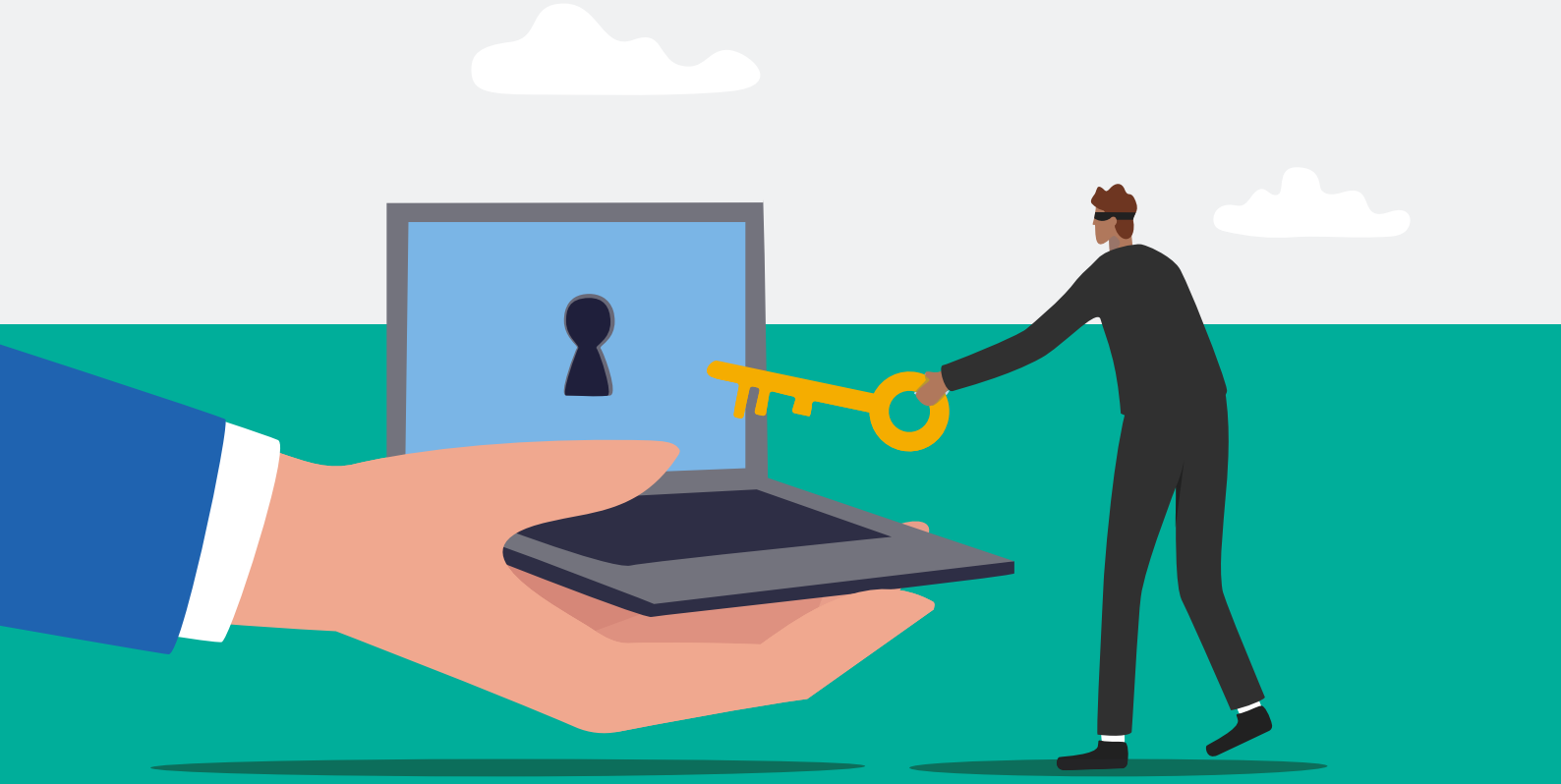
proofpoint.

E-BOOK

5 reale Cyberangriffe und wie sie gestoppt wurden

Teil 1: Social-Engineering-Angriffe



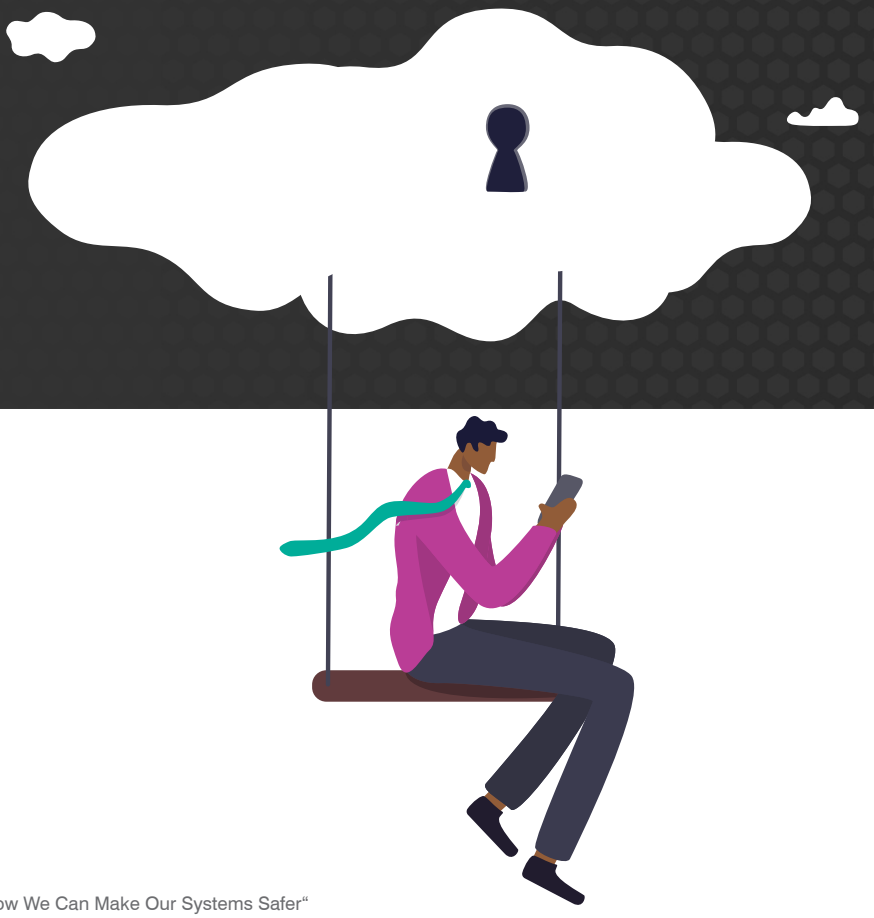
Einleitung

Cyberkriminelle sind raffiniert und hochmotiviert – und sie haben allen Grund dazu. Ihre Branche wächst und bietet hohe Rendite bei geringem Risiko. Schätzungen zufolge werden die Kosten durch Cyberkriminalität bis zum Jahr 2027 auf erschreckende 23,8 Billionen US-Dollar pro Jahr steigen.[1]

Mit der Aussicht auf derart hohe Gewinne scheinen der Kreativität bei modernen Cyberangriffen keinerlei Grenzen gesetzt. Neue und raffinierte Malware-, Phishing- und Social-Engineering-Taktiken schießen jeden Tag wie Pilze aus dem Boden, während die Verteidiger in einer Art Katz-und-Maus-Spiel versuchen, sie zu stoppen. Auch wenn es scheinbar nahezu unbegrenzte Bedrohungsvarianten gibt, haben sie doch grundlegende Gemeinsamkeiten: Sie kommen per E-Mail und sie nehmen den Menschen ins Visier.

In dieser E-Book-Reihe stellen wir einige der derzeit heimtückischsten E-Mail-Angriffe vor, von denen viele mehrere Sicherheitstools umgehen konnten, bevor wir sie entdeckten. Um zu verdeutlichen, wie es dazu kommen konnte, werden wir die einzelnen Angriffe detailliert erläutern, den genauen Ablauf beleuchten und aufzeigen, wie die Cyberkriminelle menschliche Schwachstellen ausgenutzt haben. Anschließend erläutern wir, wie Proofpoint den jeweiligen Angriff stoppen konnte.

In diesem Band befassen wir uns mit Angriffen, die auf Social Engineering basieren. In Teil 2 werden wir uns mit technischeren Angriffen beschäftigen.



1 Weltwirtschaftsforum: „2023 Was a Big Year for Cybercrime—Here's How We Can Make Our Systems Safer" (2023 war für Cyberkriminelle sehr erfolgreich: So können wir unsere Systeme besser schützen), Januar 2024.

Inhaltsverzeichnis

ABSCHNITT 1

BEC- und Supply-Chain-Angriffe

Bei einem BEC-Angriff (Business Email Compromise) imitiert der Bedrohungsakteur eine Person oder Einrichtung, die das Vertrauen des Empfängers genießt, z. B. ein Kollege, ein Anbieter oder ein Geschäftspartner. Viele der aktuellen BEC-Taktiken sind äußerst raffiniert und werden von kapitalkräftigen Akteuren durchgeführt, die sehr viel Planung und Recherche in ihre Angriffe investieren.

