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

Juli/August 2023

I. Nachtschwarze Wolke statt azurblauer Himmel? Der Microsoft Azure-Masterkey-Diebstahl

Ist es ein Desaster oder ein «einfacher» Hack? Mitte Juni hatte eine US-Behörde Microsoft über verdächtige Zugriffe auf E-Mails in ihren MS Exchange-Konten informiert. Die Analyse ergab, dass ein Signaturschlüssel zu Microsofts Clouddiensten gestohlen worden war und von den Hackern dazu genutzt wurde, sich Zugang vornehmlich zu europäischen und US-Behörden zu verschaffen.

Microsoft erklärte zunächst, dass chinesische Cyberkriminelle einen inaktiven MSA-Schlüssel erbeutet hätten, dessen Signaturen eigentlich nur für Privatkunden und -kunden vorgesehen seien. «Validation Issues» hätten aber dazu geführt, dass mit dem Schlüssel erstellte Signaturen auch von Azures Active Directories für die Business-Kundschaft anerkannt worden seien.

Bereits Ende Juli berichtete das Security-Unternehmen WiZ, dass der gestohlene Schlüssel keineswegs eher unbedeutend sei. Vielmehr handele es sich um einen OpenID Signing Key für das Azure Active Directory. In Konsequenz bedeute das, dass nahezu alle Nutzende von

Microsofts Clouddiensten der Gefahr ausgesetzt sind, dass die Cyberkriminellen sich via Outlook, Sharepoint, Office 365, Teams, OneDrive oder anderer Anwendungen, die ein «SignIn with Microsoft» anbieten, Zugang zu ihren Netzwerken, Devices oder Daten verschaffen könnten. Microsoft hat den kompromittierten Schlüssel zwar gesperrt, doch hätten die Cyberkriminellen genug Zeit gehabt, mit seiner Hilfe praktisch in der gesamten Microsoft Cloud Hintertüren einzurichten.

Darüber, dass sie das inzwischen bereits getan haben, berichtete dann Bruce Schneier in seinem Blog «Schneier on Security» am 7. August. Opfer der Attacken waren u.a. mehrere Netzwerke amerikanischer Regierungsbehörden. In einem Vergleich zu früheren SolarWinds-Attacken russischer Cyberkrimineller verweist er darauf, dass mit diesen mehr als 14'000 Netzwerke weltweit angegriffen worden waren. Und er führt weiter aus, dass deren Betreiber diese zwar gepatcht hätten, die Cyberkriminellen aber zwischenzeitlich Backdoors installiert hätten und kaum wieder aus den Netzwerken herauszubekommen wären. Seine Beobachtung, dass sich Cyberkriminelle weltweit darauf fokussierten, statt der gut geschützten Organisationen selbst deren Infrastruktur-Anbieter zu attackieren, haben sich im Fall des Schweizer Xplain-Hacks bestätigt. Und auch der Azure-Masterkey-Diebstahl zeigt das gleiche Muster.

Als Reaktion auf die Unzufriedenheit von Kunden mit der Behandlung des Falls durch Microsoft liess man nach einigen Tagen verlauten, dass man das Login für Clouddienste geschärft und verbessert habe und im September mit dem Rollout der Updates beginnen werde. In einem Beitrag im – ironischerweise zum Microsoft-Konzern gehörenden – Social Network LinkedIn beklagt denn auch Amit Yoran, CEO und Chairman des Cybersecurity-Unternehmens Tenable, die Intransparenz, mit der Microsoft die Glaubwürdigkeit von Cloudservices insgesamt aufs Spiel setze.

Am 4. August informierte heise.de dann darüber, dass Microsoft ein Playbook veröffentlicht habe, mit dessen Hilfe Azure-Nutzer erkennen könnten, ob ihre Organisation vom Azure-GAU betroffen ist, ob Hintertüren installiert worden sind und ob es kompromittierte Zugänge im Netzwerk gibt. Das «Token Theft Playbook» ist in englischer und deutscher Version als Playbook für Datendiebstahl erhältlich und via untenstehendem Link zum Download abrufbar.

