proofpoint.

EBOOK

2022

Guide stratégique pour une cybersécurité email optimale

Une approche centrée sur les personnes pour neutraliser les ransomwares, les malwares, le phishing et les fraudes par email

proofpoint.com/fr

L'email, le vecteur de menaces le plus critique

Chaque jour, une bataille silencieuse fait rage dans les boîtes de réception des utilisateurs, l'email comptant parmi les outils professionnels les plus courants et essentiels.

La messagerie électronique est le principal vecteur de distribution de malwares et un terrain propice à toutes sortes de fraudes. C'est par ce biais que les cybercriminels sont les plus susceptibles d'atteindre leurs cibles. Ils incitent les utilisateurs à cliquer sur des liens malveillants, à révéler leurs identifiants, voire à se plier involontairement à leurs demandes (par exemple, en transférant des fonds ou des fichiers sensibles).

Il est facile de comprendre pourquoi les cybercriminels privilégient ce canal. La messagerie électronique repose sur une architecture vieille de plusieurs décennies qui n'a pas été conçue dans une optique de sécurité. Elle est universelle. Enfin, à la différence du matériel et de l'infrastructure informatique, les attaques par email exploitent une vulnérabilité contre laquelle les correctifs ne peuvent rien faire : le facteur humain.

La migration vers le cloud et le passage au télétravail font planer une menace encore plus redoutable.

Chaque année, les entreprises investissent des milliards dans des outils de sécurité conçus pour renforcer les défenses du périmètre réseau, détecter les intrusions et sécuriser les endpoints. Pourtant, le volume et le coût des ransomwares, du piratage de la messagerie en entreprise (BEC, Business Email Compromise), du phishing d'identifiants de connexion et des compromissions de données dues à des malwares n'ont jamais été aussi élevés[1].

En effet, les attaques d'aujourd'hui exploitent la nature humaine, pas seulement les technologies. Et la messagerie électronique est le moyen le plus simple d'atteindre les utilisateurs.

Voici les conclusions de récentes études :

14,8 millions $
Coût annuel moyen du phishing pour une grande entreprise, soit plus du triple de la moyenne de 2015[2]

86 %
des entreprises ont essuyé des attaques de phishing en masse en 2021[3]

77 %
des entreprises ont été visées par des attaques BEC en 2021[4]

78 %
des entreprises ont été victimes d'attaques de ransomwares par email en 2021[5]

85 %
des compromissions de données impliquent une intervention humaine[6]

1 Ponemon Institute, « The 2021 Cost of Phishing Study » (Étude 2021 sur le coût du phishing), juin 2021.
2 Ponemon Institute, « The 2021 Cost of Phishing Study » (Étude 2021 sur le coût du phishing), juin 2021.
3 Proofpoint, « State of the Phish 2022 », février 2022.
4 Ibid.
5 Ibid.
6 Verizon, « Data Breach Investigations Report Executive Summary » (Résumé du rapport d'enquête sur les compromissions de données), mai 2021.

Il est temps de repenser l'approche existante. Le paysage actuel des menaces exige un changement des mentalités et une nouvelle stratégie axée sur la protection des utilisateurs plutôt que des infrastructures.

Que vous dirigiez un centre d'opérations de sécurité multinational ou une petite équipe de sécurité soudée, ce guide constitue un bon point de départ. Au programme :

- Pourquoi la messagerie électronique doit être votre priorité n° 1 en matière de sécurité
- Pourquoi il est si difficile de la sécuriser
- En quoi une sécurité multicouche intégrée et centrée sur les personnes est plus efficace
- Comment optimiser vos opérations de protection de la messagerie afin de réaliser des économies et de rationaliser les mesures de réponse

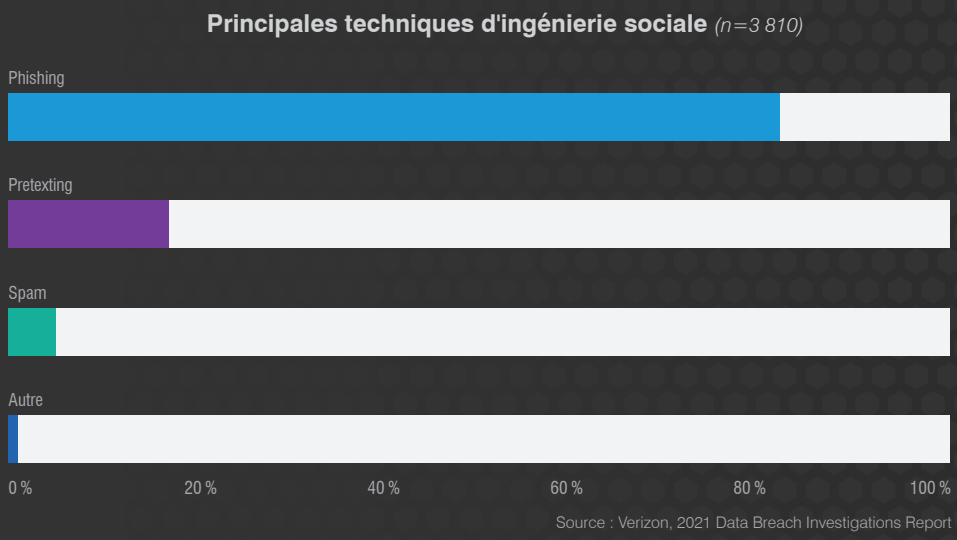


Figure 1. Principales formes d'ingénierie sociale

SECTION 1

Les cyberattaques ont une longueur d'avance sur les mécanismes de défense traditionnels

La protection de la messagerie électronique est essentielle pour préserver l'entreprise. Mais ce n'est pas une tâche aisée.

