proofpoint.

E-BOOK

BEC aufgeschlüsselt

Das Framework zur Identifizierung, Klassifizierung und Abwehr von E-Mail-Betrug für den modernen CISO

Einführung in das Framework der Proofpoint-Taxonomie für E-Mail-Betrug

BEC-Betrug (Business Email Compromise), auch bekannt als E-Mail-Betrug, ist eine der kostspieligsten und am wenigsten verstandenen Cyberbedrohungen. Diese stark zunehmende Form von E-Mail-Betrug erregt selten so viel Aufmerksamkeit wie andere medienwirksame Cyberverbrechen, verursacht jedoch erheblich mehr direkte finanzielle Schäden als andere Betrugsformen.

Allein im Jahr 2020 führten BEC-Angriffe bei Unternehmen und Privatpersonen zu Kosten von mehr als 1,8 Milliarden US-Dollar.[1] Das sind 100 Millionen US-Dollar mehr als im Jahr 2019. Gleichzeitig hat BEC einen Anteil von 44 % an den gesamten Verlusten durch Cyberkriminalität.

Da sich die BEC-Methoden weiterentwickelt haben, ist die branchenspezifische Terminologie veraltet und nicht mehr zweckdienlich. Die Begriffe, mit denen die BEC-Taktiken und -Techniken beschrieben werden, haben ihre klare Bedeutung verloren oder werden mit anderen Begriffen vermengt und missbräuchlich verwendet. Ohne ein Framework, das BEC-Angriffe beschreibt und in Begriffe fasst, ist die Erforschung und Bewältigung der Bedrohung schwierig, wenn nicht gar unmöglich.

Wir haben daher die Proofpoint-Taxonomie für E-Mail-Betrug entwickelt. Das Framework soll Sicherheitsexperten dabei helfen, diese kostspielige Bedrohung besser identifizieren, klassifizieren und letztlich blockieren zu können.

Warum es auf die richtigen Begriffe ankommt

Mit dem Begriff „BEC“ wird häufig pauschal eine gesamte Unterklasse von E-Mail-Bedrohungen beschrieben. Das Wort wird allgemein für beliebige Taktiken und Techniken finanziell motivierter und reaktionsbasierter E-Mail-Betrugsversuche mit **Social-Engineering**-Elementen verwendet.

Das ist nicht nur eine recht komplizierte Formulierung, sondern auch ein eindeutiges Zeichen dafür, dass der Begriff „BEC“ zu viele Dinge umfasst. Die Bedrohung lässt sich mit den vorhandenen Begriffen nicht mehr beschreiben, sodass es Forscher und Unternehmen schwerer haben, BEC zu untersuchen bzw. zu bewältigen.

1. FBI: „Internet Crime Report“ (Bericht zu Internetkriminalität), März 2021.

Eine neue Sichtweise auf BEC- und E-Mail-Betrug

Wir haben diese Taxonomie geschaffen, um die wesentlichen Aspekte von BEC (und E-Mail-Betrug im Allgemeinen) vereinfacht darzustellen und hervorzuheben. Damit möchten wir Unternehmen dabei helfen, die vielen realen Formen von E-Mail-Betrug besser zu identifizieren, zu verstehen und zu bewältigen.

Identität

Wir bieten einen personenzentrierten Ansatz für E-Mail-Betrug. Unser Taxonomieschema beginnt daher mit *Identität*. Identität bezieht sich in dieser Ebene auf die Personen oder die Unternehmen, die der Bedrohungsakteur (also der Angreifer) imitiert. Wir teilen Identität in „Mitarbeiter“, „Lieferant“ und „Unbekannt“ ein. Möglicherweise sollte hier noch feiner unterschieden und „Mitarbeiter“ in „Führungskräfte“ sowie „allgemeine Mitarbeiter“ eingeteilt werden.

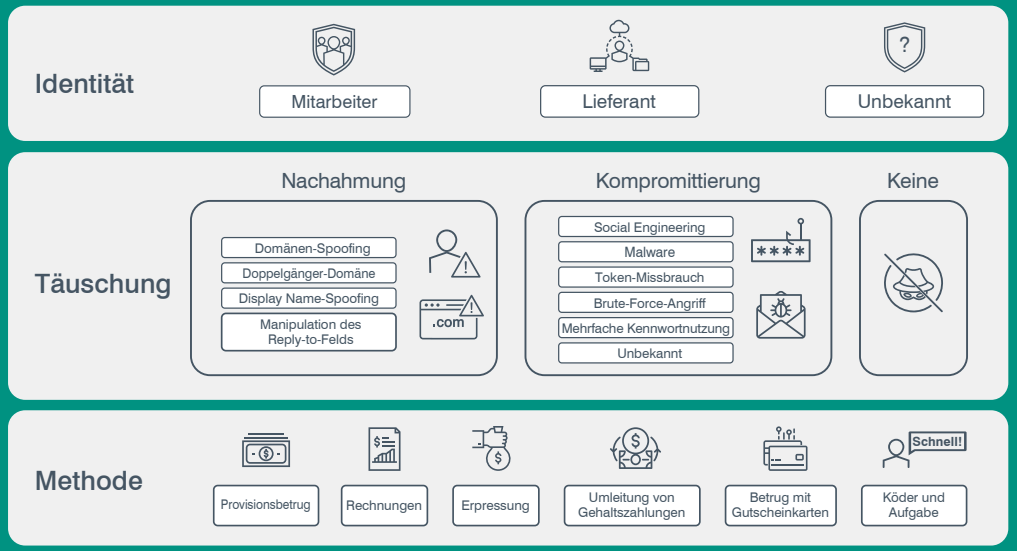


Abb. 1: Die Proofpoint-Taxonomie für E-Mail-Betrug

Täuschung

Die nächste Ebene heißt *Täuschung* und umfasst die von den E-Mail-Betrügern genutzten Techniken. Hier gibt es die Begriffe „Nachahmung“, „Kompromittierung“ und „Keine“.

„Nachahmung“ bezieht sich auf die Techniken, bei denen der Bedrohungsakteur einen oder mehrere E-Mail-Header manipuliert, um den Absender einer E-Mail zu verschleiern. Dazu zählen beispielsweise gefälschte Header, Doppelgänger-Domänen sowie andere Nachahmungstechniken.

Eine „Kompromittierung“ tritt ein, wenn der Bedrohungsakteur Zugang zu einem legitimen E-Mail-Postfach erlangt. Das Konto kann dabei vertrauenswürdigen Lieferanten, Kollegen oder Autoritätspersonen gehören. Der Empfänger hat keinen Grund, an der Echtheit der E-Mail zu zweifeln und sieht keine üblichen Anzeichen für einen Angriff.

Wenn es „keine“ Täuschungstechnik gibt, nutzt der Angreifer eine BEC-Taktik ohne Nachahmung. In diesem Fall verschickt der Bedrohungsakteur E-Mails beispielsweise über einen kostenlosen E-Mail-Anbieter, ohne etwas zu fälschen.

Methode

Die letzte Ebene *Methode* enthält Informationen, die sich am ehesten zuordnen lassen und verwertbar sind. Diese Ebene bildet den mit Abstand wichtigsten Teil der Taxonomie. Hier einige Beispiele für Methoden:

- Rechnungsbetrug
- Umleitung von Gehaltszahlungen
- Erpressung
- Köder und Aufgaben
- Betrug mit Gutscheinkarten
- Provisionsbetrug

Diese Methoden decken die Kategorien ab, die wir in Bezug auf die BEC-Bedrohungslandschaft als besonders relevant erachten und die den größten Nutzen für verschiedenste Unternehmen haben. Sie sind allgemein genug, um Abstufungen zu berücksichtigen – denn jeder Angriff ist einzigartig –, und gleichzeitig spezifisch genug, um Sie bei der Identifizierung, Klassifizierung und Bewältigung der gesamten Bandbreite an BEC-Bedrohungen unterstützen zu können.

Methode 1: Rechnungsbetrug

Rechnungsbetrug ist im Prinzip der Versuch, eine Person durch Täuschung dazu zu bringen, Produkte oder Dienstleistungen zu bezahlen, die sie nicht gekauft hat, oder eine legitime Zahlung auf das Konto des Angreifers umzuleiten. Von den E-Mail-Betrugsmethoden in unserer Taxonomie verursacht Rechnungsbetrug wahrscheinlich die größten Kosten. Da B2B-Transaktionen (Business-to-Business) häufig vorkommen und große Beträge umfassen, bieten sie Betrügern reichlich Gelegenheit und Anreiz, das große Geld zu machen.

Die Betreffzeilen betrügerischer Rechnungs-E-Mails sind meist auf die Zahlung bezogen. Die gefälschten Rechnungen sind dabei mitunter täuschend echt gestaltet und enthalten Unternehmenslogos, professionelle Formatierungen und Ähnliches. Zudem können die E-Mails konkrete Anschuldigungen enthalten und das Opfer unter Zeitdruck setzen: „Die Rechnung ist 90 Tage überfällig und muss sofort bezahlt werden." Der Bedrohungsakteur verwendet häufig Drohungen, wenn der Empfänger nicht schnell reagiert.

Auf der *Identitätsebene* kann eine betrügerische Rechnung den Eindruck erwecken, von einer beliebigen Personen ausgestellt worden zu sein – seien es Kollegen oder Personen außerhalb des Unternehmens. Am erfolgreichsten sind jedoch Betrugsversuche, die vorhandene Lieferantenbeziehungen ausnutzen. Angriffe auf Lieferanten sind ein Paradebeispiel für Rechnungsbetrug und können Unternehmen zehntausende bis mehrere Millionen US-Dollar kosten.

