SWITCH Security Report zu aktuellen Trends im Bereich IT-Security und Privacy

November/Dezember 2020

I. Choose your team carefully – Hacker nutzen gefakte MS-Teams-Updates zum Angriff auf Netzwerke vor allem von Bildungseinrichtungen

SARS-CoV-2 ist nicht das einzige Virus, mit dem man sich in der COVID19-Pandemie besser nicht infizieren sollte. Immer mehr Cyberkriminelle nutzen die COVID-19-Pandemie und die Massnahmen zu ihrer Bekämpfung, um auf immer neuen Wegen digitale Viren zu verbreiten. Aktuell warnt Microsoft davor, dass die Suche nach Microsoft Teams via Suchmaschine in den angezeigten Top-Ergebnissen und -Anzeigen auf Download-Seiten von Hackern führen kann. Dort wird dann eine gefakte Version der in Zeiten von Home Office, Videocalls und Online-Collaboration stark genutzten Software MS-Teams zum Download angeboten. Als unerwünschtes Gratis-AddOn kommt Malware auf die Devices. Durch die ZeroLogon-Schwachstelle verschafften (und verschaffen) sich die Hacker einen Administrator-Zugang zum gesamten Netzwerk und laden weitere Malware nach. Zumeist starten sie mit dem Diebstahl von sensitiven Daten, wie Zugangscodes und Zahlungsinformationen, und der Installation einer Backdoor, wie Bladabindi, um sich dauerhaft und unentdeckt Zugang zum Netzwerk zu verschaffen. Durch die Backdoor

werden dann Cobalt Strike Beacons nachgeladen, um das gesamte Netzwerk unauffällig auszuspionieren und weitere Malware einzunisten. Mehrere dieser Angriffe endeten damit, dass Erpressungssoftware die Dateien auf den befallenen Netzwerk-Devices verschlüsselte. Aktuell gibt es keine Aussagen dazu, ob die gegen Lösegeldzahlung wieder freigeschaltet wurden.

Die neue Angriffswelle zeigt sich doppelt perfide: Zum einen haben die Hacker nicht nur Suchmaschinen-Ergebnisse getürkt, um in die Top-Rankings der generischen Ergebnisse zu kommen, sondern auch Anzeigen auf den vorderen Plätzen gekauft. Zum anderen haben es die Kriminellen zunehmend auf Bildungseinrichtungen abgesehen, die in der Pandemie besonders häufig MS-Teams einsetzen, um Schul-, Lehr- und Forschungsbetrieb so gut wie möglich aufrecht erhalten zu können.

Zum Schutz empfiehlt Microsoft sechs Massnahmen:

1) Nutzen Sie Internetbrowser, die bösartige Websites erkenne und blockieren können.
2) Nutzen Sie starke, immer wieder wechselnde Passwörter, vor allem für Administratoren.
3) Beschränken Sie Administratorenrechte auf die systemrelevanten Nutzer.
4) Vermeiden Sie Service-Accounts für die gesamte Netzwerk-Domain, zumal wenn sie Administrator-ähnliche Zugriffsrechte haben.
5) Definieren Sie in einer regelmässig gepflegten Liste, nach welchen Kriterien die Ausführung von .exe-Dateien erlaubt und nach welchen sie blockiert wird und setzen Sie diese Regelung um.
6) Hindern Sie JavaScript and VBScript daran, .exe-Dateien herunterzuladen.

Nachzulesen unter:

https://www.bleepingcomputer.com/news/security/fake-microsoft-teams-updates-lead-to-cobalt-strike-deployment/
https://www.infocyte.com/blog/2020/09/02/cobalt-strike-the-new-favorite-among-thieves
https://malpedia.caad.fkie.fraunhofer.de/details/win.cobalt_strike
https://www.krone.at/2274182

II. Dreistes Corona-Phishing bringt Malware mit Bonus auf Antrag und fördert BEC

Und noch ein Fall von dreister Ausnutzung der corona-bedingt aktuellen Notsituation von Unternehmen: Phishing mit gefakten Corona-Soforthilfeanträgen. Im September bezeichnete das deutsche Bundeskriminalamt in der "Sonderauswertung Cybercrime in Zeiten der Corona-Pandemie" solche Phishing-Versuche als eine der wichtigsten ernst zu nehmenden Bedrohungen für die IT von Unternehmen und Organisationen.