En effet, les menaces propagées par email sont nombreuses et variées. Les techniques d'attaque ne cessent d'évoluer. Et les utilisateurs, maillon faible de chaque entreprise, sont constamment pris pour cibles.

Il n'est dès lors pas étonnant que les solutions conçues il y a deux ou trois ans pour contrer les attaques ne fassent déjà plus le poids.

Cette section décrit certaines des méthodes employées par les cybercriminels pour cibler les utilisateurs. (Dans bien des cas, les cybercriminels combinent différentes techniques pour contourner les défenses et booster leur taux de réussite.)

Ransomwares

Le ransomware est une menace ancienne mais néanmoins toujours d'actualité. Ce type de malware, qui doit son nom aux rançons exigées par ses auteurs pour débloquer les fichiers de la victime, est un véritable fléau pour les entreprises modernes. C'est l'une des formes de cyberattaque les plus déstabilisantes.

Les incidents majeurs qui ont affecté en 2021 l'approvisionnement en carburant[7], l'alimentaire[8] et les soins de santé[9] aux États-Unis ont clairement montré qu'aucune cible n'est hors d'atteinte.

Environ trois quarts des attaques de ransomwares commencent, directement ou indirectement, par un email de phishing[10]. Ces emails incitent les utilisateurs à ouvrir une pièce jointe malveillante ou à cliquer sur une URL dangereuse.

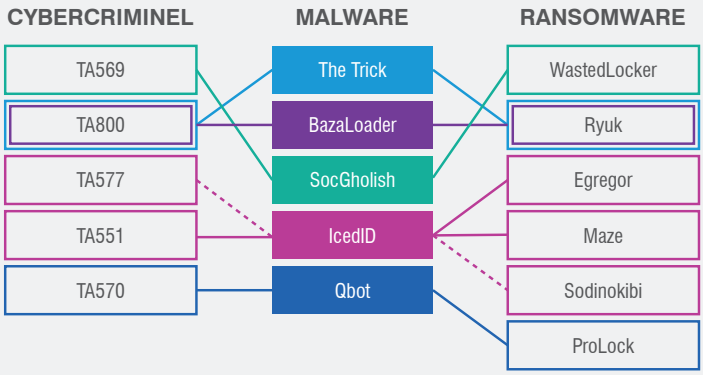


Figure 2. Liens entre les cybercriminels, les malwares initiaux et les ransomwares

La plupart des ransomwares sont distribués en tant qu'infection secondaire, après la compromission initiale d'un système par un chargeur ou un cheval de Troie. De nombreux cybercriminels spécialisés dans les chargeurs ou les chevaux de Troie vendent ensuite cet accès à des opérateurs de ransomwares. Pour la plupart des entreprises, la première ligne de défense contre les ransomwares consiste donc à se protéger contre d'autres types de malwares.

Il n'existe pas nécessairement de lien univoque entre le malware servant à l'accès initial et la souche de ransomware qui infecte ensuite les victimes. Cependant, les chercheurs de Proofpoint et du secteur de la cybersécurité en général ont mis en évidence certaines associations, comme le montre la figure 2.

7 David E. Sanger, Clifford Krauss, Nicole Perlroth (New York Times), « Cyberattack Forces a Shutdown of a Top U.S. Pipeline » (Une cyberattaque force la fermeture d'un important pipeline américain), mai 2021.
8 Julie Creswell, Nicole Perlroth, Noam Schreiber (New York Times), « Ransomware Disrupts Meat Plants in Latest Attack on Critical U.S. Business » (Un ransomware paralyse des usines de viande lors de la dernière attaque en date contre des entreprises américaines critiques), juin 2021.
9 Nicole Perlroth, Adam Satariano (New York Times), « Irish Hospitals Are Latest to Be Hit by Ransomware Attacks » (Des hôpitaux irlandais parmi les dernières victimes d'attaques de ransomwares), mai 2021.
10 Unit 42, Palo Alto Networks, « Ransomware Families: 2021 Data to Supplement the Unit 42 Ransomware Threat Report » (Familles de ransomwares : données 2021 en complément du rapport sur les ransomwares de Unit 42), juillet 2021.

Fraude par email et piratage de la messagerie en entreprise (BEC)

Le piratage de la messagerie en entreprise (BEC, Business Email Compromise), également appelé fraude par email, représente l'une des menaces les plus coûteuses et les moins bien comprises du domaine de la cybersécurité. Cette catégorie de fraude par email en plein essor ne bénéficie pas toujours d'autant d'attention que d'autres types d'attaques cybercriminelles très médiatisés. Cependant, en termes de coût financier direct, elle éclipse facilement ces autres types.

Pour la seule année 2020, les attaques BEC ont coûté plus d'1,8 milliard de dollars aux entreprises et aux particuliers[11]. Cela représente une augmentation de plus de 100 millions de dollars par rapport à 2019, et 44 % des pertes totales liées à la cybercriminalité.

