proofpoint®

GUIDE DE

SURVIE FACE AU PIRATAGE DE LA MESSAGERIE EN ENTREPRISE

(BEC)

Gestion du piratage de la messagerie en entreprise et de l'usurpation d'identité pour une entreprise mieux protégée

SOMMAIRE

RÉSUMÉ

Le piratage de la messagerie en entreprise (BEC, Business Email Compromise) est une attaque simple mais qui, pourtant, déconcerte de nombreuses entreprises dans le monde, même celles à l'avant-garde de leur secteur.

Depuis que le FBI a commencé à surveiller ces attaques en 2015, plus de 22 000 entreprises en ont été victimes un peu partout dans le monde, avec des pertes estimées à 3,08 milliards de dollars[1].

À la différence d'autres cyberattaques, les e-mails d'attaque BEC ne contiennent pas de malwares ni d'URL malveillantes. Ils s'appuient plutôt sur l'ingénierie sociale pour tromper les utilisateurs.

Ces attaques ciblent les utilisateurs de l'entreprise, en particulier le directeur financier ou les employés du service des ressources humaines, financier ou de gestion des salaires. Grâce à la technique dite d'usurpation d'identité, ces menaces incitent le personnel à croire qu'il a reçu un e-mail d'un supérieur, d'un collègue, d'un fournisseur ou d'un partenaire. L'imposteur demande des virements bancaires, des dossiers fiscaux ou d'autres données sensibles.

Ces attaques sont généralement couronnées de succès car leurs auteurs créent des e-mails qui ressemblent à s'y méprendre à des messages légitimes. Ils demandent en outre aux victimes d'effectuer des tâches qui rentrent dans le cadre de leurs fonctions.

C'est cette simplicité même qui permet à ces messages d'échapper à la vigilance des solutions de sécurité traditionnelles, conçues pour détecter des attaques exploitant les technologies.

Comment protéger votre entreprise

Heureusement, il est possible de bloquer les attaques BEC en combinant le facteur humain, les processus et la technologie.

Avant une attaque

Vous pouvez éviter de telles attaques grâce à une action sur trois fronts :

- Sensibilisation du personnel aux attaques BEC
- Procédures et règles pour les processus métier réalisés par e-mail
- Protection contre les menaces avancées qui bloque les attaques BEC avant qu'elles n'atteignent les boîtes de réception du personnel. Cette protection doit également empêcher vos collaborateurs de divulguer des informations sensibles dans le cas où ils se laisseraient piéger et communiqueraient avec les auteurs de l'attaque BEC.

Une solution efficace combine deux fonctionnalités puissantes. Elle détecte et bloque les attaques BEC au niveau de votre passerelle de messagerie. Et elle authentifie les e-mails de votre entreprise au niveau des passerelles de vos partenaires et des opérateurs de messagerie utilisés par vos clients.

Pour ce faire, vous devez utiliser les méthodes d'authentification SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) et DMARC (Domain-based Message Authentication, Reporting & Conformance). En outre, il peut être utile d'implémenter des contrôles de prévention des pertes de données (DLP) au niveau de votre passerelle de messagerie. Ceux-ci permettront de protéger les informations sensibles auxquelles les auteurs d'attaques BEC sont susceptibles de s'intéresser.

[1] FBI, « *Business E-Mail Compromise: The 3.1 Billion Dollar Scam* » (Piratage de la messagerie en entreprise : escroquerie à 3,1 milliards de dollars), juin 2016

Après une attaque

Les cybercriminels inventent constamment de nouveaux stratagèmes pour tromper vos collaborateurs, contourner vos solutions de protection et en tirer un profit financier.

Si une demande de fonds fallacieuse aboutit, la première étape du processus de restauration consiste à contacter votre banque. Demandez-lui de prendre contact avec la banque à laquelle le virement a été envoyé. Ensuite, signalez l'attaque aux autorités policières locales.

Il se peut également que vous deviez informer votre compagnie d'assurances et vos actionnaires de l'incident. Si des informations sensibles sont tombées entre les mains de cybercriminels, vous devez limiter les dégâts.

Il est tout aussi important de déterminer les raisons pour lesquelles l'attaque a pu réussir. Quelle qu'en soit la cause, actualisez vos formations pour informer votre personnel des menaces actuelles, lui expliquer le mode opératoire de l'attaque et lui présenter les nouvelles solutions disponibles.

