proofpoint.

E-BOOK

Phish im Glas

Was Anwender nicht über Cyberbedrohungen wissen – und warum das gefährlich ist

proofpoint.com/de

Einführung

Ein altes Sprichwort sagt: *Was ich nicht weißt, macht mich nicht heiß*. Im Fall von Cyberbedrohungen könnte diese Aussage jedoch kaum falscher sein.

Cyberbedrohungen, die Ihre Anwender nicht kennen, sind eine Gefahr – auch für Ihr Unternehmen. Zudem werden Angestellte ständig mit Cyberattacken angegriffen. Fehlerhaftes Verhalten aufgrund von Wisenslücken kann zu Unterbrechungen von Geschäftsabläufen, finanziellen Verlusten und langfristigen Schäden führen.

Dieses E-Book stellt reale Angriffe vor, die zeigen, dass Anwender sowohl wichtige Ziele für Angreifer als auch die letzte Verteidigungslinie des Unternehmens sind.

Wir beleuchten fünf wichtige Kategorien für Cyberangriffe und andere Cyberkriminalität, die mit der Ausnutzung von Anwendern beginnen oder darauf aufbauten:

- Phishing
- Business Email Compromise (BEC)
- Ransomware
- Cloud-Angriffe
- Webmail-Angriffe

Dabei stellen wir auch einige Fakten aus unserem State of the Phish 2022-Bericht vor, um auf die Kenntnisse, Schwächen und Stärken der Anwender in diesen Bereichen hinzuweisen. Die Daten geben wichtige Hinweise für Sicherheitsverantwortliche, die ihre Anwender, Daten und Marken schützen möchten. Sie zeigen auch, warum Mitarbeiter der neue Perimeter sind – und deshalb im Zentrum Ihrer Cybersicherheitsmaßnahmen stehen sollten.

ABSCHNITT 1

Phishing

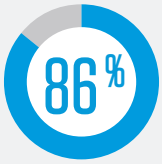
Phishing ist eine Form von Social Engineering.

Phishing wird in Form von E-Mails oder Textnachrichten übermittelt und setzt ein wachsendes Spektrum an Techniken zur Ausnutzung der menschlichen Psychologie ein. Bedrohungsakteure missbrauchen das Vertrauen von Anwendern, um an Finanzdetails, Anmeldedaten und andere vertrauliche Informationen zu gelangen.

Trends

Mit jedem weiteren Jahr wird Phishing für Angreifer immer wichtiger. Laut dem *Internet Crime Report 2021* des FBI machten Phishing und ähnliche Angriffe mehr als 38 % der gesamten in den USA gemeldeten Internetkriminalität im letzten Jahr aus. Im Jahr 2021 wurden fast 323.000 Phishing-Versuche gemeldet. Das ist ein Plus von fast 83.000 Beschwerden gegenüber dem Jahr 2020 bzw. von 209.000 gegenüber 2019.[1]

Untersuchungen für den *State of the Phish 2022*-Bericht zeigen, wie häufig und effektiv Phishing-Angriffe sind. Dabei zeigte sich für 2021:



der Unternehmen haben Angriffe mit massenhaften Phishing-Angriffen verzeichnet[2]

20 %

der Anwender haben bei Phishing-Simulationen einen Anhang geöffnet

10 %

der Anwender haben bei Phishing-Simulationen auf einen Link geklickt

Reales Beispiel: Ukrainisches Stromnetz wird ausgeschaltet

Im Dezember 2015 wurde das ukrainische Stromnetz unterbrochen und ließ ca. 225.000 Menschen in dem osteuropäischen Land für bis zu sechs Stunden ohne Strom. Dies war der erste öffentlich bekannt gewordene Cyberangriff, der zu Stromausfällen führte.[3]

Die Bedrohungsakteure hinter dem Angriff verbrachten mehrere Monate mit der Planung und Sammlung von Informationen. Zu den verwendeten Techniken gehörte auch Spearphishing. In diesem Fall gehörten IT-Mitarbeiter und Systemadministratoren bei drei ukrainischen Energieanbietern (oder Oblenergos) zu den Zielen.[4]

1 FBI IC3: „Internet Crime Report 2021“ (Bericht zu Internetkriminalität 2021), März 2022, Download: https://www.ic3.gov/Home/AnnualReports.

2 Proofpoint definiert Massen-Phishing als wahllose „Standard-Angriffe“, bei denen die gleiche E-Mail an viele Mitarbeiter in einem Unternehmen verschickt wird.

3 SANS Industrial Control Systems (ICS) und Electricity Information Sharing and Analysis Center (E-ISAC): „Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case“ (Analyse des Cyberangriffs auf das ukrainische Stromnetz), 18. März 2016.

4 ICS und E-ISAC.

Vorgehensweise

Um diese Anwender zu kompromittieren, sendeten die Angreifer einen schädlichen Microsoft Word-Anhang in einer E-Mail, die scheinbar von einer vertrauenswürdigen Quelle kam. Beim Öffnen zeigte das Dokument eine Popup-Meldung, die Anwender zum Aktivieren von Makros aufforderte. Wenn die Anwender dieser Aufforderung folgten, wurde die Malware BlackEnergy3 installiert und die Maschine infiziert, d. h. eine Backdoor für die Angreifer eingerichtet.[5]

Mithilfe dieser Spearphishing-Angriffe erlangten die kriminellen Akteure Zugriff auf das Netzwerk der Energieanbieter. Anschließend verbrachten die Angreifer mehrere Monate damit, einen Weg zum SCADA-Industriesteuernetzwerk (Supervisory Control And Data Acquisition) zu finden, um ihren großen Angriff vorzubereiten. Dazu nutzten sie verschiedene Methoden, beispielsweise Zugriff auf Microsoft Windows-Domain-Controller, um an noch mehr Anmeldedaten zu gelangen.[6]

Das Ergebnis

Der Stromausfall war nur kurz. Dennoch dauerte es mehrere Monate, bis die Kontrollzentren der betroffenen Oblenergos wieder vollständig einsatzfähig waren. Wie ein Bericht über den Angriff bemerkte, war der Zwischenfall ein böses Vorzeichen für die Sicherheit von Stromnetzen auf der ganzen Welt.[7]

Phishing: potenzielle Konsequenzen

Kontoübernahme | Finanzielle Verluste | Datenverlust | Rufschädigung

So hätten Schulungen zur Sensibilisierung geholfen

Ebenso wie die meisten Cyberangriffe begann auch die Unterbrechung des Stromnetzes 2015 mit einer Phishing-E-Mail. Nachdem sie einen Mitarbeiter dazu gebracht hatten, einen infizierten Anhang zu öffnen, verbrachten die Bedrohungsakteure mehrere Monate damit, Informationen zu sammeln und tiefer in die Umgebung einzudringen.

Security-Awareness-Schulungen hätten den Angriff schon im Vorfeld stoppen können. Durch die Schulungen hätten die Mitarbeiter gewusst, dass sie den Anhang nicht öffnen oder damit interagieren dürfen, sodass der Angreifer keinen Zugang erlangt hätte.

5 Kim Zetter *(Wired)*: „Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid" (Details zum raffinierten und einzigartigen Hack des ukrainischen Stromnetzes), 3. März 2016

6 ebd.