Les attaques BEC sont difficiles à détecter. Elles ne contiennent pas les charges virales que nous avons l'habitude d'analyser, à savoir des URL ou des pièces jointes malveillantes. Les fraudeurs s'appuient plutôt sur l'usurpation d'identité et d'autres techniques d'ingénierie sociale pour piéger les utilisateurs.

Bon nombre des attaques BEC actuelles sont très sophistiquées, bien financées et soutenues par une planification et des recherches minutieuses. De plus en plus de cybercriminels concentrent leurs efforts sur la fraude aux factures fournisseurs et les importantes transactions B2B qu'ils peuvent pirater.

Les attaques BEC exploitent les faiblesses de la nature humaine. Elles abusent de la confiance des victimes.

Leur mode opératoire est le suivant :

1. Dans un premier temps, les cybercriminels spécialisés dans les attaques BEC se font passer pour une personne ou une entité en qui les destinataires peuvent avoir confiance, comme un collègue, un supérieur ou un fournisseur.
2. Le cybercriminel envoie un email incitant les destinataires à effectuer une action visant à extorquer de l'argent ou des informations financières sensibles à l'entreprise : virements bancaires frauduleux, fausses factures, détournement de salaires, modification des informations bancaires pour les paiements à venir, et bien d'autres techniques encore.
3. Au moment où l'entreprise se rend compte de l'erreur commise, il est souvent trop tard pour récupérer l'argent.

TYPES D'ATTAQUES BEC

Les attaques BEC peuvent prendre de nombreuses formes. La seule limite est la créativité des cybercriminels. En voici six types courants :

1. **Fraude aux factures.** Les cybercriminels incitent les victimes à payer de fausses factures ou à détourner des paiements légitimes.
2. **Détournement de salaires.** Les cyberescrocs se faisant passer pour un membre du personnel demandent au département de paie de rediriger les salaires vers leur compte.
3. **Extorsion.** Les cybercriminels menacent de porter atteinte à la victime si elle ne paie pas.
4. **Leurres et tâches.** Les cyberescrocs piègent les victimes avec une question simple telle que « Est-ce que vous êtes là ? » avant d'exécuter d'autres types d'attaques BEC.
5. **Escroquerie aux cartes cadeaux.** Les cybercriminels incitent les destinataires à acheter des cartes cadeaux et à leur envoyer le numéro et le code PIN.
6. **Fraude aux avances.** Les cyberescrocs demandent de l'argent aux victimes pour débloquer une somme encore plus importante, qui ne sera jamais versée.

11 FBI, « Internet Crime Report 2020 » (Rapport 2020 sur la cybercriminalité), mars 2021.

Compromission et prise de contrôle de comptes

La compromission de comptes consiste à prendre le contrôle du compte d'un service cloud ou de messagerie d'un utilisateur légitime afin d'accéder à un large éventail de données, contacts, événements de calendrier et emails.

Au-delà des données de l'utilisateur compromis, le cybercriminel peut se servir du compte pour usurper l'identité de l'utilisateur dans le cadre d'attaques d'ingénierie sociale, que ce soit à l'intérieur ou à l'extérieur de l'entreprise (attaques BEC, attaques de la chaîne logistique, etc.).

Les cybercriminels peuvent accéder à des données sensibles, convaincre des utilisateurs ou des partenaires commerciaux externes de transférer de l'argent, ou mettre à mal la réputation et les finances d'une entreprise. Pire encore, ils peuvent également installer des portes dérobées afin de conserver un accès pour de futures attaques.

Anatomie d'une prise de contrôle de comptes

Voici comment se déroulent la plupart des prises de contrôle de comptes cloud.

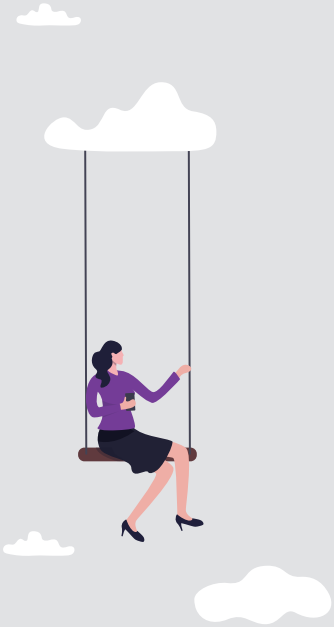
Vol d'identifiants de connexion. Le cybercriminel met la main sur les identifiants de connexion de l'utilisateur grâce au phishing d'identifiants de connexion (qui représente à lui seul environ deux tiers de l'ensemble des attaques de phishing), à des attaques par force brute, au recyclage d'identifiants de connexion (« credential stuffing ») ou à des malwares voleurs d'identifiants de connexion.

Infiltration. Une fois connecté au compte de l'utilisateur, le cybercriminel a accès aux emails, aux contacts, au calendrier et aux fichiers de la victime. Il peut alors dérober directement ces données ou s'en servir pour usurper l'identité de l'utilisateur de manière convaincante. Certains fraudeurs répondent à des fils de discussion existants ou envoient des emails contenant des malwares ou des URL dangereuses à des collègues et à des partenaires commerciaux externes. En se faisant passer pour les utilisateurs compromis, le cybercriminel peut cibler d'autres personnes à l'intérieur comme à l'extérieur de l'entreprise en leur envoyant des factures factices ou des instructions de détournement de paiements. Il peut également charger des malwares dans des partages de fichiers d'entreprise ou saboter l'entreprise par d'autres moyens.