Funktionsweise

Auf der *Täuschungsebene* erfolgt Lieferantenbetrug entweder durch Nachahmung oder Kompromittierung.

Nachahmung

Bei der Nachahmung imitiert ein Bedrohungsakteur mittels E-Mail-Spoofing einen Lieferanten. Häufig werden diese betrügerischen E-Mails über kostenlose Webmail-Domänen oder von fremden kompromittierten Konten verschickt, die der Bedrohungsakteur kontrolliert.

Wie Sie in Abb. 2 sehen, kann eine Nachahmung durchaus komplex sein. In einigen Fällen ahmen die Angreifer zunächst das ins Visier genommene Unternehmen nach, um vom Lieferanten eine echte Rechnung zu bekommen – und ahmen mit dieser Rechnung wiederum den Lieferanten nach. (Da hier eine echte Rechnung von einem tatsächlichen Lieferanten im Spiel ist, erscheint der doppelseitige Angriff womöglich zunächst als Kontenkompromittierung.)

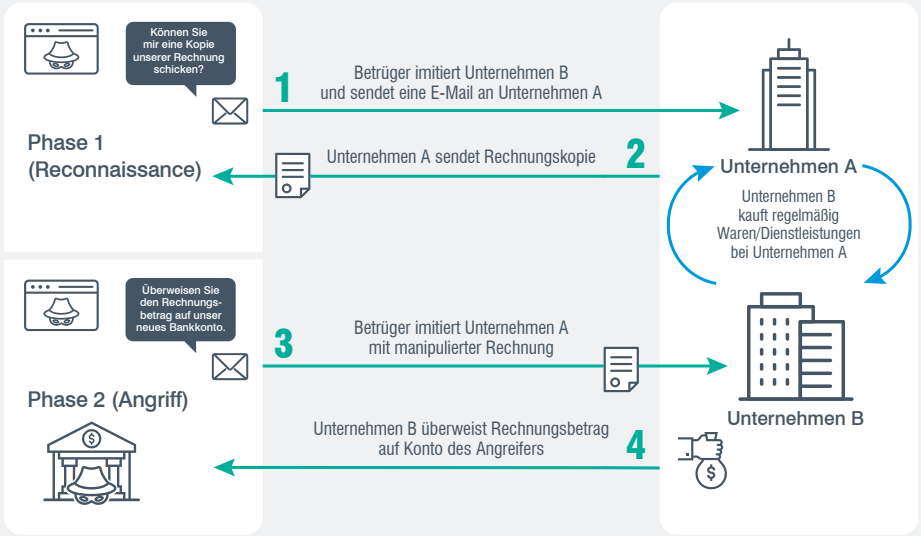


Abb. 2: Ablauf eines Lieferantenbetrugsversuchs, bei dem die Angreifer auf mehreren Ebenen Nachahmungsmethoden einsetzen

Kompromittierung

Bei der Lieferantenkompromittierung erlangt ein Bedrohungsakteur nicht autorisierten Zugang zum vertrauenswürdigen E-Mail-Konto eines Lieferanten und führt darüber BEC-Angriffe gegen die Kunden des Lieferanten durch. Den Zugriff auf das Konto erlangen die Angreifer in der Regel durch Phishing-Kampagnen oder den Kauf von Anmeldedaten.

In einigen Fällen nutzen die Angreifer sogar existierende E-Mail-Threads eines kompromittierten Kontos aus. (Diese Technik wird als „Thread-Hijacking“ bezeichnet.) Sie beobachten die realen Gespräche in einem E-Mail-Thread, imitieren diese oder reagieren darauf – und können dadurch glaubwürdige Nachrichten mit passenden Dokumenten verfassen.

Das kann als die ultimative Nachahmungstaktik bezeichnet werden. Die BEC-E-Mails werden zum Bestandteil eines aktiven Gespräches. Der Empfänger hat keinen Grund anzunehmen, dass die Person, mit der er gerade kommuniziert hat, plötzlich durch einen Impostor ersetzt wurde. Es sollte daher nicht verwundern, dass derartige E-Mails zu den überzeugendsten BEC-Betrugsversuchen zählen, die Anwender je zu Gesicht bekommen.

Warum nicht beides?

Häufig setzen Bedrohungsakteure sowohl Nachahmung als auch Kompromittierung als Täuschungstaktiken ein. Ein Teil der Angriffe ist zielgerichtet, doch viele sind opportunistisch und gehen auf Informationen zurück, die Angreifer während der Kompromittierung von Lieferketten in die Hände bekommen haben. (Wie Abb. 3 zeigt, berücksichtigt unsere Taxonomie diesen feinen Unterschied und klassifiziert solche Angriffe auf der *Täuschungsebene* als Kompromittierung und Nachahmung.)

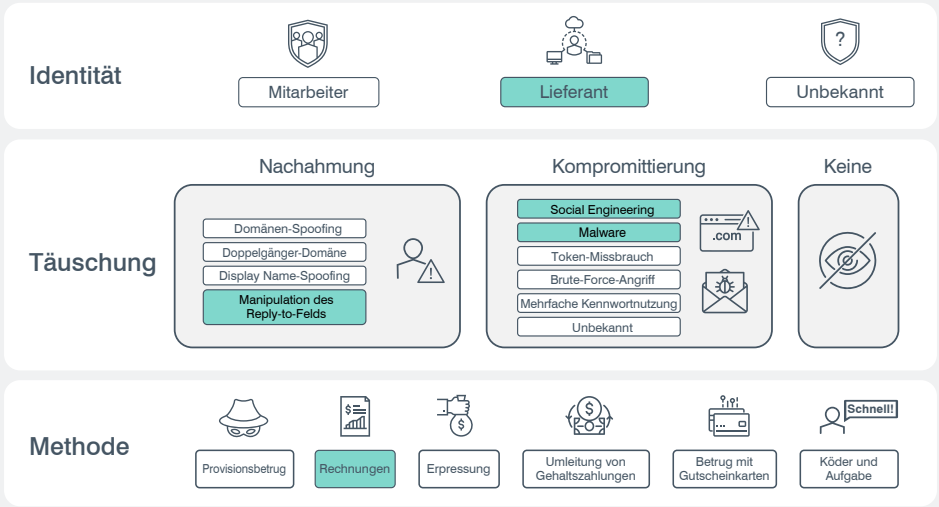


Abb. 3: Beispiel für Lieferantenbetrug mit den Täuschungstaktiken Nachahmung und Kompromittierung

Ein konkretes Beispiel

Vor kurzem beobachteten wir einen Lieferantenbetrugsversuch, bei dem der Angreifer ein Unternehmen um mehr als 100.000 US-Dollar betrügen wollte und sich dafür als der übliche Weinlieferant ausgab.

Er antwortete auf einen vorhandenen E-Mail-Thread zwischen dem Kunden und dem Lieferanten und bat den Kunden darum, den Betrag direkt auf ein angegebenes Konto zu überweisen. (Wie Abb. 4 zeigt, forderte die Nachricht zudem dazu auf, die gesamte Kommunikation per E-Mail abzuwickeln.) Obwohl der Angreifer einen realen E-Mail-Thread gekapert hatte und Insiderwissen über den Lieferanten zu haben schien, erfolgte der Angriff mithilfe gefälschter E-Mails und nicht über ein kompromittiertes E-Mail-Konto.

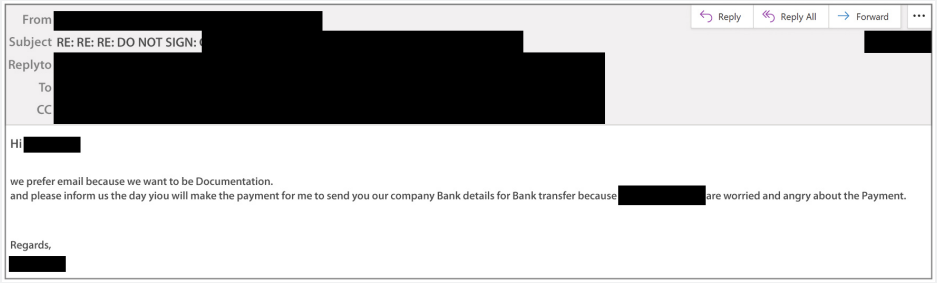


Abb. 4: Der erste Rechnungsbetrugsversuch

In Abb. 5 ist zu sehen, wie der Bedrohungsakteur seinem Anliegen noch einmal Nachdruck verlieh, nachdem er keine zufriedenstellende Reaktion erhalten hatte. Die E-Mail enthielt eine detaillierte Rechnung, die durch das Logo und den Stempel des Lieferanten noch überzeugender wirken sollte (siehe Abb. 6 auf der nächsten Seite).