In den letzten Jahren haben sich diese Angriffe für Cyberkriminelle als echte Goldesel erwiesen. Nach Angaben des *Internet Crime Report 2023* des FBI hat BEC bei US-Unternehmen Kosten in Höhe 17 Milliarden US-Dollar verursacht. Weltweit verloren Unternehmen dadurch alarmierende 50 Milliarden US-Dollar[2], während die Opfer von Ransomware Verluste in Höhe von 1,1 Milliarden US-Dollar[3] zu beklagen hatten.

2 FBI: „Business Email Compromise: The 50 $ Billion Scam“ (Business Email Compromise: Der 50-Milliarden-Dollar-Betrug), Juni 2023.

3 Wired: „Ransomware Payments Hit a Record $1.1 Billion in 2023“ (Ransomware-Zahlungen erreichten 2023 einen Rekordwert von 1,1 Milliarden USD), Februar 2024.

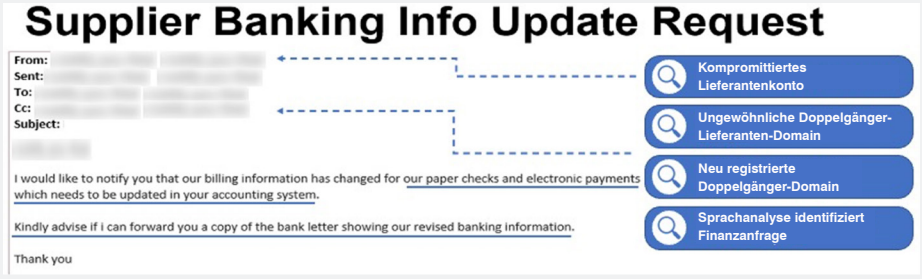
Das Szenario

Den folgenden BEC-Vorfall erkannte Proofpoint bei einem weltweit agierenden Einzelhändler mit mehr als 40.000 Anwendern. Der Angriff erfolgte über die Supply Chain (Lieferkette) des Einzelhändlers und wurde von der implementierten Lösung nicht erkannt. Dieses Beispiel zeigt eindrucksvoll, wie schnell sich die Welt der Cybersicherheit weiterentwickelt.

Ablauf des Angriffs

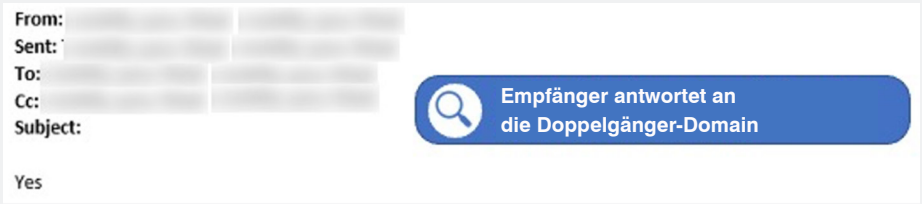
Nachfolgend ein genauerer Blick auf den Ablauf dieses Angriffs:

1. **Die betrügerische Nachricht.** Der weltweit tätige Einzelhändler erhielt eine E-Mail von einem Absender innerhalb seiner Supply Chain mit der Bitte, die Zahlungsdaten zu aktualisieren. Die scheinbare Routineanfrage erfolgte jedoch mit böswilliger Absicht, denn das Konto des Absenders war zuvor kompromittiert worden.



Die erste E-Mail des Angreifers, ergänzt mit forensischen Beobachtungen von Proofpoint.

2. **Die schädliche Doppelgänger-Domain.** Der Angreifer versuchte, die Antwort-E-Mails an eine neu registrierte Doppelgänger-Domain weiterzuleiten, um vertrauliche Informationen abzufangen und Gelder abzuzweigen.



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

Schwierigkeiten bei der Erkennung dieser Bedrohungen

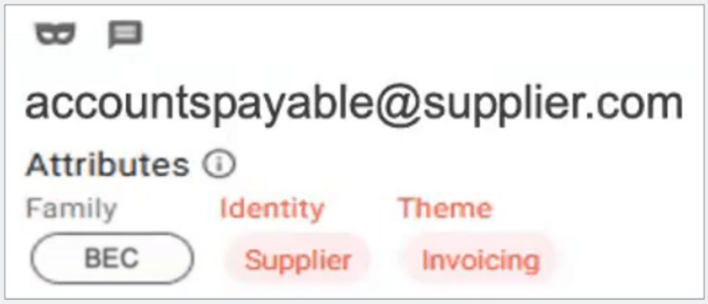
BEC-Angriffe lassen sich nur sehr schwer erkennen, denn sie enthalten nicht die üblichen Schaddaten wie schädliche URLs oder Dateianhänge. Stattdessen täuschen die Bedrohungsakteure ihre Opfer mit Nachahmungs- und Social-Engineering-Techniken.

Das beim Einzelhändler vorhandene Sicherheitstool erkannte diese Bedrohung aus verschiedenen Gründen nicht. Zunächst einmal setzt das Tool zu einseitig auf den Erkennungsfaktor Domain-Alter. Zudem ist es nicht in der Lage, Doppelgänger-Domains zu identifizieren. Und außerdem wurde die Reply-to-Adresse nicht analysiert, sodass die Umleitung an eine andere Domain nicht erkannt wurde.

Wie Proofpoint die Bedrohung erkannt hat

Der entscheidende Punkt beim Identifizieren vieler Bedrohungsarten (einschließlich BEC und Anmeldedaten-Phishing) besteht darin, das Domain-Alter mit weiteren Identifikatoren zu kombinieren, die auf böswillige Absichten schließen lassen. Proofpoint verwendet deshalb einen mehrschichtigen Ansatz, bei dem unser Erkennungsmodul künstliche Intelligenz (KI), Machine Learning (ML) und Verhaltensanalysen nutzt, um wichtige Kompromittierungsindikatoren zu identifizieren. Dabei erkennt es E-Mail-Muster, die nicht dem „normalen“ Verhalten entsprechen.

Im vorliegenden Beispiel analysierte Proofpoint die Sprache der E-Mail und stieß dabei auf eine Anfrage mit finanziellem Hintergrund. Isoliert betrachtet, erschien die Anfrage nicht ungewöhnlich. In Kombination mit der Änderung in der Reply-to-Adresse wurde sie jedoch verdächtig. Zudem wurde die Domain genau an dem Tag registriert, an dem die E-Mail versendet wurde.



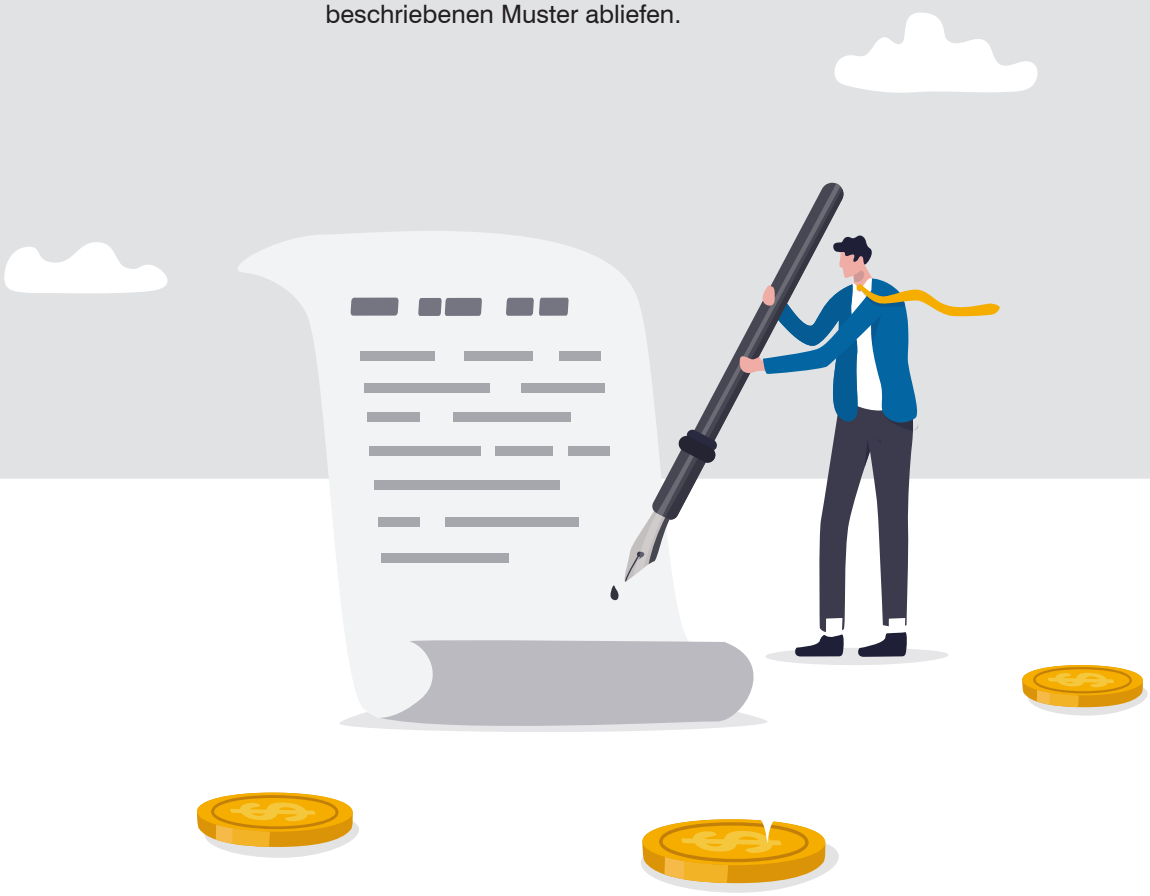
Das Dashboard von Proofpoint Targeted Attack Protection (TAP) kategorisiert jede Bedrohung. In diesem Fall erfahren wir, dass es sich um eine BEC-Bedrohung handelt, dass die Bedrohung von einem Lieferanten stammt und dass es um eine Rechnung geht.

