche Geräte häufig weniger gut geschützt sind, als von Profis administrierte Unternehmensinfrastrukturen. Auch bei der Erkennung von *Social-Engineering*-Angriffen sind Mitarbeitende im Homeoffice oft auf sich alleine gestellt, da sie verdächtige Ereignisse nicht unmittelbar mit Arbeitskolleginnen oder -kollegen besprechen können. Sensibilisierungskampagnen sowie die Etablierung und Bekanntmachung von Meldewegen an die IT-Sicherheitsverantwortlichen des Unternehmens können hier Abhilfe schaffen.

MELANI-Checklisten zu Homeoffice:

Für Unternehmen: https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/fernzugriff.html

Für Nutzende: https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/fernzugriff-enduser.html

3.6 Proximity Tracing Apps

Um die Ausbreitung des Coronavirus nachzuverfolgen und gezielt geeignete Schutzmassnahmen zu ergreifen, wurden in vielen Ländern so genannte Proximity oder Contact Tracing Apps eingeführt. Diese neue Technologie wird eingesetzt, um potenzielle Infektionsketten nachzuvollziehen und betroffene Personen über entsprechende Risiken zu informieren. Diese technischen Hilfsmittel können einen wichtigen Beitrag leisten, die Ausbreitung des Virus einzudämmen, indem sie Hinweise geben, wann sich jemand der Gefahr einer Infektion ausgesetzt hat. Betroffene Personen werden so informiert, dass sie sich testen lassen und vorläufige Massnahmen gegen eine unbewusste Weiterverbreitung ergreifen sollten.

Auch wenn sich alle das Ende der Pandemie herbeiwünschen, sind nicht alle gleich bereit, Daten preiszugeben, Einschränkungen zu akzeptieren oder Pflichten auferlegt zu bekommen. Die Lancierung von Tracing Apps führte in verschiedenen Ländern zu Kritik an der jeweiligen Ausgestaltung, sei dies wegen mangelndem Datenschutz oder allfälliger Sicherheitslücken. Es ist eine Herausforderung, die verschiedenen Interessen abzuwägen und eine Lösung zu finden, die von der jeweiligen Bevölkerung akzeptiert wird. Es handelt sich hier um eine neue Technologie, mit welcher erst Erfahrungen gesammelt werden muss und die über Zeit weiter reifen wird.

Hinweis:

Das NCSC hat im Rahmen des Schweizer Projekts COVID-19 Proximity Tracing zum Thema «Security & Privacy» eine Task Force gebildet, welche Fragen zum Thema Cybersicherheit und Schutz der Privatsphäre beurteilt. Mit einem Public Security Test wird durch weitere Fachleute und interessierte Personen die Sicherheit des gesamten Systems eingehend getestet. Der Public Security Test läuft seit dem 28. Mai 2020.

https://www.melani.admin.ch/melani/de/home/public-security-test/infos.html

4 Ereignisse / Lage

Meldeeingang Überblick

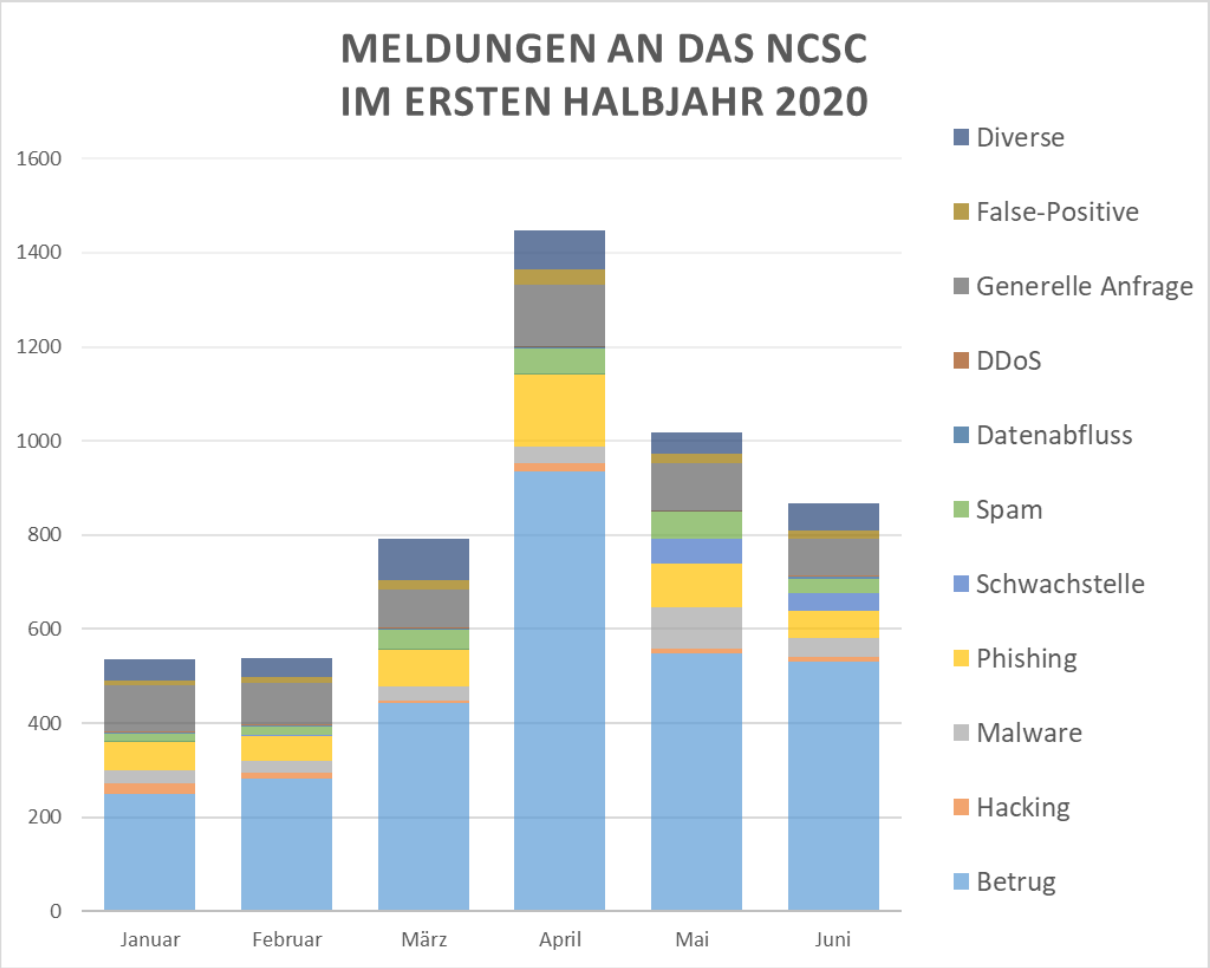

Abb. 2: Meldeeingang beim NCSC im ersten Halbjahr 2020.

Im ersten Halbjahr 2020 wurden bei der Nationalen Anlaufstelle Cybersicherheit im NCSC insgesamt 5'152 Meldungen registriert. Mit über der Hälfte respektive 2'938 Meldungen machten Betrugsversuche den grössten Anteil aus, davon betrafen alleine 825 Fälle E-Mails mit Vorschussbetrug.

Mit 270 Meldungen waren sogenannte Paket-Abofallen häufig. Diese Betrugsart ist eine Abwandlung der bereits seit langem bekannten Abofallen, wo vermeintlich kostenlose Angebote beworben werden, die sich dann nach einigen Tagen in kostenpflichtige Abonnemente umwandeln. Dies ist aber absichtlich nur im Kleingedruckten aufgeführt. In den im Sommer zirkulierten Varianten sollte für die angebliche Zustellung eines Paketes eine kleine Gebühr erhoben werden. Auch hier wurde allerdings unwissentlich ein Abonnement abgeschlossen. Kreditkartendaten mussten angegeben oder ein Code an eine Kurznummer gesendet werden. Die Betrüger haben sich in der Coronakrise auf diese neue Variante spezialisiert, weil viele Personen Online-Bestellungen tätigten und daher auf ein Paket gewartet haben (vgl. Kap. 3.1).

Ebenfalls wurden Erpresser E-Mails in grosser Zahl versendet. Fake-Sextortion[19] E-Mails machten dabei mit 578 Meldungen den grössten Anteil aus. Bei dieser Betrugsart wird behauptet, dass der Computer des Opfers gehackt wurde und Zugriff auf die Webcam bestehe, welche kompromittierende Aufnahmen gemacht haben soll. Dies ist in der Regel nicht der Fall und somit eine leere Drohung. Erpressungsversuche wurden im ersten Halbjahr 2020 ebenfalls gegen Webadministratoren beobachtet. In diesen E-Mails wurde behauptet, dass die Website gehackt und dahinterliegende Datenbanken gestohlen wurden. Schliesslich wurde mit der Veröffentlichung dieser Daten gedroht. Auch hier entsprach die Drohung nicht den Tatsachen (siehe dazu auch Kapitel 4.7.5). Dass Betrüger auch vor heftigeren Geschichten nicht zurückschrecken, zeigten zwei Bombendrohungen, die per E-Mail an Firmen versendet wurden, was sich ebenfalls als Täuschung entpuppte.

Eine alte Betrugsmasche feierte im ersten Halbjahr 2020 ihr Comeback. Der sogenannte Domainbetrug wurde 63 Mal gemeldet. Bei dieser Betrugsart meldet sich eine angebliche Domainverwaltungsfirma bei einem Websiteinhaber einer .ch-Domäne und behauptet, dass eine andere Firma Interesse an der entsprechenden .com-Domäne habe. Dies könne aber abgewendet werden, indem der Websiteinhaber diese .com-Domäne kaufe. Diese Domänen sind stark überteuert und es ist auch nicht sicher, ob diese Domänen dann tatsächlich registriert werden.

Von Firmen häufig gemeldet wurde der sogenannte CEO-Betrug (94 Meldungen). Die Täter informieren sich dabei im Vorfeld meist auf der Firmenwebsite über E-Mail Adressen und Funktionen der Mitarbeitenden. Aus diesen Informationen wird dann eine auf die Firma zugeschnittene Geschichte erfunden. Im Namen der Firmenchefs geben die Betrüger dann Anweisungen an die Buchhaltung oder die Finanzabteilung, eine dringende Zahlung vorzunehmen.

Vorfälle im Bereich Malware wurden 232 Mal gemeldet. Erwähnenswert sind hier 42 Meldungen von Fällen mit Verschlüsselungsschadsoftware (Ransomware). Diese Zahl ist zwar gegenüber den Betrugsversuchen gering, der potentielle Schaden ist aber um ein Vielfaches höher (siehe Kapitel 4.1.1).

4.1 Schadsoftware: Aktuelle Übersicht

Die untenstehende Statistik zeigt auf, von welcher Schadsoftware (Malware) die Schweizer Internet-Benutzenden am meisten betroffen sind. Diese Statistiken stammen aus verschiedenen Quellen und werden für den gesamten dem NCSC bekannten Schweizer IP-Raum aggregiert und gefiltert. Die technischen Detailinformationen werden den Schweizer ISPs zur Verfügung gestellt, damit sie betroffene Kunden über Infektionen informieren und Massnahmen empfehlen können. Die verschiedenen Malware-Familien sind manchmal schwer zu unterscheiden, da es kein internationales Namensschema gibt. Es ist wichtig zu beachten, dass diese Zahlen nur die Spitze des Eisbergs darstellen, da die Datenbank nur Daten von vereinzelten *Command and Control-Servern* enthält.

[19] https://www.melani.admin.ch/melani/de/home/meldeformular/formular0/meldeformularhaeufigefragen/Fake-Sextortion.html

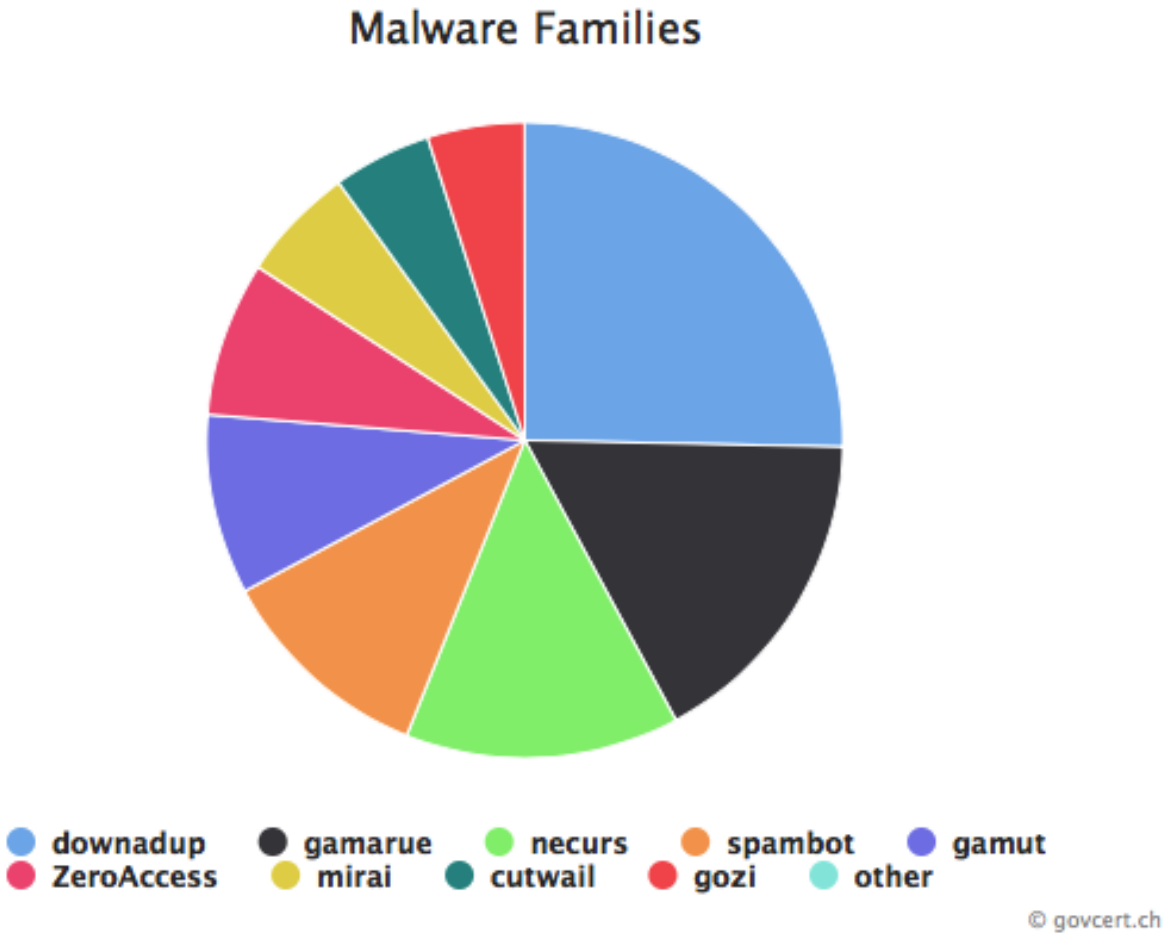

Abb. 3: Verteilung der Schadsoftware in der Schweiz, welche dem NCSC bekannt ist. Stichtag ist der 30. Juni 2020. Aktuelle Daten finden Sie unter: https://www.govcert.admin.ch/statistics/malware/

4.1.1 Ransomware Update

MELANI verfolgt das Phänomen Ransomware seit mehreren Jahren.[20] Diese kontinuierlich wachsende Bedrohung hat sich gemäss Statistiken der Firma Trustwave[21] im Jahr 2019 vervierfacht und nimmt mittlerweile bei der Rangliste der häufigsten Cybersicherheitsvorfälle den ersten Rang ein. Nicht nur die Anzahl der Infektionen mit Ransomware, sondern auch die Anzahl der Angriffsvektoren sowie der Dienste, die die Instrumente zur Durchführung eines Angriffs und Abhandlung der Lösegeldzahlung bereitstellen (*Ransomware-as-a-Service, RaaS*) nehmen zu. Ein Bericht der Firma Coveware,[22] die sich mit der Eindämmung von Ransomware-Angriffen befasst, hält fest, dass die Lösegeldforderungen im ersten Quartal des laufenden Jahres gegenüber den letzten Monaten des Jahres 2019 eine Steigerung um 33 Prozent verzeichnet haben.

---

[20] Siehe 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, 4.6.4 und 5.4.3; 2016/2, Kap. 4.6.3 und 6.1; 2017/1, Kap. 3; 2017/2, Kap. 5.4.2; 2018/2, Kap. 4.5.4 und 5.3.5; 2019/2, Kap. 4.6.1.

[21] https://www.zdnet.com/article/Ransomware-is-now-the-biggest-online-menace-you-need-to-worry-about/

[22] https://www.coveware.com/blog/q1-2020-Ransomware-marketplace-report

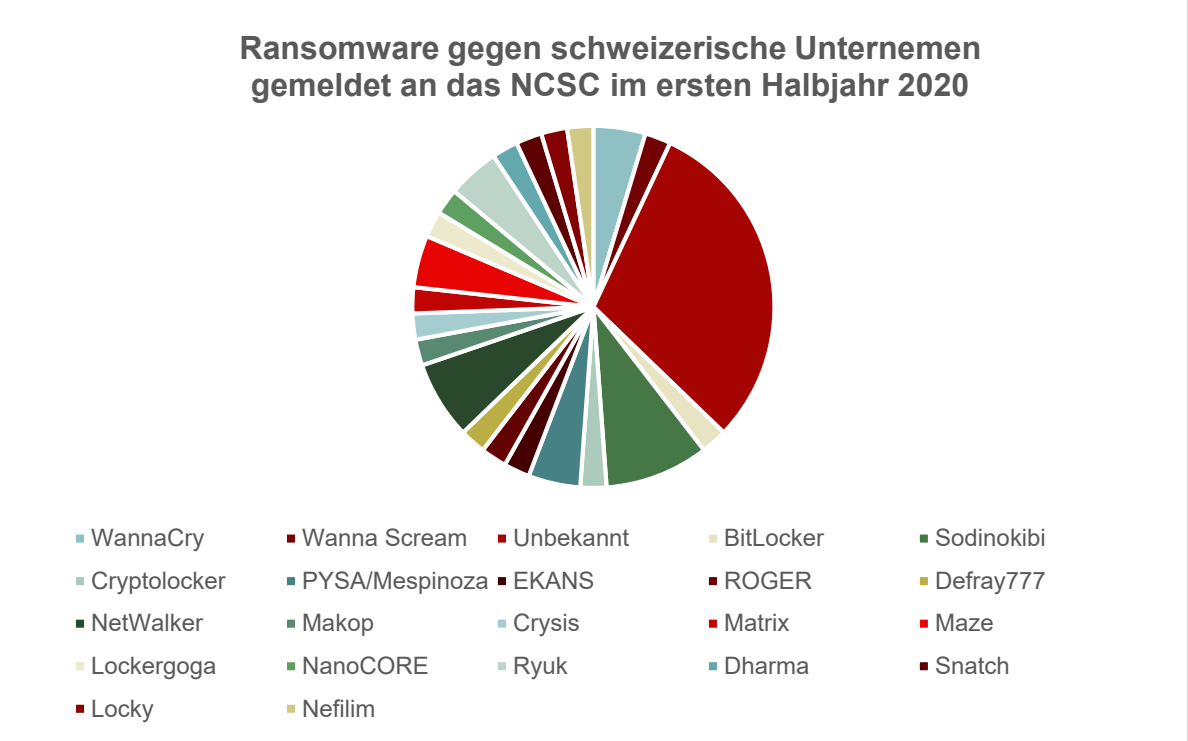

Abb. 4: Ransomware gegen schweizerische Unternehmen gemeldet an das NCSC im ersten Halbjahr 2020.

Auch im aktuellen Berichtszeitraum gerieten Schweizer Unternehmen ins Visier von Ransomware-Angriffen. Insgesamt wurden dem NCSC 42 Fälle von Ransomware-Angriffen gegen Firmen gemeldet. Leider enthielten nicht alle Meldungen Informationen über die bei dem Angriff verwendete Malware. Wie in Abbildung 4 ersichtlich wurden im Berichtszeitraum verschiedenste Arten von Ransomware-Angriffen gemeldet. Obwohl die Mehrzahl der Meldungen an das NCSC die KMU betrifft, waren auch grössere Firmen betroffen. Auf grosses Medieninteresse stiess der Angriff vom Januar auf Bouygues Construction, den französischen Baukonzern, der nach einem Angriff mit der Malware «Maze» in allen – auch den schweizerischen – Tochtergesellschaften die Produktion vorübergehend unterbrechen musste, um den Vorfall zu beheben.[23] Anfang Mai wurde der Schienenfahrzeughersteller Stadler Rail mit Ransomware angegriffen. Die Firma wurde mit der Drohung erpresst, die entwendeten Daten würden veröffentlicht, wenn sie das Lösegeld in Höhe von CHF 5,8 Millionen nicht bezahle.[24] Um die Wahrscheinlichkeit zu erhöhen, dass das Lösegeld tatsächlich ausgezahlt wird, passen die Kriminellen die geforderten Beträge an die ihrer Meinung nach finanziellen Möglichkeiten der Opfer an. Private Opfer müssen somit viel kleinere Beträge zahlen – oft weniger als CHF 1'000.-. Die geforderten Beträge unterscheiden sich auch stark von Kampagne zu Kampagne. «Ryuk», bekannt u. a. für happige Lösegeldforderungen, hat zum Beispiel von einem KMU rund CHF 300'000.- Lösegeld verlangt, während «WannaCry» von einem vergleichbaren Unternehmen lediglich CHF 1'500.- forderte, wobei nach der Zahlung nur ein Teil der Daten auch wirklich entschlüsselt wurde.

