E-BOOK

Die Cloud im Visier

Wie Cyberkriminelle Microsoft 365-Schwachstellen bei File-Sharing-Funktionen, Identitäten und die Lieferkette ausnutzen

proofpoint.

Einleitung

In der heutigen digitalen Zeit ist Microsoft 365 ein unverzichtbares Hilfsmittel für den Arbeitsalltag – und dadurch leider auch das primäre Ziel von Cyberkriminellen. Trotz der zahlreichen, in Microsoft 365 nativ vorhandenen Funktionen zur Abwehr von Cyberangriffen sind diese Tools aktuellen raffinierten Attacken einfach nicht gewachsen.

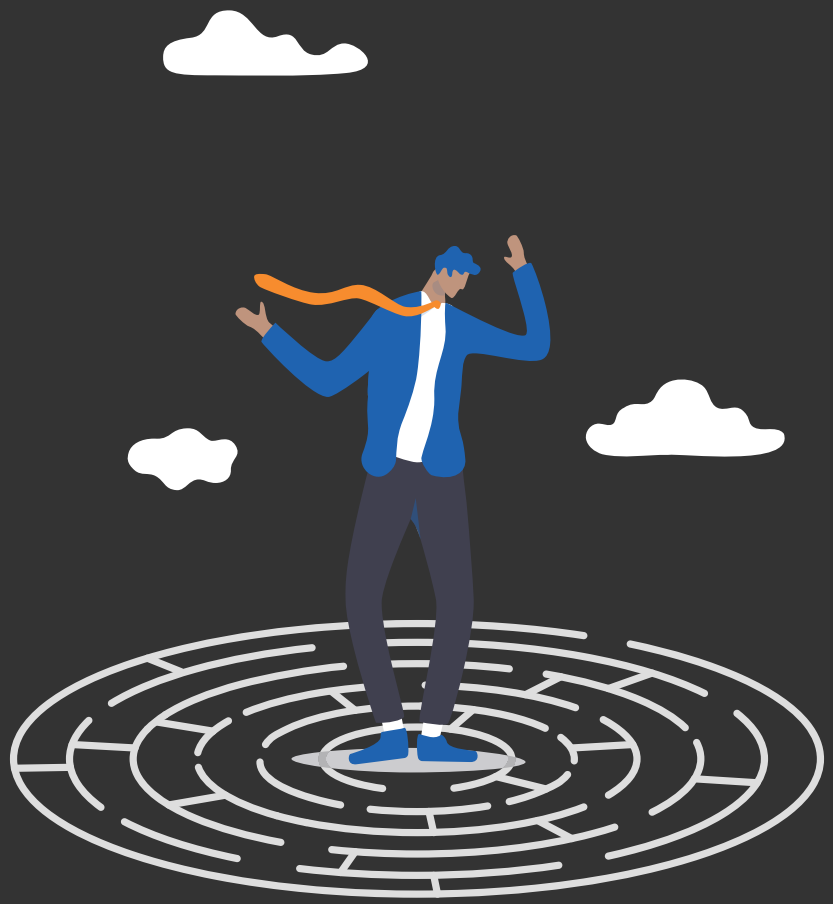
Jedes Jahr verursachen personenzentrierte Microsoft 365-Angriffe bei Unternehmen Kosten in Millionenhöhe und ärgern Sicherheitsteams ebenso wie Endnutzer. Mittlerweile betonen sogar Branchenexperten wie Gartner, dass die integrierten Cloud-Tools durch externe Lösungen ergänzt werden sollten.[1]

Der Grund: Cyberkriminelle werden immer besser darin, die Anwender selbst anzugreifen, sodass sich ihre Angriffe immer schwerer stoppen lassen.

Die Kompromittierung von Anwendern ist meist der erste Schritt in einer längeren Ereigniskette, die auch als „Cyber-Angriffskette“ bezeichnet wird. An deren Anfang steht die erfolgreiche Kompromittierung eines Anwenders. Anschließend folgen dann der Missbrauch von Berechtigungen, Datendiebstahl und weitere schädliche Aktivitäten.

Schritte in der Cyber-Angriffskette.

1 Gartner: „Market Guide for Email Security“ (Gartner Market Guide für E-Mail-Sicherheit), Februar 2023.



Dieses E-Book stellt die fünf Arten personenzentrierter Angriffe vor, mit denen Cyberkriminelle einen Fuß in die Tür bekommen – und schwerwiegendere Kompromittierungen möglich machen. Diese Angriffsformen lassen sich allein mit den Funktionen von Microsoft 365 nur schwer erkennen:

1. Business Email Compromise (BEC)
2. Angriffe per Telefon (TOAD)
3. Manipulierte freigegebene Dateien
4. Kontoübernahmen
5. Kompromittierte Lieferantenkonten

Jeder Abschnitt zeigt die Vielfalt und Raffinesse dieser Angriffe anhand mehrerer Beispiele, die deutlich machen, dass Microsoft 365-Anwender ohne zusätzliche Sicherheitsmaßnahmen gegen einen fähigen Angreifer kaum eine Chance haben.

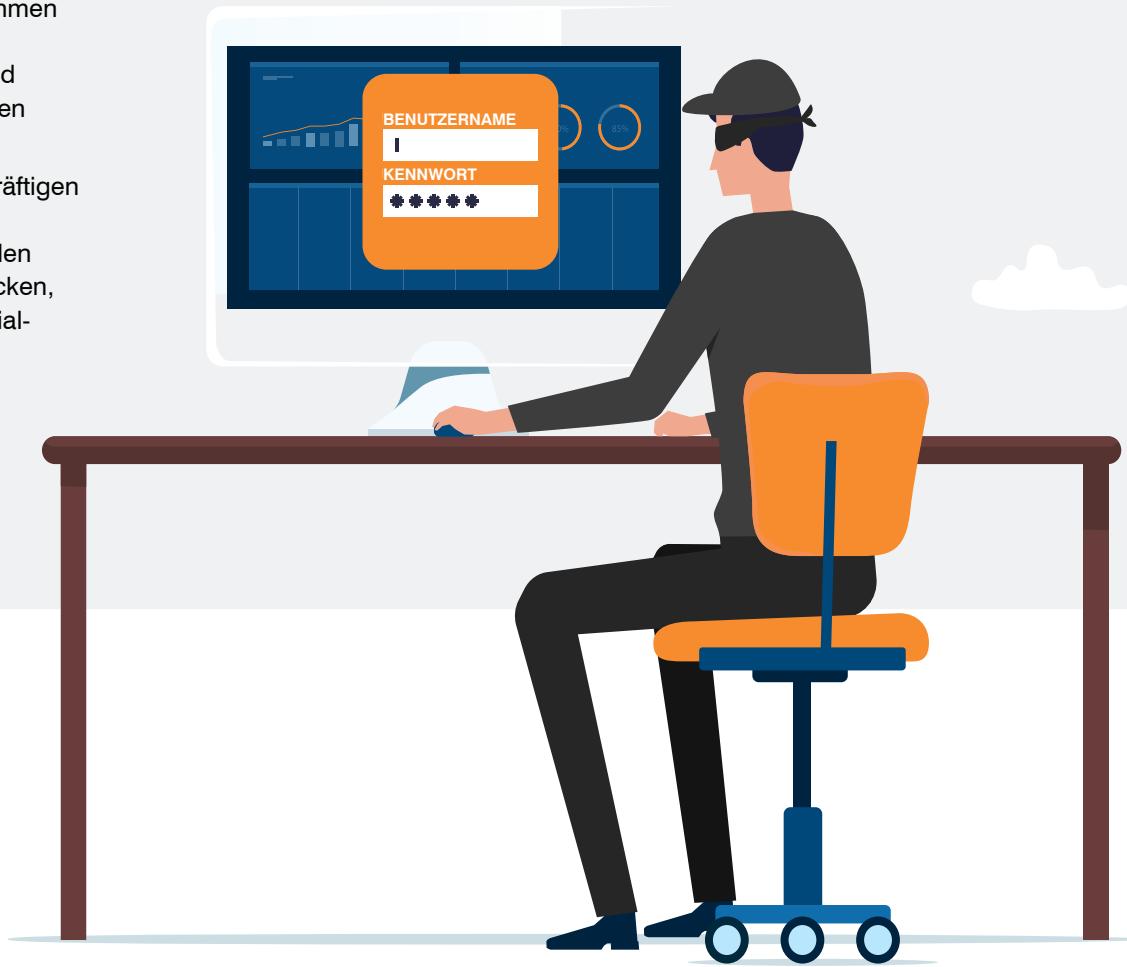
Alle diese Beispiele wurden von Proofpoint bei Risikoanalysen von Unternehmen aufgedeckt.