ABSCHNITT 2

Phishing mit digitalen Signaturen

Beim Phishing mit digitalen (E-Mail-)Signaturen erhalten Empfänger eine E-Mail, in der sie aufgefordert werden, ein Dokument zu unterzeichnen. Das eigentliche Interesse der Angreifer liegt jedoch in den Anmeldedaten oder anderen personenbezogenen Daten. Die Nachricht enthält mitunter einen Anhang in Form einer Vereinbarung oder Rechnung, die unterschrieben werden soll.

Im Jahr 2023 stellte Proofpoint in nur einem Monat mehr als 75.000 unterschiedliche Bedrohungen fest, die nach dem hier beschriebenen Muster abliefen.



Das Szenario

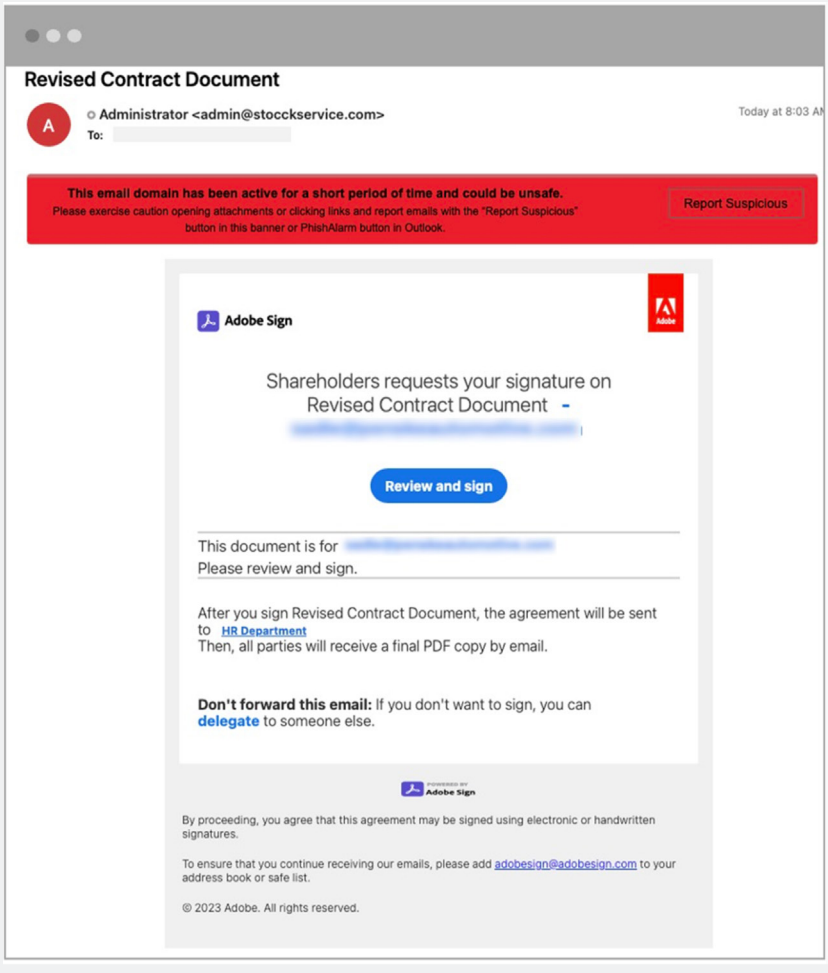
Proofpoint erkannte eine SaaS-Anwendung, die in AWS (Amazon Web Services) Amplify gehostet war und versuchte, Anmeldedaten zu erfassen. Die Anwendung wurde von einem unseren Kunden genutzt, genauer gesagt von einem Automobilunternehmen mit 2.000 Mitarbeitern.

Ein krimineller Akteur hatte einen Phishing-Köder ausgelegt, bei dem es sich scheinbar um einen Link zu einem vertraulichen Dokument handelte – in diesem Fall ein aktualisierter Vertrag, der zu prüfen und zu unterzeichnen war. Ziel der Attacke war ein Sachbearbeiter in der Vertragsabteilung mit weiteren treuhänderischen Zuständigkeiten. Im Rahmen ihrer Tätigkeit haben solche Mitarbeiter oft mit Vorstandsmitgliedern, Kunden und Lieferanten zu tun, sodass eine solche Anfrage für sie durchaus normal ist.

Ablauf des Angriffs

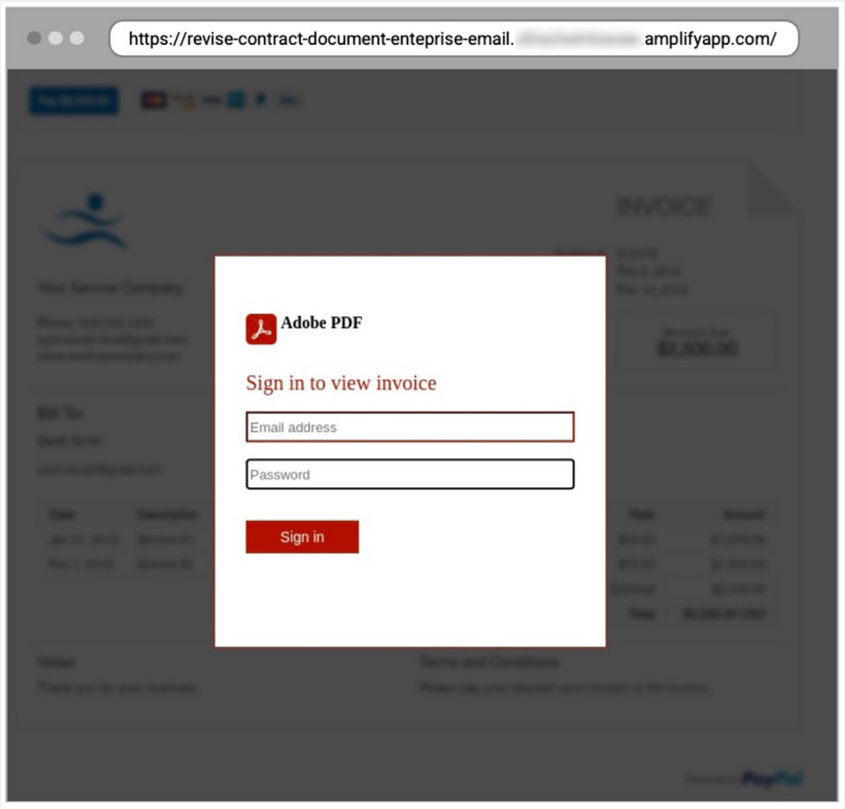
Nachfolgend ein genauerer Blick auf den Ablauf dieses Angriffs:

1. **Die betrügerische Nachricht.** Unser Kunde erhielt eine E-Mail, in der ein Mitarbeiter gebeten wurde, einen aktualisierten Vertrag zu prüfen und zu unterzeichnen.



Die schädliche E-Mail.

2. **Die schädliche URL.** Ein Klick auf die schädliche URL hätte einen Anmeldebildschirm angezeigt, der einer legitimen Anmeldemaske realistisch nachempfunden ist. Ziel des Angreifers war es, den Mitarbeiter zur Herausgabe seiner Zugangsdaten zu verleiten.



Die gefälschte Anmeldeseite, die auf amplifyapp.com gehostet wurde.

Schwierigkeiten bei der Erkennung dieser Bedrohungen

Bei solchen Angriffen werden oft Anwendungen wie AWS Amplify und andere SaaS-Dienste wie DocuSign, Adobe Sign oder OneSpan Sign genutzt, da sie Kriminellen eine einfache und unverdächtige Möglichkeit zum Verteilen schädlicher Inhalte bieten.

In diesem Fall war die URL-Domain mehr als fünf Jahre alt. Die IP-Adresse gehörte zu Amazon, was den Anschein der Legitimität für viele unterstreichen dürfte. Die meisten Anbieter von E-Mail-Sicherheitslösungen sind in der Lage, einen gängigen Anmeldedaten-Phishing-Angriff zu erkennen. Die vertrauenswürdige Domain des SaaS-Anbieters erhöht jedoch für die meisten Erkennungsmodule die Komplexität. In der Tat fingen 19 andere Anbieter von E-Mail-Sicherheitsprodukten diese Bedrohung nicht ab, wobei viele dieser Anbieter behaupten, fortschrittliche KI und ML zum Stoppen solcher Angriffe zu verwenden.

