proofpoint®

BEC SURVIVAL GUIDE

SO ÜBERSTEHEN SIE BUSINESS EMAIL COMPROMISE-ANGRIFFE

Über den Umgang mit BEC-Angriffen (Business Email Compromise) und CEO-Betrug zum Schutz Ihres Unternehmens

INHALT

KURZFASSUNG

Business Email Compromise-Angriffe (BEC) setzen auf eine einfache Methode, mit der bereits einige der fortschrittlichsten Unternehmen der Welt getäuscht werden konnten.

Seit das FBI im Jahr 2015 begann, BEC-Angriffe nachzuverfolgen, wurden weltweit mehr als 22.000 Unternehmen Opfer dieser Betrugsform und verloren dabei schätzungsweise 3,08 Milliarden US-Dollar.[1]

Im Gegensatz zu anderen Cyberangriffsformen nutzen BEC-E-Mails weder Malware noch böswillige URLs, sondern Social-Engineering-Taktiken.

Bei BEC-Attacken werden häufig CFOs oder Mitarbeiter der Personal- bzw. Finanzabteilung oder der Lohnbuchhaltung gezielt angegriffen. Mit einer als „Spoofing" bezeichneten Methode werden die Opfer getäuscht und davon überzeugt, dass die erhaltene E-Mail von ihrem Vorgesetzten, einem Kollegen, einem Lieferanten oder einem Geschäftspartner stammt. Der Betrüger fordert den Empfänger zur Tätigung einer Überweisung oder zur Weitergabe von Steuerunterlagen oder anderer vertraulicher Daten auf.

Die BEC-Angreifer sind deshalb so erfolgreich, weil die von ihnen verfassten E-Mails legitime Nachrichten überzeugend nachahmen. Zudem bitten sie ihre Opfer um die Durchführung von Aufgaben, die in deren normalen Tätigkeitsbereich fallen.

Aufgrund dieser äußerst einfachen Strategie überwinden diese E-Mails problemlos herkömmliche, auf technologiebasierte Angriffe ausgerichtete Sicherheitslösungen.

So schützen Sie Ihr Unternehmen

Zum Glück können Sie BEC-Angriffe mit einer Strategie stoppen, die die Faktoren Mitarbeiter, Prozesse und Technologie kombiniert.

Vor einem Angriff

BEC-Angriffe lassen sich mit einem dreifachen Ansatz vermeiden:

- Machen Sie Ihre Mitarbeiter bei Schulungen auf BEC-Angriffe aufmerksam.
- Implementieren Sie Prozesse und Richtlinien für geschäftliche Abläufe, die per E-Mail erfolgen.
- Nutzen Sie erweiterten Bedrohungsschutz, der BEC-Angriffe blockiert, bevor sie die Postfächer der Mitarbeiter erreichen. Diese Schutzlösung sollte auch Aktionen von Mitarbeitern blockieren, die von BEC-Angreifern zur Weitergabe vertraulicher Informationen verleitet wurden.

Eine effektive Lösung kombiniert zwei leistungsstarke Funktionen: Erkennung und Blockierung von BEC-Angriffen an Ihrem E-Mail-Gateway. Außerdem authentifiziert sie Ihre Unternehmens-E-Mails an den Gateways Ihrer Partner sowie bei den Verbraucher-E-Mail-Providern Ihrer Kunden.

Erwägen Sie die Implementierung von Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) sowie Domain-based Message Authentication, Reporting and Conformance (DMARC). Zusätzlich kann es sinnvoll sein, Kontrollen zum Schutz vor Datenkompromittierung (DLP) an Ihrem E-Mail-Gateway bereitzustellen, um die Arten vertraulicher Informationen zu schützen, die BEC-Betrüger typischerweise angreifen.

[1] FBI: „Business E-Mail Compromise: The 3.1 Billion Dollar Scam" (Business E-Mail Compromise: Der 3,1-Milliarden-Dollar-Betrug), Juni 2016.

Nach einem Angriff

Cyberkriminelle suchen nach immer neuen Möglichkeiten, Ihre Mitarbeiter hinters Licht zu führen, Ihre Technologien zu umgehen und eigene Vorteile zur erzielen.

Wenn ein Angriff mit einer Banküberweisung erfolgreich war, beginnen Sie bei der anschließenden Problembehebung damit, dass Sie Ihre Bank kontaktieren. Bitten Sie Ihre Mitarbeiter, die Bank zu kontaktieren, an die die Überweisung getätigt wurde. Wenden Sie sich anschließend an Ihre örtlichen Strafverfolgungsbehörden, um den Angriff zu melden.

Möglicherweise müssen Sie außerdem Ihre Versicherung und Ihre Aktionäre bzw. Gesellschafter benachrichtigen. Und wenn vertrauliche Informationen in die Hände der Cyberkriminellen geraten sind, müssen Sie die Nebenwirkungen minimieren.

Außerdem muss analysiert werden, warum der Angriff erfolgreich war. Unabhängig von der Ursache für den Angriff müssen Sie Ihre Schulungsmaßnahmen anpassen, damit Ihre Mitarbeiter in Bezug auf aktuelle Bedrohungen, die Vorgehensweise der Kriminellen sowie neue Lösungen auf dem neuesten Stand sind.