ABSCHNITT 1

BUSINESS EMAIL COMPROMISE

Business Email Compromise (BEC) ist eine der Angriffsformen, die bei Unternehmen aller Größen und Branchen die größten Schäden verursacht – und die Verluste wachsen von Jahr zu Jahr. 2022 stellte das FBI fest, dass Unternehmen aufgrund von BEC-Betrug 2,7 Milliarden US-Dollar eingebüßt hatten. Das sind 300 Millionen US-Dollar mehr als noch 2021.

Viele der aktuellen BEC-Taktiken sind äußerst raffiniert und werden von kapitalkräftigen Akteuren durchgeführt, die sehr viel Planung und Recherche in ihre Angriffe investieren. Die Angriffe lassen sich nur sehr schwer aufdecken, da die Kriminellen nicht die üblichen Schaddaten – schädliche URLs oder Dateianhänge – verschicken, die sich analysieren lassen. Stattdessen setzen sie auf Nachahmungs- und Social-Engineering-Techniken.



2 FBI: „2022 Internet Crime Report“ (Bericht zu Internetkriminalität 2022), 2023.

Umgebung:
Microsoft 365

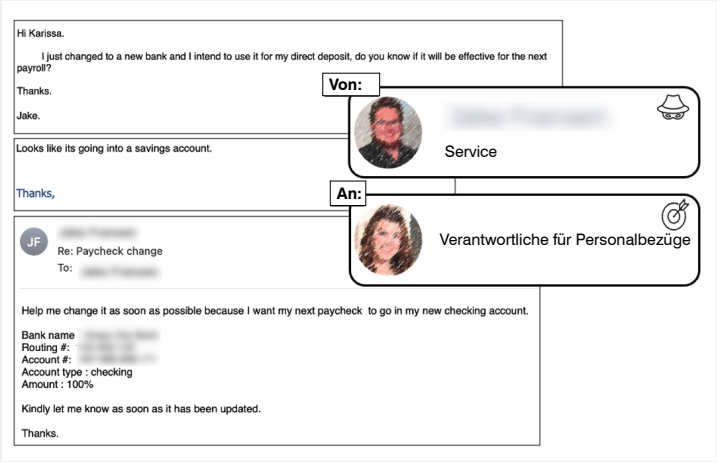
Bedrohungskategorie:
Social Engineering

Angriffstyp:
Umleitung von Gehaltszahlungen

Ziel:
Verantwortliche für Personalbezüge

Angriff mit Umleitung von Gehaltszahlungen

Umleitungen von Gehaltszahlungen sind E-Mail-Betrugsversuche, die sich meist gegen Angestellte in der Finanz-, Steuer-, Gehalts- und Personalabteilung richten. Bei diesen Angriffen bemühen sich die Bedrohungsakteure, das Vertrauen der Mitarbeiter zu erlangen, um Zahlungsdaten zu ändern und die Gehälter der Angestellten zu stehlen. Da bei dieser Angriffsart Social-Engineering-Taktiken angewandt werden, lassen sie sich nur sehr schwer erkennen. Umleitungen von Gehaltszahlungen werden als ein mittleres Risiko für Unternehmen eingestuft.



Beispiel eines Angriffs mit Umleitung von Gehaltszahlungen.

Bei diesem Angriff sendete ein Betrüger eine E-Mail an eine Verantwortlichen für Personalbezüge, wobei er ein Gmail-Konto nutzte und sich als Mitarbeiter ausgab, der seine Überweisungsdaten zu einem neuen Bankkonto geändert haben wollte. Hier tauschten der Betrüger und das Opfer sogar mehrere Nachrichten aus. Bei von Proofpoint durchgeführten Analysen sowie POCs (Proof of Concepts) zeigte sich, dass die integrierten E-Mail-Sicherheitskontrollen von Microsoft solche Angriffe nicht stoppen konnten.

Umgebung:
Microsoft 365

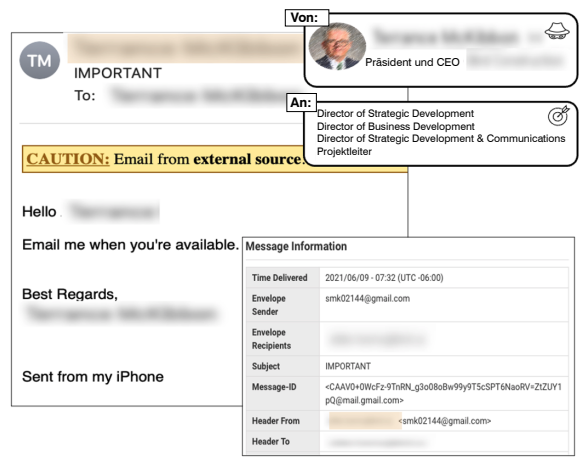
Bedrohungskategorie:
Social Engineering

Angriffstyp:
Nachahmung

Ziel:
Führungskräfte für strategische und geschäftliche Entwicklung

Angriff mit Nachahmung einer Führungskraft

Wenn sich ein Bedrohungsakteur erfolgreich als Mitarbeiter ausgibt, kann der Betrug das Unternehmen teuer zu stehen kommen. Doch wenn hochrangige Führungskräfte nachgeahmt werden, können die Folgen möglicherweise katastrophal sein. In den letzten Jahren haben solche Angriffe erheblich zugenommen: Seit März 2020 hat Proofpoint die Nachahmung von insgesamt mehr als 7.000 CEOs beobachtet. Dabei wurde mindestens bei der Hälfte aller Proofpoint-Kunden mindestens einmal das Konto einer hochrangigen Führungskraft für einen Betrugsversuch missbraucht.



Beispiel eines Angriffs mit Nachahmung einer Führungskraft.

In diesem Fall sendete ein Angreifer mehreren Angestellten E-Mails von einem Gmail-Konto. Dabei gab er sich als CEO aus und forderte sie zu einer Aktion auf. Hätten die Angestellten darauf geantwortet, wäre es dem Betrüger ein Leichtes gewesen, Daten zu extrahieren oder Gelder umzuleiten. Bei von Proofpoint durchgeführten Analysen sowie POCs zeigte sich, dass die integrierten E-Mail-Sicherheitskontrollen von Microsoft solche Angriffe nicht stoppen konnten.

Umgebung:
Microsoft 365

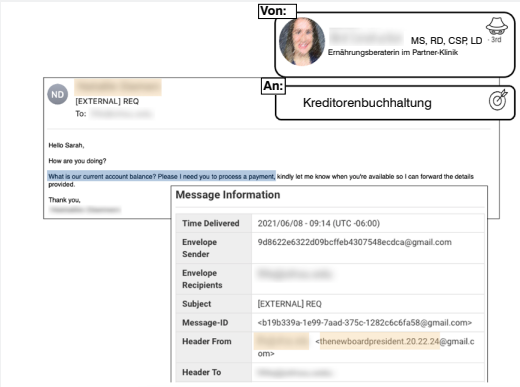
Bedrohungskategorie:
Social Engineering

Angriffstyp:
Rechnungsbetrug

Ziel:
Finanzabteilung

Angriff mit Lieferantenrechnungen

Einen Großteil der BEC-Angriffe gegen Verbraucher machen Betrugsversuche aus, die beispielsweise zum Kauf von Gutscheinkarten auffordern. Im Gegensatz dazu erfolgen BEC-Betrugsversuche gegen Lieferanten äußerst gezielt. Sie sind dadurch zwar seltener, führen jedoch oft zu weitaus größeren finanziellen Verlusten. Proofpoint konnte mehrere Betrugsversuche mit Lieferantenrechnungen stoppen, die bei den betroffenen Unternehmen jeweils Verluste in Millionenhöhe verursacht hätten. Bei solchen Angriffen senden Bedrohungsakteure ihren Opfern falsche Rechnungen oder neue Bankdaten, sodass die Gelder an ein von ihnen kontrolliertes Bankkonto überwiesen werden.