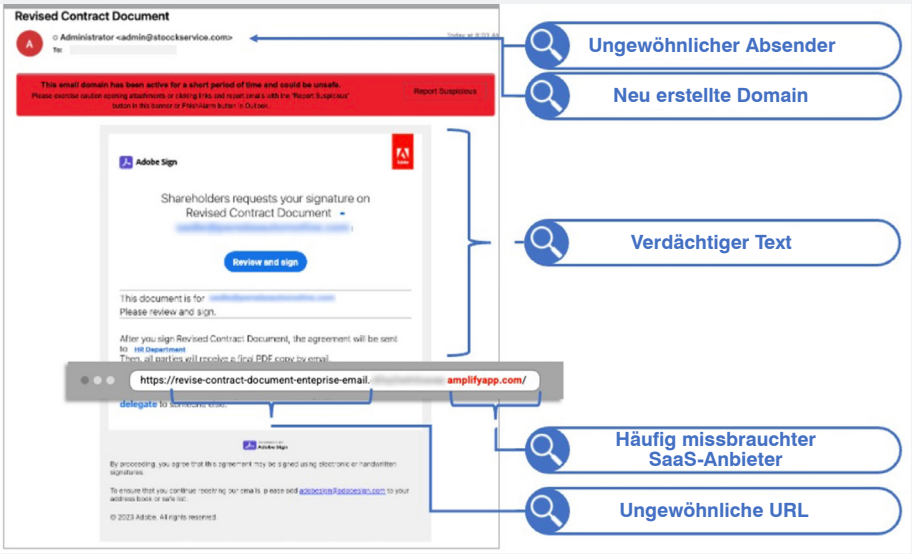
Wie Proofpoint die Bedrohung erkannt hat

Das verhaltensbasierte KI-Modul von Proofpoint erkennt und blockiert eine ganze Reihe von Bedrohungen anhand von verschiedenen Indikatoren auf Nachrichtenebene. Dadurch kann Proofpoint auch bisher komplett unbekannte Phishing-Bedrohungen relativ früh in der Angriffskette erkennen und blockieren – noch bevor sie in das E-Mail-Postfach zugestellt werden.

Bei der mehrschichtigen, fundierten Analyse des Anwenderprofils stellte Proofpoint anhand von historischen Kommunikationsmustern fest, dass der Kontakt zwischen Absender und Empfänger eher ungewöhnlich war. Der Absender hatte selten mit dem Empfänger oder einer anderen Person in dem Automobilunternehmen kommuniziert.

Proofpoint führte mithilfe verhaltensbasierter KI- und ML-Tools eine genaue Analyse der URL durch, einschließlich Relevanz der URL basierend auf vorherigen historischen Datenpunkten und anderen ungewöhnlichen Aktivitäten. Die URL wurde bei keinem der Sendemuster im Unternehmen jemals vom Empfänger oder einem anderen Mitarbeiter verwendet.

Proofpoint erkannte außerdem, dass eine legitime und bekannte Domain eines SaaS-Anbieters genutzt wurde, die bei anderen von uns geschützten Unternehmen von einem Angreifer missbraucht wurde, um schädlichen Inhalt zu verteilen.



Zusammenfassung der von Proofpoint gemachten Beobachtungen, die zur Einstufung der E-Mail als Bedrohung geführt haben.

ABSCHNITT 3

TOAD-Bedrohungen

Social-Engineering-Taktiken entwickeln sich kontinuierlich weiter, da kriminelle Akteure stets neue und kreative Wegen für den Erstangriff auf vertrauliche Systeme suchen. Angriffe per Telefon (Telephone-Oriented Attack Delivery, TOAD) sind ein Beispiel dafür. Bei dieser Taktik senden die Angreifer eine E-Mail, in der sie den Empfänger zum Anruf bei einem (falschen) Callcenter auffordern.

In der Regel werden Anwender nicht vor schädlichen Telefonanrufen geschützt. Deshalb ist das Stoppen dieser E-Mails besonders wichtig. Gleichzeitig sind diese Angriffe schwer zu erkennen, da sie meist keine URLs oder Anhänge enthalten.

Im Rahmen der Bedrohungsbewertungen eines einzigen Monats im Jahr 2023 erkannte Proofpoint mehr als 19.000 TOAD-Angriffe, die 14 unterschiedlichen E-Mail-Sicherheitstools entgangen waren.

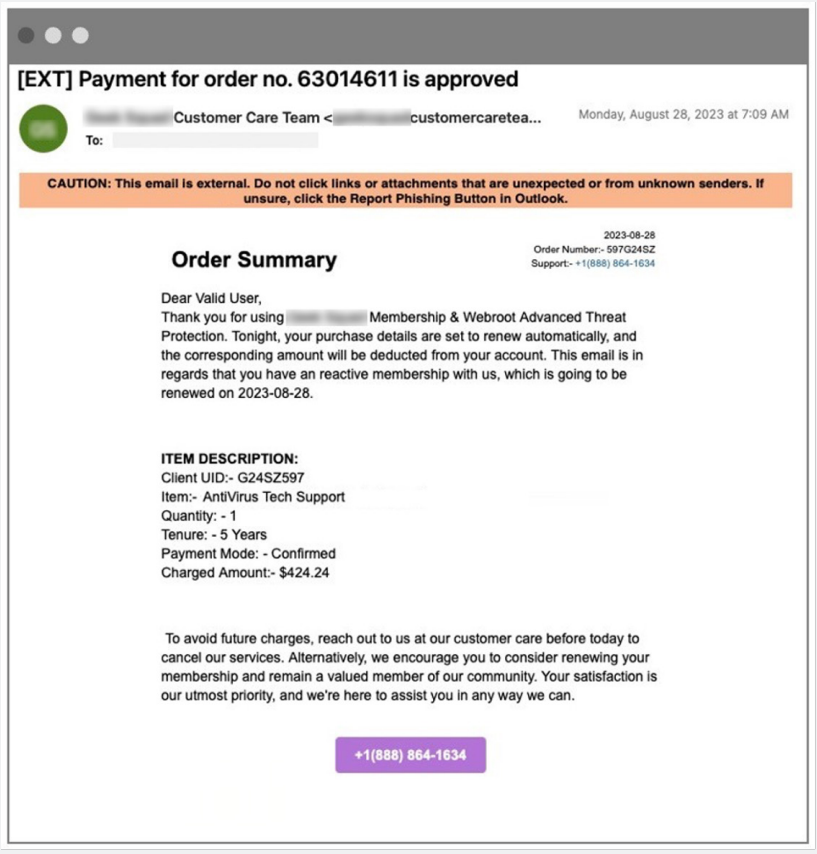
Das Szenario

Bei einem Fertigungsunternehmen mit mehr als 45.000 Mitarbeitern erkannte Proofpoint die hier beschriebene TOAD-Bedrohung. Ein krimineller Akteur gab sich als Mitarbeiter eines bekannten Virenschutzanbieters aus und sendete einem der Mitarbeiter des Fertigungsunternehmens eine betrügerische Nachricht, die keine URL und keinen Anhang, sondern eine Telefonnummer nannte.

Ablauf des Angriffs

Nachfolgend ein genauerer Blick auf den Ablauf dieses Angriffs:

1. **Die betrügerische Nachricht.** In der E-Mail wurde angekündigt, dass demnächst eine Bestellung durch ein bekanntes Technologieunternehmen erfolgen solle.


[EXT] Payment for order no. 63014611 is approved

Customer Care Team <customercaretea...

Monday, August 28, 2023 at 7:09 AM

To:

CAUTION: This email is external. Do not click links or attachments that are unexpected or from unknown senders. If unsure, click the Report Phishing Button in Outlook.

Order Summary

2023-08-28
Order Number:- 597G24SZ
Support:- +1(888) 864-1634

Dear Valid User,
Thank you for using Membership & Webroot Advanced Threat Protection. Tonight, your purchase details are set to renew automatically, and the corresponding amount will be deducted from your account. This email is in regards that you have an reactive membership with us, which is going to be renewed on 2023-08-28.

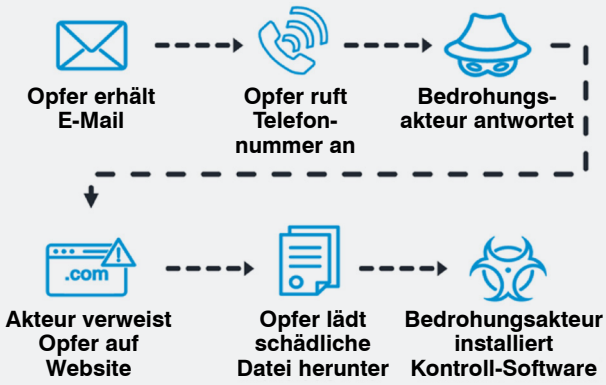
ITEM DESCRIPTION:
Client UID:- G24SZ597
Item:- AntiVirus Tech Support
Quantity: - 1
Tenure: - 5 Years
Payment Mode: - Confirmed
Charged Amount:- $424.24

To avoid future charges, reach out to us at our customer care before today to cancel our services. Alternatively, we encourage you to consider renewing your membership and remain a valued member of our community. Your satisfaction is our utmost priority, and we're here to assist you in any way we can.

+1(888) 864-1634

Das Original der schädlichen E-Mail im Posteingang des Empfängers.