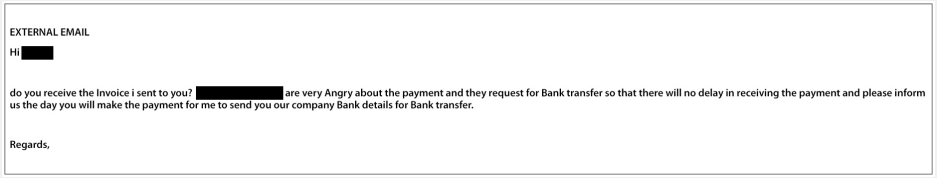
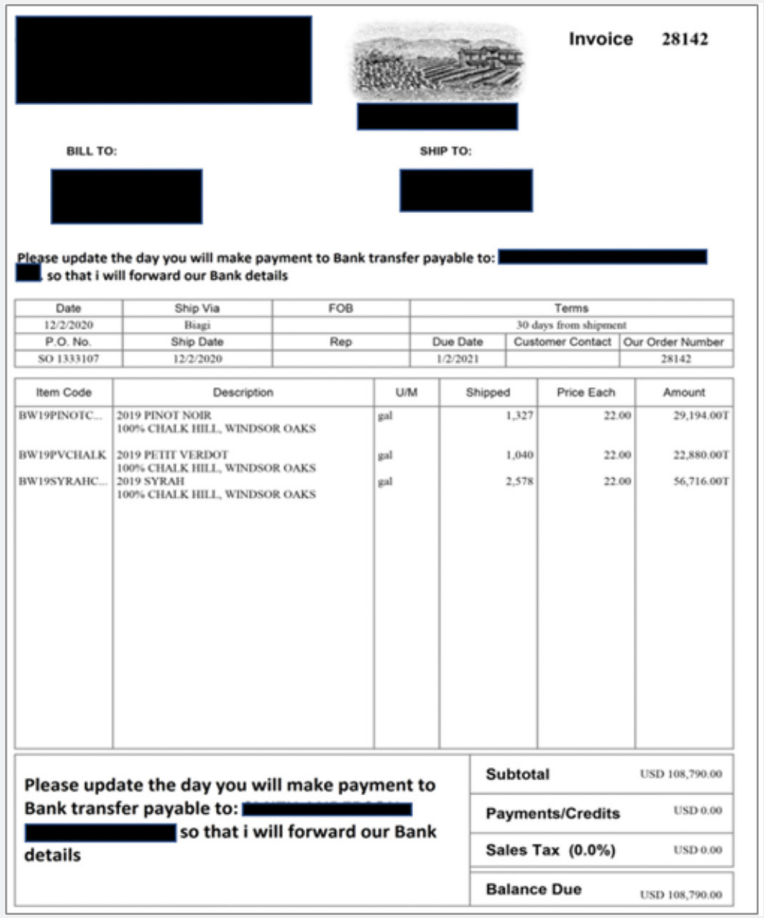


Abb. 5: Ein weiterer Versuch desselben Angreifers



[redacted]

Invoice 28142

BILL TO:

[redacted]

SHIP TO:

[redacted]

Please update the day you will make payment to Bank transfer payable to: [redacted]
[redacted] so that i will forward our Bank details

Date	Ship Via	FOB	Terms		
12/2/2020	Biagi		30 days from shipment		
P.O. No.	Ship Date	Rep	Due Date	Customer Contact	Our Order Number
SO 1333107	12/2/2020		1/2/2021		28142

Item Code	Description	U/M	Shipped	Price Each	Amount
BW19PINOTC...	2019 PINOT NOIR 100% CHALK HILL, WINDSOR OAKS	gal	1,327	22.00	29,194.00T
BW19PVCHALK	2019 PETIT VERDOT 100% CHALK HILL, WINDSOR OAKS	gal	1,040	22.00	22,880.00T
BW19SYRAHC...	2019 SYRAH 100% CHALK HILL, WINDSOR OAKS	gal	2,578	22.00	56,716.00T

Please update the day you will make payment to Bank transfer payable to: [redacted] so that i will forward our Bank details

Subtotal	USD 108,790.00
Payments/Credits	USD 0.00
Sales Tax (0.0%)	USD 0.00
Balance Due	USD 108,790.00

Abb. 6: PDF-Datei der Rechnung

Da die E-Mails Informationen enthielten, die nur der echte Weinlieferant wissen konnte, vermuten wir, dass der Lieferant vor dem BEC-Betrugsversuch kompromittiert wurde. Wahrscheinlich gelangte der Angreifer durch die Kompromittierung an die Informationen und wusste daher, wie er den Anzeigenamen und das Reply-To-Feld manipulieren musste, um den Anbieter nachzuahmen. (Abb. 7 zeigt, wie wir diesen Angriff zuordnen.)

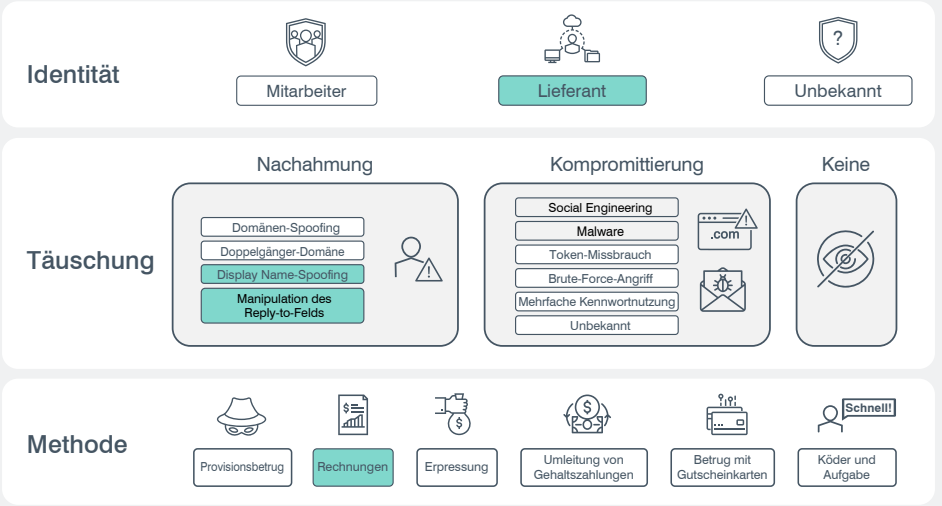


Abb. 7: Praxisbeispiel für einen Lieferantenbetrug

Methode 2: Umleitung von Gehaltszahlungen

Umleitungen von Gehaltszahlungen zählen zu den schlichtesten BEC-Betrugsmethoden, die wir zu sehen bekommen. Egal ob sich ein Angriff gegen die Finanz-, Steuer- bzw. Personalabteilung oder die Lohnbuchhaltung richtet, der Zweck ist stets einfach: Die Empfänger sollen dazu gebracht werden, die schwer erarbeiteten Gehälter der Mitarbeiter zum Angreifer umzuleiten.

Wir erkennen pro Tag etwa 2.000 Umleitungsversuche von Gehaltszahlungen (siehe Abb. 8) und stufen diese Angriffe als mittleres Risiko für Unternehmen ein.

Dem FBI zufolge beträgt der durchschnittliche Verlust durch solche Angriffe 7.904 US-Dollar pro gemeldetem Zwischenfall.[2] Die US-Steuerbehörde IRS führt Umleitungen von Gehaltszahlungen auf ihrer „Dirty Dozen"-Liste von Steuerbetrugsmaschen für das Jahr 2020.[3] Der Behörde zufolge versuchen Angreifer, ihre Opfer mithilfe von IRS-Dokumenten von der Echtheit betrügerischer Kontodatenänderungen zu überzeugen.

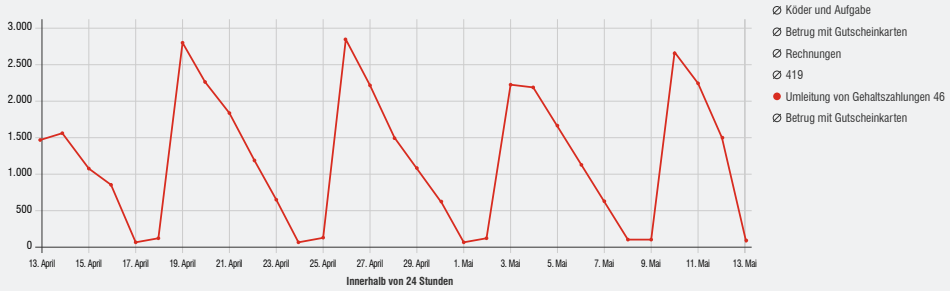


Abb. 8: Umleitungsversuche von Gehaltszahlungen (Gesamtanzahl in einem Zeitraum von 24 Stunden, vom 13.04. bis 13.05.2021)

1. FBI: „2020 Internet Crime Report" (Bericht zu Internetkriminalität 2020), März 2021.
2. IRS: „Dirty Dozen" (Das schmutzige Dutzend), September 2021.

Funktionsweise

Bei Umleitungsversuchen von Gehaltszahlungen wird die Kompromittierung zwar mitunter als *Täuschungstechnik* verwendet, doch in der Regel greifen die Kriminellen zur Nachahmung. (Bedrohungsakteure, die Zugang zu kompromittierten Konten haben, konzentrieren sich eher auf lukrativere BEC-Methoden wie Rechnungsbetrug.)

