proofpoint.

E-BOOK

Das Handbuch zu Business Email Compromise (BEC)

Ein 6-Stufen-Plan zur Abwehr von Zahlungsumleitungen sowie Betrugsversuchen mit Lieferantenrechnungen und Gutscheinkarten

Die derzeit kostspieligste Cyberbedrohung – ohne eine einfache Lösung

Im Internet Crime Report 2020 des vom FBI verwalteten Internet Crime Complaint Centers (IC3) heißt es, dass durch die Internet-Verbrechensserie im letzten Jahr durch E-Mail-Betrug Verluste in Höhe von etwa 1,8 Milliarden US-Dollar entstanden sind.

In der Finanzabteilung eines Automobilzulieferers, der zu einem der weltweit größten Automobilhersteller gehört, trifft eine E-Mail ein, in der jemand um die Überweisung von 37 Millionen US-Dollar bittet. Obwohl dies eine vergleichsweise hohe Summe ist, stellt die Überweisung für das globale Unternehmen einen üblichen Geschäftsvorgang dar. Doch dieses Mal kam die Anfrage weder von einem Anbieter oder Geschäftspartner noch von einer Führungskraft. Sie stammte von einem Angreifer, der sich als jemand anderer ausgab – und war eines der größten bisher dokumentierten Beispiele für Business Email Compromise (BEC), auch als Chefmasche bekannt.[1]

In Arizona schickt ein Geschäftsmann eine E-Mail an seine Kollegin, um sie darüber zu informieren, dass das Unternehmen eine Geschäftsbeziehung mit einem neuen Anbieter namens RS Enterprise eingehen wird. Der Geschäftsmann ist auf Reisen und kann daher die Zahlung der vereinbarten 157.000 US-Dollar an den Anbieter nicht selbst abwickeln. Um es ihr leicht zu machen, schickt er daher alle Informationen für die Überweisung an seine Kollegin. Mehr als 350 Menschen in Arizona erhielten E-Mails mit ähnlichen Anweisungen – Nachrichten, die von einem Anbieter oder anderen vertrauten Geschäftskollegen zu stammen schienen. Die wirklichen Absender waren Cyberkriminelle, die laut dem FBI mehr als 30 Millionen US-Dollar erbeuteten.[2]

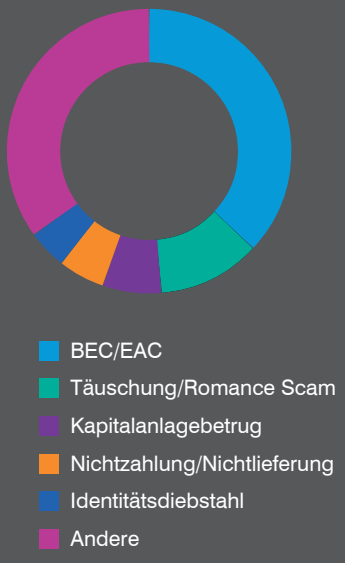
Ein Mann verschickt eine wehleidige E-Mail, in der er dem Empfänger schreibt, dass er sich in Quarantäne begeben hat, weil er an COVID-19 erkrankt ist. Er ist verzweifelt, weil er in der Eile vergessen hat, sein Mobiltelefon und andere wichtige Dinge mit nach Hause zu nehmen. Daher bittet er den Empfänger, iTunes- oder Walmart-Gutscheinkarten im Wert von 250 US-Dollar zu kaufen. Er bittet

1 Nicole Lindsey (*CPO Magazine*): „Toyota Subsidiary Loses $37 Million Due to BEC“ (Toyota-Tochterunternehmen verliert 37 Mio. USD durch BEC), September 2019.

2 Susan Campbell (*azfamily.com*): „Arizona workers lost $30 million to work email scams, FBI says“ (Laut FBI verloren Arbeiter in Arizona 30 Mio. USD durch E-Mail-Betrug), April 2021.

Gemeldete Verluste durch BEC

Anteil an der Gesamtzahl der gemeldeten Verluste durch Cyberkriminalität



Quelle: FBI

außerdem um Fotos der Karten und Codes, sodass er diese nutzen kann, um in der Quarantäne das Notwendigste einzukaufen.[3]

Ein teurer Trend

Diese Geschichten sind Beispiele für jüngst erfolgte BEC-Betrugsversuche. Es sind nur drei von vielen Tausend, die Anfang 2020 durchgeführt wurden und Anwender und Unternehmen in den USA ins Visier nahmen. Tatsächlich war das Jahr 2020 für Cyberkriminelle ein besonders lukratives Jahr, denn sie konnten das durch die Pandemie ausgelöste Chaos und die verstärkte Abhängigkeit der Menschen von Technik in vollem Umfang ausnutzen.

Unter diesen böswilligen Aktivitäten stechen besonders BEC-Angriffe hervor, da sie die größten Schäden bei den Opfern verursacht haben. Im Internet Crime Report 2020 des vom FBI verwalteten Internet Crime Complaint Centers (IC3) heißt es, dass durch die Internet-Verbrechensserie im letzten Jahr durch E-Mail-Betrug Verluste in Höhe von etwa 1,8 Milliarden US-Dollar entstanden sind.[4] Dem Bericht zufolge entspricht dies fast der Hälfte (44 %) der gesamten Unternehmens- und Verbraucherverluste durch Cyberkriminalität, die im letzten Jahr gemeldet wurden.

Der Betrag von 1,8 Milliarden US-Dollar ist zudem 64 Mal größer als die finanziellen Verluste durch die zahlreichen Ransomware-Kampagnen, die Cyberkriminelle im Jahr 2020 führten.[5] Die Höhe der finanziellen Verluste ist noch eindrucksvoller, wenn man bedenkt, dass nur 19.369 der registrierten 791.790 Beschwerden, die das IC3 von Cyberkriminalitätsopfern im Jahr 2020 erhalten hat, mit E-Mail-Betrugsversuchen verbunden waren. Das entspricht gerade einmal 2,4 % aller Beschwerden.

Die gute Nachricht ist, dass diese Bedrohungen mit den richtigen Erkenntnissen, Ansätzen und Maßnahmen abgewehrt werden können. In diesem E-Book erfahren Sie, wie BEC-Angriffe funktionieren, in welchen Formen sie auftreten und wie Sie vermeiden können, in der nächsten Schlagzeile zu landen.

3 "Lance Whitney (*TechRepublic*): „Scammers exploit coronavirus for Business Email Compromise campaigns" (Betrüger nutzen Coronavirus für BEC-Kampagnen), April 2020.

4 FBI: „2020 Internet Crime Report" (Bericht zu Internetkriminalität 2020), März 2021.

5 Sara Pan (*Proofpoint*): „FBI Internet Crime Report Shows that Email Fraud Represents the Largest Financial Losses in 2020" (FBI-Bericht zu Internet-kriminalität: E-Mail-Betrug verursachte 2020 die größten finanziellen Verluste), März 2021.

Inhaltsverzeichnis

Warum sind BEC-Betrugsversuche so erfolgreich?