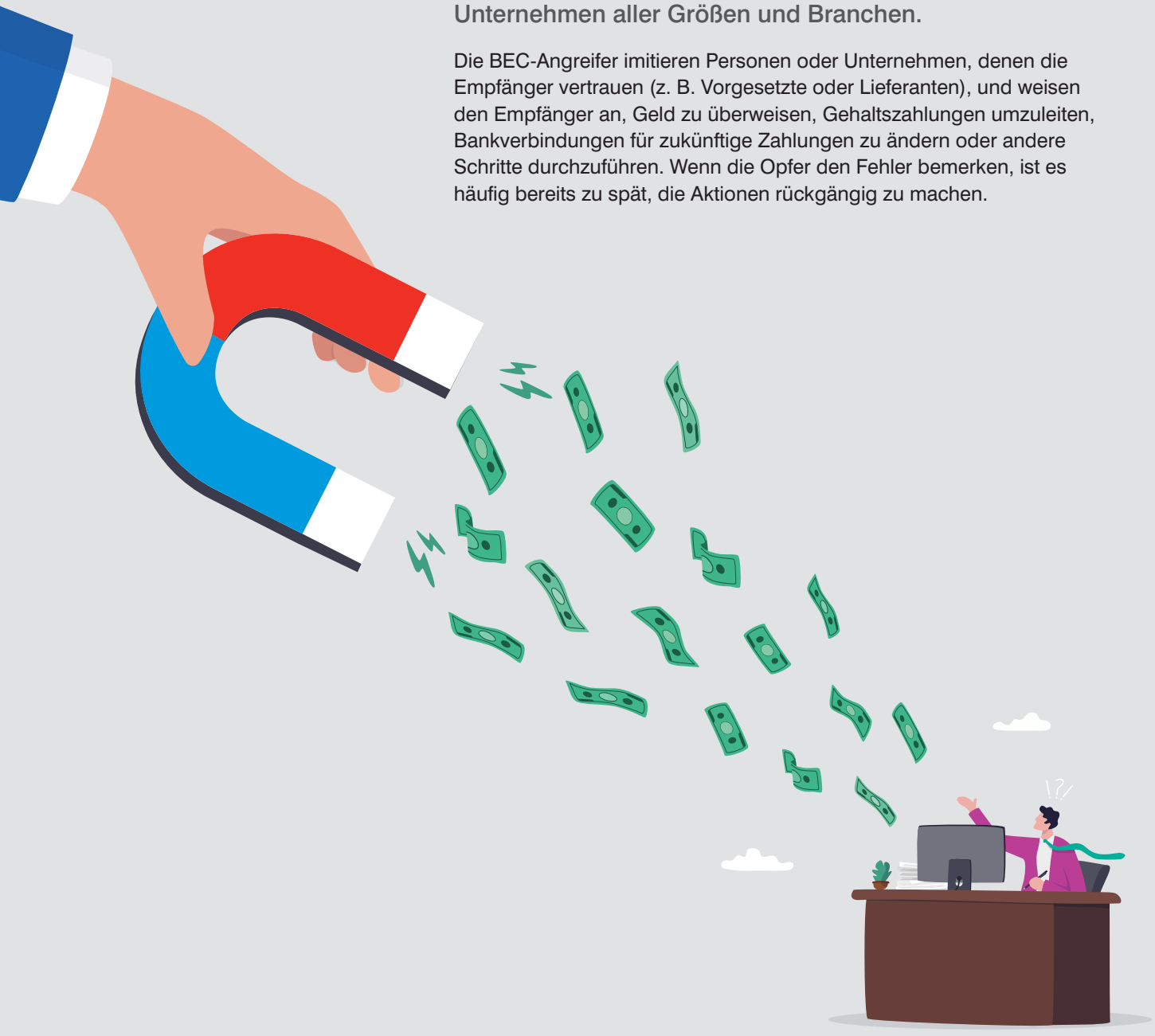
7 ebd.

ABSCHNITT 2

Business Email Compromise (BEC)

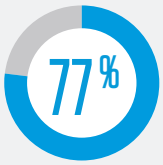
BEC-Angriffe (Business Email Compromise) betreffen Unternehmen aller Größen und Branchen.

Die BEC-Angreifer imitieren Personen oder Unternehmen, denen die Empfänger vertrauen (z. B. Vorgesetzte oder Lieferanten), und weisen den Empfänger an, Geld zu überweisen, Gehaltszahlungen umzuleiten, Bankverbindungen für zukünftige Zahlungen zu ändern oder andere Schritte durchzuführen. Wenn die Opfer den Fehler bemerken, ist es häufig bereits zu spät, die Aktionen rückgängig zu machen.



Trends

BEC-Kampagnen können sehr einträglich sein. Laut dem *Internet Crime Report 2021* des FBI haben BEC-Angriffe in den USA allein im letzten Jahr zu bereinigten Kosten von 2,4 Milliarden US-Dollar geführt.[8] Angesichts der potenziellen Gewinne überrascht es daher nicht, dass 77 % aller Unternehmen auf der ganzen Welt im Jahr 2021 BEC-Angriffe verzeichneten, wie der *State of the Phish 2022*-Bericht zeigte.



der weltweiten Unternehmen
haben 2021 BEC-Angriffe erlebt

BEC-Attacken gehen häufig äußerst raffiniert vor und werden von kapitalkräftigen Akteuren durchgeführt, die sehr viel Planung und Recherche investieren.[9] Viele Angreifer konzentrieren ihre Bemühungen auf Betrugsversuche mit Lieferantenrechnungen, da sie auf diese Weise große B2B-Transaktionen (Business-to-Business) umleiten können. Zu den Standardtaktiken gehören gefälschte Rechnungen, bei denen sich die Betrüger als Lieferanten ausgeben und Zahlungen an echte Anbieter zu ihren eigenen Konten umleiten.

Reales Beispiel: Ubiquiti verliert 46,7 Mio. USD durch Anbieterbetrug

Eine weitere gut abgehangene, aber weiterhin effektive BEC-Strategie ist CEO-Betrug, bei dem sich die Angreifer als Geschäftsführer oder sonstige Führungskraft ausgeben. Meist fordern sie eine Person in der Finanzabteilung per E-Mail auf, eine Überweisung zu tätigen – wobei das Geld an ein internationales Konto geht, das die Angreifer kontrollieren.

Eben diese Variante von BEC-Betrug kam auch im Fall von Ubiquiti Inc. zum Einsatz. Den Cyberkriminellen gelang es, das Technologieunternehmen um 46,7 Millionen US-Dollar zu erleichtern, bevor das Problem überhaupt bemerkt wurde. Angestellte, die zum Überweisen von Geldern berechtigt sind, stellen entsprechende Anweisungen von Vorgesetzten unter Umständen selbst dann nicht in Frage, wenn die Aufforderungen ungewöhnlich erscheinen.

Vorgehensweise

Mitte Mai 2015 erhielt der erst seit wenigen Wochen angestellte CFO (Chief Financial Officer) von Ubiquiti eine Reihe von E-Mails, die scheinbar von seinem Geschäftsführer sowie von einem Londoner Anwalt stammten. Die Betrüger gaben sich als CEO von Ubiquiti aus und erklärten, dass das Unternehmen eine Übernahme plante. Die E-Mail bat den Finanzvorstand darum, diese Nachricht vertraulich zu behandeln, und wies darauf hin, dass für einen erfolgreichen Geschäftsabschluss mehrere Überweisungen erforderlich sein würden. Anschließend sendeten die Betrüger eine weitere E-Mail mit Anweisungen und Kontodaten sowie eine gefälschte Autorisierung der Zahlung.[10]

8 FBI IC3.

9 Proofpoint: „E-Mail-Betrug im Posteingang. Die größten, gefährlichsten und dreistesten BEC-Angriffe“, April 2022.

10 Nathan Vardi *(Forbes)*: „How a Tech Billionaire’s Company Misplaced $46.7 Million and Didn’t Know It“ (Wie das Unternehmen eines Technologie-Milliardärs 46,7 Mio. USD verlor und es nicht bemerkte), Februar 2016.

