mimecast

Global Threat Intelligence Report

Januar - Juni

Einleitung

Um den neuesten Cyberbedrohungen zu begegnen, müssen große und kleine Unternehmen zuverlässige Bedrohungsinformationen nutzen, ihre Cybersicherheitsprozesse und -infrastrukturen schnell aktualisieren und ihre Kommunikation, Mitarbeiter und Daten besser schützen.

Mimecast generiert Bedrohungsinformationen durch die Analyse von mehr als 1,7 Milliarden Nachrichten pro Tag für mehr als 42.000 Kunden. Da E-Mail und Messaging die am häufigsten genutzten Kanäle für Cyber-Bedrohungen sind, ist Mimecast in der Lage, Bedrohungen zu erkennen und zu analysieren, bevor sie sich ausbreiten.

In diesem Global Threat Intelligence Report fasst Mimecast die Ergebnisse unserer Bedrohungsanalysen für das 1. Halbjahr 2024 zusammen und kombiniert unsere Daten mit Open-Source-Informationen aus der gesamten Cybersicherheits-Community.

Der Bericht enthält eine Analyse der Bedrohungsaktivitäten, Statistiken zu Angriffstrends und eine Reihe von Empfehlungen für Unternehmen jeder Größe, um die Risiken von Cyberbedrohungen effektiver zu mindern.

Wir laden Sie ein, den Mimecast Threat Intelligence Report für das 1. Halbjahr 2024 zu entdecken und freuen uns darauf, Ihnen in Zukunft weitere Erkenntnisse zur Verfügung zu stellen.

1.7 Milliarden Nachrichten

42,000 Kunden

Zusammenfassung

Im ersten Halbjahr 2024 wurde das französische Sprichwort „Plus ça change, plus c'est la même chose" bestätigt - je mehr sich die Dinge ändern, desto mehr bleiben sie gleich.

Der Einsatz von KI-Technologie sowohl durch Angreifer als auch durch Verteidiger verspricht weiterhin massive Veränderungen in der Cybersicherheit, doch bisher sind die Auswirkungen auf beiden Seiten begrenzt. Der Kampf um die Vorherrschaft im Cyberspace bleibt unerbittlich, da Cyberkriminelle Cloud-Dienste und As-a-Service-Angebote nutzen, um die Verfügbarkeit von Angriffstools, Phishing-Kits und Datenbanken mit gestohlenen Informationen weiter zu erhöhen. Die Strafverfolgungsbehörden scheinen sich an die veränderten Bedingungen anzupassen, wobei die grenzüberschreitende Zusammenarbeit zur Zerschlagung großer Gruppen führte.

E-Mail-Angriffe entwickeln sich weiter, da Angreifer immer seltener auf Malware setzen und stattdessen bösartige Links zu legitimen Cloud-Filesharing-Diensten wie SharePoint und Google Drive verwenden.

Der vorübergehende Anstieg der Angriffe auf mittelständische Unternehmen hat nachgelassen, und kleine Unternehmen sind wieder am stärksten gefährdet. Der Diebstahl von Zugangsdaten ist zu einer zentralen Strategie der Angreifer geworden. Sie verkaufen gestohlene Zugangsdaten auf Schwarzmärkten oder nutzen sie für Credential Stuffing-Angriffe, um sich Zugang zu Cloud-Diensten von Unternehmen zu verschaffen.

Die Zukunft hält jedoch einige absehbare Herausforderungen bereit.

Angesichts der zunehmenden Migration von Unternehmen in die Cloud und des fortschreitenden Ausbaus der Infrastruktur hat sich die Angriffsfläche insgesamt vergrößert. Die zunehmende Abhängigkeit von in der Cloud gespeicherten Daten bedeutet, dass die Sicherheitskontrollen immer unklarer werden, während die Abhängigkeit von Software und Infrastruktur von Drittanbietern die Sicherheit der Lieferkette zu einem großen Problem macht. Angesichts der anhaltenden Ransomware-Angriffe ist die Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Daten - der CIA-Triade - entscheidend für den Geschäftserfolg, da Angriffe auf Daten zu Dienstunterbrechungen und schwerwiegenden Auswirkungen auf den Geschäftsbetrieb führen können. Schließlich werden generative KI und maschinelles Lernen die Zielgenauigkeit und den Inhalt von Phishing-Kampagnen verbessern und damit die Anforderungen an die Verteidiger erhöhen, neue und neuartige Angriffstechniken zu erkennen und schnell darauf zu reagieren.

1 Wichtigste Erkenntnisse

1

E-Mail-Angriffe entwickeln sich weg von Malware hin zur Verwendung von Links, wobei mehrschichtige die Erkennung erschweren. Diese Entwicklung erfordert auch mehr Interaktion von den Opfern, einschließlich des Anklickens von mehr Links und der Beantwortung von CAPTCHAs und gefälschten Anfragen zur Multi-Faktor-Authentifizierung.

2

Die Branchen Banken, Kunst und Unterhaltung sowie Reisen und Gastgewerbe verzeichneten im zweiten Quartal 2024 die meisten bösartigen URL-Nachrichten. Gleichzeitig erhielten IT-Berater und Rechtsexperten die meisten Spam-und Identitätsdiebstahlmeldungen.

3

Angreifer nutzen Entwicklungsdienste wie Replit zur Durchführung und Entwicklung von Kampagnen. Dienste zur gemeinsamen Nutzung von Dateien, einschließlich SharePoint und Google Drive sind ebenfalls beliebte Möglichkeiten zur Freigabe von Zwischendokumenten, die auf Seiten mit Anmeldedaten verweisen.

4

Identitätsdiebstahl war die häufigste Angriffsart, von der europäische Nutzer betroffen waren, während Spam in Afrika am häufigsten vorkam. Im asiatisch-pazifischen Raum stieg die Zahl der Angriffe auf kleine Unternehmen dramatisch an.

Der Threatcast

In diesem Jahr ist mit einer Zunahme von Spam- und Phishing-Angriffen sowie Desinformationskampagnen zu rechnen, da eine Reihe wichtiger Ereignisse auf der ganzen Welt reichlich Stoff für Phishing-Köder und Motivation für Angreifer bieten. Im Jahr 2024 beginnt eine äußerst wichtige Wahlsaison. Neben wichtigen Abstimmungen in den USA und Europa sowie vorgezogenen Neuwahlen in Frankreich werden insgesamt mehr demokratische Staaten als in den Vorjahren über die Zukunft ihres Landes entscheiden. Die anhaltende russische Invasion in der Ukraine und der Konflikt zwischen Israel und der Hamas im Gazastreifen haben zu einer deutlichen Zunahme von Desinformationsversuchen geführt. Große Sportereignisse - von den Olympischen und Paralympischen Sommerspielen in Paris bis hin zu den jüngsten Fußballturnieren Euro 2024 und COPA America - waren Ziel von Angriffen verschiedener Gruppen.

Sechs schwerwiegende Vorfälle in der ersten Hälfte des Jahres 2024 verdeutlichen die potenziellen Risiken, die sich aus der aktuellen Bedrohungslage ergeben. Die Berichte reichen von opportunistischen Hackern, die mehr Informationen über Cloud-Nutzer sammeln, über die Kompromittierung von Cloud-E-Mail-Systemen bis hin zu Fehlinformationen, die von Minderheitsgruppen verbreitet werden, um bei Wahlen an Boden zu gewinnen.

Wichtige Ereignisse

JAN.

Trello leakt 15 Millionen Nutzerdatensätze

Schwachstelle: Unsichere öffentliche API
Auswirkung: E-Mail-Adressen werden zur Basis künftiger Angriffe

Im Januar entdeckten Threat Intelligence-Analysten mehr als 15 Millionen Datensätze von Trello-Nutzern, die im Dark Web zum Verkauf angeboten wurden. Ein Hacker nutzte API-Aufrufe, um Informationen aus der API mit allzu großzügigen Zugriffsrechten zu sammeln, die es jedem ermöglichten, Benutzerkonten abzufragen und Trello-Boards zu finden, die mit diesen Konten verbunden waren. Der Angreifer erbeutete Benutzernamen, E-Mail-Adressen und vollständige Namen - Daten, die für eine Vielzahl von Messaging-Angriffen verwendet werden können. Atlassian, der Eigentümer von Trello, hat die API geändert, um das Sammeln solcher Informationen in Zukunft zu erschweren.

FEB.

i-SOON-Insider gibt Hacking-Informationen preis[1]

Schwachstelle: Leak durch Insider
Auswirkung: Vertrauliche Informationen über chinesische Hackerangriffe veröffentlicht

Mehr als 570 Dateien mit insgesamt 170 MB an Daten, die die Aktivitäten des chinesischen Sicherheitsunternehmens Shanghai Anxun Information Co., bekannt als „i-SOON", beschreiben, wurden auf die Code-Repository-Plattform Github hochgeladen. Ein Datenleak, das anscheinend von einem verärgerten Mitarbeiter verursacht wurde, enthüllte, dass das Unternehmen im Auftrag der chinesischen Regierung Spionageoperationen gegen mehr als 20 Regierungen in anderen Ländern, darunter die USA und Japan, sowie Südkorea und Gebiete wie Taiwan durchgeführt hatte.

