11. Mai 2021 | Nationales Zentrum für Cybersicherheit NCSC

Halbjahresbericht 2020/2 (Juli-Dezember)

Informationssicherung

Lage in der Schweiz und International

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Nationales Zentrum für Cybersicherheit NCSC

1 Übersicht / Inhalt

2 Editorial

Das Schweizer Gesundheitswesen hat Beschwerden

Von Kim Rochat – Mitbegründer von Medidee Services und verantwortlich für die Einheit Digital Health

Kim Rochat, Mitbegründer von Medidee Services und verantwortlich für die Einheit Digital Health

Das Gesundheitswesen erlebt dank dem Einsatz von Spitzentechnologien eine rasante Entwicklung. Die Digitalisierung von Anwendungen und Diensten, die stetig perfektionierte Datenverarbeitung, der Einsatz von Mobile Computing, künstlicher Intelligenz und die zunehmende Vernetzung der Systeme ermöglichen bei der Versorgungskapazität und der Personalisierung der Medizin deutliche Fortschritte zum Nutzen der Bevölkerung. Das Gesundheitswesen ist zunehmend vernetzter; das entspricht einerseits einem Bedürfnis und stellt andererseits eine unvermeidliche Entwicklung sowie eine riesige Chance dar.

Das Gesundheitswesen ist für unser Land in zweifacher Hinsicht von strategischer Bedeutung. Zum einen ist die Spitalkapazität eine kritische Ressource, die jederzeit verfügbar sein muss, um die Gesundheitsbedürfnisse der Bevölkerung zu erfüllen. Die Pandemie ruft uns in Erinnerung, wie wichtig unsere Kapazitäten in diesem Bereich sind. Das Gesundheitswesen ist aber auch ein Schlüsselsektor unserer Wirtschaft. Seit langem nimmt die Schweiz mit mehreren hier angesiedelten globalen Marktleadern eine weltweit führende Stellung im Pharmabereich ein. Neu hinzu kommen führende Akteure im Bereich der Medizinalgeräte. Die Medizintechnik-Industrie, die im Umfeld von zwei international renommierten Technischen Hochschulen sowie einem dichten Netz von Fachhochschulen operiert, beschäftigt aktuell fast 60‘000 Menschen und erwirtschaftet einen Umsatz von mehr als 15 Milliarden Schweizer Franken, was 2,3 Prozent unseres BIP entspricht.

Viele Hersteller von Medizinaltechnik tragen darüber hinaus massgeblich zur Cybersicherheit in unserem Gesundheitssystem bei. Auch die EU ist sich als Gesetzgeberin des Problems bewusst: Am 26. Mai dieses Jahres tritt eine neue, 2017 verabschiedete Gesetzgebung in Kraft - die Verordnung (EU) 2017/745 über Medizinprodukte. Sie verpflichtet die Hersteller, dafür zu sorgen, dass ihre Geräte nicht nur für Patienten und Anwender (Safety), sondern auch in Bezug auf den Datenschutz oder die Prävention einer missbräuchlichen Nutzung (Security) sicher sind.

Obwohl sich die Schweiz aufgrund ihrer unentschlossenen Haltung gegenüber dem Rahmenabkommen selbst von der gegenseitigen Anerkennung von Medizinprodukten (MRA-Abkommen) mit der EU ausgeschlossen hat, hat sie sich mit ihrer neuen Medizinprodukteverordnung (MepV) dennoch an das europäische Recht angepasst. Die am 26. Mai 2021 in Kraft tretende Verordnung verweist in ihrem Artikel 6 direkt auf europäisches Recht. Zur Erinnerung: Schweizer Hersteller müssen fortan die Cybersicherheit der von ihnen in Verkehr gebrachten Geräte gewährleisten. Es muss deshalb sichergestellt werden, dass die einheimischen Hersteller in der Lage sind, diese neue Vorschrift umgehend zu erfüllen.

Darüber hinaus war die Schweiz kreativer, indem sie in Artikel 74 ihrer Verordnung (MepV) die Gesundheitseinrichtungen dazu verpflichtete, «alle technischen und organisatorischen Massnahmen zu treffen, die nach dem Stand der Technik notwendig sind, um bei netzwerkfähigen Produkten den Schutz vor elektronischen Angriffen und Zugriffen sicherzustellen». Dieser Artikel bestätigt nicht nur ein weiteres Mal, dass der Gesetzgeber dem technologischen Fortschritt hinterherhinkt; er bereitet unseren Gesundheitseinrichtungen auch Schwierigkeiten, weil er nur einen Aspekt des Grundproblems anspricht. Obwohl es unbestritten ist, dass Gesundheitseinrichtungen ihre IT-Systeme robust und wirksam schützen müssen, sind sie oft nicht in der Lage, sich gegen die Risiken, denen bestimmte medizinische Geräte sie aussetzen, zu schützen. Viele Geräte sind nicht so konzipiert, dass sie eine angemessene Sicherheit bieten, oder die Gesundheitseinrichtungen können es sich nicht leisten, veraltete Geräte zu ersetzen. Bei einem Projekt in einem regionalen Krankenhaus, an dem ich beteiligt war, wusste man, dass mehr als 30 Systeme, u. a. auch Beatmungsgeräte und Infusionspumpen technologisch veraltet waren – ein inakzeptables Risiko für die Patientinnen und Patienten!

Sowohl im Schweizer wie im europäischen Gesundheitssektor besteht bei der Infrastruktur ein dringender Ausbaubedarf. Gleichzeitig bieten die laufenden regulatorischen Änderungen und die sich beschleunigende Digitalisierung des Gesundheitswesens eine enorme Chance für die Branche. Unsere französischen Nachbarn haben sich dieser Herausforderung gestellt. Am 18. Februar verkündete Frankreichs Präsident eine neue Strategie zur Entwicklung des Cybersicherheitssektors. Er stellte auch in Aussicht, dass eine Milliarde Euro im Cyberbereich, insbesondere für die Schaffung eines Cyber Campus, zur Verfügung gestellt würden. 515 Millionen Euro sind im Rahmen dieses Plans für die Entwicklung hoheitlicher Lösungen und 176 Millionen Euro für die Bedürfnisse des öffentlichen Sektors, namentlich der Krankenhäuser und Gemeinden, vorgesehen.

Der Strategieplan NCS 2.0 stellt diesbezüglich in der Schweiz einen grossen Schritt nach vorne dar, weil er in diesem Bereich relevante Ziele setzt. Zugute kommt uns auch die hervorragende Arbeit von Akteuren wie bspw. dem Nationalen Zentrum für Cybersicherheit (NCSC). Zudem gab es erfolgreiche Initiativen wie den Cyber-Defence Campus (CYD). Die digitale Sicherheitsstrategie der Schweiz muss jedoch noch «einen Zacken zulegen» und ehrgeiziger werden. Unser Land muss sich die Mittel geben, die nötig sind, um diese Herausforderungen meistern zu können. Unsere Regierung muss dezidiert die Führung übernehmen und gleichzeitig die verschiedenen Akteure bei der Umsetzung dieser Informationssysteme strukturierter und systematischer einbeziehen, indem sie die Forschung, die Industrie und das Gesundheitswesen bei der Suche nach gemeinsamen Lösungen stärker unterstützt. Die Spitäler, die das Opfer von Ransomware-Angriffen wurden (in Frankreich kam es in letzter Zeit zu mehreren solchen Vorfällen), führen es uns regelmässig vor Augen: Für die Bevölkerung lebensnotwendige Dienste können durch kriminelle Banden ausser Gefecht gesetzt werden. Dieses Risiko ist bekannt und es ist inakzeptabel, dass in einer Demokratie wie der unseren zu wenig getan wird, um es abzuwehren.

Die Herausforderung, der sich unsere Politikerinnen und Politiker unverzüglich stellen müssen, liegt darin, den nächsten einheimischen Cybersecurity-Einhörnern den Weg zu ebnen, indem wir unser akademisches Potenzial und unsere nationalen Infrastrukturen optimal nutzen, um unser Gesundheitssystem dabei zu unterstützen, sich vor den immer grösseren und immer schneller auftauchenden Risiken zu schützen. Eine Politik der kleinen Schritte genügt nicht mehr, um sich dieser Herausforderung zu stellen.

3 Fokus: Digitales Gesundheitswesen

3.1 Einleitung

Die Digitalisierung schreitet auch im Gesundheitswesen mit allen Vor- und Nachteilen unaufhaltsam voran. Globalisierte Lieferketten und computergesteuerte Logistik sind an der Tagesordnung. Patientendossiers werden digital geführt, was neben platzsparender Aufbewahrung und aufwandsarmer Datensicherung die einfache Weitergabe der Krankengeschichten an behandelnde Ärzte ermöglicht. Wie in anderen Bereichen vergrössert sich durch die zunehmende Digitalisierung die potenzielle Angriffsfläche.

3.2 Patientendaten

Daten über die Gesundheit von Personen sind gemäss Datenschutzgesetz «besonders schützenswerte Personendaten» und sollen entsprechend besonders gut vor unbefugter Kenntnisnahme geschützt werden. Sie sind einmalig und lassen sich bei Missbrauch nicht wie Passwörter einfach ändern. Gesundheitsdaten müssen aber auch vor Zerstörung geschützt sein. Ergebnisse früherer Untersuchungen lassen sich nicht nachträglich erheben. Die Digitalisierung kann dieses Risiko entschärfen. Daneben ist auch der Schutz von Patientendaten vor unbefugter Veränderung sicherzustellen. Infusionen mit der falschen Blutgruppe können tragisch enden. Falschinformationen über Medikamentenunverträglichkeiten oder Allergien können verheerende Folgen haben. Ausschliesslich berechtigte Personen sollen auf solche Daten zugreifen können und der Kreis von Personen, die diese Daten ändern können, muss weitestgehend eingeschränkt sein.

3.3 Digitale medizinische Geräte

Medizinische Geräte sind mittlerweile vielfach kleine oder grosse vernetzte Computer. Röntgenbilder werden digital erfasst und Untersuchungsergebnisse werden mehr oder weniger direkt ins Netzwerk der Praxis oder des Spitals eingespiesen oder in eine Cloud hochgeladen. Untersuchungsergebnisse von bildgebenden Verfahren wie Computertomographie-Scans oder Röntgenbilder wurden schon mehrfach auf ungenügend gesicherten Cloud-Servern und auf aus dem Internet erreichbaren Datenträgern festgestellt – inklusive zugehöriger Patientendaten.[1] Je grösser und komplizierter der Analyseapparat, desto eher hat er zudem eine Schnittstelle zu seinem Hersteller, der die Funktion überwacht und das Gerät bei Bedarf auch aus der Ferne warten kann.

Den risikoadäquaten Umgang mit der totalen Vernetzung und dem Fernzugriff auf digitale Daten sowie eine angemessene sektorspezifische Kultur muss der Gesundheitssektor weiter etablieren. Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) schreibt in seinem Abschlussbericht[2] zum Projekt «ManiMed» (Manipulation von Medizinprodukten), dass in jedem Produkt Schwachstellen gefunden wurden. In fast allen Fällen sei die IT-Sicherheit und nicht unmittelbar die Patientensicherheit betroffen gewesen.

