Switch Security Report

zu aktuellen Trends im Bereich IT-Security und Privacy

Januar/Februar 2024

I. Der Angriff der Killer-Zahnbürsten – nachbohren ist besser als in saure (News)Äpfel beissen!

Am 30. Januar berichtete die Aargauer Zeitung unter Berufung auf Experten der Cybersecurity-Firma Fortinet, dass aktuell drei Millionen smarte elektronische Zahnbürsten mit Malware infiziert worden seien. Dies, um sie in einem Botnet für DDoS-Attacken auf Schweizer Unternehmen zu missbrauchen. Bei einem erfolgreichen Angriff auf die Website eines nicht näher genannten Unternehmens sei diesem ein Schaden von mehreren Millionen Franken entstanden. Die Meldung verbreitete sich viral über IT-affine Portale rund um den Globus. Andere Sicherheitsfachleute wurden hellhörig und schlugen Fake-News-Alarm. Und dieser erwies sich als berechtigt. Die Aargauer Zeitung und Fortinet schoben sich gegenseitig die Verantwortung zu. Fortinet erklärte, man habe der Aargauer Zeitung anhand eines hypothetischen Beispielszenarios aufzeigen wollen, welches Gefahrenpotenzial jedes vernetzte IoT-Gerät – vom Babyphone über die Smart-Home-Kamera bis zur smarten Zahnbürste – berge. Offenbar wurde dieses Szenario aufgrund von Übersetzungsfehlern als real wahrgenommen und publiziert. Die Aargauer Zeitung wies ihrerseits darauf hin, dass dies von Fortinet vor der Veröffentlichung des Artikels anders dargestellt worden sei.

Mittlerweile bemühen sich Blogs und Newsplattformen – darunter auch jene, die die Story verbreitet hatten – um Gegendarstellungen und Richtigstellungen. Bleepingcomputer.com weist

darauf hin, dass der Wahrheitsgehalt der Story aufgrund fehlender Details und technischer Ungenauigkeiten von vornherein hätte in Frage gestellt werden müssen. So sind viele IoT-Geräte (auch smarte Zahnbürsten) nicht direkt mit dem Internet verbunden, sondern senden ihre Daten via Bluetooth an eine App, die diese dann an einen Webserver weiterleitet. Daher wäre für einen Angriff von Killerzahnbürsten eine wesentlich komplexere Struktur erforderlich.

Unterdessen raten Expertinnen und Experten, Berichte über gross angelegte Cyberattacken vor ihrer Veröffentlichung gründlich zu prüfen, damit die Awareness und Wachsamkeit angesichts der weltweit zunehmenden Cyberkriminalität und kriegerischen Cyberaktivitäten nicht nachlassen. So hat sich u.a. die Münchner Sicherheitskonferenz in ihrer 2024er-Auflage erstmals in signifikantem Umfang mit Cybersicherheitsfragen befasst. Und der Cybersicherheitsexperte Paul Ducklin gibt in seinem unten verlinkten Blogbeitrag fundierte Tipps, wie man die Balance zwischen schneller Information und Verdeutlichung einer Bedrohung einerseits und viral verbreitenden Fake News andererseits finden kann. Sein wichtigster Rat: «Don’t make much ado about nothing!»

Nachzulesen unter:

https://www.aargauerzeitung.ch/wirtschaft/kriminalitaet-die-zahnbuersten-greifen-an-das-sind-die-aktuellen-cybergefahren-und-so-koennen-sie-sich-schuetzen-ld.2569480
https://www.aargauerzeitung.ch/wirtschaft/cyberangriff-die-gehackten-zahnbuersten-gehen-medial-um-die-welt-und-loesen-fragen-aus-wie-es-dazu-kam-ld.2577182
https://www.tomshardware.com/networking/three-million-malware-infected-smart-toothbrushes-used-in-swiss-ddos-attacks-botnet-causes-millions-of-euros-in-damages
https://www.golem.de/news/iot-hacker-missbrauchen-zahnbuersten-fuer-ddos-angriffe-2402-181921.html
https://www.independent.co.uk/tech/toothbrush-hack-cyber-attack-botnet-b2492018.html
https://www.bleepingcomputer.com/news/security/no-3-million-electric-toothbrushes-were-not-used-in-a-ddos-attack/
https://pducklin.com/2024/02/08/tall-toothbrush-tales-how-to-avoid-x-million-y-attacked-z-hype/