Kurz gesagt: Diese Angriffe sind schwer zu erkennen und haben eine hohe Überzeugungskraft.

In BEC-Angriffen werden verstärkt Social-Engineering-Techniken eingesetzt, um Opfer zu täuschen und deren Vertrauen zu missbrauchen. Das bedeutet, dass die Nachrichten in der Regel keine Malware oder schädlichen URLs enthalten, die von üblichen Cybersicherheits-Schutzmaßnahmen wie zum Beispiel älteren Tools, Einzelprodukten und nativen Cloud-Plattform-Schutzmaßnahmen blockiert oder abgefangen und analysiert werden können.

BEC-Angriffe sind zudem meist sehr zielgerichtet – die kriminellen Akteure verschicken eventuell nur einige wenige E-Mails an ausgewählte Anwender. Durch die geringe Menge an Nachrichten bleiben die Angreifer unter dem Radar vieler Sicherheitstools.

Täuschungsstrategien: Nachahmungstechniken

Cyberkriminelle nutzen verschiedene Techniken, um BEC-Angriffe vorzubereiten und durchzuführen. Beispielsweise spielen Taktiken zur Identitätstäuschung bei BEC eine zentrale Rolle, da die Angreifer ihre Empfänger von der Echtheit der Anweisungen überzeugen müssen.

Um ihre Ziele zu identifizieren und herauszufinden, mit wem diese zusammenarbeiten und wem sie vertrauen, forschen Betrüger Unternehmen oft gründlich aus – ein Prozess, bei dem sie in der Regel über öffentlich zugängliche Ressourcen wie LinkedIn ermitteln, welche Mitarbeiter in einem Unternehmen Zugriff auf wichtige Daten, Systeme und Ressourcen haben. Als nächstes nutzen sie wahrscheinlich eine oder mehrere der folgenden Strategien zur Einleitung des BEC-Angriffs. (Tatsächlich setzen die meisten BEC-Angriffe mehrere Taktiken zur Identitätstäuschung ein.)

Display Name-Spoofing

Angreifer verwenden im Absenderfeld einer E-Mail die Namen von Führungskräften, Anwälten, Geschäftspartnern, Lieferanten des Unternehmens oder anderen Personen bzw. Einrichtungen, denen Anwender typischerweise vertrauen. Dieses Feld der E-Mail-Kennung können die Betrüger in der Regel am leichtesten manipulieren. Die meisten BEC-Angreifer nutzen Display Name-Spoofing parallel zu anderen Spoofing-Methoden wie Domänen-Spoofing.

Domänen-Spoofing

Bei diesem Phishing-Betrug imitieren die Angreifer die Marke eines Unternehmens, um mit einem BEC-Angriff an Geld oder Daten zu gelangen. Die beim Versand der betrügerischen E-Mails genutzte Domäne entspricht dabei genau der vertrauenswürdigen Domäne (bzw. Domänen) des Unternehmens.
Die Cyberkriminellen errichten teilweise auch gefälschte Webseiten auf einer nachgeahmten Internetadresse und imitieren die Marke eines Unternehmens, um die Anwender davon zu überzeugen, dass sie mit einer legitimen Organisation kommunizieren.

Doppelgänger-Domänen

Eine weitere Nachahmungstechnik ist die Registrierung einer Domäne, die der vertrauenswürdigen Domäne des angegriffenen Unternehmens täuschend ähnlich sieht.
Ein Beispiel: Ein krimineller Akteur will Anwender täuschen, die bei „tollesunternehmen.com“ arbeiten oder geschäftlich damit zu tun haben, und registriert dafür Domänen wie „tolles-unternehmen.com“ oder „tolllesunternehmen.com“ und verschickt dann betrügerische E-Mails mit diesen Doppelgänger-Domänen. Die gefälschte Domäne ist der echten Domäne so täuschend ähnlich, dass nur wenige Anwender den Unterschied bemerken – bis es zu spät ist.

Kontenkompromittierung und -übernahme

Das kann als die ultimative Nachahmungstechnik bezeichnet werden. Wenn Angreifer das Konto eines vertrauenswürdigen Absenders kompromittieren, haben sie Zugriff auf den E-Mail-Verlauf, die Kontakte und den Kalender dieser Person. Anders ausgedrückt: Sie haben alle nötigen Informationen und Zugriffsmöglichkeiten, um die Person, die das Konto besitzt, zu imitieren. In gewisser Hinsicht tun sie nicht nur so, als wären sie der Anwender – praktisch gesehen *sind* sie der Anwender.

Invasion der Körperfresser: So werden Konten kompromittiert

Anmeldedaten-Phishing

Mit dieser Kompromittierungsstrategie, die seit Jahrzehnten existiert, sollen Anwender dazu gebracht werden, vertrauliche Kontoanmeldedaten preiszugeben. Angegriffene Anwender erhalten beispielsweise eine E-Mail, die von der IT-Abteilung des Unternehmens zu stammen scheint – eventuell sogar mit dem Anzeigenamen „Helpdesk“ im Absenderfeld – und sie dazu auffordert, auf einen Link zu klicken, um ihre Anmeldedaten für eine Geschäftsanwendung zu bestätigen.

Brute-Force-Angriffe gegen Kennwörter

Dies ist eine weitere Methode, um Anwenderkonten zu übernehmen, die schon eine Weile existieren. Im Prinzip versuchen die kriminellen Akteure dabei, die Anmeldedaten eines Anwenders zu erraten, bis sie sich mit Gewalt Zugang zum Konto verschafft haben – ein aggressives Vorgehen, das jedoch oft schnell und effektiv zum Ziel führt, da viele Mitarbeiter leicht zu erratende Benutzernamen und Kennwörter nutzen. Für viele Angreifer bleibt es daher weiterhin eine der wichtigsten Methoden.

OAuth-Token von Cloud-Anwendungen

Eine Open Authentication-App (OAuth) integriert sich mit einem Cloud-Dienst und kann von einem anderen Anbieter als dem Cloud-Dienst-Anbieter bereitgestellt werden. Diese Apps fügen Cloud-Diensten wie Microsoft 365 und Google Workspace geschäftliche Funktionen zu und verbessern die Benutzeroberfläche. Die meisten OAuth-Apps fordern Zugriffsberechtigungen an, verwalten Anwenderdaten und melden sich im Namen der Anwender bei anderen Cloud-Anwendungen an.

Angesichts ihrer gegebenenfalls weitreichenden Berechtigungen werden OAuth-Apps zunehmend zu Angriffsflächen und -vektoren. Kriminelle Akteure bringen Anwender über Drittanbieter-Add-ons und Social-Engineering-Taktiken dazu, ihnen mittels Token-basierter Authentifizierung Zugriff auf die Cloud-Anwendungen des Unternehmens zu erteilen. Sobald ein OAuth-Token autorisiert wurde, bleibt der Zugang so lange bestehen, bis er manuell gesperrt wird.