Das Ergebnis

Im Laufe der nächsten 17 Tage tätigte der CFO insgesamt 14 Überweisungen mit einer Gesamthöhe von 46,7 Millionen US-Dollar an Konten in China, Ungarn, Russland und Polen. Anfang Juni wurde schließlich der echte Geschäftsführer des Unternehmens von einem FBI-Agenten kontaktiert und darüber informiert, dass erhebliche Geldsummen vom Bankkonto in der Ubiquiti-Niederlassung in Hongkong gestohlen wurden.[11] Bis zu diesem Zeitpunkt hatte der CEO überhaupt keine Kenntnis von den Überweisungen.

Im August 2015 gab Ubiquiti dann in einem Quartalsfinanzbericht an die US-Börsenaufsichtsbehörde (Securities and Exchange Commission) bekannt, dass das Unternehmen den Betrug im Juni entdeckt hatte. Der Zwischenfall wurde als „Nachahmung von Mitarbeitern und betrügerische Anfragen durch externe Parteien“ beschrieben.

Ubiquiti konnte nur einen Teil der Verluste zurückholen und hatte mit Rufschäden zu kämpfen. Kurz vor der Bekanntgabe des BEC-Zwischenfalls trat der Finanzvorstand zurück. Eine interne Untersuchung kam zu dem Ergebnis, dass die interne Kontrolle über die Finanzberichterstattung ineffektiv war, und das Unternehmen führte verschärfte Sicherheitsmaßnahmen ein.[12]

BEC: potenzielle Konsequenzen

Direkte finanzielle Verluste

Datenverlust

So hätten Schulungen zur Sensibilisierung geholfen

Anbieterbetrug und andere BEC-Formen richten sich grundsätzlich gegen Menschen. Sie sind jedoch nur dann erfolgreich, wenn die Empfänger davon ausgehen, dass sie es mit einer vertrauenswürdigen Partei zu tun haben. Durch effektive Security-Awareness-Schulungen hätte der CFO wissen können, dass er auf verdächtige Anzeichen dafür suchen musste, dass die E-Mails von einem Betrüger und nicht vom CEO sowie den Unternehmensanwälten stammten.

In Verbindung mit sinnvollen Finanzkontrollen können Anwenderschulungen Ihre Mitarbeiter anleiten, instinktiv auf Doppelgänger- oder Fremd-Domains, unsichere URLs und Social-Engineering-Techniken zu achten, die weniger aufmerksame Anwender ködern könnten.

11 ebd.

12 KrebsOnSecurity: „Tech Firm Ubiquiti Suffers $46M Cyberheist“ (Technologiefirma Ubiquiti verliert 46 Mio. USD bei Cyberdiebstahl), August 2015.

ABSCHNITT 3

Ransomware

Ransomware dient der Erpressung, d. h. die Malware sperrt Daten und Computersysteme, bis das Opfer zahlt, um wieder Zugriff zu erlangen.

Meist fordern die Angreifer das Geld in einer Kryptowährung wie Bitcoin, da solche Überweisungen schnell und nur schwer zu verfolgen sind. Die Forderung ist oft mit einem Ablaufdatum verbunden: Wenn das Opfer nicht rechtzeitig zahlt, verliert es entweder die Daten endgültig oder muss ein höheres Lösegeld zahlen, um sie zurückzuerhalten. Um den Druck auf die Opfer weiter zu erhöhen, drohen die Angreifer häufig damit, die Daten zu veröffentlichen. In einigen Fällen zahlen die Opfer zwar, verlieren aber dennoch ihre Daten.

Die bei Ransomware-Angriffen am häufigsten eingesetzten Malware-Typen sind Encrypter (engl. Verschlüsseler) und Screen Locker (engl. Bildschirmsperrer). Encrypter verschlüsseln die Daten auf einem System und machen den Inhalt ohne den Entschlüsselungsschlüssel unbenutzbar. Screen Locker wiederum nutzen einen Sperrbildschirm, um den Anwenderzugriff auf das kompromittierte System zu blockieren.

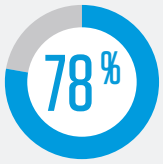
Ransomware-Angriffe gibt es schon seit Jahrzehnten, doch erst seit einigen Jahren machen sie Schlagzeilen wegen ihrer schwerwiegenden Schäden, der enormen Lösegeldzahlungen und der angegriffenen kritischen Infrastruktur, insbesondere im Gesundheitswesen und dem Energiesektor.

Gleichzeitig haben sie sich weiterentwickelt. Ransomware-Betreiber kaufen ihren Zugang häufig von unabhängigen Cybercrime-Gruppen, die lohnenswerte Ziele infiltrieren und anschließend den Zugang für einen Anteil an der Beute verkaufen. Auch Cybercrime-Gruppen, die bereits Bank-Malware und andere Trojaner verteilen, können sich am Ransomware-Partnernetzwerk beteiligen. Dadurch ist ein robustes und lukratives kriminelles Ökosystem entstanden, in dem sich verschiedene Personen und Organisationen immer stärker spezialisieren, um größere Profite für alle herauszuholen – auf Kosten der Opfer.

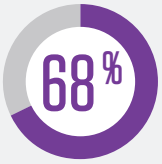
Trends

Die Zahl der Ransomware-Angriffe nimmt ebenfalls zu. So zeigte der *Data Breach Investigations Report 2022* von Verizon, dass Ransomware-Kompromittierungen von 2020 bis 2021 um 13 % zugenommen haben, was so viel ist wie der gesamte Anstieg der letzten fünf Jahre.[13]

Dies sind einige Erkenntnisse aus dem *State of the Phish 2022*-Bericht:



der Unternehmen haben 2021 Ransomware-Angriffe per E-Mail erlebt



der Unternehmen wurden mit Ransomware infiziert

der infizierten Unternehmen zahlten Lösegeld

13 Verizon: „Data Breach Investigations Report“ (Untersuchungsbericht zu Datenkompromittierungen), Mai 2022.

Reales Beispiel: Aufeinander folgende Ransomware-Angriffe stürzen Regierung von Costa Rica ins Chaos

Ein schwerer Ransomware-Angriff traf die Regierung von Costa Rica im April 2022 und attackierte fast 30 Institutionen, darunter unter anderem das Finanzministerium, den Sozialversicherungsfond und sogar das Nationale Meteorologische Institut. Die Ransomware-Gruppe Conti übernahm die Verantwortung für die Kampagne und forderte ein Lösegeld von 10 Millionen US-Dollar als Gegenleistung dafür, dass sie keine vertraulichen Informationen des Finanzministeriums veröffentlichen würden, die sie zuvor von den Servern exfiltriert hatten.[14]

Als die Regierung die Zahlung verweigerte, erhöhte Conti die Lösegeldforderung auf 20 Millionen US-Dollar und begann kurze Zeit später, gestohlene Dateien auf der eigenen Website hochzuladen. In einem verzweifelten letzten Versuch senkte die Conti-Gruppe das geforderte Lösegeld auf 15 Millionen US-Dollar.[15] Die ganze Geschichte nahm bizarre Züge an, als die Angreifer damit drohten, die Regierung zu stürzen.[16]

Ende Mai, als die Regierung von Costa Rica noch mit der Behebung der Conti-Schäden beschäftigt war, wurde der Nationale Gesundheitsdienst (CCSS) von der Gruppe Hive mit Ransomware angegriffen. Der Dienst wurde erst auf den Angriff aufmerksam, als seine Drucker damit begannen, massenhaft die Lösegeldnachricht von Hive zu drucken. Dabei wurde jedoch kein genauer Betrag genannt.[17] Diese Forderung kam erst später, als Hive vom CCSS eine Zahlung in Höhe von 5 Millionen US-Dollar in Bitcoin verlangte, um keine vertraulichen Informationen zu leaken.[18]

14 Carly Page *(TechCrunch)*: „Fears Grow for Smaller Nations After Ransomware Attack on Costa Rica Escalates“ (Kleinere Staaten in Sorge nach eskaliertem Ransomware-Angriff auf Costa Rica), 20. Mai 2022.