---

23 https://www.itnews.com.au/news/bouygues-construction-it-taken-out-by-Ransomware-537516

24 https://www.srf.ch/news/cyberAngriff-auf-stadler-rail-solange-es-etwas-zu-holen-gibt-wird-schindluder-getrieben; https://www.swissinfo.ch/eng/cyberattack-_hackers-demand-millions-in-ransom-for-stolen-stadler-rail-documents/45794036

Entwicklungen bei der Vorgehensweise

Bereits im November 2019 hatte eine Gruppe, die die Ransomware «Maze» benutzt, ihr Geschäftsmodell angepasst: Sie begann, vor der eigentlichen Verschlüsselungsattacke, die Daten des Opfers herunterzuladen, um daraufhin mit der Drohung der Publikation auf einem eigens dafür geschaffenen Blog Geld zu erpressen, falls die Erpressung mit der Verschlüsslung nicht zum gewünschten Erfolg führte. Diese Vorgehensweise ist deswegen erfolgversprechend, weil sie ausser einer Rufschädigung und der Publikation von Geschäftsgeheimnissen auch rechtliche Folgen im Zusammenhang mit der Bearbeitung der Personendaten haben kann. Zudem können die publizierten Daten für weitere Angriffe genutzt werden. Im ersten Halbjahr 2020 stieg die Zahl der Gruppen, die diese Strategie anwendeten, sehr stark. Die Cybersicherheitsfirma Coveware zählt ausser «Maze» sechs weitere Ransomware-Familien auf, welche im Zusammenhang mit Datenpublikationen festgestellt wurden: «Sodinokibi/REvil», «DoppelPaymer» (der Nachfolger von «BitPaymer»), «Mespinoza/PYSA», «NetWalker», «CLoP» und «Nephilim»[25] (wie auch seine neue Version Nemty).[26, 27] Alle diese Schadsoftwares sind auch in der Schweiz in Umlauf, doch nicht alle Infektionen, die MELANI gemeldet werden, sind mit einem Datenleck verbunden. Bei einem Ransomware-Angriff im Rahmen einer der genannten Kampagnen muss immer auch mit einem Datendiebstahl gerechnet werden. Betreiber von «Maze» behaupten, in der Schweiz nicht nur Stadler Rail verschlüsselt und seiner Daten beraubt zu haben, sondern auch die Versicherung Chubb, die die Infektion jedoch nicht bestätigt hat.[28]

Im letzten Halbjahresbericht[29] hat MELANI vorausgesagt, dass die Cyberkriminellen andere Mittel und Wege finden würden, um aus den entwendeten Daten (je nach ihrem Wert) Profit zu ziehen. Zum Beispiel indem sie sich nicht darauf beschränken, die Daten zur Ausübung von Druck zu benützen. Dies ist nun eingetreten: Jüngst haben die für die Verbreitung der Ransomware «Sodinokibi/REvil» verantwortlichen Cyberkriminellen gestohlene Daten versteigert, als die Opfer sich geweigert hatten, das Lösegeld für die Entschlüsselung zu bezahlen.[30] Andere Gruppen würden sogar doppeltes Lösegeld verlangen, erstens, um die verschlüsselten Dokumente zurückzuholen, zweitens, um die definitive Vernichtung der gestohlenen Daten zu gewährleisten.[31] Die Geldforderungen schwanken je nach Opfer und Kampagne, aber in einigen Fällen schiessen sie sprichwörtlich durch die Decke. Um nur ein Beispiel zu nennen: Im Juli forderte «Sodinokibi/REvil» von der Promi-Anwaltskanzlei Grubman Shire Meiselas & Sacks eine Lösegeldzahlung in der Höhe von USD 42 Millionen, damit die gestohlenen Daten nicht publiziert werden und um den Entschlüsselungscode zu erhalten. Weil das Opfer die

---

25 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/investigation-into-a-nefilim-attack-shows-signs-of-lateral-movement-possible-data-exfiltration/

26 Als weitere Illustration der Tatsache, dass dieses Schema bei den Cyberkriminellen zunehmend Anklang findet, kann die Gründung einer Plattform durch eine andere Ransomware gelten, auf der entwendete Daten publiziert werden, jedoch ohne bisherige Publikation eines Datenlecks. Es handelt sich um «Sekhmet», siehe auch: https://www.bleepingcomputer.com/news/security/three-more-Ransomware-families-create-sites-to-leak-stolen-data/

27 Hinzu kommt die Ransomware «RagnarLocker» (auch bekannt als «Ragnarok»), die in der Schweiz bisher noch nicht aufgetaucht ist: https://www.securityweek.com/ragnar-locker-Ransomware-uses-virtual-machines-evasion

28 https://www.bankinfosecurity.com/insurer-chubb-investigating-security-incident-a-14023

29 MELANI Halbjahresbericht 2019/2, Kapitel 4.6.1.

30 https://www.bleepingcomputer.com/news/security/revil-Ransomware-creates-ebay-like-auction-site-for-stolen-data/

31 https://krebsonsecurity.com/2020/06/revil-Ransomware-gang-starts-auctioning-victim-data/

Zahlung verweigerte, begannen die Erpresser eine Menge Dokumente über Persönlichkeiten aus dem Unterhaltungssektor zu versteigern, wobei die Anfangspreise zwischen USD 600'000 und einer Million lagen.[32] Der Verkauf von gestohlenen Daten über kriminelle Foren ist kein neues Phänomen, aber die Publikation und Verwendung als Druckmittel stellt eine neue Variante dar, die immer mehr Opfer dazu veranlassen könnte, nachzugeben und das Lösegeld zu bezahlen. Siehe auch Kapitel 4.5 zu Datenlecks.

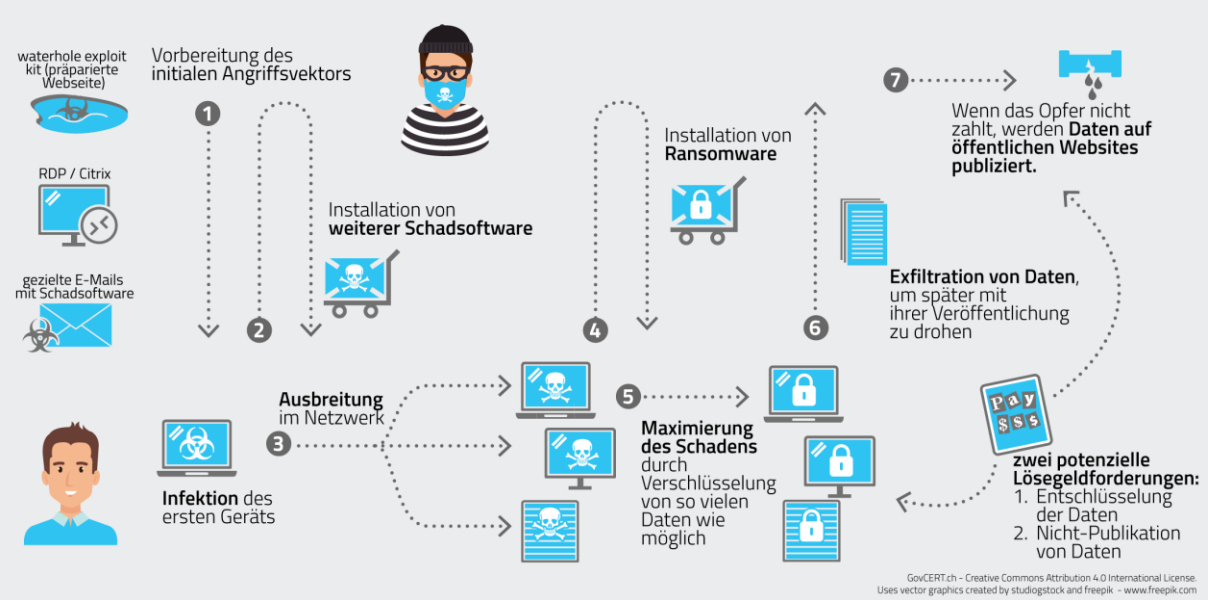

Abb. 5: Gegenwärtiger Modus Operandi bei Ransomware-Angriffen

Die Möglichkeit, üppige Gewinne zu erzielen und die Komplexität der mehrstufigen Angriffe haben dazu geführt, dass es immer mehr Zusammenarbeitsmodelle zwischen verschiedenen Gruppen sowie zwischen Gruppenmitgliedern und Freelancern gibt. Gemäss FireEye zum Beispiel werde die Ransomware «Maze» nicht von einer einzigen Gruppe genutzt, sondern verschiedene Akteure sind als partnerschaftliches Netzwerk (Affiliate-Netzwerk) organisiert. Anders ausgedrückt arbeiten die Entwickler von Ransomware mit anderen Akteuren zusammen, die beispielsweise die Schadsoftware-Verbreitung übernehmen, den Netzwerkzugang etablieren, für die Auskundschaftung von infizierten Netzwerken oder für andere spezifische Aspekte verantwortlich sind. Sie agieren entweder als Angestellte oder erhalten eine Kommission, sobald das Opfer das Lösegeld bezahlt hat.[33]

«Maze» wurde zunächst vor allem mit Hilfe infizierter E-Mails verbreitet; im ersten Halbjahr 2020 kam es vermehrt zu Infektionen mit dieser Ransomware im Rahmen strukturierter Angriffe, die eine bereits bestehende Infektion mit einer anderen Schadsoftware nutzen und vor der Verschlüsselung einen umfassenden Datendiebstahl durch eine feinmaschigere Infiltration des Netzes ermöglichen. Der Sicherheitsdienstleister FireEye stellte grosse Unterschiede im Ablauf der beobachteten Angriffe fest, beispielsweise hinsichtlich der Zeitspanne zwischen der Anfangsinfektion und der Verwendung der Ransomware oder hinsichtlich des verwendeten

32 https://www.scmagazine.com/home/security-news/cybercrime/lebron-james-among-the-1st-stars-to-have-their-stolen-law-firm-files-put-up-for-auction/

33 https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-Ransomware-incidents.html

Intrusionsvektors (zum Beispiel offene RDP-Ports oder andere via Internet zugängliche und schlecht konfigurierte Dienste, solche mit schwachen Passwörtern oder via zuvor abgeflossene und nun im Darknet angebotene Zugangsdaten). Es gibt auch grosse Unterschiede bezüglich der Strategien für eine grössere Beständigkeit der Präsenz (engl.: *persistence*) im Netzwerk oder die Möglichkeit der Interaktion mit den Systemen des Opfers in den einzelnen Phasen der Auskundschaftung und der Ausbreitung im Netzwerk (engl.: *lateral movement*). Diese Vielfalt wird als weiterer Hinweis auf die Beteiligung mehrerer Akteure gedeutet. «Maze»-Betreiber haben ausserdem auf ihrer Website Daten veröffentlicht, die bei einem Architekturbüro von «LockBit»-Betreibern gestohlen wurden. Ein Mitglied der «Maze»-Gruppe hatte erklärt, sie seien bereit, demnächst auch mit einer dritten Gruppe Arbeitsbeziehungen aufzunehmen.[34]

«Maze» ist nicht die einzige Ransomware, bei welcher die Betreiber auf die Strategie der «vereinten Kräfte» setzt. Auch die Operatoren von «NetWalker» bauen seit März 2020 Affiliate-Netzwerke auf, die an Fachtagungen im Rahmen eines «Underground-Blogs» ihre Ransomware propagieren. Um Partner zu rekrutieren, werden kolossale Entschädigungen in Höhe von 70 Prozent eines Lösegelds versprochen; das stellt Einkünfte von USD 487'000 bis zu sage und schreibe einer Million in Aussicht. Zudem wurde auch für «NetWalker» eine Plattform zur Veröffentlichung der entwendeten Daten geschaffen. So können ihre Partner zwecks Optimierung der Gewinne der verschiedenen Angriffe selbständig Informationen über die Opfer der erzielten Infektionen publizieren.[35]

Technische Entwicklungen

Im letzten Halbjahresbericht[36] wurde bereits darauf eingegangen, dass eine Ransomware-Infektion in vielen Fällen keine Interaktion der Nutzenden erfordert. Zusammen mit anderen Besonderheiten, zum Beispiel der Möglichkeit, dieselbe Malware für eine grosse Anzahl von Opfern zu verwenden, erklärt dies den Erfolg dieses Phänomens. Einer der häufigsten Angriffsvektoren, der bei Ransomware-Kampagnen zwischen Januar und Juni 2020 ausgenutzt wurde, um sich in ein Firmennetz einzuschleichen, waren die nur ungenügend geschützten *RDP*-Ports,[37] deren Berechtigungen auf dem Schwarzmarkt zu sehr tiefen Preisen erworben werden können. Auch Server mit Sicherheitslücken können als Einfallstore zur IT-Infrastruktur ausgenützt werden. Im ersten Halbjahr 2020 war die Schadsoftware «Sodinokibi/REvil», die bereits über Sicherheitslücken in *VPN* Produkten der Firma Pulse Secure eingeschleust worden war, die erste Ransomware, die unter Ausnutzung der Citrix-Schwachstelle «CVE-2019-19781» (siehe Kap. 4.4) in einem Firmennetz platziert wurde. Im Berichtszeitraum wurden nebst «Sodinokibi/REvil» zwei weitere Ransomware beobachtet, «Maze» und «RagnarLocker», die diese Schwachstelle als Penetrationsvektor benützen.[38] Auch in der Schweiz wird

---

34 https://www.scmagazine.com/home/security-news/Ransomware/new-Ransomware-trends-spotted-auctioning-stolen-files-cybergangs-joining-forces/

35 https://www.bleepingcomputer.com/news/security/Ransomware-recruits-affiliates-with-huge-payouts-automated-leaks/

36 MELANI-Halbjahresbericht 2019/2, Kap. 4.6.1.

37 Auch das FBI vertritt diese Ansicht; es erklärte an der RSA-Sicherheitskonferenz vom Februar 2020, dass in 70-80 Prozent der Ransomware-Angriffe ein Zugang via RDP-Port als Angriffsvektor verwendet wird: https://www.bleepingcomputer.com/news/security/Ransomwares-big-jump-ransoms-grew-14-times-in-one-year/

38 https://www.zdnet.com/article/hackers-target-unpatched-citrix-servers-to-deploy-Ransomware/

nicht ausgeschlossen, dass es über verwundbare Pulse Secure VPN- und Citrix-Server zu Infektionen gekommen ist.

Die letzten Monate hindurch hat das NCSC eine starke Zunahme von Attacken auf RDP (Remote Desktop Protocol) als initialem Angriffsvektor für gezielte Ransomware Angriffe festgestellt. Es gibt eine Vielzahl an Scans gegen RDP Ports, bei denen die Angreifer versuchen, schwache Passwörter auszunutzen (durch Dictionary und Brute Force Angriffe). Eine weitere Taktik ist das Ausnützen von nicht gepatchten und damit verwundbaren Servern. Dasselbe Vorgehen hat das NCSC bei anderen, exponierten Protokollen für den Remote Zugriff beobachtet, so z. B. bei Pulse Secure VPN, oder bei Citrix NetScaler Verwundbarkeiten, welche beispielsweise von «REvil» gesucht und als initialer Vektor genutzt werden. Das NCSC geht davon aus, dass solche Zugangsdaten auch in entsprechenden Foren von Kriminellen gehandelt werden und auf diese Weise verschiedene Angreifergruppierungen Zugänge zu diesen Netzen erlangen können.

Empfehlung:

Folgende Massnahmen sollten so rasch als möglich umgesetzt werden:

- Alle Remote Zugänge (RDP, Citrix, VPN) müssen mit einer Zwei-Faktor Authentifizierung geschützt werden
- Zusätzlich können sie auf einen nicht-Standardport gelegt werden, so dass sie schwieriger aufzufinden sind (Vorsicht: Dies alleine ist keine ausreichende Sicherheitsmassnahme).
- Einführen und Durchsetzen einer Passwortrichtlinie, welche einfache Passwörter verhindert.
- Falls möglich: Nur einzelne respektive bestimmte IP-Adressen zulassen, z. B. nur IP-Adressen aus der Schweiz.
- Überwachen der Logfiles auf fehlgeschlagene und erfolgreiche Logins.

Im Berichtshalbjahr wurden einige Ransomware-Angriffe beobachtet, die innovative Techniken verwendeten, um Sicherheitsmassnahmen zu umgehen und sich länger im Netz des Opfers zu halten. «RagnarLocker» zum Beispiel installierte eine eigene 280 MB grosse virtuelle Windows XP-Maschine (Virtual Machine, VM), um darin ungestört von den Monitoring Programmen des Hosts zu laufen. Sämtliche Laufwerke des betroffenen Computers wurden auch innerhalb der VM zugänglich gemacht und konnten so durch die Ransomware verschlüsselt werden.[39] «NetWalker» hingegen hat eine bereits von anderen Malware-Typen verwendete Technik entwickelt, die «Reflective DLL injection» genannt wird. Sie erlaubt die Einspeisung einer DLL-Datei (*dynamic-link library*), deren Ausführungscode für die Schadsoftware sich nur im Arbeitsspeicher befindet. Das bedeutet, dass der binäre Code der Ransomware für Monitoring-Instrumente, die nur die Festplatte untersuchen, unauffindbar bleibt.[40] Als weitere Massnahme blockiert «NetWalker» zudem Prozesse von Sicherheitsprogrammen.

39 https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-virtual-machine-to-dodge-security/

40 https://blog.trendmicro.com/trendlabs-security-intelligence/netwalker-fileless-Ransomware-injected-via-reflective-loading/

Weiterentwicklung der Ziele

Ein global auftretender besorgniserregender Trend betrifft Ransomware-Angriffe gegen industrielle Kontrollsysteme. MELANI widmet diesem Phänomen in diesem Halbjahresbericht ein separates Kapitel (s. Kap. 4.3.1).

Eine weitere, neulich zu beobachtende Entwicklung hängt mit der «Maze»-Infektion zusammen, die Cognizant, einer der weltweit grössten Managed Service Anbieter (MSP), am 18. April bekanntgab.[41] Dieser Vorfall reiht sich in die lange Serie von Angriffen gegen Service- und IT-Provider im zweiten Halbjahr 2019 ein,[42] angesichts derer gemäss dem im März erschienenen Bedrohungsanalysebericht von CrowdStrike von einem echten Trend gesprochen werden kann.[43] Aus den besonders gegen Service Provider aktiven Ransomware sticht «Ryuk» hervor, zu dessen Opfern mindestens Data Resolution (Dezember 2018), CloudJumper (Mai 2019), CorVel (Juli 2019) und TSM Consulting (August 2019) gehören. Im März 2020 hat «Ryuk» zudem den Finanztechnologiedienstleister Finastra infiziert, der über 8'500 Kundinnen und Kunden Software und Dienste liefert, darunter 90 der 1'000 weltweit grössten Banken. Um eine Verbreitung der Infektion abzuwenden, hat Finastra rasch einen Teil seiner Server deaktiviert, was für die zahlreichen Kunden des Dienstes zu einem vorübergehenden Unterbruch führte.[44] Die Infektion eines MSP oder eines Lieferanten von Cloud-Leistungen hat das Potenzial für riesige Schäden, weil er als Einfallstor in die Unternehmen dienen kann, deren IT-Infrastruktur von den Obengenannten betrieben wird, z. B. unter Ausnützung der Monitoring- und Fernsteuerungssoftware (*Remote Monitoring and Management*, RMM). Deshalb hat Cognizant seine Kundschaft umgehend informiert und Erkennungsmerkmale (*Indicators of Compromise*, IoC) geliefert, um allfällige Infektionen im eigenen Netz erkennen zu können.

Um weniger aufzufallen, haben sich einige Ransomware-Angreifer darauf spezialisiert, als Einfallstor die Programme zu verwenden, die von den MSP benutzt werden wie beispielsweise Desktop-Sharing- oder Fernzugriffssoftware. Auf diese Weise wurde im April der Konzern Energias de Portugal (EDP), einer der grössten Energieproduzenten Europas, mit «Ragnar-Locker» angegriffen. Einige Ransomware-Gruppen, z. B. «Sodinokibi/REvil», gehen den umgekehrten Weg: Nach Angriffen auf verschiedene kleine MSPs, u. a. PerCSoft (August 2019), Complete Technology Solutions (Dezember 2019) und Synoptek (Januar 2020) schien die Gruppe laut Coveware seit Anfang 2020 mehr an Grossunternehmen mit verwundbarem VPN interessiert zu sein.

41 https://www.bleepingcomputer.com/news/security/it-services-giant-cognizant-suffers-maze-Ransomware-cyber-attack/

42 https://www.zdnet.com/article/at-least-13-managed-service-providers-were-used-to-push-Ransomware-this-year/

43 https://www.channelfutures.com/mssp-insider/msps-under-heavy-Ransomware-attack ; https://www.crowdstrike.com/press-releases/crowdstrike-global-threat-report-reveals-big-game-hunting-telecommunication-targeting-top-adversary-trends/

44 https://www.bloomberg.com/news/articles/2020-04-08/how-finastra-survived-a-Ransomware-attack-without-paying-ransom

Empfehlungen:

Für Unternehmen haben sich folgende Massnahmen bewährt, um sich vor Ransomware-Angriffen zu schützen: Achten Sie auf vollständige Datensicherungspraktiken (Backup). Dies kann die Sicherheit erhöhen, nach einer Ransomware-Attacke sämtliche Daten wiederherstellen 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 Vorfallbewältigung, 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

4.1.2 «Gozi» erneut aktiv

Die für Angriffe auf E-Banking entwickelte Malware «Gozi»[45] ist seit über zehn Jahren in der Schweiz präsent, doch in den letzten Jahren war sie nur sporadisch aktiv.