2. **Abfolge des TOAD-Angriffs.** Hätte der Mitarbeiter die Telefonnummer gewählt, hätte der Angreifer ihn auf seinen Computer weiterleiten und auffordern können, eine schädliche URL aufzurufen. Dies wiederum hätte verschiedene Bedrohungen ermöglichen können, darunter Fernzugriff, Diebstahl vertraulicher Daten oder eine Ransomware-Infektion.



Die typische Abfolge eines TOAD-Angriffs.

Schwierigkeiten bei der Erkennung dieser Bedrohungen

TOAD-Bedrohungen sind besonders schwer zu erkennen, weil sie selten Schaddaten enthalten. Darüber hinaus bedienen sich die Angreifer oft bekannter Domains, die Google, Microsoft oder anderen legitimen E-Mail-Diensten gehören.

Da diese konkrete TOAD-Bedrohung von einer Google-Domain aus gesendet wurde, bestand die Nachricht E-Mail-Authentifizierungsprüfungen wie SPF (Sender Policy Framework) und DMARC. Die Nachricht enthielt außerdem keine Schaddaten und wurde möglicherweise deshalb vom implementierten Sicherheitstool übersehen und zugestellt.

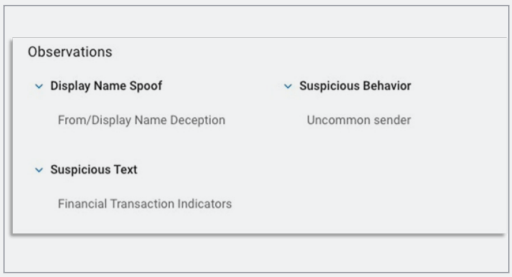
Wie Proofpoint die Bedrohung erkannt hat

Proofpoint setzt fortschrittliche KI- und ML-Technologien ein, um Verhaltensindikatoren zu analysieren und zu kombinieren und TOAD-Bedrohungen zu erkennen. Dieser Ansatz ist zuverlässiger, als lediglich eine Datenbank mit zuvor bei TOAD-Angriffen verwendeten schädlichen Telefonnummern zu überprüfen.

Bei der Analyse der Nachricht durch das verhaltensbasierte KI-Modul von Proofpoint wurden Inhalte zu einer finanziellen Transaktion in Kombination mit einem Hinweis auf Dringlichkeit festgestellt – ein typischer Hinweis auf eine potenziell schädliche E-Mail. TOAD-Bedrohungen gehen immer mit der Angabe einer Telefonnummer und der Aufforderung an den Empfänger einher, unter dieser Nummer anzurufen. Deshalb scannt Proofpoint Nachrichten auf das Vorhandensein einer Telefonnummer.

Unsere mehrschichtige Analyse unter Hinzuziehung historischer Kommunikationsmuster ergab außerdem, dass der Empfänger in der Vergangenheit noch nie eine E-Mail von dem betreffenden Absender erhalten hatte. Genauer gesagt hatte bislang niemand in dem Unternehmen je eine E-Mail von diesem Absender erhalten.

Ein typisches Merkmal von TOAD-Angriffen sind Nachrichten, die scheinbar von einer legitimen großen Marke stammen, wodurch eine Art natürliches Vertrauen aufgebaut werden soll. Bei unserer Analyse sind wir ebenfalls auf diese Taktik gestoßen.



Zusammenfassung der von Proofpoint gemachten Beobachtungen, die zur Einstufung der E-Mail als Bedrohung führten.

ABSCHNITT 4

Umleitung von Gehaltszahlungen

Die Umleitung von Gehaltszahlungen ist eine Form von BEC (Business Email Compromise). Primäre Ziele dieser Angriffe sind meist Sachbearbeiter für Gehaltszahlungen. In der Regel geben sich die kriminellen Akteure als Mitarbeiter aus, die ihre Bankverbindung aktualisieren möchten. Das neuen Bankkonto gehört jedoch den Angreifern. Sobald die betrügerische Transaktion abgeschlossen ist, kann die überwiesene Summe vom Unternehmen nicht mehr zurückgebucht werden.

Die Umleitung von Gehaltszahlungen ist zwar keine neue Form von BEC, jedoch nimmt die Häufigkeit dieser Angriffstaktik zu. Proofpoint beobachtet, dass diese Art von Bedrohung von den Abwehrmechanismen anderer E-Mail-Sicherheitstools weiterhin nicht aufgehalten wird. Bei unseren kürzlich durchgeführten Bedrohungsbewertungen wurden mehr als 400 Bedrohungen von 12 anderen E-Mail-Sicherheitstools übersehen.

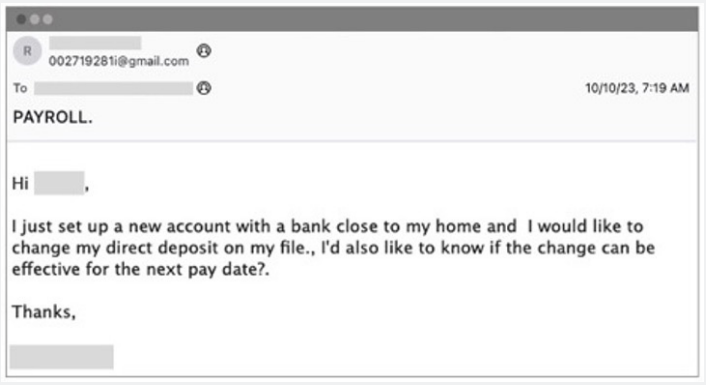
Das Szenario

Eine dieser Bedrohungen wurde von Proofpoint bei einem Energie- und Versorgungsunternehmen mit 300 Mitarbeitern erkannt. Im vorliegenden Fall gab sich der Angreifer als Mitarbeiter ohne Führungsverantwortung aus und sendete eine E-Mail an den Personalchef des Unternehmens. Die Nachricht wurde vom implementierten E-Mail-Sicherheitstool des Unternehmens problemlos zugestellt und auch das API-basierte Tool zur Behebung nach der Zustellung erkannte die Bedrohung nicht.

Ablauf des Angriffs

Nachfolgend ein genauerer Blick auf den Ablauf dieses Angriffs:

1. **Die betrügerische Nachricht.** Der Angreifer sendete eine Anfrage an die Personalabteilung mit der Bitte, seine Bankverbindungsdaten zu aktualisieren. Die Nachricht wurde von einem Konto aus gesendet, bei dem es sich scheinbar um das private E-Mail-Konto eines legitimen Mitarbeiters handelte.


R [redacted] 002719281i@gmail.com

To [redacted] 10/10/23, 7:19 AM

PAYROLL.

Hi [redacted],

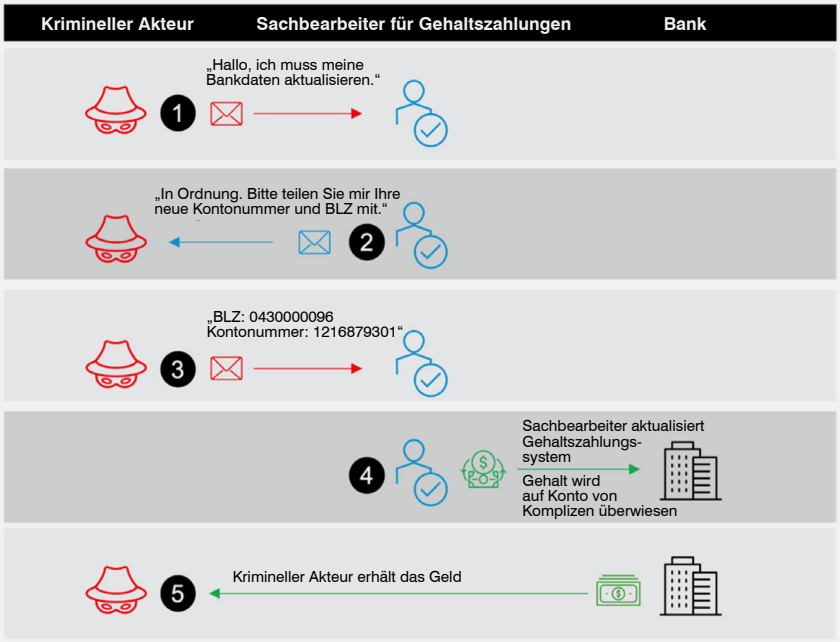
I just set up a new account with a bank close to my home and I would like to change my direct deposit on my file., I'd also like to know if the change can be effective for the next pay date?.

Thanks,

[redacted]

Das Original der schädlichen Nachricht, die im Posteingang des Empfängers einging.

2. **Abfolge des Angriffs mit Umleitung von Gehaltszahlungen.** Hätte der Empfänger auf die Nachricht reagiert, hätte die Überweisung des Gehalts auf ein anderes Bankkonto erfolgen können, das natürlich nicht dem Mitarbeiter gehörte, dessen Identität nachgeahmt wurde.



Die typische Abfolge eines Angriffs mit Umleitung von Gehaltszahlungen.

Schwierigkeiten bei der Erkennung dieser Bedrohungen

Diese Bedrohungen enthalten meist keine Schaddaten wie Anhänge oder URLs, werden üblicherweise von privaten E-Mail-Diensten wie Google, Yahoo und iCloud gesendet und richten sich an bestimmte Anwender.