Lockbit-Betrieb durch globale Bemühungen unterbrochen[2]

Schwachstelle: Maßnahmen der Strafverfolgungsbehörden
Auswirkungen: Störung einer großen Cybercrime-Organisation

Die britische National Crime Agency hat gemeinsam mit Ermittlern von zehn Strafverfolgungsbehörden weltweit die Aktivitäten der Ransomware-Gruppe LockBit gestört, indem sie im Rahmen der Operation Cronos die Kontrolle über die Infrastruktur und Server der Gruppe übernommen und rund 11.000 Domains beschlagnahmt hat. Es wird angenommen, dass die LockBit-Gruppe für ein Viertel der Ransomware-Angriffe im vergangenen Jahr verantwortlich war und mehr als 120 Millionen US-Dollar an Lösegeldern erhalten hat. Im Rahmen der Operation der Strafverfolgungsbehörden kam es zu Verhaftungen in Polen, der Ukraine und den USA.

1. Benincasa, Eugenio. „From Vegas to Chengdu: Hacking Contests, Bug Bounties, and China's Offensive Cyber Ecosystem." ETH Zurich. Whitepaper. 10. Jun. 2024. https://css.ethz.ch/en/center/CSS-news/2024/06/from-vegas-to-chengdu-hacking-contests-bug-bounties-and-chinas-offensive-cyber-ecosystem.html. I 2. Burgess, Matt. „A Global Police Operation Just Took Down the Notorious LockBit Ransomware Gang". Wired. 28. Feb. 2024. https://www.wired.com/story/lockbit-ransomware-takedown-website-nca-fbi/.

CISA veröffentlicht Details zum Microsoft-E-Mail-Hack[3]

Schwachstelle: Gestohlener Signaturschlüssel
Auswirkung: Sensible E-Mails von hochrangigen US-Beamten wurden offengelegt.

APR.

In einem im April veröffentlichten Bericht gab die Cybersecurity and Infrastructure Security Agency (CISA) Einzelheiten zu einem Eingriff in die Systeme von Microsoft Exchange Online durch die mit der Volksrepublik China in Verbindung stehende Cyber-Spionagegruppe Storm-0558 bekannt. Mit einem im Jahr 2016 gestohlenen Schlüssel verschafften sich die Angreifer Zugriff auf die E-Mails von mehr als 500 Personen in 22 Organisationen, darunter Beamte des US-Außenministeriums, des US-Handelsministeriums und des US-Repräsentantenhauses. Der Bericht folgt einer Analyse von Microsoft vom Januar 2024 über einen zweiten Hackerangriff auf E-Mails von Microsoft-Führungskräften durch eine mit Russland in Verbindung stehende Gruppe im November 2023.

Unsichere Anmeldeinformationen führen zu Datenleak bei Snowflake[4]

Schwachstelle: Fehlende Multifaktor-Authentifizierung
Auswirkung: Kundendaten aus dem Cloud-Speicher geleakt

MAI.

Mindestens 165 Kunden des Cloud-Datenanbieters Snowflake - in den Medienberichten werden Ticketmaster und die Santander Bank namentlich genannt - mussten erleben, wie ihre Daten an die Öffentlichkeit gelangten, nachdem gestohlene Anmeldeinformationen verwendet wurden, um sich Zugang zu ihren Snowflake-Konten zu verschaffen. Die Konten wurden wahrscheinlich durch Phishing-Angriffe gestohlen und waren entweder nicht mit einer Zwei-Faktor-Authentifizierung ausgestattet oder so konfiguriert, dass der Zugriff mit einem Benutzernamen und einem Passwort als Backup möglich war.

Desinformationsangriffe beeinflussen die EU-Wahlen[5]

Schwachstelle: Weit verbreitete Desinformationsangriffe über E-Mail und soziale Medien
Auswirkung: Zunehmende Polarisierung, mögliche Auswirkungen auf Wahlen

JUN.

Fehlinformationen über die Regierungen der Europäischen Union haben im Mai und Juni stark zugenommen, so das European Digital Media Observatory, eine Gruppe, die sich der Bekämpfung von Desinformation verschrieben hat. Politiker und Verfechter der Demokratie befürchten, dass eine ähnliche Welle von Desinformation durch ausländische Gegner in den USA nicht wirksam bekämpft werden kann, da die Bemühungen der Rechten, Desinformationskampagnen zu stoppen, eine gewisse Wirkung gezeigt haben.[6]

3. CISA. „Cyber Safety Review Board veröffentlicht Bericht zum Microsoft Online Exchange-Vorfall vom Sommer 2023." Beratung des Heimatschutzministeriums. 2. April 2024. https://www.dhs.gov/news/2024/04/02/cyber-safety-review-board-releases-report-microsoft-online-exchange-incident-summer. I 4. „UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion". Google Mandiant Blog. 10. Jun. 2024. https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion. I 5. Tsu, Tiffany. „Convergence of Anger' Drives Disinformation Around E.U. Elections". The New York Times. 7. Jun. 2024. https://www.nytimes.com/2024/06/07/business/media/eu-elections-disinformation.html. I 6. Menn, Joseph. „Stanford's top disinformation research group collapses under pressure". The Washington Post. 14. Jun. 2024. https://www.washingtonpost.com/technology/2024/06/14/stanford-internet-observatory-disinformation-research-lawsuits-politics/.

Die Bedrohungslandschaft des 1. Halbjahrs 2024 in Diagrammen

Spam- und Imitationsangriffe dominierten die Bedrohungslandschaft, wobei bösartige Links weiterhin das bevorzugte Mittel der Angreifer zur Infizierung von Endnutzersystemen waren.

Der Bankensektor, das Reise- und Gastgewerbe sowie der Kunst- und Unterhaltungssektor waren die drei Branchen, die am häufigsten ins Visier der Angreifer gerieten. Personalabteilungen, die lange Zeit im Fokus der Angreifer standen, waren ein weniger beliebtes Ziel. In diesem Bericht werden in allen Diagrammen globale Daten verwendet. Regionale Ansichten für den asiatisch-pazifischen Raum, Kanada, Europa, Subsahara-Afrika und den Nahen Osten, Großbritannien, die USA und die Karibik sind im Mimecast Threat Intelligence Hub verfügbar.

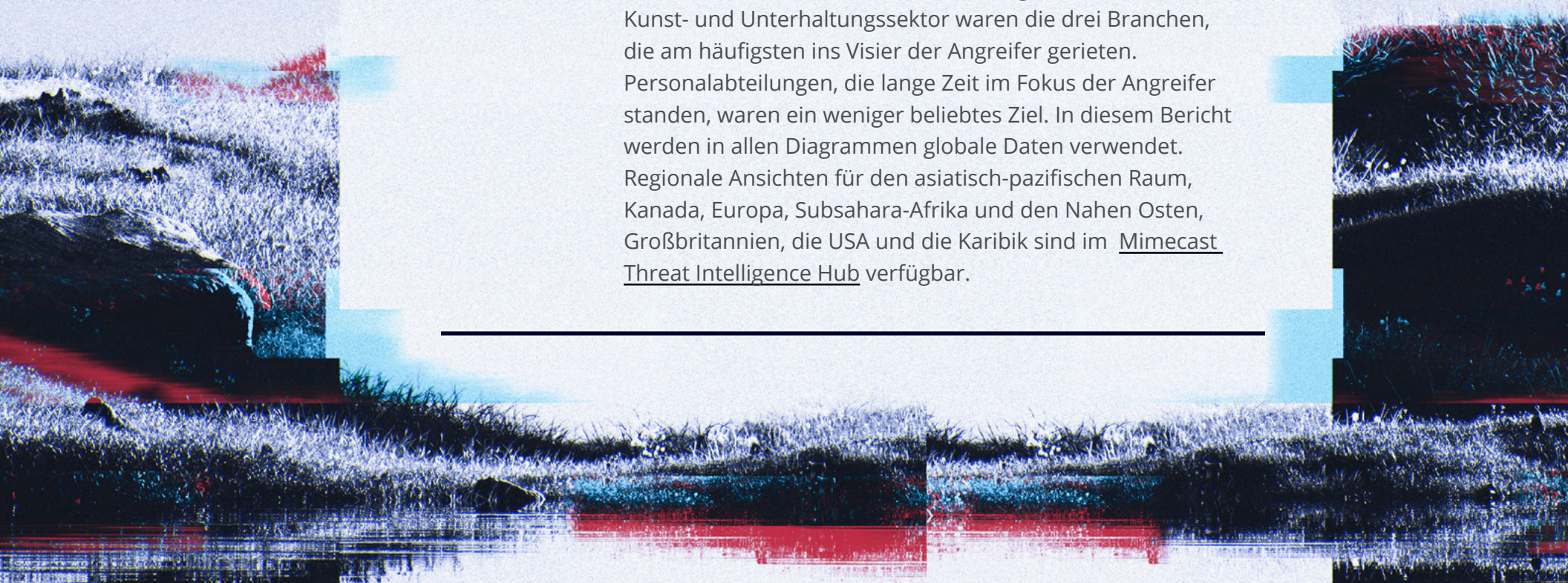
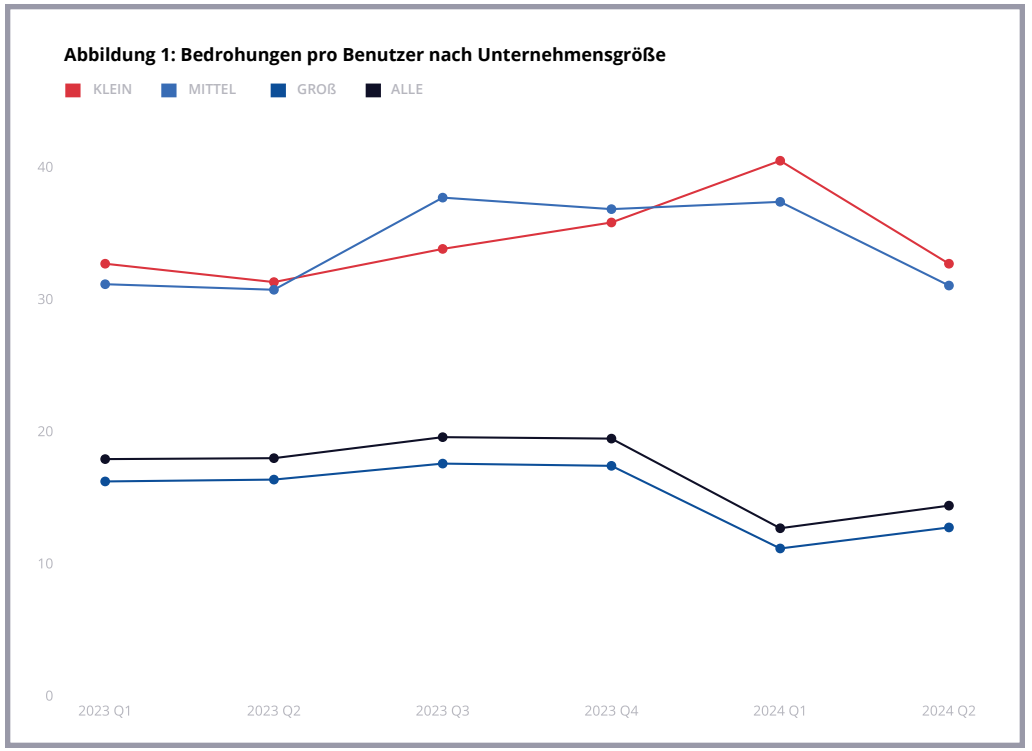