Im März dieses Jahres wurde beobachtet, dass «Gozi» mit E-Mails verbreitet wurde, die auf eine reale frühere E-Mail-Korrespondenz des Opfers Bezug nahm (sog. *thread hijacking*). Diese Methode wird bereits von anderen Banken-Trojanern, u. a. «Emotet», eingesetzt. Das E-Mail enthielt ein Passwort, mit dem eine .zip-Datei geöffnet werden konnte, die allerdings nicht im Anhang, sondern auf Google Drive gespeichert war. Im Archiv befand sich vermeintlich eine Präsentation. Tatsächlich handelte es sich um eine Javascript-Datei, welche «Gozi» herunterlud und ausführte. Im April wurde «Gozi» dann in einer infizierten .xls-Datei als Anhang versendet. Die auf Italienisch verfassten E-Mails nahmen jeweils Bezug auf eine Rechnung.

Die Malware «Gozi» und ihre Varianten, die auf illegalen Online-Handelsplattformen angeboten und deshalb von verschiedenen Cyberkriminellen benutzt werden, wurden seit Jahren auf verschiedene Art verbreitet, u. a. über kompromittierte Websites von Online-Tageszeitungen

[45] GovCERT Blogs zu Gozi: https://www.govcert.admin.ch/blog/18/gozi-isfb-when-a-bug-really-is-a-feature; https://www.govcert.ch/blog/when-gozi-lost-its-head/ (beide in Englisch)

sowie manipulierte Software, die in explizit dafür hergestellten Inseraten beworben wurde. «Gozi» nimmt nebst E-Banking-Systemen auch Zahlungs-Software und Wallets für Kryptowährungen ins Visier.[46]

4.1.3 Bisher verborgenes Modul von «Emotet»

Anfang 2020 haben Sicherheitsforscher von Binary Defense ein WLAN-Modul in der Malware «Emotet» entdeckt.[47] Mit diesem bisher kaum erforschten Modul werden die drahtlosen Netze (*wireless local area network*, WLAN) abgefragt, mit denen das Opfer verbunden ist. Zudem versucht «Emotet» mit einer vordefinierten Liste von gängigen Passwörtern auf alle anderen drahtlosen Netzwerke zuzugreifen, die sich in Reichweite befinden. Ist ein WLAN gar nicht geschützt oder mit einem auf der vordefinierten Liste enthaltenen Passwort gesichert, kann «Emotet» auf dieses Netzwerk zugreifen. Ausgehend vom ersten Opfer wird die Malware dann die Computer im Netzwerk, in das sie eingedrungen ist, infizieren und sich dort verbreiten.

Nach ersten Erkenntnissen scheint das Modul seit 2018 zu existieren. Da Malware-Analysen zumeist auf virtuellen Maschinen ohne WLAN durchgeführt werden, war es aber lange nicht aufgefallen. Diese Entdeckung illustriert, dass Angreifer immer neue Wege suchen, Schadsoftware zu verbreiten und es ihnen dabei nicht an Kreativität mangelt.

«Emotet» ist oft ein Einfallstor für weitere Malware wie Verschlüsselungstrojaner (Ransomware).[48]

Schlussfolgerung:

Die Verbreitung von Schadsoftware ist ein ständiges Katz- und Mausspiel zwischen den Angreifern und den Verteidigern. Wenn der Erfolg mit angewandten Methoden nachlässt, weil ein Verbreitungsvektor besser abgesichert wurde, finden Schadsoftware-Entwickler neue Infektionsvarianten oder lassen alte wiederaufleben, auf die von Sicherheitsexperten weniger geachtet wird. WLAN als erste Netzwerkkomponente für die Verbindung ins Internet ist als Vektor lokal begrenzt und skaliert nicht gleich, wie Angriffe über E-Mail und das Web. WLAN als Angriffsvektor sollte dennoch nicht unterschätzt werden.

Auf unserer Website finden Sie Empfehlungen zu WLAN Sicherheit:

https://www.melani.admin.ch/melani/de/home/schuetzen/sekundaere-grundschutz.html

46 MELANI Halbjahresbericht 2018/1, Kap. 4.7.3.

47 https://www.binarydefense.com/emotet-evolves-with-new-wi-fi-spreader/

48 Siehe hierzu MELANI Halbjahresberichte 2019/1, Kap. 3.4.1 und 2019/2, Kap. 4.6.1.

4.2 Angriffe auf Websites und –dienste

4.2.1 HPC Supercomputer

Mitte Mai 2020 meldete das Sicherheitsteam von EGI (European Grid Infrastructure, ein Zusammenschluss von Universitäten mit Hochleistungsrechenzentren) einen Angriff, von dem mehrere EGI-Mitglieder betroffen waren.[49] Hochleistungsrechenzentren (*High-performance Computing*, HPC) sind ein wichtiges Instrument zur Lösung komplexer Berechnungen wie etwa aerodynamischen Modellierungen oder aktuell COVID-19-Ausbreitungsmodellen. Die Rechenleistung kann auch zum Schürfen von Kryptowährungen (engl.: *crypto mining*) oder zur Dechiffrierung von verschlüsselten Daten verwendet werden. Ausserdem verfügen die Zentren über erhebliche Bandbreiten. HPC sind deshalb interessante Angriffsziele. Dank dem Bericht des EGI-Sicherheitsteams konnten viele Rechenzentren weltweit, darunter mehrere in der Schweiz,[50] unerlaubte Zugriffe auf ihre Systeme eruieren und die eingedrungenen Angreifer abwehren. Das Ziel der Angreifer ist bislang nicht bekannt.

4.2.2 DDoS Update

DDoS-Angriffe zielen darauf ab, die Verfügbarkeit eines Informatiksystems zu stören, um dann von der betroffenen Organisation Geld zu erpressen oder ihr durch die Unerreichbarkeit ihrer Websites und Dienste Schaden zuzufügen. Erfolgreiche DDoS-Angriffe haben in den vergangenen Jahren zahlenmässig abgenommen. Zu verdanken ist dies den Akteuren, die sich im Bereich der Informatiksicherheit auf die DDoS-Bekämpfung spezialisiert haben. Bei Link11, einem Dienstleister zur Eindämmung von DDoS, betrug der grösste im ersten Quartal 2020 abgewehrte Angriff 406 Gbit/s, während Cloudflare einen DDoS-Angriff mit einem Spitzenwert von über 550 Gbit/s erlebte.[51]

Diese Dienste stellten gegenüber dem Vorjahr eine Zunahme der Komplexität und des Volumens von solchen Angriffen fest. In den ersten drei Monaten dieses Jahres verzeichnete Link11 ganze 51 Angriffe mit einem Volumen von mehr als 50 Gbit/s, während die mittlere Bandbreite 5,0 Gbit/s erreichte (was eine Steigerung um 0,7 Gbit/s im Vergleich zum Vorjahresquartal darstellt).[52] Cloudflare berichtet über eine Zunahme von kleinen Angriffen von kurzer Dauer, von denen 92 Prozent nicht einmal 10 Gbit/s erreichen. Zudem dauerten 79 Prozent der Angriffe zwischen 30 und 60 Minuten, was gegenüber dem zweiten Semester 2019 bei den kurzen Angriffen einem Anstieg von 19 Prozent entspricht.[53]

Die Menge der von Cloudflare verzeichneten DDoS-Angriffe ist offenbar vor allem seit März, parallel zur COVID-19-Pandemie, gewachsen. Diese Feststellung wurde von anderen IT-Sicherheitsfirmen bestätigt, unter anderem von Netscout, das festhält, in einem Zeitfenster von 31 Tagen noch nie eine solche Anzahl DDoS-Angriffe registriert zu haben wie zwischen dem 11. März und dem 11. April 2020 (über 864,000).[54] Die Cyberkriminellen hätten sich wegen

---

49 https://csirt.egi.eu/academic-data-centers-abused-for-crypto-currency-mining/

50 https://www.rts.ch/info/suisse/11329094-soupcons-de-hacking-du-plus-gros-superordinateur-de-suisse-.html; https://www.tagesanzeiger.ch/eth-supercomputer-gehackt-370887112689

51 https://www.zdnet.com/article/aws-said-it-mitigated-a-2-3-tbps-ddos-attack-the-largest-ever/

52 https://www.helpnetsecurity.com/2020/04/20/ddos-attacks-increasing/

53 https://blog.cloudflare.com/network-layer-ddos-attack-trends-for-q1-2020/

54 https://www.netscout.com/blog/asert/measuring-cruellest-month

der Verlagerung der täglichen Aktivitäten wie Arbeit (Homeoffice) und Schule (Homeschooling) auf Online-Lösungen und der damit einhergehenden Abhängigkeit von Konnektivität und Diensterreichbarkeiten eine mögliche Wirkungssteigerung solcher Angriffe versprochen. Die Politik des Social Distancing in mehreren Staaten hat die Abhängigkeit ihrer Volkswirtschaften vom Netz sowie die Bedeutung einiger Online-Informationskanäle vergrössert. Dies trifft zum Beispiel auf die Websites der Regierungsstellen zu, die für die öffentliche Gesundheit zuständig sind. Sie wurden täglich von zahlreichen Bürgerinnen und Bürgern besucht, die sich über das Coronavirus informieren wollten. In diesem Zusammenhang war die Website des US-Gesundheitsministeriums Mitte März von einem DDoS-Angriff betroffen, der die Systeme der Regierungsbehörde jedoch nicht signifikant zu verlangsamen vermochte.[55] Dank DDoS-as-a-service-Anbietern kann ein solcher Angriff rasch und kostengünstig ausgeführt werden. Das NCSC hat in der Schweiz keine signifikante Zunahme von DDoS-Angriffen während der ausserordentlichen Lage verzeichnet. Generell konnten in der ersten Jahreshälfte 2020 in der Schweiz einige unspezifische Angriffswellen beobachtet werden, die meisten davon ohne Lösegeldforderung. Dies weist darauf hin, dass die Akteure lediglich die getroffene Infrastruktur testen oder Schwachstellen finden wollten.

Zwischen all diesen schwachen und kurzen Angriffen fanden jedoch auch zwei Angriffe statt, die zu den grössten je registrierten Angriffen dieser Art gehören. Der erste Angriff Mitte Februar wurde durch den Schutz von Amazon (AWS Shield) eingedämmt, dauerte drei Tage und erreichte eine Verkehrsspitze von 2,3 Tbit/s. Der Angriff richtete sich gegen einen spezifischen Kunden, der von Amazon jedoch nicht genannt wurde.[56] Der zweite Angriff, der sich gegen eine europäische Bank richtete und Ende Juni stattfand, zeichnete sich nicht primär durch eine hohe Bandbreitenintensität (knapp 418 Gbit/s), sondern durch den intensivsten, je registrierten Datenpaketfluss pro Sekunde aus: 809 Millionen p/s.[57] Vor diesem, durch den Infrastrukturdienstleister Akamai eingedämmten Angriff, hatte der stärkste jemals bekanntgewordene derartige DDoS-Angriff rund 580 Millionen Pakete pro Sekunde erreicht.[58] Die beiden Angriffe im ersten Semester 2020 dürfen für sich in Anspruch nehmen, die grössten je erfassten DDoS-Vorfälle zu sein. Die Schwierigkeit, den grösseren Angriff der beiden festzulegen, liegt darin, dass die Angreifer unterschiedliche Methoden verwendeten, um ihr Ziel zu treffen: Bit pro Sekunde (bit/s) im ersten Fall und Pakete pro Sekunde (p/s) im zweiten Fall. Angriffe mit hoher bit/s-Zahl bezwecken die Lahmlegung der Internet-Pipeline, während es bei den Angriffen mit hoher p/s-Zahl darum geht, Netzdispositive oder Apps in Datacenters oder in einer Cloud zu treffen.[59] Der Angriff vom Februar hat ein Paketvolumen von 293 Millionen p/s erreicht, was viel weniger ist als im Juni. Ein dritter Angriff mit einer Spitze von 754 Millionen p/s wurde zwischen dem 18. und 21. Juni registriert. Der viertägige Angriff wurde von über 316'000 IP-Adressen gegen eine Adresse von Cloudflare ausgeführt.[60]

---

55 https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response

56 https://www.zdnet.com/article/aws-said-it-mitigated-a-2-3-tbps-ddos-attack-the-largest-ever/

57 https://blogs.akamai.com/2020/06/largest-ever-recorded-packet-per-secondbased-ddos-attack-mitigated-by-akamai.html

58 https://www.imperva.com/blog/this-ddos-attack-unleashed-the-most-packets-per-second-ever-heres-why-thats-important/

59 https://www.bleepingcomputer.com/news/security/european-bank-suffers-biggest-pps-ddos-attack-new-botnet-suspected/

60 https://blog.cloudflare.com/mitigating-a-754-million-pps-ddos-attack-automatically/

Empfehlungen:

In Unternehmen, die stark von der Verfügbarkeit von IT-Systemen abhängig sind, muss der Sicherung der entsprechenden Kanäle absolute Priorität eingeräumt werden. Eruieren Sie, welche Dienste so wichtig sind, dass deren Ausfall weitreichende Auswirkungen auf Ihre Organisation haben könnte. Denken Sie dabei auch an Basissysteme, ohne die Ihre kritischen Geschäftsanwendungen nicht funktionieren. Entwickeln Sie eine Strategie bezüglich DDoS-Attacken. Die zuständigen internen und externen Stellen sowie weitere Personen, die im Falle eines Angriffs agieren können, müssen bekannt sein. Idealerweise befasst sich ein Unternehmen im Rahmen des allgemeinen Risikomanagements schon vor einem Angriff auf Stufe der Geschäftsleitung mit der DDoS-Problematik und etabliert auf Betriebsebene eine gewisse DDoS-Abwehrbereitschaft. Ein DDoS-Angriff kann jede Organisation treffen. Sprechen Sie mit Ihrem Internet-Anbieter über Ihre Bedürfnisse und angemessene Vorkehrungen.

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 Industrielle Kontrollsysteme

Die zunehmende Digitalisierung und Vernetzung im Bereich der Grundversorgung führt zwar zu effizienterer Bewirtschaftung von Leistungen wie Strom- und Wasserversorgung, birgt jedoch auch Risiken bezüglich Verwundbarkeit und damit ihrer Zuverlässigkeit. Während solche Systeme traditionell lokal oder regional beschränkt waren und vielfach über eigene physische Netze bedient wurden, sind sie nun zunehmend auch aus der Ferne über das Internet steuerbar. Idealerweise sind entsprechende Bedienelemente jedoch nicht direkt vom Internet aus erreichbar, sondern durch verschiedene Schutzmassnahmen vor unbefugtem Zugriff gesichert.

4.3.1 Industrielle Kontrollsysteme (ICS) im Visier von Ransomware

Wie im Kapitel 4.1.1 aufgezeigt, nahm die Anzahl der Angriffe mit Ransomware weltweit weiter zu. Bisher hatten es Angriffe mit Ransomware auf die IT-Infrastruktur der Opfer abgesehen und Kontrollsysteme meist nur kollateral in Mitleidenschaft gezogen. Im ersten Halbjahr 2020 wurde nun eine Ransomware beobachtet, die eigens dazu entworfen worden war, Prozesssteuerungen zu treffen. Gemeint ist «EKANS». Aktiv ist «EKANS» seit Dezember 2019, doch bekannt wurde die Ransomware erst Anfang Jahr.[61] Sie verfügt über spezifische Fähigkeiten, um Prozesse im Zusammenhang mit industriellen Kontrollsystemen anzugreifen. «EKANS», die or allem für gezielte Angriffe eingesetzt wird, überprüft nach dem Eindringen ins Netz, ob die internen Domains und die IP-Adressen mit dem Ziel übereinstimmen. Bevor die Ransomware Dateien verschlüsselt, entwendet sie Daten und erzwingt danach den Stillstand einer ganzen Reihe von Prozessen, ohne diese jedoch zu manipulieren oder Befehle zu versenden.

61 https://www.bloomberg.com/news/articles/2020-01-28/-snake-Ransomware-linked-to-iran-targets-industrial-controls; https://www.otorio.com/blog/snake-industrial-focused-Ransomware-with-ties-to-iran/

Diese Prozesse betreffen nicht nur die industriellen Kontrollsysteme (ICS), sondern auch Sicherheits- oder Management-Software, Datenbanken und Daten-Backup-Lösungen. Der Lieferant von Sicherheitsdiensten, Dragos, der über diese Bedrohung einen detaillierten Bericht veröffentlicht hat, nennt unter den angegriffenen ICS-Produkten die Software «Proficy Historian» von General Electric und die Server für die Konzession von Lizenzen von «GE Fanuc ma», aber auch die Anwendung «HMIWeb» von Honeywell und die Lizenzverwalter «FLEXNet», «Sentinel HASP» und «ThingWorx Industrial Connectivity Suite».[62] Nach der Verschlüsselung der Dateien zeigt «EKANS» eine Lösegeldforderung an.

«EKANS» wurde anfänglich als Vorreiter für diese Art von Angriffen gesehen. Doch Dragos hat im Rahmen der Analyse der Malware signifikante Analogien zu einer Variante der Ransomware «MegaCortex» festgestellt, die bereits seit dem vergangenen Sommer industrielle Kontrollsysteme ins Visier nahm. Durch die Entdeckung dieser Ähnlichkeiten wurde die Bedeutung von «EKANS» etwas relativiert. Auch weil die Liste der Prozesse, die «MegaCortex» ins Visier nimmt (über 1'000), länger ist als diejenige von «EKANS» (64). Während bei beiden Ransomware dieselben Industriekontrollprozesse betroffen sind, blockiert «MegaCortex» auch unzählige Sicherheitsprozesse. Die einzige nennenswerte Entwicklung von «EKANS» wäre die Obfuskation, die Verschleierung des Programmcodes, um die Entdeckung zu erschweren.

Diese beiden Ransomware stellen für den Industriesektor und für viele kritische Infrastrukturen eine Bedrohung dar. Ransomware, die grundsätzlich die IT-Infrastruktur ins Visier nimmt, kann sich zumeist nur auf Windows-basierte Kontrollsysteme auswirken, die ausserdem über das Netz erreichbar sind, und muss demnach ein gewisses Ausbreitungsvermögen besitzen. «EKANS» und «MegaCortex» wurden hingegen entwickelt, um spezifisch Industrie-Automatisierungssysteme zu treffen. Bisher hat jedoch keines der öffentlich bekannten Opfer von «EKANS» eine Beeinträchtigung der ICS aufgrund eines Angriffs bestätigt. Der Automobil-Grosskonzern Honda[63] zum Beispiel hat zugegeben, Opfer einer Infektion geworden zu sein, die das IT-Netz betraf, jedoch keine Auswirkungen auf Produktion oder Verkauf hatte und auch für die Kundschaft folgenlos blieb. Der Energiemulti Enel[64] stellte am 7. Juni ein Eindringen ins IT-System fest, doch das Antivirus-Programm sei in der Lage gewesen, die Ransomware aufzuhalten, bevor sie in Aktion treten konnte. Das Betriebsnetz sei vorsichtshalber kurz isoliert worden. Auch in diesem Fall hätten die Kontrollsysteme keinen Schaden erlitten und es seien keine Datenlecks bekannt geworden. Unter den öffentlich bekannten Opfern von «EKANS» taucht auch Fresenius Medical Care auf, ein grosser privater europäischer Spitalanbieter. Nach dem Ransomware-Angriff wurden höchst sensible Informationen wie die Ergebnisse ärztlicher Untersuchungen, Notizen über Behandlungen und Allergien, aber auch Namen, Beruf, Telefonnummern und Adressen von Patientinnen und Patienten ins Netz gestellt.[65] Gemäss dem Internet Security Unternehmen Kaspersky gehören auch Fahrzeug- und Automobilhersteller zu den Opfern von «EKANS»; zudem vermuten sie, dass es in mindestens einem Fall nicht bei einer Infektion des Büronetzwerks blieb, denn die Schadsoftware wurde auf dem Videoüberwachungssystem einer Organisation in China entdeckt und blockiert.[66]

---

62 https://www.dragos.com/blog/industry-news/ekans-Ransomware-and-ics-operations/

63 https://www.bleepingcomputer.com/news/security/honda-investigates-possible-Ransomware-attack-networks-impacted/

64 https://www.bleepingcomputer.com/news/security/power-company-enel-group-suffers-snake-Ransomware-attack/

65 https://www.bleepingcomputer.com/news/security/snake-Ransomware-leaks-patient-data-from-fresenius-medical-care/

66 https://ics-cert.kaspersky.com/media/Kaspersky_ics_cert_alert_Snake_EN.pdf

Abgesehen von den Ransomware, die in erster Linie industrielle Kontrollsysteme ins Visier nehmen, wurde im ersten Halbjahr 2020 eine beachtliche Anzahl von Angriffen gegen kritische Infrastrukturen im Energiesektor verzeichnet. Auch solche Angriffe bergen für die Produktivität eines Unternehmens Risiken. Am 18. Februar zum Beispiel registrierte die amerikanische Cybersicherheitsbehörde CISA einen Angriff auf das Netz für operative Technologien (OT) einer Kompressionsanlage für Naturgas. Der nicht öffentlich genannte Akteur drang über einen Link in einem gezielt verschickten E-Mail in das IT-Netz der Firma ein. Anschliessend sei ihm eine Ausbreitung im Netzwerk (engl.: lateral movement) gelungen und er habe in das OT-Netz eindringen können. Daraufhin initiierte der Akteur die Verschlüsselung auf beiden Netzen. Zu den infizierten OT-Prozessen gehören Schnittstellen zwischen Mensch und Maschine (Human Machine Interface, HMI), die Datenchronologie und die sogenannten Polling-Server. Das Opfer wurde gezwungen, den Betrieb zu unterbrechen, um jede Spur der Malware zu löschen, was eine entsprechende Produktivitäts- und Gewinneinbusse nach sich zog.[67]

Nachfolgend eine Übersicht über die erfolgreichen und öffentlich bekannt gewordenen Ransomware-Angriffe, die im Berichtshalbjahr gegen Organisationen im Energiesektor geführt wurden.