II. Any Information on AnyDesk?

Wir haben in diesen Security Reports immer wieder darauf hingewiesen, dass die Bedrohungslage weiterhin angespannt ist. Ebenso, dass sowohl private als auch staatsnah oder staatlich agierende Hacker und Hackergruppen zunehmend Ziele angreifen, die eine Skalierung des Schadens versprechen. Jüngstes Beispiel: AnyDesk. Die Stuttgarter Softwareschmiede mit Filialen in Tampa Bay, Shanghai und Hong Kong hat weltweit bei 170'000 Kunden Systeme für Fernzugriff und Fernwartung im Einsatz. Am 31. Januar berichtete heise.de, dass die Fernwartungssoftware bereits seit einer Woche nur mit Störungen funktioniere, AnyDesk dafür Wartungsfenster und ein Softwareupdate angeboten habe, aber keine näheren Informationen zu den Hintergründen, obwohl thehackernews.com in einem Artikel vom 3. Februar 2024 darauf hinweist, dass AnyDesk Kunden bereits am 24. Januar 2024 über das Kundenportal vor Störungen und Unterbrechungen des Systembetriebs gewarnt habe.

Dass das Unternehmen den Störfall dennoch erst am 1. Februar 2024 an die Behörden meldete,

stiess bei Kreisen von Sicherheitsfachleuten auf Kritik. So zitierte cybersecuritydive.com den Chief Trust Officer von SentinelOne mit den Worten: "…they knew this on Jan.29 but didn't announce until the end of day on Friday. Not cool!" (redaktioneller Hinweis: das war der 2. Februar)

Am 2. Februar 2024 gab AnyDesk dann in einer eigener Mitteilung bekannt, dass man einen Einbruch in verschiedene Produktionssysteme des Unternehmens entdeckt habe. Man habe daraufhin gemeinsam mit den Sicherheitsfachleuten von CrowdStrike alle Systeme überprüft und wo nötig neu aufgesetzt, Zertifikate erneuert und einen Passwort-Reset auf Kundenseite erzwungen. Ein Abfluss von Kundendaten oder kompromittierte Kundensysteme seien derzeit nicht erkennbar, so AnyDesk. Demgegenüber berichtete heise.de am 4. Februar 2024, dass die Cybersecurity-Firma Resecurity in einem Forum für Cyberkriminelle ein Angebot für 18'000 Datensätze von AnyDesk-Kunden entdeckt und verifiziert habe. Gegenwärtig sei aber unklar, wie aktuell diese Datensätze seien.

Fest steht hingegen, dass es sich um Login-Daten für das Kundenportal von AnyDesk handelt, die zumindest einen Teil ihres Werts dadurch verloren haben, dass AnyDesk nach Bekanntwerden des Einbruchs alle Logins für ungültig erklärt und alle Kunden aufgefordert hatte, neue Passwörter oder eine Multifaktor-Authentifizierung einzurichten. Dennoch bergen die angebotenen Daten ein Bedrohungspotenzial, da Kundendetails, wie die Anzahl der mit der Software arbeitenden Devices, Lizenzschlüssel der Software, Login-Zeiten etc. ein Ausspähen der Unternehmen ermöglichten.

AnyDesk bekräftigte daraufhin in einer weiteren Mitteilung vom 5. Februar 2024, dass keine Informationen über den Abfluss von Kundendaten oder die Kompromittierung von Kundensystemen vorlägen, empfahl aber dennoch zur Sicherheit ein Update auf die Versionen 7.0.15 oder 8.0.8. Am selben Tag bestätigte das deutsche Bundesamt für Sicherheit in der Informationstechnik BSI den Vorfall und die Angaben des Unternehmens.

Da nicht ausgeschlossen werden kann, dass sowohl Quellcode als auch Zertifikate abgeflossen sind, besteht laut BSI die Gefahr, dass AnyDesk-Kunden angegriffen werden könnten, zumal die Software häufig mit privilegierten Rechten eingesetzt wird – wie eingangs geschildert: (Zu)Viele Cyberkriminelle beherrschen ihr Geschäft! In diesem Zusammenhang wird vor allem vor Man-in-the-Middle- und Supply-Chain-Angriffen gewarnt. Das BSI empfiehlt allen AnyDesk-Kunden ein Update auf die neueste Software mit aktuellem Zertifikat. Es weist zudem darauf hin, dass Updates ausschliesslich über die Updatefunktion der Software oder die Supportseite des Herstellers bezogen werden sollten. Zudem sollten die Mitarbeitenden sensibilisiert und Passwörter erneuert werden.