Persistance. Bien souvent, le cybercriminel configure furtivement des règles de transfert automatique lui permettant d'accéder aux emails de l'utilisateur même si celui-ci modifie son mot de passe. En ayant accès à tous les emails et à toutes les invitations de calendrier de l'utilisateur, le cybercriminel obtient des informations essentielles dont il pourra tirer parti lors de futures attaques.

SECTION 2

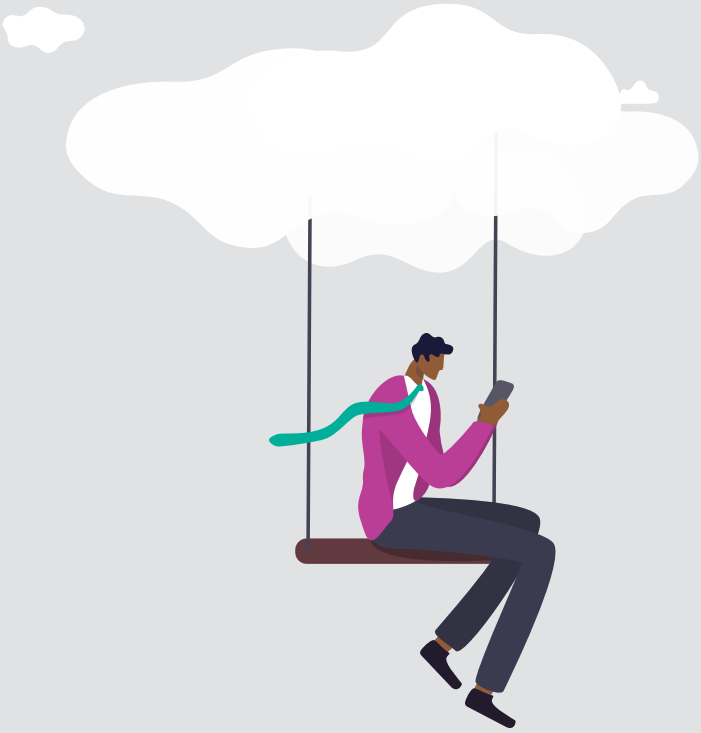
L'évolution du paysage des menaces

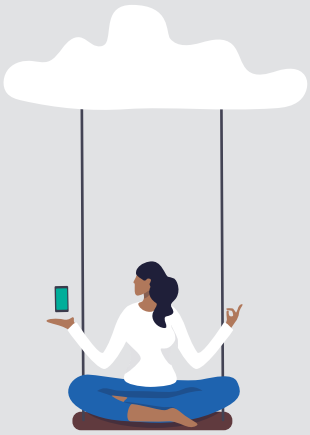


Les modèles de travail à distance et hybrides aujourd'hui adoptés par de nombreuses entreprises sont dépendants du cloud et des technologies mobiles.

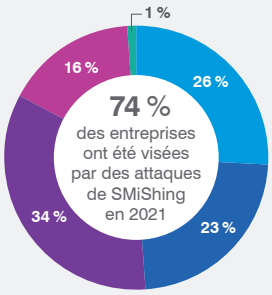
Les périmètres renforcés et les structures réseau traditionnelles appartiennent désormais au passé. Les collaborateurs constituent le nouveau périmètre de sécurité.

Malheureusement, la plupart des budgets de sécurité, qui doivent tenir compte d'autres priorités et catégories de produits, ne sont plus à la hauteur.

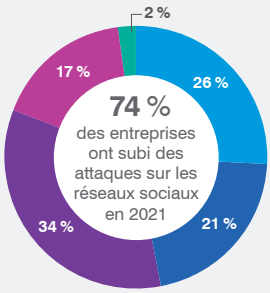




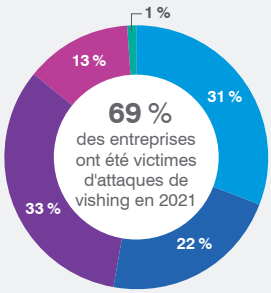
Volume des attaques de SMiShing



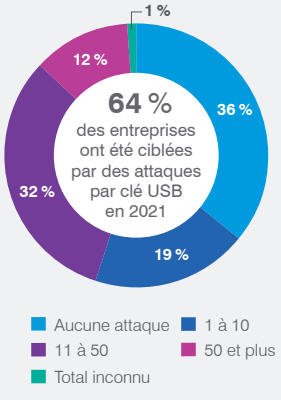
Volume des attaques sur les réseaux sociaux



Volume des attaques de vishing



Volume des attaques par clé USB



Source : State of the Phish 2022

Les attaques ciblent les individus, pas l'infrastructure

À l'heure où les entreprises dépensent des milliards chaque année pour consolider leur infrastructure, elles doivent prendre garde de ne pas négliger les risques de sécurité liés aux utilisateurs. En effet, les collaborateurs constituent le point d'entrée dans votre environnement le plus accessible et le plus lucratif.