---

1 Siehe Kap. 4.6.3 unten sowie MELANI Halbjahresbericht 2019/2, Kap. 4.5.1.

2 ManiMed Abschlussbericht (bsi.bund.de)

3.4 Datenspuren von Medizinprodukten

Neben medizinischen Geräten gibt es eine grosse Fülle weiterer Medizinprodukte.[3] Darunter fallen auch verschiedenste Verbrauchsmaterialien für Untersuchungen und Operationen. Beispielsweise werden verschiedene invasiv genutzte Einwegprodukte aus Qualitätssicherungsgründen nachverfolgt. Bei nicht unbeschränkt haltbaren und teuren Produkten wird jede Verwendung auch deshalb erfasst, weil keine grossen Vorräte gehalten werden und zeitnah Ersatz nachbestellt werden muss. Medizinische Implantate wie Hüft- und Knieprothesen werden im schweizerischen Implantat-Register (SIRIS)[4] eingetragen. Auch dies dient der Qualitätssicherung. Das Register soll eine Beurteilung der langfristigen Implantat- respektive Behandlungsqualität ermöglichen. Zudem dient es als Frühwarnsystem bei Produkte- und Prozessfehlern.

Die Nachvollziehbarkeit von für Untersuchungen und Behandlungen verwendeten Produkten erhöht zweifellos die Sicherheit der Gesundheit von Patientinnen und Patienten. Gleichzeitig ist jedoch auch auf die Vertraulichkeit und Integrität der gespeicherten Daten zu achten und Zugriffe auf, wie auch die Bearbeitung der Daten müssen nachvollziehbar sein.

3.5 Cyberbedrohungen

Spitäler und andere Gesundheitsdienstleister sind den gleichen Cyberbedrohungen ausgesetzt wie alle Unternehmen, die einen Internetanschluss haben und mit Computern arbeiten. Deshalb sind auch im Gesundheitswesen, Zugänge zu Daten und Systemen möglichst mit Mehrfaktorauthentisierung abzusichern, Infektionen mit Schadsoftware zu verhindern oder zumindest zeitnah zu erkennen und zu beheben. Eine wichtige Schutzmassnahme ist zudem, die Mitarbeitenden im sicheren Umgang mit Informatikmitteln zu sensibilisieren und die Cyberbedrohungen wie etwa Social Engineering aufzuzeigen.

Während die Bedrohungen in den meisten Sektoren sehr ähnlich oder sogar gleich sind, weisen die Konsequenzen von erfolgreichen Angriffen im Gesundheitswesen durchaus Eigenheiten auf. So sind zum einen bei einem Datenabfluss meistens unabänderliche, besonders schützenswerte Personendaten betroffen und zum anderen können Funktionsausfälle von IT-Systemen oder eine auch nur temporäre Nichtverfügbarkeit von Daten die Gesundheit oder sogar das Leben von Menschen gefährden.

3.6 Beispiel: Erpressung mit Patientendaten

Schon seit einigen Jahren grassieren Verschlüsselungstrojaner (Ransomware) als erfolgreiches kriminelles Geschäftsmodell, das auch gegen Spitäler eingesetzt wird. Mittlerweile greifen die Täter vor der Verschlüsselung möglichst viele Daten ab, um ein zusätzliches Erpressungsmittel zu haben. Bei einem Psychotherapie-Unternehmens in Finnland versuchten Er-

---

3 Medizinprodukteverordnung (MepV, SR 812.213), Art. 1.

4 Schweizer Implantat-Register SIRIS (siris-implant.ch)

presser erfolglos, vom Unternehmen Geld zu erhalten, um die Veröffentlichung von Patientendaten und Inhalten von Therapiegesprächen zu verhindern. In der Folge versuchten die Kriminellen die betroffenen Patientinnen und Patienten direkt zu erpressen.[5]

3.7 In Zeiten der Pandemie

Während einer Pandemie[6] können Krankheitsfälle in kurzer Zeit erheblich zunehmen und das Gesundheitswesen an seine Kapazitätsgrenzen führen. Wenn sich dann noch Cybervorfälle ereignen, die zu Funktionseinschränkungen bei Gesundheitsdienstleistern führen, hat dies unter Umständen lebensbedrohliche Konsequenzen. Weltweit für Aufsehen sorgte der Fall der Universitätsklinik Düsseldorf, welche im September 2020 von Ransomware betroffen war.[7]

Bereits im Sommer 2020 wurde die Hirslanden-Gruppe Opfer von Ransomware. Die verschlüsselten Daten konnten dort jedoch mithilfe von Backups wiederhergestellt werden und die Patientenversorgung soll zu keiner Zeit gefährdet gewesen sein.[8] Bei zwei weiteren Spitälern in der Schweiz konnten Infektionen mit dem Trojaner «Emotet[9]» frühzeitig erkannt und behoben werden.

Das Personal im Gesundheitswesen ist während einer Pandemie aussergewöhnlich gefordert und nicht selten überarbeitet. Auf Social Engineering-Methoden fallen Personen eher herein, wenn sie bereits aufgrund von äusseren Umständen unter Druck stehen. Social Engineering zeichnet sich unter anderem durch das Vorspiegeln von Dringlichkeit aus. Durch die Kumulation von echtem und künstlich erzeugtem Druck steigen die Erfolgschancen solcher Angriffe. Das Risiko, dass in der Eile auf einen bösartigen Link in einem E-Mail geklickt oder ein schädliches Attachment geöffnet wird, nimmt zu. Neben der Implementierung technischer Massnahmen sollten alle Mitarbeitenden auf die Gefahren von Social Engineering sensibilisiert werden. Es sind administrative Prozesse zu etablieren, mit denen Betrugsversuche und andere Social Engineering-Angriffe erkannt werden können.

Empfehlung / Schlussfolgerung:

Im Zuge der Digitalisierung neu einzuführende unterstützende technische Lösungen müssen zum einen möglichst sicher designt werden und zum anderen müssen die Personen, die damit arbeiten sollen, im korrekten und sicheren Umgang damit geschult werden. Digitale Hilfsmittel sind aus dem Gesundheitswesen wie aus dem alltäglichen Leben kaum mehr wegzudenken und werden weiter an Bedeutung gewinnen.

---

5 Vastaamo fires CEO for hiding another data breach in March 2019 (foreigner.fi); Cyber-Erpresser in Finnland: Willkommen in der Dystopie (sueddeutsche.de)

6 Siehe hierzu auch das Schwerpunktthema in Kap. 3 des MELANI Halbjahresbericht 2020/1.

7 Uniklinik Düsseldorf: Ransomware "DoppelPaymer" soll hinter dem Angriff stecken (heise.de)

8 Hirslanden von Cyberangriff getroffen: Bedrohung bleibt hoch (nzz.ch)

9 Vgl. Kap. 4.3.2.

4 Lage

4.1 Überblick Meldungen an das NCSC

Im zweiten Halbjahr 2020 sind bei der Anlaufstelle des NCSC insgesamt 5’542 Meldungen von Privatpersonen und Unternehmen eingegangen.[10]

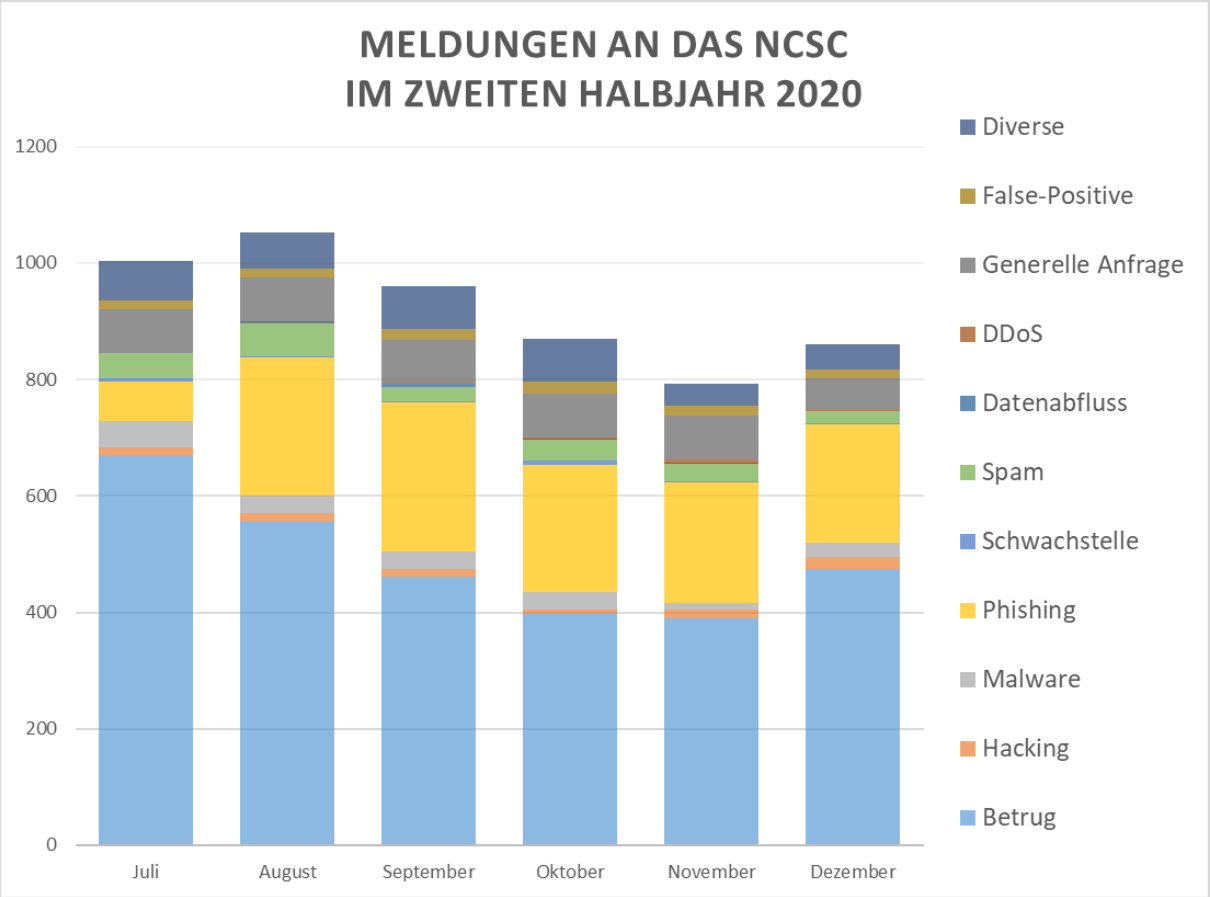


Abb. 1: Meldungen an das NCSC im zweiten Halbjahr 2020.

Betrugsmeldungen machen mit 2’917 Meldungen weiterhin den grössten Anteil aus. Internetbetrug hat unter anderem folgende Ausprägungen:

Vorschussbetrug:

Der am häufigsten gemeldete Betrugstyp mit 1’120 Meldungen bleibt der Vorschussbetrug.[11] Entsprechende E-Mails werden immer noch in grosser Zahl versendet. Allerdings dürfte der Erfolg dieser Schreiben gering sein. Nur in einem gemeldeten Fall wurde der Empfänger tatsächlich getäuscht und es ist ein finanzieller Schaden entstanden.

[10] Statistiken finden Sie auf unserer Website: Aktuelle Zahlen (ncsc.admin.ch).