Malware

Einige Angreifer nutzen Malware, um an die Informationen zu gelangen, die sie benötigen, um auf Konten von Anwendern zuzugreifen und diese zu übernehmen. Zu den häufig eingesetzten Malware-Typen bei Kontoübernahmen zählen zum Beispiel:

- Keylogger, die die Tastatureingaben von Anwendern erfassen, einschließlich der Anmeldedaten
- Informationsdiebe (Stealer), die, wie ihr Name bereits sagt, Daten wie Kontaktinformationen und Browserkennwörter stehlen.

Die mit Umleitungen von Gehaltszahlungen verbundenen finanziellen Verluste sind zwischen dem 1. Januar 2018 und dem 30. Juni 2019 sprunghaft um 815 % angestiegen.[6]

– FBI

Drei BEC-Angriffstypen

Sobald die Angreifer über alle nötigen Informationen für einen BEC-Angriff verfügen, starten sie in der Regel einen der drei folgenden Angriffstypen:

Umleitung von Gehaltszahlungen oder Überweisungen

Bei dieser Angriffsmethode fordern Cyberkriminelle buchstäblich dazu auf, ihnen das Geld zu schicken.

Bei Betrugsversuchen mit der **Umleitung von Gehaltszahlungen** beabsichtigen die Angreifer, legitime Gehaltszahlungen von den Bankkonten der Mitarbeiter auf ihre Konten umzuleiten. Sie tun dies entweder, indem sie sich als Mitarbeiter ausgeben oder Nachrichten direkt über deren kompromittierte Konten verschicken.

Bei Betrugsversuchen mit der **Umleitung von Überweisungen** gibt sich der Cyberkriminelle möglicherweise als externer Absender (z. B. als Lieferant) aus und fordert die Unternehmensvertreter auf, einen Rechnungsbetrag auf ein anderes als das sonst übliche Bankkonto (also das Konto des Angreifers) zu überweisen.

6 FBI: „Business Email Compromise: The $26 Billion Scam“ (BEC: Der 26-Milliarden-Dollar-Betrug), September 2019.

Angriffe mit Umleitungen von Gehaltszahlungen und Überweisungen haben zwar ein recht simples Ziel, doch verlangen sie von den kriminellen Akteuren einiges an Geschick. Zunächst einmal muss dafür gleich zu Beginn eine Menge an Informationen zusammengetragen werden. Für den Angriff muss ein Mitarbeiter in der Personal- oder Gehaltsabteilung korrekt identifiziert werden – Informationen, die aus öffentlich zugänglichen Ressourcen wie LinkedIn, der Unternehmenswebseite und kommerziellen Datenbanken eingeholt werden können.

Hinzu kommt noch eine weitere Schwierigkeit. Bei Angriffen mit Umleitungen von Gehaltszahlungen und Überweisungen müssen die Angreifer glaubwürdig demonstrieren, dass sie mit den Vorgängen bei Gehalts- oder Rechnungszahlungen vertraut sind, damit ihr Anliegen legitim erscheint und das Opfer keinen Verdacht schöpft.

So funktionieren Angriffe mit Umleitungen von Gehaltszahlungen und Überweisungen

1. Angreifer kontaktiert Personal- oder Gehaltsabteilung

Ein Angreifer, der einen Mitarbeiter nachahmt, kontaktiert die Personal- oder Gehaltsabteilung eines Unternehmens per E-Mail und bittet diese, seine Bankverbindungsdaten zu aktualisieren. (Die neue Bankleitzahl und Kontonummer gehören dem Angreifer, nicht dem nachgeahmten Mitarbeiter.)

2. Personal- oder Gehaltsabteilung ändert Konto

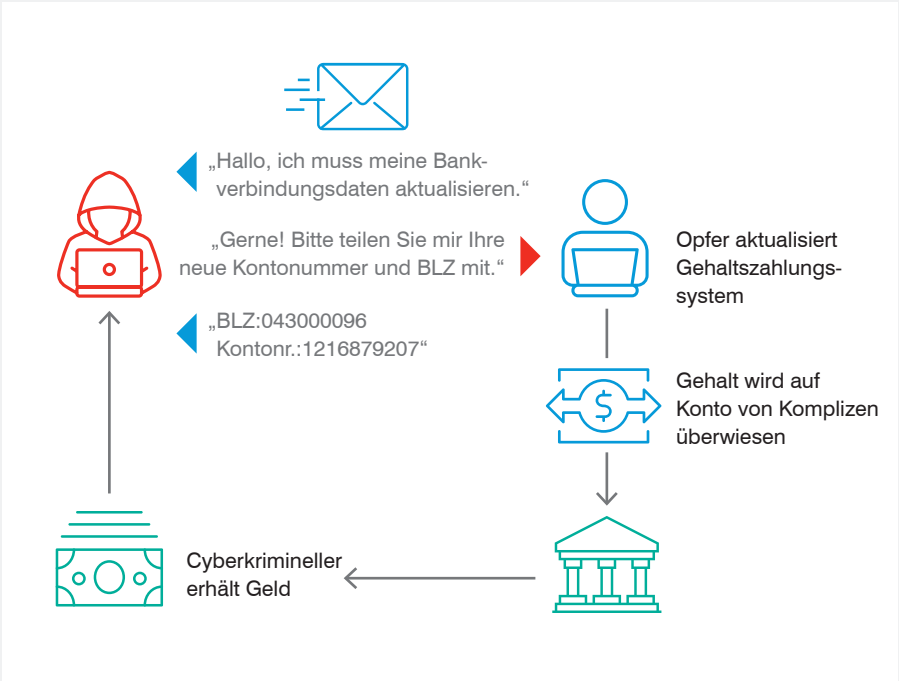
Die Personal- oder Gehaltsabteilung geht davon aus, dass die Anfrage legitim ist und ändert die Kontodaten.

3. Lohn wird gezahlt

Der nächste Lohn des Mitarbeiters wird auf das Konto des Angreifers überwiesen.

4. Angreifer hebt Geld ab

Der Angreifer hebt das Geld ab und schließt das Konto, bevor der Mitarbeiter den fehlenden Lohn bemerkt.



Gutscheinkartenbetrug

Nehmen wir an, Sie haben von Ihrer Chefin eine E-Mail mit der Bitte erhalten, einige Gutscheinkarten von einem bekannten Einzelhändler zu kaufen. Sie sagt, dass sie die Gutscheine an Teammitglieder verschenken will, um sie für die harte Arbeit an einem kürzlich abgeschlossenen Projekt zu belohnen. Und da Sie alle momentan von zu Hause aus arbeiten, bittet sie Sie darum, auch gleich die Gutscheincodes mitzuschicken, um den Mitarbeitern die Nutzung zu erleichtern.

Würden Sie diese Bitte hinterfragen oder ohne Bedenken erfüllen? Falls Sie letzteres tun würden, wären Sie damit definitiv nicht allein und leider auf einen Betrug hereingefallen.