15 Carla Rosch *(Rest of World)*: „A Massive Cyberattack in Costa Rica Leaves Citizens Hurting“ (Massiver Cyberangriff in Costa Rica führt zu Schäden im ganzen Land), 1. Juni 2022.

16 Matt Burgess *(Wired)*: „Conti’s Attack Against Costa Rica Sparks a New Ransomware Era“ (Conti-Angriff gegen Costa Rica beginnt ein neues Ransomware-Zeitalter), 12. Juni 2022.

17 KrebsOnSecurity: „Costa Rica May Be Pawn in Conti Ransomware Group’s Bid to Rebrand, Evade Sanctions“ (Costa Rica könnte von Conti-Ransomware-Gruppe für Neuaufstellung missbraucht werden, um Sanktionen zu umgehen), 31. Mai 2022.

18 Alonso Martinez *(Delfino)*: „Cybercriminals Request $5 million in Bitcoins from the CCSS“ (Cyberkriminelle fordern 5 Mio. USD vom CCSS), 2. Juni 2022.

Vorgehensweise

Laut Bedrohungsforschern erlangte „MemberX“, ein Mitglied der Conti-Gruppe, mithilfe kompromittierter Anmeldedaten über eine VPN-Verbindung Zugang zu einem System des Finanzministeriums von Costa Rica.[19] Innerhalb von 24 Stunden nach der ersten Conti-Attacke gelang es den Angreifern, Dateien im Finanzministerium zu verschlüsseln und zwei wichtige Systeme auszuschalten: den digitalen Steuerdienst sowie das IT-System der Zollkontrolle.[20]

Es gibt Spekulationen darüber, dass Conti Hilfe durch Insider gehabt haben könnte. Tatsächlich hieß es in einer der Nachrichten, die von der Gruppe nach dem Angriff im Dark Web veröffentlicht wurden, dass „Insider in der Regierung [von Costa Rica]“ Hilfe geleistet hatten. Dieser Bedrohungsakteur wurde als „UNC1756“ bezeichnet.[21]

Die Gruppe Hive wiederum nutzt für ihre Angriffe ein Ransomware-as-a-Service-Modell (RaaS). Dabei versenden die Gruppe und ihre Partner Phishing-E-Mails mit schädlichen Anhängen, suchen nach VPN-Anmeldedaten und nutzen anfällige RDP-Server (Remote Desktop Protocol), um sich lateral innerhalb des kompromittierten Netzwerks zu bewegen. Laut einem FBI-Ratgeber zu Hive exfiltriert die Gruppe typischerweise Daten und verschlüsselt Dateien im Netzwerk. Anschließend hinterlässt sie eine Lösegeldforderung in jedem betroffenen Verzeichnis auf dem angegriffenen System. Die Nachricht enthält ausführliche Anweisungen für den Kauf der Entschlüsselungssoftware und droht damit, exfiltrierte Daten des Opfers auf der Tor-Website „HiveLeaks“ zu veröffentlichen.[22]

Einige Cybersicherheitsexperten gehen davon aus, dass bei beiden Ransomware-Angriffen im Frühjahr die gleichen Cyberkriminellen involviert waren. Sie vermuten, dass Hive die Kampagne nutzte, um Conti einen Neustart und die Umgehung internationaler Sanktionen zu ermöglichen, die Lösegeldzahlungen in Ländern verbieten, die solche Aktivitäten tolerieren oder direkt unterstützen.[23] Hive behauptet auf der eigenen Website, dass keine Verbindungen zu Conti bestehen.[24]

Das Ergebnis

In Folge des ersten Ransomware-Angriffs Mitte April verlor die Wirtschaft von Costa Rica etwa 30 Millionen US-Dollar pro Tag. Während der chaotischen Behebungsphase musste die Regierung viele kritische Systeme herunterfahren. Die Außenhandelskammer von Costa Rica schätzte den Schaden allein in den ersten zwei Tagen auf über 125 Millionen US-Dollar.[25]

19 Ionut Ilascu *(BleepingComputer)*: „How Conti Ransomware Hacked and Encrypted the Costa Rican Government“ (Wie Conti die Regierung von Costa Rica hackte und verschlüsselte), 21. Juli 2022.

20 Matt Burgess *(Wired)*: „Conti’s Attack Against Costa Rica Sparks a New Ransomware Era“ (Conti-Angriff gegen Costa Rica beginnt ein neues Ransomware-Zeitalter), 12. Juni 2022.

21 Claudia Glover *(Tech Monitor)*: „’We will overthrow the government’ – Does Conti have help inside Costa Rica?“ (Wir werden die Regierung stürzen – hatte Conti Insider-Hilfe in Costa Rica?), 17. Mai 2022.

22 FBI FLASH-Bericht: „Indicators of Compromise Associated with Hive Ransomware“ (Kompromittierungsindikatoren der Hive-Ransomware), 25. August 2021.

23 KrebsOnSecurity: „Costa Rica May Be Pawn in Conti Ransomware Group’s Bid to Rebrand, Evade Sanctions“ (Costa Rica könnte von Conti-Ransomware-Gruppe für Neuaufstellung missbraucht werden, um Sanktionen zu umgehen), 31. Mai 2022.

24 ebd.

25 Carla Rosch *(Rest of World)*: „A Massive Cyberattack in Costa Rica Leaves Citizens Hurting“ (Massiver Cyberangriff in Costa Rica führt zu Schäden im ganzen Land), 1. Juni 2022.

Zudem musste die Regierung Webseiten der angegriffenen Behörden vom Netz nehmen. Sie forderte auch technische Hilfe von anderen Staaten wie den USA sowie von Technologieunternehmen wie Microsoft an. Die US-Regierung ging sogar noch weiter und lobte 5 Millionen US-Dollar für Informationen aus, die zur Verhaftung oder Verurteilung von Beteiligten an einem Conti-Ransomware-Angriff führen.[26]

Anfang Mai rief Rodrigo Chaves Robles, der neue Präsident von Costa Rica, den nationalen Cybersicherheitsnotstand aus und bezeichnete die Conti-Attacke als Terrorakt. Wenige Wochen später startete die Gruppe Hive ihren Angriff.

Die Regierung von Costa Rica war wochenlang mit der Behebung der Folgen beschäftigt. Erst Mitte Juni konnten einige Behörden ihren Betrieb wieder aufnehmen.

Ransomware: potenzielle Konsequenzen

Geschäfts-unterbrechung

Finanzielle Schäden (durch Lösegeldzahlung und Behebungsmaßnahmen)

Datenverlust (wenn die Angreifer die Drohung zur Veröffentlichung von Daten bei Nichtzahlung des Lösegeldes wahr machen)

So hätten Schulungen zur Sensibilisierung geholfen

Einige Berichte legen nahe, dass der Ransomware-Angriff auf Costa Rica möglicherweise Hilfe durch böswillige Insider erhalten hatte. Viele Ransomware-Infektionen sind jedoch ein Nebenprodukt früherer E-Mail-Kompromittierungen. Die Angreifer nutzen Techniken wie Phishing, um Anmeldeinformationen zu stehlen, die Zugang zu kritischen Systemen gewähren.