Selon le rapport d'enquête de Verizon sur les compromissions de données, 85 % des compromissions impliquent une intervention humaine[12]. Vos utilisateurs sont confrontés à un déluge ininterrompu de liens dangereux, pièces jointes malveillantes, tentatives de vol d'identifiants de connexion, attaques d'ingénierie sociale et autres menaces d'imposteurs.

Les attaques couvrent généralement plusieurs vecteurs

Pour cibler des personnes, il faut interagir avec elles dans les outils et sur les plates-formes qu'elles utilisent. Les cybercriminels suivent les utilisateurs comme leur ombre.

Les workflows modernes sont dynamiques et imprévisibles. Un utilisateur peut commencer une conversation par email, planifier une réunion de suivi dans son application de chat et collaborer sur des fichiers stockés dans le cloud.

Les attaques modernes sont elles aussi dynamiques et imprévisibles. Elles s'exécutent sur plusieurs canaux, emploient une combinaison diverse de tactiques et d'outils, et exploitent toutes les plates-formes que les collaborateurs utilisent pour faire leur travail.

Une attaque peut commencer par un email contenant un lien qui redirige vers un malware hébergé sur un site de partage de fichiers. Mais elle peut aussi prendre la forme d'une application cloud non autorisée afin de dérober des identifiants de connexion pour compromettre un compte légitime et ensuite lancer des attaques BEC depuis celui-ci.

Cette menace ne cesse de grandir. Bien souvent, un cybercriminel sophistiqué crée le « produit » malware et configure l'infrastructure sous forme de package ou de service facile à utiliser. Les cybercriminels aux compétences moins pointues peuvent louer ce service afin de lancer leurs propres attaques, soit en payant pour l'utiliser pendant une période déterminée, soit en percevant une commission pour chaque compromission réussie. Dans d'autres cas, ils font office de distributeurs : ils envoient des emails contenant le malware et touchent une commission pour chaque infection fructueuse.

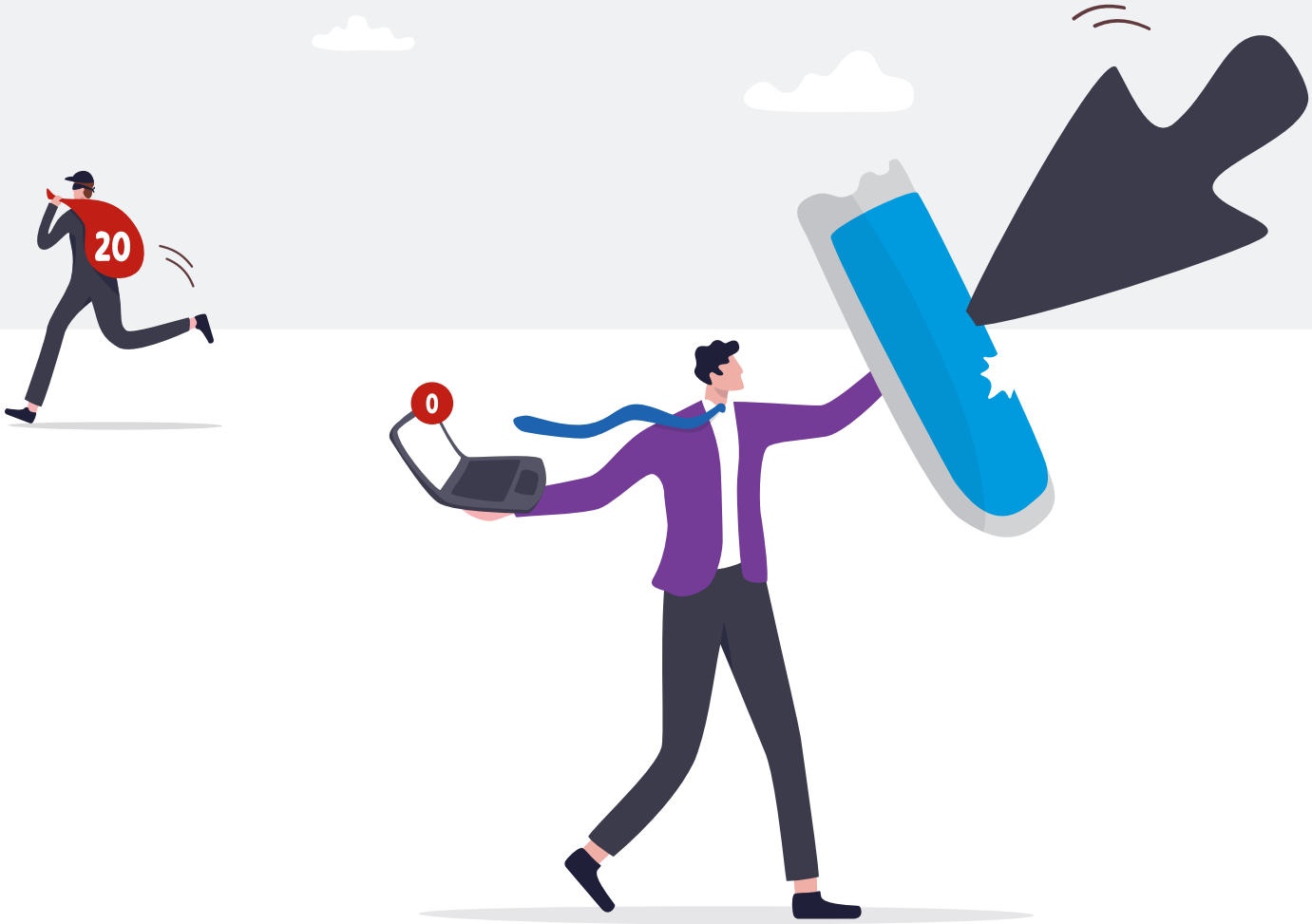
12 Verizon, « Data Breach Investigations Report Executive Summary » (Résumé du rapport d'enquête sur les compromissions de données), mai 2021.