Obwohl bei BEC-Angriffen keine Malware verwendet wird, kann ein erfolgreicher Angriff auf Schwachstellen in Ihrer Cyberabwehr hinweisen. Erwägen Sie die Durchführung einer Bedrohungsauswertung, um die verborgenen Risiken aufzudecken und einzuschätzen, wie gut Sie auf zukünftige Bedrohungen reagieren können.

Schlüssel zu einer starken Abwehr

Die Bedrohung für Unternehmen durch BEC-Angriffe wächst, weil diese auf Schwachstellen abzielen, die nicht gepatcht werden können: Menschen. Deshalb sind für zuverlässigen Schutz und effektive Reaktionen Mitarbeiterschulungen, Finanzkontrollen und Technologien unerlässlich.

Sie benötigen eine Lösung, die sich nicht ausschließlich auf Reputation und grundlegende E-Mail-Konfigurationen stützt. Dank detaillierter Kontrollen können hochentwickelte E-Mail-Lösungen betrügerische E-Mails identifizieren und isolieren, bevor sie die Postfächer Ihrer Mitarbeiter erreichen.

EINFÜHRUNG

EIN WACHSENDES PROBLEM

Es ist viel einfacher als gedacht, auf betrügerische E-Mails hereinzufallen. Stellen Sie sich folgendes Szenario vor: Sie arbeiten in einem großen Unternehmen, das ein anderes Unternehmen übernehmen möchte. Ihre Aufgabe besteht darin, Rechnungen zu begleichen. Eines Morgens erhalten Sie eine E-Mail von Ihrem Geschäftsführer, der derzeit auf Geschäftsreise ist. Er bittet Sie, eine Überweisung zu tätigen, mit der die Übernahme des anderen Unternehmens in die Wege geleitet werden soll. Dabei sollen Sie diese Informationen nicht weitergeben, da dieser Deal bis zum tatsächlichen Abschluss geheim bleiben soll.

Es ist für Ihren Geschäftsführer nicht untypisch, dass er Sie per E-Mail um eine Überweisung bittet. Und es ergibt durchaus Sinn, dass diese Neuigkeit noch nicht bekannt werden soll.

Ein anderes Beispiel: Ihr Unternehmen arbeitet mit einem Lieferanten im Ausland zusammen. Sie haben erfahren, dass der Lieferant seine Abläufe verändern möchte. In dieser Situation erhalten Sie von diesem Lieferanten eine E-Mail mit dem Hinweis, dass er die Bank wechselt. In der E-Mail erhalten Sie die nötigen Kontoangaben für alle zukünftigen Zahlungen an das neue Bankkonto.

Der Name des Lieferanten stimmt. Der Name des Absenders stimmt. Die Bank gibt es wirklich.

Dennoch handelt es sich in beiden Szenarien, die an echte Ereignisse angelehnt sind, um Betrug. Sie sind Beispiele für Business Email Compromise (BEC), eine Angriffsform, die weltweit bereits über 22.000 Unternehmen getroffen und seit der Aufnahme von FBI-Ermittlungen (im Januar 2015) geschätzt 3,08 Milliarden US-Dollar gekostet hat.[2]

BEC-Angriffe verwenden E-Mails, um Menschen zur Überweisung von Geld oder Weitergabe vertraulicher Unternehmensdaten (z. B. personenbezogene Mitarbeiterdaten) zu verleiten.

Wenn Anfragen zu Banküberweisungen oder vertraulichen Mitarbeiterdaten von der richtigen Person gesendet werden, können sie durchaus legitim sein. Unternehmen erhalten weltweit jeden Tag solche E-Mails, die moderne Geschäftsabläufe erst möglich machen. Das Problem dabei: Es ist nicht immer einfach, authentische E-Mails und betrügerische BEC-E-Mails zu unterscheiden – und eine falsche Einschätzung kann hohe Kosten verursachen.

Zum Glück ist es möglich, den Erfolg von BEC-Angriffen zu vereiteln. Der vorliegende Leitfaden soll dabei als Ausgangspunkt dienen. Wir zeigen auf, welche Faktoren BEC-Angriffe fördern, wie Sie tun können, wenn Sie Opfer eines solchen Angriffs geworden sind, und – noch wichtiger – wie Sie gar nicht erst zum Opfer werden.

[2] FBI: „Business E-Mail Compromise: The 3.1 Billion Dollar Scam“ (Business E-Mail Compromise: Der 3,1-Milliarden-Dollar-Betrug), Juni 2016.

ABLAUF VON BEC: ZIELE UND METHODEN

Ihre Mitarbeiter sind Ihre wichtigste Ressource. In Bezug auf Cyber-Sicherheit können sie aber auch das schwächste Glied sein. Sie sind für Angriffe anfällig, die nicht etwa technische Fehler, sondern vor allem menschliches Verhalten ausnutzen.

Cyberkriminelle führen Recherchen zu ihren Opfern durch und suchen dabei nach dem Mitarbeiter mit der optimalen Position. Sie studieren Ihr Unternehmen und besuchen regelmäßig Ihre Website. Sie rufen Ihre Social-Media-Auftritte (z. B. in LinkedIn) auf, um sich über Ihre Mitarbeiter zu informieren – deren Position, ehemalige Arbeitgeber, Kollegen und Interessen.