Die Schulung von Anwendern zum Erkennen und Melden verdächtiger E-Mails, besonders in Verbindung mit automatisierten Closed-Loop-Analysen, kann die Risiken durch Ransomware und andere Malware-Typen erheblich verringern.

Anwender sollten Dateianhängen und URLs instinktiv misstrauen, insbesondere in E-Mails, die natürliche Regungen wie die Suche nach persönlichen Vorteilen, Neugier, Angst, Empörung und sogar Hilfsbereitschaft ausnutzen. Und sie sollten die Anzeichen dafür kennen, dass die Absender unter falscher Flagge segeln.

26 Elizabeth Montalbano *(Threatpost)*: „Conti Ransomware Attack Spurs State of Emergency in Costa Rica“ (Notstand in Costa Rica nach Conti-Ransomware-Angriff), 10. Mai 2022.

ABSCHNITT 4

Cloud-Angriffe und Kontoübernahmen

Die Angreifer folgen Anwendern stets auf dem Fuße – und deren Weg führt immer häufiger in die Cloud. Die COVID-19-Pandemie hat den Wechsel in die Cloud beschleunigt und dementsprechend Cloud-Angriffe immer häufiger werden lassen. Wie unser Bericht *Der Faktor Mensch 2022* erklärt, wird Cloud-Kontenkompromittierung ebenso wie Phishing und Malware auf Dauer eine feste Größe unter den Cyberbedrohungen bleiben.

Bei Cloud-Kontenkompromittierung erlangen Angreifer illegal die Kontrolle über das legitime Cloud-E-Mail- oder Dienst-Konto eines Anwenders. Durch diese Cloud-Kontoübernahmen können Angreifer weitreichenden Zugriff auf Anwenderdaten, Kontakte, Kalendereinträge, E-Mails und andere System-Tools erlangen. Mithilfe von Single Sign-On-Authentifizierung können sich Bedrohungsakteure ungehindert zwischen vielen verschiedenen Systemen in der Umgebung bewegen und erhebliche Schäden anrichten.

Zur Kompromittierung von Cloud-Konten und deren Übernahme nutzen die Angreifer meist folgende Methoden:

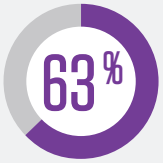
- Brute-Force-Angriffe, bei denen die Anmeldedaten automatisiert „erraten“ werden
- Phishing-Angriffe, einschließlich OAuth-Token-Phishing
- Wiederverwendung von Anmeldedaten, wobei zuvor gestohlene Benutzernamen- und Kennwort-Paare verwendet werden
- Malware wie Keylogger-Programme und Anmeldedaten-Diebe

Eine weitere wichtige Komponente von Cloud-Kontenkompromittierungen ist Persistenz, also die Etablierung von dauerhaftem Zugriff.

Trends

Unsere Daten aus dem Bericht *Der Faktor Mensch 2022* zeigen, dass jeden Monat mehr als 90 % der überwachten Cloud-Mandanten angegriffen wurden. Etwa ein Viertel (25 %) der Angriffe war erfolgreich – und insgesamt wurden fast zwei Drittel der Mandanten (63 %) im Laufe des Jahres kompromittiert.[27]

der überwachten Angriffe auf Cloud-Mandanten waren erfolgreich



der Cloud-Mandanten wurden 2021 kompromittiert

Cloud-Kontoübernahmen lassen sich oft nur schwer aufdecken sowie stoppen und können mit hohen Kosten verbunden sein. Wie eine aktuelle Untersuchung zeigte, liegt der durchschnittliche finanzielle Verlust für Unternehmen aufgrund kompromittierter Cloud-Konten bei 6,2 Millionen US-Dollar. Ebenso verzeichnen Unternehmen dadurch im Durchschnitt Anwendungsausfälle von insgesamt 138 Stunden.[28]

Schädliche Cloud-Anwendungen

Für das Problem schädlicher Cloud-Anwendungen ist zum Teil auch Schatten-IT verantwortlich. Externe Cloud-Anwendungen integrieren sich in einen Cloud-Dienst, werden jedoch nicht vom Cloud-Anbieter bereitgestellt. Diese Anwendungen nutzen das Autorisierungsprotokoll OAuth, das eingeschränkten Zugriff auf einen Cloud-Dienst erlaubt. Durch OAuth können externe Anwendungen auf Kontoinformationen und Daten von Nutzern zugreifen, ohne dafür Anmeldedaten zu verwenden.[29]

Das erscheint alles sehr komfortabel und sicher, doch externe Anwendungen lassen sich leicht ausnutzen. Bei der Installation akzeptieren Anwender häufig die angeforderten Berechtigungen, ohne sich diese genau anzusehen. Sobald Angreifer OAuth-Zugriffsrechte erlangt haben, können sie diese zur Kompromittierung und Übernahme von Cloud-Konten nutzen – und erhalten so lange Zugriff auf die Anwenderkonten und -daten, bis das OAuth-Token explizit gesperrt wird.

27 Proofpoint: „Der Faktor Mensch 2022“, Mai 2022.

28 Ponemon Institute: „Cost of Cloud Compromise and Shadow IT“ (Kosten durch Cloud-Kompromittierung und Schatten-IT), April 2021.

29 Proofpoint: „Was Sicherheitsexperten über Drittanbieter-OAuth-Apps wissen sollten“, Mai 2022.

Schädliche Dateien aus der Cloud

Sobald ein Angreifer ein Cloud-Konto übernommen hat, stehen ihm weitere Möglichkeiten für schädliche Aktivitäten zur Verfügung, beispielsweise Datendiebstahl oder Überweisungsbetrug. Beim Phishing mit Microsoft SharePoint lädt der Angreifer beispielsweise schädliche Dateien in ein kompromittiertes Cloud-Konto hoch. Die Freigabeberechtigungen sind auf „Öffentlich“ gesetzt, sodass der neue anonyme Link beliebig geteilt werden kann, sei es per E-Mail oder durch das Weitergeben an Kontakte des betroffenen Anwenders bzw. andere Ziele. Wenn diese Empfänger die Datei öffnen und auf den schädlichen Link klicken, werden sie zu Phishing-Opfern.[30]

Vor Kurzem deckten unsere Bedrohungsforscher eine gänzlich neue Spielart von Cloud-Angriffen auf. Dabei nehmen die Angreifer Daten in der Cloud ins Visier und führen Ransomware-Attacken mithilfe der Cloud-Infrastruktur durch. Zudem kompromittieren sie beliebte geschäftliche Cloud-Anwendungen wie SharePoint Online und OneDrive innerhalb der Microsoft 365-Suite.[31]

Obwohl schädliche Dateien aus der Cloud eine echte Gefahr darstellen, zeigte der *State of the Phish 2022*-Bericht, dass nur 37 % der Anwender sich dessen bewusst sind.

Reales Beispiel: OiVaVoii-Kampagne

Die Cloud kann die Zusammenarbeit und Datenweitergabe erheblich erleichtern. Gleichzeitig stellt sie jedoch auch eine komplexe Bedrohungsumgebung dar, die durch die digitale Transformation und den Trend zu Homeoffice und Hybrid-Arbeit schnell wächst.