Beispiel für einen Betrugsversuch mit Lieferantenrechnungen.

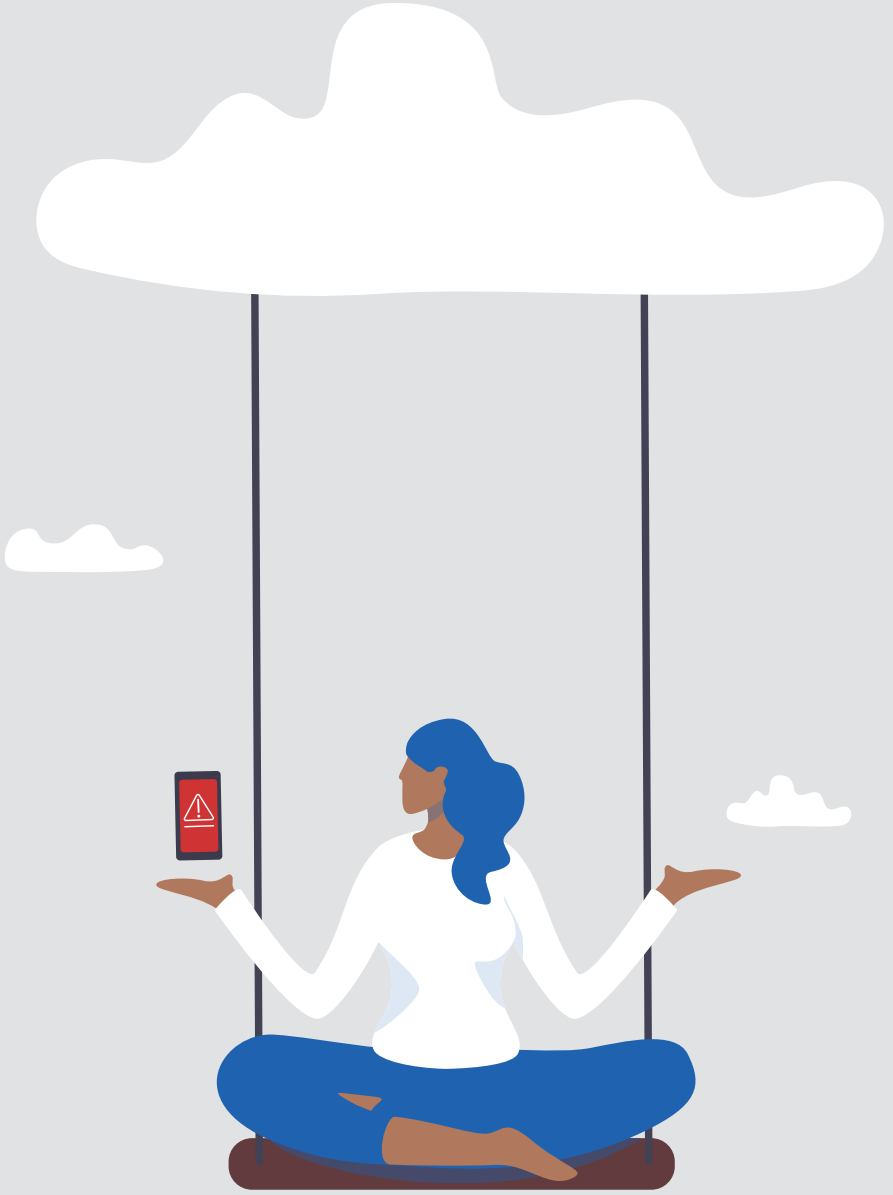
In diesem Fall gab der Angreifer sich als ehemaliger Mitarbeiter aus, der mittlerweile bei einem Partnerunternehmen arbeitete und um die Bearbeitung einer Rechnung bat. Die von einem Gmail-Konto gesendete E-Mail ging an die Finanzabteilung und entging den nativen E-Mail-Sicherheitskontrollen von Microsoft.

Häufig nutzen kriminelle Akteure für ihre Betrugsversuche Gmail oder andere kostenlose E-Mail-Services, da sie damit Authentifizierungsprüfungen wie Sender Policy Framework (SPF) und DomainKeys Identified Mail (DKIM) unterlaufen können. Die E-Mails enthalten teilweise auch schädliche URLs oder Anhänge, um an Finanzdaten und andere wertvolle Informationen zu gelangen.

ABSCHNITT 2

ANGRIFFE PER TELEFON

Bei Angriffen per Telefon (Telephone-Oriented Attack Delivery, TOAD) erhält das Opfer meist eine Nachricht mit einer gefälschten Rechnung oder wichtigen Benachrichtigung sowie einer Kundendienst-Telefonnummer, die im Falle von Fragen oder bei Fehlern angerufen werden soll. Die Telefonverbindung führt jedoch direkt zu einem Bedrohungsakteur. Im Jahr 2022 verzeichnete Proofpoint zu Spitzenzeiten mehr als 13 Millionen TOAD-Nachrichten pro Monat. Nachdem diese Technik 2021 zum ersten Mal beobachtet wurde, ist diese Zahl kontinuierlich gestiegen.[3]



3 Proofpoint: „Bericht: Der Faktor Mensch“, 2023.

Umgebung:
Microsoft 365

Bedrohungskategorie:
Social Engineering

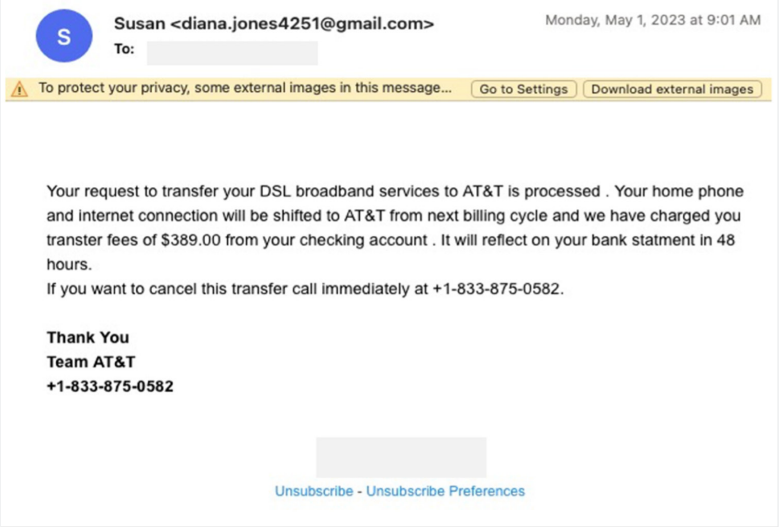
Angriffstyp:
TOAD

Ziel:
Microsoft 365-Nutzer

TOAD-Bedrohungen

E-Mail-Betrug, der durch Callcenter-Servicemitarbeiter unterstützt wird, ist sehr erfolgreich und profitabel. In vielen Fällen büßen die Opfer fünfstellige Beträge ein, die direkt von ihren Bankkonten gestohlen werden. Berichten zufolge wurden von 2021 bis 2022 insgesamt 68,4 Millionen US-Amerikaner mithilfe von Telefonbetrug um 39,5 Milliarden US-Dollar gebracht.[4]

Proofpoint beobachtet zwei Arten von Callcenter-Bedrohungsaktivitäten: Eine nutzt kostenlose und seriöse Remote-Zugriffs-Software, um Gelder zu stehlen, während die andere auf Malware setzt, die als Dokument getarnt ist und einen Computer kompromittieren soll, um die Infektion mit weiterer Malware zu ermöglichen.