[11] Informationen auf unserer Website zu Vorschussbetrug (ncsc.admin.ch)

Fake-Sextortion:

Mit 353 Meldungen stechen zudem Meldungen zu Fake-Sextortion-E-Mails[12] heraus. In einem E-Mail wird dabei behauptet, dass Foto- oder Videomaterial erstellt wurde, welches den Empfänger während eines angeblichen Besuchs auf pornografischen Websites zeigen soll. Die Erpresser versuchen mit verschiedensten Methoden die Opfer zu überzeugen, dass diese Behauptungen stimmen sollen. In einer Variante wird als Absender die Adresse des Empfängers benutzt. Dies suggeriert, dass das E-Mail-Konto unter der Kontrolle des Angreifers ist. Der Absender ist aber lediglich gefälscht. In einer anderen Variante wird als «Beweis» ein Passwort aufgeführt, welches dem Opfer gehört. Dabei handelt es sich allerdings um Passwörter aus alten Datenabflüssen.[13]

Gebührenfallen:

210 Meldungen sind im Zusammenhang mit vermeintlichen Gebühren eingegangen. Dabei handelt es sich meist um E-Mails, die eine Paketzustellung ankündigen. Den grössten Teil mit 180 Meldungen machen dabei E-Mails aus, die vorgeben von der Eidgenössischen Zollverwaltung (EZV) zu stammen und Zollgebühren meist in der Höhe von CHF 75.- fordern. Man solle «Paysafe»-Karten kaufen und die Karten-Nummer per E-Mail versenden. In die gleiche Kategorie fallen die zahlreichen E-Mails vermeintlich von Paketdienstleistern wie der Post, DHL oder DPD, welche vorgeben, dass bei einem Paketversand noch zusätzliche Gebühren per Kreditkarte bezahlt werden sollen.[14]

Kleinanzeigen, Fake-Support, CEO-Betrug:

Neben 145 Meldungen zu Kleinanzeigenbetrug[15] und 130 zu Fake-Support Anrufen[16] sticht mit 111 Meldungen der sogenannte CEO-Betrug[17] heraus. Die Angreifer beschaffen sich in diesen Fällen Informationen über eine Firma oder einen Verein aus unterschiedlichen öffentlichen Quellen und versuchen dann, die per E-Mail mit gefälschtem Absender angeschriebene Person dazu zu bewegen, eine angeblich dringende Zahlungen auszulösen.

4.2 Neues Meldeformular

Am 21. Dezember 2020 wurde das neue Meldeformular des NCSC in Betrieb genommen. Durch die Beantwortung von maximal vier Fragen werden den Meldenden eine erste automatisierte Einschätzung und hilfreiche Informationen angezeigt. Diese Nutzerführung erlaubt eine schnelle und unkomplizierte Meldung und gleichzeitig eine Einordnung des Vorfalls. Die abschliessende freiwillige Angabe von weiteren Informationen ermöglicht es dem NCSC, den Meldenden bei Bedarf noch bessere Unterstützung zu bieten. Meldungen aus der Bevölkerung leisten einen wichtigen Beitrag, damit das NCSC Trends rasch erkennen, geeignete Gegenmassnahmen ergreifen sowie ein vollständiges Cyberlagebild erstellen kann.

---

12 Informationen auf unserer Website zu Fake Sextortion (ncsc.admin.ch)

13 Vgl. Have I Been Pwned: Check if your email has been compromised in a data breach (havibeenpwned.com)

14 Siehe hierzu Kap. 4.8.2.

15 Informationen auf unserer Website zu Kleinanzeigenbetrug (ncsc.admin.ch)

16 Informationen auf unserer Website zu Fake-Support (ncsc.admin.ch)

17 Informationen auf unserer Website zu CEO-Betrug (admin.ch)

4.3 Schadsoftware/Malware

4.3.1 Ransomware

Zu den Vorfällen mit dem grössten Schadenspotential zählen Verschlüsselungstrojaner (Ransomware). In der zweiten Jahreshälfte 2020 sind beim NCSC 34 Meldungen dazu aus verschiedenen Wirtschaftssektoren in der Schweiz eingegangen. Rund 80 Prozent der Meldungen betrafen kleine und mittlere Unternehmen (KMU).

Wie bereits in früheren Halbjahresberichten thematisiert, werden mittels Ransomware die Daten eines Opfers verschlüsselt und unbrauchbar gemacht. Um die Daten zu entschlüsseln, werden die Opfer aufgefordert ein Lösegeld an die Erpresser zu bezahlen. Da oft Backups von den Daten vorhanden sind und Betroffene der Bezahlung nicht nachkommen, haben die Kriminellen begonnen sich mit einer doppelten Erpressungstaktik abzusichern. Vor der Verschlüsselungsattacke werden die Daten des Opfers abgezogen. Falls die Erpressung mit der Verschlüsslung nicht zum gewünschten Erfolg führt, wird gedroht diese zu publizieren oder im Untergrundmarkt zu verkaufen.

Vorfälle mit Ransomware können die Betriebsprozesse in Unternehmen erheblich stören. Die Bedrohung ist besonders existentiell, wenn ebenfalls die Backup verschlüsselt wurden. Die Kosten für Ausfallzeiten des Systems und die Nichtverfügbarkeit von Informationen sowie für die Vorfallsbewältigung sind immens. Bei solchen Vorfällen ist die Kommunikation auf Seite der Opfer gegenüber Kunden und Geschäftspartnern in der Praxis unterschiedlich. Die Palette reicht von Stillschweigen bis hin zur transparenten Offenlegung.

Empfehlungen:

Ransomware kann erheblichen Schaden verursachen, insbesondere dann, wenn auch Datensicherungen (Backups) davon betroffen sind. Bleiben Sie bei einem solchen Vorfall ruhig und handeln Sie überlegt. Wichtige Aspekte der Vorfallsbewältigung sind das Auffinden des Infektionsweges sowie die Verhinderung einer neuen Infektion. Setzen Sie die betroffenen Systeme neu auf und stellen Sie Daten mit vorhandenen Backups wieder her.

Falls in Ihrem Unternehmen die notwendigen Fachkenntnisse nicht vorhanden sind, holen Sie sich Unterstützung bei einem spezialisierten Unternehmen.

Weitere Informationen auf der NCSC-Website: Ransomware (ncsc.admin.ch).

Vorfälle in der Schweiz und International

In der Schweiz sind in der zweiten Jahreshälfte Ransomware-Vorfälle beim Uhrenhersteller Swatch Group,[18] beim Helikopterhersteller Kopter,[19] beim Elektrounternehmen Huber + Suhner[20] und auch bei der Hirslanden-Gruppe[21] öffentlich bekannt geworden.

[18] Swiss watchmaker Swatch shuts down IT systems to stop cyberattack (bleepingcomputer.com)
[19] Ransomware hits helicopter maker Kopter (zdnet.com)
[20] Huber + Suhner von Cyberattacke lahmgelegt (inside-it.ch)
[21] Hirslanden von Cyberangriff getroffen: Bedrohung bleibt hoch (nzz.ch)

International war beispielsweise der IT-Dienstleister Sopra Steria[22] betroffen, welcher nach dem Ausfall seiner IT den Schaden auf bis zu 50 Millionen Euro bezifferte. Ein bemerkenswerter Fall ereignete sich im Gesundheitssektor in Deutschland: Die Daten der Universitätsklinik Düsseldorf[23] wurden verschlüsselt. Das Erpresserschreiben ging aber an die Universität, welche die Cyberkriminellen eigentlich angreifen wollten. In den USA waren verschiedentlich auch Bildungseinrichtungen betroffen. Die Ransomware-Akteure haben in diesem Rahmen auch vertrauliche Schülerdaten gestohlen und damit gedroht, diese zu veröffentlichen, falls die Institutionen kein Lösegeld bezahlen.[24]

Eine weitere Eskalation in der Erpressungstaktik von Ransomware

Um Druck auf die Opfer auszuüben, greifen einige Ransomware-Akteure mittlerweile auch zum Telefon und rufen betroffene Unternehmen an. Dabei wird beispielsweise damit gedroht, Journalisten über eine Sicherheitslücke im Unternehmen des Opfers zu informieren oder sensible Dokumente auf so genannten Data Leak-Sites (DLS) zu veröffentlichen.

Ransomware-Betreiber verbessern die Widerstandsfähigkeit

Viele Ransomware-Betreiber verwenden bereits die doppelte Erpressungstaktik von Verschlüsselung und Datenabfluss. In dieser Taktik ist der Schutz von Data Leak-Sites (DLS) gegen initiierte Abschaltung (sog. «Takedowns») durch Strafverfolgungsbehörden wesentlich. Das Betreiben von DLS-Infrastrukturen in Ländern, in denen die Beziehungen der Strafverfolgungsbehörden zu anderen Ländern möglicherweise nicht kohärent sind, kann den Prozess von Takedowns deutlich erschweren. Zudem werden die gestohlenen Daten vielfach auf mehrere Server repliziert. Ein Eingriff bei einem einzelnen Server kann die Daten somit nicht aus dem Netz entfernen.

Neue Ransomware Gruppe «Egregor» tritt in die Fussstapfen von «Maze»

Die Gruppe scheint seit September 2020 aktiv zu sein. Im Oktober 2020 hat sie vor allem in den USA einzelne Ziele angegriffen, u. a. den amerikanischen Buchhändler «Barnes & Noble»[25] sowie die Videospielentwickler Ubisoft und Crytek.[26] Danach folgte ein massiver Anstieg der Angriffe, welcher beispielsweise auch den Betrieb der Metro von Vancouver störte.[27] «Egregor» scheint die Lücke zu füllen, welche durch das offensichtliche Einstellen der Tätigkeiten der «Maze»-Ransomware-Gang im Oktober 2020 entstanden ist. In der Schweiz wurde bis Ende 2020 kein Vorfall mit «Egregor» gemeldet.

Ransomware-Bande hackt Facebook-Konto, um Erpressungsanzeigen zu schalten

Die italienische Spirituosenfirma Campari Group wurde Opfer eines Ransomware-Angriffs. Über ein gehacktes Facebook-Konto veröffentlichten die Täter dann Anzeigen, in denen Campari gewarnt wurde, dass ihre Daten veröffentlicht würden, wenn sie das Lösegeld nicht zahlen. Die Facebook-Werbung trug den Titel «Sicherheitsverletzung des Netzwerks der Campari-

---

22 Cyber-Attacke kostet Sopra Steria bis zu 50 Millionen Euro (inside-it.ch)

23 Uniklinik Düsseldorf: Ransomware "DoppelPaymer" soll hinter dem Angriff stecken (heise.de)

24 K12 education giant paid the ransom to the Ryuk gang (securityaffairs.co)

25 Cyber-Attack on Major US Bookseller (infosecurity-magazine.com)

26 Ubisoft, Crytek data posted on ransomware gang's site (zdnet.com)

27 Vancouver Metro Disrupted by Egregor Ransomware (threatpost.com)

Gruppe durch das Ragnar-Locker-Team» und warnte davor, dass weitere sensible Daten veröffentlicht werden würden.