Eine aktuelle Kampagne, die gegen lukrative Anwender wie Führungskräfte gerichtet ist, zeigt deutlich, dass Zugriffsrechte für Cloud-Anwendungen bei Mitarbeitern aller Unternehmensebenen ein Risiko darstellen. Das gilt auch für Anwendungen, die harmlos wirken und aus legitimen Quellen zu stammen scheinen.

30 Itir Clarke, Eilon Bendet und Doyle Groves *(Proofpoint)*: „Why OneDrive and SharePoint Attacks Are Successful and How to Fight Back“ (Warum sind OneDrive- und SharePoint-Angriffe erfolgreich und wie lässt sich das verhindern), Oktober 2020.

31 Or Safran, David Krispin, Assaf Friedman und Saikrishna Chavali *(Proofpoint)*: „Proofpoint Discovers Potentially Dangerous Microsoft Office 365 Functionality that can Ransom Files Stored on SharePoint and OneDrive“ (Proofpoint deckt potenziell gefährliche Microsoft Office 365-Funktion auf, die Lösegelddateien in SharePoint und OneDrive speichern kann), Juni 2022.

Vorgehensweise

Im Januar 2022 beobachteten unsere Forscher zum ersten Mal die schädliche Hybrid-Cloud-Kampagne OiVaVoii und deckten fünf schädliche damit verbundene OAuth-Anwendungen auf.[32]

Mindestens drei der schädlichen externen Anwendungen wurden von zwei unterschiedlichen „verifizierten Drittanbietern“ entwickelt. Es ist anzunehmen, dass diese Anbieter Administratorkonten legitimer Microsoft 365-Mandanten kompromittiert hatten. Mindestens eine der beiden anderen Anwendungen wurde von einem nicht verifizierten Drittanbieter erstellt. Das deutet darauf hin, dass die Angreifer eine gekaperte Cloud-Umgebung oder einen dedizierten böswilligen Microsoft 365-Mandanten genutzt haben.

Das Ergebnis

Nach der Erstellung der Anwendungen sendeten die Angreifer E-Mails mit Autorisierungsanfragen an verschiedene Nutzer, darunter auch hochrangige Führungskräfte. Viele dieser Nutzer autorisierten die Anwendungen. Mit dieser einfachen Methode konnten die Angreifer OAuth-Token im Namen der kompromittierten Nutzer erstellen und die Kontoübernahme abschließen.
Alle bei der OiVaVoii-Kampagne involvierten Anwendungen forderten ähnliche Berechtigungen von den Nutzern, insbesondere Lese- und Schreibzugriff auf das Postfach. Nach dem Akzeptieren der Anfragen konnten die Angreifer schädliche E-Mails intern sowie extern versenden, wertvolle Informationen stehlen und weitere Aktionen durchführen.

Cloud-Angriffe: potenzielle Konsequenzen

Kontoübernahmen

Datenverlust
(weil Malware in die Umgebung eindringt oder Daten direkt über schädliche Anwendungen abgesaugt werden)

Geschäftsunterbrechung
(durch Ransomware und andere Malware, die in die Umgebung eindringt)

So hätten Schulungen zur Sensibilisierung geholfen

Wie auch die meisten E-Mail-Angriffe benötigen Cloud-basierte Angriffe menschliche Interaktionen, also die Preisgabe von Anmeldedaten, die Installation schädlicher Anwendungen und Klicks auf Links zu vertrauenswürdigen File-Sharing-Websites, die schädliche Dateien hosten.

Die Schulung Ihrer Mitarbeiter zur sicheren Nutzung von Cloud-Diensten sowie zur Vorsicht bei der Autorisierung unbekannter Anwendungen sollte fester Bestandteil Ihres Security-Awareness-Programms sein.

32 Eilon Bendet, Assaf Friedman und David Krispin *(Proofpoint)*: „OiVaVoii – An Active Malicious Hybrid Cloud Threats Campaign“ (OiVaVoii – Eine aktive schädliche Hybrid-Cloud-Kampagne), Januar 2022.

Warum mehrstufige Authentifizierung kein Allheilmittel ist

Viele sicherheitsbewusste Unternehmen schulen ihre Mitarbeiter zur Nutzung von mehrstufiger Authentifizierung (MFA) als Mittel zur Absicherung von Anwenderkonten. MFA ist eine weitere Sicherheitsebene zum Schutz von Konten, wenn Angreifer versuchen, sich mit gestohlenen Anmeldedaten anzumelden. Bei der Anmeldung werden die Anwender aufgefordert, nicht nur Nutzernamen und Kennwort anzugeben, sondern auch einen Code, den sie per Telefon, über ein externes Gerät oder einen physischen Sicherheitsschlüssel erhalten. Dank MFA lässt sich die Gefahr erheblich verringern, dass Angreifer Konten allein mithilfe gestohlener Anmeldedaten übernehmen können. Deshalb sollte mehrstufige Authentifizierung fester Bestandteil jedes Sicherheitsprogramms sein.

MFA ist jedoch nicht unüberwindbar. Anwenderfreundliche Phishing-Kits erleichtern den Angreifern die Umgehung dieser Sicherheitsmaßnahmen. Nach Angaben von Microsoft konnten Bedrohungsakteure seit September 2021 die MFA bei Angriffen auf mehr als 10.000 Unternehmen unterlaufen. Nachdem die Angreifer Zugriff erlangt hatten, konnten sie mithilfe kompromittierter Konten ihre BEC-Angriffe durchführen.[33]

Diese Angriffe beginnen meist mit einer Phishing-E-Mail, daher sind Schulungen wichtig, in denen Ihre Anwender lernen, verdächtige Nachrichten zu erkennen und zu melden. Beim Microsoft-Angriff enthielten die Phishing-E-Mails einen HTML-Anhang. Sobald dieser geöffnet wurde, leitete er die Anwender an einen Proxy-Server um, der den Datenverkehr zwischen den Anwendern und dem Anmeldebildschirm erfasste.

Zudem sollten Anwender wissen, dass sie niemals Dateianhänge unbekannter Absender öffnen dürfen. Dies gilt insbesondere für Dateitypen, die normalerweise nicht per E-Mail versendet werden.

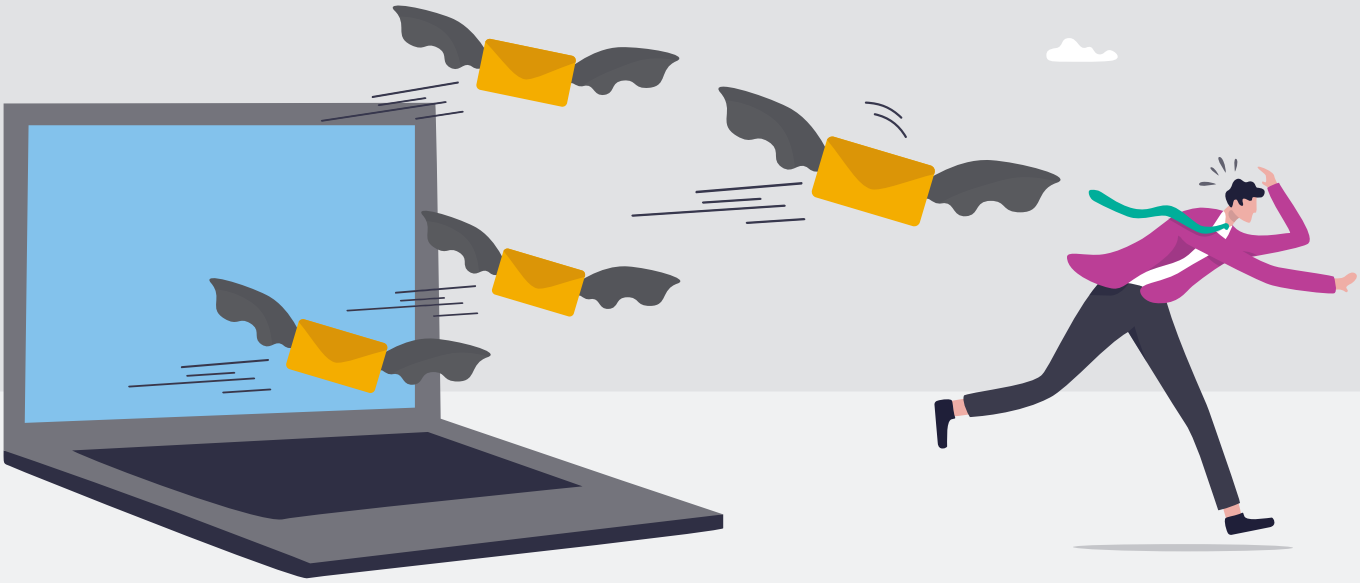
33 Microsoft: „From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud“ (Von Cookie-Diebstahl zu BEC: Angreifer nutzen AiTM-Phishing-Websites als Einfallstor für Finanzbetrug), Juli 2022.