Laut der US-Bundeshandelskommission (FTC) haben Verbraucher seit 2018 Ausgaben in Höhe von beinahe 245 Millionen US-Dollar für Gutscheinkarten gemeldet, mit denen sie Cyberkriminelle für verschiedenste Betrugsversuche bezahlt haben.[7] Das Better Business Bureau (BBB) berichtet zudem, dass die Betrüger in mehr als einem Drittel (35 %) der Betrugsversuche mit gefälschter Identität (einschließlich BEC-Angriffen) nach Gutscheinkarten fragten.[8]

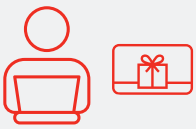
Doch warum bitten die Angreifer die Opfer um Gutscheinkarten? Weil sie damit schnell und einfach Beute machen können. Es sind keine komplizierten Anweisungen für Überweisungen nötig, die bei den Opfern Verdacht erregen oder bei üblichen internen Kontrollen in Unternehmen geprüft werden könnten.

Zudem sind Gutscheinkarten ideal zur Geldwäsche geeignet, da Betrüger damit Wertsachen kaufen und wieder verkaufen oder die Codes online veräußern können. Und sind die Gutscheinkarten einmal eingelöst, kann das Geld nicht zurückgeholt werden.

So funktionieren Angriffe mit Gutscheinkarten

1. Cyberkrimineller imitiert Mitarbeiter/ Bekannte/Geschäftsführer

Ein Angreifer ahmt eine vertraute Person im Unternehmen nach (z. B. den Geschäftsführer) und verschickt eine E-Mail an ein Opfer (z. B. einen Assistenten der Geschäftsleitung) und bittet darum, Gutscheinkarten zu kaufen. Der Angreifer deutet eventuell an, dass die Gutscheinkarten als Geschenke für Mitarbeiter, Kunden oder Anbieter dienen sollen.
Die Opfer werden zudem dazu angewiesen, die Kartennummern und alle zur Nutzung der Karten nötigen Einlösecodes zu schicken.



2. Opfer kauft Gutscheinkarten und verschickt relevante Karteninformationen

Das Opfer befolgt die Aufforderung.

3. Cyberkrimineller erhält Geld

Der Angreifer lässt sich die Kartenbeträge auszahlen oder löst die Karten für Waren ein, die er dann wieder verkauft. Oder die Codes werden direkt auf dem Schwarzmarkt verkauft.

7 FTC: „FTC Data Show Gift Cards Remain Scammers' Favorite Payment Method" (Laut FTC-Daten sind Gutscheinkarten weiterhin beliebteste Zahlungsmethode für Betrüger), Dezember 2010.

8 Better Business Bureau: „BBB Investigation on gift card payment scams: Why do scammers love gift cards?" (Untersuchung von BBB zu Gutscheinkarten-Betrug: Warum lieben Betrüger sie so sehr?), März 2021.

Anfang 2021 gerieten während eines siebentägigen Untersuchungszeitraums 98 % der Unternehmen ins Visier von Angreifern, die die Identität von Lieferanten vortäuschten oder diese kompromittieren wollten.

Betrug mit Lieferantenrechnungen

Wie der Name andeutet, geben sich die kriminellen Akteure bei Betrugsversuchen mit Lieferantenrechnungen als Anbieter, Lieferanten oder andere Geschäftspartner aus, um ein Unternehmen zur Zahlung einer gefälschten Rechnung zu bewegen. In der Regel wird dabei die E-Mail-Adresse des legitimen Lieferanten nachgeahmt oder das E-Mail-Konto eines Lieferanten-Mitarbeiters übernommen.

Die Betrugsmasche mit Lieferantenrechnungen wird in letzter Zeit immer häufiger von Angreifern genutzt, die die Lieferkette und das Partner-Ökosystem ausnutzen, um darüber indirekte Angriffe auf Unternehmen zu führen. Sie sollten sich Folgendes durch den Kopf gehen lassen:

- Anfang 2021 gerieten während eines siebentägigen Untersuchungszeitraums 98 % der Unternehmen ins Visier von Angreifern, die die Identität von Lieferanten vortäuschten oder diese kompromittieren wollten.[9]
- Ein Viertel aller Phishing-E-Mails imitiert Lieferanten oder stammt von kompromittierten Lieferanten.[10]

Angreifer imitieren Händler für Bürobedarf, Webdesign-Agenturen, Marketingfirmen, Reinigungsdienste, Caterer, Kammerjäger usw. Oft haben sie mit ihrer Nachahmungsmasche längere Zeit Erfolg, da viele Unternehmen, besonders die größeren, keinen Überblick über ihre Lieferkette haben. Sie wissen nicht, wie viele Anbieter sie haben und welche davon ein Risiko darstellen könnten.

Das Potenzial für reiche Beute

Der Betrug mit Lieferantenrechnungen verursacht aufgrund der bei B2B-Zahlungen teilweise sehr hohen Beträge die größten finanziellen Verluste unter den BEC-Angriffen.[11] Diese Betrugsversuche haben eine hohe Trefferquote, weil dabei routinemäßige Geschäftsprozesse ausgenutzt und oft legitime geschäftliche E-Mail-Adressen der Anbieter oder Geschäftspartner verwendet werden, denen die Opfer vertrauen. Kompromittierte, aber ansonsten legitime Konten werden von vielen Sicherheitskontrollen nicht erkannt.

Einige besonders dreiste und raffinierte Angreifer geben sich als Anbieter aus, die gar nicht existieren – und haben trotzdem Erfolg. Zum Beispiel prellten von 2013 bis 2015 ein Betrüger und seine Komplizen Google und Facebook mit einem komplexen Lieferantenbetrug um mehr als 100 Millionen US-Dollar. Sie gründeten dafür eine Scheinfirma in Lettland, die den Namen eines tatsächlich existierenden Unternehmens in Taiwan trug, mit dem die Tech-Unternehmen geschäftlich zu tun hatten. Google und Facebook hatten letztendlich Glück: Die Kriminellen wurden gefasst und die Unternehmen konnten Berichten zufolge ihr ganzes oder einen Großteil ihres Geldes zurückholen.[12]

9 Sara Pan (*Proofpoint*): „98 % of Organizations Received Email Threats from Suppliers: What You Should Know“ (98 % aller Unternehmen haben schon einmal E-Mail-Bedrohungen von Lieferanten erhalten: Das sollten Sie wissen), Februar 2021.

10 Ebd.

11 Sara Pan (*Proofpoint*): „FBI Internet Crime Report Shows that Email Fraud Represents the Largest Financial Losses in 2020“ (FBI-Bericht zu Internetkriminalität: E-Mail-Betrug verursachte 2020 die größten finanziellen Verluste), März 2021.

12 Vanessa Roma (*NPR*): „Man Pleads Guilty to Phishing Scheme That Fleeced Facebook, Google of $100 Million“ (Mann bekennt sich des Phishing-Angriffs schuldig, der Facebook, Google um 100 Mio. USD schröpfte), März 2019.

Von: Chris@Lieferant (kompromittiertes Lieferantenkonto)
An: Jason (Opfer)

External Message
Thanks Connie~

Dear Jason,

Hope you are well.
The following invoices are due or will be due in Apr. And now we haven't received the payment from you side.
Could you please help to arrange the payment in Apr? Thank you.