Diese neue Taktik, Angriffe über Facebook zu bewerben, illustriert die kontinuierliche Weiterentwicklung der Ransomware-Erpressung.[28]

4.3.2 «Emotet»

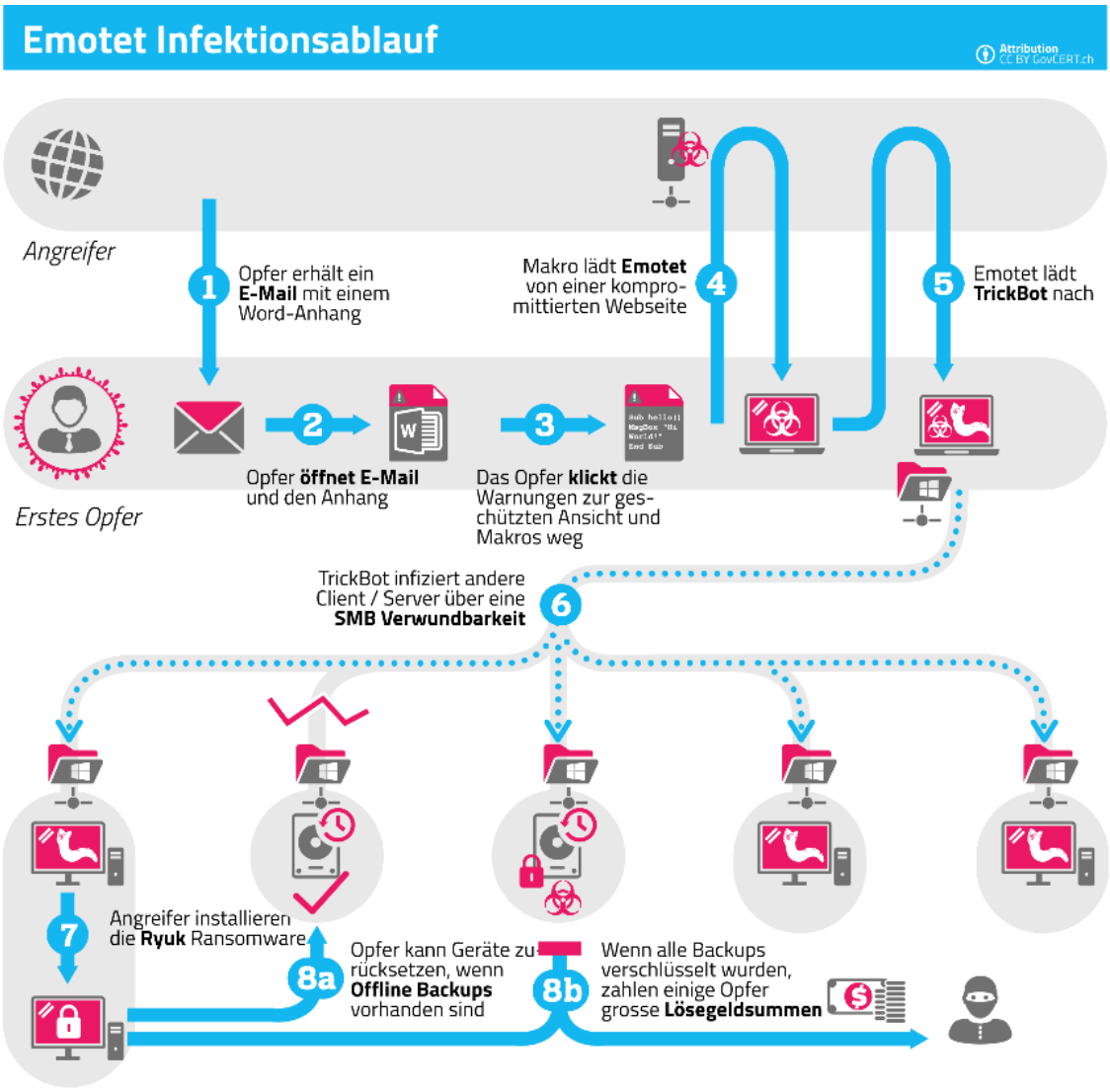


Abb. 2: Emotet Infektionsablauf

Nach mehrmonatigem Unterbruch beobachtete das NCSC seit Juli 2020 erneut verschiedene Spam-Wellen der «Emotet»-Schadsoftware. Obwohl «Emotet» in der zweiten Jahreshälfte 2020 insgesamt weniger stark aktiv war als in der ersten, zählte «Emotet» bei Jahresende erneut zur meistverbreiteten Schadsoftware in der Schweiz und international.[29] Ursprünglich als E-Banking-Trojaner bekannt, wurde «Emotet» zuletzt vor allem für den Versand von Spam sowie das Nachladen von weiterer Schadsoftware verwendet.

---

28 Ransomware Group Turns to Facebook Ads (krebsonsecurity.com)

29 Vgl. URLhaus Statistics (abuse.ch)

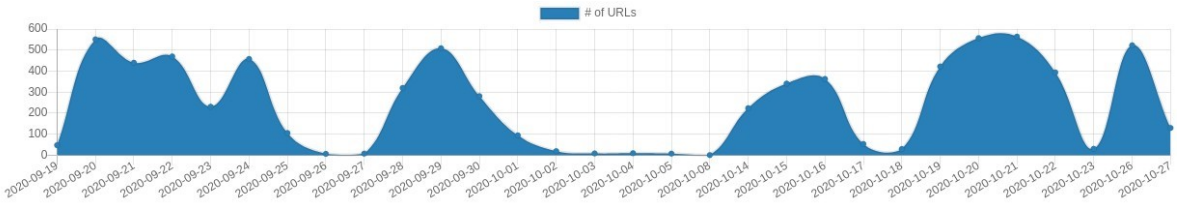


Abb. 3: Anzahl von URLs, die in Verbindung mit Emotet beobachtet wurden; wellenförmiger Verlauf der Emotet-Aktivitäten

Das NCSC warnte[30] im November 2020 insbesondere vor zunehmender «Emotet»-Aktivität, da diese Schadsoftware gezielt dazu verwendet wird, Computer und Server in Netzwerken mit einer Ransomware wie Beispielsweise «Ryuk» zu infizieren. Betroffen sind ausschliesslich Windows-Computer und -Server.

Am 27. Januar 2021 wurde die internationale Strafverfolgungsoperation «LADYBIRD» bekannt, in deren Rahmen die «Emotet»-Infrastruktur erfolgreich beschlagnahmt wurde. An der Operation beteiligten sich die Niederlande, Deutschland, Frankreich, Litauen, Kanada, USA, Grossbritannien und die Ukraine.[31] Die Operation «LADYBIRD» scheint bisher erfolgreich und die Operabilität des Botnetzes nachhaltig zerschlagen. «Emotet» ist allerdings bekannt für dynamische Weiterentwicklungen nach längeren Aktivitätspausen. Es ist möglich, dass es den Akteuren hinter «Emotet» gelingen wird, neue Infrastrukturen aufzubauen und ihre kriminellen Aktivitäten wieder aufzunehmen.

Empfehlungen:

- Das Ausführen von unsignierten Office-Makros sollte technisch unterbunden werden. Office Dokumente mit Makros sollten bereits auf dem E-Mail-Gateway bzw. Spam-Filter erkannt und gar nicht an die Empfänger ausgeliefert werden. Passwort geschützte ZIP-Dateien sollten ebenfalls auf dem E-Mail-Gateway erkannt und erst nach einer Kontrolle zugestellt werden.
- Websites, die aktiv für die Verbreitung von «Emotet» verwendet werden, sind am Netzwerkperimeter zu sperren. Eine Liste dieser Websites wird beispielsweise von URLhaus (abuse.ch) kostenlos zur Verfügung gestellt.
- Server, welche für die Steuerung von mit «Emotet» infizierten Geräten verwendet werden, sind zu blockieren. Eine Liste von IP-Adressen, welche «Emotet» zugeordnet werden können, werden unter anderem im Feodo Tracker (abuse.ch) publiziert.

Weitere Massnahmen und detaillierte Informationen finden Sie auf unserer Website:

Schützen Sie Ihr KMU (ncsc.admin.ch)

Update Verschlüsselungs-Trojaner: Neue Vorgehensweise (ncsc.admin.ch)

30 Trojaner Emotet wieder aktiv (ncsc.admin.ch)

31 World's most dangerous malware EMOTET disrupted through global action (europol.europa.eu)

4.3.3 «Trickbot»

Auch im zweiten Halbjahr 2020 blieb «Trickbot» für Unternehmen und Organisationen eine grosse Bedrohung. Seit ihrem Auftauchen 2016 hat sich diese Malware als Verbreitungsvektor für diverse Arten von Angriffen, vor allem aber auf Ransomware-Attacken spezialisiert.[32] Mitte Oktober versuchten mehrere Sicherheitsakteure, das «Trickbot»-Kontrollnetzwerk zu zerschlagen.[33] Die Operationen hatten aber nur eine begrenzte Wirkung und konnten «Trickbot» nicht nachhaltig lahmlegen.

4.4 Angriffe auf Websites und -dienste

4.4.1 DDoS-Angriffe

Eine häufige Vorgehensweise von Kriminellen besteht darin, zuerst einen tendenziell kurzen Demonstrations-DDoS-Angriff auf ein Ziel durchzuführen, um ihre grundsätzlichen Fähigkeiten unter Beweis zu stellen. In einem Erpressungs-E-Mail fordern die Täter dann eine Zahlung in einer Kryptowährung (z.B. Bitcoin). Die Erpresser behaupten, dass sie über eine bedeutend stärkere Angriffskapazität verfügen als sie für den Demonstrations-Angriff verwendet haben und drohen mit Folgeangriffen. Diese bleiben jedoch meistens aus. In Ausnahmefällen – insbesondere wenn bereits die Demonstrations-Angriffe zu nennenswerten Einschränkungen geführt haben – werden die Folgeangriffe tatsächlich durchgeführt. Diese erreichen jedoch nie die angedrohte Kapazität. Wie bereits in der ersten Jahreshälfte 2020,[34] haben solche Angriffe in der zweiten Jahreshälfte international weiter zugenommen. Die Analysten von Nexusguard[35] berichteten von einem Anstieg der gesamten DDoS-Angriffe um 287 Prozent im dritten Quartal im Vergleich zum Vorjahreszeitraum.

Seit August wurde eine globale Kampagne von DDoS-Erpressungsangriffen in verschiedenen Wirtschaftssektoren festgestellt. Das FBI warnte sogar US-Firmen, dass Tausende von Organisationen auf der ganzen Welt aus verschiedensten Branchen mit DDoS-Attacken innerhalb von sechs Tagen bedroht wurden.

Das NCSC hat in der Schweiz in der ersten Jahreshälfte keine signifikante Zunahme von DDoS-Attacken festgestellt. Dies änderte sich jedoch in der zweiten Jahreshälfte. Die Schweiz wurde von der erwähnten globalen DDoS-Welle nicht verschont. Auch hierzulande waren im August diverse Wirtschaftssektoren, vor allem der Finanz- und Energiesektor, von DDoS-Attacken und entsprechenden Erpressungsforderungen betroffen. Im Berichtszeitraum wurden dem NCSC 19 DDoS-Attacken gemeldet. Die maximalen Traffic Volumina lagen zwischen 150Gbit/s und 200Gbit/s. Die Angreifer haben sich in den Erpresserschreiben oftmals mit Namen berühmt-berüchtigter staatlicher Gruppierungen wie «Lazarus» oder «FancyBear» geschmückt, um den Opfern Angst zu machen und sie zur Zahlung zu bewegen. Im November

---

32 Siehe MELANI Halbjahresberichte 2018/2, Kap. 4.5.4; 2019/1, Kap. 3.4.1 und 4.6; 2019/2, Kap. 4.6.1 sowie Blogpost Trickbot - An analysis of data collected from the botnet (govcert.admin.ch)

33 Attacks Aimed at Disrupting the Trickbot Botnet (krebsonsecurity.com);
Cyber Command, Microsoft take action against Trickbot botnet before Election Day (cyberscoop.com);
Microsoft and others orchestrate takedown of TrickBot botnet (zdnet.com)

34 Siehe MELANI Halbjahresbericht 2020/1, Kap. 4.2.2.

35 DDoS Threat Report 2020 Q3 (nexusguard.com)

kehrten die Angreifer zurück und versuchten teilweise die gleichen Unternehmen erneut (und wiederum erfolglos) zu erpressen.