Interessanterweise erkennen API-basierte E-Mail-Sicherheitstools, die nach Bedrohungen in bereits zugestellten E-Mails suchen, diese Art von Bedrohung mit recht hoher Wahrscheinlich nicht. Dies ist zum Teil auf die Funktionsweise dieser Tools zurückzuführen. Sie arbeiten mit einem internen Verzeichnis der Anzeigenamen aller Mitarbeiter, das vom Sicherheits- oder IT-Team manuell befüllt und gepflegt werden muss. Das ist nicht nur sehr zeitaufwändig, sondern auch schwer skalierbar.

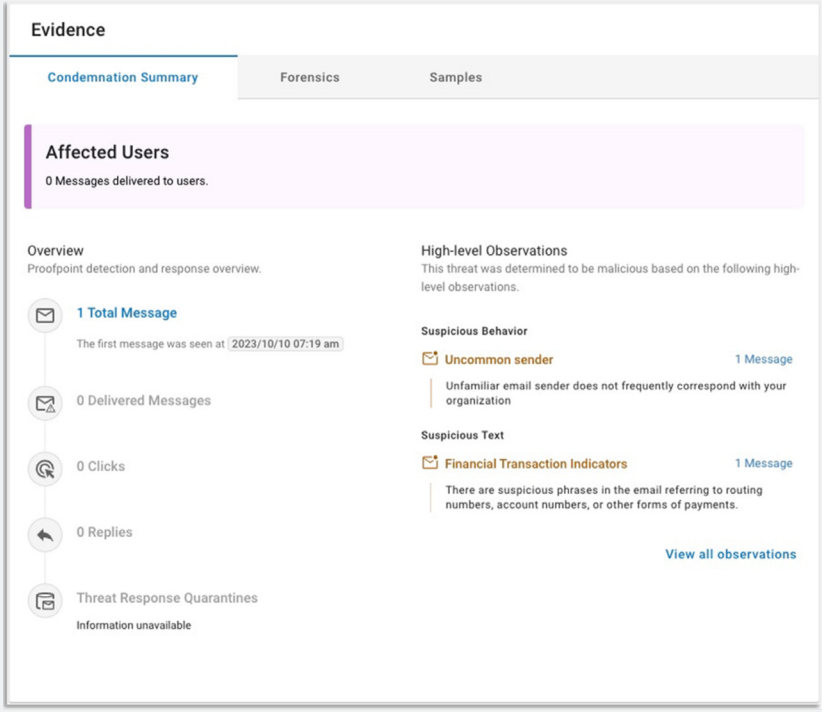
Um den Aufwand in Grenzen zu halten, aktivieren viele Unternehmen die Anzeigenamenprävention ausschließlich für ihre wichtigsten Führungskräfte. Kriminelle Akteure, die sich auf die Umleitung von Gehaltszahlungen konzentrieren, ahmen jedoch nicht nur Führungskräfte nach, sondern interessieren sich für alle Person mit Zugriff auf Finanzmittel. In unserem hier genannten Beispiel hat der Angreifer genau diese Schwachstelle ausgenutzt.

Wie Proofpoint die Bedrohung erkannt hat

Damit ein E-Mail-Sicherheitstool den wahren Zweck einer E-Mail erkennen kann, muss es den Tonfall und die Absicht einer Nachricht interpretieren können. Proofpoint nutzt dazu mehrere Erkennungsindikatoren, Analysemodule und verhaltensbezogene KI. Unsere KI- und ML-gestützten Erkennungsmodule werden kontinuierlich mit Millionen täglich analysierten E-Mail-Nachrichten aus unserem weltweiten Bedrohungsdaten-Ökosystem trainiert.

Einer der Indikatoren zur Erkennung schädlicher E-Mails ist die Häufigkeit und Regelmäßigkeit, mit der Absender und Empfänger Nachrichten austauschen. Im hier genannten Beispiel war es eher unüblich, dass der Personalchef E-Mails vom privaten E-Mail-Konto von Mitarbeitern erhielt.

Die meisten E-Mail-Sicherheitstools verwenden isolierte Indikatoren für unübliche Absender, sodass sie sehr viele False Positives generieren. Proofpoint geht anders vor. Wir kombinieren mehrere Indikatoren und verlassen uns nicht zu sehr auf nur einen oder zwei Hinweise. Durch die Kombination des Indikators für unübliche Absender mit einer Analyse der im Textteil der Nachricht verwendeten Sprache können wir den Tonfall extrahieren und die Absicht einer E-Mail interpretieren.



Zusammenfassung der von Proofpoint erkannten Indikatoren, die zur Einstufung der E-Mail als Bedrohung führten.

ABSCHNITT 5

Kompromittierung der Supply Chain

Die Kompromittierung der Supply Chain ist eine weitere Form von BEC (Business Email Compromise), die derzeit im Aufwind ist. Bei diesen Angriffen versuchen kriminelle Akteure, in ein Unternehmen zu gelangen, indem sie zunächst die Sicherheitsmechanismen der Lieferanten, Anbieter oder anderen Partner der Supply Chain des Unternehmens überwinden. Angreifer wissen, dass Unternehmen mit komplexeren Supply Chains stärkere Cybersicherheitsvorkehrungen treffen und deshalb ein schwieriges Ziel darstellen.

Statt einen direkten Angriff gegen das Unternehmen zu starten, infiltrieren kriminelle Akteure deshalb einen der vertrauenswürdigen Partner des Unternehmens und geben sich dann als dieser aus. Dabei kommen oft Taktiken wie Thread-Hijacking oder Conversation-Hijacking zum Einsatz, bei denen die Akteure bestimmte E-Mail-Konten angreifen und kompromittieren, um die Kommunikation der Beteiligten auszuspionieren. Wenn der Angreifer den Zeitpunkt für günstig hält, schleust er sich selbst in den E-Mail-Austausch ein. In einigen Fällen sind die Angreifer aber auch dreist genug, ein neues Gespräch zu starten.

Diese Angriffe kommen immer häufiger vor und werden immer raffinierter. Der bedeutendste dieser Angriffe im Jahr 2023 kostete das betroffene Unternehmen mehr als 9,9 Milliarden US-Dollar. Über 1.000 Unternehmen und 60 Millionen Personen bekamen die Auswirkungen davon zu spüren.[4]

4 TechCrunch: „MOVEit, the Biggest Hack of the Year, by the Numbers“ (MOVEit, der größte Hack des Jahrs – die Zahlen), August 2023.

Das Szenario

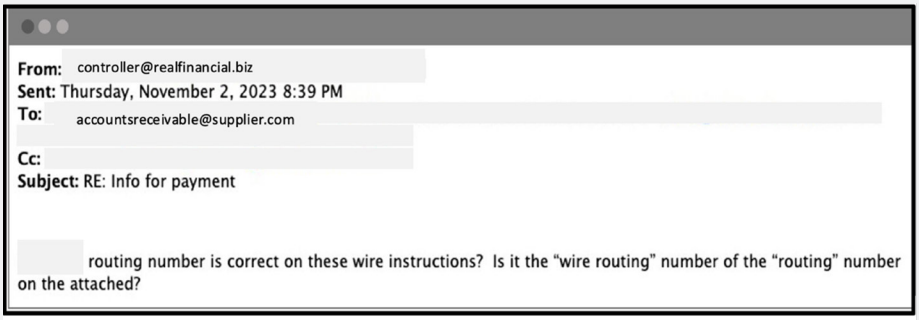
Proofpoint erkannte eine betrügerische Nachricht, die von einem Mitarbeiter der Buchhaltung eines kleinen Finanzdienstleisters in Florida zu stammen schien. Tatsächlich handelte es sich jedoch um einen kriminellen Akteur, der die Identität einer anderen Person übernommen hatte. Das eigentliche Ziel war ein Supply-Chain-Angriff gegen eine große Anwaltskanzlei in Boston.

In einer E-Mail an die Kanzlei bat der Angreifer den dortigen Controller, eine Zahlung zu stoppen und die Zahlungsinformationen zugunsten eines anderen Kontos zu aktualisieren.