Diagramm 1

TPUs nach Unternehmensgröße

Insgesamt ist die Anzahl der Bedrohungen, die sich gegen Nutzerinnen und Nutzer richten, um rund ein Drittel gesunken, von durchschnittlich 19 TPUs Ende letzten Jahres (Q4 2023) auf 14 TPUs im letzten Quartal (Q2 2024). Auch die Bedrohungen für Großunternehmen gingen im ersten Quartal zurück, stiegen aber im zweiten Quartal dieses Jahres wieder an. Dagegen blieben die TPUs für mittlere Unternehmen im ersten Quartal unverändert, sanken dann aber im zweiten Quartal deutlich auf 31 TPUs.

Nur bei den kleinen Unternehmen war ein deutlicher Anstieg der Angriffe auf 40 TPUs im ersten Quartal zu verzeichnen, der zum Teil auf eine Zunahme der Angriffe in Kanada, Europa und den Vereinigten Staaten zurückzuführen ist. Im 2. Quartal war jedoch ein Rückgang zu verzeichnen. Kleine Unternehmen sind nach wie vor am stärksten von Angriffen bedroht.

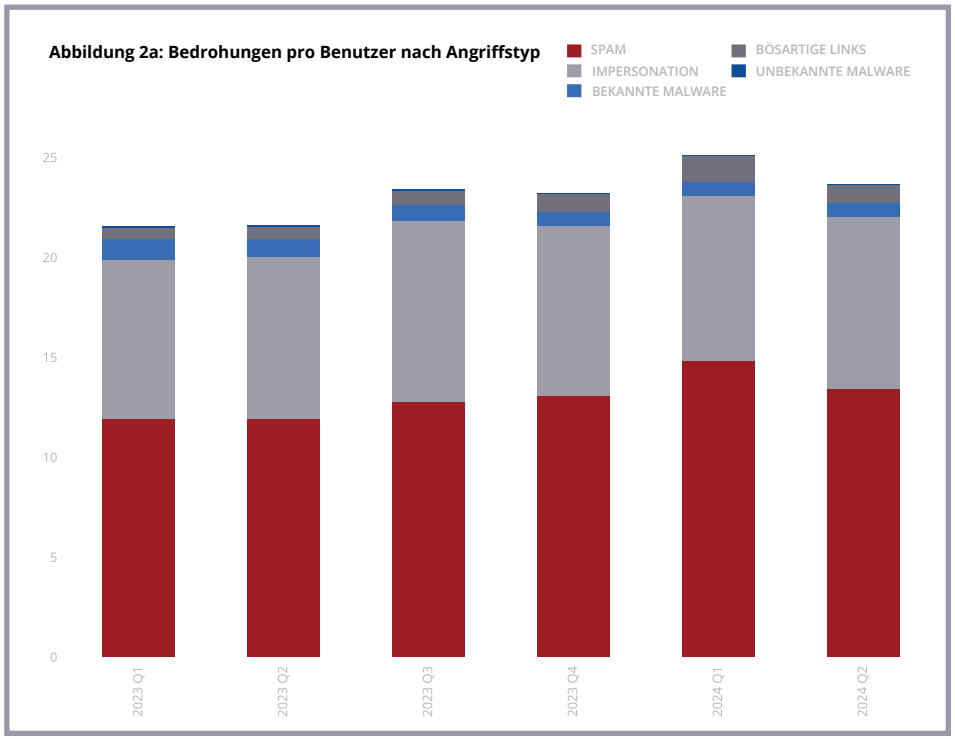


IHRE REGION ANSEHEN

Diagramm 2

Auswirkungen des Angriffstyps auf TPUs

Bei den von Mimecast abgewehrten Angriffen dominierten weiterhin Spam-Attacken und Identitätsdiebstahl. Für den durchschnittlichen Nutzer blockierte die Plattform 13 Spam-Angriffe und neun Identitätsbetrugsversuche. Die Häufigkeit von Spamangriffen stieg im ersten Quartal 2024 sprunghaft an, und zwar um 13 % im Vergleich zum Vorquartal (4. Quartal 2023) und um 24 % im Vergleich zum gleichen Quartal 2023. Obwohl Spam im zweiten Quartal 2024 zurückging, verzeichnete diese Bedrohungskategorie im Vergleich zum Vorjahr einen Anstieg um 12 % Fälschungsangriffe blieben von Quartal zu Quartal relativ konstant und stiegen in den ersten beiden Quartalen 2024 im Vergleich zum Vorjahr nur leicht um 5 % bzw. 6 % an. Angriffe, die weder in die Kategorie Spam noch in die Kategorie Identitätsdiebstahl fallen, zeigen einige interessante Trends (siehe Abbildung 2b). Die Angreifer haben ihre Strategie in Bezug auf E-Mail-Anhänge dahingehend geändert, dass sie bösartige Links als primäre Nutzlast ihrer E-Mail-Angriffe verwenden. Die Anzahl bösartiger Links stieg im ersten Quartal um 133 % - mehr als eine Verdoppelung - und im zweiten Quartal um 53 % im Vergleich zum Vorjahr. Das durchschnittliche Mimecast-Benutzerkonto verzeichnete im zweiten Quartal ein Drittel weniger Links als im ersten Quartal, allerdings ist dieser Rückgang eher auf den massiven Anstieg im ersten Quartal zurückzuführen. Sowohl bekannte Malware (durch Antiviren-Schutzmaßnahmen blockiert) als auch unbekannte Malware (durch Anhangschutz erkannt und blockiert) gingen im Vergleich zum Vorjahr deutlich zurück, und zwar um 36 % bzw. 54 % im ersten bzw. zweiten Quartal.



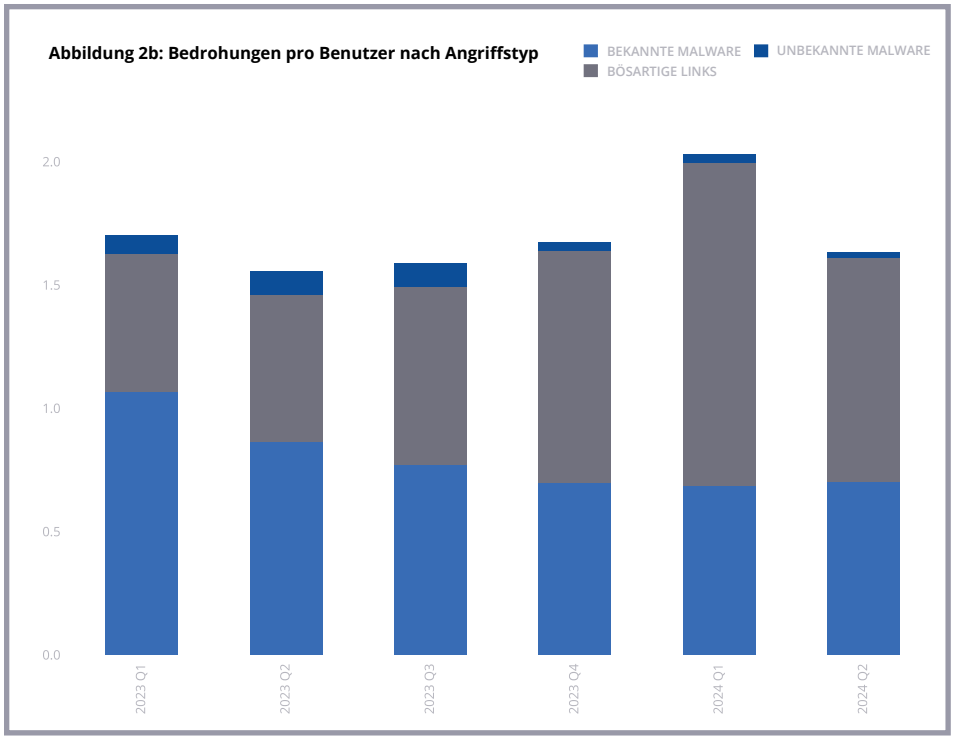


Diagramm 3

Top-Branchen nach TPU

Im ersten Halbjahr 2024 waren der Bankensektor, das Reise- und Gastgewerbe sowie Kunst und Unterhaltung die drei am stärksten betroffenen Branchen. In diesen Branchen wurden durchschnittlich 19, 13 bzw. 9 Angriffe pro Nutzer registriert, wobei Spam und Identitätsdiebstahl, die in der Regel die häufigsten Bedrohungen darstellen, nicht berücksichtigt wurden. Insgesamt waren bösartige URLs am weitesten verbreitet. Sie waren für rund zehnmal mehr Angriffe verantwortlich als bekannte Schadprogramme und für rund 100-mal mehr Angriffe als unbekannte Schadprogramme.