Datum	Ransomware	Opfer	Folgen
1. April	Maze	Berkine, ein Konzern, der die staatliche algerische Ölgesellschaft Sonatrach und ihren amerikanischen Handelspartner Anadarko umfasst	Veröffentlicht wurden über 500 MB Dokumente mit streng vertraulichen Informationen (u. a. Lohnliste und Koordinaten der Angestellten, Informationen über Produktionsmenge, Budget und Zielsetzungen).[68]
14. April	Ragnar Locker	Energias de Portugal (EDP), portugiesischer Energiemulti (Strom und Gas)	Nach der Verschlüsselung der Unternehmensdaten haben die Ransomware-Operatoren ein Lösegeld von USD 11 Millionen gefordert. Ausserdem sollen die Cyberkriminellen 10 TB sensible Dokumente gestohlen haben, unter Androhung derer Publikation und der tatsächlichen Veröffentlichung eines Teils der Daten als Warnung. Der Angriff soll die Stromversorgung nicht beeinträchtigt haben.[69]

67 https://us-cert.cisa.gov/ncas/alerts/aa20-049a

68 https://www.inter-lignes.com/des-documents-hyper-confidentiels-de-sonatrach-derobes-par-des-hackers/

69 https://www.bleepingcomputer.com/news/security/ragnarlocker-Ransomware-hits-edp-energy-giant-asks-for-10m/

30. April	NetWalker	Northwest Territories Power Corporation NTPC, kanadische Elektrizitätsgesellschaft	Laut der Elektrizitätsgesellschaft haben die Stromsysteme unterbruchfrei funktioniert. Die Website wurde getroffen und mittels Defacement verunstaltet, sodass eine Botschaft der Cyberkriminellen zu sehen war.[70]
4. Mai	Unbekannt, die Behörden Taiwans vermuten chinesische Urheber.[71]	Staatliche taiwanesische Ölraffinerie CPC Corp	Die Website der CPC wurde getroffen und verschiedene Tankstellen waren zeitweise geschlossen, da keine Zahlungen mit der CPC Corp-Karte mehr verarbeitet werden konnten.[72] Der Angriff habe keine Auswirkungen auf die Energieproduktion der CPC gehabt.
14. Mai	REvil / Sodinokibi	Elexon, ein massgeblicher Intermediär im Stromversorgungsnetz von Grossbritannien	Der Vorfall betraf das interne IT-Netz und setzte den E-Mail-Server ausser Betrieb. Die Systeme für die Stromübertragung haben keinen Schaden erlitten.[73] Anfang Juni veröffentlichten die Verantwortlichen auf dem Darknet einen Ordner mit 1'280 von Elexon gestohlenen Dateien.[74]

Sicherheitsmassnahmen:

Die Betreiber von industriellen Kontrollsystemen (ICS) sollten, wo immer möglich, die betrieblichen IT-Systeme vom OT-Netz getrennt halten. Für das OT-Netz sollte eine mehrstufige Struktur eingesetzt werden, in der die weniger kritischen von den wirklich kritischen Prozessen getrennt sind. Ebenso ist zu überprüfen, dass ausschliesslich dazu befugtes Personal Zugang zu den ICS hat, um sowohl den virtuellen wie physischen Zugriff auf die kritischen Systeme zu begrenzen.

DOKU

Das NCSC hat auf seiner Website eine Checkliste über “Massnahmen zum Schutz von industriellen Kontrollsystemen (ICS)” veröffentlicht:

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

Vor Kurzem hat die US-amerikanische Cybersecurity and Infrastructure Security Agency CISA einschlägige Empfehlungen ins Netz gestellt:

https://www.cisa.gov/sites/default/files/publications/Cybersecurity_Best_Practices_for_Industrial_Control_Systems.pdf

70 https://www.cbc.ca/news/canada/north/ntpc-apparent-Ransomware-attack-1.5551603
71 https://www.cyberscoop.com/cpc-Ransomware-winnti-taiwan-china/
72 https://www.taiwannews.com.tw/en/news/3927869
73 https://www.elexonportal.co.uk/news/view/27108?cachebust=ebf1vtjsp0
74 https://www.theregister.com/2020/06/01/elexon_Ransomware_was_revil_sodinokibi/

4.3.2 Sabotageangriffe im Rahmen der Konflikte im Nahen Osten

Durch einen amerikanischen Luftangriff beim Flughafen in Bagdad wurden am 3. Januar 2020 der iranische General Qassem Soleimani, Kommandant der Quds-Einheit der Revolutionsgarden, und Jamal Jafaar Ibrahimi, der langjährige Führer der Kataib Hizballah sowie stellvertretende Chef der Popular Mobilization Force (PMF), getötet.[75] Dieser kinetische Angriff ist im grösseren Zusammenhang des Nahostkonfliktes zu betrachten. Es kommt im Rahmen dieses Konfliktes nämlich nicht nur zu physischen Konfrontationen. Seit Jahren bekämpfen sich die Konfliktparteien auch regelmässig im Cyberraum und schrecken auch vor physischen Auswirkungen ihrer Cyberangriffe nicht zurück oder wollen sogar absichtlich solche erzielen.[76]

Auswirkungen von destruktiv motivierten Cyberangriffen musste Ende 2019 die nationale Ölgesellschaft Bahrains, Bapco, gewärtigen.[77] Mehrere Geräte der Systemlandschaft wurden mit Malware unbrauchbar gemacht. Obwohl von Bapco nie bestätigt, wird ein Zusammenhang mit einer Warnung[78] der Saudischen Cybersicherheitsbehörde zur datenlöschenden *Wiper*-Schadsoftware «Dustman»[79] vermutet. Der ursprüngliche Einstiegspunkt scheint ein Fernzugriffssystem gewesen zu sein. Die Cyber-Intelligence-Firma Clearsky beschreibt in einem Bericht zur Angriffskampagne «Fox Kitten»[80] erfolgreiche Zugriffe auf Firmennetzwerke über schlecht geschützte *RDP*-Zugänge oder nicht aktualisierte und somit verwundbare VPN-Server von Pulse Secure, Fortinet oder Palo Alto. Im Arsenal der vorwiegend im Nahen Osten aktiven Angreifer befindet sich auch das «PowDesk[81] Skript», das Systeme mit der Software «LANDesk Management Agent» kompromittiert. Angriffe über die Cloud der Gruppe «HOLMIUM» wurden beispielsweise von Microsoft entdeckt.[82] Dabei kamen weitere spezifische Werkzeuge wie «POWERTON»[83] zum Einsatz. Der Akteur «APT34/Oilrig» griff gemäss dem Sicherheitsdienstleister Yoroi einen E-Mail-Server der Libanesischen Regierung mit Hilfe des «Karkoff Implant» an.[84] Sind solche Angriffsversuche erfolgreich und der Zugriff ins Netzwerk etabliert, werden auch Steuerungssysteme ins Visier genommen. So warnte die Israelische Regierung im April vor Angriffen gegen *SCADA*-Systeme in der Wasserversorgung.[85] Später wurden weitere Angriffsversuche auf Wassermanagement Systeme in der israelischen Landwirtschaft publik[86] und es wird gemutmasst, dass Cyberangriffe gegen den Iranischen Hafen an der Strasse von Hormuz[87] die Vergeltung für derartige Vorgänge darstellten.

---

75 https://www.defense.gov/Newsroom/Releases/Release/Article/2049534/statement-by-the-department-of-defense/

76 Siehe MELANI Halbjahresbericht 2019/2, Kapitel 5.2.

77 https://www.zdnet.com/article/new-iranian-data-wiper-malware-hits-bapco-bahrains-national-oil-company/

78 https://www.scribd.com/document/442225568/Saudi-Arabia-CNA-report

79 https://malpedia.caad.fkie.fraunhofer.de/details/win.dustman

80 https://www.clearskysec.com/fox-kitten/

81 https://www.clearskysec.com/powdesk/

82 https://www.microsoft.com/security/blog/2020/06/18/inside-microsoft-threat-protection-mapping-attack-chains-from-cloud-to-endpoint/

83 https://attack.mitre.org/software/S0371/

84 https://securityaffairs.co/wordpress/98802/apt/karkoff-malware-lebanon.html

85 https://www.gov.il/he/departments/publications/reports/scadaalert

86 https://www.zdnet.com/article/two-more-cyber-attacks-hit-israels-water-system/

87 https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html

Ist der Versuch über die verschiedenen Varianten beim Ziel direkt nicht erfolgreich, bewegen sich die Angreifer entlang der Lieferkette, um einen etwas weiter entfernten Einstiegspunkt zu finden. So warnte das FBI im Februar vor Angriffen auf Software-Lieferanten[88] mit dem Fernzugriffstrojaner «Kwampirs».[89] Im Fokus standen speziell Firmen, welche im Bereich industrielle Kontrollsysteme im Umfeld von Energieproduktion, -übertragung und -verteilung arbeiten.

Hinweis:

Organisationen, die im Umfeld solcher Konflikte operieren, sollten sich bewusst sein, dass eine Möglichkeit besteht, von solchen Angriffen direkt oder kollateral betroffen zu werden.

4.3.3 Aufklärungsangriffe gegen Stromversorgung dauern an

Die Übertragungsnetzbetreiber der Stromversorger in Europa arbeiten im Verband ENTSO-E zusammen, um die gesamteuropäische Stromversorgung zu koordinieren. Im Frühling 2020 wurde bekannt, dass dieses Kollaborationsgremium im letzten Jahr einen Cybervorfall zu bewältigen hatte, bei dem in sein Büronetzwerk eingedrungen wurde. «Das ENTSO-E Büronetzwerk hat keine Verbindungen zu operativen Systemen der Übertragungsnetzbetreiber», betont ENTSO-E in einer kurzen Pressemitteilung im März 2020.[90] Viele der 42 Mitglieder in 35 europäischen Ländern (siehe Abb. 6) bestätigen die Einschätzung des Verbandes zur Reichweite des Angriffs, so auch der Schweizer Vertreter Swissgrid.[91] Eine direkte Beeinträchtigung der Stromversorgung in Europa war durch diesen Angriff insofern nicht möglich.

Dieser Vorfall verdeutlicht, dass es Akteure gibt, die sich dafür interessieren, wie die Elektrizitätswirtschaft in verschiedenen Teilen der Welt ausgestaltet ist. Im vorangehenden Halbjahresbericht finden sich weitere Referenzen dazu.[92] Das aktuelle Beispiel belegt, dass auch Europa davon nicht verschont wird. Die Fachjournalisten von Cyberscoop[93] sehen eine Analyse von RecordedFuture[94] in Zusammenhang mit dem Vorfall bei ENTSO-E. Die verwendete Malware «Pupy RAT» wurde in Vergangenheit unter anderem von Gruppen eingesetzt, die auch vor destruktiven Wiper-Angriffen nicht zurückschreckten. Solche zerstörerischen Angriffe wurden bisher erst im Umfeld von bestehenden Konflikten registriert, wie sie im Kapitel 4.3.2 zu den Spannungen im Nahen Osten beschrieben werden. In Anbetracht von möglichen geopolitischen Entwicklungen muss jedes Land und jedes Stromversorgungsunternehmen risikoadäquat auf entsprechende Angriffe vorbereitet zu sein. Neben dem beobachteten Aufklärungsversuch in Europa sahen sich auch amerikanische Stromversorger mit Eindringversuchen konfrontiert.[95] Dort kam die Malware «Flowcloud»[96] zum Einsatz.

---

88 https://www.zdnet.com/article/fbi-warns-about-ongoing-attacks-against-software-supply-chain-companies/

89 https://malpedia.caad.fkie.fraunhofer.de/details/win.kwampirs

90 https://www.entsoe.eu/news/2020/03/09/entso-e-has-recently-found-evidence-of-a-successful-cyber-intrusion-into-its-office-network/

91 https://www.swissgrid.ch/en/home/about-us/newsroom/newsfeed/20200309-01.html

92 MELANI Halbjahresbericht 2019/2, Kapitel 4.2.1.

93 https://www.cyberscoop.com/europe-grid-pupy-rat/

94 https://www.recordedfuture.com/pupyrat-malware-analysis/

95 https://www.proofpoint.com/us/blog/threat-insight/ta410-group-behind-lookback-attacks-against-us-utilities-sector-returns-new

96 https://www.proofpoint.com/us/blog/threat-insight/flowcloud-version-413-malware-analysis

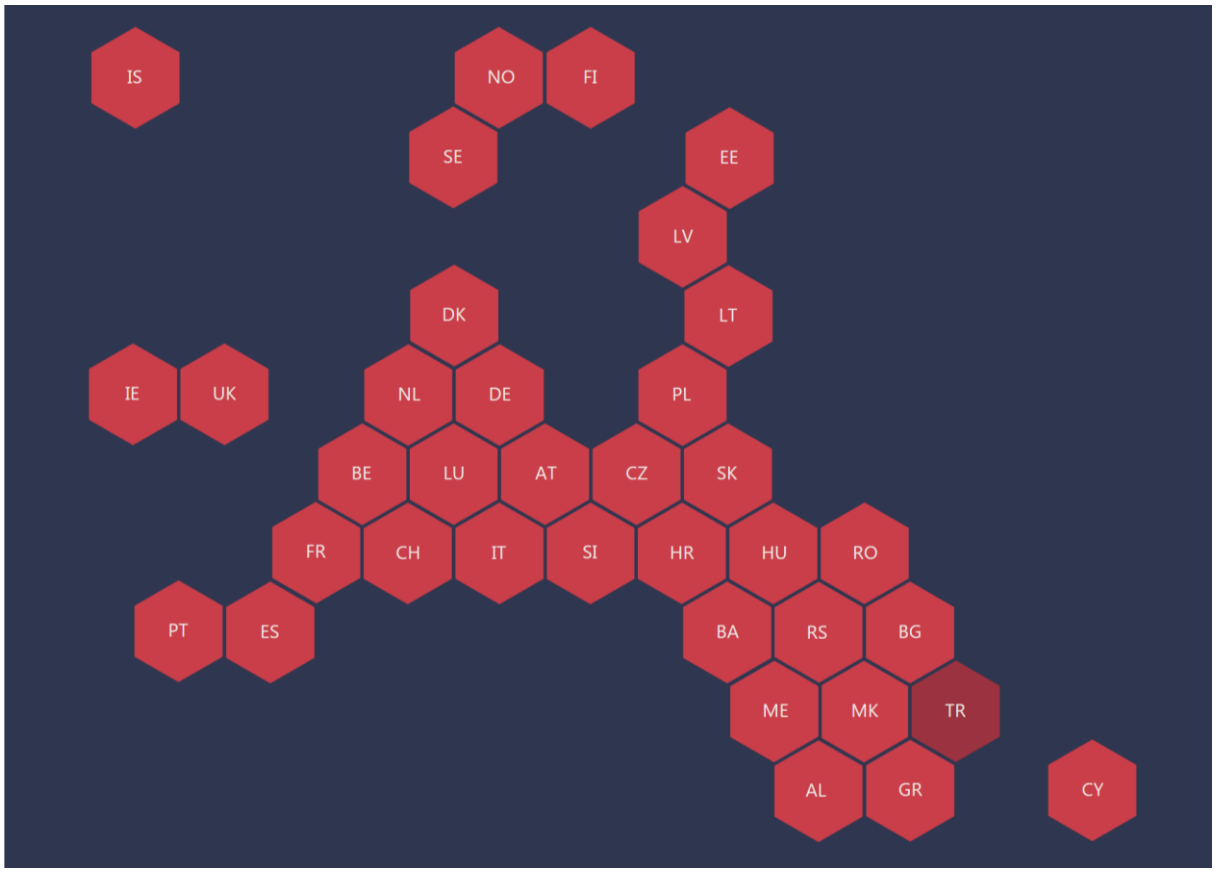

Abb. 6: Mitglieder von ENTSO-E[97]

Ein kürzlicher Ransomware-Vorfall, der ebenfalls keine Auswirkungen auf operative Steuerungssysteme hatte, betraf den britischen Überwacher des Elektrizitätsmarktes Elexon. Da sich Elexon weigerte, auf die Forderungen der Erpressergruppe «Sodinokibi/REvil» einzugehen, veröffentlichten diese zuvor abgefasste Dateien.[98] Elexon scheint damit vorerst glimpflich davongekommen zu sein. Es ist jedoch zu bedenken, dass die veröffentlichten Informationen auch von Akteuren, die nicht nur finanzielle Interessen verfolgen, zur Gestaltung künftiger Angriffe eingesetzt werden könnten. Weitere Beispiele ähnlicher Ausprägung sind die im Kapitel 4.3.1 erwähnten Vorfälle zu «RagnarLocker» in Portugal oder der Ransomware gegen die Raffinerie der CPC Corp in Taiwan. Solche Ransomware-Angriffe stellen momentan die akutere Bedrohung dar, speziell diejenigen Varianten, die auch versuchen, operative Steuerungssysteme zur Kontrolle physischer Prozesse zu stören.

Hinweis:

Das NCSC steht im Rahmen des geschlossen Kundenkreises von MELANI in regelmässigem Austausch mit Vertretern der Schweizer Stromversorgung. Gemeinsam wird daran gearbeitet, solche Angriffe in der Schweiz frühzeitig zu erkennen und zu verhindern oder deren Auswirkungen so klein wie möglich zu halten.

97 https://www.entsoe.eu/about/inside-entsoe/members/

98 https://www.theregister.com/2020/06/01/elexon_ransomware_was_revil_sodinokibi/

4.4 Schwachstellen

Im ersten Halbjahr 2020 wurden einige Schwachstellen veröffentlicht, die besonders in Verbindung mit dem Lockdown kritisch waren. Viele Unternehmen ermöglichten in dieser Zeit nämlich vermehrt Homeoffice. Die dafür erforderliche Infrastruktur ist komplex und auch in der normalen Lage, d. h. ohne ausserordentlichen Zeitdruck, nicht ganz einfach sicher einzurichten.

So waren viele Schweizer Unternehmen, darunter auch kritische Infrastrukturen, von der am 17. Dezember 2019 veröffentlichten Schwachstelle «CVE-2019-19781» am *Application Delivery Controller* (ADC) und den *Gateway*-Produkten von Citrix betroffen. Die Schwachstelle ermöglicht einem Angreifer eine Code-Ausführung auf Geräten, für die er keine Berechtigung hat. Da diese Citrix-Produkte häufig am Aussenperimeter des Netzwerks eingesetzt werden, konnte sich ein Angreifer über die Schwachstelle unberechtigten Zugriff verschaffen. Trotz Sicherheitshinweis und dringender Empfehlung von Citrix an die Kunden, die Produkte zu sichern, haben dies nicht alle getan. Am 10. Januar 2020 wurden mehrere *Exploits* für die Ausnützung dieser Schwachstelle veröffentlicht. Innert Stunden nahm die Suche nach im Internet exponierten und verwundbaren Citrix-Produkten stark zu, und in den Tagen darauf nutzten Angreifer die *Exploits*, um Unternehmensnetze zu kompromittieren und mit Ransomware-Angriffen Lösegeld zu erpressen. Nach der Veröffentlichung der Exploits informierte das NCSC mehr als fünfzig Betreiber kritischer Infrastrukturen nachdrücklich über die potenzielle Gefahr und welche Schutzmassnahmen zu ergreifen sind.

Angreifer zielen unter anderem auf Router oder VPN-Server ab, die Software-Versionen mit Schwachstellen enthalten und nicht durch zusätzliche Massnahmen geschützt sind. Ihre Strategie besteht darin, ein Einfallstor zu finden, über das sie in das Unternehmensnetzwerk eindringen und anschliessend beispielsweise eine Ransomware einsetzen können. In den letzten Jahren haben denn auch immer mehr Organisationen erhebliche Verluste erlitten, weil eine Anwendung oder ein Produkt, das eine kurz zuvor veröffentlichte Schwachstelle enthielt, dem Internet ausgesetzt war.[99]

Empfehlungen:

Unternehmen sollten ein stets aktuelles Inventar ihrer IT-Infrastruktur führen. Oberste Priorität haben dabei Produkte, die dem Internet ausgesetzt sind. Der zweite Schritt besteht aus einem Schwachstellen- und Update-Monitoring, indem die entsprechenden Herstellerhinweise im Rahmen eines Echtzeit-Risikomanagements beschafft, analysiert und priorisiert werden. Schliesslich sind Bereiche und Verfahren für dringende Updates von Schlüsselelementen (insbesondere des Perimeters) zu planen.

Veröffentlichte Schwachstellen sind in der Datenbank *Common Vulnerabilities and Exposures* CVE aufgeführt. Abrufbar unter: https://nvd.nist.gov.