Dabei verschicken die Cyberkriminellen Emails mit angehängten und gefälschten Antragsformularen für die seit Ende Oktober laufende Überbrückungshilfe II an ihre Opfer. Die haben doppelten Schaden, wenn sie die Fake-Anträge ausfüllen. Denn ihre sensiblen Daten sind abgefischt und die beantragte Überbrückungshilfe kommt auch nicht. Ganz zu schweigen vom neuerdings versprochenen – und natürlich nicht existenten – "Weihnachtsbonus" für kleine Unternehmen und Ein-Mann-Betriebe zw. Freiberufler.

Besonders betroffen sind offenbar T-Online-Kunden. Die EU-Kommissionsvertretung in Deutschland, merkte dazu dezent an, dass "die Empfängerinfrastruktur hinter T-Online keine Herkunftsüberprüfung der betrügerischen Emails durchführe". Der Magenta-Kommunikationsriese kündigte daraufhin "Gegen- und Kommunikationsmassnahmen" an.

Besagte EU-Kommissionsvertretung hat inzwischen die vierte Warnung herausgegeben und rät Empfängern solcher Emails, diese einfach zu ignorieren und ebenso unverzüglich wie endgültig zu löschen. Dies auch deshalb, weil Business Email Compromise (BEC) als eine spezifische Art der Cyberkriminalität immer höhere Schadenssummen verursacht. BEC-Angriffe beginnen in der Regel mit einem Mail, in dem Mitarbeiter (oder Unternehmer) getäuscht werden, damit sie gefälschte Rechnungen bezahlen oder Geld auf ein FakeKonto der Cyberkriminellen überweisen. So hat die Anti Phishing Workgroup APWG in ihrem "Phishing Activity Trend Report" vom September 2020 darauf hingewiesen, dass die mit Phishing erbeuteten Beträge von durchschnittlich 54.000 $ pro Fall auf 80.000 $ pro Fall angestiegen sind. Auch zeige sich mit der russischen BEC-Gang "Cosmic Lynx" seit 2019 eine Gruppe, die bislang mehr als 200 Angriffswellen gegen 46 Unternehmen oder Organisationen lanciert hat und durchschnittlich 1,27 Mio. $ einfordert.

Ende November warnte zudem das FBI davor, dass BEC-Gangster ihre Mails inzwischen auch in der Form weiterverbreiten, dass sie dem Internetclient eines Email-Accounts neue Auto-Weiterleitungsregeln implementieren. Dadurch verbreiten sie ihre Phishing Mails noch schneller und können sich letztlich in den Email-Verkehr einklinken, in dem es um Zahlungen und Finanztransaktionen geht. 2019, so das FBI, sei auf diese Art und Weise eine Schadenssumme von 1,7 Mrd. $ ergaunert worden.

Nachzulesen unter:

https://www.bka.de/SharedDocs/Pressemitteilungen/DE/Presse_2020/pm200930_BLBCybercrime.html
https://www.hwk-hannover.de/artikel/vorsicht-fake-mails-zu-corona-hilfspaket-23,0,5730.html
https://zac-niedersachsen.de/artikel/52
https://www.heise.de/news/Corona-Phishing-Betrueger-locken-mit-angeblichem-Weihnachtsbonus-fuer-Unternehmen-4974601.html
https://ec.europa.eu/germany/news/20201123-betrugsversuche-phishing_de
https://securityboulevard.com/2020/12/email-attackers-using-auto-forwarding-rules-to-perpetrate-bec-scams
https://www.zdnet.de/88382400/bec-wird-gefaehrlicher/