Im 2. Quartal 2024 wurden Nutzer aus den Bereichen IT-Beratung und Rechtsberatung mit einer erheblichen Anzahl von E-Mails mit gefälschten Identitäten konfrontiert, wobei 208 bzw. 56 Nachrichten pro Nutzer durch die Dienste von Mimecast blockiert wurden. Nutzer in den Bereichen Wissenschaft und Technologie, Recht, professionelle Dienstleistungen und IT-Beratung erhielten die meisten Spam-Mails, wobei die Mimecast-Systeme im Durchschnitt mehr als 20 Angriffe pro Nutzer blockierten.

Abbildung 3: Top-5 Branchen nach Bedrohungen pro Benutzer (TPU)

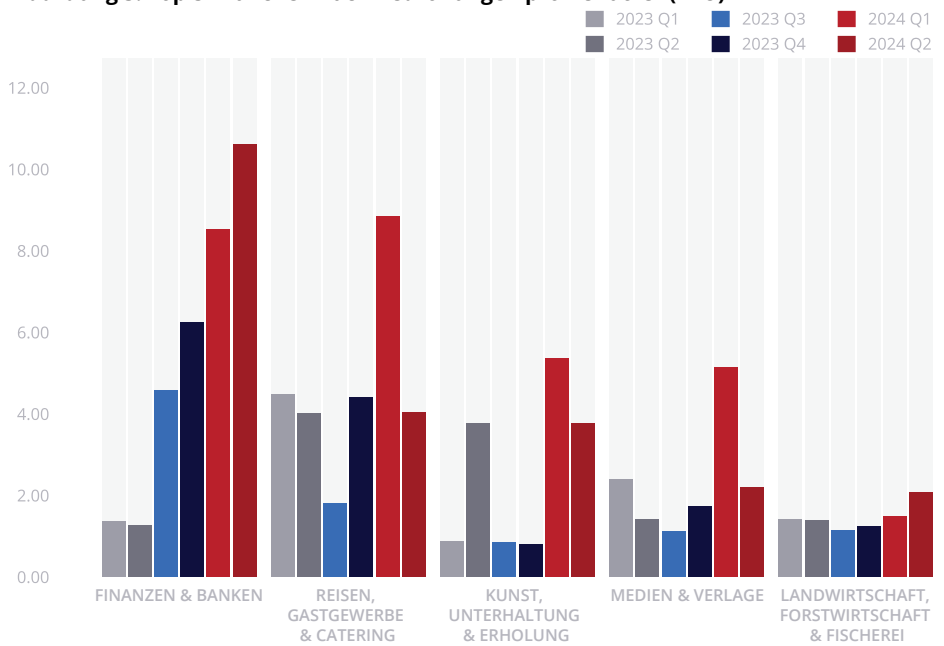


Diagramm 4

Trends zum Missbrauch von Dateifreigaben

Angreifer nutzten weiterhin vermehrt Links, um ihren Opfern Payloads zu übermitteln. Die Domain evernote.com wurde im ersten Halbjahr 2024 am häufigsten missbraucht, ähnlich wie im letzten Quartal des Jahres 2023. Die Nutzung der Google-Domain stieg im ersten Quartal des Jahres sprunghaft an und verdrängte sharepoint.com auf den zweiten Platz.

Wie in Abschnitt 2 - Auswirkungen des Angriffstyps TPU - beschrieben, bevorzugen Bedrohungsakteure zunehmend Links, die ihre Opfer zu Phishing-, Drive-by-Download- und gefälschten Websites führen, um an Anmeldeinformationen zu gelangen. Um ihre Absichten weiter zu verschleiern, nutzen sie zunehmend Filesharing-Sites, die traditionell nicht für das Hosten von Dateien verwendet werden.

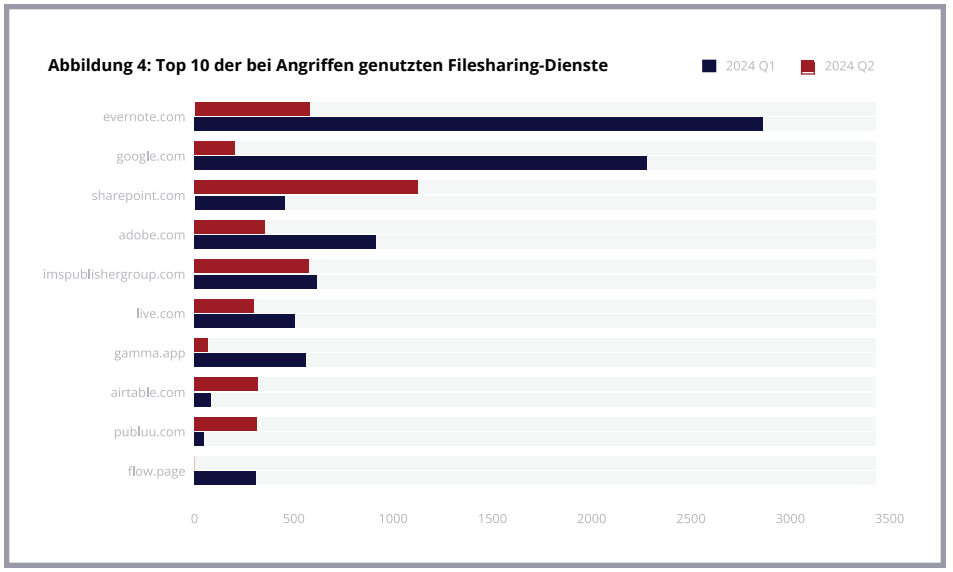
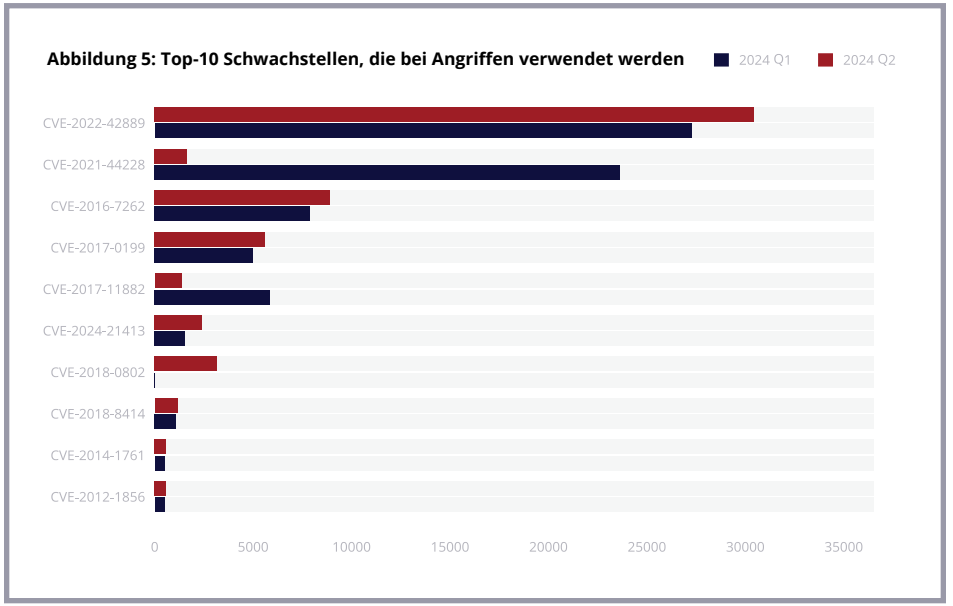


Diagramm 5

Top-Sicherheitslücken im Zeitverlauf

In den ersten sechs Monaten des Jahres 2024 ging der meiste Schadcode von fünf ausgenutzten Schwachstellen aus. Am häufigsten ausgenutzt wurde eine Schwachstelle in der Apache Commons Text Library (CVE-2022-42889), die doppelt so häufig entdeckt wurde wie die zweithäufigste. Die zweithäufigste ausgenutzte Schwachstelle (CVE-2021-44228) ist die berüchtigte Log4J2-Schwachstelle, das absolute Topangriffsziel im ersten Quartal.



Gezielte Angriffskampagnen gegen Mimecast-Benutzer

ZIELGRUPPE Chemie- und Pharmaunternehmen
INHALT Link zu Ransomware

01 BlackMatter Surge

Zwischen dem 23. und 25. April

Eine E-Mail-Kampagne, die sich hauptsächlich an Wissenschaftler und akademische Forscher in der chemischen und pharmazeutischen Industrie richtete, wurde zwischen dem 23. und 25. April an fast 6.000 Mimecast-Kunden versendet. Seit Dezember 2023 liegt die Anzahl aller anderen Einzelfälle von erkannten Ransomware-Signaturen im Bereich von 1.831 oder weniger. Die anomale Spitze von fast einer halben Million Erkennungen wurde durch die BlackMatter Ransomware-as-a-Service (RaaS)-Gruppe verursacht.