Même si les attaques BEC n'utilisent pas de malwares, une attaque réussie peut mettre en lumière des failles ou des vulnérabilités de vos cyberdéfenses. Envisagez d'effectuer une évaluation des menaces pour identifier les risques cachés et déterminer votre degré de préparation pour contrer les futures menaces.

Les clés d'une défense efficace

Les attaques BEC représentent une menace grandissante pour les entreprises car elles exploitent une vulnérabilité contre laquelle les correctifs ne peuvent rien faire : le facteur humain. C'est pourquoi la formation du personnel, la mise en place de contrôles financiers et la technologie constituent les clés d'une défense robuste et d'une réponse efficace.

Vous avez besoin d'une solution qui ne s'appuie pas uniquement sur la réputation et une configuration élémentaire de la messagerie. Grâce à des contrôles granulaires, les solutions avancées de protection de la messagerie peuvent identifier et mettre en quarantaine les e-mails d'imposture avant qu'ils n'atteignent les boîtes de réception de vos collaborateurs.

INTRODUCTION

UN PROBLÈME DE PLUS EN PLUS PRÉOCCUPANT

Tomber dans le piège tendu par un imposteur est plus facile qu'il n'y paraît. Imaginez le scénario suivant : vous travaillez pour une importante société qui a récemment procédé à plusieurs acquisitions. Votre travail consiste à régler les factures. Un matin, vous recevez un message de votre PDG actuellement en déplacement. Il vous demande de virer des fonds afin de pouvoir entamer les négociations de rachat d'une nouvelle entreprise et vous exhorte de garder l'information pour vous jusqu'à la conclusion de l'accord.

Il n'est pas rare que votre PDG vous envoie des e-mails pour vous demander de virer des fonds. Par ailleurs, il est tout aussi logique qu'il vous demande de ne pas ébruiter l'affaire.

Autre cas de figure : votre société possède un fournisseur étranger. Vous avez entendu dire que ce dernier restructurait quelque peu ses activités. Le fournisseur vous envoie un message vous informant qu'il change de banque. L'e-mail vous demande d'envoyer tous les paiements à venir à la nouvelle banque et fournit les coordonnées bancaires.

Le nom du fournisseur est réel, tout comme le nom de l'expéditeur et de la banque.

Mais dans les deux cas (tirés de l'actualité), le message est bel et bien une arnaque. Il s'agit là d'exemples de piratage de messagerie en entreprise, des attaques qui ont touché plus de 22 000 entreprises à travers le monde et auraient coûté la bagatelle de 3,08 milliards de dollars aux entreprises depuis janvier 2015, date à laquelle le FBI a commencé à surveiller ce type d'attaques[2].

Les attaques BEC utilisent des e-mails pour inciter les individus à virer des fonds ou à communiquer des informations d'entreprise sensibles (données personnelles des employés, par exemple).

Lorsqu'elles proviennent de la personne escomptée, les demandes de virement bancaire ou d'informations personnelles d'employés peuvent être légitimes. Nombre de sociétés à travers le monde en reçoivent chaque jour. C'est ainsi que les entreprises opèrent de nos jours. Tout le problème consiste à pouvoir distinguer les e-mails légitimes des arnaques élaborées par un imposteur. Il faut savoir qu'une usurpation d'identité peut coûter cher.

Heureusement, il est possible d'éviter de telles attaques. Considérez ce guide comme un point de départ. Vous y découvrirez les facteurs contribuant à la multiplication des attaques BEC, les mesures à prendre si vous êtes concerné et, le plus important, comment éviter de tomber dans le piège.

[2] FBI, « *Business E-Mail Compromise: The 3.1 Billion Dollar Scam* » (Piratage de la messagerie en entreprise : escroquerie à 3,1 milliards de dollars), juin 2016

PRINCIPES DU PIRATAGE DE LA MESSAGERIE EN ENTREPRISE : CIBLES ET TACTIQUES

Votre personnel constitue votre atout le plus précieux. Mais lorsqu'il s'agit de cybersécurité, il peut aussi devenir votre « maillon faible ». Il est vulnérable aux attaques qui exploitent la nature humaine plutôt que de se limiter aux failles techniques.