Nachzulesen unter:

https://www.heise.de/news/Gestohlener-Cloud-Master-Key-Microsoft-schweigt-so-fragen-Sie-selber-9229395.html
https://www.schneier.com/blog/archives/2023/08/microsoft-signing-key-stolen-by-chinese.html
https://www.heise.de/news/Neue-Erkenntnisse-Microsofts-Cloud-Luecken-viel-groesser-als-angenommen-9224640.html
https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access
https://www.microsoft.com/en-us/security/blog/2023/07/19/expanding-cloud-logging-to-give-customers-deeper-security-visibility
https://www.linkedin.com/pulse/microsoftthe-truth-even-worse-than-you-think-amit-yoran
https://www.heise.de/news/Nach-dem-geklauten-Master-Key-fuer-Azure-Hilfestellung-von-Microsoft-9234954.html
https://learn.microsoft.com/en-us/security/operations/token-theft-playbook
https://learn.microsoft.com/de-de/security/operations/token-theft-playbook

II. Microsoft im Schneesturm: Russische Staats-Hackinggruppe Midnight Blizzard phishen via Teams

Im Gegensatz zum Azure-Desaster handelte Microsoft in einem anderen Fall proaktiv. Am 3. August warnte der Tech-Riese aus Redmond davor, dass eine russische Hackinggruppe versuche, Anmeldedaten von MS Teams-Nutzerinnen und Nutzern abzuphishen. Die unter den Namen ATP29, Nobelium und nun als Midnight Blizzard agierenden Cyberkriminellen werden von US-amerikanischen und britischen Behörden dem russischen Staat zugerechnet und der Spionage bezichtigt.

Die aktuelle Social-Engineering-Angriffswelle ist denn auch deutlich raffinierter als die sattsam bekannten Telefon-Phishing-Versuche, in denen sich Cyberkriminelle als Microsoft-Support ausgeben: Sie konzentrieren sich nämlich auf kleine und kleinere Unternehmen, die sie bereits in früheren Angriffen kompromittiert haben. Sie benennen eine dort beschäftigte Person um, fügen eine neue onmicrosoft.com-Subdomäne hinzu und senden unter der neuen Domain eine ausgehende Nachricht via Teams an Ziel-Nutzende in globalen Organisationen. Bei diesen geben sie sich als Microsoft Support aus und versuchen in Chats, das Opfer zur Herausgabe der Multi-Faktor-Authentifizierungsdaten zu bewegen.

Gemäss Angaben von Microsoft sollen bislang 40 Regierungsorganisationen, NGOs, aber auch Unternehmen aus den Bereichen diskrete Fertigung, IT, Medien oder Technologie Opfer solcher Angriffe geworden sein. Microsoft rät daher, das Bewusstsein der Nutzenden für Sicherheitsfragen wieder und wieder zu schärfen und Authentifizierungsanfragen, die nicht direkt von Benutzerinnen und Benutzern initiiert wurden, als bösartig zu behandeln.

Nachzulesen unter:

https://www.microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams
https://www.bleepingcomputer.com/news/security/russian-hackers-target-govt-orgs-in-microsoft-teams-phishing-attacks
https://www.heise.de/news/Midnight-Blizzard-Microsoft-warnt-vor-Hackern-die-Anmeldedaten-erbeuten-wollen-9233919.html
https://securityaffairs.com/149103/apt/apt29-microsoft-teams-phishing-attacks.html

III. LinkedIn: Zwei-Faktor-Authentifizierung aktivieren, bevor es Cyberkriminelle tun

Mitte August machte das Cybersecurity-Unternehmen Cyberint in einem Blogpost darauf aufmerksam, dass die Angriffe auf Accounts im Business-Netzwerk LinkedIn massiv zugenommen hätten. Cyberkriminelle würden versuchen, sich mit Brute-Force-Angriffen die Zugangsdaten der Mitglieder zu verschaffen oder das Konto schlichtweg zu löschen. Es ist daher ratsam, das Passwort zu erneuern und die Zwei-Faktor-Authentifizierung einzuschalten – auch wenn dies potenziell dazu führen kann, dass LinkedIn das Konto bei erkannten Angriffsversuchen temporär sperrt. In diesem Fall erhalten Betroffene danach von LinkedIn die

Aufforderung, das Konto zu verifizieren und ein neues Passwort anzulegen. Danach ist das Konto wieder freigegeben.

Sinnvoll sind beide Massnahmen allein deshalb, weil nach einem Cyberangriff auf LinkedIn vor zwei Jahren 700 Millionen Nutzerdaten im Darknet zum Verkauf angeboten waren. Die nutzen Cyberkriminellen nun offenbar auch, um sich in ungeschützte Konten einzuloggen, dann dort das Passwort zu ändern und die Zwei-Faktor-Authentifizierung zu aktivieren und so die echten User auszusperren.