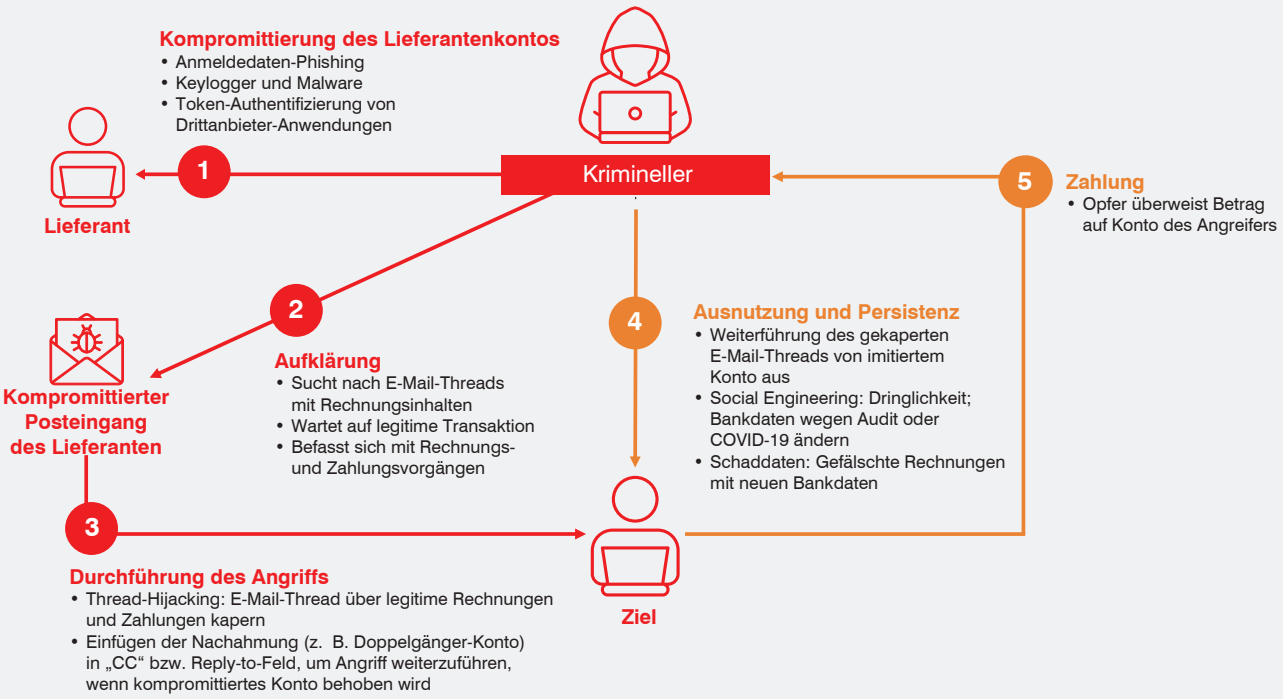
Total amount: USD 2,791,867.92

Class	Number	Amount(USD)	Days Late	Transaction Date	Due Date
Invoice		179,976.49	43	12-26-2019	03-10-2020
Invoice		15,328.07	34	01-04-2020	03-19-2020
Invoice		36,128.50	31	01-07-2020	03-22-2020
Invoice		29,744.80	31	01-07-2020	03-22-2020
Invoice		62,243.65	29	01-09-2020	03-24-2020
Invoice		9,306.72	28	01-10-2020	03-25-2020
Invoice		8,846.00	28	01-10-2020	03-25-2020
Invoice		1,873.20	28	01-10-2020	03-25-2020
Invoice		3,439.44	27	01-11-2020	03-26-2020
Invoice		54,257.82	27	01-11-2020	03-26-2020
Invoice		1,267.58	24	01-14-2020	03-29-2020
Invoice		11,290.40	22	01-16-2020	03-31-2020

Beispiel einer E-Mail, die im Rahmen eines Betrugsversuchs mit Lieferantenrechnungen verschickt wurde

Angreifer können beim Betrug mit Lieferantenrechnungen sowohl Nachahmungstaktiken als auch kompromittierte Konten nutzen, um Anmeldedaten zu stehlen, Malware zu verbreiten und gefälschte Rechnungen zu verschicken. Während die Angreifer also aus diesen Betrugsversuchen Kapital schlagen wollen, legen sie gleichzeitig auch den Grundstein für weitere Angriffe – vorausgesetzt, sie haben dazu die Zeit und Gelegenheit.

So funktioniert Betrug mit Lieferantenrechnungen



1. Krimineller Akteur übernimmt E-Mail-Konto

Betrug mit Lieferantenrechnungen beginnt in der Regel damit, dass ein Angreifer das E-Mail-Konto eines Mitarbeiters bei einem vertrauenswürdigen Lieferanten übernimmt oder ein täuschend ähnliches Doppelgänger-Konto anlegt.

2. Angreifer sucht nach E-Mails über Rechnungen

Der Angreifer durchsucht anschließend die Kontaktliste im kompromittierten Lieferantenkonto und sucht im Posteingang nach E-Mails über Rechnungen.

3. Angreifer nutzt legitime Transaktion aus

Mit den Informationen über die Rechnungs- und Zahlungsvorgänge des betroffenen Unternehmens in der Hand wartet der Angreifer auf die Gelegenheit, eine legitime Transaktion für sich auszunutzen.

4. Angreifer antwortet auf einen bestehenden E-Mail-Thread

Zu diesem Zeitpunkt wechselt der Angreifer üblicherweise zu einem Doppelgänger-Konto und antwortet auf einen bestehenden E-Mail-Thread, um den Zugang zur legitimen Konversation zu wahren – selbst wenn das betroffene Unternehmen die Kontrolle über das Konto wiedererlangt.

5. Angreifer schickt gefälschte Rechnung

Wenn der Lieferant eine Rechnung an das betroffene Unternehmen schickt, greift der Angreifer ein und schickt stattdessen eine gefälschte Rechnung. Die Rechnung enthält Überweisungsdaten zu einem Konto, das unter der Kontrolle des Angreifers steht, und möglicherweise ebenso eine Aufforderung an das Unternehmen, die bestehenden Überweisungsdaten zu ändern.

6. Unternehmen überweist Rechnungsbetrag auf Konto des Angreifers

Das betroffene Unternehmen zahlt die Rechnung und der Betrag wird auf das Konto des Angreifers überwiesen. Bis der echte Lieferant die fehlende Zahlung bemerkt, hat der Angreifer das Geld bereits abgehoben und das Konto geschlossen.

Sechs Maßnahmen zum Schutz Ihres Unternehmens vor BEC-Angriffen

Cyberkriminelle setzen mehrere Taktiken und Kombinationen von Nachahmung und Kontenkompromittierung bei E-Mail-Betrugsversuchen ein. Zudem läuft jeder Angriff anders ab. Ein wichtiges Merkmal aller erfolgreichen Angriffe ist jedoch der Vertrauensmissbrauch der Mitarbeiter.