ZIELE

Wenn Cyberkriminelle Geld stehlen möchten, informieren sie sich über die Mitarbeiter in Ihrer Finanzabteilung. Etwa 47 % der betrügerischen E-Mails greifen den CFO an.[3] Sie suchen nach vertraulichen Unternehmensdaten oder personenbezogenen Mitarbeiterinformationen und versuchen, so viel wie möglich über die Mitarbeiter Ihrer Personalabteilung zu erfahren. Etwa 25 % der Angriffe zielen auf die Finanzabteilung ab.[4]

Sie suchen nach neuen Mitarbeitern, die möglicherweise noch nicht mit den Richtlinien und Vorgehensweisen in Ihrem Unternehmen vertraut sind. Sie finden heraus, wann und wo Ihre führenden Mitarbeiter auf Geschäftsreise sind und zu welchen Tageszeiten bzw. Wochentagen in Ihrem Unternehmen am meisten los ist. Diese Informationen genügen, um betrügerische Nachrichten täuschend echt erscheinen zu lassen und das Opportunitätsfenster zum eigenen Vorteil auszunutzen.

METHODEN

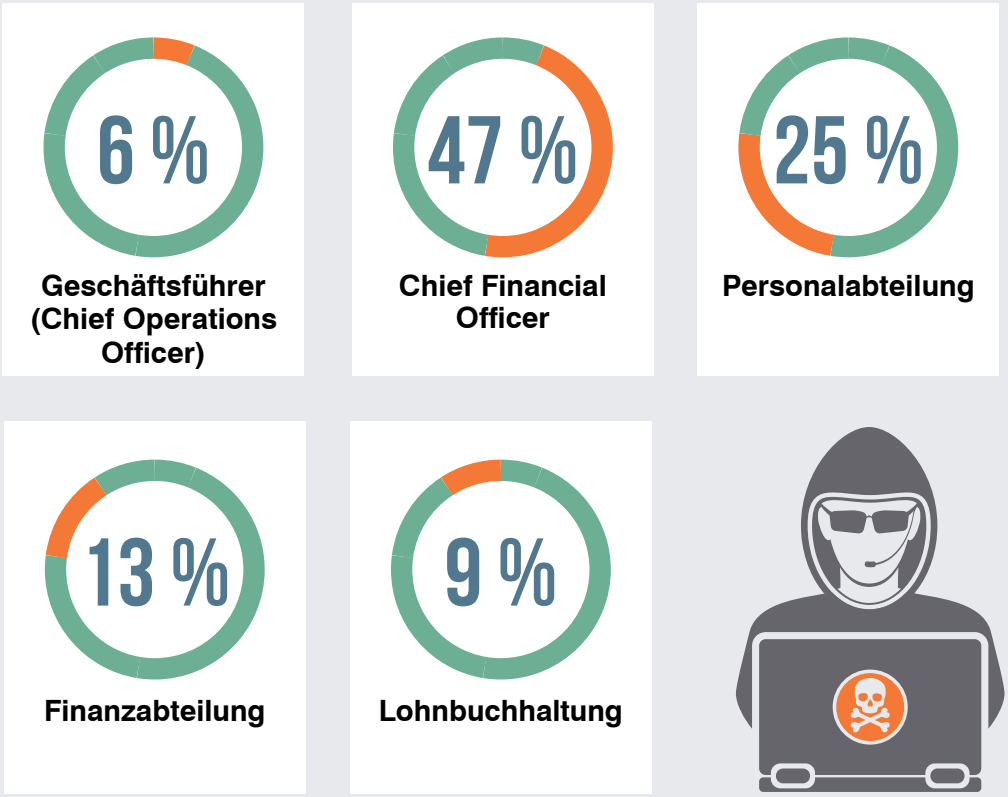
BEC-Angriffe zielen auf Menschen ab. Die Angriffe sind so konzipiert, dass Ihre Mitarbeiter davon ausgehen müssen, eine E-Mail von einer hochrangigen Führungskraft in Ihrem Unternehmen (z. B. vom Geschäftsführer) oder von einem Lieferanten, Geschäftspartner bzw. Kollegen erhalten zu haben. Der Absender der betrügerischen E-Mail bittet zum Beispiel um die Überweisung von Geld oder die Übermittlung von Steuerdaten, anderer vertraulicher Unternehmensdaten oder von personenbezogenen Informationen.

Auf dem ersten Blick scheint nichts an der E-Mail ungewöhnlich. Doch kleine Abweichungen, z. B. im Namen des Absenders oder in der Absender- bzw. Reply-to-Adresse, weisen auf den Betrugsversuch hin. Cyberkriminelle bauen darauf, dass die Empfänger sich nicht die Zeit nehmen, die E-Mails zu verifizieren.

[3 & 4] Proofpoint-Forschungsergebnisse, März 2016.

WER WIRD ANGEGRIFFEN?