BlackMatter wurde jedoch im Jahr 2021 aufgelöst und sein Quellcode anschließend von anderen Gruppen wie LockBit 3.0 und Kasseika verwendet. Angesichts früherer Leaks von Ransomware-Quellcode und seiner Wiederverwendung in anderen Ransomware-Familien gehen die Bedrohungsforscher von Mimecast davon aus, dass Teile des Ransomware-Codes von BlackMatter derzeit aktiv von anderen Gruppen und Partnern verwendet werden.

ZIELGRUPPE unspezifische Zielgruppe **INHALT** Ein verschleierter LinkedIn-Link, der zu bösartigen Inhalten führt

02

Missbrauch von LinkedIn-Weiterleitungen

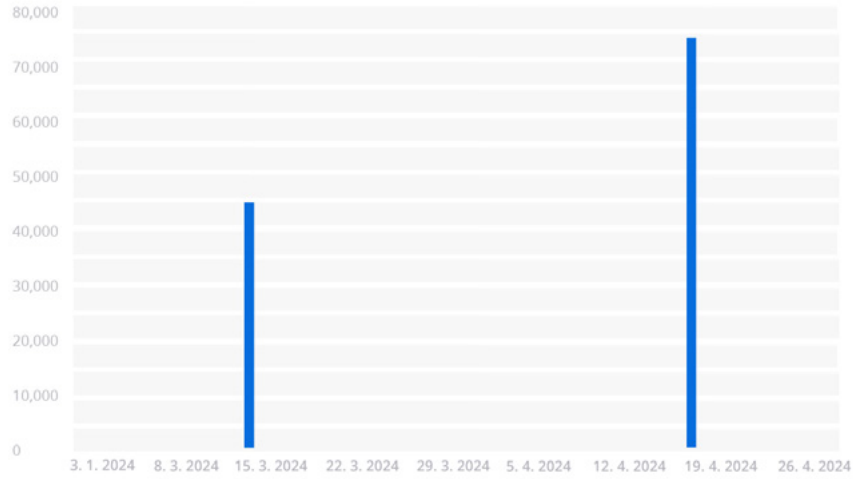
Zwischen März und April

In zwei großen Kampagnen zwischen März und April 2024 wurden E-Mails verwendet, die einen speziellen Link zu einer LinkedIn-Domain enthielten, der das Opfer beim Anklicken zu statischen - aber bösartigen - Inhalten weiterleitete. Bei diesem Angriff handelt es sich nicht um eine herkömmliche offene Weiterleitung, sondern um einen von einem Angreifer erstellten Link, der die Fähigkeit von LinkedIn ausnutzt, auf statische Inhalte zu verlinken.

Mimecast entdeckte mindestens 117.000 E-Mails, die diese Technik verwendeten. Bei beiden Kampagnen erhielten die Empfänger eine Benachrichtigung, dass sie eine Audionachricht erhalten hatten. Ein Klick auf den Link führte jedoch zu einer Weiterleitungskette, die zu einer Cloudflare CAPTCHA-Verifizierungsseite und schließlich zu einer gefälschten Microsoft Outlook Anmeldeseite führte. Die Angreifer nutzten außerdem ein Amazon Simple Email Service (SES)-Konto - ein häufig missbrauchter Dienst, der die Wahrscheinlichkeit erhöht, dass E-Mails E-Mail-Sicherheitsprüfungen wie SPF, DKIM und DMARC bestehen.

KLICKEN SIE HIER, UM ALLE DETAILS DER KAMPAGNE ANZUZEIGEN.

hxxps://www.linkedin[.]com/redir/redirect?url=https%3A%2Flookerstudio%2Egoogle%2Ecom%2Fs%2FscrHqwjeA3k&urlhash=dcQj&trk=public_profile-settings_topcard-website



ZIELGRUPPE Getränke- und Bauindustrie **INHALT** Ein in eine E-Mail eingebetteter Phishing-Link, der zu einer Filesharing-Site führt

03

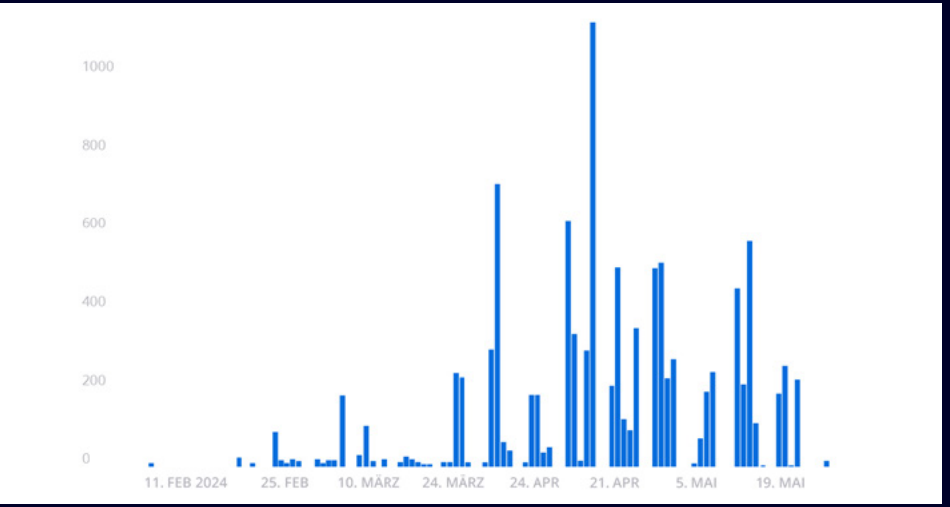
SharePoint-/Google Drive-Ordner als Umgehungstechnik verwendet

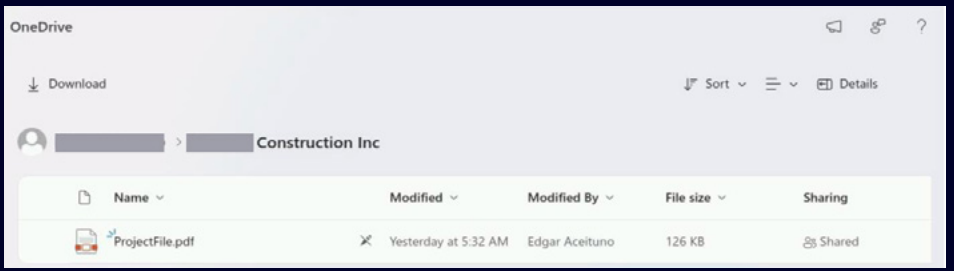
Zwischen Februar und März

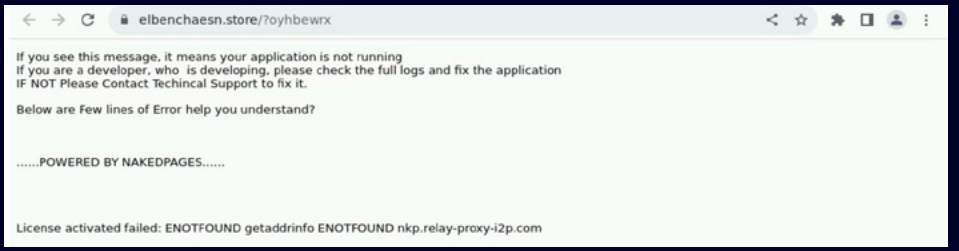
Angreifer nutzen SharePoint und Google Drive, um bösartige Dokumente zu speichern, die vorgeben, Projektangebote oder Rechnungen für Dienstleistungen zu sein. Für die Kampagnen werden gefälschte Office-365-Konten von Unternehmen aus der gleichen Branche verwendet, was die Wahrscheinlichkeit erhöht, dass die Zielperson die E-Mail für legitim hält.

Bei einem Klick auf das Dokument werden die Opfer auf eine Seite von Microsoft weitergeleitet, die mit dem Nakedpages-Phishing-Kit erstellt wurde, um Anmeldeinformationen zu sammeln. Die Fehlerinformationen auf einer Seite beziehen sich auf einen I2P-Proxy, eine auf Datenschutz ausgerichtete Netzwerkschicht, die anonyme Kommunikation ermöglicht. Dies kann darauf hinweisen, dass das Kit über eine Funktion zum Exfiltrieren von Daten oder zur anonymen Kommunikation verfügt.

KLICKEN SIE HIER, UM ALLE DETAILS DER KAMPAGNE ANZUZEIGEN.