Schlussfolgerung / Empfehlungen:

DDoS-Erpressung ist ein Massengeschäft. Die Angreifer versuchen relativ undifferenziert bei möglichst vielen Unternehmen ihr Glück. Funktioniert die Abwehr, ziehen sie typischerweise weiter auf der Suche nach erfolgversprechenderen Zielen. Wenn sie jedoch mit einem (Demonstrations-) DDoS-Angriff erfolgreich die Systeme eines Unternehmens stören können, gerät dieses als potenzielles Opfer in den Fokus und die Angreifer verstärken ihre Bemühungen in der Hoffnung, dass ein Lösegeld bezahlt wird. Entsprechend ist es von Vorteil, auf allfällige DDoS-Angriffe angemessen vorbereitet zu sein.

Für geschäftskritische Systeme empfiehlt das NCSC, einen kommerziellen DDoS-Schutz (DDoS Mitigation Service) zu abonnieren. Viele Internet Service Provider (ISPs) bieten eine solche Dienstleistung für einen entsprechenden Aufpreis an.

Verschiedene präventive und reaktive Massnahmen, um mit DDoS-Angriffen umzugehen, finden Sie auch auf unserer Website: Angriff auf die Verfügbarkeit (DDoS) (ncsc.admin.ch)

4.4.2 Kompromittierte Websites

Angreifer können mit gestohlenen Zugangsdaten oder via nicht-gepatchte Sicherheitslücken auf die Website-Administration zugreifen und dort beliebigen Code platzieren.

Die Auswirkungen von kompromittierten Websites sind vielfältig. Wesentlich ist, dass infolge Kompromittierung die Vertraulichkeit und Integrität der eingegebenen und der gespeicherten Daten nicht mehr gewährleistet werden kann.

Da der Untergrundmarkt arbeitsteilig organisiert ist, beobachtet man als regelmässiges Phänomen auch die Nutzung der kompromittierten Websites durch verschiedene Akteure: Zugänge zu einer Website-Administration können mehrfach verkauft und weitergegeben werden. Wenn der Angriffsvektor eine Sicherheitslücke ist, können auch verschiedene Akteure unabhängig voneinander die Website kompromittieren. Dies stellt hohe Anforderungen an die Website-Administratoren, bei der Bereinigung wirklich sämtlichen bösartigen Code zu entfernen.

Empfehlungen:

Wurde die Website gehackt ist eine systematische Bereinigung durch Lokalisierung und Entfernung des Schadcodes auf der Website erforderlich. Weiter ist die aktuellste Version des Content Management Systems (CMS) und der Plug-Ins einzuspielen. Sämtliche Computer, welche für die Website-Administration genutzt werden müssen auf Schadsoftware durchsucht und gegebenenfalls bereinigt werden. Schliesslich sind alle Zugangspasswörter zu ändern. Weitere Informationen finden Sie auf unserer Website:

Webseite gehackt - Was nun? (ncsc.admin.ch)

Nach der Bereinigung der Website empfehlen sich zusätzliche Massnahmen, um den Cyberkriminellen in Zukunft einen erneuten Zugang zu verwehren. Auf unserer Website finden Sie

Massnahmen zum Schutz von CMS (ncsc.admin.ch)

4.4.3 Crypto-Scams

Der Hype um Kryptowährungen treibt verschiedenste Blüten – auch viele betrügerische. Unter den Begriff «Crypto-Scams» fallen verschiedenste Phänomene: Betrügerische Investitionsangebote, gefälschte Handelsplattformen (inklusive zugehöriger App) und sogar frei erfundene Kryptowährungen. Ein Betrug kann auch mit einem kompromittierten Social-Network-Konto beginnen. So geschehen im Juli 2020: In einem spektakulären Angriff wurden 130 Twitterkonten von prominenten Personen oder Firmen gehackt.[36] Über die Konten von Barack Obama, Joe Biden, Elon Musk, Mike Bloomberg oder Bill Gates wurden Tweets veröffentlicht, die Belohnungen für Geldüberweisungen an eine bestimmte Bitcoin-Adresse versprachen:

Abb. 4: Beispiel einer Nachricht auf einem gehackten Account

Der Angriff dauerte nur wenigen Minuten, in denen rund USD 180'000 auf Bitcoin-Konten der Hacker überwiesen wurden.

4.5 Industrielle Kontrollsysteme (ICS)

Die digitale Steuerung physischer Prozesse trägt einen grossen Anteil zum Lebensstandard bei, an den sich die Gesellschaft speziell in den Industrienationen gewöhnt hat. Der reibungslose Betrieb solcher Systeme stellt daher ein lohnendes Ziel für Angreifer dar. Die Steigerung des Automatisierungs- und Vernetzungsgrades dieser Systeme stellt parallel eine immer grössere Herausforderung für die Betreiber dar, den Anforderungen an deren Absicherung gerecht zu werden.

4.5.1 Bedrohungen gegen ICS werden vielfältiger

In vielen bisherigen Halbjahresberichten wurden Bedrohungen erwähnt, die auch auf industrielle Kontrollsysteme (ICS) abzielen. Zu einigen der verantwortlichen Akteure gab es in den letzten Monaten neue Erkenntnisgewinne, gleichzeitig traten aber neue Bedrohungsformen und -Akteure in Erscheinung.

---

[36] 2020 Twitter bitcoin scam (en.wikipedia.org)

Das US-Justizministerium erhob im Oktober 2020 Anklage gegen sechs Mitglieder einer Einheit des russischen Militärnachrichtendienstes GRU.[37] Die Gruppe, die von privaten Sicherheitsdienstleistern «Sandworm» getauft wurde, wird unter anderem für die Stromausfälle in der Ukraine Ende 2015 und 2016, sowie die destruktive Schadsoftware «NotPetya» verantwortlich gemacht. Das US-Finanzministerium sanktionierte einige Tage später ein russisches Forschungsinstitut, welches an den Angriffen mit der Malware Triton/Trisis beteiligt gewesen sei.[38] Bei diesen Angriffen wurde versucht, die industriellen Prozesssicherungssysteme (Safety Instrumented System, SIS) auszuhebeln, welche garantieren sollen, dass weder Menschen noch Maschinen bei Störungen einer Anlage zu Schaden kommen. In einer gemeinsamen Warnmeldung[39] informierten das amerikanische FBI und die Cybersicherheitsbehörde CISA über Vorfälle, die mit der Gruppierung «Berserk Bear» in Verbindung gebracht werden. Die US-Behörden beobachteten zwar keine Sabotageversuche der Eindringlinge, vermuten aber anhand der Vorgehensweise, dass solche zumindest vorbereitet werden könnten.

Mehrere Angriffe auf Wasserversorgungssysteme in Israel werden iranischen Akteuren zugeschrieben.[40]

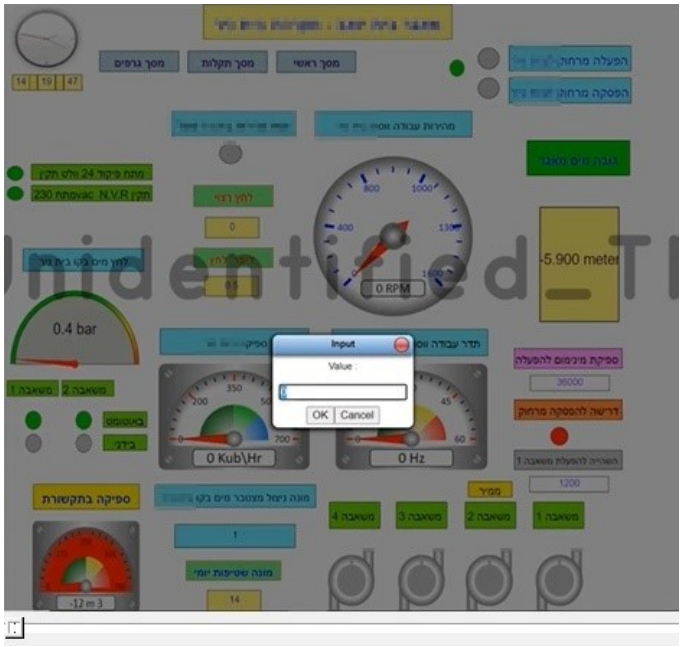


Abb. 5: Ausschnitt aus dem Demonstrationsvideo der offenen Wasserversorgungssteuerung

Neben der Wasser- bleibt auch die Stromversorgung von Cybervorfällen gefährdet. Indische Behörden vermuten hinter einem Stromausfall in Mumbai vom 13. Oktober 2020 einen Cybersabotageversuch.[41]

---

37 Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace (justice.gov);
US Indicts Sandworm, Russia's Most Destructive Cyberwar Unit (wired.com)

38 US Treasury sanctions Russian research institute behind Triton malware (zdnet.com)

39 Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets (cisa.gov)

40 Two more cyber-attacks hit Israel's water system (zdnet.com);
What We've Learned from the December 1st Attack on an Israeli Water Reservoir (otorio.com)

41 October Mumbai power outage may have been caused by a cyber attack (securityaffairs.co)

Politisch und militärisch motivierte Angriffe gegen kritische Infrastrukturen werden weiterhin vor allem im Umfeld ohnehin eskalierter Konflikte beobachtet.

Bedrohung für Betreiber kritischer Kontrollsysteme stellen jedoch weiterhin Ransomware-Angriffe dar, die auch industrielle Prozesse miteinbeziehen, wie dies beispielsweise die Schadsoftware «EKANS»[42] mehrfach demonstrierte.

4.5.2 Herausforderung Absicherung der Supply Chain in der Digitalisierung industrieller Prozesse

Die Kontrollsysteme bestehen aus verschiedenen Komponenten unterschiedlicher Hersteller oder Open Source-Projekten. Taucht eine Schwachstelle früh in der Lieferkette auf, ist es für die Systembetreiber häufig schwierig einzuschätzen, ob ihre Steuerungen, Sensoren und Aktoren von der Schwachstelle betroffen sind, geschweige denn wie die Sicherheitslücke in ihrer Implementation behoben werden kann.

Exemplarisch zeigte sich diese Problemstellung, als man verschiedene Schwachstellen in Open source-Projekten entdeckte, welche die Nutzung von Netzwerkprotokollen in unterschiedlichsten Geräten ermöglichen. Die von den Entdeckern «AMNESIA:33»[43] betitelte Gruppe von Schwachstellen betraf über hundert Hersteller von Komponenten und Geräten. Das NCSC engagierte sich bei der Zusammenarbeit mit betroffenen Herstellern in der Schweiz, um die koordinierte Offenlegung der Schwachstellen und die Bereitstellung der Updates zu ermöglichen.

Um die Betreiber kritischer Infrastrukturen bei der Bewältigung dieser vielschichtigen Herausforderungen zu unterstützen, engagiert sich das NCSC mit seinem Fachwissen bei der Initiative des Kantons Zug beim Aufbau eines Nationalen Testinstituts für Cybersicherheit (NTC).[44]

4.6 Datenabflüsse

Datenlecks sind weiterhin ein aktuelles Phänomen und treten in verschiedensten Kontexten auf. Gestohlene Daten werden je nachdem von den Angreifern selbst weiterverwendet. Viel häufiger werden sie jedoch im Untergrundmarkt verkauft oder in Hackerforen publiziert. Viele Datenabflüsse werden erst durch das Auftauchen entsprechender Angebote bemerkt. Gewisse Akteure versuchen auch, die Opfer mit der Drohung erpressen, die Daten zu publizieren. Bei Ransomware hat dies neben der Verschlüsselung von Daten in das Geschäftsmodell der Akteure Eingang gefunden.