Diese komplexen, hochentwickelten und schwer erkennbaren Angriffe können nicht durch eine einzelne Verteidigungslinie abgewehrt werden. Stattdessen ist ein mehrschichtiger, vollständig integrierter und personenzentrierter Ansatz erforderlich.

Im Folgenden erläutern wir sechs Strategien für den Aufbau eines derartigen Sicherheitssystems:

1. Überblick über die BEC-Risiken Ihrer Anwender erlangen

Ein personenorientierter Ansatz beginnt selbstverständlich mit dem Menschen. Jede Person ist einzigartig, genau wie ihr Wert für Cyberangreifer und damit auch das Risiko für ein Unternehmen. Das Risikoprofil eines Anwenders besteht aus einer beliebigen Kombination von drei Faktoren: Schwachstellen, Angriffe und Berechtigungen.

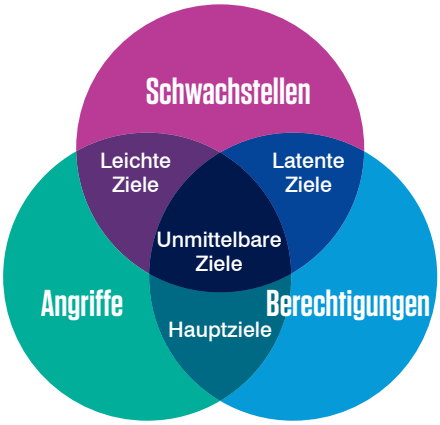
Anhand folgender Punkte können Sie die Risikoprofile der Anwender in Ihrem Unternehmen beurteilen:

- **Ihre digitalen Gewohnheiten und Schwächen (Schwachstellen).** Folgende Fragen sollten Sie sich unter anderem stellen: Welche Rollen haben Anwender? Für welche Vorgänge sind sie autorisiert? Wie arbeiten sie? Worauf klicken sie? Auf welche Art greifen sie auf Unternehmensressourcen zu? Auf welche Arten von Anwendungen und Daten können sie zugreifen?
- **Bedrohungstypen, denen sie begegnen könnten (Angriffe).** Könnten die Anwender Opfer zielgerichteter Angriffe (z. B. BEC) werden und daher fortgeschrittene Schutzmaßnahmen und Schulungen benötigen? Oder werden sie eher mit gewöhnlichen Standard-Bedrohungen konfrontiert sein, die mithilfe von Standardschutzmaßnahmen und grundlegenden Cybersicherheitsschulungen eingedämmt werden können?
- **Ihre Zugangsberechtigungen (Berechtigungen).** Bei den Berechtigungen werden alle potenziell hochwertigen Assets erfasst, auf die Anwender Zugriff haben, zum Beispiel Daten, finanzielle Befugnisse und wichtige Kontakte. Auch der Rang von Anwendern im Unternehmen (z. B. in der Finanzabteilung oder in der Geschäftsleitung) ist ein Faktor für die Bewertung von Berechtigungen. Das ist jedoch nicht der einzige Faktor – und häufig noch nicht einmal der wichtigste.

Erhöhte Risiken in jeder dieser drei Kategorien sind ein Grund zur Sorge und in den meisten Fällen auch für zusätzliche Sicherheitsmaßnahmen. Zwei oder mehr erhöhte Risikostufen sind ein Hinweis auf ein dringendes Sicherheitsproblem.

Diese vier Anwenderkategorien zeigen, welchen Einfluss Kombinationen aus Schwachstellen, Angriffen und Berechtigungen auf Ihr Gesamtrisiko haben:

- **Latente Ziele:** Anwender mit umfangreichen Berechtigungen, die gleichzeitig anfälliger für Phishing-Köder sind.
- **Leichte Ziele:** Häufig angegriffene Anwender, die für Bedrohungen anfällig sind.



BEWERTUNG DES ANWENDERRISIKOS

Ebenso wie jeder Mensch einzigartig ist, sind auch sein Wert für die Cyberangreifer und das Risiko für den Arbeitgeber individuell.

Menschen haben ihre ganz eigenen digitalen Gewohnheiten und **Schwachstellen**. Sie werden mit unterschiedlichen Mitteln und wechselnder Intensität **angegriffen** und verfügen jeweils über ganz eigene **Zugriffsberechtigungen** für Daten, Systeme und Ressourcen.

Diese miteinander verknüpften Faktoren bestimmen das individuelle Gesamtrisiko eines Anwenders.

- **Hauptziele:** Anwender mit weitreichenden Berechtigungen, die einer ständigen Flut von Angriffen ausgesetzt sind, was im Erfolgsfall erhebliche Schäden im Unternehmen anrichten könnte.
- **Unmittelbare Ziele:** Die vierte Kategorie umfasst Anwender, die vom Unternehmen als dringende Priorität für Schutzmaßnahmen betrachtet werden sollten. Bei ihnen sind alle drei Risikofaktoren erhöht: Schwachstellen, Angriffe und Berechtigungen. Sie sind mit anderen Worten anfällig für die Tools und Taktiken von Bedrohungsakteuren. Sie werden gezielt von Angreifern ins Visier genommen und haben Zugang zu Daten, Systemen und anderen Ressourcen, was im Falle einer erfolgreichen Kompromittierung zu dauerhaften Schäden führen könnte.

2. Übersicht über Lieferanten verbessern

Sie sollten wissen, wer Ihre Lieferanten sind, über welche Domänen sie E-Mails an Ihre Anwender schicken und mit wem Ihre Anwender bei diesen Firmen in der Regel in Kontakt stehen.

Die Identifizierung der Mitarbeiter in Ihrem Unternehmen, die anfälliger sind, häufiger angegriffen werden und höhere Berechtigungen haben, ist ein wichtiger Schritt bei der Verhinderung von BEC-Angriffen. Doch das Lieferketten- und Partner-Ökosystem ist ein wichtiger Bedrohungsvektor, über den Cyberkriminelle Ziele indirekt angreifen können. Aus diesem Grund müssen Sie dafür sorgen, dass Sie einen guten Überblick über die Lieferkette Ihres Unternehmens haben und die Risiken verstehen, die von einigen externen Parteien ausgehen könnten.

Sie sollten wissen, wer Ihre Lieferanten sind, über welche Domänen sie E-Mails an Ihre Anwender schicken und mit wem Ihre Anwender bei diesen Firmen in der Regel in Kontakt stehen. Zudem sollten Sie – soweit es möglich ist – in Erfahrung bringen, wer Ihre Lieferanten beliefert. Nehmen Sie sich die Zeit und erstellen Sie eine Liste aller Anbieter, die so viele Details wie nötig enthält, damit Sie einen Überblick über die Risiken Ihrer Lieferanten erhalten.