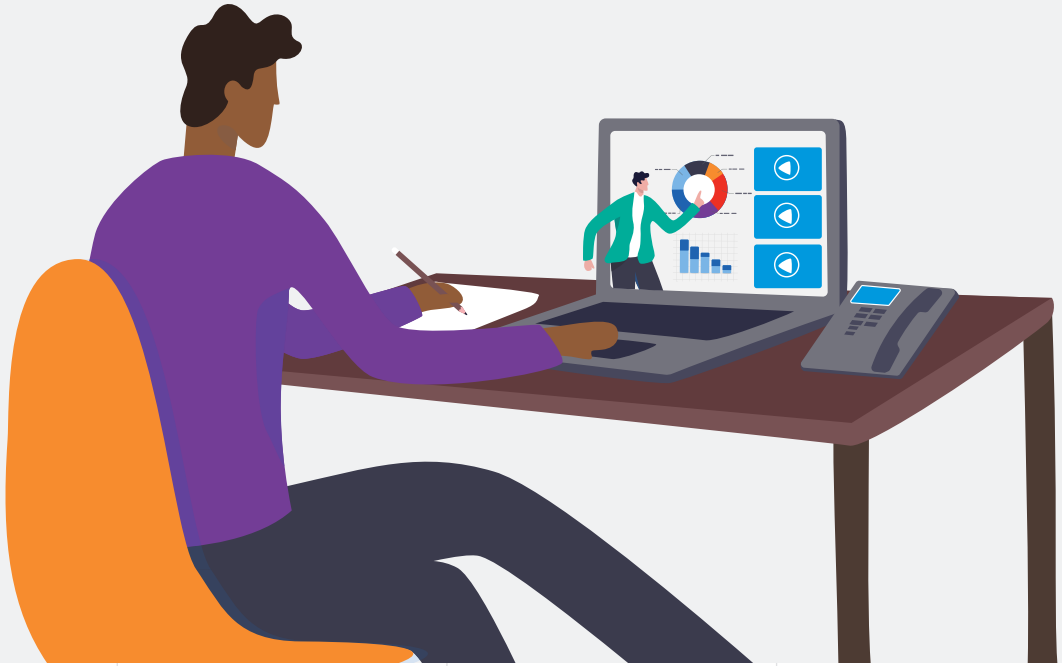
Beispiel eines TOAD-Angriffs.

4 Truecaller: „U.S. Spam & Scam Report“ (Bericht zu Spam und Betrugsversuchen in den USA), 2022.

Bei einem typischen Callcenter-Angriff erhält ein Anwender eine dringende Nachricht ähnlich der oben gezeigten E-Mail. Sie enthält häufig eine Rechnung für einen großen Kauf und stammt scheinbar von einem seriösen Unternehmen. Der Empfänger soll eine in der E-Mail angegebene Telefonnummer anrufen, um die Überweisung zu stornieren oder Widerspruch einzulegen.

Falls der Anwender dort anruft, leitet ihn ein Kundendienst-Vertreter per Telefon zu einer Website oder einem Mobilgeräte-App-Store. Proofpoint-Forscher haben verschiedene weitere Schritte beobachtet, z. B. sollen die Opfer dazu gebracht werden, Malware herunterzuladen, Gelder zu überweisen oder Remote-Zugriff zuzulassen.

Microsoft kann diese Nachrichten nicht erkennen, da sie keine Schaddaten oder gefährlichen URLs enthalten.



ABSCHNITT 3

MANIPULIERTE FREIGEGEBENE DATEIEN

Zu den häufigsten Angriffen mit schädlichen URLs gehören manipulierte freigegebene Dateien. Interne Proofpoint-Bedrohungsdaten zeigen, dass URLs drei Viertel der gesamten Cyberbedrohungen ausmachen. Bei mehr als 50 % dieser Angriffe kommen File-Sharing-URLs zum Einsatz.

Da Anwender Services wie Microsoft OneDrive und Microsoft SharePoint häufig einsetzen und ihnen deshalb grundsätzlich vertrauen, sind sie auch bei Angreifern sehr beliebt. Microsoft ist bei diesen Angriffen in einer besonderen Position: Der Anbieter hostet diese schädlichen Dateien nicht nur, er lässt auch zu, dass sie seine E-Mail-Sicherheitslösungen passieren.

Im Jahr 2021 stellten wir fest, dass bei mehr als 45 Millionen URL-basierten Bedrohungen, die an unsere Kunden gesendet wurden, die schädlichen Inhalte von Microsoft gehostet wurden.

Umgebung:
Microsoft 365

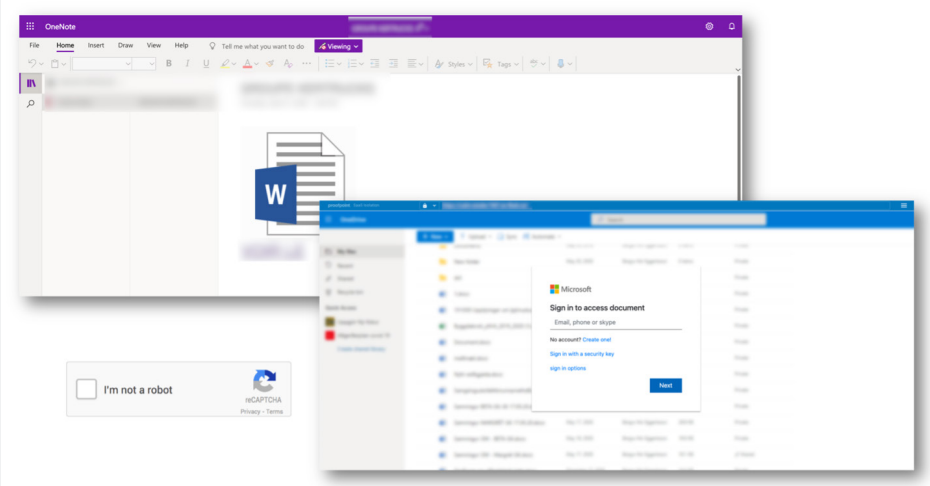
Bedrohungskategorie:
File-Sharing-URLs

Angriffstyp:
Anmeldedaten-Phishing

Ziel:
Anwender
mit gemeinsam
genutztem Postfach

Anmeldedaten-Phishing in OneNote

Laut Daten von Proofpoint setzen die Bedrohungsakteure im Jahresvergleich 50 mal häufiger auf CAPTCHA.[5]
Bei diesen Angriffen versuchen sie, die Anmeldedaten von Anwendern zu stehlen, indem sie ihnen Links zu gefälschten Dokumenten zusenden. Wenn die Empfänger auf diese Links klicken, sehen sie ein CAPTCHA. Nach dem Setzen der Häkchen werden sie zu einer gefälschten Microsoft-Seite weitergeleitet, auf der sie ihre Anmeldedaten eingeben sollen.



Beispiel einer Microsoft OneNote-Seite mit einem Link zu einem manipulierten Word-Dokument.

5 Proofpoint: „Bericht: Der Faktor Mensch“, 2022.

In diesem Beispiel gab sich ein Angreifer als Drittanbieter aus, der eine Arbeitsanforderung an ein gemeinsam genutztes Postfach eines Telekom-Unternehmens gesendet hatte. Ziel des Akteurs war es, die Postfachnutzer zur Weitergabe ihrer Anmeldedaten zu verleiten, indem er ihnen den Link zu einem manipulierten Word-Dokument mit einem CAPTCHA sendete. Der per OneDrive verteilte Link zur schädlichen Webseite konnte die nativen Microsoft-Sicherheitskontrollen problemlos passieren.