Les cybercriminels mènent des recherches poussées sur leurs victimes afin de savoir qui cibler au sein de l'entreprise. Ils étudient l'organisation interne et visitent fréquemment votre site Web. Ils consultent les réseaux sociaux tels que LinkedIn pour en savoir plus sur vos collaborateurs, leur poste, leurs précédentes fonctions, leurs collègues et leurs centres d'intérêt.

CIBLES

Si les cybercriminels en veulent à votre argent, ils se renseigneront sur le personnel du département financier. Près de 47 % des e-mails d'imposture ciblent les directeurs financiers[3]. S'ils cherchent à voler des informations d'entreprise sensibles ou les dossiers du personnel, ils chercheront à tout savoir des employés travaillant pour les ressources humaines. Près de 25 % des attaques visent le département des ressources humaines[4].

Ils se concentrent sur les nouvelles recrues, moins au fait des règles et procédures de votre entreprise. Ils se renseignent sur les déplacements des dirigeants et leur destination ainsi que sur les heures et jours de grande activité dans l'entreprise. Tout cela dans le but de donner aux messages usurpés une apparence aussi légitime et authentique que possible et profiter de l'opportunité qui leur est donnée.

TACTIQUES

Les attaques BEC ciblent des individus. Elles sont conçues pour inciter vos collaborateurs à croire qu'ils ont reçu un e-mail d'un dirigeant de votre entreprise (le PDG, par exemple) ou encore d'un fournisseur, d'un partenaire ou d'un collègue. L'expéditeur du message d'usurpation d'identité demande une action de la part du destinataire, par exemple un virement bancaire ou l'envoi de dossiers fiscaux ou d'autres données personnelles ou sensibles de l'entreprise.

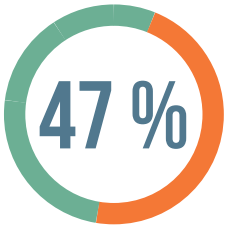
De prime abord, l'e-mail semble tout à fait normal. Toutefois, de légères différences, par exemple dans le nom de l'expéditeur, son adresse ou l'adresse de réponse, peuvent être des indices révélateurs d'une tentative d'arnaque. Les cybercriminels misent sur le fait que la cible ne prendra pas le temps de vérifier le message.

[3 et 4] Étude Proofpoint, mars 2016

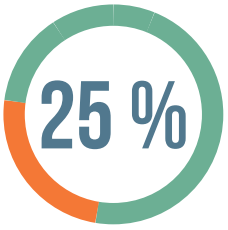
PERSONNES VISÉES

Vous trouverez ci-après une répartition statistique des employés et des départements visés par les attaques BEC.

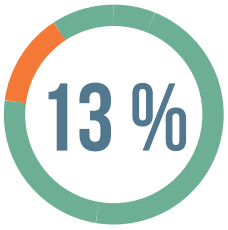
Directeur opérationnel



Directeur financier



Ressources humaines



Service financier

Gestion des salaires

Source : Proofpoint

LES MULTIPLES FORMES DU PIRATAGE DE LA MESSAGERIE EN ENTREPRISE

Voici les quatre formes les plus courantes d'attaques BEC :

75 %

Usurpation du nom

Cette variante représente 75 % des attaques. Elle utilise le nom du dirigeant dont l'identité a été usurpée dans le champ « De ». Mais l'adresse e-mail provient en réalité d'un compte de service externe (Gmail, par exemple) qui appartient au cyberpirate.

21 %

Usurpation de l'adresse de réponse

Cette technique utilise les véritables nom et adresse e-mail de l'expéditeur dont l'identité a été usurpée (généralement le PDG). Le nom de réponse utilise également le nom de l'expéditeur en question. Cependant, l'adresse de réponse (Reply-To), à laquelle seront envoyées les réponses au message, est celle de l'auteur de l'attaque.

2 %

Usurpation de l'expéditeur (sans adresse de réponse)

Cette forme de message BEC utilise le nom et l'adresse e-mail du dirigeant dont l'identité a été usurpée. Par contre, l'e-mail ne contient pas d'adresse de réponse. Par conséquent, tout dialogue entre les parties est impossible. L'e-mail comprend souvent des instructions de virement bancaire afin d'éviter tout échange ultérieur.