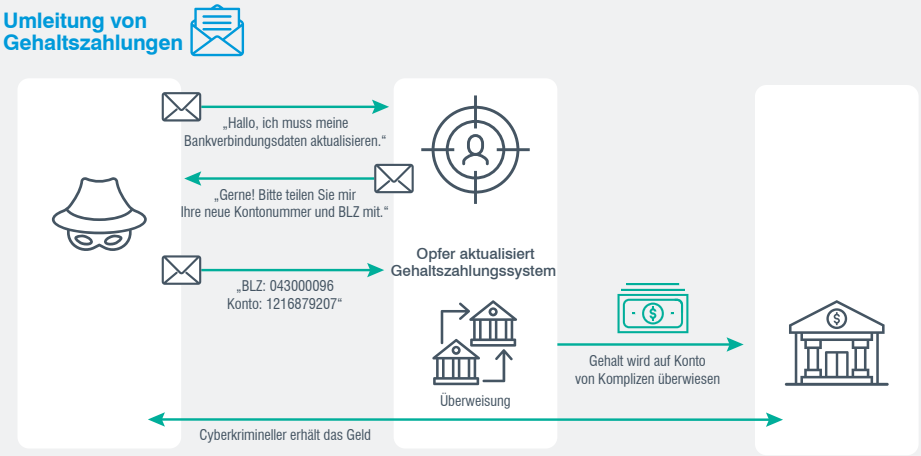


Abb. 9: Ablauf eines Angriffs mit Umleitung von Gehaltszahlungen, der Nachahmung einsetzt

Die meisten Angriffe mit Nachahmung werden über kostenlose E-Mail-Dienste wie Gmail verschickt. In der Regel fälschen die Bedrohungsakteure den Anzeigenamen, damit die E-Mail den Eindruck erweckt, von einem Mitarbeiter zu stammen (siehe Abb. 9 oben).

In einigen Fällen nehmen die Angreifer hochrangige Mitarbeiter und Führungskräfte ins Visier, um größere Gehälter zu erbeuten. Um ihre E-Mails glaubwürdiger wirken zu lassen, nutzen die Bedrohungsakteure E-Mail-Adressen, die von anderen Führungskräften zu stammen scheinen. Und die pflichtbewussten Opfer werden durch Dringlichkeit zum Handeln bewegt. (Siehe Abb. 10 auf der nächsten Seite. Andere aktuelle Beispiele sind „ceo@companywebaxccs.com" und „ceo_task2@icloud.com".)

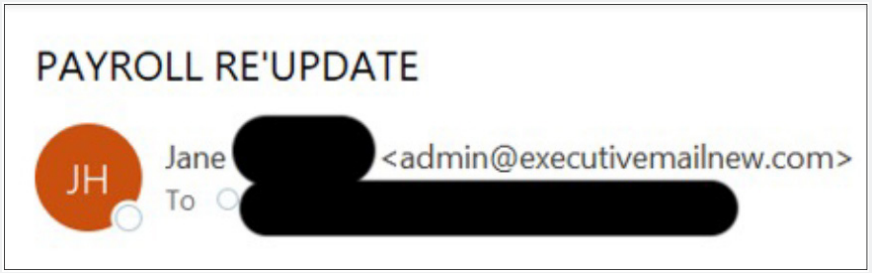


Abb. 10: Eine E-Mail-Domäne, die Autorität vermitteln soll

In Abb. 11 sehen Sie, wie unsere Taxonomie die beiden oben beschriebenen Angriffe einordnen würde.

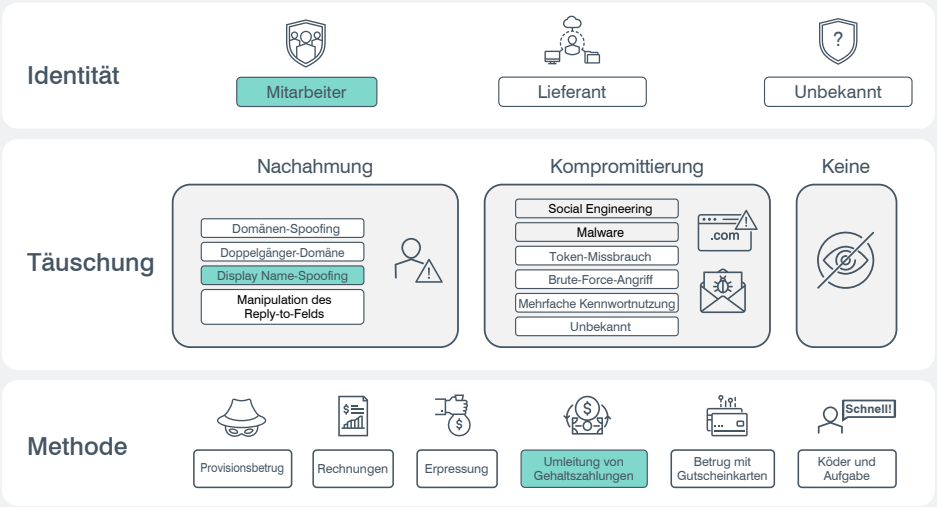


Abb. 11: Angriff mit Umleitung von Gehaltszahlungen mit gefälschtem Anzeigenamen

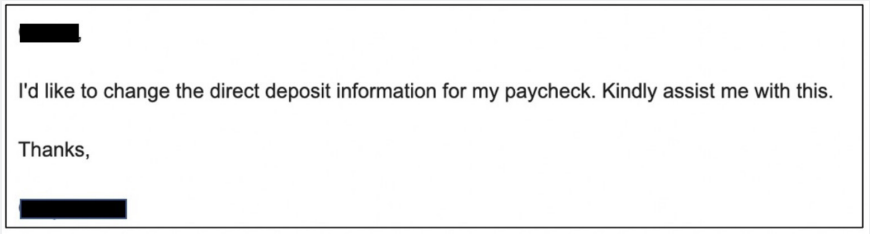
Reale Beispiele

Umleitungen von Gehaltszahlungen sind vor allem an ihrem einfachen Aufbau erkennbar. In einem kürzlich von uns beobachteten Angriff ahmte der Bedrohungsakteur mehrere Mitarbeiter in E-Mails nach, die er an die Gehaltsabteilung eines Großunternehmens schickte. Abb. 12 zeigt, dass alle E-Mails den gleichen Inhalt hatten und sich nur in folgenden Punkten unterschieden:

- An wen die E-Mail gesendet wurde
- Wer imitiert wurde
- Welche Sprache verwendet wurde (englisch, deutsch oder spanisch)

Abb. 12: Beispiel von E-Mails, in denen Mitarbeiter nachgeahmt wurden, um Gehaltszahlungen umzuleiten

Einige Betrugsversuche sind noch einfacher und dreister. Abb. 13 zeigt den Versuch eines Angreifers, den Geschäftsführer eines Unternehmens zu imitieren.


[redacted]

I'd like to change the direct deposit information for my paycheck. Kindly assist me with this.

Thanks,

[redacted]

Abb. 13: E-Mail, die einen Geschäftsführer nachahmt, um Gehaltszahlungen umzuleiten

Obwohl diese Angriffe so einfach aufgebaut sind, können sie doch äußerst wirksam sein, da die Angreifer hier einen normalen Geschäftsprozess ausnutzen. Die Mitarbeiter von Lohnbuchhaltungs-, Finanz-, Steuer- und Personalabteilungen erhalten beinahe täglich E-Mails mit solchen Anfragen, von denen die meisten echt sind.

Methode 3: Erpressung

E-Mail-Betrug mit Erpressung funktioniert genauso wie andere Formen der Erpressung. Die Angreifer drohen den Opfern damit, Eigentum zu zerstören, Gewalttaten zu verüben oder vertrauliche, peinliche oder kompromittierende Informationen zu veröffentlichen, um sie dazu zu bringen, den Angreifern Geld (in der Regel Kryptowährung) zu zahlen oder andere Wertsachen zu überlassen. Erpressung lässt sich in folgende Unterarten gliedern:

- **Veröffentlichung von Daten:** Der Bedrohungsakteur droht damit, vertrauliche, peinliche oder kompromittierende Informationen, wie zum Beispiel Kundendaten, Geschäftsgeheimnisse oder (echte oder gefälschte) Beweise für strafbare Aktivitäten, zu veröffentlichen.
- **DDoS-Angriffe (Distributed Denial of Service):** Der Angreifer droht, den Online-Betrieb des Opfers mit Datenverkehr zu überfluten und damit für legitime Anwender unzugänglich zu machen.
- **Körperlicher Schaden:** Der Angreifer droht dem Empfänger oder dem Unternehmen körperlichen Schaden an. Häufig genutzte Taktiken sind Bombendrohungen, Androhungen von Auftragsmorden und Warnungen vor möglichen Gewalttaten.
- **Sextortion:** Der Angreifer droht, Fotos und Videos des Opfers mit sexuellem Hintergrund zu veröffentlichen. Sextortion ist wahrscheinlich die am weitesten verbreitete dieser Erpressungsarten.

Funktionsweise

Anders als die anderen in diesem E-Book aufgeführten Methoden kommt beim E-Mail-Betrug mit Erpressung nur eine Täuschungstaktik – die Nachahmung – zum Einsatz. In einigen Fällen wird auch gar keine verwendet. Wenn der Angreifer auf Nachahmung setzt, versucht er meist, die E-Mail so aussehen zu lassen, als stamme sie vom E-Mail-Konto des Opfers.

In der Regel schickt der Bedrohungsakteur den Opfern eine E-Mail, in der er behauptet, er habe auf ihren Rechner zugegriffen und beim Anschauen nicht jugendfreier Inhalte aufgezeichnet. Die E-Mail enthält vertrauliche Inhalte, die so aussehen, als kämen sie vom eigenen E-Mail-Konto des Empfängers. Der Angreifer droht dem Empfänger, die unangenehmen Inhalte an Kollegen und Familienmitglieder weiterzuleiten, wenn er nicht zahlt.

Abb. 14 zeigt, wie sich ein solcher Angriff in unser BEC-Framework einordnen lässt.