III. Stopp für Stoppt den Hass im Netz?

Dass im Netz an vielen Stellen ungezügelter Hass grassiert ist ebenso schändlich wie allseits bekannt. Deshalb haben Deutschland und Frankreich bereits – nicht unumstrittene – Gesetze gegen den Hass im Netz erlassen. Als Reaktion auf das französische Gesetz hatte die EU-Kommission die Mitgliedsstaaten gebeten, von weiteren Alleingängen abzusehen und stattdessen den Digital Services Act der EU umzusetzen, den die Kommission am 9. Dezember dieses Jahres veröffentlichen wollte.

Das hat der österreichischen Regierung offenbar zu lange gedauert. Sie hat Mitte November ein eigenes Gesetzespaket gegen den Hass im Netz vorgestellt. Darin inkludiert ist auch das KoPl-G, sprich: das Kommunikationsplattformen-Gesetz. Es droht den Plattformen mit hohen Strafen für den Fall, dass sie Hass-Postings und offensichtlich strafrechtlich relevante Beiträge nicht innerhalb kurzer Frist löschen. Damit es in Kraft treten kann, muss die EU-Kommission grünes Licht geben. Genau dagegen protestieren nun nicht nur die grossen Service-Provider, sondern auch Abgeordnete des Europäischen Parlaments. Während man ersteren unterstellen muss, dass sie die mit dem Gesetz verbundenen Auflagen und Aufwändungen scheuen, ist das Argumente-Spektrum der Abgeordneten aus unterschiedlichen Parteien und Länder breiter. Es reicht von Befürchtungen, dass nationale Alleingänge den Digital Services Act unterminieren und dazu führen könnten, dass EU-einheitliche Meldesysteme verhindert werden würden, die für eine rasche Liquidation von Hass-Content sorgen würden, bis hin zur Vermutung, das Unternehmen aus Vorsicht künftig zu viele Inhalte löschen könnten.

Nachzulesen unter:

https://www.zeit.de/digital/datenschutz/2020-06/hass-im-internet-gesetz-bundestag-hasskommentare-datenschutz
https://netzpolitik.org/2020/netzwerkdurchsetzungsgesetz-justizministerin-lobt-gesetz-gegen-hass-im-netz
https://digitalservicesact.eu
https://futurezone.at/netzpolitik/neues-gesetz-zu-hass-im-netz-was-sich-aendert/401019845
https://futurezone.at/netzpolitik/abgeordnete-eu-soll-hass-im-netz-gesetz-blockieren/401114265

IV. Macht zu die Tür, die Tor macht dicht: Was Sneakers mit dem Internet of Things vernetzt

Nein, hier geht es nicht um smarte turnschuh-ähnliche Fussbekleidungen, sondern um einen Film aus 1992, das Internet der Dinge (IoT für Internet of Things), eine neues US-amerikanisches Beschaffungsgesetz und LidarPhone – ein im November 2020 veröffentlichtes Forschungsprojekt, in dem ein staubsaugender vernetzter Roboter zum Hausspion umfunktioniert wurde. Hier schliesst sich der Kreis zum Film. Denn dort wühlen

Schnüffler um den im physischen Sinn smarten Robert Redford im realen Müll des CIO einer von der Mafia kontrollierten Firma, um dessen Präferenzen auszuspionieren und damit letztlich die Zugangscodes zum Supercomputer der Firma in die Hände zu bekommen. Derlei Infos könnten sie inzwischen eleganter, geruchsneutraler und weniger auffällig erlangen, würden sie LidarPhone benutzen.