2 %

Usurpation basée sur la ressemblance du nom de domaine

Dans ce type d'attaque BEC, l'adresse d'expédition de l'attaquant ressemble à l'adresse du dirigeant dont l'identité a été usurpée. Le domaine « similaire » peut être identique à une lettre près au nom légitime : « entreprise**authentque**.com » au lieu de « entreprise**authentique**.com » par exemple.

Source : Proofpoint

RAISONS DE LA RÉUSSITE DES ATTAQUES BEC

Le modèle d'une attaque BEC ressemble beaucoup aux superproductions hollywoodiennes. La plupart des tentatives échouent lamentablement, mais celles qui réussissent peuvent rapporter gros.

Pour les cybercriminels, la différence entre la réussite et l'échec peut tenir à la qualité de leurs recherches sur l'entreprise, au ciblage des bonnes personnes et au moment de la remise des e-mails usurpés.

En plus d'imiter l'apparence d'un e-mail légitime, les cybercriminels ont recours à la manipulation psychologique. Ils misent sur l'empressement des employés à contenter leurs supérieurs, en invoquant l'urgence et la discrétion. Pour éviter d'éveiller les soupçons, les cyberpirates demandent aux victimes d'effectuer des tâches qui font partie de leur quotidien.

Les e-mails d'usurpation d'identité arrivent souvent lorsque les décideurs sont absents, pour éviter toute possibilité de vérification de l'authenticité du message. Ils peuvent également être envoyés lors de pics d'activité, à un moment où les victimes sont surchargées de travail et se soucient peu des menaces BEC.

Les e-mails BEC posent un véritable problème car, à la différence d'autres cyberattaques, ils ne contiennent pas de pièces jointes ou d'URL malveillantes. Les cyberpirates ont plutôt recours à l'ingénierie sociale pour ce type d'attaques. En d'autres termes, ces e-mails peuvent échapper aux solutions de sécurité traditionnelles qui se concentrent sur le contenu ou les comportements malveillants exploitant des vulnérabilités technologiques.

Pour les cybercriminels, les attaques BEC représentent une opportunité juteuse, présentant peu de risques. Qui plus est, elles ne nécessitent pas d'infrastructure coûteuse. Enfin, comme les attaques dépassent souvent les frontières, peu de cyberescrocs sont poursuivis en justice.

ATTAQUES BEC RÉCENTES

Voici quelques exemples d'attaques BEC documentées.

FACC AG (signalée en janvier 2016)

Les cybercriminels ont lancé une attaque BEC contre une société d'ingénierie autrichienne qui conçoit et fabrique des composants aéronautiques pour s'emparer au final de 55,7 millions de dollars. Le PDG et le directeur financier de la société ont été limogés à la suite de cette attaque.

Filiale de Crelan aux Pays-Bas

Crelan (signalée en janvier 2016)

Après un audit interne, la banque belge a découvert qu'elle avait perdu plus de 70 millions de dollars à cause d'e-mails d'usurpation d'identité.

TWoA (signalée en décembre 2015)

Une université néozélandaise a perdu plus de 100 000 dollars après que le directeur financier s'est laissé piéger par l'e-mail d'un imposteur qui réclamait un paiement.

Ubiquiti Networks, Inc. (signalée en août 2015)

Le fournisseur de produits réseau sans fil haut de gamme a payé près de 47 millions de dollars à un cyberpirate se faisant passer pour un fournisseur.

Luminant Corp. (signalée en 2013)

La société de distribution d'électricité texane a envoyé plus de 98 000 dollars en réponse à un e-mail comportant un nom de domaine frauduleux.

PROTECTION DE L'ENTREPRISE

Le point positif est qu'il est possible de bloquer les attaques BEC avant qu'elles n'arrivent à leurs fins. La meilleure défense consiste à associer le facteur humain, un processus adéquat et la technologie — les trois sont indispensables.

AVANT UNE ATTAQUE : PRÉPARATION ET PRÉVENTION

La formation peut aider vos employés à déceler les signes d'une imposture et à respecter les bonnes pratiques pour éviter de tomber dans le panneau. L'utilisation des règles et procédures appropriées peut aider votre personnel à traiter correctement les demandes envoyées par e-mail. Enfin, se doter des solutions technologiques adéquates est essentiel pour détecter et bloquer les attaques avant qu'elles n'atteignent vos employés.