Nachzulesen unter:

https://www.heise.de/news/Fernwartungssoftware-Anydesk-kaempft-mit-Stoerungen-9614705.html
https://thehackernews.com/2024/02/anydesk-hacked-popular-remote-desktop.html
https://www.cybersecuritydive.com/news/anydesk-attack-credential-reset/706554/

https://AnyDesk.com/en/public-statement-2-2-2024
https://www.bleepingcomputer.com/news/security/anydesk-says-hackers-breached-its-production-servers-reset-passwords/#google_vignette
https://www.heise.de/news/IT-Sicherheitsvorfall-Anydesk-bestaetigt-Einbruch-in-Produktionssysteme-9617356.html
https://www.heise.de/news/Kundendaten-von-Anydesk-zum-Verkauf-angeboten-9617991.html
https://anydesk.com/en/public-statement
https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2024/2024-213655-1032.pdf?__blob=publicationFile&v=2

III. Alle Bienen ausgeflogen – US State Department lobt trotz beachtlicher Erfolge millionenschwere Belohnungen für Hinweise auf Cybererpresser aus

Im Jahr 2023 gab es neben Rekordschäden durch Ransomware auch gute Nachrichten zu: Den Sicherheitsbehörden war es in Zusammenarbeit gelungen, Infrastrukturen der berüchtigten Cybererpresser-Organisation HIVE (Bienenstock) zu übernehmen. Kurz darauf waren auch die Webseiten der mit HIVE konkurrierenden ALPHV/Blackcat-Kriminellen im Darknet nicht mehr auffindbar. Dort lieferten sich verschiedene Ransomware-Anbieter und Cybererpresser Abwerbeschlachten um vermeintlich ehemalige Mitarbeitende und Affiliates von HIVE und ALPHV. Anfang Februar 2024 gab EUROPOL bekannt, dass es in internationaler Zusammenarbeit gelungen sei, das grösste und aktivste Netzwerk für Ransomware as a Service zu übernehmen: LockBit. Es bleibt abzuwarten, wie lange und wie nachhaltig diese Erfolge sein werden. Denn zum einen sind z.B. die ALPHV/Blackcat-Seiten inzwischen wieder online. Und zum anderen fehlt offenbar von den Hintermännern (und sicher auch -frauen) von HIVE jede Spur.

Doch auch hier gibt es Hoffnung: Denn bei der hohen Taktung, mit denen diese Gruppen unterwegs waren/sind, ist jede Woche ohne Aktivität ein Gewinn. So gab die US-Bundespolizei FBI im November 2022 bekannt, dass die HIVE-Kriminellen zwischen Juli 2021 und Oktober 2022 über 100 Millionen Dollar Lösegeld von mehr als 130'000 Unternehmen erpresst hätten.

Und inzwischen hat das US State Department nun einen Köder für die ausgeflogenen Bienchen aus dem HIVE-Stock ausgesetzt, der alle Kriminellen zu ihrem schändlichen Treiben motiviert: Geld, viel Geld sogar. Jetzt lobt die US-Regierung bis zu 10 Millionen Dollar Belohnung für Hinweise aus, die zu den Kriminellen hinter dem HIVE-Netzwerk führen. Und zwar nicht nur für Bürgerinnen und Bürger der Vereinigten Staaten, sondern weltweit. Diese können die Hinweise in allen US-Konsulaten oder -Botschaften abgeben.

Die pikante Ironie an HIVE: Unter genau demselben Namen HIVE lancierte der ebenfalls US-amerikanische Geheimdienst CIA eine Suite von Schadprogrammen, die es staatlichen Agenten ermöglicht, Daten von überwachten Devices abzugreifen oder neue Befehle an diese zu senden. Darüber berichtete u.a. securityaffairs.com im Januar 2023. Es bleibt also zu hoffen, dass es sich bei Auslobung oder gar Auszahlung des millionenschweren Lösegeldes nicht bloss um einen buchhalterischen Trick zur Verschiebung von Budgetposten handelt, sondern dass es der US-

Regierung ernst damit ist, den immer stickiger werdenden Sumpf der Cybererpressung trocken zu legen.

Dass dem so ist, lässt sich daraus schliessen, dass das US State Department am 15. Februar 2024 ein Belohnungspaket in Höhe von 15 Millionen Dollar für die Lokalisierung oder Identifizierung der Führung von ALPHV/Blackcat und deren Partner ausgesetzt hat. Es wäre der Jackpot für die Behörden, für die oder den Hinweisgebenden und letztlich uns alle.