Der hohe monetäre Wert bestimmter Datenarten wie etwa medizinische Daten, Kunden- oder Identitätsdaten und in geringerem Masse auch Bankdaten, machen diese zu bevorzugten Zielen. Auch Daten zu geistigem Eigentum sind sehr begehrt und Gegenstand fortgeschrittener Spionagekampagnen.

---

42 This is how EKANS ransomware is targeting industrial control systems (zdnet.com)

43 AMNESIA:33 How TCP/IP Stacks Breed Critical Vulnerabilities in IoT, OT and IT Devices (forescout.com)

44 Kanton Zug plant nationale Prüfstelle für IT-Hardware (netzwoche.ch); Beteiligung des Bundes beim Aufbau und Betrieb des Nationalen Testinstituts für Cybersicherheit (parlament.ch)

4.6.1 Datendiebstahl von Schweizer Bürgern in Argentinien

Ende August 2020 wurden bei einem Ransomware-Angriff auf die argentinische Einwanderungsbehörde zehntausende Personendaten gestohlen, auch von rund 11'000 Schweizer Bürgerinnen und Bürgern.[45] Nachdem die betroffene Behörde kein Lösegeld bezahlt hatte, veröffentlichten die Diebe die Daten im Darkweb. Die Daten umfassten Name, Vorname, Geburtsdatum, Passnummer und Reiseziel der Betroffenen, jedoch keine Kopien der Pässe.

4.6.2 Zugangsdaten in der Hand von Hackern

Im August 2020 wurde entdeckt, dass Hacker IP-Adressen, Benutzernamen und Passwörter von VPN-Servern des Herstellers Pulse Secure von über 900 Unternehmen gestohlen[46] und anschliessend auf einem russischen Hackerforum veröffentlicht hatten. Die Daten werden für Angriffe von Ransomware-Gruppen genutzt, die diese Foren frequentieren. Das NCSC hat nach diesem Datendiebstal Kontakt mit den betroffenen Schweizer Unternehmen aufgenommen und sie über die Situation informiert, damit sie die betroffenen Zugangsdaten ändern konnten.

4.6.3 Versehentlich exponierte Daten

Die Offenlegung sensibler Daten muss nicht die Folge eines Cyberangriffs sein, sie kann auch von einem Konfigurationsfehler der Organisationen selbst ausgehen. Einem Bericht der Sicherheitsfirma Risk Based Security zufolge sind Datenlecks in 69 Prozent der Fälle mit interner Beteiligung versehentlich entstanden.[47] So wurde die britische Sicherheitsfirma Sophos darauf aufmerksam gemacht, dass ihre Kundendaten online einsehbar waren.[48] Die starke Nutzung von Cloud-Plattformen verstärkt dieses Phänomen, denn diese Plattformen erfordern eine fehlerfreie Konfiguration. Dem amerikanischen Pharmariesen Pfizer etwa ist ein Fehler bei der Konfiguration einer Google-Cloud-Plattform unterlaufen, wodurch Patientendaten insbesondere zu Krebsbehandlungen exponiert wurden.[49] Bei Untersuchungen von Internetressourcen hat die Cybersicherheitsfima CybelAngel über 45 Millionen offen zugängliche medizinische Bilder inklusive Patientendaten verteilt auf über zweitausend ungeschützte Server gefunden.[50]

Schlussfolgerung / Empfehlungen:

Der sorgfältige und verantwortungsbewusste Umgang mit Daten ist für Unternehmen ein wichtiges Themenfeld. Neben angemessenen Sicherheitsmassnahmen sollte sich jedes Unternehmen auch auf das Szenario Datenleck vorbereiten und einen entsprechenden Notfallplan (sog. «Data Breach Response-Plan») vorgängig erstellen, welcher im Ereignisfall ein schnelles und koordiniertes Handeln ermöglicht.

Weitere Informationen auf der NCSC-Website: Datenabfluss (ncsc.admin.ch)

45 Argentina hack reveals data on thousands of Swiss travellers (swissinfo.ch)
46 Hacker leaks passwords for 900+ enterprise VPN servers (zdnet.com)
47 2020 Year End Data Breach QuickView Report (riskbasedsecurity.com)
48 Sophos notifies customers of data exposure after database misconfiguration (zdnet.com)
49 Pharma Giant Pfizer Leaks Customer Prescription Info, Call Transcripts (threatpost.com)
50 More Than 45 Million Unprotected Medical Images Accessible Online (cybelangel.com)

4.7 Spionage

4.7.1 COVID-19 und Spionage

Die COVID-19 Pandemie führte zu einem internationalen Wettlauf im Bereich der medizinischen Erforschung des Virus und insbesondere hinsichtlich der Entwicklung von Impfstoffen. Während im ersten Halbjahr 2020 bereits Warnungen zu Spionageversuchen im Impfbereich publiziert wurden,[51] kam es in der zweiten Hälfte 2020 zu mehreren, öffentlich bestätigten Cyberspionageangriffen auf medizinische Forschungseinrichtungen und Pharmaunternehmen. Neue Techniken und Taktiken wurden aber bisher nicht beobachtet. Ausserdem blieben auch Behörden Aufklärungsziele vom Spionagekampagnen mit Bezug zu COVID-19, insbesondere im medizinischen Handlungsfeld, wie etwa der Zulassung von medizinischen Produkten.

Das Britische Zentrum für Cybersicherheit NCSC-UK publizierte zusammen mit Kanadas Informationssicherheitsbehörde CSE sowie der amerikanischen Cybersicherheitsbehörde CISA am 16. Juli ein Dokument, welches Cyberspionageangriffe auf COVID-19 Impfforschung dem Akteur «APT29» zuschrieb und insbesondere auf die Schadsoftware «Wellmess» hinwies.[52] APT29 ist auch bekannt unter dem Namen «Dukes» oder «CozyBear» und wird oft mit Russland assoziiert.[53]

Microsoft warnte im September vor Aufklärungskampagnen gegen Forschungsinstitutionen und Unternehmen im Bereich der Impfentwicklung[54] und publizierte im November Beobachtungen von Cyberangriffen gegen sieben Impfforschungsunternehmen.[55]

Im November wurde die Europäische Arzneimittelagentur (EMA) Opfer eines gezielten Cyberangriffs über dessen Herkunft, Ausmass und Konsequenzen aufgrund der laufenden Untersuchungen noch nicht sicheres bekannt ist.[56] Pfizer und Moderna publizierten Medienmitteilungen, welche bestätigten, dass Eindringlinge in den Systemen der EMA-Dokumente zu ihrer Impfstoffentwicklung stahlen.[57] Zu Beginn 2021 wurden dort gestohlene Daten betreffend des Pfizer/Biontech COVID-19 Impfstoffes im Internet publiziert.[58] Zur Täterschaft ist bisher nichts bekannt und der Fall wird weiterhin untersucht.

Im Dezember veröffentlichten Kaspersky Lab einen Bericht, der die nordkoreanische Hackergruppe «Lazarus» für Cyberspionageangriffe auf ein Pharmaunternehmen im September verantwortlich machte sowie für einen Angriff auf ein Gesundheitsministerium im Oktober, wobei verschiedene Typen von Schadsoftware eingesetzt wurden.[59]

---

51 Siehe MELANI Halbjahresbericht 2020/1, Kap. 4.6.1.

52 Advisory-APT29-targets-COVID-19-vaccine-development.pdf (ncsc.gov.uk)

53 APT 29 (Threat Actor) (fraunhofer.de)

54 Microsoft report shows increasing sophistication of cyber threats (microsoft.com)

55 Cyberattacks targeting health care must stop (microsoft.com)

56 Cyberattack on the European Medicines Agency (europa.eu)

57 Statement on Cyberattack on the European Medicines Agency (modernatx.com); Statement Regarding Cyber Attack on European Medicines Agency (biontech.de)

58 Hackers leak stolen Pfizer COVID-19 vaccine data online (bleepingcomputer.com)

59 Lazarus covets COVID-19-related intelligence (securelist.com)

Schlussfolgerung:

Alle Akteure, welche im Bereich COVID-19 Forschung betreiben und insbesondere in der Impfstoffentwicklung tätig sind, müssen mit Spionageangriffen diversen Ursprungs rechnen. Sowohl staatliche, als auch private Organisationen sind an entsprechenden Daten, Forschungsergebnissen und Geschäftsgeheimnissen interessiert.

4.7.2 Supply Chain Angriff: SolarWinds Orion IT

Am 13. Dezember meldeten amerikanische Behörden, dass eine Angreifergruppe über ein kompromittiertes Update der Software Orion IT in ihr Netzwerk eingedrungen war. In das offizielle Programm-Update war effektiv im März 2020 eine Hintertür eingebaut worden. Rund 18'000 Anwender dieser Software hatten das Update heruntergeladen. Die Angreifer suchten darunter interessante Ziele aus, um dort den Angriff weiterzuführen und schlossen bei den kollateral betroffenen Opfern die Hintertür wieder.

Amerikanischen Quellen zufolge war diese Operation Teil einer grösseren Spionagekampagne, die weitere Unternehmen traf und das Vorgehen wies Ähnlichkeiten mit demjenigen des Akteurs «APT29» auf.

Schlussfolgerung / Empfehlungen:

Durch die Kompromittierung eines Dienstleisters verschafften sich die Angreifer einen vorgelagerten Zugang zu ihren Zielen. Diese sogenannte «Supply Chain Attack»-Strategie ist in den letzten Jahren immer häufiger zu beobachten (siehe AVAST CC Cleaner, ASUS, Cloudhopper). Sie ist insbesondere deshalb interessant, weil sie den Zugang zu mehreren Zielen gleichzeitig ermöglicht und das Eindringen in einer ersten Phase besser verbirgt. Die finalen Ziele solcher Kampagnen sind typischerweise bedeutsam für die Angreifer und beeinflusst die Auswahl, welcher Zulieferer als Mittel zum Zweck ausgesucht wird. In Zukunft dürfte die Methode des Supply Chain-Angriffs jedoch auch von opportunistischen Angreifern genutzt werden, um möglichst viele Opfer zu generieren.

Zusätzlich zu einer Referenzbasis für die zulässige Kommunikation im eigenen Netzwerk, um Anomalien zu erkennen, empfiehlt es sich, beim Abschluss von Dienstleistungsverträgen die Informationen und Meldungen zu definieren, die ein Dienstleister im Falle eines Angriffs kommunizieren muss.

4.7.3 Hintertüren in chinesischer Steuersoftware

Im Sommer 2020 deckte die Sicherheitsfirma Trustwave zwei Schadprogramme namens GoldenSpy[60] und GoldenHelper[61] in Software für Steuerzwecke auf, die für in China niedergelassene westliche Unternehmen eingeführt wurde. Die Programme ermöglichen einen Fernzugriff

60 'GoldenSpy' Malware Hidden In Chinese Tax Software (securityweek.com)

61 Researchers Find More Malware Delivered via Chinese Tax Software (securityweek.com)

auf das Clientsystem. Von den Trustwave-Kunden waren ein Unternehmen im Bereich neue Technologien und ein grosses Finanzinstitut betroffen.

Schlussfolgerung / Empfehlungen:

Zum Schutz vor Spionagesoftware sollten Unternehmen behördlich angeordnete Software auf einem vom Rest des Netzwerks getrennten Computer installieren.