Im November 2020 veröffentlichten die IT-Forscher Sriram Sami, Yimin Dai, Sean Rui Xiang Tan, Nirupam Roy und Jun Han die Ergebnisse eines Projekts, in dem sie einen auch in der Schweiz verkauften vernetzten Robot-Staubsauger in einen Abhörspion umrüsteten. Der Weg dazu: Robotsauger nutzen ein lasergestütztes Bewegungs- und Messsystem zur sicheren Orientierung und schadensfreien Bewegung im Raum: LIDAR (für Light Detection and Ranging). Das haben die Forscher nach dem Hack des smarten Saugers in eine Art Mikrofon umgewandelt, mit dem sie z.B Sprachsignale im Raum aufnehmen und auf ihren Rechnern abspeichern konnten. Angesichts der corona-bedingten Zunahme von Homeoffice und Videocalls ein interessanter Weg für Kriminelle und Spione, um an sensible Informationen zu kommen (und ganz ohne Mülltonnen-Gewühle). Besonders beachtenswert dabei ist aber, dass IoT-Geräte gar kein Mikrofon verbaut haben müssen, und dennoch als Abhörwanzen eingesetzt werden können.

Dazu braucht es sicher ein sehr grosses Mass an IT- und Sensorik-KnowHow. Und dann muss das angepeilte IoT-Gerät erst einmal gehackt werden. Das dürfte aber bei den meisten vernetzten Geräten der leichteste Teil der Übung sein. Wiederholt haben wir an dieser Stelle darauf hingewiesen, wie nachlässig viele IoT-Devices – vor allem periphere wie Überachungskameras oder smarte Haushaltsgeräte – verschlüsselt (oder eben nicht verschlüsselt) sind. Mit Sicherheitscodes wie "1234", "9" oder "0" öffnen sie Hackern die Tür in Netzwerke so weit wie seinerzeit die Trojaner dem hölzernen Pferd ihrer griechischen Belagerer.

Das hat auch der amerikanische Gesetzgeber erkannt. Im Weissen Haus liegt ein von beiden Kammern beschlossenes Gesetz zur Verbesserung der IT-Sicherheit bei Bundesbehörden. Der "IoT Cybersecurity Amendment Act of 2020" fordert diese dazu auf, nur noch solche vernetzten Geräte zu verwenden, die den noch festzulegenden Sicherheitsstandards des National Institutes of Standards and Technology (NIST) Genüge leisten. Alle anderen müssten dann aussortiert und ersetzt werden. Aufgeschreckt wurde der amerikanische Gesetzgeber wohl auch durch den jährlichen "Unit 42 IoT Threat Report" des Forschungsteams für Cybersicherheit von Palo Alto Networks, Unit 42. Dessen im März 2020 veröffentlichte Ausgabe zeigt drastisch, welche grosse Risiken IoT-Geräte für die Cybersicherheit darstellen, weil Betriebssysteme und Protokolle oft veraltet bzw. nicht aktualisiert seien oder 98 % des gesamten Netzwerkdatenverkehrs zwischen IoT-Geräten nicht verschlüsselt ablaufen. Damit es nicht beim guten Vorsatz bleibt, soll die

Budgetbehörde OMB die Umsetzung der gesetzlichen Regelungen zeitnah nach Einführung des Gesetzes überprüfen. Zudem sollen auch Lieferanten und alle Subunternehmer über den Verkauf hinaus Informationen zu Sicherheitslücken und deren Behebung liefern, wenn sie Bundesbehörden beliefern möchten.

Es bleibt zu hoffen, dass sich möglichst viele Hersteller, Dienstleister und Anwender auf ein Mehr an Sicherheit bei IoT-Geräten besinnen.

Nachzulesen unter:

https://dl.acm.org/doi/10.1145/3384419.3430781
https://www.tagesanzeiger.ch/vorsicht-der-staubsauger-hoert-mit-234979732541
https://www.heise.de/news/IoT-Gesetz-zwingt-US-Behoerden-zu-mehr-IT-Sicherheit-4972510.html
https://start.paloaltonetworks.com/unit-42-iot-threat-report

Dieser SWITCH Security Report wurde von Dieter Brecheis und Frank Herberg verfasst.