Ablauf des Angriffs

Nachfolgend ein genauerer Blick auf den Ablauf dieses Angriffs:

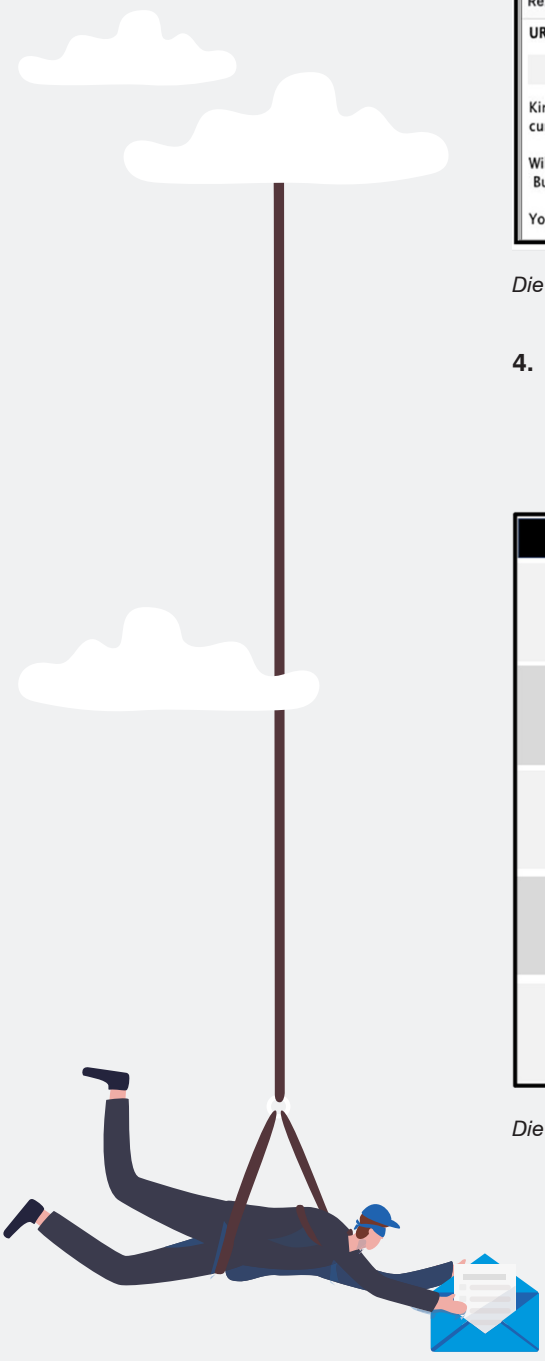
1. **Die legitime Kundennachricht.** Der Kunde sendete eine E-Mail an den Lieferanten und bat ihn, die Richtigkeit der Zahlungsinformationen für die Überweisung zu bestätigen.



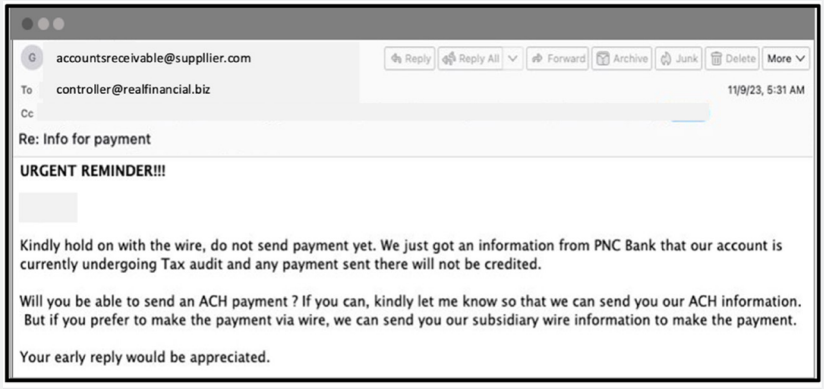
Die legitime Kundennachricht zur Bestätigung der Zahlungsinformationen für die Überweisung.

2. **Die legitime E-Mail des Lieferanten.** Der Lieferant antwortete, um die Zahlungsinformationen zu verifizieren.

Die legitime E-Mail des Lieferanten zum Überprüfen der Zahlungsinformationen.

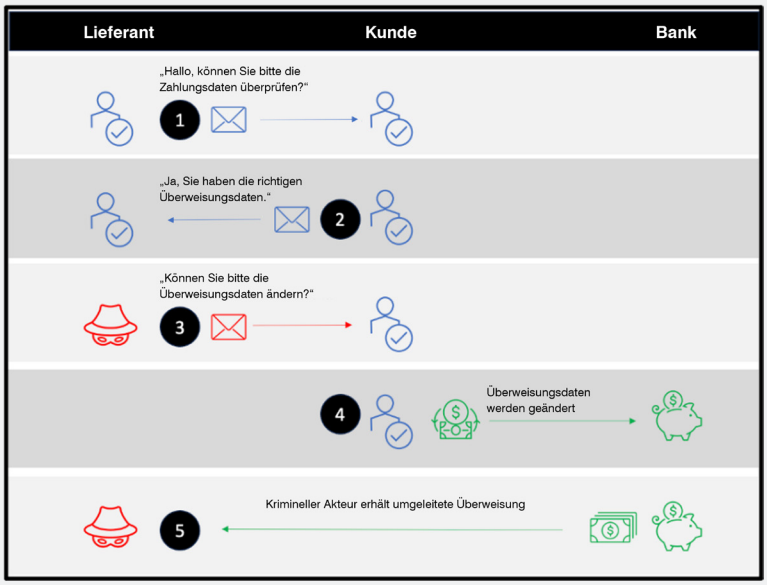


3. **Die betrügerische E-Mail des Lieferanten.** Der Angreifer schaltet sich in den Austausch ein und sendet über ein anderes E-Mail-Konto, das dem ursprünglichen zum Verwechseln ähnlich sieht, eine E-Mail an den Kunden. Tatsächlich stammte die E-Mail von einer Doppelgänger-Domain, die einen zusätzlichen Buchstaben in der E-Mail-Adresse des Absenders enthielt. Damit die E-Mail authentisch wirkte, hatte der Angreifer die gesamte E-Mail-Konversation kopiert und unten eingefügt.



Die betrügerische E-Mail des Angreifers.

4. **Abfolge des Angriffs zur Kompromittierung der Supply Chain.** Der kriminelle Akteur bat darum, die Überweisung über eine automatisierte Clearingstelle (ACH) auf ein anderes Konto vorzunehmen. Inhaber dieses neuen Kontos war der Angreifer.



Die typische Abfolge eines Supply-Chain-Angriffs.

Schwierigkeiten bei der Erkennung dieser Bedrohungen

Angriffe zur Kompromittierung der Supply Chain beinhalten selten Schaddaten. Dies ist einer der Gründe, warum sie schwer zu erkennen und zu stoppen sind. Der kriminelle Akteur überzeugt den Empfänger mithilfe von Social Engineering, ihn beim Erreichen seines Ziels zu unterstützen.

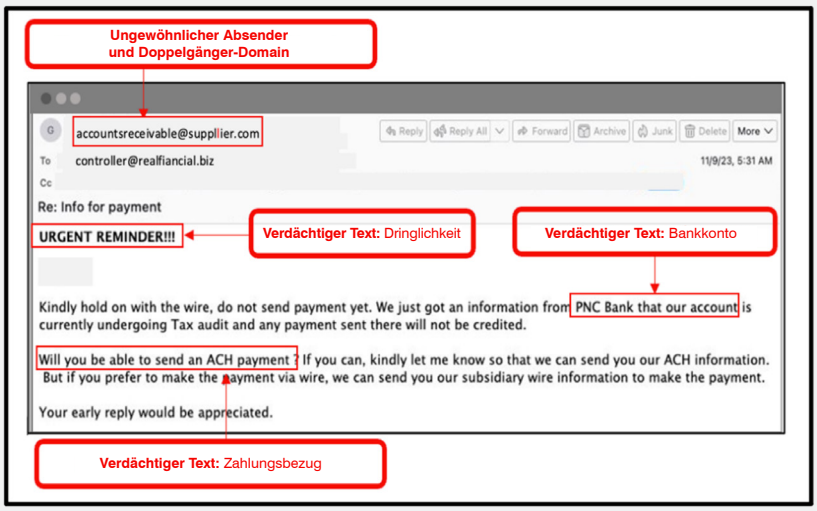
In diesem Beispiel bat der Lieferant darum, die Bankverbindungsdaten für den Zahlungseingang zu ändern. Eine solche Anfrage ist nicht unüblich, sodass API-basierte E-Mail-Sicherheitstools derartige Angriffe selten erkennen. API-basierte Tools stützen sich auf Indikatoren für unübliche Absender und generieren deshalb eine große Anzahl von False Positives und Alarmen. Angesichts dieses begrenzten verhaltensbezogenen KI-Ansatzes ist durchaus nachvollziehbar, warum viele Unternehmen über die unzähligen irrelevanten Warnmeldungen klagen, die durch Erkennungsmuster für unübliche Absender erzeugt werden.

Damit ein E-Mail-Sicherheitstool diese Arten von schädlichen Nachrichten erkennt, muss es den Tonfall im Kontext sowie die Absicht einer Nachricht interpretieren können. Denn nur so ist es möglich, das wahre Ziel einer Nachricht aufzudecken, bevor sie in den Posteingang des Empfängers zugestellt wird.

Wie Proofpoint die Bedrohung erkannt hat

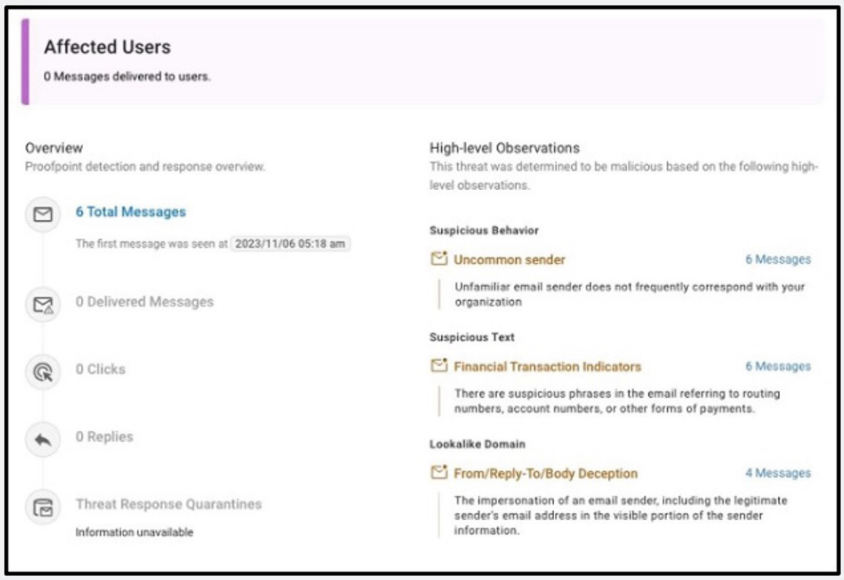
Proofpoint kombiniert Bedrohungsdaten mit verhaltensbezogener KI und ML und bestimmt auf diese Weise, ob eine geschäftliche E-Mail echt oder gefälscht ist. Wir trainieren unsere Erkennungsmodule kontinuierlich mit Millionen täglich analysierten E-Mails aus unserem weltweiten Bedrohungsdaten-Ökosystem, sodass wir beim Erkennen und Blockieren solcher Nachrichten ein höheres Maß an Konfidenz gewährleisten können.