Interessant dabei war, dass die OneDrive-Seite auch einen Monat nach der Entlarvung durch Proofpoint noch verfügbar war. Sie ist nur eine von Millionen File-Sharing-Seiten, die die Marke Microsoft jeden Monat missbrauchen.

Umgebung:
Microsoft 365

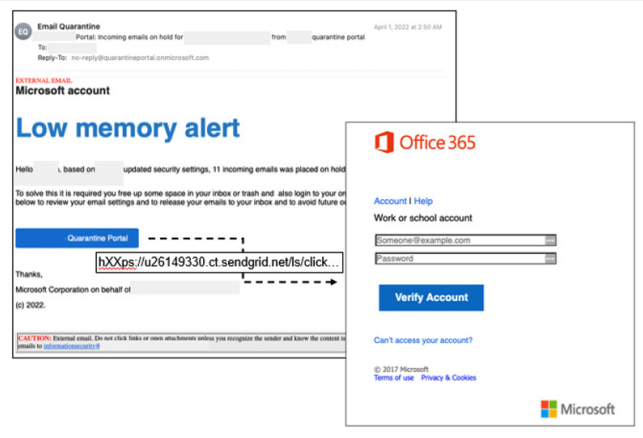
Bedrohungskategorie:
Missbrauch legitimer Cloud-Dienste

Angriffstyp:
Anmeldedaten-Phishing

Ziel:
Microsoft 365-Nutzer

Anmeldedaten-Phishing durch Missbrauch legitimer Cloud-Dienste

Der Diebstahl von Microsoft 365-Anmeldedaten ist eine beliebte Methode, mit der Bedrohungsakteure versuchen, E-Mail-Konten zu kompromittieren. Sobald sie Zugriff auf das Konto eines Anwenders erlangt haben, erfahren die Angreifer nützliche Details, mit denen sie sehr überzeugende Nachrichten verfassen können, was sie für den Diebstahl wertvoller Daten oder das Abzweigen von Geldern nutzen.



Beispiel für Anmeldedatendiebstahl, der die Marke Microsoft nachahmt und auf einer legitimen, Cloud-basierten File-Sharing-Website gehostet wird.

In diesem Beispiel nutzte der Angreifer den Hoster SendGrid und sendete seine Nachricht von einer gefälschten Microsoft-Domain (onmicrosoft.com), um seriös zu erscheinen. In der E-Mail-Signatur verwendete er als Unterzeichner den Namen der Microsoft Corporation.

Es ist bemerkenswert, dass Bedrohungen, die legitime Cloud-Dienste nutzen, von Microsoft häufig unbemerkt bleiben. Der Grund hierfür ist die Art und Weise, wie bei Microsoft Links verarbeitet werden. Die Microsoft-Funktion „Sichere Links“ bietet keine prädiktiven Sandbox-Analysen zum Klickzeitpunkt. Stattdessen bewertet der Anbieter die Reputation und kann daher keine unbekannten Bedrohungen erkennen, die von legitimen Cloud- und File-Sharing-Diensten stammen.

ABSCHNITT 4

KONTOÜBERNAHMEN

Angriffe mit Kontenübernahme sind eine bei Bedrohungsakteuren gängige Taktik. Dabei stehlen sie die Anmeldedaten von Anwendern, um ihre Unternehmensidentität zu übernehmen. Selbst ein einziger Satz Anmeldedaten ist für die Angreifer äußerst wertvoll, da sie damit auf E-Mails, Dokumentspeicher und andere Single Sign-On-Services zugreifen können. Bei so umfassendem Zugriff können die Auswirkungen eines erfolgreichen Angriffs katastrophal sein. Im Jahr 2021 betrugen die Verluste durch Cloud-Kontenkompromittierung durchschnittlich 6,2 Millionen US-Dollar.[6] Und die Zahl dieser Angriffe steigt. Im Jahr 2022 stellte Verizon fest, dass 76 % aller Social-Engineering-Angriffe auch Anmeldedatendiebstahl umfassen.[7]

6 Ponemon Institute: „Cost of Cloud Compromise and Shadow IT“ (Kosten durch Cloud-Kompromittierung und Schatten-IT), 2021.
7 Verizon: „Data Breach Investigations Report“ (Untersuchungsbericht zu Datenkompromittierungen), 2023.

Umgebung:
Microsoft 365

Bedrohungskategorie:
URL-basiert

Angriffstyp:
Diebstahl von Anmeldedaten

Ziel:
Kundendienst-Abteilung

Angriff zur Erfassung von Microsoft 365-Anmeldedaten

Viele Anmeldedaten-Angriffe bedienen sich derselben Taktik: Sie imitieren Microsoft, um die nativen Sicherheitsfunktionen von Microsoft zu überwinden. Der Missbrauch bekannter Marken und unseres Vertrauens darin ist eine der einfachsten Formen von Social Engineering. Hier ist Microsoft klarer Favorit: Wie Untersuchungen von Proofpoint zeigen, nimmt Microsoft vier der Top 5-Positionen bei missbrauchten Marken über alle Bedrohungen des Jahres 2022 hinweg ein.[8]

Beispiel eines Angriffs zur Anmeldedatensammlung.

8 Proofpoint: „Bericht: Der Faktor Mensch“, 2023.

Dieser Angriff mit Anmeldedatendiebstahl unterlief die nativen E-Mail-Sicherheitskontrollen von Microsoft. Der Angreifer sendete eine Nachricht an einen Kundendienst-Mitarbeiter und gab sich als Mitglied des IT-Supports aus. Die E-Mail enthielt auch einen bekannten Anzeigenamen sowie Microsoft-Markennamen, um seriöser zu erscheinen. Proofpoint erlebt häufig, dass Bedrohungsakteure auf legitime URLs setzen (in diesem Fall sendgrid.net), um Microsoft-URL-Scans zu unterlaufen.

Umgebung:
Microsoft 365

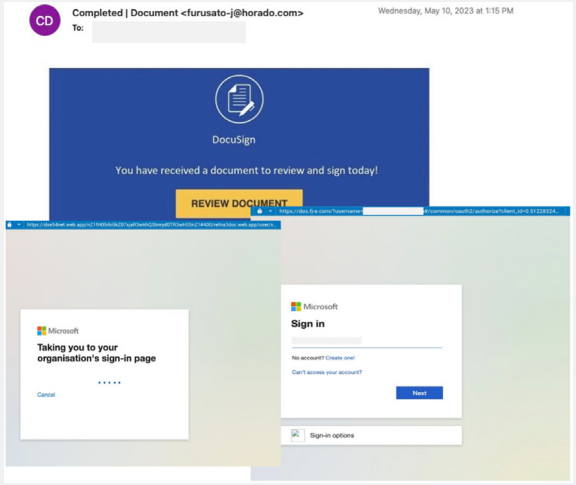
Bedrohungskategorie:
MFA-Erfassung

Angriffstyp:
Anmeldedaten-Phishing

Ziel:
Microsoft 365-Nutzer

MFA-Phishing

Mehrstufige Authentifizierung (MFA) ist nicht mehr zuverlässig in der Lage, Kontoübernahmen zu verhindern, da die Angreifer immer besser darin werden, diese Sicherheitsmaßnahme zu umgehen. So zeigten Proofpoint-Untersuchungen, dass im Jahr 2022 mehr als eine Million Nachrichten pro Monat auf MFA-Umgehung setzten.[9]



Beispiel für MFA-Phishing mit einer URL, die zu einer Microsoft-Doppelgänger-Anmeldeseite führt.

Bei diesem Angriff wurden die nativen Microsoft-Sicherheitskontrollen mithilfe einer vermeintlichen DocuSign-Seite mit einem Link zur Anwendersignatur unterlaufen. Anstatt die Anwender zu DocuSign, zu leiten, führt die URL sie zu einer Microsoft-Doppelgänger-Anmeldeseite.