ZIELGRUPPE Mitarbeiter von Unternehmen **INHALT** Ein schädliches PDF-Dokument mit einer HTML-Dateierweiterung

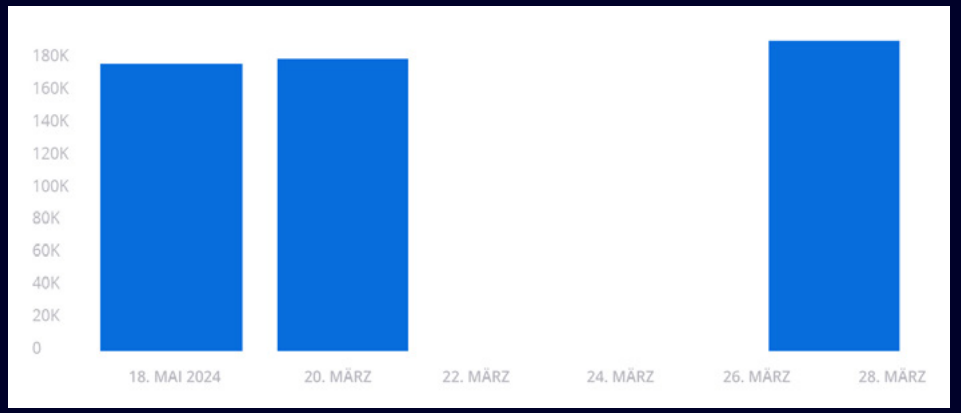
04

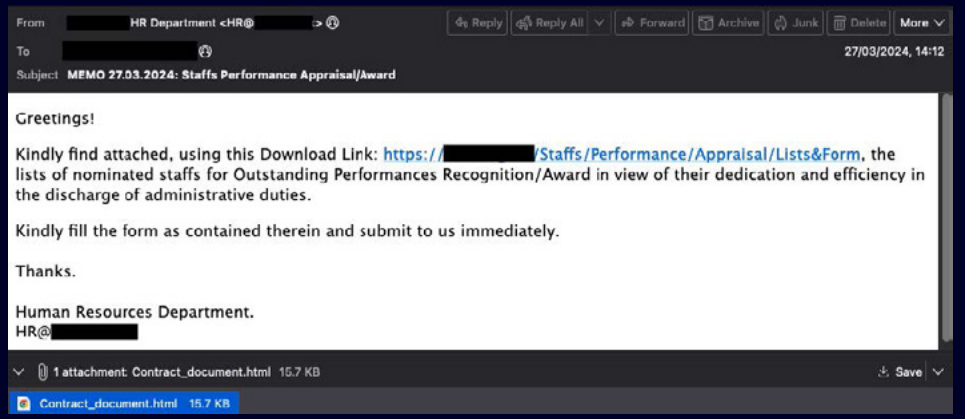
Nutzung von Online-KI-Tools als Kampagneninfrastruktur

Im März

An drei Tagen im März verschickten die Angreifer über den Massen-Mailing-Dienst Mailgun 380.000 E-Mails mit einem PDF-Dokument im Anhang, das mit einer HTML-Dateierweiterung endete. Beim Anklicken der Datei öffnete sich das PDF im Webbrowser des Empfängers und zeigte zwei Links zu einer anderen Seite, die auf dem Replit AI Development Service gehostet war.

Die Angreifer geben sich als interne HR-Teams aus und geben Updates zu Leistungsbeurteilungen, Urlaubsrichtlinien oder Pflichtschulungen bekannt (siehe Abbildung unten). Die letzte Zielseite ist eine Seite, die als Microsoft Outlook-Portal getarnt ist und dazu dient, Anmeldeinformationen abzugreifen.





KLICKEN SIE HIER, UM ALLE DETAILS DER KAMPAGNE ANZUZEIGEN.

ZIELGRUPPE Bekannte australische Anwaltskanzleien

INHALT Links zu Zwischenseiten auf Plattformen wie Atlassian, Archbee und Nuclino

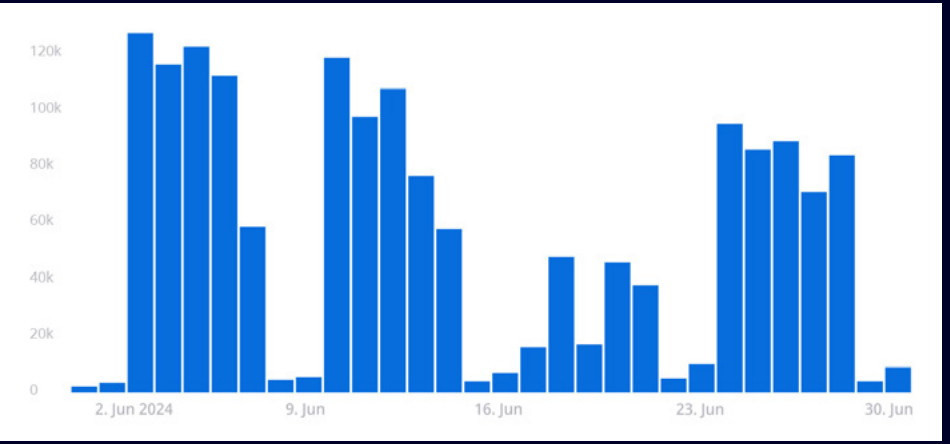
05

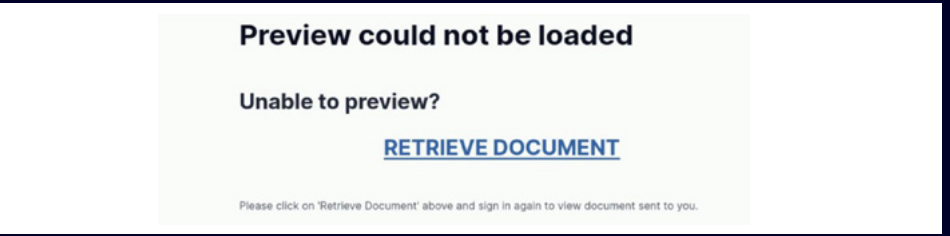
Missbrauch von Atlassian, Archbee- und Nuclino-Workspaces

Zwischen Mai und Juni

In einer groß angelegten Kampagne wurden verschleierte URLs in E-Mails verwendet, um Benutzer, die auf die Links klickten, auf eine Zwischenseite auf einer von mehreren Kollaborationsplattformen, darunter Atlassian, Archbee und Nuclino, umzuleiten. Die Lock-E-Mail der Kampagne scheint von einem internen Team zu stammen, das behauptet, das Gerät des Empfängers weise Konformitätsprobleme auf. Die Benachrichtigung enthält auch einige detaillierte Informationen über das System des Nutzers.

Wie bei vielen modernen Kampagnen führt ein Klick auf den Link in der E-Mail zu einer Weiterleitungskette. Auch das Ziel ist bekannt: eine gefälschte Anmeldeseite für Microsoft Outlook.





KLICKEN SIE HIER, UM ALLE DETAILS DER KAMPAGNE ANZUZEIGEN.

ZIELGRUPPE Verbraucher **INHALT** Eine Vielzahl gefälschter Rechnungen, einschließlich einer Telefonnummer zu einem KI-gestützten Callcenter

06

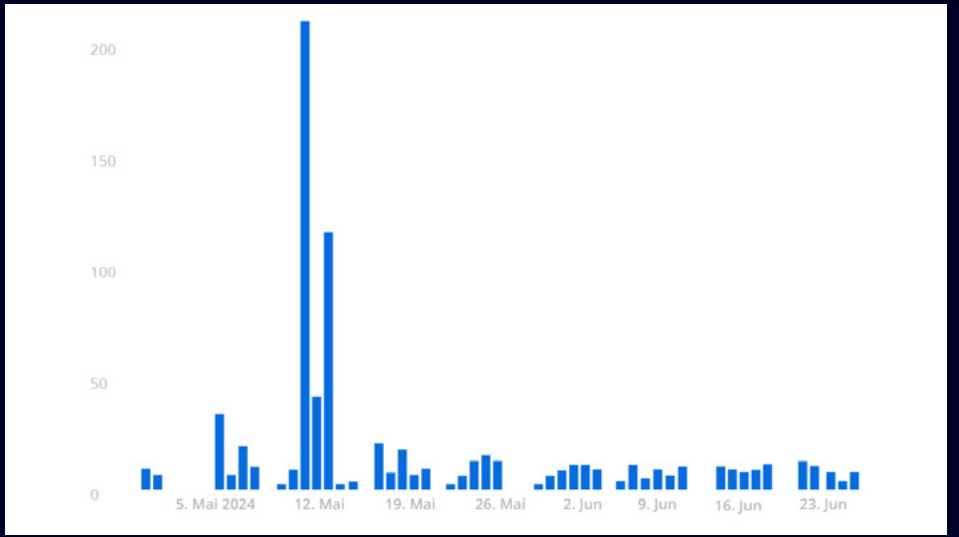
E-Mail-Betrug unterstützt durch KI-Bot-Callcenter

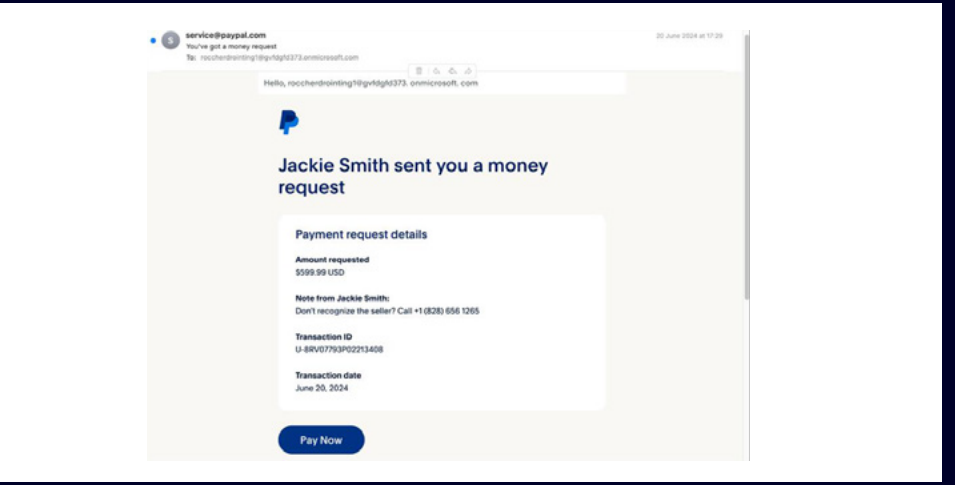
Im Mai

Mit Hilfe von Microsoft-Verteilerlisten, die den Massenversand von E-Mails ermöglichen und dabei mehrere E-Mail-Sicherheitschecks wie SPF und DMARC passieren, erstellen Angreifer Nachrichten, die den Empfänger scheinbar über eine bevorstehende Rechnung oder eine Kontobelastung informieren. Ruft der Empfänger dann die angegebene Telefonnummer an, wird er mit einem Callcenter verbunden, das zunehmend automatisiert über ein Large Language Model (LLM) betrieben wird und die vom Betrüger gewünschten Informationen sammelt.