Anteil der durch BEC angegriffenen Mitarbeiter und Abteilungen



Quelle: Proofpoint

DIE VIELEN FORMEN VON BEC

Dies sind die häufigsten BEC-E-Mail-Varianten:

75 %

Gefälschter Name

Diese Variante, die bei 75 % aller Angriffe zum Einsatz kommt, verwendet den Namen der vorgeblichen Führungskraft im Absenderfeld. Die E-Mail-Adresse stammt dabei jedoch von einem externen Dienst (z. B. Gmail), der vom Angreifer verwendet wird.

21 %

Reply-to-Spoofing

Diese Technik verwendet den echten Namen und die echte E-Mail-Adresse der Person, von der die E-Mail angeblich gesendet wurde (meist der Geschäftsführer). Auch der Name im Antwortfeld verweist auf den Namen des angeblichen Absenders. Die Reply-to-Adresse, an die die Antworten tatsächlich gesendet werden, gehört jedoch dem Angreifer.

2 %

Gefälschter Absender (ohne Reply-to-Adresse)

Diese Variante der BEC-E-Mails verwendet den Namen und die E-Mail-Adresse des angeblichen Absenders. Die E-Mail enthält jedoch keine Reply-to-Adresse, sodass kein Zweiwege-Austausch möglich ist. Diese E-Mails enthalten häufig Aufforderungen zu Banküberweisungen, sodass Folgenachrichten nicht erforderlich sind.

2 %

Doppelgänger-Domäne

Bei dieser Variante des BEC-Angriffs ähnelt die Versandadresse des Angreifers der des angeblichen Absenders. Häufig unterscheidet sich die Adresse in nur einem Buchstaben von der tatsächlichen Adresse, z. B. „**echttes**Unternehmen.com“ anstelle von „**echtes**Unternehmen.com“.

Quelle: Proofpoint

GRÜNDE FÜR DEN ERFOLG VON BEC-ANGRIFFEN

Das BEC-Geschäft ähnelt stark dem Blockbuster-Modell in Hollywood. Die meisten Versuche sind Flops, aber mit den wenigen Erfolgen lassen sich spektakuläre Gewinne erzielen.

Für Cyberkriminelle kann Erfolg oder Misserfolg davon abhängen, ob gut recherchiert, die richtige Person als Ziel ausgewählt und der geeignete Zeitpunkt für den Versand der betrügerischen E-Mails gewählt wurde.

Die Betrüger imitieren jedoch nicht nur das Aussehen legitimer E-Mails, sondern wenden zusätzlich psychologische Tricks an. Sie setzen darauf, dass Mitarbeiter ihren Vorgesetzten einen Gefallen tun möchten und erschaffen daher ein falsches Gefühl der Dringlichkeit und Heimlichkeit. Um keinen Verdacht zu erregen, bitten die Angreifer ihre Opfer um die Durchführung von Aufgaben, die zu deren alltäglichen Arbeitsablauf gehören.

Die betrügerischen E-Mails werden häufig dann versendet, wenn die Entscheidungsträger nicht im Büro sind, sodass sich der Inhalt der Nachricht nur schlecht verifizieren lässt. Oder sie gehen zu besonders geschäftigen Zeiten ein, wenn die Opfer mit vielen Aufgaben jonglieren und nicht so gründlich auf BEC-Bedrohungen achten.

BEC-E-Mails sind eine Herausforderung, weil sie im Gegensatz zu anderen Cyberangriffen weder Malware-Anhänge noch böswillige URLs enthalten und stattdessen Social-Engineering-Taktiken anwenden. Dadurch können die betrügerischen E-Mails herkömmliche Sicherheitslösungen überwinden, die sich auf böswillige Inhalte oder Verhaltensweisen konzentrieren, die technische Schwachstellen ausnutzen.

Für Cyberkriminelle bedeuten BEC-Angriffe geringes Risiko bei hohem Gewinnpotenzial – ohne dass hierfür eine kostenintensive Infrastruktur erforderlich ist. Und da die Angriffe meist grenzüberschreitend erfolgen, werden auch nur wenige Betrüger verurteilt.

AKTUELLE BEC-ANGRIFFE

Beispiele für bekannt gewordene BEC-Angriffe:

FACC AG (im Januar 2016 gemeldet)

Cyberkriminelle erbeuteten mit einem BEC-Angriff 55,7 Millionen US-Dollar von einem australischen Unternehmen, das Komponenten für die Luftfahrt entwirft und herstellt. Im Anschluss an den Angriff wurden der CEO und der CFO des Unternehmens entlassen.

Crelan (im Januar 2016 gemeldet)

Nach einem internen Audit stellte die belgische Bank fest, dass sie aufgrund betrügerischer E-Mails mehr als 70 Millionen US-Dollar verloren hatte.

Eine Niederlassung der Crelan-Bank in den Niederlanden.

TWoA (im Dezember 2015 gemeldet)

Ein College in Neuseeland verlor mehr als 100.000 US-Dollar, als der CFO auf eine E-Mail hereinfiel, die zur Zahlung aufforderte.

Ubiquiti Networks, Inc. (im August 2015 gemeldet)

Der Anbieter hochwertiger WLAN-Produkte bezahlte fast 47 Millionen US-Dollar an Angreifer, die sich als Lieferanten ausgaben.