Formation

Une formation de sensibilisation aux attaques BEC et à la cybersécurité en général peut aider votre entreprise à éviter les attaques ou à en limiter l'impact si jamais elles réussissaient. Plus le personnel est informé sur le sujet, plus l'entreprise a des chances d'y résister.

La formation doit couvrir le paysage des menaces, les dernières techniques d'ingénierie sociale et les moyens pour détecter les e-mails d'usurpation d'identité. Assurez-vous que le personnel est au courant des règles et procédures de fonctionnement habituelles concernant les demandes de fonds et de données sensibles émanant des dirigeants, des partenaires et des clients.

Si possible, pensez à présenter des exemples d'attaques BEC réelles dans le cadre de la formation afin de montrer le déroulement concret de telles attaques.

Processus

Basées sur les techniques d'ingénierie sociale, les attaques BEC sont conçues pour tromper les utilisateurs, et ont donc tout pour être crédibles. Même les employés les plus circonspects peuvent se laisser abuser par une arnaque bien conçue et exécutée. C'est pourquoi un processus clair et rigoureux de traitement et d'examen des demandes envoyées par e-mail peut constituer un contrôle essentiel contre les demandes frauduleuses.

Le FBI suggère de créer des règles pour marquer les adresses e-mail dont les extensions ressemblent à s'y méprendre au domaine de messagerie de votre entreprise. L'enregistrement de domaines qui varient légèrement du nom de domaine de votre entreprise peut empêcher les cybercriminels d'utiliser ces variantes pour tromper votre personnel[5].

Envisagez d'implémenter des contrôles internes qui comportent un processus de vérification en deux étapes (ou plus) pour le service financier et celui des achats. À titre d'exemple, le contrôle peut exiger l'autorisation de plusieurs personnes, des approbations écrites pour les montants importants et une confirmation par téléphone. Lorsque vous utilisez la confirmation par téléphone dans le cadre d'un processus de vérification en deux étapes, utilisez des numéros que vous connaissez, pas ceux indiqués dans l'e-mail de demande.

SEPT CONSEILS POUR TRAITER UN E-MAIL SUSPECT

CONSEIL N° 1 : NE VOUS FIEZ PAS AU NOM D'AFFICHAGE

Une tactique fort prisée des cybercriminels consiste à usurper le nom d'affichage d'un e-mail. Vérifiez toujours l'adresse e-mail dans l'en-tête « From ».

CONSEIL N° 2 : NE VOUS FIEZ PAS À L'EN-TÊTE DE L'ADRESSE E-MAIL

Les cybercriminels n'usurpent pas seulement le nom d'affichage des marques mais aussi l'en-tête de l'adresse e-mail, y compris le nom de domaine. Vérifiez que toutes les informations sont correctes. En cas de doute, vérifiez l'authenticité du message auprès de la personne qui l'a prétendument envoyé.

CONSEIL N° 3 : VÉRIFIEZ LES FAUTES D'ORTHOGRAPHE

En général, les messages légitimes ne comportent pas de fautes d'orthographe ou de grammaire majeures. Lisez attentivement vos e-mails et signalez tout ce qui vous semble suspect.

CONSEIL N° 4 : MÉFIEZ-VOUS LORSQUE DES DIRIGEANTS VOUS DEMANDENT DES INFORMATIONS INHABITUELLES

Combien de dirigeants d'entreprise souhaitent examiner les informations fiscales de leurs employés ? Arrive-t-il souvent à votre PDG d'avoir son compte bloqué et de vous demander l'accès à votre réseau ou un mot de passe ?

CONSEIL N° 5 : PRENEZ LE TEMPS DE RÉFLÉCHIR LORSQUE VOUS RECEVEZ DES DEMANDES URGENTES

Existe-t-il une bonne raison pour cette demande ? Invoquer l'urgence ou la discrétion, surtout sans passer par la voie habituelle, est une tactique courante dans les attaques BEC. Une fois encore, vérifiez l'authenticité du message auprès de la personne qui l'a prétendument envoyé.

CONSEIL N° 6 : EXAMINEZ LA SIGNATURE

Un manque de détails concernant le signataire ou l'absence de coordonnées de contact est un indice souvent révélateur d'une attaque BEC. Les entreprises légitimes fournissent tous les détails nécessaires.