Im Mai entdeckte Mimecast mehr als 1,6 Millionen solcher E-Mails, die an Verbraucher gerichtet waren.

KLICKEN SIE HIER, UM ALLE DETAILS DER KAMPAGNE ANZUZEIGEN.





Empfehlungen

Bedrohungsspezifische Empfehlungen

1

Blockieren Sie die Verwendung von Bildern in E-Mails
Angreifer nutzen zunehmend bildbasierte Dateitypen, um Phishing-Köder und Schadcodes unter Umgehung von Erkennungsmechanismen einzuschleusen. Analysen von Mimecast haben gezeigt, dass Angreifer auch Verschlüsselungen und fremdsprachige Texte in Bildern verwenden, um unerkannt zu bleiben. Unternehmen sollten ihre E-Mail-Clients so konfigurieren, dass das Laden von Bildern in Nachrichten verhindert wird. Nur Bilder, die vom Benutzer explizit markiert wurden, sollten isoliert werden.

Hinweis: Benutzer von Cyber-Grafiken sollten vertrauenswürdige Websites nutzen, um sicherzustellen, dass Banner korrekt geladen werden.

2

Segmentieren Sie das Netzwerk und zeichnen Sie den internen Datenverkehr auf
Angreifer können sich im Netzwerk schnell in alle Richtungen bewegen, insbesondere während eines Ransomware-Angriffs. Die Segmentierung des internen Netzwerks und die Platzierung kritischer Ressourcen in separaten Bereichen kann den durch Ransomware und andere Angriffe verursachten Schaden verringern. Die Überwachung des internen Datenverkehrs, insbesondere die Segmentierung der Kommunikation, kann zu einer früheren Erkennung von Bedrohungen führen.

3

Verwenden Sie sichere Mechanismen für Benutzeranmeldeinformationen und implementieren Sie MFA
Um in Netzwerke einzudringen, verwenden Malware-Bedrohungen häufig gängige Passwörter. Aktuelle Angriffe zeigen, wie schwache Passwörter zu Sicherheitslücken führen können. Stärken Sie jedes Netzwerk durch die Durchsetzung von Richtlinien für sichere Passwörter, insbesondere für Benutzer mit erweiterten Zugriffsrechten. Die IT-Sicherheit muss sich von Standard-Administratorpasswörtern verabschieden. Das Erfordernis einer mehrstufigen Authentifizierung kann die Beeinträchtigung gestohlener Konten oder Anmeldeinformationen drastisch reduzieren.

4

Bieten Sie Schulungen zur Sensibilisierung an

Menschen sind das Herz eines Unternehmens. Dennoch sind Fehler in der täglichen Arbeit menschlich. Wenn die Mitarbeiter für Cyber-Risiken sensibilisiert sind und wissen, wie sie diese erkennen können, ist dies die erste Verteidigungslinie gegen viele Angriffe, einschließlich E-Mail-basierter Gefahrenquelle.

5

Fordern Sie mehr Sicherheit von Drittanbietern

Angriffe auf Unternehmen in den Bereichen Herstellung, Transport, Lagerung und Auslieferung sowie im Einzel- und Großhandel stellen ein erhebliches Risiko für Dritte dar, die Lieferkette zu gefährden.

Unternehmen sollten ihre Dienstleistungsvereinbarungen überprüfen, um Mindeststandards für Daten- und Cybersicherheit festzulegen. Darüber hinaus sollten sie nach Möglichkeiten suchen, ihre Lieferanten genauer zu verfolgen, z. B. durch die Nutzung externer Bewertungsdienste oder eine genauere Prüfung von Akquisitionen.

6

Scannen Sie Ihre Umgebung auf Fehlkonfigurationen oder offene externe Ports

Unternehmen sollten ihre Infrastruktur regelmäßig auf bekannte ausnutzbare Schwachstellen überprüfen, z. B. unsichere offene externe Netzwerkports oder öffentliche Cloud-Umgebungen. Mit Tools wie Cloud Security Posture Management können Unternehmen fehlerhafte Konfigurationen in ihrer öffentlichen Cloud schnell identifizieren. So lässt sich sicherstellen, dass alle öffentlich zugänglichen Server-Ports geschlossen oder angemessen gesichert und geschützt sind.

So hat Mimecast beispielsweise einen stetigen Anstieg von Angriffen auf Remote Desktop Protocol (RDP)-Ports festgestellt, die für 80 Prozent der tatsächlichen Ransomware-Angriffe verantwortlich sind. Angreifer werden weiterhin nach offenen RDP-Ports suchen, um Organisationen anzugreifen.

Best Practices und Empfehlungen

31. JANUAR 2024 **US Cyber Command, CISA, FBI, ONCD**	**Hearing on CCP Cyber Threat**	Amerikanische Cybersicherheitsbeamte haben ihre Besorgnis über die zunehmenden Aktivitäten chinesischer Cyberbedrohungsakteure im asiatisch-pazifischen Raum zum Ausdruck gebracht, insbesondere über den strategischen Einsatz und die strategische Platzierung von Malware gegen kritische Infrastrukturen in der gesamten Region. Ein mit China verbundener Akteur, Volt Typhoon, hat im Jahr 2021 bereits Angriffe in der Region durchgeführt.
14. FEBRUAR 2024 **Microsoft and Open AI**	**Staying Ahead of Threat Actors in the Age of AI**	Bedrohungsakteure, einschließlich Cyberkriminellen und staatlichen Gegnern, experimentieren mit LLM in verschiedenen Phasen der Angriffskette, einschließlich der Übersetzung von Text, um Nachrichten professioneller erscheinen zu lassen, und als Mittel zur Automatisierung der Erkundung. Zu den APT-Gruppen, von denen bekannt ist, dass sie ChatGPT von Open AI für diese Zwecke testen, gehören die mit Russland verbundene Gruppe Forest Blizzard, die Gruppe Emerald Sleet mit Verbindungen zu Nordkorea, die Gruppe Crimson Sandstorm mit Verbindungen zum Iran sowie die mit China verbundenen Gruppen Charcoal Typhoon und Salmon Typhoon.
29. MÄRZ 2024 **CISA**	**Reported Supply Chain Compromise Affecting XZ Utils Data Compression Library, CVE-2024-3094**	Einem Angreifer gelang es, einen Entwickler dazu zu bringen, Updates für das Open-Source-Projekt XZ Utils zu akzeptieren, die in Wirklichkeit eine Hintertür zu jedem System darstellten, auf dem die Software ausgeführt wurde. Nach jahrelangem Vertrauensaufbau mit dem Projektleiter war die Hintertür nur noch wenige Wochen von der Integration in eine große Linux-Distribution entfernt, als ein Microsoft-Entwickler den Code entdeckte und die Community informierte.

2. APRIL 2024 **CISA**	**Cyber Safety Review Board Releases Report on Microsoft Online Exchange Incident from Summer 2023**	Der Bericht ist der dritte Vorfall, der vom Cyber Safety Review Board (CSRB) untersucht wurde. Dabei geht es um den Einbruch in Microsoft Exchange Online im Mai 2023 durch Storm-0558, eine Hackergruppe mit Verbindungen zur Volksrepublik China, die für die Operation Aurora im Jahr 2009 und die RSA SecureID-Verletzung im Jahr 2011 verantwortlich gemacht wird. Bei dem Angriff wurden E-Mail-Konten des US-Außenministeriums, des US-Handelsministeriums, des US-Repräsentantenhauses und 22 weiterer Organisationen offengelegt. Das CSRB hat Empfehlungen für Microsoft im Besonderen, für Cloud-Anbieter im Allgemeinen und für Cloud-Kunden formuliert.
2. MAI 2024 **FBI, State, NSA**	**North Korean Actors Exploit Weak DMARC Security Policies to Mask Spearphishing Efforts**	Nordkoreanische Cyber-Akteure führen häufig Spearphishing-Kampagnen durch, die auf Journalisten, Akademiker und politische Beamte, insbesondere Ostasienexperten, abzielen. Die Aktivitäten, die mit Kimsuky oder Emerald Sleet in Verbindung gebracht werden, zielen auf Unternehmen mit schwachen E-Mail-Richtlinien (Domain-based Message, Reporting and Conformance -DMARC) ab, um einer Entdeckung zu entgehen.
26. JUNI 2024 **CISA, FBI, ACSC**	**Exploring Memory Safety in Critical Open Source Projects**	Regierungsgruppen haben einen dringenden Appell an Open-Source-Softwareprojekte und ihre Nutzer veröffentlicht, auf speichersichere Programmiersprachen umzusteigen. Mehr als die Hälfte aller Codezeilen (55 %) sind in nicht sicheren Programmiersprachen geschrieben. Allerdings basieren selbst Projekte, die in sicheren Programmiersprachen geschrieben wurden, auf nicht ausreichend sicheren Komponenten.