Luminant Corp. (im Jahr 2013 gemeldet)

Der Energieversorger aus Texas (USA) überwies als Reaktion auf eine E-Mail mit gefälschtem Domänennamen mehr als 98.000 US-Dollar.

SO SCHÜTZEN SIE IHR UNTERNEHMEN

Die gute Nachricht: Sie können BEC-Angriffe stoppen, bevor sie erfolgreich abgeschlossen sind. Die beste Schutzmaßnahme verbindet Mitarbeiter, Prozesse und Technologien. Sie benötigen alle drei Faktoren.

VOR EINEM ANGRIFF: VORBEREITUNG UND PRÄVENTION

Mit Schulungen können Sie dazu beitragen, dass Ihre Mitarbeiter die Hinweise auf betrügerische E-Mails erkennen und die empfohlenen Vorgehensweisen anwenden, um nicht auf BEC-Angriffe hereinzufallen. Mit den richtigen Verfahren und Richtlinien können Sie Ihre Mitarbeiter dabei unterstützen, E-Mail-Anfragen auf sichere Weise zu handhaben. Zusätzlich ist die richtige Technologie erforderlich, um Angriffe zu erkennen und zu stoppen, bevor sie die Postfächer erreichen.

Schulungen

Mit Schulungen zur Verbesserung des Sicherheitsbewusstseins in Bezug auf Cybersicherheit im Allgemeinen und BEC-Angriffe im Besonderen können Sie Angriffe vermeiden und die Auswirkungen erfolgreicher Angriffe minimieren. Je besser sich Ihre Mitarbeiter auskennen, desto stärker ist Ihre Verteidigungsposition.

Die Schulungen sollten die Bedrohungslandschaft, aktuelle Social-Engineering-Taktiken sowie die Erkennung betrügerischer E-Mails abdecken. Stellen Sie sicher, dass Ihre Mitarbeiter die normalen Abläufe und Richtlinien kennen, wie Führungskräfte, Geschäftspartner und Kunden entweder Geld oder vertrauliche Daten anfordern.

Behandeln Sie in Ihren Schulungen möglichst auch Details zu tatsächlichen BEC-Angriffen, um zu zeigen, wie sich die Angriffsstrategien in Wirklichkeit abspielen.

Prozesse

BEC-Angriffe verwenden Social-Engineering-Taktiken zum Täuschen von Menschen und sind daher so konzipiert, dass sie glaubwürdig erscheinen. Selbst der beste Mitarbeiter kann einen gut erstellten und ausgeführten BEC-Betrug für echt halten. Daher können klare und strenge Prozesse zur Handhabung und Überprüfung von E-Mail-Anfragen betrügerische Nachrichten enttarnen.

Das FBI empfiehlt, mithilfe von Regeln solche E-Mails zu kennzeichnen, deren Erweiterungen der E-Mail-Domäne Ihres Unternehmens verdächtig ähnlich sind. Durch die Registrierung von Domänen, die nur leicht von der tatsächlichen Domäne Ihres Unternehmens abweichen, können diese Varianten nicht mehr von Kriminellen zum Täuschen Ihrer Mitarbeiter missbraucht werden.[5]

Erwägen Sie die Implementierung interner Finanz- und Kaufkontrollen, die einen zweistufigen (oder noch komplexeren) Verifizierungsprozess erfordern. Die Kontrollen könnten zum Beispiel verlangen, dass zur Autorisierung mehr als eine Person erforderlich ist und für hohe Summe schriftliche Genehmigungen vorliegen sowie telefonische Bestätigungen erfolgen müssen. Wenn bei einer zweistufigen Verifizierung die Bestätigung per Telefon verlangt wird, verwenden Sie bereits bekannte Telefonnummern – nicht die Nummern, die in der E-Mail-Anfrage angegeben sind.

[5] FBI: „Business E-Mail Compromise“, August 2015.
[6] FBI: „Business E-Mail Compromise: The 3.1 Billion Dollar Scam“ (Business E-Mail Compromise: Der 3,1-Milliarden-Dollar-Betrug), Juni 2016.

SIEBEN TIPPS ZUM UMGANG MIT VERDÄCHTIGEN E-MAILS

TIPP 1: VERTRAUEN SIE NICHT DEM ANZEIGENAMEN

Eine beliebte Taktik der Cyberkriminellen besteht darin, den Anzeigenamen für die E-Mail zu fälschen. Überprüfen Sie daher immer die E-Mail-Adresse im From-Header.

TIPP 2: VERTRAUEN SIE NICHT DEM HEADER IN DER E-MAIL-ADRESSE

Cyberkriminelle fälschen nicht nur Marken im Anzeigenamen, sondern auch im Header der E-Mail-Adresse, einschließlich dem Domänennamen. Vergewissern Sie sich, dass alle Angaben richtig sind. Wenn Ihnen etwas verdächtig vorkommt, lassen Sie sich die Authentizität der Nachrichten von der Person bestätigen, die als Absender angegeben ist.

TIPP 3: ACHTEN SIE AUF RECHTSCHREIBFEHLER

Legitime Nachrichten enthalten meist keine schwerwiegenden Rechtschreib- oder Grammatikfehler. Lesen Sie eingegangene E-Mails sorgfältig durch und melden Sie alles, was Ihnen verdächtig vorkommt.