Um diesen Prozess zu vereinfachen, sollten Sie sich für eine Lösung entscheiden, die Folgendes automatisieren kann:

- Identifizierung Ihrer Lieferanten und der von ihnen verwendeten Domänen zum Versenden von E-Mails an Ihre Anwender
- Suche von Lieferanten-Doppelgänger-Domänen
- Erkennung von Bedrohungen durch Lieferanten-Domänen, z. B. Impostor-Bedrohungen, Phishing, Malware und Spam
- Validierung von Lieferanten-DMARC-Datensätzen und Blockierung von Angriffen, die Lieferanten-Domänen nachahmen

3. BEC-Bedrohungen erkennen und blockieren, noch bevor sie Ihr Unternehmen erreichen

Die dritte Empfehlung mag offensichtlich erscheinen, doch sollten Sie bedenken, dass nicht alle Schutzmaßnahmen Nachahmungstaktiken wirksam erkennen und blockieren können.

BEC-Angriffe sind anders als andere Cyberbedrohungen. Sie zu stoppen erfordert den Einsatz fortgeschrittener Lösungen und Strategien, die zur dynamischen Analyse und Überwachung potenzieller Bedrohungen dienen. Um BEC-Angriffe zu identifizieren und zu stoppen, reicht die Erkennung mit statischen Regeln reicht nicht aus, denn die Techniken und Taktiken entwickeln sich einfach zu schnell weiter.

Wo Sie nach Anzeichen für BEC-Angriffe suchen sollten

- E-Mail-Header
- IP-Adresse des Absenders
- Absender-/Empfänger-Beziehung
- Reputation des Absenders
- Emotionale, stilistische und sprachliche Besonderheiten

Betrug mit Lieferantenrechnungen zu erkennen – bei dem in der Regel ein legitimes, aber kompromittiertes Lieferantenkonto verwendet wird –, kann sogar noch schwieriger sein. Ihre Abwehr muss selbst die raffiniertesten Lieferanten-Betrugsversuche blockieren können. Wählen Sie eine Lösung, die Nachrichten auf zahlreiche Taktiken, die zum Lieferantenbetrug gehören, dynamisch analysiert.

Taktiken beim Betrug mit Lieferantenrechnungen

- Änderungen der Reply-to-Adresse
- Verwendung schädlicher IP-Adressen
- Verwendung nachgeahmter Lieferantendomänen
- Wörter und Formulierungen, die für Lieferantenbetrug typisch sind

Machine Learning

Im Gegensatz zu älteren Tools können sich Machine Learning-Tools an die neuesten BEC-Bedrohungen anpassen, ohne ständig manuell neu eingestellt werden zu müssen.

Im Gegensatz zu älteren Tools können sich Machine Learning-Tools an die neuesten BEC-Bedrohungen anpassen, ohne ständig manuell neu eingestellt werden zu müssen. Die effektivste Machine Learning-Technologie kann schnell auf geänderte Angreifertaktiken reagieren und sie stoppen.

Doch eins sollten Sie wissen: Machine Learning allein ist keine Wunderwaffe. Machine Learning-Modelle sind nur so effektiv wie der Umfang der Daten, mit denen sie trainiert werden, sowie die menschliche Kompetenz für Bedrohungen, mit der sie optimiert werden. Wenn die Modelle mit schlechten oder unvollständigen Daten und ohne Bedrohungskontext trainiert werden, erzeugen sie viele False Positives. Das bedeutet mehr Arbeit für die Sicherheits- und Messaging-Teams und ein schlechtes Benutzererlebnis.

4. Widerstandsfähigkeit Ihrer Anwender stärken

Bei BEC-Angriffen werden Social-Engineering-Taktiken und keine technischen Exploits genutzt. Zudem sind sie nur erfolgreich, wenn Anwender darauf hereinfallen. Daher sind gut geschulte Anwender die letzte und stärkste Verteidigungslinie Ihres Unternehmens.

Alle Mitarbeiter sollten über Impostor-Bedrohungen informiert sein. Da sich diese Angriffe jedoch ganz gezielt gegen einige bestimmte Personen richten, sollten Sie besonders Mitarbeiter in bestimmten Abteilungen (z. B. in der Buchhaltung, in der Finanz- und der Personalabteilung sowie im Einkauf) im Sicherheitsbewusstsein schulen, damit sie häufig genutzte Täuschungstaktiken kennen und darauf achten können. Zudem sollten Sie Folgendes tun:

- Bieten Sie Mitarbeitern in wichtigen Positionen im Unternehmen (z. B. CEO und CFO) angemessene Schulungsmöglichkeiten.
- Schulen Sie andere Mitarbeiter, die ein erhöhtes Risiko darstellen, weil sie anfälliger sind, häufiger angegriffen werden oder mehr Berechtigungen haben.
- Erwägen Sie, externen Partnern und Freiberuflern mit Zugang zum Unternehmenssystem Schulungen zur Steigerung des Sicherheitsbewusstseins anzubieten. Diese Arbeitskräfte sind oft ein wichtiger Bestandteil der modernen Arbeitslandschaft – besonders im heutigen Arbeitsumfeld, wo häufiger verteilt und im Home Office gearbeitet wird. In puncto Sicherheit werden sie jedoch oft übersehen.
- Besprechen Sie die Risiken durch Betrug mit Lieferantenrechnungen mit den Anwendern, die am ehesten von diesem Angriffstyp betroffen sein werden.

Schulungen zur Sensibilisierung für Sicherheit und andere Schulungen zu BEC-Betrugsversuchen sollten nicht nur einmalig oder unregelmäßig stattfinden, da diese Bedrohungen wie die meisten anderen Cyberbedrohungen ständig auftreten und immer weiter entwickelt werden.

Um die passenden Schulungen für die richtigen Mitarbeiter bereitzustellen, kann es hilfreich sein, einen externen Anbieter mit Fachwissen im Bereich Awareness-Schulungen an Bord zu holen – zum Beispiel für die Durchführung von Phishing-Simulationen, die auf realen BEC-Angriffen basieren, um Anwender für Bedrohungen zu schulen, die ihnen am ehesten begegnen werden.

Für die Abwehr von BEC-Angriffen empfiehlt es sich zudem, Anwender dazu aufzufordern, verdächtige E-Mails zu melden und es ihnen dabei leicht zu machen. Das Sicherheitsteam muss außerdem schnell reagieren, wenn Anwender eine Nachricht kennzeichnen, und schnell einschätzen, ob die E-Mail eine Bedrohung darstellt oder nicht. Wenn Anwender keine schnelle (oder gar keine) Rückmeldung bekommen, sinkt eventuell ihre Motivation, auch weiterhin verdächtige Nachrichten melden. Zudem könnten sie im Umgang mit E-Mails nachlässig werden.

5. Reaktion auf Zwischenfälle und deren Behebung automatisieren

Durch die Automatisierung wichtiger Bereiche der E-Mail-Analyse und der Reaktion kann das Sicherheitsteam seine Arbeit besser priorisieren und schneller auf Bedrohungen und von Anwendern gemeldete E-Mails reagieren.