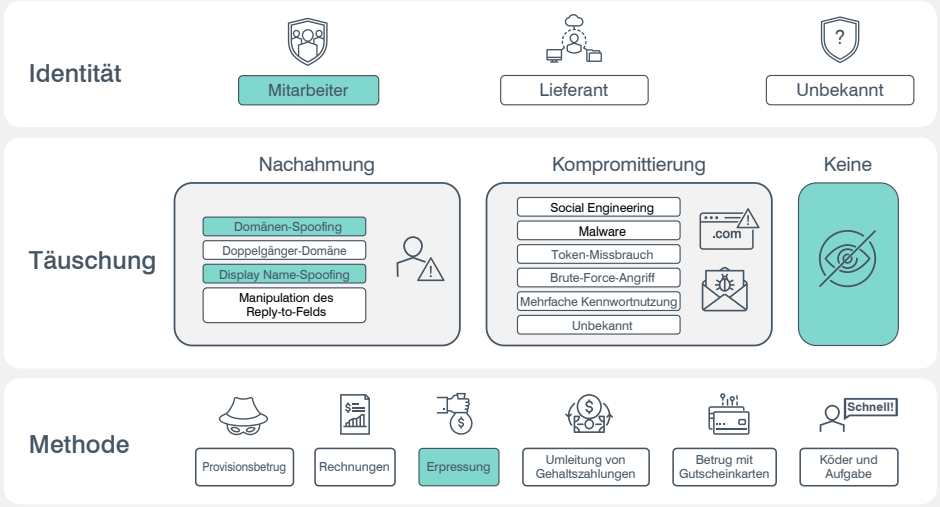


Abb. 14

Sofern die Angreifer nicht versuchen, sich als jemand anderes auszugeben, nutzen sie in der Regel kostenlose E-Mail-Anbieter und verzichten auf eine gefälschte Adresse. Ein solches Szenario lässt sich folgendermaßen in das Framework einordnen (Abb. 15).

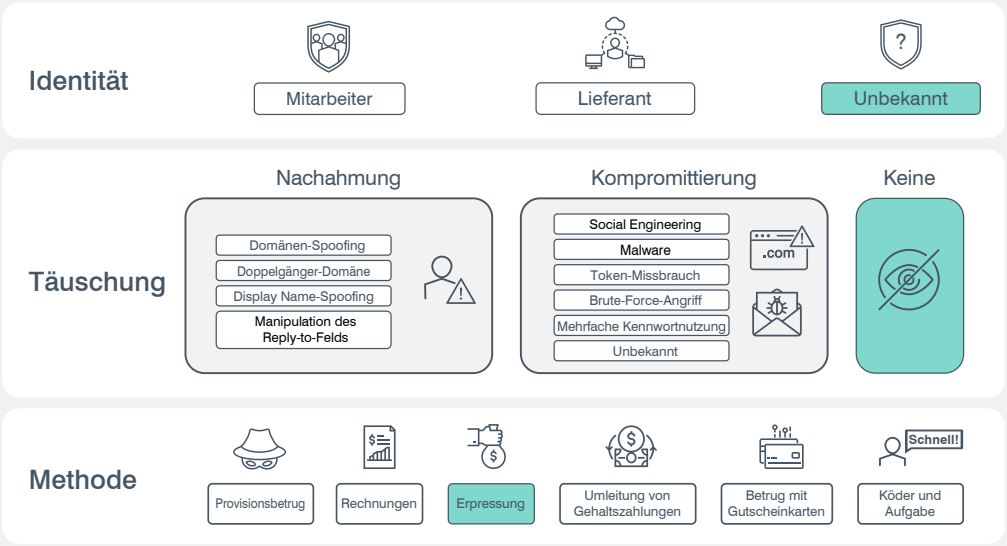
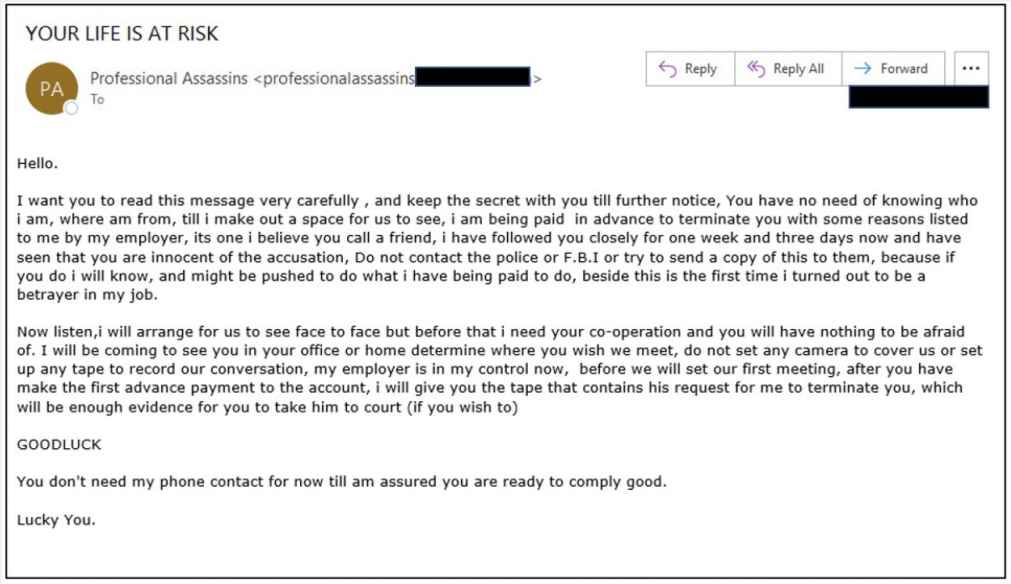


Abb. 15: Einige Erpressungsmethoden verwenden keine Taktiken zur Identitätstäuschung



YOUR LIFE IS AT RISK

PA Professional Assassins <professionalassassins[redacted]>
To

Reply | Reply All | Forward | ...

Hello.

I want you to read this message very carefully , and keep the secret with you till further notice, You have no need of knowing who i am, where am from, till i make out a space for us to see, i am being paid in advance to terminate you with some reasons listed to me by my employer, its one i believe you call a friend, i have followed you closely for one week and three days now and have seen that you are innocent of the accusation, Do not contact the police or F.B.I or try to send a copy of this to them, because if you do i will know, and might be pushed to do what i have being paid to do, beside this is the first time i turned out to be a betrayer in my job.

Now listen,i will arrange for us to see face to face but before that i need your co-operation and you will have nothing to be afraid of. I will be coming to see you in your office or home determine where you wish we meet, do not set any camera to cover us or set up any tape to record our conversation, my employer is in my control now, before we will set our first meeting, after you have make the first advance payment to the account, i will give you the tape that contains his request for me to terminate you, which will be enough evidence for you to take him to court (if you wish to)

GOODLUCK

You don't need my phone contact for now till am assured you are ready to comply good.

Lucky You.

Abb. 16: Ein Erpressungsversuch, bei dem versichert wird, einen angeblichen Auftragsmord zurückzuziehen, wenn der Empfänger dem Absender Geld schickt

Reale Beispiele

Sextortion ist unserer Erfahrung nach die mit Abstand häufigste Form der Erpressung. Häufig sind die E-Mails lang und ausführlich, das Ziel ist jedoch recht einfach: die Opfer davon zu überzeugen, sie befänden sich in einer prekären Lage und müssten die Forderungen des Bedrohungsakteurs erfüllen.

Androhungen körperlicher Gewalt kommen seltener vor, wirken jedoch auf die Opfer verständlicherweise sehr bedrohlich. Wie Sie in Abb. 16 sehen, soll den Opfern mit diesen Schlägertaktiken Angst gemacht werden, um sie zur Zahlung zu bewegen.

Wichtige Merkmale dieser Methode sind Zeitdruck, kurze Zahlungsfristen und die eindringliche Warnung, die Polizei nicht zu kontaktieren.

Methode 4: Köder und Aufgaben

Aufgrund ihres simplen Vorgehens werden E-Mails mit Ködern und Aufgaben schnell übersehen. Sie fangen mit einer Bitte um einen einfachen alltäglichen Gefallen an. Während einige Angriffe gleich mit einer Bitte beginnen, sind viele davon vage formuliert und sollen das Opfer im Verlauf mehrerer E-Mails einwickeln. In diesen Fällen enthält die erste Nachricht meist allgemeine Anfragen wie folgende:

- „Haben Sie gerade Zeit?“
- „Könnten Sie mir schnell einen Gefallen tun?“
- „Hätten Sie vielleicht einen Moment Zeit?“
- „Sind Sie da? Ich hätte gerne, dass Sie mir Gutscheinkarten kaufen.“

Köder und Aufgaben sind häufig ein Einstieg in mehrphasige Angriffe, die andere E-Mail-Betrugsmethoden umfassen. Eine Köder- und Aufgaben-E-Mail soll zunächst die Aufmerksamkeit des Empfängers wecken. Das eigentliche Ziel des Bedrohungsakteurs (z. B. Umleitungen von Überweisungen oder Rechnungsbetrug) tritt erst im Laufe der Zeit zu Tage.

Diese Angriffe bestehen aus mehreren Kategorien und lassen sich daher nur schwer einordnen. Unsere Taxonomie-Einordnung von Köder- und Aufgaben-E-Mails im Vergleich zu anderen E-Mails hängt davon ab, ob wir erkennen können, was der Bedrohungsakteur als Nächstes tut. Wenn wir nur eine einzige Köder- bzw. Aufgaben-E-Mail sehen, klassifizieren wir sie als solche. Können wir anhand der nachfolgenden E-Mails ein anderes Ziel über den Köder bzw. die Aufgabe hinaus erkennen, ordnen wir sie sowohl als Köder- und Aufgaben-E-Mail als auch als eine andere Methode ein.

