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

Januar/Februar 2023

I. Virtuelle Maschine, reale Bedrohung: weltweite Attacke auf VMware-ESXi – sofort patchen!

Unter Cyberkriminellen scheint sich ein neuer Trend zu entwickeln: Man nehme eine seit längerem bekannte Sicherheitslücke, gehe davon aus, dass sie unabhängig davon, ob Patches verfügbar sind oder nicht, auf vielen Geräten nicht geschlossen wurde und nutze sie gnadenlos aus. Was bei Microsoft Exchange Servern im Sinne der Hacker prima funktioniert hatte, trifft nun VMware. So meldete die italienische Cybersecurity-Behörde ACN anfangs Februar, dass Tausende von Servern weltweit erfolgreich angegriffen und mit Ransomware infiziert worden seien. Bleepingcomputer.com berichtete von mehr als 3'200 befallenen Servern. Am stärksten betroffen war Frankreich, gefolgt von den Vereinigten Staaten, Deutschland, Kanada und dem Vereinigten Königreich. Auch finnische und italienische Server wurden kompromittiert. Die US-amerikanische Cybersicherheitsagentur CISA bestätigte die Angriffe ebenso wie das französische CERT, das kurz nach den italienischen Behörden vor massiven Angriffen auf die seit langem bekannte VMware-ESXi-Schwachstelle mit der Bezeichnung CVE-2021-21974 gewarnt

hatte. Mit einem CVSS-Wert von 8.8 des bis 10.0 reichenden Common Vulnerability Scoring Systems gilt diese Lücke als riskant. Sie tut sich in den ESXi-Versionen 7.x (älter als ESXi70U1c-17325551), 6.7x (älter als ESXi670-202102401-SG) und 6.5x (älter als ESXi650-202102101-SG) auf.

Zwar stehen bereits seit Februar 2021 Sicherheitsupdates bereit, doch sind offenbar viele Server trotz des hohen Risikos bis jetzt nicht gepatcht worden. Das französische CERT empfiehlt auf seiner Website daher mit Nachdruck, die Patches einzuspielen, verweist aber auch darauf, dass das Schliessen der Sicherheitslücke naturgemäss nicht reicht, sollte ein Server bereits angegriffen sein.

Inzwischen hat heise.de berichtet, dass die US-amerikanische Sicherheitsbehörde CISA mit recover.sh ein Unix-Shell-Skript zur Wiederherstellung betroffener Maschinen auf GitHub im Projekt ESXIArgs-Recover bereitgestellt hat. Der Link ist unten angegeben.

Nachzulesen unter:

https://www.heise.de/news/Italiens-Cyber-Sicherheitsbehoerde-warnt-vor-weltweitem-Ransomware-Angriff-7485377.html
https://www.bleepingcomputer.com/news/security/massive-esxiargs-ransomware-attack-targets-vmware-esxi-servers-worldwide
https://techcrunch.com/2023/02/06/hackers-vmware-esxi-ransomware/
https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-015/
https://www.heise.de/news/Ransomware-Attacke-CISA-veroeffentlicht-Wiederherstellungsskript-fuer-VMware-ESXi-7488498.html
https://github.com/cisagov/ESXiArgs-Recover

II. Von FA zu 2FA – Facebook-Account mit Zwei-Faktor-Authentisierung schützen

Was sich im e-Banking oder beim Login auf besonders sensible Seiten, wie z.B. dem Online-Konto bei der eigenen Krankenversicherung, immer stärker als Standard durchsetzt, ist bei Social Media-Accounts noch eher die Ausnahme: die Zwei-Faktor-Authentisierung. Viele User fragen sich, ob der Aufwand bei ihren Accounts denn doch nicht des Guten zu viel ist. Ist er offenbar nicht, denn auch, wenn die Account-Inhalte für Hacker in den meisten Fällen keine lohnenden Verwertungsoptionen bieten, kann der Account selbst für Cyberkriminelle höchst attraktiv sein, beispielsweise, um über gehackte Facebook-Konten Kinderpornografie zu verbreiten.