Protéger chaque vecteur ne suffit pas

Les entreprises ont beau savoir que les menaces actuelles présentent de multiples facettes et ciblent avant tout les personnes, ainsi qu'investir dans des outils de sécurité pour couvrir tous les risques potentiels, si ces outils ne fonctionnent pas de manière coordonnée, ils ne peuvent pas offrir la visibilité et les informations dont les équipes de sécurité ont besoin pour gérer les risques.

Imaginez une équipe de stars du football qui ne s'entraînent pas ensemble, un orchestre de virtuoses qui n'entendent pas les autres instruments ou une équipe chirurgicale incapable de s'accorder sur le traitement des patients. Un individu, aussi compétent soit-il, ne sera jamais aussi efficace qu'un ensemble bien coordonné.

Aujourd'hui, les cybercriminels combinent différentes techniques pour lancer des attaques plus sophistiquées. Les outils isolés compliquent inutilement la tâche des équipes de sécurité, qui peinent déjà à gérer les risques actuels. C'est pourquoi une sécurité centrée sur les personnes exige une approche globale et coordonnée.

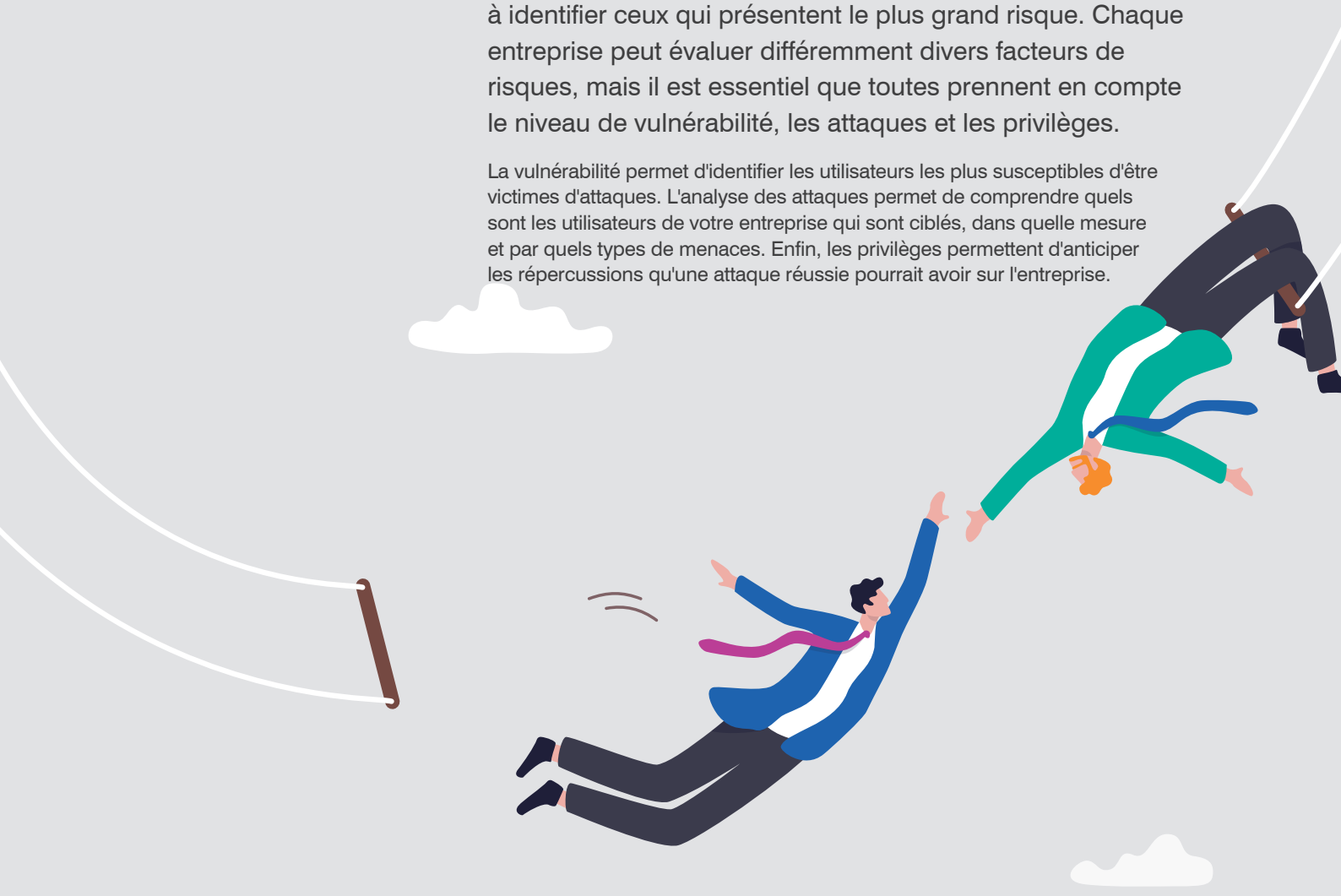


SECTION 3

Concentrez-vous sur les utilisateurs les plus à risque

La première étape pour protéger les utilisateurs consiste à identifier ceux qui présentent le plus grand risque. Chaque entreprise peut évaluer différemment divers facteurs de risques, mais il est essentiel que toutes prennent en compte le niveau de vulnérabilité, les attaques et les privilèges.

La vulnérabilité permet d'identifier les utilisateurs les plus susceptibles d'être victimes d'attaques. L'analyse des attaques permet de comprendre quels sont les utilisateurs de votre entreprise qui sont ciblés, dans quelle mesure et par quels types de menaces. Enfin, les privilèges permettent d'anticiper les répercussions qu'une attaque réussie pourrait avoir sur l'entreprise.



Concentrez-vous sur les utilisateurs qui présentent un risque plus élevé que la normale en vertu de ces facteurs associés. L'équipe de sécurité et les parties prenantes doivent leur accorder une attention prioritaire afin de comprendre pourquoi ils sont vulnérables.

Ce niveau de visibilité sur ces trois aspects constitue une composante essentielle de toute approche de sécurité centrée sur les personnes. Sans une telle visibilité, les entreprises n'auraient aucun moyen d'identifier les utilisateurs qui ont besoin de couches de sécurité supplémentaires ni de déterminer comment mieux les protéger.

Vulnérabilité : méthodes de travail et clics des utilisateurs

Il n'est pas facile d'évaluer le niveau de vulnérabilité des utilisateurs avec les outils de sécurité traditionnels qui protègent les technologies. Une approche centrée sur les personnes vous permet d'analyser les méthodes de travail et les clics des utilisateurs.