Für diesen Angriff setzte der Bedrohungsakteur auf EvilProxy, ein Phishing-Framework mit Reverse-Proxy-Funktion, das individuelle Landing Pages für jeden Empfänger erstellt, Anmeldedaten erfasst sowie MFA-Schutzmaßnahmen umgeht. Das Phishing-Kit ist relativ neu und wird in Exploit-Foren zum Kauf angeboten. Nachdem EvilProxy an die MFA-Informationen gelangt ist, bietet es dauerhaften Zugriff auf das Konto – selbst nach einer Zurücksetzung des Kennworts.

9 Proofpoint: „Bericht: Der Faktor Mensch“, 2023.

ABSCHNITT 5

KOMPROMITTIERTE LIEFERANTENKONTEN

Wie bereits erwähnt, geben sich Bedrohungsakteure bei BEC-Betrugsversuchen häufig als Lieferanten aus und verschicken dabei gefälschte Rechnungen oder bitten um die Änderung der Überweisungsdaten. Andere Angreifer kompromittieren Lieferanten und andere vertrauenswürdige externe Parteien, um Zugriff auf die Konten Ihrer Mitarbeiter zu erlangen oder Geld und Daten zu stehlen.

Sobald sie es in Ihr Netzwerk geschafft haben, erstellen sie E-Mail-Regeln zum Verbergen ihrer Spuren, greifen auf geistiges Eigentum zu, ändern Zahlungskontodaten uvm. Im Jahr 2022 verzeichneten erschreckende 69 % aller Unternehmen auf der ganzen Welt mindestens einen Angriff, der in ihrer Lieferkette begann.[10]

10 Proofpoint: „State of the Phish 2023“, Februar 2023.

Umgebung:
Microsoft 365

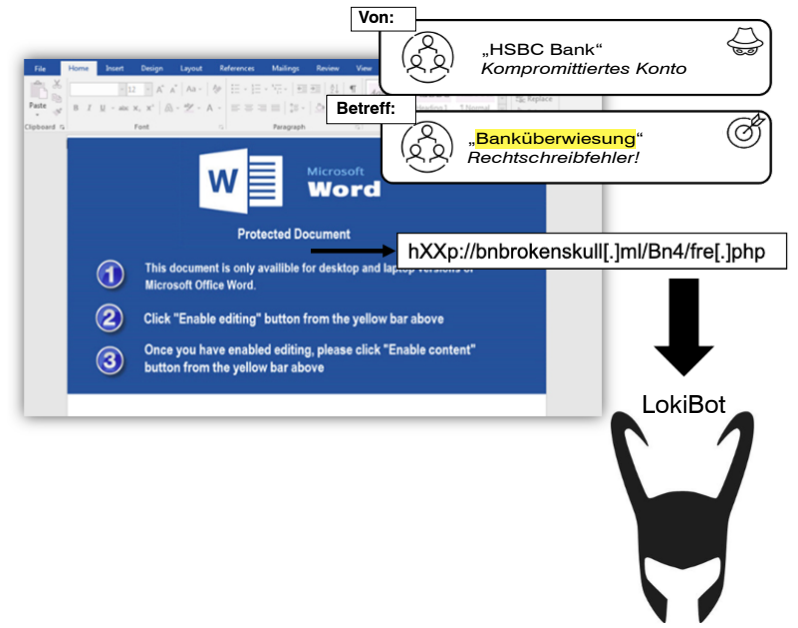
Bedrohungskategorie:
URL-basiert

Angriffstyp:
Downloader

Ziel:
Verborgener BCC-Empfänger in E-Mail

Bedrohungen mit schädlichen Anhängen

Eine Möglichkeit zum Eindringen in ein Netzwerk ist der Einsatz von Malware. Vor Kurzem führte Proofpoint eine interne Datenanalyse zu fast 4.600 Unternehmen durch. Dabei stellten wir fest, dass 85 % dieser Unternehmen innerhalb eines 7-Tage-Zeitraums (der am 31. Januar 2023 endete) mindestens einen E-Mail-Angriff über einen Lieferanten verzeichnet hatten. Bei etwa 13 % dieser Angriffe kam auch Malware zum Einsatz.[11]



Beispiel eines Angriffs mit LokiBot.

11 Proofpoint: „Verborgene Risiken: Lieferkettenangriffe erkennen und abwehren“, April 2023.

Der Angriff in diesem Beispiel wurde aus einem kompromittierten E-Mail-Konto einer weltweit tätigen Bank gestartet. Die Nachricht enthielt einen Link zu einem Word-Dokument, das mehrere Schwachstellen im Formeleditor zum Herunterladen von LokiBot ausnutzte. Dieser Bot kann Kennwörter aus Browsern, FTP/SSH-Anwendungen sowie E-Mail-Konten stehlen.

Microsoft erkannte den Angriff nicht, weil die Nachricht von einer legitimen Domain gesendet wurde, sodass sie von der statischen Zuverlässigkeitsanalyse nicht als schädlich eingestuft wurde. Außerdem hatte die Nachricht die SPF-Authentifizierung bestanden und die Schaddaten verwendeten Taktiken zur Sandbox-Umgehung sowie Dateiverschleierung.

Umgebung:
Microsoft 365

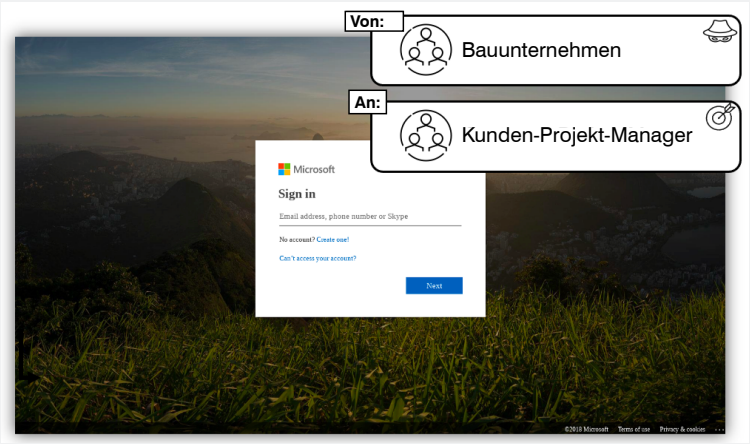
Bedrohungskategorie:
URL-basiert

Angriffstyp:
Anmeldedaten-Phishing

Ziel:
Kunden-Projekt-Manager

Bedrohung mit Anmeldedaten-Phishing

Für den Diebstahl von Anmeldedaten nutzen Bedrohungsakteure auch kompromittierte Lieferantenkonten, wodurch das Schadenspotenzial noch weiter steigt. Leider interagieren Anwender häufig unbesorgt mit diesen Bedrohungen, da diese Nachrichten von einer legitimen Domain versendet werden und daher sehr „echt“ aussehen.



Diese Anmeldeseite imitiert eine Microsoft 365-Anmeldung.

Der oben genannte Angriff wurde von einem kompromittierten Konto gesendet, das einem seriösen Bauunternehmen gehört. Von diesem Konto werden regelmäßig E-Mails an einen Projektleiter geschickt, der Kunde des Unternehmens ist. Die schädliche E-Mail enthielt eine URL zu einer Seite, die Microsoft imitierte, um Microsoft 365-Anmeldedaten zu erfassen.

Die Bedrohung konnte aus mehreren Gründen in den Posteingang des Projektleiters gelangen. Erstens erkennt der Reputationsscan von Microsoft neue schädliche URLs häufig auch dann nicht, wenn sie die Marke Microsoft imitieren. Außerdem wurde diese Nachricht von einer legitimen Lieferanten-Domain gesendet, sodass die statische Zuverlässigkeitsanalyse von Microsoft den Versender nicht als schädlich erkannte. Zudem lieferten die Envelope-Daten keine offensichtlichen Hinweise auf Spoofing.