In einem (unten verlinkten) Beitrag auf der LinkedIn-Hilfeseite hat das Unternehmen alle Antworten und To-dos zusammengestellt. Und zwar sowohl für den Fall, dass Mitglieder ihr Konto zwar noch öffnen können, aber einen Missbrauch vermuten, wie auch für den, dass ihnen der Zugang zum eigenen Konto trotz valider Login-Daten nicht mehr gelingt.

Nachzulesen unter:

https://cyberint.com/blog/research/linkedin-accounts-under-attack-how-to-protect-yourself
https://www.golem.de/news/jetzt-2fa-aktivieren-hackerangriffe-auf-linkedin-konten-nehmen-massiv-zu-2308-176794.html
https://www.businessinsider.de/wirtschaft/verbraucher/cyber-angriff-auf-linkedin-fast-jeder-nutzer-ist-betroffen/
https://www.linkedin.com/help/linkedin/answer/a1340402

IV. Darf sich KI ins Meeting ein-zoomen?

Die Corona-Pandemie hat Zoom nach eigenen Angaben zum Marktführer bei Stand-Alone-Videokonferenz-Software gemacht – waren 2019 noch «nur» 10 Millionen monatliche Nutzende aktiv, schnellte diese Zahl auf 200 Millionen im März 2020 hoch. Ähnlich sprunghaft stiegen auch Börsenwert und Gewinn des 2011 in San José gegründeten Unternehmens. Im März veränderte der Anbieter dann seine Allgemeinen Geschäftsbedingungen, um Daten aus den aufgezeichneten Konferenzen zu Trainingszwecken aufzuzeichnen. Trainieren wollte Zoom damit aber nicht eigene Mitarbeitende, sondern Künstliche Intelligenzen.

Seitdem hat Zoom laut Angaben des Chaos Computer Clubs Zürich Stimmmaterial, Bilder, Chat-Inhalte und Präsentationsmaterial dazu gespeichert, KI zu trainieren, ohne die Nutzerinnen und Nutzer darüber zu informieren, geschweige denn, deren Einverständnis einzuholen. Publik wurde dieser durch die neuen AGB abgesicherte Datengebrauch erst durch eine Veröffentlichung von stackdiary.com am 6. August. Die darauffolgende Protestwelle breitete sich viral aus und drückte nicht nur den Börsenkurs des Unternehmens spürbar nach unten, sondern brachte bereits am nächsten Tag eine erste Änderung der Zoom-AGBs mit sich, in dem der Videokonferenzdienst versprach, Daten nur noch mit Zustimmung der Userinnen und User zu nutzen.

Tatsächlich aber lief die Welle weiter, so dass sich Zoom-Gründer und -CEO Eric Yuan dazu gezwungen sah, nach einer Vollbremsung um 180 Grad zu wenden und am 11. August nochmals veränderte AGBs zu veröffentlichen, in denen Zoom jede Verwendung von Konferenzdaten zum Training eigener wie fremder KI ausschliesst: “Zoom does not use any of your audio, video, chat, screen sharing, attachments or other communications-like Customer Content (such as poll results, whiteboard and reactions) to train Zoom or third-party artificial intelligence models."

Nachzulesen unter:

https://www.beobachter.ch/digital/zoom-verwendet-nutzerdaten-fur-ki-trainings-628402
https://march24.ch/articles/202564-zoom-nutzt-userdaten-zum-training-von-ki
https://www.inside-it.ch/zoom-will-userdaten-fuers-ki-training-nutzen-20230808
https://stackdiary.com/zoom-terms-now-allow-training-ai-on-user-content-with-no-opt-out
https://www.zeit.de/digital/datenschutz/2023-08/datenschutz-videokonferenz-zoom-nutzerdaten-kuenstliche-intelligenz-ki-training
https://www.handelszeitung.ch/newsticker/zoom-datennutzung-zum-ki-training-nur-mit-zustimmung-der-nutzer-626368
https://www.finanzen.ch/nachrichten/aktien/nach-heftiger-empoerung-zoom-rudert-bei-datennutzung-fuer-ki-training-zurueck-1032571838

In eigener Sache: Weiterentwicklung des SWITCH Security Reports

Es freut uns sehr, dass Sie zum Empfangskreis des Security Reports gehören. Mit Ihrer Meinung entscheiden Sie mit, in welche Richtung wir dieses Informationsprodukt weiterentwickeln. Bitte nehmen Sie sich dazu 1 Minute Zeit und beantworten Sie vier Fragen.

Mit diesem Link gelangen Sie direkt zur Umfrage.

Vielen Dank für Ihre Teilnahme.

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