Ces méthodes de travail comprennent les outils, systèmes et plates-formes des utilisateurs pour exercer leurs fonctions. L'analyse de leurs clics permet d'évaluer leur niveau de sensibilisation à la sécurité et leur propension à se laisser duper.

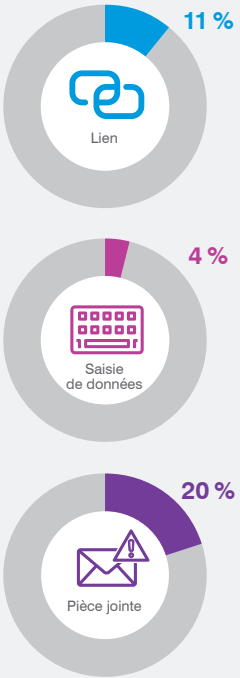
Méthodes de travail de vos collaborateurs

Vous pouvez vous faire une idée générale de la vulnérabilité des collaborateurs en évaluant les outils, les plates-formes et les applications qu'ils utilisent. Par exemple :

- Les applications cloud qu'ils utilisent et si celles-ci ont été validées par le département informatique
- Le nombre et le type d'appareils utilisés pour accéder à la messagerie électronique
- Le niveau de sécurité de ces appareils
- La mise en œuvre de bonnes pratiques numériques (mots de passe forts et uniques, maintien à jour des logiciels, etc.)
- L'utilisation systématique de l'authentification multifacteur pour accéder aux systèmes d'entreprise et même à leurs comptes personnels

Une visibilité granulaire est essentielle.

Types de modèles de phishing : taux d'échec moyens



Source : State of the Phish 2022

Les clics de vos collaborateurs

La vulnérabilité peut être évaluée plus précisément grâce à des formations à la sécurité informatique, à des simulations d'attaques de phishing et à l'analyse des réactions des collaborateurs face aux menaces réelles.

Composante essentielle de toute stratégie de sécurité efficace, une formation de sensibilisation à la sécurité informatique permet d'identifier les utilisateurs les moins bien préparés à reconnaître les cybermenaces et à donner l'alerte. En règle générale, les utilisateurs qui obtiennent de mauvais résultats aux exercices de formation, ou qui ne les ont pas effectués, sont plus vulnérables que leurs pairs mieux notés.

À moins de laisser le champ libre aux cybercriminels pour identifier les utilisateurs qui cliquent sur un lien, remplissent un formulaire ou ouvrent un fichier, les simulations d'attaques de phishing sont l'un des meilleurs moyens d'évaluer le niveau de vulnérabilité.

Enfin, il est primordial que vous assuriez le suivi des collaborateurs qui interagissent avec des emails malveillants connus, même en cas de blocage, d'isolation ou de réécriture du clic.

Ces données réelles, combinées aux informations de sensibilisation à la sécurité informatique, offrent une vue globale de la vulnérabilité de la messagerie grâce au suivi des formations achevées, des simulations d'attaques de phishing et des interactions avec des messages malveillants.