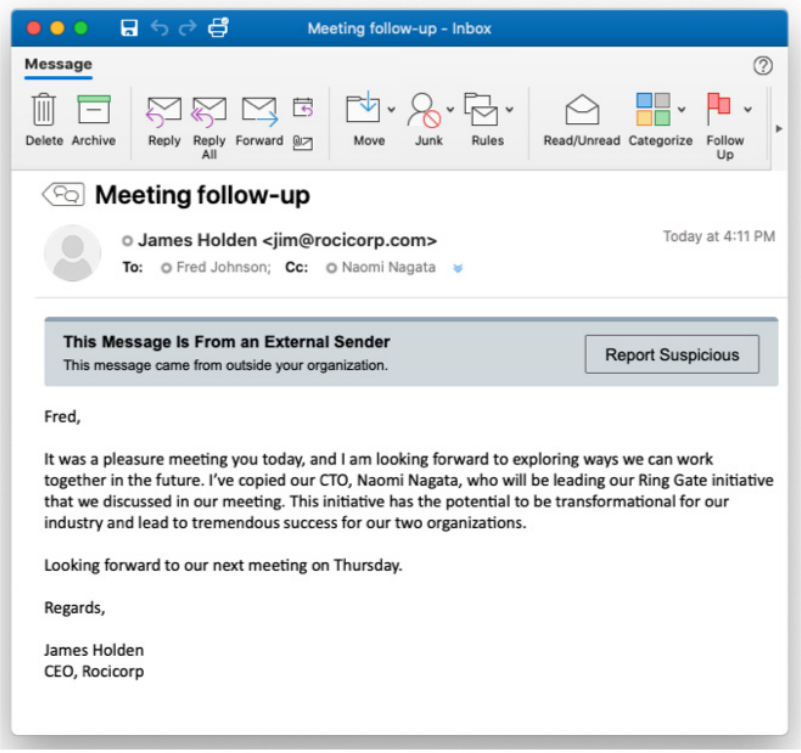
Die meisten Unternehmen haben Probleme durch zu kleine Sicherheitsteams, die von der Verwaltung unzähliger, nicht miteinander kommunizierender Sicherheitsanbieter und -produkte überfordert sind. Das erschwert die schnelle Suche, Untersuchung und Behebung von BEC-Bedrohungen im gesamten Unternehmen – und verlängert den Zeitraum, in dem das Unternehmen gefährdet bleibt.

Durch die Automatisierung wichtiger Bereiche der E-Mail-Analyse und der Reaktion kann das Sicherheitsteam seine Arbeit besser priorisieren und schneller auf Bedrohungen und von Anwendern gemeldete E-Mails reagieren. Das Sicherheitsteam sollte besorgte Anwender darüber informieren, dass sie während der laufenden Analyse bei Bedarf Zugang zu Informationen einer E-Mail, die als verdächtig eingestuft wurde, erhalten können.

Eine automatische Kennzeichnung externer E-Mails informiert die Empfänger über den Ursprung einer E-Mail und kann Anwendern Anlass geben, eine Nachricht näher anzuschauen und zu prüfen, ob es sich um einen legitimen oder nachgeahmten Absender handelt.

Wird die Nachricht als schädlich erkannt, dann wird sie – einschließlich aller Kopien und Weiterleitungen – automatisch unter Quarantäne gestellt. Ihr Team muss nicht jeden einzelnen Vorfall manuell handhaben und untersuchen und spart somit Zeit und Aufwand.

Um den Kreis zu schließen, erhalten Ihre Anwender eine angepasste E-Mail mit der Information, dass die Nachricht als schädlich eingestuft wurde. Das fördert richtiges Verhalten und motiviert Ihre Mitarbeiter, ähnliche Nachrichten auch weiterhin zu melden.



6. Vor Angriffen schützen, die sich gegen Ihre Kunden und Ihre Marke richten

Sie sollten daher eine Lösung wählen, die Ihre Marke und den Ruf Ihres Unternehmens schützt, indem sie den Versand betrügerischer E-Mails über Ihre vertrauenswürdigen Domänen verhindert.

Bei Marken-Spoofing richten die Angreifer sich direkt gegen Ihre Kunden und Geschäftspartner und versuchen, über Ihren Firmennamen und Ihre Marke an Geld zu gelangen.

Dies muss nicht sofort zu finanziellen Verlusten für Ihr Unternehmen führen, doch die Angriffe können den Ruf Ihres Unternehmens schädigen, das Kundenvertrauen beeinträchtigen und langfristige Geschäftsschäden verursachen.

Sie sollten daher eine Lösung wählen, die Ihre Marke und den Ruf Ihres Unternehmens schützt, indem sie den Versand betrügerischer E-Mails über Ihre vertrauenswürdigen Domänen verhindert. Alle zugestellten und von Ihrem Unternehmen aus versendeten E-Mails sollten dabei durch branchenübliche DMARC-Kontrollen (Domain-based Message Authentication, Reporting and Conformance) authentifiziert werden.

Außerdem sollten Sie einen Überblick über alle E-Mails erhalten, die unter Verwendung Ihrer E-Mail-Domäne versendet werden, einschließlich vertrauenswürdiger externer Versender.

Auch wenn Sie Ihre Domäne gesperrt haben, können Doppelgänger-Domänen zu einem Problem werden, da Kunden auf BEC-E-Mails hereinfallen könnten, die von Ihrem Unternehmen zu stammen scheinen. Suchen Sie nach neu registrierten Domänen, die Ihre Marke bei E-Mail-Angriffen oder auf Phishing-Webseiten imitieren, bevor sie von einem geparkten Status aus aktiv oder „scharf geschaltet“ werden. Das Gleiche gilt für Angreifer, die Ihre Marke auf anderen digitalen Kanälen imitieren, zum Beispiel auf Web-Domänen, in sozialen Netzwerken und im Darknet.

Fazit: Die Stärke einer einheitlichen personenzentrierten Abwehr

Um einen mehrschichtigen, vollständig integrierten, personenzentrierten Ansatz für den Schutz Ihres Unternehmens vor BEC-Angriffen aufzubauen, ist es nötig, sich von der „Silo-Denkweise“ in der Sicherheit zu trennen und vernetzt zu denken. Auch wenn Sie Einzelprodukte nutzen, um alle Angriffsmöglichkeiten abzusichern, müssen diese Elemente eng zusammenarbeiten und sich so gegenseitig unterstützen.

Wenn Sie über eine zentrale oder integrierte E-Mail-Sicherheitslösung verfügen, können Sie Sicherheitsabläufe vereinfachen und Ihre IT-Ressourcen besser nutzen. Auf diese Weise können Sie Ihre Kosten sowie Ihren Arbeitsaufwand verringern und – noch wichtiger – Ihr Unternehmen vor der sich ständig weiterentwickelnden BEC-Bedrohungslandschaft effektiver schützen.

Weitere Informationen zu Proofpoint-Lösungen zum Schutz Ihres Unternehmens vor BEC-Angriffen finden Sie unter:

proofpoint.com/us/solutions/bec-and-eac-protection.

WEITERE INFORMATIONEN

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

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) 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.

0503-004-01-01 06/21