Empfehlungen/Checkliste von Mimecast

Dieser Abschnitt bietet Mimecast-Benutzern konkrete und umsetzbare Schritte, um ihre Benutzer vor den im Bericht genannten Bedrohungen zu schützen.

Single sign-on
Es wird empfohlen, **eine Single Sign-on-Lösung zur Anmeldung** für die Anmeldung bei Ihrem Identitätsprovider zu verwenden oder die in Mimecast integrierte Multi-Faktor-Authentifizierung zu nutzen, um die Möglichkeiten eines Angreifers, E-Mails als Angriffspunkt zu missbrauchen, zu verringern.

DNS-Authentifizierungsrichtlinien
Stellen Sie sicher, dass **DNS-Authentifizierungsrichtlinien** DMARC-Einträge berücksichtigen. Eine zweite Richtlinie, die auf eine Richtliniengruppe mit der DMARC-Fehleraktion „Ignorieren/Verwalten und Zulassen von Absendern“ eingestellt ist, bietet einen effektiven Umgehungmechanismus für alle legitimen E-Mails, die aufgrund von DMARC-Fehlern abgelehnt oder isoliert werden.

Schutz vor Identitätsmissbrauch
Optimieren Sie den Schutz vor Identitätsbetrug gemäß den Best Practice-Richtlinien von zwei Treffern. Setzen Sie das Kennzeichen „Betreff/Text“ und fügen Sie eine separate C-Level/VIP-Richtlinie auf der Grundlage von Namensübereinstimmungen mit einer Sperre für die Überprüfung durch den Administrator hinzu. Erstellen Sie außerdem eine weitere Richtlinie für alle Übereinstimmungen mit drei oder mehr Treffern mit Sperrung durch den Administrator.

Umschreibung von URLs
Die Einrichtung eines **umfassenden URL Rewritings** stellt sicher, dass alle URLs beim Anklicken gescannt werden. Beachten Sie jedoch, dass das Umschreiben alle Elemente umfasst, die einer URL ähneln, z. B. IP-Adressen und interne Links.

Auto-Allow Richtlinien
Erwägen Sie, auf „strict“ statt auf „allow“ zu setzen, um sicherzustellen, dass das Spam-Scanning auf Unternehmensebene für externe E-Mail-Empfänger nicht umgangen wird. Dies sollte in Verbindung mit **„Auto Allow Spam Detection “** so konfiguriert werden, dass Inhalte zur Überprüfung zurückgestellt werden, um sicherzustellen, dass keine potenziell schädlichen Nachrichten die Prüfung umgehen.

SIEM- und XDR-Anbieter
Nutzen Sie vorgefertigte Integrationen, die mit den meisten SIEM- und XDR-Anbietern kompatibel sind, um Protokollierung und Analyse zur Durchsetzung von Sicherheitsrichtlinien bereitzustellen.

Bedrohungsmeldungen von Drittanbietern
Nutzen Sie Ihre eigenen Bedrohungsdaten als Grundlage für die Nutzung aller Bedrohungsdaten von Drittanbietern zur automatisierten Ablehnung von übereinstimmenden Indikatoren.

Berichterstattung für Endbenutzer
Es wird empfohlen, dass Endbenutzer verdächtige Nachrichten, die sie **über Mimecast-Tools für Benutzer** erhalten, dem Mimecast-SOC zur weiteren Analyse melden.

5 Zusammenfassung

Die sich wandelnde Bedrohungslandschaft stellt mit der zunehmenden Digitalisierung von Geschäftsprozessen in der Cloud weiterhin eine Herausforderung für die Cybersicherheitsteams dar. Die Folge sind Ransomware-Attacken, komplexe Kompromittierungen der digitalen Lieferkette, integrierte Schwachstellen und vermehrte Attacken auf Identifizierungssysteme.

Insgesamt haben sich viele der im letzten Jahr angedeuteten Trends im ersten Halbjahr 2024 weiter verfestigt. Bösartige Links sind nach wie vor der bevorzugte Weg für Bedrohungsakteure, um Nutzdaten auf die Systeme der Opfer zu übertragen. Beschäftigte in kleinen und mittleren Unternehmen sind weiterhin mehr als doppelt so vielen Bedrohungen ausgesetzt wie Nutzer in großen Unternehmen. Auch legale Filesharing-Dienste werden weiterhin von böswilligen Akteuren missbraucht.

Gleichzeitig treiben cyberkriminelle Gruppen ihre Aktivitäten weiter voran. Die Auswirkungen der umfangreichen Strafverfolgungsmaßnahmen gegen bekannte Gruppen wie LockBit haben wahrscheinlich zu einem kurzfristigen Rückgang bösartiger Aktivitäten geführt, die sich jedoch im Laufe des Jahres wieder normalisieren dürften.

Kurzfristig hält die Zukunft einige vorhersehbare Herausforderungen bereit. In dem Maße, in dem Unternehmen in die Cloud wechseln und ihre Infrastruktur ausbauen, vergrößert sich die gesamte Angriffsfläche. Wenn sichergestellt wird, dass die neue Infrastruktur sicher konfiguriert und nach Möglichkeit überwacht wird, kann dieser Herausforderung erfolgreich entgegen gewirkt werden.

Die zunehmende Abhängigkeit von Datensätzen in der Cloud bedeutet, dass die Sicherheit oft außerhalb der Kontrolle des Eigentümers liegt, während die inhärente Abhängigkeit von Software und Infrastruktur Dritter die Sicherheit der Lieferkette zu einem großen Problem macht.

Angesichts der anhaltenden Ransomware-Angriffe ist die Aufrechterhaltung der Datenverfügbarkeit ein Schlüsselfaktor für den Geschäftserfolg, da eine Unterbrechung des Geschäftsbetriebs oder ein Denial-of-Service-Angriff sehr kostspielig für den Ruf des Unternehmens und die Bereitstellung von Diensten ist. Backups werden immer zielgerichteter verwaltet und erfordern einen Sicherheitsfokus, um sicherzustellen, dass sie in einer sicheren Umgebung verbleiben.

Fehler von Mitarbeitern sind seit jeher ein Faktor bei der Ermittlung von Risiken für Unternehmen, da sie direkten Zugang zu relevanten Informationen oder Netzwerken haben. Mitarbeiter sind nach wie vor ein sehr erfolgreicher Angriffspunkt, und es ist unwahrscheinlich, dass sich diese äußerst anpassungsfähige Taktik ändern wird.

Der Einsatz von generativer KI und maschinellem Lernen wird die Zielgenauigkeit und den Inhalt von Phishing-Kampagnen verbessern und damit den Bedarf der Verteidiger an technischen Indikatoren erhöhen, um neue und neuartige Angriffe erkennen und darauf reagieren zu können.

mimecast

Mimecast ist eine KI-gestützte, API-fähige und vernetzte Human Risk Management-Plattform. Sie wurde entwickelt, um Unternehmen vor dem gesamten Spektrum von Cyberbedrohungen zu schützen. Dafür integriert sie moderne, benutzerfreundliche Technologie mit Strategien für das Erkennen von Risiken und den Aufbau von Sicherheitskompetenz, die immer den Nutzer im Fokus behalten. Darauf ausgelegt, unsichtbare Risiken sichtbar zu machen und Dateneinblicke so aufzubereiten, dass sie als Entscheidungsgrundlage dienen können, eröffnet sie Unternehmen proaktive Handlungsmöglichkeiten.
Sie hilft, Kommunikations- und Kollaborationslandschaften zu schützen, kritische Daten zu sichern, Mitarbeiter aktiv in das Risikomanagement einzubeziehen und eine Sicherheitskultur zu fördern, die mit Unternehmenszielen wie Geschäftskontinuität und Steigerung der Produktivität in Einklang steht. Über 42.000 Unternehmen weltweit vertrauen Mimecast, um der sich dynamisch entwickelnden Bedrohungslandschaft einen Schritt voraus zu sein. Von internen Risiken bis hin zu externen Gefahren – Mimecast bietet Kunden mehr. Mehr Sichtbarkeit. Mehr Einblicke. Mehr Agilität. Mehr Sicherheit.

Mimecast Threat Intelligence Team

Das Threat Intelligence Team von Mimecast besteht aus einer weltweit verteilten Gruppe von Ingenieuren, Wissenschaftlern, Analysten und Bedrohungsforschern, die das Mimecast Security Operations Center (MSOC) unterstützen. Hier werden täglich mehr als eine Milliarde E-Mails kontinuierlich auf Bedrohungen überwacht. Die Cybersicherheitsexperten von Mimecast analysieren und untersuchen Angriffe und testen ihre Wirksamkeit, um anspruchsvolle und aktuelle Bedrohungsinformationen zu entwickeln, die die neuesten Schutzmaßnahmen auf die Sicherheitslösungen von Mimecast anwenden.

Weitere Informationen finden Sie hier:

Besuchen Sie den Mimecast Threat Intelligence Hub, um über alle Threat Intelligence-Aktivitäten von Benachrichtigungen bis hin zu Berichten und regionalen Webinaren auf dem Laufenden zu bleiben.

Verstehen Sie die größten Cybersicherheitslücken:

Sehen Sie sich den Bericht E-Mail-Sicherheit – ein Lagebericht aus dem Jahr 2024 an, um die größten Lücken in der Cybersicherheit zu verstehen