Nachzulesen unter:

https://www.heise.de/news/AlphV-meldet-sich-zurueck-Verhaftungen-und-Betrug-bei-anderen-Gruppen-9574446.html
https://www.bleepingcomputer.com/news/security/lockbit-ransomware-disrupted-by-global-police-operation/#google_vignette
https://www.heise.de/news/Operation-Cronos-Internationalen-Behoerden-gelingt-Schlag-gegen-Lockbit-9632833.html
https://www.heise.de/news/Ransomware-Lockbit-durch-Ermittler-zerschlagen-zwei-Festnahmen-9633327.html
https://www.bleepingcomputer.com/news/security/fbi-hive-ransomware-extorted-100m-from-over-1-300-victims
https://gbhackers.com/hive-ransomware-10-million-reward
https://www.heise.de/news/Hive-10-Millionen-US-Dollar-Belohnung-fuer-Hinweise-zur-Ransomware-Gruppe-9623257.html
https://securityaffairs.com/140878/malware/cia-hive-malware-detected.html
https://www.state.gov/reward-for-information-alphv-blackcat-ransomware-as-a-service
https://www.heise.de/news/ALPHV-15-Millionen-US-Dollar-fuer-Tipps-zur-Ergreifung-der-Ransomware-Gruppe-9630351.html

IV. Von Smallville zu SkyNet – Künstliche Intelligenzen setzen Atomwaffen ein, um Frieden zu stiften

Fast 40 Jahre liegen zwischen Smallville und SkyNet – und der Unterschied zwischen friedlichem Zusammenleben und dem Untergang der Menschheit. Während die auf ChatGPT basierende Simulation Smallville 2023 von Forschenden der Standford University und Google einem Dorf mit 25 Einwohnern ein eher friedliches Dasein beschert, bringt – «Terminator»-Fans wissen es – die Weiterentwicklung der künstlichen Intelligenz SkyNet der Menschheit Tod und Verderben im schier aussichtslosen Kampf gegen die von derselben KI entwickelten Kriegsmaschinen und Roboter. Nun haben Forschende des Georgia Institute of Technology, der Stanford University, der Northeastern University und der Hoover Wargaming and Crisis Simulation Initiative simuliert, welche Entwicklung die Menschheit zu erwarten hätte, wenn die fünf technisch führenden grossen Sprachmodelle militärische und diplomatische Entscheidungen treffen würden. Spoiler: Smallville ist es nicht. In verschiedenen Krisenszenarien, in denen die Forschenden acht so genannte Nations Agents mit unterschiedlichen Zielen gegeneinander antreten liessen, zeigten alle Modelle «schwer vorhersehbare Eskalationsmuster», bis hin zum Einsatz von Atomwaffen.

Dass künstliche Intelligenzen bereits heute sowohl in Cyber- als auch in physischen Kriegen eingesetzt werden, ist längst keine Simulation mehr, sondern bittere Realität. So auch im von Russland angezettelten Ukraine-Krieg, in dem die NATO-Staaten KI-gesteuerte Drohnenschwärme in die Ukraine liefern wollen. OpenAI und Microsoft haben unterdessen Benutzerkonten für ihre künstlichen Intelligenzen geschlossen, die sogenannten staatlichen

Bedrohungsakteuren zugeschrieben werden. So sollen nach Angaben der beiden Unternehmen die dem chinesischen Staat zugeschriebenen Gruppen «Charcoal Typhoon» und «Salmon Typhoon» OpenAI-Dienste dazu genutzt haben, um Informationen über Cybersecurity Tools, fehlerfreie Codierung, die Erstellung von Phishing-Kampagnen und mehr zu erhalten. Die mit Russland in Verbindung gebrachte Gruppe «Forest Blizzard» habe es auf Satellitenkommunikation und Radartechnik abgesehen. Die Nordkorea zugerechnete Gruppe «Emerald Street» habe versucht, Fachleute und Organisationen zu identifizieren, die sich mit Verteidigungsfragen im asiatisch-pazifischen Raum beschäftigten. Die im Iran vermutete Gruppe «Crimson Sandstorm» habe sich mit Malware-Erkennung und der Erstellung von Inhalten sowie mit der Web- und App-Entwicklung für Spear-Phishing-Kampagnen beschäftigt.