[99] Siehe MELANI Halbjahresbericht 2019/2, Kap. 4.6.1; MELANI Halbjahresbericht 2020/1, Kap. 4.1.1

4.5 Datenabflüsse

Das Phänomen des Datenlecks ist nicht neu, aber solche Ereignisses haben im Berichtszeitraum an Frequenz zugelegt. Es ist davon auszugehen, dass dieser Trend sich fortsetzt. Daten von Firmen zu leaken oder zu verkaufen steht bei einigen Cyberkriminellen hoch im Kurs. Gemäss einer Studie werden in den nächsten zwei Jahren jedes vierte Unternehmen Opfer eines Datenlecks werden.[100]

Im Mai dieses Jahres musste EasyJet informieren, dass sie Opfer eines hoch entwickelten Cyberangriffs geworden und Daten von etwa neun Millionen Kunden betroffen waren, darunter E-Mail-Adressen, Reisedaten, aber auch Kreditkartendaten. Gemäss Angaben von EasyJet brauchte es Zeit, um das Ausmass des Angriffs zu erfassen und zu erkennen, wer betroffen war. Das Unternehmen gab keine Einzelheiten über die Art des Angriffs oder die Motive an, sagte jedoch, dass seine Ermittlungen darauf hindeuteten, dass die Hacker es auf geistiges Eigentum des Unternehmens abgesehen hätten und nicht auf Informationen, die für Identitätsdiebstahl verwendet werden könnten. Trotzdem warnte das Unternehmen seine Kunden vor möglichen Phishing-Angriffen und empfiehlt nach wie vor erhöhte Aufmerksamkeit. Gemäss Europäischer Datenschutzgrundverordnung (EU-DSGVO) könnte EasyJet eine Geldstrafe in Höhe von bis zu 4 Prozent seines weltweiten Jahresumsatzes drohen, wenn festgestellt wird, dass Kundendaten falsch gehandhabt worden sind. Falls Fahrlässigkeit nachgewiesen werden kann, ist auch eine Schadenersatzklage seitens der Kunden möglich, was die Kosten für die Fluggesellschaft erheblich erhöhen würde.

Auch die Hotelkette Marriott International meldete im Februar 2020 einen Vorfall, von dem persönliche Daten von bis zu 5,2 Millionen Gästen betroffen waren. Marriott geht davon aus, dass der Angriff Mitte Januar 2020 begonnen hat. Entdeckt wurde der Vorfall aber erst gegen Ende Februar, als eine unerwartete Menge an Gästedaten unter Verwendung der Anmeldedaten von zwei Angestellten eines Franchise-Unternehmens abgerufen worden waren. Im Anschluss eröffnete Marriott eine Untersuchung, führte eine verstärkte Überwachung ein und organisierte Ressourcen zur Information und Unterstützung der Gäste, u. a. ein Portal für potenziell betroffene Personen, welches per Abfrage Auskunft über Datenschutzverletzungen gab. Dies ist bereits der zweite Vorfall, den Marriott in den letzten zwei Jahren gemeldet hat. Das Unternehmen gab im November 2018 bekannt, dass die Reservationsdatenbank von Starwood Hotels gehackt wurde.

Gemäss einer neuen Umfrage hatten fast 80 Prozent der Unternehmen in den vergangenen 18 Monaten mindestens eine Verletzung ihrer Cloud-Daten zu beklagen und rund 43 Prozent meldeten zehn oder mehr Verletzungen.[101] Laut den 300 Informationssicherheitsverantwortlichen (CISO), die an der Umfrage teilgenommen hatten, waren Sicherheitsfehlkonfigurationen (67 Prozent), mangelnde Transparenz der Zugriffseinstellungen und -aktivitäten (64 Prozent) sowie Fehler bei den Berechtigungen im Identitäts- und Zugriffsmanagement (61 Prozent) ihre grössten Sorgen im Zusammenhang mit Daten in Cloud-Umgebungen.[102] Auch übermässige Berechtigungen sind ein Fallstrick und können lange unbemerkt bleiben, da sie oft standardmässig erteilt werden, wenn eine neue Ressource oder ein neuer Dienst zur Cloud-Umgebung

---

100 https://www.itgovernance.co.uk/blog/do-you-have-a-data-breach-response-plan

101 https://www.helpnetsecurity.com/2020/06/03/cloud-data-breach/

102 https://www.itgovernance.co.uk/blog/do-you-have-a-data-breach-response-plan; https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/

hinzugefügt wird. Sie sind ein primäres Ziel für Angreifer, da sie für böswillige Aktivitäten wie den Diebstahl sensibler Daten und die Einschleusung von Malware genutzt werden können. Oberste Sicherheitsprioritäten für den Cloud-Zugriff sind daher die Wahrung der Vertraulichkeit sensibler Daten, die Einhaltung gesetzlicher Vorschriften und die Sicherstellung der richtigen Zugriffsebene.

Die Motivation, Daten zu leaken, kann nicht nur finanzieller, sondern auch ideeller Natur sein. So hat eine Gruppe namens «Distributed Denial of Secrets (DDoSecrets)» am 19. Juni 2020 einen 269 GB grossen Daten-Dump in Umlauf gebracht, welcher über 24 Jahre Polizeiaufzeichnungen aus über 200 amerikanischen Polizeidienststellen offenlegt.[103] Ihr Ziel sei ein freier Zugang zu Daten, welche von öffentlichem Interesse seien sowie eine kollektive Transparenz. Das wahrscheinliche Motiv hinter dem Leck deutet auf eine Vergeltung angesichts der aktuellen Anti-Rassismus-Proteste gegen die Polizei in den USA hin. Ein Datenleck dieses Ausmasses bei Strafverfolgungsbehörden gab es noch nie. Unter den unzähligen Dokumenten, wie beispielsweise Berichte und Bulletins des FBI, welche Personendaten enthalten, finden sich auch ausführliche Bankangaben, Fotos von Verdächtigen, Telefonnummern und E-Mail-Adressen von Opfern und Tätern. Es liegt auf der Hand, dass solche Daten auch künftig von Hacktivisten und Cyberkriminellen ausgenutzt werden können. Sorgen bereitet den Behörden in diesem Fall vor allem die Gefahr für die Opfer. Die Authentizität der Daten wurden inzwischen bestätigt. Das Leck sei durch eine Sicherheitslücke bei der Software-Entwicklungsfirma Netsential ermöglicht worden, die ihren Sitz in Houston, Texas hat. Inwiefern dieser Hack Auswirkungen auf die weiteren Kunden von Netsential hat, ist noch nicht klar.

Wie bereits in Kapitel 4.1.1 erwähnt, ist mittlerweile auch bei Ransomware-Vorfällen immer mit einem Datenabfluss zu rechnen. Grosse Treiber dieser Entwicklung ist die Gruppe «Maze», die eine spezielle «Maze News»-Website erstellt hat, auf der gestohlene Daten von Opfern, die der Lösegeldforderung nicht nachkamen, öffentlich zugänglich gemacht werden. Diese Erpressungstaktik wurde schnell von anderen Gruppen übernommen, darunter «Nefilim», «Sekhmet» und «Sodinokibi/REvil». Mit einer durchschnittlichen Lösegeldzahlung von über USD 100'000 und einigen Opfern, die angeblich Millionen zahlten, waren einzelne Gruppen mit Erpressungen von Unternehmen allein bereits sehr erfolgreich. Unlängst gab es jedoch Berichte über eine Zusammenarbeit zwischen der «Maze»- und der «Lockbit»-Gruppe sowie den Betreibern von «Sodinokibi/REvil», die gestohlene Daten nicht einfach publizieren, wenn die Opfer nicht zahlen, sondern sie stattdessen an den Höchstbietenden versteigern. Durch die arbeitsteilige Organisation der Gruppen, den gemeinsamen Austausch von Ratschlägen, Taktiken und einer zentralisierten Plattform für Datenlecks können sich die Erpresserbanden mehr auf die Entwicklung raffinierterer Angriffe und erfolgreicher Erpressungsversuche konzentrieren. Solche Arbeitsteilung konnte bereits in einigen Fällen beobachtet werden. So tauchten Lecks auf, deren Informationen nicht von einem Ransomware-Angriff von «Maze» stammten, sondern aus einem anderen Vorfall, für den «LockBit» verantwortlich gemacht wird.

Trends im Bereich Ransomware und Datenlecks weisen klar in Richtung «Dienstleistung». Verschlüsselung durch Ransomware und Datenlecks als Dienstleistung können im Darknet bezogen werden. Eine weitere Neuerung ist, dass Daten nicht einfach veröffentlicht, sondern verkauft oder sogar versteigert werden.

---

[103] https://krebsonsecurity.com/2020/06/blueleaks-exposes-files-from-hundreds-of-police-departments/

Schlussfolgerung / Empfehlungen:

Der sorgfältige und verantwortungsbewusste Umgang mit Daten ist für Unternehmen ein grosses Spannungsfeld, welches nicht zu vernachlässigen ist. Einerseits steht der Ruf der Unternehmung auf dem Spiel, die Folgekosten sind beachtlich. Auch haben die Menschen oder Kunden das Recht zu erwarten, dass Unternehmen und Organisationen sicher und verantwortungsvoll mit ihren personenbezogenen Daten umgehen. Eine wichtige Massnahme ist die Erstellung eines so genannten *Data Breach Response*-Plans. Bereits die Erarbeitung eines solchen Plans zeigt auf, wo die spezifischen Risiken sind und wie diese minimiert werden können.

Die vorangehende Beschreibung zeigt auf, wie vielseitig die Ansätze sind, welche in einem Datenleck münden können. Jedes Unternehmen sollte sich auf das Szenario Datenleck vorbereiten. Dies beinhaltet unter anderem folgende Massnahmen: Systeminventar, Bedrohungs- und Verwundbarkeitsanalyse, Risikoeinschätzung, -bewertung und -minimierung, konstante Weiterentwicklung der Kontrollmechanismen sowie Monitoring.

Für den Fall, dass das Unternehmen trotzdem von einem Datenleck betroffen ist, sollte unbedingt ein sogenannter Data Breach Response-Plan bereit liegen, welcher ein schnelles und koordiniertes Handeln ermöglicht. Dieser sollte nebst der klassischen Vorfallbewältigung auch Prozesse beinhalten, die das Schadensausmass aufzeigen (welche Daten in welchem Umfang sind betroffen) sowie der Benachrichtigung der Opfer und des Reportings aufzeigen. Falls externe Leistungen (Beratung, operative Unterstützung, usw.) nötig sind, ist es wichtig, die Partner vorgängig bereits zu kennen und die Dienstleistung vertraglich festgehalten zu haben. Die Kommunikation (Betroffene, Medien) ist ein weiterer zentraler Punkt, welcher nicht nur inhaltlich geregelt sein muss, sondern auch Aussagen über die Verfügbarkeit von Ressourcen machen soll (z. B. Unterstützung bei Bewältigung einer Flut von Anrufen und E-Mails). Weiter dürfte neben der technischen Analyse und Einschätzung des Vorfalls auch eine zeitnahe juristische Einschätzung der Situation und der möglichen rechtlichen sowie finanziellen Konsequenzen nötig sein. Schliesslich sollte auch das Reputations-Management beachtet werden.

4.6 Spionage

Spionage ist nach wie vor eine sehr reale Bedrohung, wie die Ereignisse der letzten Monate einmal mehr gezeigt haben. Die führende Rolle spielen weiterhin staatliche und staatlich gesponserte Gruppen. Es gibt jedoch auch bereits private Unternehmen, die für gezieltes Ausspähen angeheuert werden können (siehe Kapitel 4.6.3).

4.6.1 Spionage in Zeiten von COVID-19

Gemäss Kaspersky haben im ersten Halbjahr 2020 *APT*s wie «Kimsuky», «APT27», «Lazarus» oder «ViciousPanda» sowie auch andere Cyberakteure die Coronakrise für sich ausgenutzt.[104] Die Pandemie hatte zwar keinen Einfluss auf die eingesetzten Taktiken, Techniken und Prozesse (Tactics, Techniques and Procedures, TTP) dieser Gruppen, war aber bei verschiedenen Angriffsszenarien das Hauptthema (siehe dazu Kapitel 3.1 zu Social Engineering).

[104] https://securelist.com/apt-trends-report-q1-2020/96826/

Während einer Pandemie bündelt sich das Interesse an Informationen zwangsläufig auf das Gesundheitswesen im weitesten Sinne. So wurde beispielsweise einer der Schlüsselakteure der Krise weltweit, die Weltgesundheitsorganisation (WHO), bedeutend häufiger angegriffen als in normalen Zeiten. Wie der CISO der WHO gegenüber Reuters erklärte, waren die Spionageversuche das Werk von Elite-Hackern.[105] Im Visier von Spionageaktivitäten waren neben der WHO auch mehrere Einrichtungen, die nach einem COVID-19-Impfstoff forschen. Denn um die Entdeckung eines Impfstoffes ist ein Wettlauf entbrannt. Die USA, Kanada und Grossbritannien beschuldigten einen russischen Geheimdienst Einrichtungen in ihren Ländern auszuspionieren.[106] Die Vereinigten Staaten haben zudem Anklage gegen zwei chinesische Staatsbürger erhoben, die beschuldigt werden, Spionageoperationen im Auftrag des chinesischen Ministeriums für Staatssicherheit durchgeführt zu haben.[107] Diese Spionageversuche zielten auf amerikanische Biotechnologiefirmen ab, die auf der Suche nach einem Impfstoff gegen COVID-19 sind.[108] Es scheint, dass die beschuldigten Hacker Teil einer kriminellen Gruppe sind, die seit mindestens 2009 in vielen Bereichen Spionagekampagnen durchführt und insbesondere durch den Diebstahl von geistigem Eigentum erhebliche finanzielle Gewinne erzielt hat.

4.6.2 Wirtschaftsspionage auch in der Schweiz Realität

Bei Wirtschaftsspionage geht es um die Beschaffung von bewusst geheim gehaltenen wirtschaftlichen, wissenschaftlichen oder technologischen Informationen oder Daten (Geschäftsgeheimnisse). Das Ausmass der Wirtschaftsspionage in der Schweiz ist angesichts der sehr sensiblen Thematik und der kaum öffentlich verfügbaren Daten schwer abschätzbar. Um das Problem sichtbarer zu machen, hat der Nachrichtendienst des Bundes (NDB) eine Studie zur Wirtschaftsspionage in der Schweiz ausgeschrieben. Im Januar 2020 wurde die vom Institut für Strafrecht und Kriminologie der Universität Bern durchgeführte qualitative und quantitative Studie zu Wirtschaftsspionage gegen Schweizer Unternehmen unterschiedlicher Grösse in verschiedenen Wirtschaftszweigen veröffentlicht.[109]

Die Ergebnisse der Studie zeigen, dass 15-33 Prozent der Schweizer Unternehmen unabhängig von ihrer Grösse von Wirtschaftsspionage betroffen sind. Besonders gefährdet sind die Branchen Informatik, Telekommunikation, Life Science, Maschinenbau, Industrie und Pharma. In 40 Prozent der Fälle waren (ehemalige oder aktuelle) Mitarbeitende des Unternehmens involviert. In anderen Branchen können vor allem Firmen, die ein Nischenprodukt oder ein speziell sicherheitsrelevantes Produkt herstellen, zum Ziel von Wirtschaftsspionage werden. Die Unternehmen, die an der Studie teilgenommen haben, weisen auf die Schwierigkeit der Unterscheidung zwischen direkt auf wirtschaftlichen Gewinn abzielenden Angriffen und solchen

---

105 https://www.reuters.com/article/us-health-coronavirus-who-hack-exclusive/exclusive-elite-hackers-target-who-as-coronavirus-cyberattacks-spike-idUSKBN21A3BN

106 Grossbritannien: https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development; USA: https://us-cert.cisa.gov/ncas/current-activity/2020/07/16/malicious-activity-targeting-covid-19-research-vaccine-development; Kanada: https://cse-cst.gc.ca/en/media/2020-07-16

107 https://www.courtlistener.com/recap/gov.uscourts.waed.91446/gov.uscourts.waed.91446.15.0.pdf

108 https://www.cisa.gov/publication/fbi-cisa-psa-prc-targeting-covid-19-research-organizations; https://www.nytimes.com/2020/07/21/us/politics/china-hacking-coronavirus-vaccine.html

109 https://boris.unibe.ch/139072/

zum Beschaffen von Daten zu Spionagezwecken hin. Ebenfalls schwierig scheint die Zuordnung der Fälle. 38 Prozent konnten nicht zugeordnet werden. Bei den entstandenen Schäden wurden am häufigsten genannt: Verlust von Wettbewerbsvorteilen (18 Prozent), Ausfall der Informatik (14 Prozent) sowie Kunden- und Auftragsverluste (11 Prozent). In 11 Prozent der Fälle war die Existenz des Unternehmens bedroht.

4.6.3 Auftragsspionage

Im Juni 2020 hat das kanadische Forschungslabor Citizen Lab einen Bericht über massive «hack-for-hire»-Spionagetätigkeiten durch eine Gruppe namens «Dark Basin» veröffentlicht.[110] «Dark Basin» hat seit 2017 Journalisten und Aktivisten, aber auch Banken, Hedgefonds und in anderen Bereichen tätige Unternehmen angegriffen. Gemäss Aussage von Citizen Lab besteht mit hoher Wahrscheinlichkeit eine Verbindung mit einer indischen Firma namens BellTroXInfoTech Services. Die Gruppe soll für verschiedene nicht identifizierte Auftraggeber gehandelt haben.

Bei einer dieser Operationen zielte eine grosse Phishing-Aktion auf verschiedene Non-Profit-Organisationen ab, denen gemeinsam war, dass sie an der Kampagne «#exxonknew» teilgenommen hatten. Diese Kampagne warf dem US-amerikanischen Mineralölkonzern Exxon vor, die Folgen des Klimawandels jahrzehntelang bewusst verharmlost zu haben. Ein anderer Dark-Basin-Feldzug betraf Angestellte der deutschen Fintech-Firma Wirecard AG sowie Journalisten, die einem Betrugsverdacht gegen dieses Unternehmen nachgingen.[111]

4.6.4 Neues von «Winnti»

Der Sicherheitsdienstleister FireEye hat eine grosse Spionageaktion der chinesischen Gruppe «APT41» aufgedeckt.[112] Zwischen dem 20. Januar und dem 11. März 2020 versuchte «APT41» bei 75 FireEye-Kunden Schwachstellen in den Anwendungen Citrix NetScaler/ADC, Cisco-Router und Zoho ManageEngine Desktop Central auszunutzen. Von dem Angriff waren viele Länder betroffen, unter anderem auch die Schweiz. Betroffen waren verschiedenste Sektoren, darunter der Regierungs- und der Finanzbereich. «APT41» ist ein hoch entwickelter Akteur, der seine Tätigkeiten regelmässig diversifiziert. Diese Gruppierung ist auch unter dem Namen «Winnti» bekannt, über die auch im letzten Halbjahresbericht[113] berichtet worden ist.

4.6.5 «Sandworm» zielt auf beliebten Linux Mail Server

Der amerikanische Nachrichtendienst NSA hat am 28. Mai 2020 Empfehlungen abgegeben zur Abwehr von Eindringversuchten via Schwachstellen im *Exim Mail Transfer Agent (MTA)*.[114] Die NSA beschuldigt in ihrer Pressemeldung eine Gruppierung namens «Sandworm», für die Angriffe verantwortlich zu sein und ordnet diese der Hauptabteilung für spezielle Technologien

---

110 https://citizenlab.ca/2020/06/dark-basin-uncovering-a-massive-hack-for-hire-operation/

111 https://www.ft.com/content/19c6be2a-ee67-11e9-bfa4-b25f11f42901

112 https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html

113 MELANI Halbjahresbericht 2019/2, Kapitel 4.1.2.

114 https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/2196511/exim-mail-transfer-agent-actively-exploited-by-russian-gru-cyber-actors/

(GTsST) des russischen militärischen Nachrichtendienstes GRU zu. «Sandworm» wird verdächtigt, an den Angriffen auf die ukrainische Stromversorgung zu Jahresende 2015[115] und 2016[116] zumindest beteiligt gewesen zu sein.

Die Schwachstelle (CVE-2019-10149) war bereits ein Jahr lang bekannt und Aktualisierungen für die betroffenen Systeme waren seit langem verfügbar.[117] Dennoch waren zum Zeitpunkt der Warnung noch rund 2,5 Millionen verwundbare Systeme über die dedizierte Suchmaschine Shodan auffindbar.[118] Exim MTA wird häufig eingesetzt, da die Software in vielen Linux-Distributionen standardmässig die E-Mail-Funktionalität zur Verfügung stellt. Verwundbare Systeme erlauben Angreifern aus der Ferne beliebigen eigenen Code einzuschleusen und auszuführen.

4.6.6 Andauernde Bedrohung durch «Berserk Bear»

Seit die USA im Frühling 2018 vor den Aufklärungsversuchen der Gruppe gewarnt hatten,[119] die sich damals mehrheitlich gegen amerikanische Energieversoger richteten, schafften es die Angreifer immer wieder in die Schlagzeilen.[120] Zuletzt wurde die Kompromittierung der Website des Flughafens San Francisco bekannt,[121] womit Zugangsdaten von nichts ahnenden Besuchern abzugreifen versucht wurde.[122]

Nachdem bereits am Vortag die Fachjournalisten von Cyberscoop über die Warnung der deutschen Behörden berichteten,[123] vermeldete die deutsche Tagesschau am 27. Mai 2020 plakativ «Russische Bären unter Hackerverdacht».[124] In einem nicht für die Öffentlichkeit bestimmten Dokument warnen der Bundesnachrichtendienst (BND), das Bundesamt für Verfassungsschutz (BfV) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) vor andauernden Angriffsversuchen der unter dem Pseudonym «Berserk Bear»[125] bekannten Gruppierung. Die Bedrohung richtet sich speziell gegen Firmen in der Energie-, Wasser- und Telekommunikationsbranche.