TIPP 4: SEIEN SIE VORSICHTIG, WENN FÜHRENDE MITARBEITER UM UNGEWÖHNLICHE INFORMATIONEN BITTEN

Wie wahrscheinlich ist es, dass Geschäftsführer Steuerdaten einzelner Mitarbeiter überprüfen möchten? Wie häufig wird Ihr Geschäftsführer ausgesperrt und benötigt Zugang zu Ihrem Netzwerk oder ein Kennwort?

TIPP 5: DENKEN SIE ÜBER DRINGENDE ANFRAGEN ZWEIMAL NACH

Gibt es einen guten Grund für diese Aktion? Die Schaffung eines Gefühls von Dringlichkeit und Heimlichkeit ist eine typische Taktik bei BEC-Angriffen – besonders dann, wenn normale Kanäle umgangen werden sollen. Auch in diesem Fall sollten Sie sich die Authentizität der Nachrichten von der Person bestätigen lassen, die als Absender angegeben ist.

TIPP 6: ÜBERPRÜFEN SIE DIE SIGNATUR

Fehlende Details zum Absender oder fehlende Kontaktdaten für das Unternehmen deuten stark auf einen BEC-Angriff hin. Signaturen legitimer Unternehmen enthalten immer Kontaktdaten.

TIPP 7: GLAUBEN SIE NICHT ALLES, WAS SIE SEHEN

Cyberkriminelle sind in dem, was sie tun, außerordentlich gut. Viele betrügerische E-Mails enthalten überzeugende Markenlogos sowie scheinbar gültige E-Mail-Adressen und sind täuschend echt formuliert. Seien Sie bei eingehenden E-Mail-Nachrichten skeptisch.

Laut FBI verzögern einige Finanzinstitute die Verarbeitung von Kundenanfragen bei internationalen Überweisungen, um die Legitimität der Anfragen überprüfen zu können.[6]

Technologien

Eine umfassende technische Lösung ist die dritte und wahrscheinlich wichtigste Säule einer starken BEC-Abwehr.

Ihre Lösung sollte erweiterte Konfigurationsoptionen zur Kennzeichnung verdächtiger Nachrichten basierend auf Attributen wie Übermittlungsrichtung und Betreffzeile unterstützen.

Zudem sollte die Lösung in der Lage sein, BEC-Bedrohungen am E-Mail-Gateway zu erkennen und zu klassifizieren. Eine bewährte Erkennungsmethode ist dabei die dynamische Klassifizierung. Bei diesem Ansatz werden mit dynamischen und algorithmischen Ansätzen die Absender-Empfänger-Beziehung, die Domänenreputation sowie weitere Attribute überprüft. Auf diese Weise können verschiedene Varianten von BEC-Angriffen erkannt werden – und das selbst dann, wenn sie sich verändern.

Eine effektive Lösung ermöglicht auch die proaktive Authentifizierung oder einen richtlinienbasierten Schutz für Ihre Mitarbeiter, Geschäftspartner, Lieferanten und Kunden. Da sich BEC-Angriffe zunehmend gegen Geschäftspartner und Lieferanten richten, die sich außerhalb Ihres E-Mail-Gateways befinden, sollte Ihr Unternehmen eine Möglichkeit bieten, mit der verifiziert werden kann, dass die E-Mails von Ihnen und nicht von einem Betrüger stammen. Mit zweistufigen E-Mail-Authentifizierungstechnologien wie Sender Policy Framework (SPF) und DomainKeys Identified Mail (DKIM) können Sie den Absender einer Nachricht identifizieren:

SPF legt fest, wer im Namen eine Domäne eine E-Mail senden kann und listet die IP-Adressen autorisierter Absender in einem DNS-Datensatz auf. Wenn die Versand-IP-Adresse der E-Mail nicht im SPF-Datensatz gelistet ist, besteht die Nachricht die Authentifizierung nicht.

DKIM hingegen ermöglicht es, eine Nachricht so zu übertragen, dass sie vom E-Mail-Anbieter verifiziert werden kann. E-Mails können von einer festgelegten Domäne digital signiert werden. Die Verifizierung erfolgt mithilfe kryptografischer Authentifizierung innerhalb der digitalen Signatur der E-Mail.

Der neue Authentifizierungsstandard Domain-based Message Authentication Reporting and Conformance (DMARC) verbessert den von SPF und DKIM bereitgestellten Schutz noch weiter. DMARC ist eine offene E-Mail-Technologie, die legitime Absender authentifiziert und die Sicherheit auf Partner und Verbraucher ausdehnt. Für 85 % der weltweiten Verbraucher-Postfächer ist DMARC aktiviert.

Jede der Authentifizierungstechnologien hat ihre Vor- und Nachteile, doch in Verbindung mit den Cybersicherheits-maßnahmen für Ihre Unternehmensinfrastruktur können die kombinierten Ansätze eine Vielzahl von BEC-Angriffen abwehren.