Umgebung:
Microsoft 365

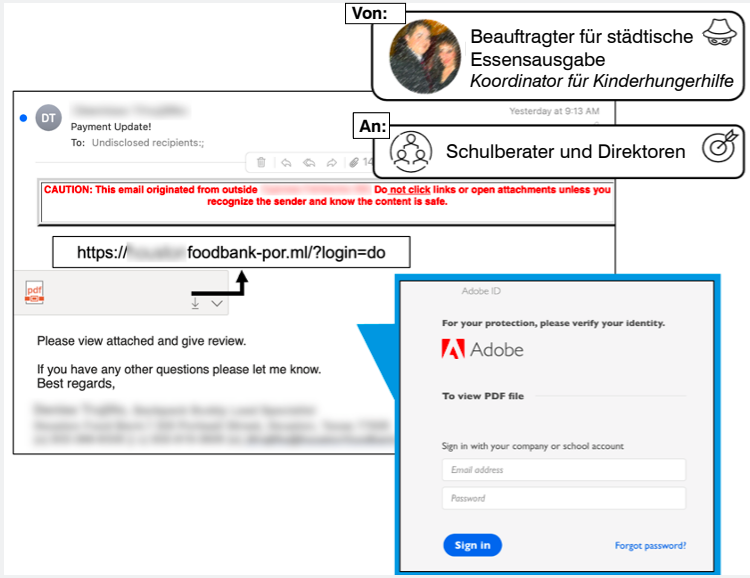
Bedrohungskategorie:
Anhang-basierte Bedrohung mit gefälschter URL

Angriffstyp:
Anmeldedaten-Phishing

Ziel:
Lehrerbeirat und Verwaltung einer Schule

Eingebetteter URL-Angriff

Nicht alle Bedrohungsakteure richten ihre Bemühungen gegen Microsoft 365. Angesichts des zunehmenden Einsatzes von Cloud-Anwendungen ist die Kompromittierung von Cloud-Konten, die weniger gut geschützt sind als Microsoft 365, häufig sehr viel einfacher. Um die Wahrscheinlichkeit zu vergrößern, dass Opfer einen Angriff aktivieren, sendet der Bedrohungsakteur eine E-Mail vom kompromittierten Konto eines Partners.



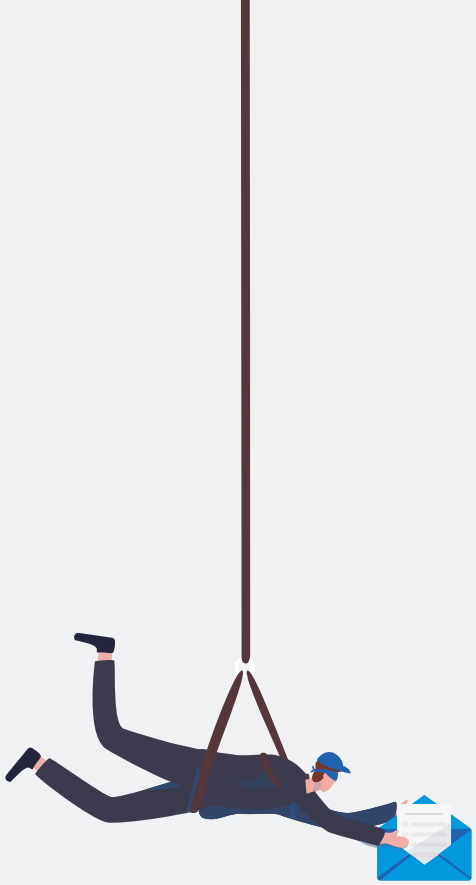
Bedrohungsinformation

Phishing-Angriff wurde von einem kompromittierten Partnerkonto gesendet, um Vertrauen aufzubauen und Empfänger zur Preisgabe von Anmeldedaten zu verleiten, was zu Datenverlust führt.

Bedrohungsrisiko

1. Gesendet von kompromittiertem Partner
2. Bestand SPF/DKIM-Authentifizierung
3. Name vertrauenswürdig, da regelmäßiger Schriftwechsel
4. Führt zu Kontenkompromittierung

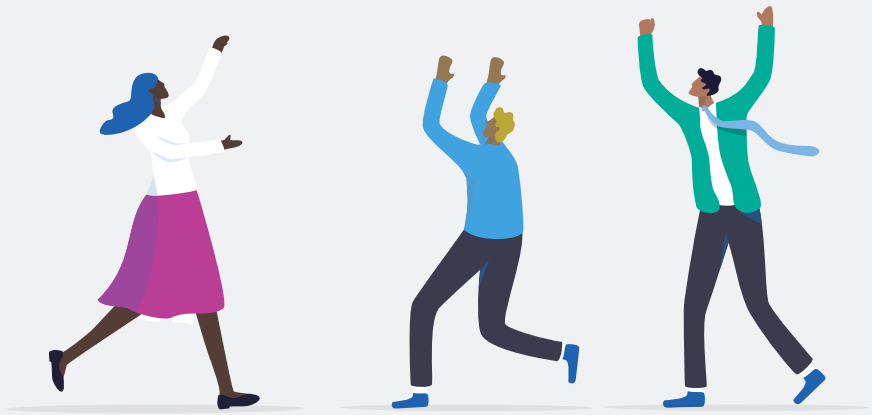
Diese Anmeldeseite imitiert die Anmeldung bei Adobe.



Dieser Angriff zum Erfassen von Anmeldedaten wurde vom kompromittierten Konto eines seriösen Partners gesendet, dem der Anwender regelmäßig E-Mails schickt. Wie oben gezeigt, leitet ein Link in der Nachricht den Anwender zu einer gefälschten Adobe-Seite, um dessen Anmeldedaten zu erfassen.

Microsoft war aus mehreren Gründen nicht in der Lage, diesen Angriff zu stoppen: Erstens kam die E-Mail vom Konto eines seriösen Partners und konnte dadurch die SPF/DKIM-Authentifizierung unterlaufen. Und da mit diesem Konto regelmäßig E-Mails ausgetauscht wurden, galt es als vertrauenswürdig und passierte daher die statische Microsoft-Zuverlässigkeitsanalyse.

Zudem war es dem Bedrohungsakteur gelungen, die Sandbox-Analyse zu umgehen, indem die Schaddaten (d. h. die URL) im Anhang und nicht in der E-Mail enthalten war. Die Zuverlässigkeitsanalyse von Microsoft hat häufig Probleme mit der Identifizierung neuer schädlicher URLs und hat auch diese URL nicht erkannt.



Umgebung:
Microsoft 365

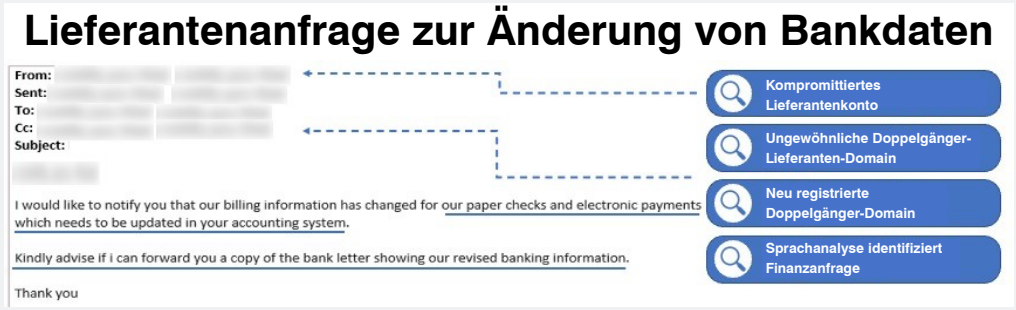
Bedrohungskategorie:
Social Engineering, kompromittiertes Lieferantenkonto

Angriffstyp:
Rechnungsbetrug

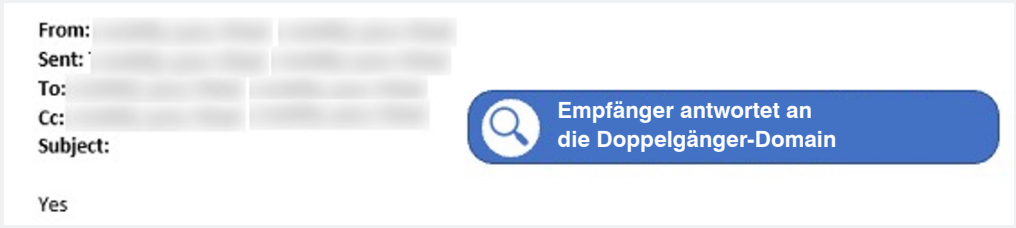
Ziel:
Kundenbetreuer

Bedrohung durch Nachahmung eines Lieferanten

Wenn eine schädliche E-Mail scheinbar von einer bekannten Person kommt, sind die Empfänger eher geneigt, darauf zu reagieren. Wenn ein solcher Angriff von einem scheinbar seriösen Lieferanten kommt, wird er dadurch erheblich gefährlicher.