Das BfV hatte bereits im Sommer 2018 vor diesen Angriffen gewarnt,[126] die sich auch gegen deutsche Unternehmen richteten. Gemäss Recherchen des Bayrischen Rundfunks sahen sich die deutschen Behörden veranlasst, auf Grund der weiter andauernden, teils erfolgreichen Kompromittierungsversuche nochmals mit Nachdruck auf die Gefahr hinzuweisen.

---

115 MELANI Halbjahresbericht 2015/2, Kapitel 5.3.1.

116 MELANI Halbjahresbericht 2016/2, Kapitel 5.3.1.

117 https://www.qualys.com/2019/06/05/cve-2019-10149/return-wizard-rce-exim.txt

118 https://www.bleepingcomputer.com/news/security/nsa-russian-govt-hackers-exploiting-critical-exim-flaw-since-2019/

119 https://us-cert.cisa.gov/ncas/alerts/TA18-074A

120 https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112

121 https://www.bleepingcomputer.com/news/security/russian-hackers-tried-to-steal-san-francisco-airport-windows-accounts/

122 https://attack.mitre.org/techniques/T1187/

123 https://www.cyberscoop.com/german-intelligence-memo-berserk-bear-critical-infrastructure/

124 https://www.tagesschau.de/investigativ/br-recherche/hacker-angriff-infrastruktur-101.html

125 https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2018GlobalThreatReport.pdf

126 https://www.wirtschaftsschutz.info/SharedDocs/Kurzmeldungen/DE/ITSicherheit/Cyberbrief_1_18_dow.html

Hinweis:

Bei «Berserk Bear» handelt es sich um einen Akteur, der sich in der Vergangenheit bereits mehrfach in Netzwerken bis zu Systemen mit Verknüpfungen zu Prozesssteuerungen, beispielsweise der Stromversorgung, vorgearbeitet hat. Von dort ist es nicht mehr weit zu Cybersabotage, die sich auch physisch auswirkt.

4.6.7 Australien – Ziel von Cyberangriffen

Australien war gemäss Regierungsaussagen in den letzten Monaten Ziel einer intensiven Welle hoch entwickelter Angriffe gegen eine Vielzahl von Einrichtungen der Regierung, der Politik, im Bildungs- und Gesundheitswesen, in der Industrie und bei Betreibern kritischer Infrastrukturen. Australien war zwar schon häufig im Visier von Angreifern, diese Welle zeichnete sich aber durch ihre hohe Frequenz, ihr Ausmass, die ausgefeilte Technik und potenzielle Auswirkungen aus.

Gemäss einem Bericht des Australian Cyber Security Centre[127] arbeiteten die Angreifer mit einer sogenannten «Copy-Paste-Compromise»-Taktik, um in die Systeme ihrer Opfer einzudringen. Das heisst, die Angreifer haben weitgehend bestehende *Exploits* und andere Open-Source-Werkzeuge genutzt, die sie einfach «kopieren und einfügen» konnten. Um in die Zielnetzwerke zu gelangen, wurden beispielsweise Schwachstellen in nicht aktualisierten Versionen von Telerik UI, Microsoft Internet Information Services (IIS), Sharepoint oder Citrix (siehe Kap. 4.4) ausgenutzt. Wo das nicht möglich war, wurde mittels *Spear phishing* vorgegangen. Mit gestohlenen Identitäten verschafften sich die Angreifer legitime Fernzugänge. Über *Webshells* und den *HTTP/HTTPS*-Verkehr nutzten sie kompromittierte Websites als *Command-and-Control-Server*. Einmal im Zielnetzwerk, kamen Open-Source- aber auch massgeschneiderte Werkzeuge zum Einsatz, um die Beständigkeit ihrer Präsenz (engl.: *persistence*) und Interaktion im Netzwerk sicherzustellen.

Die australische Regierung geht davon aus, dass sie es mit staatlichen Angriffen zu tun hatte, wobei Premierminister Scott Morrison keinen Namen nannte. Später war in Regierungsquellen von China als mutmasslichem Angreifer die Rede.[128] Die chinesische Regierung dementierte umgehend und beschuldigte das Strategic Policy Institute, absichtlich falsche Anschuldigungen erhoben zu haben.[129]

Weniger als einen Monat nach dem Bekanntwerden der Angriffe publizierte ein von der australischen Regierung eingesetztes Expertengremium einen Bericht mit Empfehlungen für die australische Cybersicherheitsstrategie 2020.[130] Die Empfehlungen umfassen fünf Bereiche:

- Abschreckung: böswillige Akteure von Angriffen auf australische Ziele abhalten;
- Prävention: Online-Kompromittierung von Personen und Sektoren verhindern;

---

127 https://www.cyber.gov.au/sites/default/files/2020-06/ACSC-Advisory-2020-008-Copy-Paste-Compromises.pdf

128 https://www.theguardian.com/australia-news/2020/jun/19/australia-cyber-attack-attacks-hack-state-based-actor-says-australian-prime-minister-scott-morrison

129 https://www.abc.net.au/news/2020-06-19/china-responds-to-accusation-of-australia-cyber-attack/12375324

130 https://www.homeaffairs.gov.au/cyber-security-subsite/files/2020-cyber-security-strategy-iap-report.pdf

- Erkennung: Cyberbedrohungen erkennen und rasch darauf reagieren;
- Resilienz: Auswirkungen von Cybersicherheitsvorfällen minimieren;
- Investitionen: in Cybersicherheit investieren.

Für die Umsetzung der neuen Strategie will Australien über die nächsten zehn Jahre beispiellose 1,35 Milliarden AUD investieren (rund 900 Mio. CHF). Rund ein Drittel davon ist für die Anstellung von fünfhundert Cybersicherheitsspezialistinnen und -spezialisten bei der australischen Regierung vorgesehen.[131]

4.6.8 Österreich im Visier

Österreich war Ziel zweier Spionageangriffe, die in den letzten Monaten bekannt wurden. Ein Angriff Anfang 2020 eines angeblich staatlichen Akteurs betraf das österreichische Aussenministerium. Die Einzelheiten dazu sind nicht öffentlich bekannt.[132]

Österreichs grösster Telekomanbieter A1 Telekom Austria bestätigte im Juni 2020 einen Angriff, nachdem ein Whistleblower im Umfeld der Firma einen Sicherheitsexperten avisiert hatte.[133] Die Operation scheint schon im November 2019 erfolgt und im Dezember entdeckt worden zu sein. Es dauerte sechs Monate, bis A1 Telekom den Angreifer endgültig loswurde.[134] Laut A1 hatten die böswilligen Akteure nur einen begrenzten Teil ihres Netzwerks kompromittiert, die Komplexität der Systeme habe Schlimmeres verhindert. Wie sich zeigte, konnten sich die Angreifer aber doch erheblich ausbreiten, indem sie zuerst die Rechte eines lokalen und anschliessend eines Domänen-Administrators erlangten und so ins Windows-Netz gelangten.[135] A1 beteuert, dass die Eindringlinge keine Daten abzogen. Der Whistleblower hingegen behauptet, die Angreifer seien an sensible Kundendaten gelangt. A1 konnte keine Zuordnung der Täterschaft vornehmen. Anders der anonyme Zeuge, der den Angriff einem staatlichen chinesischen Akteur zuschrieb, nämlich der auf Telekomkonzerne spezialisierten Gruppe «Gallium».

4.7 Social Engineering und Phishing

4.7.1 Phishing

Systeme wie Google reCAPTCHA Version 3 haben die Funktionsweise der CAPTCHA revolutioniert. Bei diesen Systemen handelt es sich um Sicherheitssysteme, die einer Website erlauben – mithilfe von Puzzles, die vervollständigt werden müssen oder mit verzerrten Schriften, die interpretiert werden müssen – auszuschliessen, dass sich hinter dem angeblichen Nutzer ein Roboter versteckt. Auf diese Weise soll z. B. verhindert werden, dass ein Formular automatisiert in grosser Zahl ausgefüllt wird. Die reCAPTCHA erleichtern diesen Prozess, indem

131 https://www.itnews.com.au/news/govt-reveals-135bn-investment-into-cybersecurity-over-next-decade-549856
132 https://www.bbc.com/news/world-europe-50997773
133 https://blog.haschek.at/2020/the-a1-telekom-hack.html
134 https://www.zdnet.com/article/hackers-breached-a1-telekom-austrias-largest-isp/
135 https://www.heise.de/hintergrund/Massiver-Angriff-auf-A1-Telekom-Austria-4775451.html

sie die Website-Besucherinnen und –Besucher lediglich dazu auffordern, mit einem Klick im entsprechenden Kästchen zu bestätigen, dass sie keine Roboter sind.

Die Forschenden des IT-Sicherheitsunternehmens Barracuda haben festgestellt, dass Cyberkriminelle reCAPTCHA von Google benutzten um zu erschweren, dass ihre Angriffe aufgedeckt werden.[136] Mit dieser Massnahme können automatische Sicherheits-Systeme zur Überprüfung von Links in E-Mails nicht auf die eigentliche Phishing-Seite zugreifen und sie somit auch nicht als Phishing erkennen. Das Einfügen eines reCAPTCHA vor der Phishing-Seite bietet den Angreifern einen zusätzlichen Vorteil, weil dies von den Besucherinnen und Besuchern als Sicherheitsmassnahme wahrgenommen wird und sie in ihrem Irrglauben bestärkt, auf einer legitimen Website zu sein. In dem von Barracuda beobachteten Angriff verschickten die Cyberkriminellen ein E-Mail mit einer angeblich verlorengegangenen Sprachnachricht im Anhang. Beim Klick auf den Anhang wurde der Empfänger auf eine Internetseite weitergeleitet, die nur das reCAPTCHA enthielt. Nach der Bestätigung, man sei kein Roboter, gelangte man auf eine Seite, die sich als Login-Seite von Microsoft ausgab.[137]

Angriffe mit CAPTCHAs wurden auch in der Schweiz gesichtet, jedoch nicht gegen Schweizerische Firmenmarken sondern gegen internationale Zahlungssysteme, welche auch von Schweizer Bürgerinnen und Bürgern verwendet werden (z. B. PayPal).

Phishing as a service

Cybercrime-as-a-Service (CaaS) ist ein seit Jahren in allen Bereichen der Cyberkriminalität verbreitetes Konzept. Im Darknet wird ein breites Sortiment von Angriffsinstrumenten angeboten. Gemäss dem singalesischen IT-Sicherheitsunternehmen Group-IB werden immer mehr Sets für Phishing-Angriffe nachgefragt und die Angebote hätten sich gegenüber dem Vorjahr verdoppelt. Es hat zudem eine Verteuerung dieser Produkte festgestellt. Als «Set für Phishing-Angriffe» werden Script-Sets bezeichnet, mit denen eine Phishing-Webseite betrieben werden kann. 2019 zählten Amazon, Google, Instagram, Office 365 und PayPal zu den beliebtesten für Phishing verwendeten Marken. D. h. Phishing-Sets für sehr bekannte Marken mit einer grossen Anzahl an Nutzenden werden am meisten nachgefragt. Diese Angriffsinstrumente werden sozusagen von der Stange an Cyberkriminelle mit begrenzten technischen Fähigkeiten verkauft und ermöglichen die Erstellung unzähliger Phishing-Seiten.[138]

136 https://blog.barracuda.com/2020/04/30/threat-spotlight-malicious-recaptcha/ ;

137 https://hotforsecurity.bitdefender.com/blog/cybercriminal-are-using-google-recaptcha-to-hide-their-phishing-attacks-23156.html

138 https://securityaffairs.co/wordpress/101616/cyber-crime/underground-market-phishing-kits.html

Lage in der Schweiz

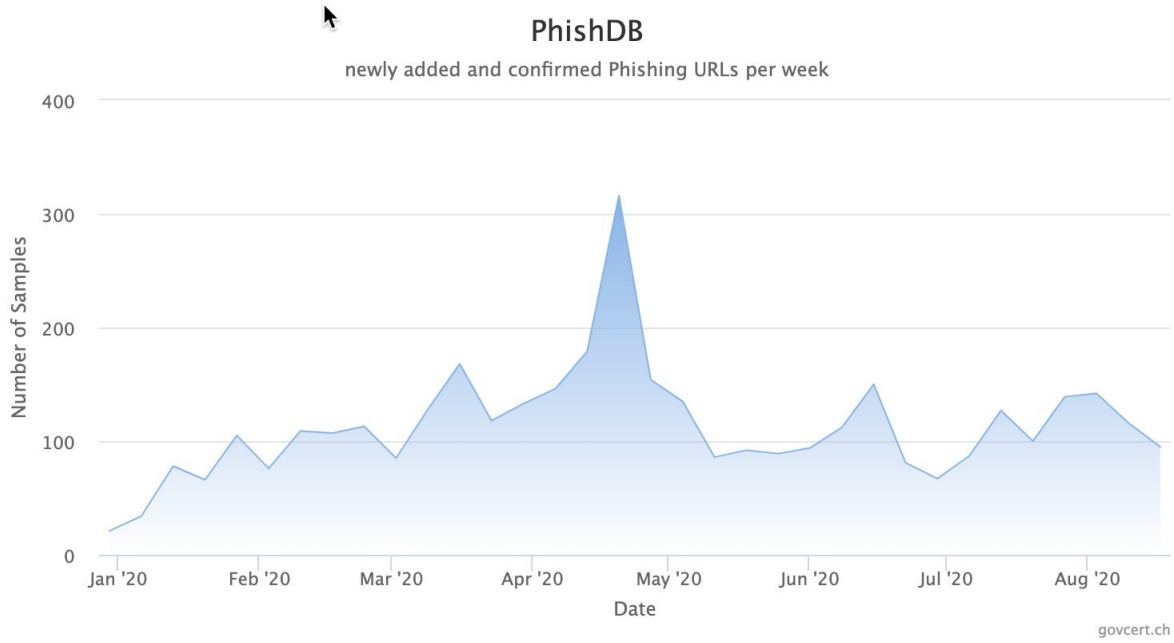

Abb. 7: Gemeldete und bestätigte Phishing-Seiten pro Woche auf antiphishing.ch im ersten Halbjahr 2020.

Im ersten Halbjahr 2020 wurden aufgrund mehrerer zehntausend Meldungen über das vom NCSC betriebenen Portal antiphishing.ch insgesamt 3'029 verschiedene Phishing-Webseiten entdeckt. Die Abbildung 7 zeigt die wöchentlich identifizierten Phishing-Webseiten im ersten Halbjahr 2020.

Ab April 2020 verzeichnete das NCSC eine Zunahme der Phishing-Angriffe auf Websitebetreiber und Domainbesitzer. Um sich Zugangsdaten für die Administration von Websites zu beschaffen, schickten die Cyberkriminellen den Websitebetreibern und Domainbesitzern Phishing-E-Mails, die angeblich vom jeweiligen Hosting Provider stammten. Die meisten dieser E-Mails enthielten einen persönlichen Link, der via eine infizierte Website auf die finale Phishing-Seite weiterleitete. Dort war jeweils der Domainname und/oder der Name des Hosting-Providers bereits vorausgefüllt und das Opfer wurde aufgefordert, seine Zugangsdaten einzugeben.

Empfehlungen:

INFO

Das GovCERT hat auf seinem Blog einen Beitrag (auf Englisch) veröffentlicht, der die Angriffe auf Webmaster detailliert beschreibt, zusammen mit allgemeinen Empfehlungen für Nutzende sowie spezifischen Ratschlägen für Hosting-Provider.

4.7.2 Spoofing – Gefälschte Absender

Spoofing (aus dem Englischen *to spoof* = jemanden täuschen oder etwas fälschen) bedeutet in der Informationstechnik das Vortäuschen einer Identität insbesondere durch die Veränderung von Adressierungselementen, wie z. B. dem E-Mail-Absender oder Telefonnummern, aber auch Websites, IP-Adressen, MAC-Adressen (Media Access Protocol) oder ARP-Nachrichten (Address Resolution Protocol) können gefälscht werden.[139] Spoofing wird eingesetzt, um dem Adressaten Vertrauenswürdigkeit zu suggerieren und ihn schliesslich zu einem bestimmten Verhalten zu bewegen. Es ist entsprechend eine Social-Engineering-Technik.

Spoofing-Methoden werden entlang der digitalen Möglichkeiten kontinuierlich weiterentwickelt und verbessert. Daher ist Spoofing trotz teilweise vorhandenen Schutzmassnahmen weit verbreitet. Sowohl kriminelle als auch staatliche Akteure setzen eine Vielzahl unterschiedlicher Spoofing-Methoden in verschiedenen Kontexten erfolgreich ein. Dazu fälschen sie E-Mail-Adressen, Telefonnummern, SMS-Absender, Logos und Firmennamen, um das menschliche Vertrauen und Informationsbedürfnis der Empfänger auszunützen. Während der COVID-19-Pandemie wurde beispielsweise Schadsoftware per E-Mail an die Schweizer Bevölkerung versendet, mit dem Bundesamt für Gesundheit als gefälschtem Absender (siehe Kap. 3.1.1).

Spoofing von E-Mail-Adressen: Das Spoofing von E-Mail-Adressen gestaltet sich einfach, da das verwendete Protokoll SMTP (Simple Mail Transfer Protocol) die Absenderadresse nicht überprüft. Ist ein E-Mail-Server ungeschützt im Internet offen verfügbar, kann sich jeder Nutzer damit verbinden und E-Mails versenden. Der anzuzeigende Absendername kann beliebig gewählt werden. Sofern beim E-Mail-Server keinerlei Einschränkungen konfiguriert sind, kann auch die Absenderadresse frei definiert werden und einen Domainnamen enthalten, mit dem der Server nicht assoziiert ist, wie beispielsweise rechnung@ncsc.ch.

Es sind allerdings technische Schutzmassnahmen möglich:

- Im Sender-Policy-Framework (SPF) können Server eingetragen werden, die berechtigt sind, E-Mails mit einer bestimmten Domäne als Absenderadresse zu versenden. Versendende, übermittelnde und empfangende Server können E-Mails anhand des SPF überprüfen und gegebenenfalls ausfiltern.
- DomainKeys Identified Mail (DKIM) versieht ein E-Mail mit einer digitalen Signatur, mit welcher vom Empfängersystem überprüft werden kann, ob die in der E-Mail-Absenderadresse enthaltene Domäne korrekt ist und dass das E-Mail auf dem Weg der Zustellung nicht verändert wurde. Schlägt die Überprüfung fehl, wird die Annahme des E-Mails verweigert.
- Die Domain-based Message Authentication and Conformance (DMARC), baut auf der Authentisierung des Absenders (SPF) und der Überprüfung der Integrität (DKIM) auf und setzt dabei eine Signaturprüfung voraus.

Spoofing von Telefonnummern und SMS-Absendern: Dank Internettelefonie (Voice over IP, VoIP) können Nummern heutzutage relativ einfach gefälscht oder verschleiert werden. Es gibt sogar einen Markt für Dienste, die Rufnummernfälschung (Caller-ID-Spoofing) anbieten. Über Internetdienste können auch SMS verschickt werden. Da dafür kein Mobiltelefon und auch keine entsprechende Nummer benötigt wird, kann bei einigen Diensten der Anzeigename

[139] Vgl. z. B. https://www.cybersecurityintelligence.com/blog/beware-spoofing-attacks-4890.html

beliebig gewählt werden. Internationale Initiativen versuchen das Spoofing von Rufnummern zu unterbinden.[140] Zur Zeit gibt es jedoch noch keine anbieterübergreifende technische Massnahme, mit welcher Rufnummer-Spoofing unterbunden werden könnte. Die Einführung eines entsprechenden Standards dürfte noch lange auf sich warten lassen. In den meisten Staaten ist Rufnummer-Spoofing nicht strafrechtlich verboten, sondern fällt unter Privatrecht, so auch in der Schweiz. Entsprechend kann nur die Person rechtlich gegen das Spoofing vorgehen, deren Identität missbraucht wurde – nicht die Empfänger solcher Nachrichten. Mit der geplanten Revision des Datenschutzgesetzes soll jedoch eine Bestimmung ins Strafgesetz eingeführt werden, gemäss welcher Identitätsdiebstahl und damit auch gewisse Formen von Rufnummern-Spoofing unter Strafe gestellt wird.

Spoofing von Websites: Websites können kopiert und unter einer anderen Webadresse aufgeschaltet werden. Auch auf nachgeahmten Websites kann mit der Einbindung von originalen Logos ein Wiedererkennungseffekt erzielt werden. Wenn Nutzende den in der Adresszeile aufgeführten Domainnamen nicht prüfen und ihnen nicht auffällt, dass kein bzw. ein falsches Zertifikat verwendet wird, können sie durch solche Websites getäuscht werden. Betrüger registrieren häufig sogenannte Typo-Domains, die sich nur unmerklich von der Originaladresse unterscheiden, wie etwa: "svvisscom.ch" statt "swisscom.ch". Typo-Domänen können auch für den Versand von E-Mails verwendet und so etwa für Phishing, Betrug oder zur Verbreitung von Schadsoftware benutzt werden.