DIE VORTEILE VON DMARC

Mit einer aktiven DMARC-Richtlinie können Absender angeben, ob sie durch SPF, DKIM oder beides geschützt sind. DMARC teilt dem Empfänger mit, wie er vorgehen soll, wenn keine der Authentifizierungsmethoden bestanden wird (z. B. ob die Nachricht in den Spamordner verschoben oder komplett zurückgewiesen werden soll).

DMARC UNTERSTÜTZT ABSENDER WIE FOLGT:

- Sie erhalten einen Überblick darüber, wer Nachrichten in Ihrem Namen versendet, welche E-Mails authentifiziert werden (und welche nicht) und warum.
- Sie können E-Mail-Empfängern mitteilen, wie nicht authentifizierte E-Mails gehandhabt werden sollen.
- Angriffe, die eigene Domänen fälschen, werden blockiert, bevor die Nachrichten die Postfächer der Mitarbeiter und Verbraucher erreichen.

DMARC UNTERSTÜTZT EMPFÄNGER WIE FOLGT:

- Sie können zwischen legitimen und böswilligen Absendern unterscheiden.
- Sie stärken Kundentreue und Mitarbeiterschutz.
- Sie verbessern und schützen die Reputation des E-Mail-Kanals.

NACH EINEM ANGRIFF

Die beste BEC-Strategie besteht darin, den Angriff von Anfang an zu verhindern. Doch Cyberkriminelle suchen nach immer neuen Möglichkeiten, Ihre Mitarbeiter hinters Licht zu führen, Ihre Technologien zu umgehen und eigene Vorteile zur erzielen.

Im Gegensatz zu den meisten Cyberbedrohungen verwenden BEC-Angriffe keine Malware und hinterlassen auch keine Spuren auf Ihrem System, sodass nichts beseitigt werden kann. Die finanziellen Auswirkungen jedoch können langwierig sein.

Wenn der Angreifer Geld gestohlen hat, bemühen sich Unternehmen häufig darum, das Geld zurückzuholen – meist jedoch erfolglos. Im Fall von Ubiquiti (siehe Seite 14) konnte das Unternehmen nur einen kleinen Teil der gestohlenen fast 47 Millionen US-Dollar zurückholen.[7]

Zu den anderen sofort umsetzbaren Schritten gehören die Dokumentation und Meldung des Angriffs – unabhängig vom Umfang und Zeitpunkt des Verlusts. Wenn der Angriff gerade erst erfolgt ist, empfiehlt das BKA den Unternehmen, die örtliche Polizeidienststelle oder das zuständige Landeskriminalamt zu kontaktieren.

Bei der Meldung eines BEC-Angriffs folgende Informationen zur Verfügung gestellt werden:

- Name der zahlenden Person, Adresse, Name der Bank und Kontonummer
- Name des Empfängers, Name der Bank, Kontonummer, Adresse (sofern verfügbar) und Name der Zwischenbank (sofern verfügbar)
- SWIFT-Nummer, Datum und Betrag der Überweisung sowie alle weiteren Informationen

Außerdem sollten Sie Ihre Versicherungen und Aktionäre bzw. Gesellschafter (sofern zutreffend) benachrichtigen und Schadensbegrenzung leisten. Wenn zum Beispiel vertrauliche Informationen weitergegeben wurden, sollten Sie das Risiko minimieren, dass diese Daten missbraucht werden können. Wenn Steuerinformationen gestohlen wurden, können Sie den betroffenen Mitarbeitern zum Beispiel Identitätsdiebstahlschutz zur Verfügung stellen.

Außerdem muss analysiert werden, warum der Angriff erfolgreich war. Sind Ihre aktuellen Cybersicherheitstools in der Lage, Ihr Unternehmen vor BEC und anderen Bedrohungen zu schützen? Wo sind die Schutzlücken? Erwägen Sie die Durchführung einer Bedrohungsauswertung, um verborgene Risiken aufzudecken.

Unabhängig von der Ursache für den Angriff ist es üblicherweise sinnvoll, die Schulungsmaßnahmen anzupassen, damit Ihre Mitarbeiter in Bezug auf aktuelle Bedrohungen, die Vorgehensweise der Kriminellen sowie neue Lösungen auf dem neuesten Stand sind.

Meldung eines BEC-Angriffs

In vielen Ländern gibt es staatliche Organisationen, die sich mit Cyberbetrug (einschließlich BEC-Angriffen) befassen. Hier seien einige Beispiele genannt:

- USA: Internet Crime Complaint Center des FBI (www.IC3.gov)
- Kanada: Canadian Anti-Fraud Centre/Centre Antifraude du Canada (www.antifraudcentre.ca)
- Großbritannien: Action Fraud (www.actionfraud.police.uk)
- Australien: Australian Cybercrime Online Reporting Network (www.acorn.gov.au)
- Singapur: Singapore Computer Emergency Response Team (www.csa.gov.sg/singcert)
- Niederlande: Fraud Helpdesk (www.fraudhelpdesk.org)
- Deutschland: Bundeskriminalamt (BKA) (www.bka.de)

[7] Krebs on Security: „Tech Firm Ubiquiti Suffers $46M Cyberheist“ (Tech-Unternehmen Ubiquiti verliert durch Cyberbetrug 46 Millionen US-Dollar), August 2015.