Statt uns nur auf einen oder zwei Indikatoren zu verlassen, kombinieren wir mehrere Indikatoren. Dadurch wird eine zu große Zahl von False Positives vermieden. Ein Indikator ist die Häufigkeit und Regelmäßigkeit, mit der Absender und Empfänger Nachrichten austauschen. Zusätzlich analysieren wir den Tonfall der Sprache im Textteil der Nachricht und interpretieren die Absicht der Nachricht. Darüber hinaus achten wir auf Doppelgänger-Domains und die Dringlichkeit von Zahlungsaufforderungen.



Mehrere Bedrohungsindikatoren in einer betrügerischen Lieferanten-E-Mail.

Aufgrund des Inhalts, der Absicht und der in der E-Mail verwendeten Sprache kam Proofpoint zu dem Schluss, dass es sich bei der Nachricht in unserem Beispiel um eine betrügerische Anfrage mit Finanzbezug handelte. Diese Kampagne richtete sich nur gegen einen Kunden und beinhaltete nur wenige Nachrichten mit nachgeahmter Absenderidentität. Bei keinem anderen Kunden von Proofpoint ist dieser Angriff bislang vorgekommen.

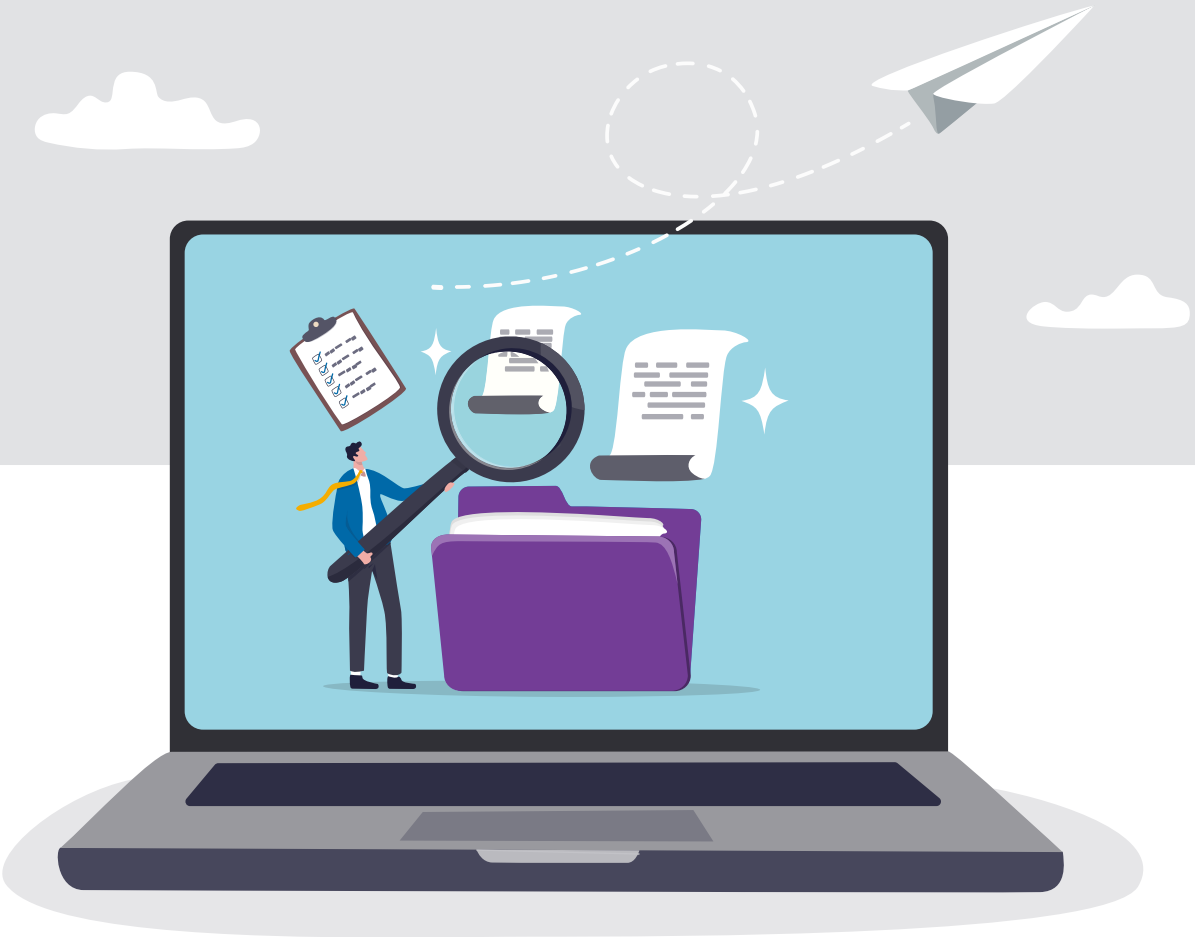


Zusammenfassung der von Proofpoint erkannten Indikatoren, die zur Einstufung der E-Mail als Bedrohung führten.

ABSCHNITT 6

Fazit

Alle diese Betrugstaktiken zeigen deutlich, warum zuverlässige mehrschichtige Cybersicherheitsmaßnahmen unverzichtbar sind.



Um mit der Entwicklung der Bedrohungen Schritt zu halten, benötigen Sie einen umfassender Ansatz zum Schutz vor personenzentrierten Bedrohungen:

- **Erkennen Sie Bedrohungen vor der Zustellung.** Sie können Ihre Anwender nur schützen, wenn Sie schädliche Nachrichten blockieren, bevor sie zugestellt werden. Untersuchungen von Proofpoint haben gezeigt, dass jeder siebte Anwender schädliche E-Mails innerhalb von einer Minute nach der Zustellung anklickt. Wählen Sie deshalb ein Tool, das ML-gestützte Algorithmen und erweiterte Bedrohungsdaten kombiniert, um komplexe Bedrohungen zu identifizieren und zu blockieren.
- **Schulen Sie Ihre Anwender.** Ihre Mitarbeiter, Auftragnehmer und Partner sind die erste Verteidigungslinie Ihres Unternehmens. Stellen Sie sicher, dass sie Security-Awareness-Schulungen zu allen Arten von Angriffen erhalten. Erinnern Sie sie daran, ungewöhnliches Verhalten von E-Mail-Absendern umgehend zu melden.
- **Führen Sie regelmäßig Audits durch.** Anhand von Audits lassen sich potenzielle Schwachstellen in Ihrer Umgebung einfacher identifizieren. Achten Sie auf Unregelmäßigkeiten in Ihren Konfigurationen und Zugriffsprotokollen.
- **Richten Sie Ihr System für die Überwachung von Konfigurationsfehlern ein.** Suchen Sie dabei nicht nur nach fehlerhaften Konfigurationen, sondern aktivieren Sie auch die automatische Behebung, damit unerlaubte Änderungen rechtzeitig und schnell korrigiert werden. Dadurch verhindern Sie, dass Angreifer Persistenz aufbauen können.
- **Erstellen Sie einen Plan für die Reaktion auf Zwischenfälle.** Definieren Sie mehrere Angriffsszenarien und legen Sie fest, wie Sie diese untersuchen und beheben werden. Testen Sie, wie effektiv Ihr Plan tatsächlich ist, indem Sie regelmäßige Simulationen durchführen.

Die nächsten Schritte

Der Schutz Ihres Unternehmens ist angesichts der zunehmenden E-Mail-Bedrohungen wichtiger denn je. Schützen Sie Ihr Unternehmen, Ihre Mitarbeiter und Ihre Kunden mit einem proaktiven Ansatz vor komplexen Angriffen wie Ransomware, BEC und Anmeldedaten-Phishing.

Mit der Risikoanalyse für E-Mail-Sicherheit von Proofpoint erhalten Sie einen umfassenden Überblick sowie wertvolle Erkenntnisse zu Angriffsrisiken und erfahren, wer mit E-Mail-basierten Bedrohungen angegriffen wird.

Warten Sie nicht zu lange, bis Sie Ihre E-Mail-Sicherheit testen. Kontaktieren Sie Proofpoint, um eine kostenlose **Risikoanalyse für E-Mail-Sicherheit** zu vereinbaren.

MEHR ERFAHREN

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 85 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.

0503-006-04-01 07/24