Konkrete Massnahmen für den vorliegenden Fall:

- Die Kompromittierungsindikatoren (Indicators of Compromise, IOC) in der FBI-Warnung in das Bedrohungsmonitoring aufnehmen (und auf allfällige neue IOC achten)
- Wenn Unternehmen diese Software bereits installiert haben, dies als möglichen Incident behandeln und die Anweisungen von Trustwave befolgen.

4.8 Social Engineering and Phishing

Die Vielfalt der verwendeten Inhaltstaktiken bei Phishing- und anderen Social Engineering-Angriffen ist nahezu unerschöpflich und sehr breitgefächert. Es sind mehr oder weniger originelle Geschichten mit angeblichen Vorkommnissen, die einen alltäglichen Bezug vortäuschen.

4.8.1 Übersicht Phishing

In der zweiten Jahreshälfte konnten 4'498 Phishing-Webseiten deaktiviert werden, welche über das vom NCSC betriebenen Portal antiphishing.ch gemeldet wurden. Im Vergleich zur ersten Jahreshälfte mit 3'029 Phishing-Webseiten, entspricht dies einer Zunahme von über 30 Prozent.

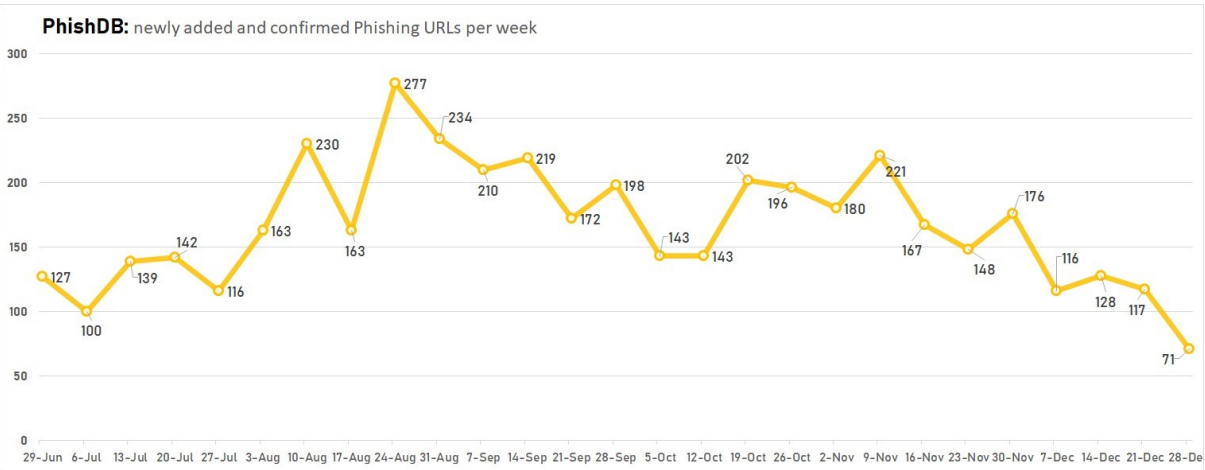


Abb. 6: Anzahl durch das NCSC überprüfte und bestätigte Phishing URLs pro Woche im zweiten Semester 2020. Aktuelle Daten finden Sie unter: https://www.govcert.admin.ch/statistics/phishing/

Einige Kampagnen täuschten Nachrichten von Telekommunikationsfirmen vor und behaupteten eine angebliche Rückerstattung einer doppelt geleisteten Zahlung. Andere Kampagnen verwendeten gefälschten Logos von Finanzinstituten und Unternehmen des Öffentlichen Verkehrs. Ziel von Phishing ist typischerweise, Login-Daten zum entsprechenden Onlineportal, Kreditkartendaten, Handynummern und weitere Informationen zu ergattern.

Bei zahlreichen Kampagnen wurde versucht, einen allfälligen per SMS übermittelten Sicherheitscode abzufangen, um die sog. Zwei-Faktor-Authentifizierung zu überwinden.

Hinweis:

Allgemeine Informationen auf unserer Website zu Phishing (ncsc.admin.ch)

4.8.2 Phishing-Szenario Paketversand

Pandemiebedingt wurde auch in der zweiten Jahreshälfte 2020 vermehrt online eingekauft. Die Wahrscheinlichkeit, dass jemand ein Paket erwartete, war gross. Diese Situation wurde bei diversen Phishing-Kampagnen per E-Mail und SMS aufgegriffen und ausgenutzt.

Fake-Gebühr für erneute Paketzustellung (via E-Mail)

In E-Mails eines bekannten Paketlieferdienstes wurde mitgeteilt, dass ein Paket aufgrund eines Problems nicht zugestellt werden konnte. Für die erneute Zustellung sei eine Gebühr fällig, damit das Paket in einer meist sehr kurzen Frist (innert 24 Stunden) erneut geliefert werden könne. Mittels eines Links wurde man auf eine gefälschte Website geleitet, welche vom Original kaum zu unterscheiden war. Für die Bezahlung musste man den Namen und die Kreditkartendaten angeben. Rein optisch wurde der Eindruck erweckt, als wäre der ganze Zahlungsablauf ordnungsgemäss erfolgt. Die Eingabe dieser Daten ermöglichte es den Kriminellen, die Kreditkarte für ihre eigenen Einkäufe einzusetzen.

Fake-Gebühr für zurückbehaltene Pakete (via SMS)

Bei einer anderen Variante gab eine vermeintlich von einem Paketlieferdienst stammende SMS vor, ein Paket sei aufgrund des fehlenden Portos zurückbehalten worden. Um die Lieferung zu bestätigen, müsse man den in der SMS aufgeführten Link anklicken. Der Link führte jedoch auf eine von Cyberkriminellen gestaltete Website, auf der man persönliche Angaben sowie Kreditkartendaten angeben musste. In der Folge wurden der Karte des Opfers monatlich Gebühren belastet oder sogar das ganze Konto geplündert.

4.8.3 Diebstahl von Apple-ID oder Installation von Spyware (via SMS)

SMS mit dem Inhalt: «Sie haben eine DIE POST-Sendung» und einem Link, führten je nach Typ des Mobiltelefons auf verschiedene Webseiten. Apple-Nutzende sollten auf einer Phishing-Seite ihre Apple-ID eingeben. Android Nutzer wurden aufgefordert, eine App zu installieren. Bei der App handelte es sich um Spyware, die Daten ausspäht und auch eine Hintertür (Backdoor) enthält. Die für den Versand verwendeten Nummern stammten von infizierten Handys, oder es handelte sich um gefälschte Nummern.

4.8.4 Missbrauch von Google-Diensten für Phishing

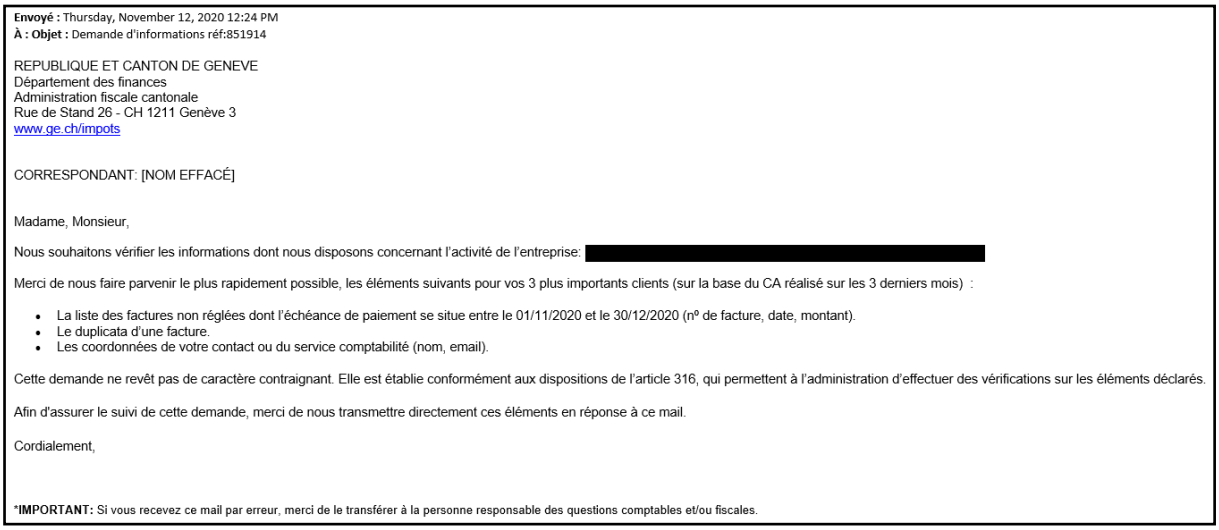
Die Sicherheitsfirma Armorblox[62] analysierte kürzlich, wie Cyberkriminelle eine Reihe von Google-Diensten für Phishing- oder Betrugskampagnen missbrauchen. In den meisten Fällen ist das Ziel der Angreifer der Diebstahl von sensiblen Daten (Zugangsdaten, Bankdaten und

62 OK Google, Build Me a Phishing Campaign (armorblox.com)

persönliche Daten). Google-Dienste werden von den wenigsten Unternehmen blockiert, was sich für die Angreifer als effiziente Methode zur Umgehung von Sicherheitsmechanismen erwiesen hat. Dies besonders dann, wenn Letztere diese Taktik mit fortgeschrittenen Social Engineering-Methoden kombinieren, um die Opfer zu überzeugen, z. B. eine Datei herunterzuladen oder ein Formular auszufüllen.

4.8.5 Missbrauch der Identität von Steuerbehörden

Bekanntheitsgrad und Dringlichkeit sind essentielle Mechanismen von Social Engineering. Daher bedienen sich Cyberkriminelle regelmässig der Identität von Behörden und insbesondere von Steuerbehörden, um an sensible Informationen zu gelangen. Im November 2020 erhielten mehrere Dutzend Unternehmen E-Mails, welche die Identität von Mitarbeitenden der kantonalen Steuerbehörde Genf vortäuschten. In den E-Mails wurde nach Kundendaten und offenen Rechnungen gefragt. Höchstwahrscheinlich dienste dies der Vorbereitung von Überweisungsbetrug (Wire Fraud). Die Steuerbehörde Genf warnte die Öffentlichkeit auf ihrer Website und per Newsletter.[63] 37 Unternehmen meldeten den Eingang betrügerischer E-Mails dieser Art.



Envoyé : Thursday, November 12, 2020 12:24 PM
À : Objet : Demande d'informations réf:851914

REPUBLIQUE ET CANTON DE GENEVE
Département des finances
Administration fiscale cantonale
Rue de Stand 26 - CH 1211 Genève 3
www.ge.ch/impots

CORRESPONDANT: [NOM EFFACÉ]

Madame, Monsieur,

Nous souhaitons vérifier les informations dont nous disposons concernant l'activité de l'entreprise: [redacted]

Merci de nous faire parvenir le plus rapidement possible, les éléments suivants pour vos 3 plus importants clients (sur la base du CA réalisé sur les 3 derniers mois) :

- La liste des factures non réglées dont l'échéance de paiement se situe entre le 01/11/2020 et le 30/12/2020 (nº de facture, date, montant).
- Le duplicata d'une facture.
- Les coordonnées de votre contact ou du service comptabilité (nom, email).

Cette demande ne revêt pas de caractère contraignant. Elle est établie conformément aux dispositions de l'article 316, qui permettent à l'administration d'effectuer des vérifications sur les éléments déclarés.