SCHLUSS-FOLGERUNG UND EMPFEHLUNGEN

Die Bedrohung für Unternehmen durch BEC-Angriffe wächst, weil diese auf Schwachstellen abzielen, die nicht gepatcht werden können: Menschen. Deshalb sind für zuverlässigen Schutz und schnelle Reaktionen Mitarbeiter-schulungen, Finanzkontrollen und insbesondere Technologien unerlässlich.

Sie benötigen eine Lösung, die sich nicht ausschließlich auf Reputation und grundlegende E-Mail-Filterung stützt. Dank detaillierter Kontrollen können hochentwickelte E-Mail-Lösungen betrügerische E-Mails identifizieren und isolieren, bevor sie die Postfächer Ihrer Mitarbeiter erreichen.

Weitere Informationen zu BEC-Angriffen sowie dazu, wie Proofpoint Sie beim Schutz Ihres Unternehmens unterstützen kann, erhalten Sie unter www.proofpoint.com/de.

PRÜFLISTE: SO ÜBERSTEHEN SIE BEC-ANGRIFFE

Mit dieser kurzen Checkliste können Sie überprüfen, ob Sie BEC-Betrugsversuche verhindern und handhaben können.

Vor einem Angriff: Prävention

- ☐ **Führen Sie bei Ihren Mitarbeitern Schulungen zur Stärkung des Sicherheitsbewusstseins durch.**
  - ☐ Bedrohungslandschaft
  - ☐ Neueste Social-Engineering-Taktiken
  - ☐ Identifizierung betrügerischer E-Mails
  - ☐ Vorgehensweisen von Führungskräften, Geschäftspartnern und Kunden bei Anfragen
- ☐ **Entwickeln Sie ein eindeutiges Verfahren zur Handhabung und Überprüfung von E-Mails.**
  - ☐ Regeln zur Kennzeichnung von E-Mails mit Erweiterungen, die Ihren Unternehmens-E-Mails verdächtig ähnlich sind
  - ☐ Registrierung von Domänen mit ähnlichen Namen – bevor Kriminelle es tun
  - ☐ Implementierung interner Finanz- und Kaufkontrollen, die einen zweistufigen (oder noch komplexeren) Verifizierungsprozess erfordern
    - ☐ Hinzuziehen von mehreren Personen zur Autorisierung
    - ☐ Schriftliche Genehmigungen bei hohen Summen
    - ☐ Bestätigung per Telefon
    - ☐ Verzögerte Bearbeitung, um die Legitimität zu überprüfen
- ☐ **Implementieren Sie eine umfassende technische Lösung.**
  - ☐ Erweiterte Konfigurationsoptionen zur Kennzeichnung verdächtiger Nachrichten basierend auf Attributen
  - ☐ Erkennung und Klassifizierung von BEC-Bedrohungen am E-Mail-Gateway
  - ☐ Proaktive Authentifizierung oder richtlinienbasierter Schutz für Mitarbeiter, Geschäftspartner, Lieferanten und Kunden (SPF, DKIM und DMARC)

Nach einem Angriff: Rückabwicklung und Wiederaufnahme der Geschäftstätigkeiten

- ☐ **Kontaktieren Sie Ihr Finanzinstitut.**
- ☐ **Bitten Sie Ihr Finanzinstitut, die Bank zu kontaktieren, an die die Überweisung getätigt wurde.**
- ☐ **Kontaktieren Sie die örtlichen Strafverfolgungsbehörden.**
- ☐ **Leisten Sie Schadensbegrenzung.**
- ☐ **Analysieren Sie die Gründe für den Erfolg des Angriffs.**
- ☐ **Passen Sie Ihre Schulungen an.**
- ☐ **Bewerten Sie Ihre Sicherheitslage neu und überprüfen Sie, ob Ihre Sicherheitstools folgende Vorteile bieten:**
  - ☐ Erkennung und Klassifizierung von BEC-E-Mails am Gateway
  - ☐ Bereitstellung proaktiver Authentifizierung oder von richtlinienbasiertem Schutz
  - ☐ Verwendung von SPF, DKIM und DMARC

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) ist ein Cybersicherheitsunternehmen der nächsten Generation, das Unternehmen dabei unterstützt, die Arbeitsabläufe ihrer Mitarbeiter vor hochentwickelten Bedrohungen und Compliance-Risiken zu schützen. Dank Proofpoint können Cybersicherheitsexperten ihre Benutzer vor raffinierten und zielgerichteten Angriffen (per E-Mail, Mobilgeräte-Apps und Social Media) schützen, wichtige Informationen absichern und ihre Sicherheitsteams mit den notwendigen Bedrohungsdaten sowie Tools ausstatten, um bei Zwischenfällen schnell zu reagieren. Führende Unternehmen aller Größen, darunter mehr als 50 Prozent der Fortune 100, nutzen Proofpoint-Lösungen. Diese wurden für moderne IT-Umgebungen mit Mobilgeräten und Social Media konzipiert und nutzen die Möglichkeiten der Cloud sowie eine Big-Data-Analyseplattform zur Abwehr aktueller raffinierter Bedrohungen.

proofpoint. proofpoint.com/de