Dies war die erste E-Mail des Angreifers.



Dies war die Antwort des Kunden, die an eine Doppelgänger-Domain gesendet wurde.

Die erste E-Mail ging von einem seriösen Lieferantenkonto an einen weltweit tätigen Einzelhändler. Der Absender bat um die Aktualisierung seiner Zahlungsdaten. Die scheinbare Routineanfrage erfolgte jedoch mit böswilliger Absicht, denn das Konto des Absenders war zuvor kompromittiert worden. Der Angreifer versuchte, die Antwort-E-Mails an eine neu registrierte Doppelgänger-Domain weiterzuleiten, um vertrauliche Informationen abzufangen und Gelder abzuzweigen.

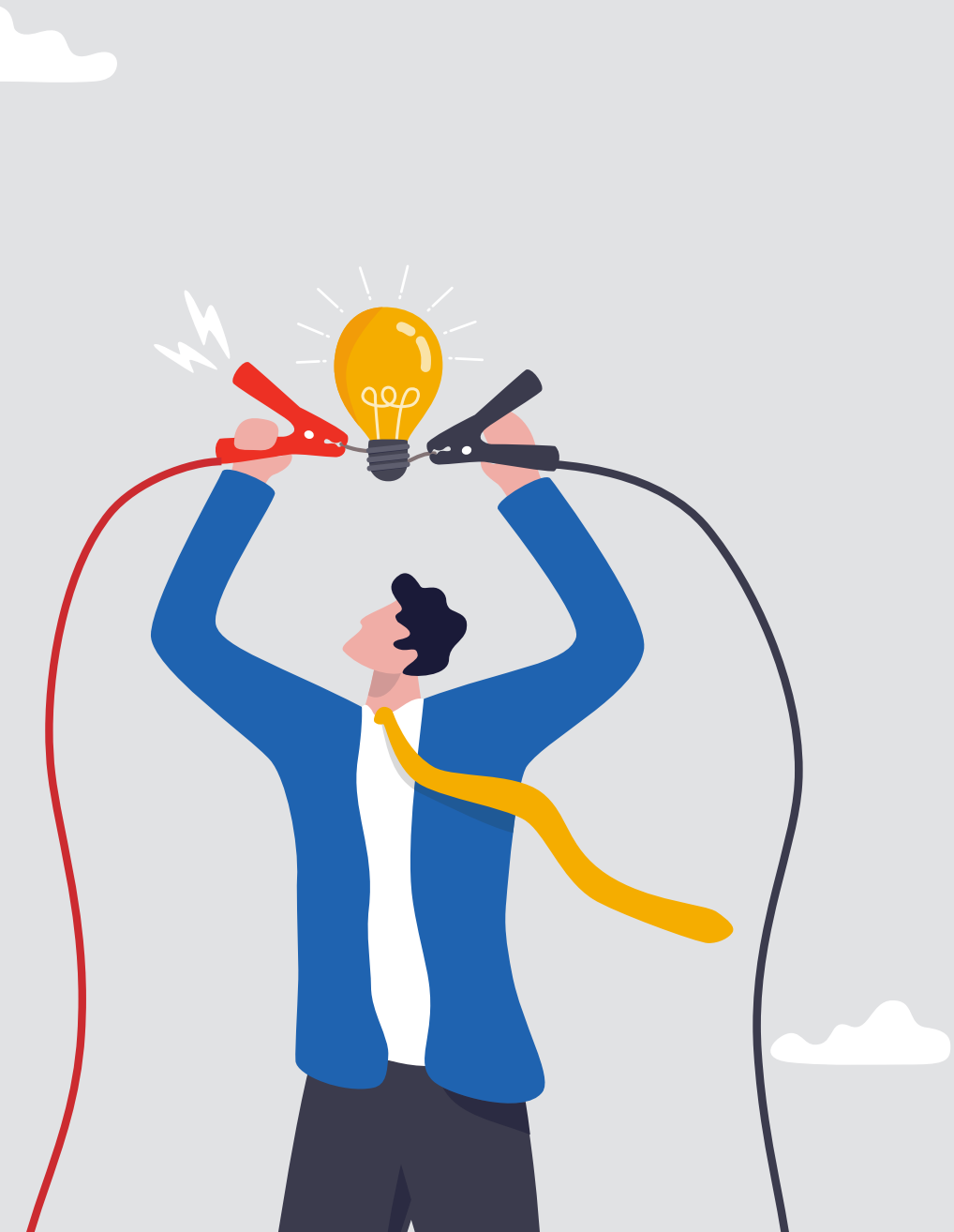
Microsoft konnte diese Bedrohung nicht stoppen, da sie von einem legitimen Kunden stammte und daher die SPF/DKIM-Authentifizierung bestand. Und da mit diesem Konto regelmäßig E-Mails ausgetauscht wurden, galt es als vertrauenswürdig und passierte daher die statische Microsoft-Zuverlässigkeitsanalyse.

FAZIT

Bei der Absicherung Ihres Unternehmens sind die integrierten Sicherheitsfunktionen von Microsoft 365 ein guter Ausgangspunkt. Da sich die Bedrohungen jedoch häufen und weiterentwickeln, benötigen Sie weitere Schutzebenen.

Cyberangreifer müssen nicht mehr isolierte Techniken einsetzen, sondern können raffinierte Taktiken nach Bedarf zusammenstellen, um die Empfänger effektiv zu attackieren. Außerdem suchen sie nach Beziehungen, die ausgenutzt, Vertrauensstellungen, die missbraucht und Zugriffsmöglichkeiten, die eingesetzt werden können. Um sie stoppen zu können, benötigen Sie einen mehrschichtigen, personenzentrierten Ansatz, der die gesamte Angriffskette abdeckt.

Weitere Informationen dazu, wie Proofpoint die native Microsoft 365-Sicherheit verbessern und Ihre Mitarbeiter vor raffinierten Cyberangriffen schützen kann, finden Sie unter proofpoint.com.

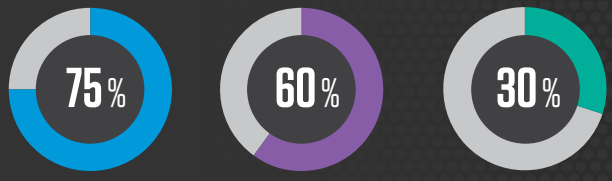


Gründe für Proofpoint

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:



8.000 GROSSUNTERNEHMEN

200.000 KLEINE UNTERNEHMEN

WEITERE INFORMATIONEN

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

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. ist ein führendes Unternehmen für Cybersicherheit und Compliance. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter 75 Prozent der Fortune-100-Unternehmen, setzen auf die personenzentrierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter **www.proofpoint.de**.

proofpoint.

0503-003-04-04 08/23