Spoofing-Methoden werden von manchen Angreifern auch erfolgreich kombiniert eingesetzt: Die «Retefe»-Gruppe benutzt Anrufe mit gefälschten Telefonnummern, um ihre Opfer unter einem Vorwand zu überzeugen, eine PDF-Datei zu öffnen, welche vor, während oder nach dem Telefongespräch per E-Mail zugestellt wird (siehe Kap. 4.7.4). Klickt das Opfer auf den darin enthaltenen Link, wird der Computer mit dem E-Banking-Trojaner «Retefe» infiziert. Zum Schutz von Schweizer Unternehmen und der Bevölkerung stellt das NCSC den Internetanbietern Informationen zur Verfügung, damit sie Zugriffsversuche ihrer Kunden auf Websites, über welche «Retefe» verbreitet wird, blockieren können. Um schädliche Links zu verschleiern werden oft Linkverkürzungsmethoden verwendet, sogenannte *shortener services* wie z. B. bit.ly oder goo.gl.

Hinweis / Empfehlung:

Absenderadressen bei jeglichen Nachrichten können grundsätzlich gefälscht werden.

Insbesondere beim Empfang von neuartigen oder ungewöhnlichen Nachrichten gilt es immer, eine gesunde Portion Skepsis aufzubringen. Statt Links in solchen Nachrichten zu folgen, sollten Sie sich wenn möglich über den gewohnten Weg in Ihr Nutzerkonto einloggen. Verifizieren Sie vor der Eingabe von persönlichen Daten, Passwörtern oder Kreditkarteninformationen immer, ob Sie sich tatsächlich auf der gewünschten Seite befinden.

Klicken Sie in verdächtigen Nachrichten nicht auf Links – auch nicht aus reiner Neugier. Sie riskieren sonst Ihr Gerät mit Schadsoftware zu infizieren oder auf dubiosen Websites zu landen. Fragen Sie im Zweifelsfall beim vermeintlichen Absender über eine auf seiner Website angegebene oder anderweitig bereits bekannte Kontaktmöglichkeit nach, worum es sich genau handelt und ob die Nachricht tatsächlich von ihm stammt.

[140] Z. B. "STIR/SHAKEN", siehe https://www.metaswitch.com/knowledge-center/reference/what-is-stir/shaken

4.7.3 Smishing

Smishing ist eine Zusammensetzung der Wörter SMS und Phishing. Smishing meint im Allgemeinen den Missbrauch von SMS, aber zunehmend auch Instant-Messaging-Applikationen wie WhatsApp, als Angriffsvektor zum Diebstahl von sensiblen Informationen, wie etwa Zugangsdaten, Passwörtern, Kreditkarten- und Kontoinformationen. Häufig werden dabei die Absendernummern und –namen gefälscht (siehe Kapitel 4.7.2 zu Spoofing hiervor). Smishing wird von Kriminellen auch benutzt, um mobile Zahlungsdienste zu missbrauchen, den *mTAN* abzugreifen oder die Zweifaktor-Authentifizierung zu umgehen, z. B. mit einem *SMS-Stealer*. In der Schweiz und im Ausland wurde auch die Kombination von Social-Engineering-Techniken beobachtet: Opfer wurden per Kurznachricht dazu aufgefordert, einen per SMS gerade erhaltenen Authentifizierungscode weiterzuleiten, unter der Behauptung, dass dieser versehentlich zugestellt worden sei oder der Vortäuschung eines Notfalls. Mit dieser Methode können theoretisch alle mit Zwei-Faktor-Authentifizierung geschützten Dienste kompromittiert werden, sofern ein Angreifer vorher Login, Passwort und Telefonnummer des Opfers in Erfahrung gebracht hat. Im Fall von WhatsApp kann gemäss Standardeinstellungen mit einem solchen Authentifizierungscode allein das gesamte Benutzerkonto einer Person übernommen werden.[141]

Gerade Mobiltelefon-Bezahldienste standen im ersten Halbjahr 2020 im Visier von Betrügern. Mit solchen Diensten können Rechnungen über die Telefonrechnung bezahlt werden. Der Dienstleister sendet hierzu einen SMS-Code an das Mobiltelefon, der dann zur Bestätigung auf der Webseite wiederum eingegeben werden muss. In einem Fall wurde den Opfern vorgegaukelt, dass ein Paket nicht zugestellt werden konnte. Um die Zustellung zu initiieren musste die Telefonnummer angegeben und anschliessend eine App heruntergeladen werden. Bei der App handelte es sich um einen *SMS-Stealer*. Die Betrüger lösten anschliessend Bezahlungen mit der Mobiltelefonnummer des Opfers aus und die App leitete den Bestätigungscode direkt an die Kriminellen weiter.

Vermehrt wird auch die Verbreitung von Links zu Schadsoftware per SMS beobachtet, wie etwa «Emotet» oder «EventBot», die dazu dient, Zugangsdaten zu E-Banking- und Finanz-Applikationen zu stehlen.[142] Bei Smishing kommen auch gefälschte Absender und, wie bereits erwähnt, Social-Engineering-Techniken im Allgemeinen zum Einsatz, um bei Zielpersonen ein bestimmtes Verhalten zu provozieren. Hierfür bedienen sich Angreifer auch aktueller Grossereignisse und ihren Auswirkungen, wie etwa der COVID-19 Pandemie: Im März 2020 warnten die südkoreanischen Behörden beispielsweise vor Smishing im Zusammenhang mit Informationen zur Verbreitung von COVID-19. Bereits Mitte Februar waren in Südkorea fast 10'000 Nachrichten verschickt worden, die behaupteten von Unternehmen zu stammen, die kostenlos Schutzmasken zur Verfügung stellen.[143]

Smishing-Angriffe stellen eine wachsende Bedrohung dar, sowohl für die Bevölkerung als auch für Unternehmen: In den USA wurde im ersten Quartal 2020 alleine bei Unternehmen ein Anstieg von Phishing auf Mobilgeräten um 37 Prozent verzeichnet.[144] In der Schweiz halten

---

[141] Vgl. diesbezüglich auch https://www.20min.ch/story/mit-diesem-code-bist-du-dein-whatsapp-8203-8203-konto-los-252382069481 und https://www.mimikama.at/allgemein/vorsicht-wenn-ein-whatsapp-kontakt-einen-verifizierungscode-verlangt/

[142] Betreffend «EventBot», siehe https://www.zdnet.de/88379272/cybereason-warnt-vor-neuem-mobilen-banking-trojaner/; betreffend «Emotet», siehe: https://threatpost.com/sms-attack-spreads-emotet-bank-credentials/153015/

[143] https://www.zdnet.com/article/south-korea-sees-rise-in-smishing-with-coronavirus-misinformation/;

[144] https://blog.lookout.com/global-mobile-phishing-encounters-surged-by-37-percent-amid-wfh-shift

sich die öffentlich bekannten Fälle noch in einem kleineren Rahmen: Bis Juli 2020 wurden dem NCSC insgesamt 16 Smishing Fälle gemeldet, wobei fast die Hälfte der Fälle im Monat Juni registriert wurde. Für das nächste Halbjahr rechnet das NCSC jedoch mit einer Zunahme dieses Phänomens.

Auch Betrugsmaschen kursieren über SMS und Messaging-Dienste: Nachrichten mit gefälschtem Absender bekannter Schweizer Firmen wie Coop, Migros oder der Post verleiteten Empfänger zum Abschluss kostenpflichtiger Mehrwertdienste, etwa unter Vorgabe eines Gewinnspiels oder Gutscheins (siehe Kap. 3.1.3).

Hinweis / Empfehlung:

Absenderadressen bei jeglichen Nachrichten können grundsätzlich gefälscht werden.

Bei der E-Mail-Infrastruktur wurden über die Jahre sehr effiziente Filtermethoden entwickelt, insbesondere um Spam-Nachrichten auszusortieren. Diese Technologie lässt sich nicht ohne Weiteres bei SMS anwenden. Bei Messenger-Diensten wie WhatsApp oder Threema wird überhaupt kein entsprechender Mechanismus eingeführt werden können, da die Nachrichten verschlüsselt vom Absender zum Empfänger übertragen werden und kein Intermediär den Inhalt prüfen kann.

Klicken Sie in verdächtigen Nachrichten nicht auf Links – auch nicht aus reiner Neugier. Sie riskieren sonst Ihr Gerät mit Schadsoftware zu infizieren oder auf dubiosen Websites zu landen. Fragen Sie im Zweifelsfall beim vermeintlichen Absender über eine auf seiner Website angegebene oder anderweitig bereits bekannte Kontaktmöglichkeit nach, worum es sich genau handelt und ob die Nachricht tatsächlich von ihm stammt.

Verifizieren Sie vor der Eingabe von persönlichen Daten, Passwörtern oder Kreditkarteninformationen immer, ob Sie sich tatsächlich auf der gewünschten Seite befinden.

4.7.4 Bei Anruf Malware

Dass Betrüger auch einen grossen Aufwand auf sich nehmen, um Malware bei einem Opfer zu installieren, zeigen Fälle, die dem NCSC im ersten Halbjahr 2020 in verschiedenen Varianten 64 Mal gemeldet wurden. Allen Varianten gleich war der Umstand, dass das Opfer zusätzlich zum versendeten E-Mail noch angerufen wurde. Entweder starteten die Betrüger mit einem Telefonanruf bei dem ein E-Mail mit einem PDF-Dokument angekündigt wurde oder die Betrüger kontaktierten das Opfer im Nachhinein, um sicherzugehen, dass dieses das E-Mail auch tatsächlich beachtet, das angehängte Dokument öffnet und auf den darin enthaltenen Link klickt. Mit dem Anklicken dieses Links wurde dann die Schadsoftware installiert.

Oft verwendete Namen der anrufenden Firma, welche sich jeweils als Zustellservice ausgab, waren CH-Express, Delivery Experts oder Delivery Schweiz. Angegriffen wurden vor allem kleinere Firmen wie Architekturbüros, Gartenbaufirmen oder Schreinereien. Meist ging es bei der Zustellung um Anfragen für Offerten. In vielen Fällen gab sich die Täterschaft als eine Hochschule aus und verwendete für den Versand der E-Mails einen Domainnamen, welcher dem echten Domainnamen der Hochschule zum Verwechseln ähnlich ist (so genannte *Typo-Domain*). In einer späteren Phase richteten sich die Angriffsversuche allerdings auch gegen Privatpersonen.

Abb. 8: Vorgehensweise zur Infektion mit dem Trojaner «Retefe». Das für den Anruf verwendete Szenario kann beliebig ändern.

Die aktuelle Pandemie wurde ebenfalls herangezogen, um die Opfer zu überzeugen, die Schadsoftware zu installieren. So wurde behauptet, dass man aufgrund der Infektionsgefahr den Empfang eines Paketes nicht per Unterschrift bestätigen könne, sondern dass per E-Mail ein Bestätigungscode versendet werde, den der Empfänger dem Kurier mitteilen müsse. Auch hier wurde telefonisch vorgegaukelt, dass der Code in der PDF-Datei enthalten sei, welche dem E-Mail angehängt ist und nur angeklickt werden müsse (s.a. Kap. 4.7.2 zu Spoofing). Detaillierte Informationen sind auf der Seite von cybercrimepolice.ch aufgeführt.[145]

Schlussfolgerung / Empfehlungen:

Dass die Angreifer den Aufwand auf sich nehmen, jedes einzelne Opfer anzurufen, erstaunt. Anscheinend ist es für die Angreifer nicht mehr so einfach, Malware auf ein Gerät zu bringen, so dass die Kriminellen diesen grösseren Aufwand auf sich nehmen müssen. Ebenfalls erstaunlich ist, dass sich der bösartige Link nicht direkt im E-Mail sondern in der angehängten PDF-Datei befindet. Ob sich das aber auch lohnt, ist zu bezweifeln. Dieser Ansatz dürfte eher kontraproduktiv sein, da es den Angriff komplizierter macht und so das Opfer Zeit erhält, über die Plausibilität der Geschichte nachzudenken. Nicht wenige wurden nach dem Öffnen der PDF-Datei skeptisch und haben abgebrochen. Es gilt deshalb mehr denn je vorsichtig beim Öffnen von Links und Anhängen zu sein und sich vor allem nicht zu einer Aktion drängen zu lassen.

145 https://www.cybercrimepolice.ch/de/fall/online-betrueger-aufforderung-packetsendung-freischalten-nicht-nur-per-mail-sondern-neu-auch-per-telefon/

4.7.5 Erpresste Websitebetreiber

Im Berichtszeitraum erhielten zahlreiche Websitebetreiber betrügerische Erpressungs-E-Mails, in denen Kriminelle behaupten, sie hätten diese Website dank einer Schwachstelle gehackt und die ganze dahinterliegende Datenbank gestohlen.[146] Sie drohten, die Kunden zu informieren, die gestohlenen Daten zu veröffentlichen oder zu verkaufen und damit den Ruf des Opfers zu schädigen, es sei denn, es werde ein Lösegeld in Bitcoins bezahlt. In der Schweiz wurden in Englisch und Deutsch verfasste E-Mails beobachtet. In einem Fall behauptet der Absender, der angebliche Angriff sei von einem Konkurrenzunternehmen in Auftrag gegeben worden, in der Absicht, den Empfänger des E-Mails zu sabotieren. Der Auftraggeber würde jedoch über den zuvor vereinten Preis feilschen wollen, was den Cyberkriminellen verärgert und dazu veranlasst habe, das angebliche Opfer zu kontaktieren, mit dem Angebot, die gestohlenen Daten zurückzugeben, natürlich gegen eine üppige Entschädigung. In dieser Variante werden als weiteres Druckmittel auch die rechtlichen Probleme erwähnt, mit denen sich das Opfer aufgrund der Verletzung der Europäischen Datenschutzgrundverordnung (EU-DSGVO) konfrontiert sehen würde (siehe auch Kap. 4.5 zu Datenabflüssen).

Im Rahmen dieses Betrugs nützen die Cyberkriminellen die Angst der Websitebetreiber vor den Folgen eines allfälligen Datenlecks aus, in der Hoffnung, dass sie deswegen das Lösegeld bezahlen würden. Die Websites sind jedoch nicht wirklich kompromittiert, zumindest nicht in denjenigen Fällen, von denen das NCSC Kenntnis hat. Diese E-Mails erinnern sehr stark an die Wellen sogenannter «Fake-Sextortion», über die in den vergangenen Halbjahresberichten mehrmals informiert wurde. Bei diesen behaupten die Betrüger, die Computerkamera des Opfers gehackt und dieses beim Konsum von Pornografie erwischt zu haben.[147] Auch in diesen Fällen waren die Computer gar nicht wirklich angegriffen worden und die Cyberkriminellen besassen gar kein Material, mit dem die erpresste Person geschädigt werden konnte. Doch die Angreifer nutzten die Methoden des Social Engineering aus, um das Opfer dennoch dazu zu bringen, einen bestimmten Betrag in Bitcoins zu bezahlen.

Empfehlungen:

Bewahren Sie Ruhe, wenn Sie ein Erpresserschreiben erhalten. Lassen Sie sich nicht unter zeitlichen Druck setzen. Vielfach sind Erpressungen haltlos und werden an eine grosse Zahl von Personen geschickt, in der Hoffnung, dass einige der Empfänger sich einschüchtern lassen und vorschnell bezahlen. Erpressungsversuche sind grundsätzlich strafbar und können bei der Polizei zur Anzeige gebracht werden.

Wenn Sie Hinweise haben, dass die Behauptungen zutreffen könnten, melden Sie sich unbedingt bei der nächsten Kantonspolizeistelle (siehe https://polizei.ch/), damit Ermittlungen gegen die Täter aufgenommen werden können.

146 https://www.watchlist-internet.at/news/website-betreiberinnen-aufgepasst-erpressungsmails-im-umlauf/

147 Siehe MELANI Halbjahresbericht 2018/2 Kap 4.4.2 und 2019/2, Kap. 4.4.3; MELANI Website: https://www.melani.admin.ch/melani/de/home/meldeformular/formular0/meldeformularhaeufigefragen/FakeSextortion.html

4.8 Präventive Massnahmen und Strafverfolgung

4.8.1 Anklage gegen deutschen «Bulletproof Hoster»

«*Bulletproof Hosting*» sind Datencenter, die darauf ausgelegt sind, sich behördlichem Zugriff – insbesondere von Strafverfolgungsorganen – zu entziehen. Zum einen werden häufig Standorte in Ländern ausgesucht, wo die Justiz nicht sehr effektiv funktioniert, zum anderen (oder zusätzlich) wird der Standort durch verschiedenste Falschangaben und Strohmänner bei der administrativen und technischen Einbindung ins Internet verschleiert. «Bulletproof Hosting» dient verschiedensten Formen von Kriminalität.

Den deutschen Behörden gelang im letzten Herbst nach vier Jahren strafrechtlichen Ermittlungen der Zugriff auf einen solchen Bulletproof Hoster, welcher jahrelang aus einem ausrangierten NATO-Bunker in Deutschland operierte und verschiedenen Cyberkriminellen seine Plattform zur Verfügung stellte. So wurden unter anderem der Drogenumschlagplatz «Wall Street Market», der Darknet-Marktplatz «Flugsvamp», der 90 Prozent des Online-Drogenhandels in Schweden abwickelte, sowie das «Mirai-Botnetz» auf Servern des Cyberbunkers verwaltet. Im Herbst letzten Jahres haben mehr als 700 Einsatzkräfte das Gelände des Bunkers in Traben-Trarbach durchsucht und mehr als 800 Server vom Netz genommen. Nun erhebt die Generalstaatsanwaltschaft Anklage gegen acht Personen wegen Beihilfe zu zahlreichen Straftaten, darunter Datenhehlerei, Botnetz-Attacken, Drogenhandel. Weiter wurden auch Verbindungen zu Kinderpornografie und Mordaufträgen gefunden. Das komplexe Verfahren umfasst Datenspeicher mit einer Kapazität von insgesamt zwei Petabyte und lässt die Ermittlungskräfte an ihre Kapazitätsgrenzen stossen.

Beihilfe nach deutschem Recht bedarf immer auch, dass eine Haupttat vorliegt. Dies bedeutet, dass die Ermittler zuerst die Straftaten an sich aufklären mussten, welche mit im Cyberbunker gehosteten Websites verübt worden waren. Dabei war es eine Herausforderung, auf das interne E-Mail-System des Cyberbunkers zuzugreifen, worüber die Kommunikation zwischen Hoster und den Kunden stattfand. Diese Kommunikation ist ausschlaggebend, um den angeschuldigten Betreibern nachzuweisen, dass sie nicht lediglich als technische Dienstleister agierten, welche keine Verantwortlichkeit trifft, sondern willentlich an den Straftaten mitwirkten und sich somit der Beihilfe strafbar machten.[148]

4.8.2 Schweizerische Strafverfolgung verhaftet Cyberkriminelle

Schweizerische und polnische Strafverfolgungsbehörden haben mit Unterstützung von Europol im April 2020 die Hackergruppe «InfinityBlack» aufgelöst. «InfinityBlack» war eine Gruppe von Cyberkriminellen, die an der Verbreitung gestohlener Benutzerdaten, der Erstellung und Verbreitung von Malware und Hackertools sowie an Betrug beteiligt war.

Die Polizei beschlagnahmte elektronische Geräte, externe Festplatten und Hardware-Brieftaschen mit Kryptogeld im Wert von rund 100'000 Euro. Zwei Plattformen mit Datenbanken, die über 170 Millionen Einträge enthielten, wurden von der Polizei ebenfalls beschlagnahmt und geschlossen.

---

[148] https://www.heise.de/newsticker/meldung/Cyberbunker-Staatsanwaltschaft-erhebt-Anklage-gegen-Betreiber-4698785.html

Das Geschäftsmodell der Hackergruppe bestand darin, Online-Plattformen zum Verkauf von Benutzeranmeldeinformationen (sogenannten «Combos») zu schaffen. Die Gruppe war effizient in drei definierten Teams organisiert. Die Entwickler schufen Werkzeuge, um die Qualität der gestohlenen Datenbanken zu testen, während die Tester die Eignung der Berechtigungsdaten analysierten. Die Projektleiter schliesslich verkauften die Daten gegen Zahlungen in Kryptowährung. Die Hacker erlangten so Zugang zu einer grossen Zahl von Schweizer Kundenkonten. Obwohl die Verluste auf nur 50'000 Euro geschätzt werden, hatten die Hacker Zugang zu Konten, von welchen insgesamt mehr als 610'000 Euro hätten abfliessen können. Die Haupteinnahmequelle der Hackergruppe bestand darin, Anmeldedaten für das Treueprogramm eines schweizerischen Grossverteilers zu stehlen und sie an andere, weniger technisch versierte kriminelle Gruppen weiterzuverkaufen. Diese tauschten in der Folge die Treuepunkte gegen teure elektronische Geräte ein. Die Betrüger und Hacker, unter ihnen Minderjährige und junge Erwachsene, wurden entlarvt, als sie die gestohlenen Punkte in Geschäften in der Schweiz gegen Ware eintauschen wollten. Nach der Verhaftung der Täter deckte die Polizei Verbindungen zu einer Hackergruppe in Polen auf. Die Übermittlung der Daten der durchsuchten Computer an die polnischen Behörden führten schliesslich zu weiteren Verhaftungen von «InfinityBlack»-Mitgliedern in Polen.[149]

5 Forschung und Entwicklung

5.1 SCION: Ein sicheres Internet mit hoher Leistung

Ilona Wettstein, Adrian Perrig, ETH Zürich, Network Security Group

Die zunehmende Digitalisierung aller Lebens- und Wirtschaftsbereiche erfordert ein sicheres Internet. So vertrauen täglich Milliarden Menschen darauf, dass sie Daten verschicken können, ohne dass diese verloren gehen, abgezweigt oder unterwegs analysiert werden. Gleichzeitig soll Sicherheit nicht mit einer Einbusse von Leistung einhergehen, d. h. die Sicherheitsmechanismen sollen die Netzwerkkapazität nicht reduzieren oder zu zusätzlichen Verzögerungen bei der Zustellung von Daten führen.