CONSEIL N° 7 : NE CROYEZ PAS TOUT CE QUE VOUS VOYEZ

Les cybercriminels sont passés maîtres dans l'art de la tromperie. De nombreux e-mails incluent des logos de marque convaincants, un bon niveau de langue et une adresse e-mail valide. N'hésitez pas à remettre en question les messages qu'on vous envoie.

[5] FBI, « *Business E-Mail Compromise* » (Piratage de la messagerie en entreprise), août 2015
[6] FBI, « *Business E-Mail Compromise: The 3.1 Billion Dollar Scam* » (Piratage de la messagerie en entreprise : escroquerie à 3,1 milliards de dollars), juin 2016

Selon le FBI, certaines institutions financières reportent le traitement des demandes de virement international de clients pour avoir le temps de vérifier leur légitimité[6].

Technologie

Une solution technologique complète constitue le troisième pilier, et sans doute le plus important, d'une défense robuste contre les attaques BEC.

Votre solution doit prendre en charge des options de configuration avancées pour marquer les messages suspects sur la base d'attributs tels que l'adresse ou la ligne d'objet.

Elle doit également être en mesure de détecter et de classifier les menaces BEC au niveau de la passerelle de messagerie. Parmi les méthodes de détection éprouvées, citons la classification dynamique. Cette approche utilise des processus algorithmique et dynamique pour examiner la relation entre l'expéditeur et le destinataire, la réputation du domaine et d'autres attributs. Elle permet d'intercepter divers types d'attaques BEC, même lorsque ces dernières sont modifiées.

Une solution efficace inclut également une authentification proactive ou une sécurité basée sur des règles pour protéger votre personnel, vos partenaires, vos fournisseurs et vos clients. Comme les attaques BEC ciblent de plus en plus les partenaires et les fournisseurs au-delà de votre propre passerelle de messagerie, votre entreprise doit offrir un moyen de vérifier que les e-mails émanent bien d'elle et non d'un imposteur. Deux technologies d'authentification permettent d'identifier l'expéditeur d'un message : SPF (Sender Policy Framework) et DKIM (DomainKeys Identified Mail).

La norme SPF précise qui peut envoyer un e-mail pour le compte d'un domaine. Elle répertorie les adresses IP des expéditeurs autorisés dans un enregistrement DNS. Si l'adresse IP à l'origine du message n'est pas répertoriée dans l'enregistrement SPF, son authentification échoue.

Quant à la norme DKIM, elle permet de transmettre un message de sorte qu'il puisse être vérifié par l'opérateur de messagerie. Les e-mails peuvent être associés à une signature numérique émanant d'un domaine spécifié. La vérification repose sur l'authentification cryptographique de la signature numérique du message.

Un outil d'authentification plus récent, DMARC (Domain-based Message Authentication Reporting & Conformance), vient renforcer la protection offerte par SPF et DKIM. DMARC est un protocole de messagerie ouvert qui authentifie les expéditeurs légitimes et étend la sécurité aux partenaires et aux particuliers. L'authentification DMARC est activée sur 85 % des boîtes aux lettres de particuliers à travers le monde.

Chacune de ces technologies possède ses avantages et ses inconvénients, mais utilisées en association avec votre infrastructure de cybersécurité, elles permettent de bloquer un large éventail d'attaques BEC.

AVANTAGES DE DMARC

Une règle DMARC permet aux expéditeurs de préciser que leurs messages sont protégés par SPF, DKIM ou les deux. DMARC indique à un destinataire ce qu'il doit faire lorsqu'aucune des deux méthodes d'authentification n'aboutit, par exemple déplacer le message vers le dossier Courrier indésirable ou encore le rejeter.

DMARC OFFRE LES AVANTAGES SUIVANTS AUX EXPÉDITEURS :

- Visibilité sur la personne qui envoie le message en votre nom, les messages authentifiés, ceux qui ne le sont pas et les raisons à cela
- Indication aux destinataires de la mesure à prendre si l'authentification du message échoue
- Blocage des attaques usurpant les domaines avant qu'elles n'atteignent les boîtes de réception des employés et des particuliers

DMARC OFFRE LES AVANTAGES SUIVANTS AUX DESTINATAIRES :

- Possibilité de distinguer les expéditeurs légitimes et malveillants
- Renforcement de la fidélité des consommateurs et protection des employés
- Amélioration et protection de la réputation du canal e-mail

APRÈS L'ATTAQUE

Face aux attaques BEC, la meilleure stratégie consiste naturellement à les éviter. Malheureusement, les cybercriminels mettent constamment au point de nouveaux stratagèmes pour tromper vos collaborateurs, contourner vos solutions de protection et en tirer un profit financier.