ABSCHNITT 5

Webbasierte E-Mail-Angriffe

Der Trend zur Arbeit im Homeoffice bietet Cyberkriminellen noch mehr Gelegenheiten, Zugang zu Unternehmenssystemen zu erlangen. Die meisten Angestellten nutzen für die Telearbeit ein VPN (virtuelles privates Netzwerk), das sicheren Zugriff auf das Firmennetzwerk erlaubt, wenn sie mit ihren privaten Geräten von zu Hause arbeiten. Mit diesen privaten Geräten greifen sie auch auf ihre privaten webbasierten E-Mail-Konten zu. Gleichzeitig nutzen viele Angestellte unternehmenseigene Geräte für den Zugriff auf ihre privaten Konten.

Wenn es Angreifern gelingt, nicht arbeitsbezogene Konten von Anwendern zu kompromittieren, können sie dort Anmeldedaten für unternehmenseigene Anwendungen, Daten und Systeme finden. Ebenso können sie ausnutzen, dass viele Angestellte ihre privaten E-Mail-Konten oder Mobiltelefonnummern für die Zwei-Faktor-Authentifizierung oder Kennwortrücksetzungen nutzen. Mithilfe dieser Informationen können die Angreifer ohne große Mühe Zugang zu Unternehmensnetzwerken erlangen.

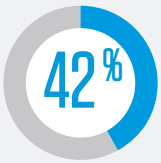


Trends

Wie Daten aus unserem *State of the Phish 2022*-Bericht zeigen, sind viele Anwender durch Webmail-Angriffe gefährdet, die ihren Unternehmen Schaden zufügen können.

Außerdem scheinen viele Arbeitnehmer zu glauben, dass ihre Webmail-Anbieter sie vor diesen Angriffen schützen.

Unsere Untersuchung hat Folgendes gezeigt:



der Anwender nutzen private E-Mails auf unternehmenseigenen Geräten

der Anwender wissen, dass ihre Anbieter für private E-Mails nicht alle gefährlichen Nachrichten blockieren können

Reales Beispiel: LAPSUS$

Manchmal steht bei Cyberangreifern nicht das Geld an erster Stelle, sondern das Anrichten von Chaos und die damit verbundene Aufmerksamkeit. Ein Beispiel dafür ist die Gruppe LAPSUS$, die Ende 2021 auftauchte und sich auf Datendiebstahl sowie Erpressung spezialisiert hat. Obwohl mehrere ihrer Mitglieder (alle im Alter von 16 und 21 Jahren) im März von der britischen Polizei verhaftet wurden, könnte die Cybercrime-Gruppe immer noch aktiv sein.[34]

Vorgehensweise

Innerhalb weniger Monate versuchte die LAPSUS$-Gruppe, das brasilianische Gesundheitsministerium zu erpressen und veröffentlichte Screenshots interner Tools, die zu NVIDIA, Samsung und Vodafone gehören.[35] Bemerkenswert war dabei der unkonventionelle Erpressungsansatz. Die Gruppe exfiltrierte vertrauliche Daten und drohte anschließend damit, sie bei Nichtzahlung des Lösegeldes online zu veröffentlichen. Im Grunde handelte es sich also um einen Ransomware-Angriff – nur ohne Ransomware.

Das Ergebnis

Die Gruppe ging dabei so dreist vor, dass sie Nutzer in der Telegram-App darüber abstimmen ließ, welche Daten des Opfers sie als Nächstes veröffentlichen sollte.[36] Um Zugang zu den jeweiligen Unternehmensnetzwerken zu erlangen, sah sich die LAPSUS$-Gruppe häufig in privaten E-Mail-Konten der Angestellten nach Anmeldedaten und Remote-Zugriffssystemen um.[37]

34 Scott Ikeda *(CPO Magazine)*: „Suspected Lapsus$ Hackers Arrested; London Group Between the Ages of 16 and 21“ (Mutmaßliche Lapsus$-Hacker verhaftet; Londoner Gruppe im Alter zwischen 16 und 21 Jahren), März 2022.

35 KrebsOnSecurity: „A Closer Look at the LAPSUS$ Data Extortion Group“ (Ein genauer Blick auf die Datenerpressergruppe LAPSUS$), März 2022.

36 Lily May Newman *(Wired)*: „The Lapsus$ Hacking Group Is Off to a Chaotic Start“ (Die Hackergruppe Lapsus$ legt einen chaotischen Start hin), März 2022.

37 Microsoft: „DEV-0537 criminal actor targeting organizations for data exfiltration and destruction“ (Bedrohungsakteur DEV-0537 attackiert Unternehmen mit Datenexfiltration und -zerstörung), März 2022.

Microsoft Security bezeichnete die LAPSUS$-Gruppe als „DEV-0537“.

„Im Gegensatz zu den meisten Cybercrime-Gruppen, die unter dem Radar bleiben, scheint DEV-0537 nicht sehr daran gelegen zu sein, seine Spuren zu verwischen“, so der Software-Gigant. „Die Gruppe geht sogar so weit, dass sie in sozialen Netzwerken ihre Angriffe bekannt gibt oder ihre Absicht verkündet, Anmeldedaten für Unternehmen zu kaufen, die sie im Visier hat.“[38]

Die „Werbung“ der Gruppe umfasste Telegram-Nachrichten, in denen LAPSUS$ Mitarbeiter und andere Insider bei Telekommunikationsunternehmen, großen Software- und Spiele-Entwicklern, Callcenter-Betreibern und Server-Hostern anzuwerben versuchte. Ihr Ziel dabei: Angestellte zu bestechen, um ihre VPN-Anmeldedaten oder eine andere Form von Remote-Zugang zu erhalten. Außerdem bot LAPSUS$ kooperierenden Insidern auch Geldzahlungen an. Eine der Werbebotschaften sprach von der Möglichkeit, in einer Woche 20.000 US-Dollar und mehr zu verdienen.[39]

Microsoft Security berichtete auch, dass LAPSUS$ mit anderen Mitteln Erstzugang zu seinen Opfern erlangte, beispielsweise durch den Kauf von Anmeldedaten und Sitzungs-Token in kriminellen Untergrundforen. Eine weitere Methode war die Suche nach Anmeldeinformationen in öffentlichen Code-Repositorys.