Funktionsweise

Köder- und Aufgaben-E-Mails verwenden nur eine einzige Form der *Täuschung* in unserer Taxonomie: Nachahmung. In der Regel geben sich die Angreifer als eine Person aus, die das Opfer kennt oder der sie vertraut. Dazu zählen zum Beispiel:

- Private und berufliche Autoritätspersonen
- Enge Freunde
- Familienmitglieder

Wenn sich die Angreifer als eine vertraute Person ausgeben, können sie die Zweifel zerstreuen, die die Empfänger bei einer unerwarteten oder ungewöhnlichen Anfrage haben könnten, und zwingen diese somit beinahe zu einer Reaktion.

Durch eine Antwort wird das erste Ziel des Bedrohungsakteurs erfüllt: ein aktives E-Mail-Konto und damit potenziell empfängliche Opfer auszumachen.

Wie in Abb. 17 dargestellt, täuschen die meisten Köder- und Aufgaben-E-Mails das Opfer mit einem gefälschten Anzeigenamen. In einigen Fällen werden andere Nachahmungstaktiken wie gefälschte Domänen oder Reply-to-Adressen verwendet. Wenn der Bedrohungsakteur eine Reaktion erhält, ändert er möglicherweise seine Täuschungstaktiken, um seine Glaubwürdigkeit zu erhöhen.

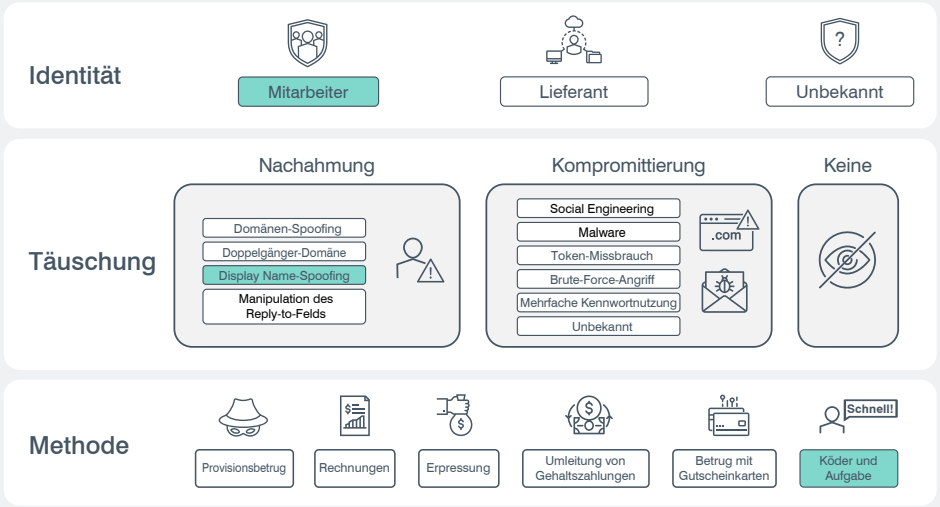


Abb. 17

Reale Beispiele

Viele der von uns beobachteten Betrugsversuche mit Ködern und Aufgaben beginnen mit einer kurzen E-Mail, mit der getestet wird, wie empfänglich das Ziel ist. Wie Abb. 18 zeigt, wird in diesen ersten E-Mails häufig noch kein Gefühl der Dringlichkeit erzeugt.

Abb. 18: Die erste Köder- und Aufgaben-E-Mail

E-Mail-Betrug durch Köder und Aufgaben ist weit verbreitet und macht unseren Beobachtungen zufolge mehr als die Hälfte der Bedrohungen im Jahr 2021 aus. (Wir blockieren täglich etwa 30.000 dieser E-Mails.)

Die E-Mails machen zunächst einen harmlosen Eindruck. Fällt das Opfer jedoch auf sie herein, können darauf schwerere Formen des E-Mail-Betrugs folgen (z. B. Betrug mit Gutscheinkarten, Rechnungsbetrug, Umleitungen von Gehaltszahlungen), die hohe Kosten verursachen können.

Methode 5: Betrug mit Gutscheinkarten

Beim Betrug mit Gutscheinkarten erbeuten Bedrohungsakteure Geld in Form von Gutscheinkarten. Die Opfer werden dazu gebracht, die Karten zu kaufen und den Angreifern die Nummern und PINs zu schicken. Diese lösen die Karten ein oder verkaufen sie weiter.

Diese Methode funktioniert nur, weil Unternehmen ihre Mitarbeiter und Partner häufig mit Gutscheinkarten belohnen, weshalb die Anfrage auf die Opfer nicht immer ungewöhnlich wirkt. Wenn die E-Mail dringend klingt und eine vernünftige Erklärung enthält, handeln die meisten Empfänger daher ohne nachzudenken.

Funktionsweise

Um die Bitte legitim erscheinen zu lassen, ahmen die Bedrohungsakteure auf der *Täuschungsebene* häufig eine Führungskraft oder Autoritätsperson nach. Wie auch bei anderen Formen des E-Mail-Betrugs fallen die Opfer eher auf die Methode herein, wenn sich die Angreifer als vertraute Personen wie Freunde oder Familienmitglieder ausgeben.

Bei den meisten Betrugsversuchen mit Gutscheinkarten werden die Empfänger mit gefälschten Anzeigenamen getäuscht (siehe Abb. 19). In einigen Fällen kommen andere Nachahmungstaktiken wie gefälschte Domänen oder manipulierte Reply-to-Adressen zum Einsatz.

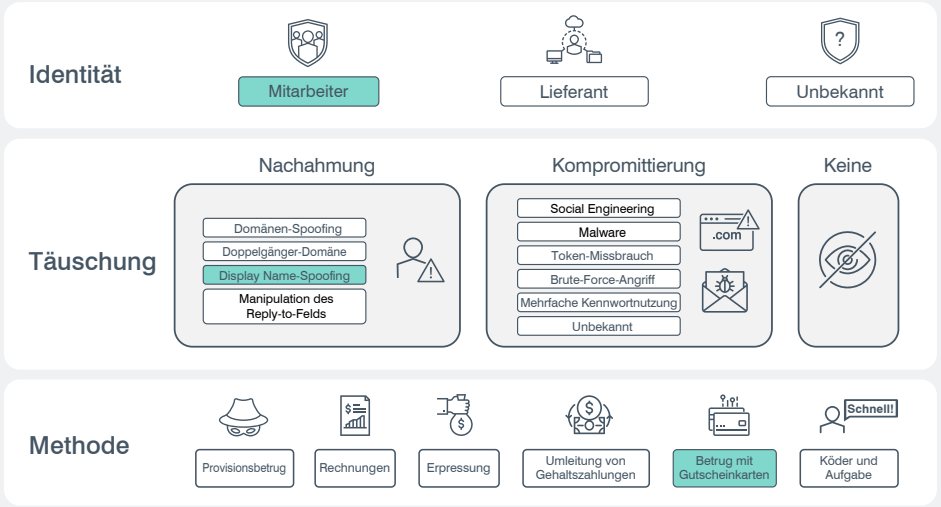


Abb. 19: Taxonomie für den Betrug mit Gutscheinkarten

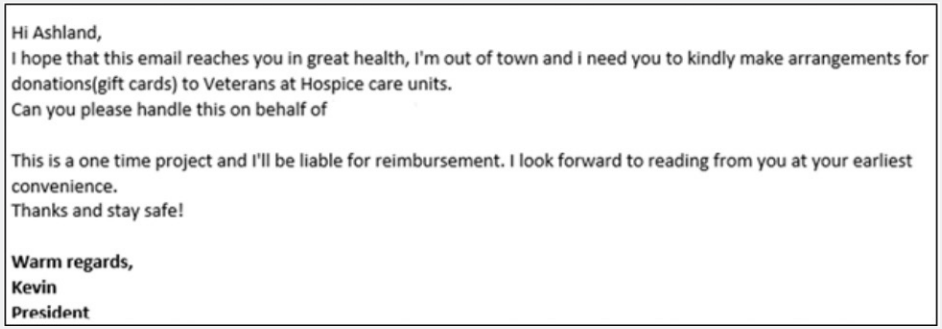
Reale Beispiele

Um die E-Mails legitim erscheinen zu lassen, werden beim Betrug mit Gutscheinkarten alle möglichen Arten von Ködern eingesetzt (siehe Abb. 20, Abb. 21 und Abb. 22 auf der nächsten Seite). Die Bedrohungsakteure nutzen aktuelle Ereignisse wie die Pandemie oder nationale Feiertage für ihre Zwecke. Egal, wie der Köder aussieht: Das Ziel ist, einen plausiblen Grund für die Bitte anzugeben und Mitgefühl zu erzeugen, um die Erfolgschancen zu erhöhen.

Mitgefühl mit dem Betrüger

Abb. 20 und 21 veranschaulichen, wie sehr die Bedrohungsakteure auf die Tränendrüse drücken.

In Abb. 20 behauptet der Absender, es gehe um nichts Geringeres als ein Hospiz für Kriegsveteranen. In Abb. 21 behaupten die Angreifer dagegen, sie seien nicht in der Stadt, müssten sich – wahrscheinlich pandemiebedingt – isolieren und könnten deshalb kein Geschenk für den anstehenden Geburtstag der Nichte besorgen.