À la différence d'autres cybermenaces, les attaques BEC n'utilisent pas de malwares et ne s'implantent pas dans votre système. Il n'y a donc rien à éliminer. Cependant, les dommages financiers peuvent être conséquents.

Si le cyberpirate a subtilisé de l'argent, les entreprises tentent souvent de le récupérer dans les plus brefs délais. Malheureusement, leurs efforts sont souvent vains. Dans le cas d'Ubiquiti (voir page 14), la société n'a pu récupérer qu'une petite partie des près de 47 millions de dollars volés[7].

Parmi les autres mesures à prendre immédiatement, citons la documentation et le signalement de l'attaque, quel que soit le montant des pertes ou le moment où elle est intervenue. Si l'attaque est récente, le FBI conseille aux entreprises de contacter l'un de ses bureaux locaux. L'agence collabore avec le FinCEN (Financial Crimes Enforcement Network), un département du ministère américain du Trésor, pour tenter de restituer ou de geler les fonds.

Lorsque vous signalez une attaque BEC, l'agence recommande d'inclure les informations suivantes pour faciliter le recouvrement éventuel :

- Nom de l'expéditeur, localisation géographique, nom de la banque et numéro de compte bancaire
- Nom du destinataire, nom de la banque, numéro de compte, localisation géographique (le cas échéant) et nom de la banque intermédiaire (le cas échéant)
- Numéro SWIFT, date, montant de la transaction et toute autre information complémentaire, par exemple un compte FFC (For Further Credit)

Le cas échéant, vous devez également avertir votre compagnie d'assurance et vos actionnaires et prendre les mesures qui s'imposent pour limiter les dommages. Par exemple, en cas de communication d'informations sensibles, vous devez limiter les risques d'une utilisation abusive. En cas de vol de données fiscales, envisagez d'offrir aux employés concernés une protection contre le vol d'identité.

Il est tout aussi important de déterminer les raisons pour lesquelles l'attaque a pu réussir. Vos outils de cybersécurité actuels sont-ils capables de vous protéger contre les attaques BEC et d'autres menaces ? Votre environnement comporte-t-il des failles ? Une évaluation des menaces peut permettre d'identifier les risques cachés.

Quelle qu'en soit la cause, il est toujours intéressant d'actualiser vos formations pour informer votre personnel des menaces actuelles, lui expliquer le mode opératoire de l'attaque et lui présenter les nouvelles solutions disponibles.

Signalement d'une attaque BEC

De nombreux pays possèdent des organismes en charge des fraudes informatiques, y compris les attaques BEC. En voici quelques-uns :

- États-Unis – Service IC3 (Internet Crime Complaint Center) du FBI (www.IC3.gov)
- Canada – Centre Antifraude du Canada (Canadian Anti-Fraud Centre) (www.antifraudcentre.ca)
- Royaume-Uni – Action Fraud (www.actionfraud.police.uk)
- Australie – ACORN (Australian Cybercrime Online Reporting Network) (www.acorn.gov.au)
- Singapour – Singapore Computer Emergency Response Team (SingCERT) (www.csa.gov.sg/singcert)
- Pays-Bas – Fraud Helpdesk (www.fraudhelpdesk.org)
- Allemagne – BKA (police fédérale judiciaire allemande) (www.bka.de)

[7] Krebs on Security, « *Tech Firm Ubiquiti Suffers $46M Cyberheist* » (Un cyberhold-up à 46 millions de dollars pour la société technologique Ubiquiti), août 2015.

CONCLUSION ET RECOMMANDATIONS

Les attaques BEC représentent une menace grandissante pour les entreprises car elles exploitent une vulnérabilité contre laquelle les correctifs ne peuvent rien faire : le facteur humain. C'est pourquoi la formation du personnel, les contrôles financiers et surtout la technologie constituent les clés d'une défense robuste et d'une réponse efficace.