Genau darauf hat das Landeskriminalamt des deutschen Bundeslandes Niedersachsen hingewiesen. Die norddeutschen Ermittler beobachten dieses Phänomen erst seit kurzem und bezeichnen es als «Facebookhacking» oder «Facebookphishing». Zunächst erbeuten die Kriminellen die Zugangsdaten zu den Accounts – meist via Phishing oder indem sie weitverbreitete Passwörter ausprobieren (credential stuffing). Dann übernehmen sie die

Konten ihrer Opfer und laden ihr schändliches Material hoch.

Die Opfer werden dabei mindestens doppelt geschädigt: Einmal, weil Facebooks Mutterkonzern Meta das Konto wegen illegaler kinderpornografischer Inhalte sofort sperrt und den Vorfall ans National Center for Missing & Exploited Children NCMEC meldet. Als halbstaatliche US-amerikanische Einrichtung leitet das NCMEC strafrechtlich relevante Informationen umgehend an US-Strafverfolgungsbehörden. Sind die Zugangskonten ausserhalb der USA gemeldet, werden die jeweiligen Instanzen des betroffenen Landes informiert. Und dort – und das ist der zweite Schaden mit oft weitreichenderen Konsequenzen – werden die Kontoinhaber in einem Strafverfahren wegen Besitzes oder Verbreitung von Kinder- oder Jugendpornografie beschuldigt. Zwar weist das LKA Niedersachsen in seiner Meldung darauf hin, dass die deutschen Staatsanwaltschaften in den meisten Fällen die Verfahren einstellen, sobald sichergestellt ist, dass der Account gehackt worden war. Angenehm ist das Prozedere aber für die Betroffenen sicher nicht.

Wer sich davor schützen will, hat bei Facebook schon seit längerem die Möglichkeit, ein TOTP (Time-based One-Time Password) zu generieren oder (nicht so gut) eine Zwei-Faktor-Authentifizierung via SMS zu nutzen. Wie das geht, steht im Hilfebereich auf facebook.com. Allerdings war Ende Januar bekannt geworden, dass sowohl bei Facebook als auch beim Schwester-Medium Instagram eine Schwachstelle erlaubt, die Zwei-Faktor-Authentifizierung via SMS zu umgehen. Der Zuckerberg-Konzern hat die Schwachstelle bestätigt und ihrem Entdecker 27'000 Dollar aus dem hauseigenen Bug-Bounty-Programm ausgezahlt. Ob die Lücke zwischenzeitlich geschlossen ist, ist bis dato aber nicht bekannt.

Nachzulesen unter:

https://www.heise.de/news/LKA-Warnung-Kinderpornografie-Posts-nach-Facebook-Hacks-7487612.html
https://www.golem.de/news/2fa-wie-sicher-sind-totp-fido-sms-und-push-apps-2206-166287-3.html
https://www.facebook.com/help/358336074294704
https://www.heise.de/news/Zwei-Faktor-Authentifizierung-Facebook-Instagram-Bug-ermoeglichte-Umgehung-7476725.html

III. AI breaking bad – wie Cyberkriminelle ChatGPT und andere künstliche Intelligenzen nutzen

In einem t3n-Porträt wird Open AI-Geschäftsführer Sam Altmann mit den Worten zitiert «Ich bin vor allem besorgt, dass sie (die KI-Anwendung, Anm. d. Red.) versehentlich missbraucht wird.» An diesem Punkt kann der Mann, der hinter ChatGPT steht, beruhigt werden. Denn KI- (oder AI-) Anwendungen werden zwar missbraucht, aber nicht versehentlich, sondern ganz bewusst. Und das in immer grösserem Ausmass.

So befassten sich Ende Januar mehrere Security-Blogs mit dem Thema. Unter anderem

stellte die bekannte Cybersecurity-Firma McAfee am 25. Januar einen Blogbeitrag online, in dem explizit davor gewarnt wird, dass sich Hacker die unbestritten enormen Fähigkeiten der AI ChatGPT auf mehreren Wegen zunutze machen.

Zum einen könnten sie Malware sowohl quantitativ als auch qualitativ in neue Dimensionen führen, weil ChatGPT keine Pausen braucht, sondern 24/7 und rund um die Uhr Malware schreiben kann. Schlimmer noch: ChatGPT und andere hochentwickelte AI sind in der Lage, sogenannte polymorphe Malware zu entwickeln, die sich quasi selbstlernend weiterentwickelt und so nahezu kaum mehr auffindbar, geschweige denn zu bekämpfen ist.