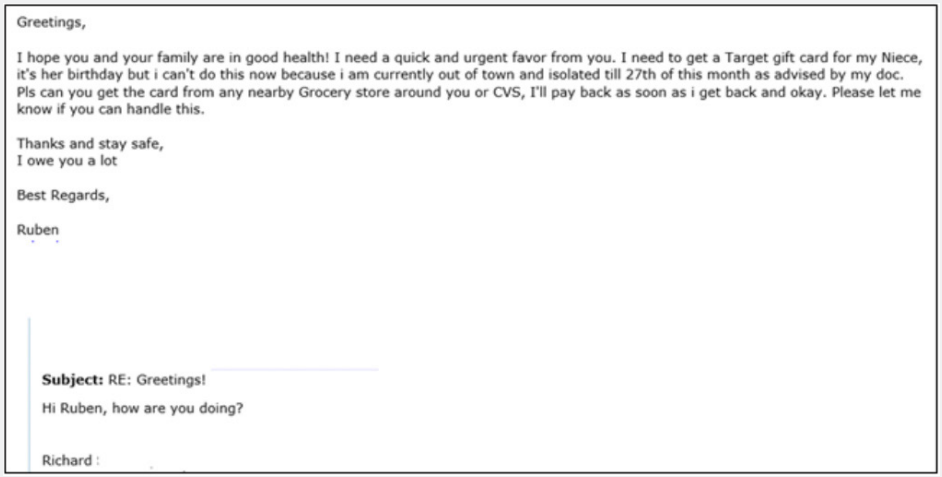


Hi Ashland,
I hope that this email reaches you in great health, I'm out of town and i need you to kindly make arrangements for donations(gift cards) to Veterans at Hospice care units.
Can you please handle this on behalf of

This is a one time project and I'll be liable for reimbursement. I look forward to reading from you at your earliest convenience.
Thanks and stay safe!

Warm regards,
Kevin
President

Abb. 20: E-Mail, in der das Opfer gebeten wird, Gutscheinkarten für eine angebliche Spende an ein Hospiz zu kaufen



Greetings,

I hope you and your family are in good health! I need a quick and urgent favor from you. I need to get a Target gift card for my Niece, it's her birthday but i can't do this now because i am currently out of town and isolated till 27th of this month as advised by my doc. Pls can you get the card from any nearby Grocery store around you or CVS, I'll pay back as soon as i get back and okay. Please let me know if you can handle this.

Thanks and stay safe,
I owe you a lot

Best Regards,

Ruben

Subject: RE: Greetings!

Hi Ruben, how are you doing?

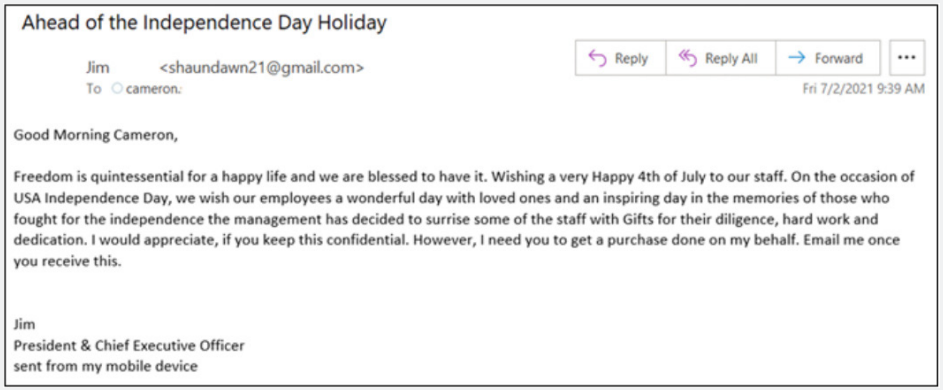
Richard :

Abb. 21: E-Mail, die das Opfer bittet, Gutscheinkarten zu kaufen, da sich der Absender isolieren müsse

Abb. 22 zeigt ebenso, dass einige Angreifer beim Betrug mit Gutscheinkarten die Empfänglichkeit ihrer potenziellen Opfer mit einer kurzen Köder- und Aufgaben-E-Mail testen. (Mehr Informationen zu diesem Köder finden Sie im vorherigen Abschnitt „**Methode 4: Köder und Aufgaben**“.) In diesem Fall wollte der Bedrohungsakteur zunächst herausfinden, ob das anvisierte Opfer Zeit hat. Die Bitte mit den Gutscheinkarten kam erst, nachdem die Person geantwortet hatte.

Betrug mit Gutscheinkarten in Unternehmen

In unserem letzten Beispiel (Abb. 22) erzählt der Bedrohungsakteur, er wolle Geschenkkarten besorgen, um sich bei seinen Mitarbeitern zu bedanken – eine weit verbreitete Praxis in Unternehmen. In diesem Fall steht die Bitte im Zusammenhang mit dem US-amerikanischen Unabhängigkeitstag.



Ahead of the Independence Day Holiday

Jim <shaundawn21@gmail.com>
To cameron.

Reply | Reply All | Forward | ...
Fri 7/2/2021 9:39 AM

Good Morning Cameron,

Freedom is quintessential for a happy life and we are blessed to have it. Wishing a very Happy 4th of July to our staff. On the occasion of USA Independence Day, we wish our employees a wonderful day with loved ones and an inspiring day in the memories of those who fought for the independence the management has decided to surrise some of the staff with Gifts for their diligence, hard work and dedication. I would appreciate, if you keep this confidential. However, I need you to get a purchase done on my behalf. Email me once you receive this.

Jim
President & Chief Executive Officer
sent from my mobile device

Abb. 22: Eine E-Mail, in der sich der Absender als Geschäftsführer des Unternehmens ausgibt und das Opfer bittet, Gutscheinkarten für die Mitarbeiter zu kaufen; der Angreifer bittet um Diskretion, angeblich um die Überraschung nicht zu verderben

Geschenke mit böser Überraschung

Der Betrug mit Gutscheinkarten ist eine weitverbreitete Form von E-Mail-Betrug. Mit einem Durchschnitt von 840 US-Dollar pro Zwischenfall haben die Opfer durch diese Methode seit 2018 beinahe 245 Millionen US-Dollar verloren. Wir blockieren täglich 7.000 bis 10.000 dieser E-Mails.

Methode 6: Provisionsbetrug

Provisionsbetrug ist eine alte Methode und wird in einigen Fällen – irreführenderweise – als „419“, „Nigerian 419“ oder „Nigerianischer Prinz“ bezeichnet. Der Bedrohungsakteur bittet das potenzielle Opfer um einen kleinen Geldbetrag als Vorschuss für einen späteren großen Gewinn. Die angefragte Geldsumme wird in der Regel als Startkapital dargestellt, das dazu dient, die versprochene Belohnung freizuschalten oder zu überweisen.

Bedrohungsakteure verwenden zahlreiche Variationen von Provisionsbetrug. Häufig begründen sie mit ausgeklügelten Geschichten, warum eine große Geldsumme bereitsteht und sie einen kleinen Vorschuss benötigen, um diese zum Empfänger zu bringen. Die Opfer werden dabei mit Betreffzeilen geködert, die unter anderem folgende Themen enthalten:

- Erbschaft
- Lotteriegewinne
- Preise
- Staatliche Leistungen
- Internationale Geschäfte

Nachdem das Opfer den Vorschuss geleistet hat, verlangt der Betrüger entweder (angeblich aufgrund unvorhergesehener Komplikationen) noch mehr Geld vom Opfer – oder er bricht den Kontakt einfach ab und verschwindet.

Funktionsweise

Auf der *Täuschungsebene* in unserer Taxonomie werden beim Provisionsbetrug Nachahmungstechniken eingesetzt. In der Regel geben sich die Bedrohungsakteure als Regierungsbeamte, Anwälte oder Personen in einer Notsituation aus. Raffinierte Betrüger fälschen in ihren E-Mails meist den Anzeigenamen (siehe Abb. 23) und nutzen in einigen Fällen Nachahmungstaktiken wie Domänen-Spoofing oder Doppelgänger-Domänen.

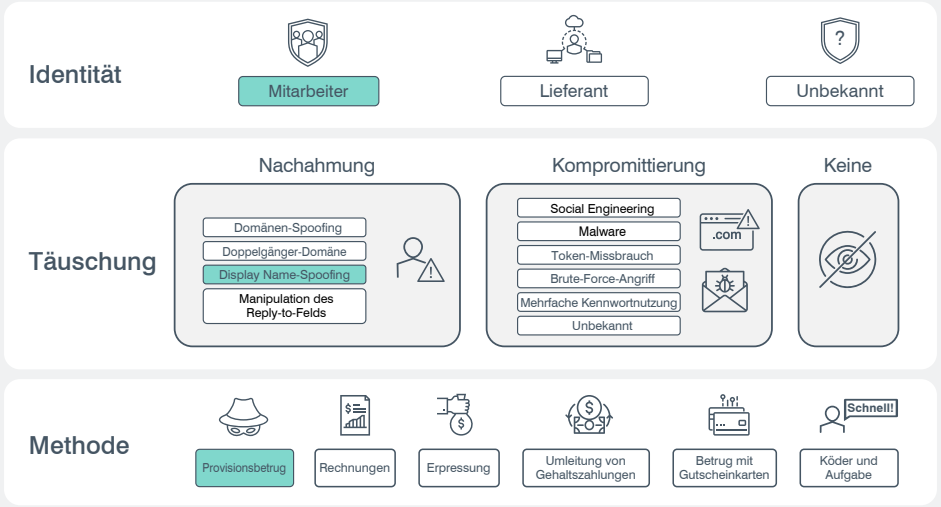


Abb. 23: Taxonomie für Provisionsbetrug

Reale Beispiele

Angreifer nutzen in ihren Provisionsbetrug-E-Mails verschiedene Köder, um ihre Opfer anzulocken und deren Vertrauen zu gewinnen bzw. sie zum Handeln zu bewegen. Wie die folgenden Beispiele zeigen, machen sich die Bedrohungsakteure dabei alles zunutze, was funktioniert, wie zum Beispiel aktuelle Ereignisse wie die Pandemie, Geschäftsabschlüsse und Auszahlungen an Begünstigte.