Afin d'assurer le suivi de cette demande, merci de nous transmettre directement ces éléments en réponse à ce mail.

Cordialement,

*IMPORTANT: Si vous recevez ce mail par erreur, merci de le transférer à la personne responsable des questions comptables et/ou fiscales.

Abb. 7: Beispiel eines Social Engineering E-Mails.

Empfehlungen:

Seien Sie beim Empfang unerwarteter Nachrichten vorsichtig. Der Absender und die Legitimität des Auftrags sollten überprüft werden. Besondere Vorsicht ist bei der Weitergabe von sensiblen Daten und bei finanziellen Transaktionen geboten. Sensibilisieren Sie insbesondere die Mitarbeitenden in Finanzabteilungen und Schlüsselpositionen. Sollte eine irrtümliche Zahlung erfolgt sein, wenden Sie sich umgehend an Ihre Bank. Allenfalls hat diese eine Möglichkeit, die Zahlung zu stoppen oder rückgängig zu machen.

63 L'AFC met en garde les entreprises contre des tentatives de phishing (ge.ch)

4.8.6 Spear-Phishing

Mit Spear Phishing werden Personen raffiniert und gezielt getäuscht, damit sie das tun, was der Angreifer will. Dieses Vorgehen erfordert Ressourcen und Zeit, weshalb ihre Verwendung oft auf staatliche Akteure oder gut organisierte Täterbanden hindeutet.

So berichtete beispielsweise Microsoft[64] über Aktivitäten des Akteurs «Phosphorus». Diese mutmasslich iranische Gruppe versuchte rund 100 Sicherheitsexperten dazu zu bringen, ihre E-Mail-Kontodaten preiszugeben. Sie setzten dafür gefälschte Plattformen für in München und Saudi-Arabien stattfindende internationale Sicherheitskonferenzen auf. Nachdem sie die Sicherheitsexperten identifiziert hatten, schickten sie ihnen Einladungen zu den Konferenzen. Die Zielpersonen sollten ihre biographischen Angaben mit Login und Passwort auf den vermeintlichen Konferenzwebsites eintragen. Mit diesen Angaben konnten die Täter dann auf die E-Mail-Konten der Opfer zugreifen und Daten stehlen.

In anderen Spear-Phishing-Angriffen gaben sich die Angreifer als Recruiter aus, kontaktierten ihre Opfer über das berufliche Netzwerk LinkedIn und stellten ihnen eine interessante Stelle in Aussicht. Verschiedene Akteurgruppen wie zum Beispiel die nordkoreanische «Lazarus»[65] nutzen diese Taktik. Bei der Operation «Dream Job» ging diese staatliche Tätergruppe wie folgt vor:

1. Es wird ein falsches LinkedIn-Konto als Recruiter eines grossen bekannten Unternehmens erstellt.
2. Sondierungsphase: Die Täter sammeln möglichst viele Informationen über ihre Zielperson für die spätere Verwendung.
3. Vorbereitung des «Traumjob»: Es wird ein falsches Jobangebot erstellt, das den Wünschen der Zielperson entspricht.
4. Kontaktnahme mit dem Opfer: Der falsche Recruiter kontaktiert die Zielperson über ihr LinkedIn-Kontaktnetz; es folgt eine Korrespondenz zum Jobangebot über Whatsapp oder per E-Mail.
5. Versand der Detailangaben zum Jobangebot in einer mit Schadsoftware angereicherten Word- oder PDF-Datei, die das Opfer via DropBox oder OneDrive herunterlädt. Dabei wird darauf geachtet, dass der Versand zu einem taktisch günstigen Zeitpunkt erfolgt, damit das Opfer am Arbeitsplatz ist und die Datei dort öffnet.
6. Die Infizierung erfolgt und die Täter breiten sich im anvisierten Netzwerk aus.
7. Das falsche LinkedIn-Profil wird gelöscht und die Konversation wird abgebrochen.

Einmal ins Unternehmensnetz eingedrungen, führen die Angreifer Spionage- oder Business-E-Mail-Compromise[66]-Aktivitäten aus.

Diese Taktik ist sehr raffiniert, weil sie von der Diskretion der Beteiligten ausgehen kann. Der gegenwärtige COVID-19-Kontext, in dem das Interesse an sicheren Stellen in grossen bekannten Unternehmen zugenommen hat, scheint die Taktik noch zu begünstigen.

---

64 Cyberattacks target international conference attendees (microsoft.com)

65 Dream-Job-Campaign (clearskysec.com)

66 Auf unserer Website finden Sie Informationen zu BEC-Betrug (ncsc.admin.ch)

5 Weitere Themen

5.1 Meldepflicht für kritische Infrastrukturen bei Cyberangriffen

Der Bundesrat hat im Dezember 2020 den Grundsatzentscheid getroffen, dass für Betreiber kritischer Infrastrukturen bei Cyberangriffen und der Entdeckung von Sicherheitslücken eine generelle Meldepflicht eingeführt werden soll.[67]

Der bisherige Austausch zu Cybervorfällen erfolgt auf freiwilliger Basis an das NCSC. Gemäss der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) ist die Einführung der Meldepflicht für kritische Infrastrukturen zu prüfen. Der Bundesrat hat nun das Eidgenössische Finanzdepartement (EFD) damit beauftragt, bis Ende 2021 einen entsprechenden Gesetzesentwurf zu erarbeiten. Darin sollen unter Berücksichtigung bereits bestehender Meldepflichten Kriterien festgelegt werden, wer welche Vorfälle innerhalb welcher Frist melden muss. Dabei sollen keine Daten über die Meldenden weitergegeben werden. Gleichzeitig will der Bundesrat eine zentrale Meldestelle schaffen.

Die im Rahmen der Meldungen erhobenen Daten dienen dazu, systematisch Frühwarnungen abzusetzen. Ziel dieses Informationsaustausches ist es, Angriffsmethoden frühzeitig zu erkennen, die Einschätzung der Bedrohungslage zusätzlich zu verbessern und die Sicherheit der Schweiz weiter zu stärken.

5.2 Kantone wollen den Kampf gegen Internetkriminalität besser koordinieren

Die Polizeikommandanten der Kantone wollen den Kampf gegen Cyber- und Pädokriminalität besser koordinieren. Zu diesem Zweck haben die Konferenz der Kantonalen Polizeikommandanten (KKPKS) und die Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) eine Vereinbarung getroffen, welche die Organisation und die Finanzierung eines «Netzwerks digitale Ermittlungsunterstützung Internetkriminalität (NEDIK)» regelt. Die Vereinbarung ist am 1. Januar 2021 in Kraft getreten.[68]

NEDIK wurde bereits 2018 durch die Konferenz der Kantonalen Polizeikommandanten der Schweiz (KKPKS) gegründet. Mit der nun geschlossenen Verwaltungsvereinbarung wird die Organisation und Finanzierung von Leistungen des Ermittlungsnetzwerks geregelt. Ziel von NEDIK ist unter anderem der gegenseitige Wissenstransfer, die Erstellung der nationalen Fallübersicht und die Triage von interkantonalen Fällen sicherzustellen. Weiter leistet NEDIK einen Beitrag an die Prävention und arbeitet mit der Schweizerischen Kriminalprävention (SKP) und mit dem Nationalen Zentrum für Cybersicherheit (NCSC) zusammen. NEDIK wird spezifische Analyseinstrumente einsetzen und eine zentrale Wissensdatenbank betreiben, um die digitale Kriminalität effizient zu bekämpfen. Innerhalb des Ermittlungsnetzwerks NEDIK übernimmt schliesslich das Bundesamt für Polizei (fedpol) die überkantonale und transnationale Rolle der Koordination und stellt die internationale Fallkoordination mit den Partnerbehörden wie beispielsweise Europol und Interpol sicher.

---

67 Bundesrat spricht sich für eine Meldepflicht für kritische Infrastrukturen bei Cyberangriffen aus (admin.ch)

68 Verstärkter Einsatz der Kantone gegen Cyber- und Pädokriminalität (kkjpd.ch)

5.3 Strategie Digitalaussenpolitik des Bundesrates

Die Digitalisierung eröffnet der Schweiz und ihrer Aussenpolitik neue Chancen. Denn die Schweiz verfügt über hervorragende Forschungsinstitutionen und zahlreiche internationale Organisationen sind in Genf vor Ort. Dieser Mix ermöglicht der Schweiz im Bereich der digitalen Gouvernanz eine besondere Rolle. Diese Rolle ist wichtig, denn die zunehmenden geopolitischen Spannungen zeigen sich auch im digitalen Raum, weil Daten heute eine zentrale Quelle von Macht sind. Auch gibt es Anzeichen für einen weltweiten Technologiewettlauf, insbesondere im Bereich der Künstlichen Intelligenz. Deshalb hat der Bundesrat die Digitalisierung in der Aussenpolitischen Strategie zu einem thematischen Schwerpunkt gemacht und mit der Strategie Digitalaussenpolitik[69] die Aktionsfelder definiert: Digitale Gouvernanz, Wohlstand und nachhaltige Entwicklung, Cybersicherheit und Digitale Selbstbestimmung.

In der digitalen Gouvernanz setzt sich die Schweiz für eine massvolle Regulierung ein und möchte das internationale Genf zum global führenden Hub für Digitalisierung und Zukunftstechnologien machen. Nichtstaatliche Akteure sind dabei besonders wichtig und werden in die Suche nach Lösungen einbezogen. Bei Wohlstand und Nachhaltigkeit geht es um die Förderung guter internationaler Rahmenbedingungen für die digitale Wirtschaft und neue Technologien. Im Cyberspace setzt sich die Schweiz für das Völkerrecht ein und fördert den Dialog mit der Privatwirtschaft über Verhaltensstandards im Cyberspace. Das Hauptziel digitaler Selbstbestimmung schliesslich ist es, den verantwortungsvollen Umgang mit Daten zu fördern und für mehr digitale Selbstbestimmung der Bürger zu sorgen.

5.4 Erste EU-Sanktionen gegen Cyberangreifer

Die EU hat 2020 erstmals von der 2019 verabschiedeten Cyber-Diplomacy-Toolbox[70] Gebrauch gemacht und Sanktionen gegen mutmassliche Cyberangreifer erlassen.

Gegen zwei Personen und eine mit dem russischen Militärgeheimdienst (GRU) verbundene Einrichtung wurden eine Reiseverbot und eine Vermögenssperre verhängt. Sie waren am Angriff auf das deutsche Parlament 2015 beteiligt, bei dem Parlamentsdaten gestohlen wurden. Auch Dritten wurde es verboten, den sanktionierten Personen und der Einrichtung finanzielle Mittel zur Verfügung zu stellen.[71]

Ähnliche Sanktionen wurden gegen sechs Personen und drei Einrichtungen chinesischer, russischer und nordkoreanischer Nationalität verhängt, aufgrund Beteiligung an den Kampagnen Wannacry, NotPetya, CloudHopper sowie an den Angriffen auf die Organisation für das Verbot chemischer Waffen (OVCW) und auf das ukrainische Stromnetz.[72]

---

69 Strategie Digitalaussenpolitik (eda.admin.ch)

70 BESCHLUSS 2019/797 DES RATES über restriktive Maßnahmen gegen Cyberangriffe (europa.eu)

71 Malicious cyber-attacks: EU sanctions two individuals and one body over 2015 Bundestag hack (europa.eu)

72 EU imposes the first ever sanctions against cyber-attacks (europa.eu)