In einer ersten Reaktion haben Microsoft und OpenAI Grundsätze zum Umgang mit KI-Risiken dieser Art verabschiedet. Gleichzeitig haben Forschende der Universitäten Cambridge, Harvard und Toronto sowie von OpenAI jüngst gefordert, die eingangs erwähnten Risiken durch verschiedene Massnahmen zu begrenzen – vom Exportverbot von Hochleistung-Chips und andere für KI-Anwendungen notwendige Hard- und Software bis hin zu realen und virtuellen Notausschaltern. Gleichzeitig weisen sie aber auch auf neue Gefahren hin, die durch den Einbau solcher Kill Switches entstehen. So könnten u.a. Cyberkriminelle durch die Ansteuerung und Nutzung solcher Kill Switches KI zu einem ungünstigen Zeitpunkt ausschalten oder «umdrehen». Alles in allem zeigt sich, dass die Diskussion über Chancen und Risiken, erst recht aber eine wie auch immer geartete funktionierende Regulierung von KI derzeit weit hinter dem Entwicklungstempo der KI selbst hinterherhinkt. Die Terminators dieser Welt wird's freuen.

Nachzulesen unter:

https://www.br.de/nachrichten/netzwelt/smallville-ein-dorf-mit-25-ki-bewohnern-auf-basis-von-chatgpt,TbVH5PS
https://www.heise.de/news/Fuer-den-Frieden-KI-setzt-in-Kriegssimulation-Atomwaffen-ein-9628928.html
https://www.heise.de/news/Ukraine-Krieg-NATO-Staaten-wollen-wohl-tausende-Drohnen-mit-KI-Technik-liefern-9631963.html
https://www.heise.de/news/KI-OpenAI-und-Microsoft-schliessen-Konten-staatlicher-Bedrohungsakteure-9631899.html
https://www.heise.de/news/Gegen-die-Apokalypse-Wissenschaftler-fordern-Kill-Switch-fuer-KI-9631689.html

V. Grosse Schäden auch ohne KI – NoName057(16) greift weiterhin und unverändert massiv Ziele in Europa an

Dass es keine KI braucht, um Infrastruktureinrichtungen oder Unternehmen andersdenkender Staaten auszuschalten, beweist die prorussische Hackergruppe NoName057/16. Ihr werden seit März 2022 über 1'500 (in Worten: eintausendfünfhundert!) DDos-Attacken auf aus Sicht der Angreifer antirussisch handelnde Ziele zugeschrieben. Viele davon auch in der Schweiz, worüber wir bereits in der Ausgabe von Mai/Juni 2023 dieses Reports berichteten. Die dort als «Wagner-Söldner des Internets» bezeichnete Gruppe hat inzwischen ihre eigene Malware namens DDoSia weiterentwickelt, die statt in Python jetzt in Golang codiert ist. Auch der ungewöhnliche Ansatz,

alle Aktivitäten über den russischen Messenger Telegram anzukündigen, wurde inzwischen so weiterentwickelt, dass der Recruiting- und Onboarding-Prozess für neue Hacktivisten überaus niedrigschwellig über Telegram abläuft. Fast schon zynisch ist der Gamification-Ansatz, bei dem Angreifer DDoSia für Attacken gegen Ziele im Westen einsetzen und Punkte sammeln können. Dafür hat die Gruppe sogar eine eigene Kryptowährung entwickelt. Und die Bemühungen tragen Früchte. So berichtet der Cybersecurity-Anbieter Netscout, dass die Zahl der beteiligten BotNet-Server innerhalb nur eines Jahres von ursprünglich 400 auf knapp unter 10'000 angewachsen sei.

Waren zu Beginn des Ukraine-Krieges neben der Ukraine vor allem die baltischen Staaten massiven DDoSia-Angriffen ausgesetzt, so sind aktuell Tschechien, Polen und Spanien die Hauptangriffsziele, auch wenn die Ukraine, die USA, Kanada oder andere westliche Staaten immer wieder DDoSia-Attacken erdulden müssen. In allen Ländern treffen die NoName057(16)-Angriffswellen vor allem die öffentliche Verwaltung, den Transport- und Logistik-Sektor sowie das Finanz- und Bankenwesen. Damit ist auch die Schweiz wieder ins Visier der Cyberkriminellen geraten. Und es ist zu befürchten, dass die Angriffe nach der Verhängung neuer Sanktionen gegen die russischen Kriegstreiber zunehmen werden.

Nachzulesen unter:

https://www.netscout.com/blog/asert/noname057-16
https://de.wikipedia.org/wiki/NoName057(16)
https://thecyberexpress.com/noname-ransomware-attack-on-ukraine
https://securityaffairs.com/151149/hacking/noname-ddos-attack-canadian-airports.html
https://www.inside-it.ch/ddos-angreifer-noname-gehen-wieder-auf-die-schweiz-los-20230908

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