In Abb. 24 (siehe nächste Seite) versucht der Absender, aus der Pandemie Kapital zu schlagen. In Abb. 25 (ebenfalls auf der nächsten Seite) drängt der Absender den Empfänger dazu, schnell zu handeln und gibt ihm damit weniger Zeit zu beurteilen, ob die E-Mail betrügerisch ist.

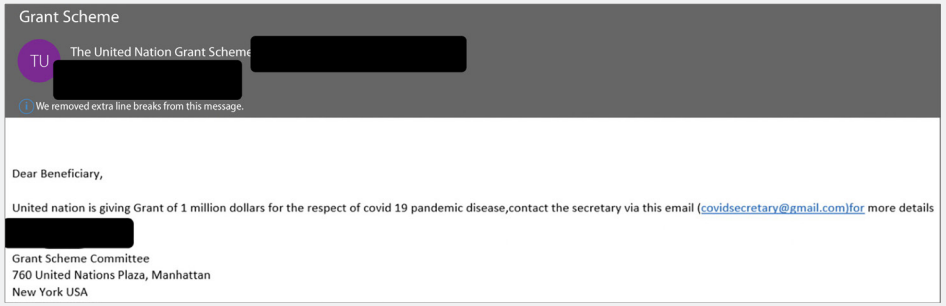


Abb. 24: Eine Provisionsbetrug-E-Mail, die einen Zuschuss von einer Million US-Dollar verspricht

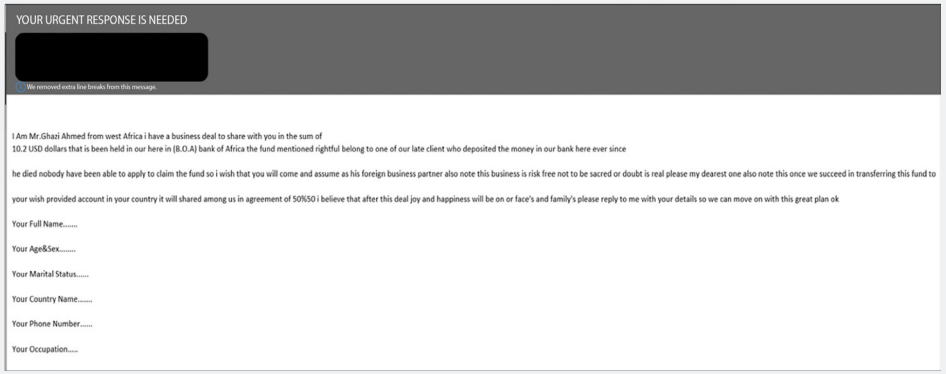


Abb. 25: Diese E-Mail bietet an, eine nicht geltend gemachte Erbschaft zu teilen

In Abb. 26 versucht der Bedrohungsakteur, sein Opfer mit einer großen Versicherungssumme anzulocken – eine weitverbreitete Strategie beim Provisionsbetrug, die die menschliche Gier ausnutzt. Der Angreifer versucht hier nicht nur, den Empfänger um eine „Sicherheitsgebühr" von 95 US-Dollar zu betrügen, sondern möchte auch an seine personenbezogenen Daten.

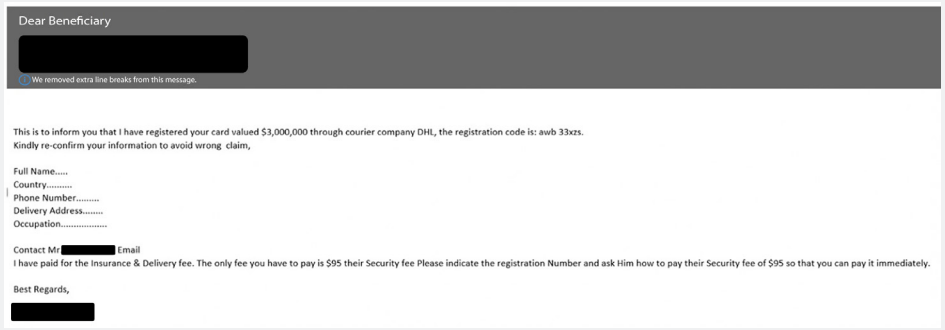


Abb. 26: Eine E-Mail, in der die Zahlung von 3 Millionen US-Dollar versprochen wird, wenn der Empfänger eine „Sicherheitsgebühr" von 95 US-Dollar zahlt

Die meisten Provisionsbetrug-E-Mails sind einfach aufgebaut und leicht zu erkennen; nur wenige sind gut durchdacht oder komplexer als die hier gezeigten Beispiele.

Provisionsbetrug-E-Mails machen einen kleinen Teil der von uns beobachteten betrügerischen E-Mails aus. Dennoch fallen immer wieder Empfänger darauf herein, wobei der durchschnittliche Schaden etwa 5.100 US-Dollar pro Zwischenfall beträgt. Obwohl die Erfolgsrate hier wahrscheinlich sehr viel geringer ist als für andere Arten von Betrug (z. B. Betrug mit Gutscheinkarten), kann Provisionsbetrug für Bedrohungsakteure durchaus lukrativ sein.

Schlussfolgerung und Empfehlungen

Die in unserer Taxonomie aufgeführten Arten von E-Mail-Betrug sind heimtückisch und werden erbarmungslos genutzt. Sie lassen sich mit traditionellen, auf den Perimeter fokussierten Sicherheitstools und Gateways nur schwer bewältigen. Ebenso wie die meisten moderne Angriffe zielen sie auf Menschen ab, nicht auf die Technologie. Deshalb ist für deren Abwehr ein personenzentrierter Ansatz erforderlich.

Finanzkontrollen wie beispielsweise die Auflage, dass Änderungen von Girokonten oder Gehaltsabrechnungen von zwei oder mehr Personen genehmigt werden müssen, sind ein guter Anfang. Zur Abwehr von BEC-Betrug ist jedoch auch ein hochentwickelter E-Mail-Schutz nötig. Um sich einen besseren Überblick über die menschliche Angriffsfläche zu verschaffen und BEC-Betrugsversuche in allen Formen abwehren zu können, benötigen Sie eine umfassende Plattform mit integrierten Kontrollen für alle E-Mail- und Cloud-Konten sowie Anwender und Lieferanten.

Wählen Sie eine Lösung, die folgende Funktionen umfasst:

- Überblick über die menschliche Angriffsfläche. Sie sollten wissen, welche Mitarbeiter am häufigsten angegriffen werden, welche Bedrohungsakteure Ihr Unternehmen ins Visier nehmen und welche Lieferanten eventuell kompromittiert sind oder nachgeahmt werden.
- Hochentwickelte Erkennungsfunktionen zur Abwehr von BEC, E-Mail-Betrug und anderen Bedrohungen, die keine Malware verwenden. Bei E-Mail-Betrugsversuchen werden Social Engineering und andere stetig weiterentwickelte Taktiken eingesetzt, die die menschliche Natur ausnutzen. Das bedeutet, dass statische Regelsätze trotz regelmäßiger Updates nicht ausreichen, um die Taktiken zu identifizieren und zu stoppen. Die besten Lösungen nutzen zudem Machine Learning, das Faktoren wie E-Mail-Header, die Beziehung zwischen Absender und Empfänger sowie den Ruf des Absenders analysiert. Doch Machine Learning ist nur so gut wie die verarbeiteten Daten und die verwendeten Trainingsmodelle. Entscheiden Sie sich daher für einen Anbieter, der mit umfangreichen und vielfältigen Datensätzen ausgestattet ist sowie über menschliches Know-how verfügt.
- Die Möglichkeit, Angreifer daran zu hindern, Anwenderkonten zu kapern und diese für E-Mail-Betrugsversuche zu missbrauchen. Da immer mehr Unternehmen in die Cloud umziehen, müssen zum Schutz vor E-Mail-Betrug auch Cloud-Konten geschützt werden. Wählen Sie Tools, die verhindern, dass die Konten Ihrer Anwender gekapert und für E-Mail-Betrugsversuche genutzt werden.
- Schulungen zur Steigerung des Sicherheitsbewusstseins zur Ergänzung technischer Kontrollen. Mit den richtigen Schulungen – insbesondere, wenn diese auf realen Bedrohungen basieren – können Sie Ihre Endnutzer zur letzten Verteidigungslinie machen. Erleichtern Sie Ihren Anwendern die Meldung verdächtiger Nachrichten und machen Sie es Ihrem Sicherheitsteam einfacher, die Meldungen automatisiert zu analysieren und zu beheben.

WEITERE INFORMATIONEN

Weitere Informationen dazu, wie Proofpoint Ihnen helfen kann, Ihr Unternehmen vor BEC und anderen Arten von E-Mail-Betrug zu schützen, finden Sie unter **www.proofpoint.com/us/solutions/bec-and-eac-protection**.

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 mehr als die Hälfte der Fortune-1000-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.

0501-010-01-01 04/22