Vous avez besoin d'une solution qui ne s'appuie pas uniquement sur la réputation et un filtrage élémentaire de la messagerie. Grâce à des contrôles granulaires, les solutions avancées de sécurisation de la messagerie peuvent identifier et mettre en quarantaine les e-mails d'imposture avant qu'ils n'atteignent les boîtes de réception de vos collaborateurs.

Pour en savoir plus sur le piratage de la messagerie en entreprise et découvrir comment Proofpoint peut vous aider à protéger votre entreprise, visitez notre site à l'adresse : www.proofpoint.com/fr.

LISTE DE CONTRÔLE POUR SURVIVRE À UN PIRATAGE DE LA MESSAGERIE EN ENTREPRISE

Voici une petite liste de contrôle qui vous aidera à déterminer si vous êtes prêt à bloquer et gérer les attaques BEC et les imposteurs.

Avant une attaque : prévention

- ☐ **Sensibilisation du personnel à la sécurité**
  - ☐ Paysage des menaces
  - ☐ Dernières techniques d'ingénierie sociale
  - ☐ Identification des e-mails d'usurpation d'identité
  - ☐ Habitudes des dirigeants, des partenaires et des clients en matière de demandes
- ☐ **Mise au point d'un processus clair et rigoureux pour le traitement et l'examen des e-mails**
  - ☐ Règles pour marquer les adresses e-mail dotées d'extensions qui ressemblent à s'y méprendre à vos adresses e-mail d'entreprise
  - ☐ Enregistrement des domaines de nom similaire avant que les cybercriminels ne le fassent
  - ☐ Contrôles internes comportant un processus de vérification en deux étapes (ou plus) pour le service financier et celui des achats
    - ☐ Recours à plusieurs personnes pour l'approbation
    - ☐ Approbations écrites pour les montants importants
    - ☐ Confirmation par téléphone
    - ☐ Traitement reporté pour vérifier la légitimité de la demande
- ☐ **Implémentation d'une solution technologique complète**
  - ☐ Options de configuration avancées pour marquer les messages suspects en fonction de différents attributs
  - ☐ Détection et classification des menaces BEC au niveau de la passerelle de messagerie
  - ☐ Authentification proactive ou protection basée sur des règles pour vos employés, partenaires, fournisseurs et clients — SPF, DKIM et DMARC

Après l'attaque : rétablissement et reprise des activités

- ☐ **Contacter votre institution financière**
- ☐ **Lui demander de contacter l'établissement financier qui a reçu le virement**
- ☐ **Contacter la police locale**
- ☐ **Limiter les dommages**
- ☐ **Déterminer les raisons du succès de l'attaque**
- ☐ **Actualiser les formations**
- ☐ **Réévaluer votre niveau de sécurité – Évaluation de vos outils de protection de la messagerie**
  - ☐ Détectent-ils et classifient-ils les e-mails BEC au niveau de la passerelle ?
  - ☐ Offrent-ils une authentification proactive ou une protection basée sur des règles ?
  - ☐ Utilisent-ils SPF, DKIM et DMARC ?

À PROPOS DE PROOFPOINT

Proofpoint, Inc. (NASDAQ : PFPT), société spécialisée dans les solutions de cybersécurité de nouvelle génération, permet aux entreprises de barrer la route aux menaces avancées de façon à garantir à leur personnel un environnement de travail sûr, tout en écartant les risques de non-conformité. Grâce à Proofpoint, les responsables de la cybersécurité peuvent protéger leurs utilisateurs contre les attaques avancées (qu'elles utilisent comme vecteur la messagerie électronique, les applications mobiles ou les médias sociaux) et sécuriser les informations critiques créées au sein de l'entreprise. De plus, leurs équipes disposent des outils et renseignements adéquats pour réagir rapidement en cas d'incident. Des entreprises de renom et de toutes tailles, dont plus de la moitié de celles figurant au classement Fortune 100, ont adopté les solutions Proofpoint. Ces dernières sont conçues pour les environnements informatiques d'aujourd'hui, tournés vers les applications mobiles et les médias sociaux, et s'appuient sur de puissantes technologies cloud ainsi que sur une plate-forme analytique orientée Big Data pour lutter contre les menaces sophistiquées, même les plus récentes.

proofpoint. proofpoint.com/fr