Zum anderen könnte ChatGPT als Cyrano de Bergerac des 22. Jahrhunderts auf Dating-Plattformen mit unbegrenzten und formvollendet formulierten Liebesschwüren von Fake-Profilen unbedarfte User dazu verleiten, sensible persönliche Daten oder gleich Geld zu schicken.

Apropos formvollendet: Konnten Phishing-Mails oft schon allein anhand inkorrekter Orthografie oder Grammatik erkannt werden, so wird das dann nahezu unmöglich, wenn Hacker unversehentlich die Dienste von ChatGPT nutzen – wobei man schon fragen könnte, was grösser ist: die Rechtschreib- und Grammatiklücken nordkoreanischer Phisher oder die (vielleicht sogar als Ablenkungsmanöver bewusst inszenierte?) Naivität eines Sam Altman. Dessen Company stellt nämlich neben ChatGPT mit der künstlichen Intelligenz DALL-E die Basis zur AI-basierten Erstellung von Phantombildern bereit. Die Kritik richtet sich dabei nicht nur dagegen, dass diese Bilder auf weit weniger komplexen Kriterien beruhen würden, als dies im Fall von Zeugenaussagen auf Basis menschlicher Erinnerungen geschehen würde. Vielmehr wird DALL-E selbst vorgeworfen, stark vorurteilsbehaftet zu sein. So hätte nach Berichten von futurezone.at die AI nach Eingabe des Akronyms «CEO» ausschliesslich Bilder weisser Männer generiert, während nach Eingabe von «Gangster» Bilder dunkelhäutiger Männer und Latinos und bei «Pflegepersonal» stets Bilder weiblicher Personen auf den Ausgabebildschirmen erschienen.

Ungeachtet dessen sehen alle Tech-Giganten in AI the «Next Big Thing». Nachdem Microsoft ChatGPT in seine Suchmaschine BING integriert hat, verwundert es daher kaum, dass Google mit «Bard» ein eigenes Angebot angekündigt hat, um seine Suchmaschinen-Position zu verteidigen und neue Möglichkeiten zu erschliessen. Man darf gespannt sein, ob die Cola-Wars aus den 1990er Jahren ihre moderne Fortsetzung in den AI-Battles des 22. Jahrhunderts finden werden.

Nachzulesen unter:

https://t3n.de/news/sam-altmann-der-mann-hinter-chatgpt-open-ai-1530670
https://securityaffairs.com/140380/hacking/hackers-exploiting-chatgpt.html
https://www.mcafee.com/blogs/internet-security/chatgpt-a-scammers-newest-tool/
https://cyberscoop.com/chatgpt-ai-malware/

https://futurezone.at/digital-life/ki-phantombilder-phantomzeichnungen-polizei-zeugen-kuenstliche-intelligent-dall-e-openai/402321494
https://futurezone.at/science/bildgenerator-kuenstliche-intelligenz-dall-e-imagen-google-artificial-intelligence/402050017
https://www.indiatimes.com/technology/news/ai-programme-generates-police-sketches-of-potential-suspects-592537.html
https://www.handelszeitung.ch/tech/chat-gpt-open-ai-und-microsoft-starten-offensive-gegen-google-571387
https://www.hackread.com/google-bard-chatgpt-rival/

IV. Cybererpresser im Minus = Cyberangriffe im Plus

Im 2022 sollen die Profite aus Ransomeware-Angriffen um 40% eingebrochen sein. Das geht aus einer Statistik hervor, die Ende Januar von der Blockchain-Plattform «chainalysis» veröffentlicht wurde. Gleichzeitig verweist sie auf eine ungleich höhere Dunkelziffer. Wie hoch diese tatsächlich sein muss, lässt sich daraus ableiten, dass nach internen Berichten der UN allein die nordkoreanischen Staatscyberkriminellen des globalen Obererpressers Kim Jong-Un 2022 Rekordeinnahmen von etwa 1,2 Milliarden US-Dollar erzielt hätten.