Webmail-Angriffe: potenzielle Konsequenzen

Datenverlust | Geschäfts-unterbrechung | Finanzielle Verluste | Rufschädigung

So hätten Schulungen zur Sensibilisierung geholfen

Die LAPSUS$-Gruppe nutzte unter anderem folgende Methoden:

- Kompromittierung von Webmails und Remote-Zugriffsmethoden
- Anwerbung von Insidern bei Unternehmen, Lieferanten oder Geschäftspartnern
- Diebstahl von vertraulichen Daten und geistigem Eigentum
- Lösegeldforderungen

Viele erfolgreiche Infektionen wären vermieden worden, wenn die Anwender gewusst hätten, wie sie ihre Anmeldedaten schützen, private E-Mails sicher nutzen und Lösegeldforderungen melden können.

38 ebd.

39 KrebsOnSecurity: „A Closer Look at the LAPSUS$ Data Extortion Group“ (Ein genauer Blick auf die Datenerpressergruppe LAPSUS$), März 2022.

ABSCHNITT 6

Schlussfolgerungen und Empfehlungen

Die Herausforderung besteht darin, dass Sie den besten Weg finden müssen, um Ihre Anwender über die dynamische Bedrohungslandschaft auf dem Laufenden zu halten. Letztendlich sollen sie motiviert werden, in Bezug auf Cyberbedrohungen ebenso wachsam zu sein wie Ihre Sicherheitsteams und dadurch zu proaktiven Verteidigern zu werden.

Damit Schulungen für das Sicherheitsbewusstsein funktionieren, müssen Ihre Anwender die Antworten den Grund kennen: Warum sollten sie sich um Cyberbedrohungen kümmern? Warum tragen auch sie die Verantwortung für den Schutz ihres Unternehmens? Die kurze Antwort ist: Sie sind der neue Perimeter. Und wenn das Unternehmen eine reale Chance haben soll, raffinierte Cyberangreifer auf Abstand zu halten, muss es einen personenzentrierten Sicherheitsansatz implementieren.

Die fünf Arten von Cyberbedrohungen sowie die Beispiele für Angriffe, die in diesem E-Book vorgestellt werden, haben eines gemeinsam: Sie sind gegen Menschen gerichtet. Die Angreifer sichern sich die – freiwillige oder unfreiwillige – Mithilfe der Anwender, um ihre Kampagnen voranzubringen und die Ziele zu erreichen.

Diese Bedrohungen und Zwischenfälle zeigen deutlich, dass Menschen bei den aktuellen Bedrohungen der wichtigste Faktor sind. Deshalb sollten Anwenderschulungen zur Steigerung des Sicherheitsbewusstseins zu den Hauptkomponenten Ihrer Cybersicherheitsstrategie gehören.

Auf das Wesentliche konzentrieren

Alle Mitarbeiter, die Einfluss auf die Cybersicherheitslage Ihres Unternehmens haben, sollten in den bewährten Methoden für Cybersicherheit geschult werden. Bei den Bewertungen und Schulungen Ihrer Mitarbeiter sollten Sie jedoch zielgerichtet und strategisch vorgehen.

Ebenso sollten Sie die Themen priorisieren, die für Ihre Branche und Ihr Unternehmen – und Ihre Mitarbeiter – relevant sind. Nutzen Sie die realen Beispiele aus diesem E-Book, um passend zu Ihrem Risikoprofil Zielgruppen anzusprechen, die wegen ihrer Tätigkeit, der beruflichen Position, ihres Arbeitsortes und der Arbeitsweise sowie anderer Faktoren sehr wahrscheinlich ähnliche Angriffe erleben werden.

Bedrohungsdaten zu Ihrem Vorteil nutzen

Bedrohungsdaten können Ihnen bei der Entscheidung helfen, wann Sie konkrete Anwender konkret schulen sollten. Um die Erkenntnisse über bekannte und neue Bedrohungen zu Ihrem Vorteil nutzen zu können, müssen Sie folgende Anwender identifizieren können:

Stark anfällige Anwender: Diese Anwender neigen dazu, auf simulierte Phishing-E-Mails zu klicken und nehmen nicht an Schulungen teil.

Häufig angegriffene Anwender: Diese Anwender werden mit zahlreichen zielgerichteten sowie raffinierten Angriffen attackiert.

Anwender mit umfangreichen Zugriffsrechten: Diese Anwender haben Zugriff auf wertvolle Daten, Systeme und andere kritische Ressourcen, die das Unternehmen schützen muss.

Kurz gesagt ist für einen erfolgreichen personenzentrierten Sicherheitsansatz notwendig, dass Sie jederzeit wissen, welche Mitarbeiter und Abteilungen in Ihrem Unternehmen angegriffen werden. Es bedeutet auch, dass Sie die Methoden der Angreifer zur Kompromittierung Ihrer Anwender und der Umgebung kennen.

Kontinuierlich wichtige Security-Awareness-Kennzahlen zur Ermittlung des Erfolgs auswerten

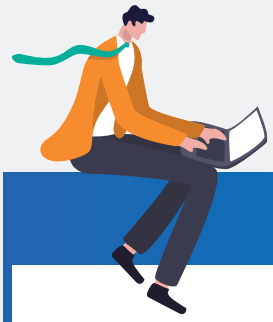
Für die Ermittlung des Erfolgs Ihrer Schulungen sollten Sie nicht nur eine einzige Kennzahl heranziehen (z. B. die Fehlerquote bei den Phishing-Tests). Um den „Erfolg“ zu ermitteln, sollten Sie mehrere Komponenten heranziehen und auch unternehmensspezifische Faktoren berücksichtigen.

Folgende Kennzahlen sind nützlich:

- Fehlerquoten bei Phishing-Simulationen
- Berichte zu Phishing-Simulationen
- Wissenstests
- Richtigkeit gemeldeter E-Mails
- Teilnahme an Schulungen

Ein letzter Tipp: Vergessen Sie nicht, dass Ihre Security-Awareness-Schulungen mit den dynamischen Bedrohungen Schritt halten müssen. Und bedenken Sie, dass es auch in Ihrem Unternehmen ständig Veränderungen gibt. Achten Sie daher darauf, dass die vermittelten Informationen für die Anwender relevant sind. Die oben genannten Kennzahlen können helfen, die Effektivität Ihres Programms zu ermitteln und Anpassungen vorzunehmen.

Für weitere Informationen zur Verbesserung Ihrer Security-Awareness-Schulungsprogramme laden Sie den *State of the Phish 2022*-Bericht von Proofpoint herunter.

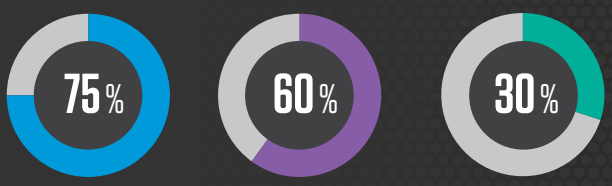


Vorteile von Proofpoint

Wir analysieren täglich mehr als:

2,6 Mrd. E-MAILS	**49 Mrd.** URLs	**1,9 Mrd.** ANHÄNGE
1,7 Mrd. MOBILGERÄTE-NACHRICHTEN	**430 Mio.** WEB-DOMAINS	**143.000** SOCIAL-MEDIA-KONTEN

Auf unsere Lösungen vertrauen mehr als:



DER FORTUNE 100 | DER FORTUNE 1000 | DER FORTUNE GLOBAL 2000

8.000 GROSSUNTERNEHMEN

200.000 KLEINE UNTERNEHMEN

WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter **proofpoint.com.de**.