149 https://www.europol.europa.eu/newsroom/news/hacker-group-selling-databases-millions-of-user-credentials-busted-in-poland-and-switzerland ; https://www.blick.ch/news/cyberkriminalitaet-treuepunkte-hacker-nach-polizeioperation-in-waadt-in-polen-gefasst-id15877097.html; https://www.watson.ch/!158091108

Dem Internet liegt das seit 30 Jahren beinahe unveränderte *Border Gateway Protocol (BGP)* zugrunde, das Datenpakete durch das Internet leitet. An jedem Netzwerkknoten entscheidet es, welchen Weg ein Datenpaket nehmen soll. Durch die starke Expansion des Internets weist dieses Protokoll heute viele Schwachstellen auf und es wird ersichtlich, dass das Internet auf einem zerbröckelnden Fundament gebaut ist: Datenverkehr wird durch staatliche oder kriminelle Akteure umgeleitet und kann durch diese ausspioniert oder unterbrochen werden.

SCION ist eine neuartige Internet-Architektur.[150] Der Name steht für «**S**calability, **C**ontrol, and **I**solation **O**n **N**ext-Generation Networks». Die Architektur wurde an der ETH Zürich entwickelt, ersetzt BGP durch ein sichereres und effizienteres Protokoll und löst viele weitere Sicherheitsprobleme des heutigen Internets, z. B. gefälschte Sicherheitszertifikate oder *Distributed-Denial-of-Service-Angriffe* (DDoS-Attacks). Im Gegensatz zum bisherigen Internet, in welchem alle Routing-Entscheidungen durch die Netzwerkknoten übernommen werden, bietet SCION den Nutzern Transparenz und Kontrolle über die Netzwerkpfade. Den Datenpaketen werden die genauen Pfade für ihren Weg durch das Internet bereits zum Zeitpunkt des Abschickens mitgegeben und können daher nicht fehlgeleitet werden. Zudem kann mit diesem Ansatz durch intelligente Pfadwahl die Übermittlungszeit der Datenpakete optimiert werden. Durch die Benutzung mehrerer Pfade kann SCION ausserdem innert Millisekunden auf einen neuen Pfad ausweichen, sollte es eine Beeinträchtigung der Kommunikation geben.

Die entwickelte Architektur wird bereits von den Eidgenössischen Hochschulen und von mehreren Banken eingesetzt. Eine SCION-Verbindung bietet eine Vielzahl entscheidender Vorteile:

- Garantierte Kommunikation und Souveränität im Internet: Die Kommunikation kann nicht durch Angriffe aus dem Ausland oder einzelner Akteure unterbunden werden (kein «*Kill Switch*»).
- Ermöglichen einer organisatorischen oder geographischen Beschränkung des Datenverkehrs. So wird verhindert, dass vertrauliche Informationen durch nicht-vertrauenswürdige Netzwerke fliessen.
- Gleichzeitige Nutzung mehrerer Verbindungen zur Optimierung der Kommunikation und Erhöhung der Zuverlässigkeit selbst bei Ausfällen von Verbindungen («Business Continuity»).
- Höhere Kapazität durch die Nutzung von mehreren Netzwerkpfaden.

Das Internet der nächsten Generation verspricht somit nicht nur höhere Sicherheit, sondern auch eine bessere Leistung als das heutige Internet. Mehrere Internet Service Provider fungieren in einem Konsortium als Integratoren und Anbieter der Verbindungen in der Schweiz und im Ausland. Kommerzialisiert und implementiert wird SCION derzeit von Anapaya Systems, einem Spin-off der ETH Zürich.[151]

---

150 https://www.scion-architecture.net/

151 https://www.anapaya.net/

6 Ausblick und Tendenzen der Lage

6.1 Arbeiten überall – nicht mehr unbedingt im Büro

Wie bereits im Schwerpunktthema angesprochen (Kapitel 3.5), hat sich die Arbeitswelt durch die COVID-19-Pandemie insbesondere für Büroangestellte verändert. Viele konnten oder mussten im Homeoffice arbeiten. Dadurch haben viele Unternehmen und Arbeitende Erfahrungen mit Homeoffice und anderen Arbeitsmodellen gesammelt, bei denen nicht mehr im Büro, sondern von beliebigen Standorten aus gearbeitet wird. Dies wird zu einer grösseren allgemeinen Akzeptanz von – wenn nicht sogar Forderung nach – ortsunabhängigem Arbeiten führen. Es ist noch nicht absehbar, wann genau die aktuelle Pandemie vorüber sein wird und wieder zur vorherigen Normalität zurückgekehrt werden könnte. Dabei muss berücksichtigt werden, dass die Rückkehr zu vorpandemischen Arbeitsumständen vielleicht weder möglich noch wünschenswert ist. Während einige Unternehmen bereits vor längerer Zeit eine stabile und sichere Infrastruktur für ortsunabhängiges Arbeiten aufgebaut haben, verfügen andere bislang erst über kurzfristig implementierte und eher improvisierte Lösungen. Es lohnt sich, bereits jetzt von den gemachten Erfahrungen zu profitieren und die verwendeten Lösungen zu überprüfen, um sie zu verbessern oder ein Projekt zur kompletten Neugestaltung zu starten, damit neben den benötigten Kapazitäten der Infrastruktur auch die Sicherheit von Geräten, Netzwerken und Daten von Anfang an adäquat berücksichtigt werden kann (Security by Design).

Fernzugriffsinfrastrukturen bieten einen Angriffsvektor zur Kompromittierung von Unternehmensnetzwerken. Sowohl Verbindungen über VPN als auch via RDP müssen sicher konfiguriert und adäquat geschützt werden. Bereits seit einiger Zeit suchen Akteure das Internet nach verwundbaren Implementationen von Fernzugriffslösungen ab. Nach der pandemiebedingten Zunahme der Verwendung von Fernzugriffslösungen haben entsprechende Scanning-Aktivitäten signifikant zugenommen (siehe Kap. 3.5). Jedes verwundbare System wird früher oder später gefunden und angegriffen. Über Fernzugriffe kann nicht zuletzt eine Ransomware ins Firmennetzwerk eingeschleust werden (siehe Kap. 4.1.1 zu Ransomware und Kap. 4.4 zu Schwachstellen).

Cloud-Kollaborationsplattformen und Konferenzsoftware sind wichtige Hilfsmittel für das ortsunabhängige Arbeiten. Auch bei deren Verwendung müssen angemessen sichere Konfigurationen gewählt und Mitarbeitende im sicheren Umgang mit diesen Hilfsmitteln geschult werden.

Das Arbeiten auf privaten Geräten (*Bring Your Own Device*, BYOD), die nicht von der IT-Abteilung des Unternehmens unterhalten werden, verringert die Kontrolle des Unternehmens über die Sicherheit seiner Daten und nimmt Arbeitnehmende stärker in die Pflicht. Damit sie dieser Pflicht adäquat nachkommen können, müssen sie vom Unternehmen gemachte Vorgaben kennen und verstehen sowie regelmässig auf Bedrohungen und Gefahren hin sensibilisiert werden.

Empfehlungen:

Angesichts der vielseitigen Risiken, die ortsunabhängiges Arbeiten mit sich bringen, sollten eine klare Strategie und ein umfassendes Implementierungskonzept erstellt werden. Neben technischen Sicherheitsmassnahmen sind auch Nutzeraspekte zu berücksichtigen, denn die Anwendenden können mit ihrem Verhalten massgeblich zur Reduktion von Risiken beitragen.

Lassen Sie sich von den MELANI-Checklisten zu Homeoffice inspirieren:

Für Unternehmen: https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/fernzugriff.html

Für Nutzende: https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/fernzugriff-enduser.html

6.2 Die Geopolitisierung des Internets

Wer sich mit den Anfängen des Internets auseinandersetzt, wähnt sich schon sehr bald in einer Welt rein technisch versierter Forscher, hochbürokratischer Standardisierungsgremien und IT-affiner Frühnutzer. Diese hatten wohl vieles, aber kaum Konzepte wie internationale Sicherheits-, Geo- oder Machtpolitik, UNO und Diplomatie im Sinn. Organisationen wie die Advanced Research Projects Agency (ARPA), die Internationale Fernmeldeunion (ITU), die Internet Assigned Numbers Authority (IANA), die Internet Corporation for Assigned Names and Numbers (ICANN) und der in Genf stationierte Conseil Européen pour la Recherche Nucléaire (CERN) waren oder sind heute noch die massgebenden Gründer oder Hüter des heutigen Internets. Einer weltumspannenden Infrastruktur, die die meisten im Jahre 2020 als gegeben betrachten und, wie die Namen der involvierten Organisationen suggerieren, in erster Linie einfach als der nächste technische Schritt in Sachen Kommunikation und Technologie erachtet wurde - am besten unterhalten in den Händen von unpolitischen Fachexperten.

Unterdessen bildet das Internet das zentrale Element fast jeder wirtschafts- und sozialpolitischen Entwicklung, insbesondere natürlich der Digitalisierung. Es ermöglicht beispielsweise die Fernsteuerung von Kraftwerken, das vielbeschworene Internet of Things (IoT), die Industrialisierung 4.0 und – gerade während Corona-Zeiten – die Aufrechterhaltung der Produktivität durch Homeoffice. Was einst als redundante Technologie gedacht war, die es erlaubte Informationen auf einfache Weise zu teilen und selbst beim Ausfall eines Teilsystems weiter zu funktionieren, wurde zum globalen Rückgrat kritischer Prozesse in allen Bereichen. Diese Erkenntnis kristallisierte sich natürlich nicht erst 2020 heraus, sondern erreichte schon sehr viel früher die internationale, sicherheitspolitische Ebene. Die COVID-19-Krise hat uns aber deutlich daran erinnert, dass aufgrund der starken Vernetzung und Digitalisierung kritische Infrastrukturen wie beispielsweise Spitäler das Ziel von Cyberangriffen sein können.

Die von Russland 1998 eingebrachte UNO-Resolution zu «Developments in the field of information and telecommunications in the context of international security» hob die fortschreitende Vernetzung und Digitalisierung auf die internationale Bühne. Die UNO-Mitgliedsstaaten sollten sich fortan regelmässig dazu austauschen, wie der mögliche Missbrauch und die Ausnutzung von Informations- und Kommunikationstechnologien auf internationaler Ebene unterbunden

werden kann. Als Folge davon setzte die UNO 2004 eine erste so genannte «Group of Government Experts» (GGE) ein, bestehend aus 15 Mitgliedsstaaten. Der Fokus lag bei dieser Gruppe unter anderem auf der Frage, ob mit Blick auf Informations- und Kommunikationstechnologien auch die Inhalte, oder nur die Infrastruktur, die den Austausch von Inhalten ermöglicht, im Fokus stehen soll. Es erstaunt bei dieser kontroversen Ausgangslage nicht, dass die erste GGE mit Abschluss ihres Mandates 2005 keinen Konsensbericht produzierte.

Die Diskussionen, was nun genau in die Definition von Informations- und Kommunikationstechnologien gehört, was eigentlich eine kritische Infrastruktur ist und wie das internationale Recht im Cyberspace anwendbar ist, ziehen sich wie ein roter Faden durch die Diskussionen nachfolgender GGEs. Dabei gelang es der GGE von 2015 in ihrem Bericht unter anderem, allgemein gültige aber nicht rechtlich bindende Normen für die UNO-Mitgliedsstaaten aufzustellen, betreffend «gutem Verhalten» im Umgang mit Informations- und Kommunikationstechnologien. Dies beinhaltete beispielsweise, dass keine Cyberangriffe auf kritische Infrastrukturen ausgeführt werden sollen. Ebenfalls wurde die Anwendbarkeit des internationalen Rechts im Cyberraum bestätigt. Ähnliche Bestrebungen und Diskussionen werden auch auf regionaler Ebene geführt, beispielsweise im Rahmen der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE).

Was einst als rein technisches Projekt begann, um widerstandsfähige und redundante IT-Netze zu errichten, ist heute in seiner globalen Ausprägung zum Spielball nationaler – teils gegensätzlicher – sicherheitspolitischer Interessen geworden. Im momentan verhärteten internationalen Klima sind denn auch diesbezügliche Fortschritte auf internationaler Ebene rar. Nach dem Bericht der GGE von 2015 konnten praktisch keine konkreten Erfolge mehr erzielt werden. Die GGE von 2017 endete ohne Konsens. Eine neue GGE wurde 2019 lanciert. Daneben nahm 2019 auch eine so genannte Open Ended Working Group (OEWG) unter Schweizer Vorsitz Beratungen und Konsultation auf. Trotz der aktuellen Schwierigkeiten ist es wichtig, die verschiedenen Prozesse und Dialoge in Gang zu halten –dieser Einsatz auf diplomatischer Ebene ist im Interesse aller. Die Schweiz hat die Notwendigkeit, das Thema Cyberspace auch im internationalen und sicherheitspolitischen Umfeld anzugehen, bereits vor einiger Zeit erkannt. Als kleine, offene Volkswirtschaft mit einer starken internationalen Vernetzung ist die Schweiz auf Berechenbarkeit und Ordnung im internationalen, sicherheitspolitischen Kontext angewiesen. Darum war die Schweiz auch Mitglied der GGEs von 2017 und 2019, der OEWG und spielt zudem eine aktive Rolle bei der Ausarbeitung von Normen und vertrauensbildenden Massnahmen im Rahmen der OSZE. Dies ist durchaus auch eine Chance, denn die Schweiz ist international sehr gut positioniert, um Debatten zur Digitalisierung, dem Cyberspace und dessen Gouvernanz zu führen, das internationale Genf ist dafür geradezu prädestiniert. Dies beinhaltet ganz konkrete Beiträge, wie beispielsweise der von der Schweiz 2018 lancierte «Geneva Dialogue on Responsible Behavior in Cyberspace», der 2020 mit zahlreichen internationalen Vertretern der Wirtschaft erfolgreich weitergeführt wird. An über zehn virtuellen Treffen konnten gute Praktiken im Bereich Cybersicherheit entwickelt werden, die einen weltweit geteilten Konsens zwischen global tätigen IT-Unternehmen und IT-nahen Branchen widerspiegeln. Damit leistet die Schweiz einen wichtigen Beitrag zur Präzisierung von internationalen Normen und Prinzipien im Cyberraum, beispielsweise der Normen der GGE oder den Prinzipien des «Paris Call for Trust and Security in Cyberspace».[152] Auch wird dadurch Genf als Zentrum der globalen Digital- und Technologiepolitik nochmals unterstrichen.

[152] https://pariscall.international/en/

7 Publizierte MELANI Produkte

7.1 GovCERT Blog (auf Englisch)

7.1.1 Analysis of an Unusual HawkEye Sample

20.02.2020 - Currently, we are observing HawkEye samples being distributed by large mal-spam waves. HawkEye is a keylogger which has been around quite a long time (since 2013) and has evolved since then and gained more functionality. There are several good blog posts about HawkEye in general. Recently we observed an interesting obfuscation method in a Hawk-Eye binary, which we are going to describe in this blog post.

➔ https://www.govcert.admin.ch/blog/analysis-of-an-unusual-hawkeye-sample/

7.1.2 Phishing Attackers Targeting Webmasters

22.04.2020 - Since the beginning of April 2020, we are seeing an increase in phishing attacks against webmasters and domain owners in Switzerland. Unknown threat actors are phishing for credentials for accounts on web admin panels of at least three major hosting providers in Switzerland.

➔ https://www.govcert.admin.ch/blog/phishing-attackers-targeting-webmasters/

7.2 MELANI Newsletter

7.2.1 Vorsicht: Weiterhin erhöhtes Sicherheitsrisiko durch Ransomware gegen KMUs

19.02.2020 - In den vergangenen Wochen hat MELANI / GovCERT mehr als ein Dutzend Ransomware-Fälle bearbeitet, bei welchen unbekannte Täter die Systeme von Schweizer KMUs und Grossbetrieben verschlüsselt und damit unbrauchbar gemacht haben. Die Angreifer stellten Lösegeldforderungen von mehreren zehntausend Franken, vereinzelt auch von Millionenbeträgen.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/sicherheitsrisiko-durch-ransomware.html

7.2.2 Warnung vor gefälschten E-Mails im Namen des BAG

14.03.2020 - Seit Freitagmittag (13. März 2020) versuchen Cyberkriminelle die Verunsicherung der Bevölkerung aufgrund der Situation um das Coronavirus auszunutzen. Anhand von E-Mails mit gefälschtem Absender des BAG versuchen sie, Malware zu verbreiten. Die Melde- und Analysestelle Informationssicherung MELANI warnt die Bevölkerung. Diese E-Mails sind umgehend zu löschen.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/gefaelschte-emails-im-namen-des-bag.html

7.2.3 Kritische Verwundbarkeit in Microsoft Windows Server (SIGRed)

15.07.2020 - Am vergangenen Dienstagabend (14. Juli 2020) hat Microsoft ein Sicherheitsupdate für eine kritische Verwundbarkeit im Windows Domain Namen System (winDNS) veröffentlicht. Microsoft stuft die Verwundbarkeit mit 10.0 Punkte im CVSS (Common Vulnerability Scoring System) ein, was dem Maximum auf der verfügbaren Skala entspricht.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/sigred.html

7.2.4 Trojaner Emotet wieder aktiv

23.07.2020 - Nach mehrmonatigem Unterbruch beobachtetet MELANI erneut verschiedene Malspam-Wellen mit infiziertem Word-Dokumenten im Anhang. Dabei handelt es sich um einen bereits länger bekannten Trojaner namens Emotet (auch bekannt als Heodo). Ursprünglich als E-Banking-Trojaner bekannt, wird Emotet heute vor allem für den Versand von Spam sowie das Nachladen von weiterer Schadsoftware (Malware) verwendet.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/Trojaner-Emotet-greift-Unternehmensnetzwerke-an.html

7.3 Checklisten und Anleitungen

7.3.1 Home-Office: Sicherer Umgang mit Fernzugriffen

24.03.2020 - Aufgrund der momentan sehr hohen Nutzung von Fernzugriffen möchten wir Sie an einige Grundsätze erinnern, um die Risiken im Umgang mit dieser Technologie zu minimieren. Mit der vermehrten Nutzung von Fernzugriffen in Unternehmensnetzwerke dürften diese Risiken stark zunehmen. Die Angreifer könnten die aktuelle Situation dazu nutzen, um mit verschiedenen Vorgehensweisen Zugriff auf Unternehmensnetzwerke zu erhalten

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

7.3.2 Home-Office: Endbenutzer Guideline

02.04.2020 - Als Ergänzung zum Dokument “Home-Office: Sicherer Umgang mit Fernzugriffen” möchten wir eine kurze Information für den Endbenutzer bereitstellen, wie er seine eigene Umgebung besser schützen kann und somit auch das Risiko für den Arbeitgeber zu reduzieren vermag.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/fernzugriff-enduser.html

8 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.
Cryptomining	Nutzung der Rechenleistung eines Computers, um neue Einheiten von Kryptowährungen zu finden und zu validieren, z. B Bitcoin.
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-Code	(kurz: Exploit) Ein Programm, ein Script oder eine Codezeile, mit der sich Schwachstellen in Computersystemen ausnutzen lassen.
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.
Infostealer	Malware, die Tastatureingaben, Screenshots, Netzwerkaktivitäten und andere Informationen sammeln kann.
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

Begriff	Beschreibung
	der Begriff «Industrielle Kontrollsysteme» (engl. Industrial Control Systems, ICS) geläufig.
Malspam	Massenhaft versendete E-Mails, mit welchen Schadsoftware verbreitet wird.
Malware / Schadsoftware	Oberbegriff für Software, die schädliche Funktionen auf einem Rechner ausführt (wie beispielsweise Viren, Würmer, Trojanische Pferde).
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.

Begriff	Beschreibung
Proxy	Ein Proxy ist eine Kommunikationsschnittstelle in einem Netzwerk. Er arbeitet als Vermittler, der auf der einen Seite Anfragen entgegennimmt, um dann über seine eigene Adresse eine Verbindung zur anderen Seite herzustellen.
RaaS Ransomware-as-a-Service	Ransomware als einkaufbare Dienstleistung ermöglicht technisch wenig versierten Kriminellen durch einfach zu bedienende Werkzeuge Angriffe durchzuführen.
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.
Spyware	Spyware soll ohne Wissen des Benutzers Informationen über dessen Surfgewohnheiten oder Systemeinstellungen sammeln und diese an eine vordefinierte Adresse übermitteln.
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

Begriff	Beschreibung
	Ausstecken eines USB-Gerätes nicht heruntergefahren werden. Die neuen Geräte werden meist (allerdings abhängig vom Betriebssystem) automatisch erkannt und konfiguriert.
Watering-Hole-Angriffe	Gezielte Infektion durch Schadsoftware über Websites, welche bevorzugt nur von einer spezifischen Benutzergruppe besucht werden.
Webseiteninfektion	Infektion eines Computers mit Malware allein durch den Besuch einer Web-Seite. Vielfach beinhalten die betroffenen Web-Seiten seriöse Angebote und sind zwecks Verteilung der Malware zuvor kompromittiert worden. Die Infektion erfolgt meistens durch das Ausprobieren von 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.).