Demgegenüber weist die chainalysis-Statistik einen Gesamt-«Ertrag» aller offiziell bekannten Ransomware-Einnahmen für 2022 in Höhe von 457 gegenüber 766 Millionen US-Dollar in 2021 aus – ein Minus von 309 Mio. Dollar. Davon lassen sich alleine ca. 130 Mio. Dollar mit der Zerschlagung von «Hive» erklären. Dieses seit 2021 international agierende Netzwerk von Cyberkriminellen hatte sich auf das Angebot von «Ransomware-as-a-Service» spezialisiert. Es wird für Angriffe auf mehr als 1'500 Opfer mit einer Schadenssumme von mehr als 100 Mio. Dollar verantwortlich gemacht.

In einer ebenfalls international koordinierten Undercover-Aktion haben Investigativ-Teams unter der Leitung des FBI zusammen mit deutschen und niederländischen Ermittlern seit 2022 das Hive-Netzwerk infiltriert. Sie zogen über 300 Entschlüsselungscodes ab und leiteten diese an angegriffene Opfer weiter. Damit konnten sie ihre Geräte entschlüsseln und von Hive geforderte Lösegeldforderungen verweigern. Zudem sicherten die Ermittler etwa 1.000 weitere decryption keys aus früheren Angriffen.

Dass immer mehr Angegriffene den Forderungen zur Zahlung eines Lösegelds nicht nachkommen, berichtet auch bleepingcomputer.com unter Berufung auf Statistiken des Cybersecurity-Unternehmens Coveware. Ihnen zufolge war der Anteil jener Opfer, die sich weigerten, Lösegeld zu zahlen, 2022 erstmals grösser als jener, die zahlten. Lag dieses Verhältnis 2019 noch bei 24% zu 76%, kippte es 2022 auf 59% zu 41%.

Bedauerlicherweise (wenn auch zu erwarten) reagieren die Cybergangster auf diese für sie unerfreuliche Entwicklung, indem sie ihre Geschäftsmodelle gerade in verschiedene Richtungen verändern: Zum einen erhöhen sie die Lösegeldforderungen, um mehr Geld aus ihren Opfern herauszupressen. Zum anderen greifen sie ihre Opfer nicht nur mit

einer bestimmten Ransomware (wie z.B. Cryptolocker, Petya, Bad Rabbit o.a.) an, sondern setzen mehrere solcher Ransomware Strains gleichzeitig ein. Darüber hinaus greifen sie Opfer, die bereits einmal gezahlt haben, erneut an. Coveware bemerkt dazu, dass diese Strategie früher eher gegen kleine Unternehmen und Organisationen gerichtet war, inzwischen aber auch gegen mittlere und grosse Player zum Einsatz kommt.

Ausserdem ist zu beobachten, dass einige Gruppen den Erpressungsprozess selbst verändern. Während die Kriminellen beim «Double Pay Day» nach der ersten Lösegeldzahlung für die Entschlüsselung der Daten eine Zweite dafür verlangen, dass diese Daten nicht veröffentlicht werden, verzichten die Hacker in manchen aktuellen Ransomware-Attacken gleich auf den Verschlüsselungsteil eines Angriffs und fokussieren sich darauf, die Daten zu stehlen und mit ihrer Veröffentlichung zu drohen. Das macht die Angriffe einfacher und schneller und gibt den Angreifern damit mehr Sicherheit vor Entdeckung und Verfolgung. Ausserdem steigt damit die Wahrscheinlichkeit, dass Organisationen der kritischen Infrastrukturn bezahlen, weil sie verhindern wollen (oder müssen), dass sensible Daten an die Öffentlichkeit gelangen.

Nachzulesen unter:

https://blog.chainalysis.com/reports/crypto-ransomware-revenue-down-as-victims-refuse-to-pay
https://www.stern.de/digital/un-bericht--un--nordkoreas-hacker-stehlen-rekordsummen---kim-ruestet-auf-33172534.html
https://www.zdnet.com/article/doj-takes-down-ransomware-group-with-a-21st-century-cyber-stakeout
https://www.bleepingcomputer.com/news/security/ransomware-profits-drop-40-percent-in-2022-as-victims-refuse-to-pay
https://www.darkreading.com/attacks-breaches/ransomware-profits-decline-victims-refuse-pay

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