Attaques : stratégies déployées pour cibler les utilisateurs

Bien que toutes les cyberattaques soient potentiellement nuisibles, certaines sont plus dangereuses, ciblées ou sophistiquées que d'autres. C'est pourquoi l'évaluation de cet aspect des risques peut s'avérer plus difficile qu'il n'y paraît.

Les attaques « classiques » qui ratissent large sont probablement plus nombreuses que d'autres types de menaces. Toutefois, elles sont identifiables et plus facilement jugulées.

D'autres menaces n'apparaissent que dans quelques rares types d'attaques, mais représentent un danger plus grand en raison de leur sophistication ou des personnes ciblées.

Il est primordial de faire la différence entre ces deux profils de malware pour identifier les utilisateurs qui présentent un risque plus élevé. Proofpoint appelle ces utilisateurs des VAP (Very Attacked People™, ou personnes très attaquées). Une visibilité complète sur l'ensemble du trafic de messagerie et une threat intelligence riche sont essentielles pour déterminer quels utilisateurs sont ciblés et dans quelle mesure.

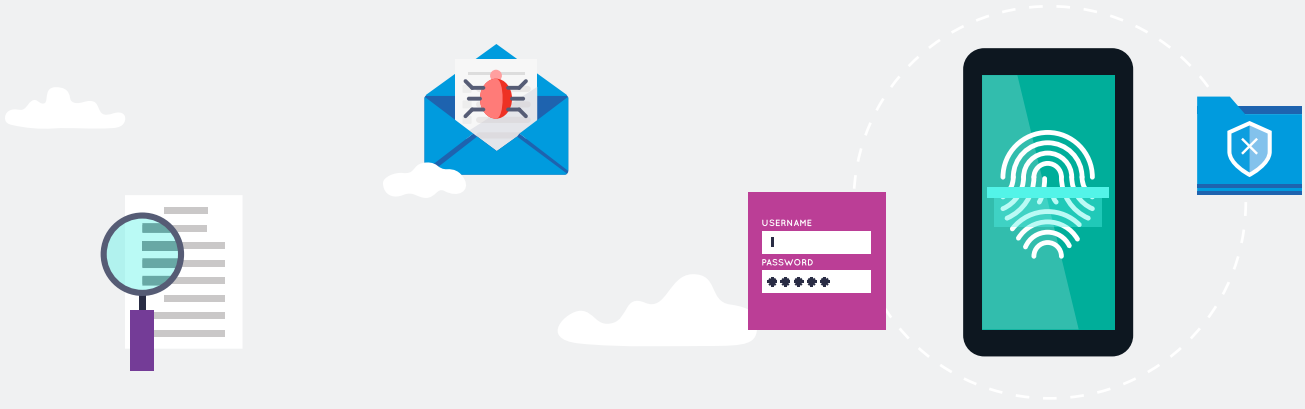
Voici les principaux facteurs à prendre en compte dans cette évaluation :

- Sophistication de l'attaque
- Portée et cible des attaques
- Type d'attaque
- Volume global de l'attaque

Vous devez également tenir compte du service, du département ou du groupe auquel appartient l'utilisateur.

Par exemple, certains utilisateurs peuvent sembler ne présenter aucun risque si l'on observe le volume ou le type d'emails malveillants qui leur sont directement adressés. Pourtant, ils peuvent représenter un risque plus élevé parce qu'ils travaillent dans un service très exposé aux attaques et sont donc plus susceptibles de devenir une cible clé à l'avenir.

Une threat intelligence pertinente peut identifier les outils employés par les cybercriminels et associer des incidents sans gravité apparente à des campagnes de plus grande envergure.



Privilèges : éléments auxquels les utilisateurs ont accès

L'évaluation des privilèges des utilisateurs commence par l'inventaire de tous les éléments potentiellement de valeur auxquels ils ont accès (données, autorité financière, relations clés, etc.). Vous devez savoir où résident vos données les plus sensibles et quels utilisateurs et applications y ont accès.

Les utilisateurs qui ont accès à des systèmes critiques ou à des éléments de propriété intellectuelle pourraient avoir besoin d'une protection supplémentaire, même s'ils ne sont pas particulièrement vulnérables ou ne sont pas encore la cible des cybercriminels.

La position de l'utilisateur dans l'organigramme de l'entreprise est bien entendu un facteur à prendre en compte lors de l'évaluation des privilèges. Ce n'est cependant pas le seul facteur — et bien souvent, il est loin d'être le plus important.

Une assistante de direction peut constituer une cible plus intéressante qu'un manager dans un objectif d'espionnage industriel, car elle a accès à l'emploi du temps du PDG. De la même façon, une infirmière travaillant à l'hôpital et ayant accès aux dossiers des patients peut constituer une cible plus judicieuse que le directeur général pour les usurpateurs d'identité.

Pour les cybercriminels, toute personne leur permettant d'arriver à leurs fins constitue une cible précieuse.

Il est tout aussi essentiel de protéger les utilisateurs à privilèges élevés des attaques extérieures que de protéger votre entreprise des utilisateurs à privilèges élevés. Entre de mauvaises mains, un accès privilégié peut causer des dégâts considérables, que ce soit par malveillance, par négligence ou à la suite d'une compromission. Les comptes compromis peuvent exporter des fichiers sensibles ou tenter de compromettre ou de manipuler d'autres utilisateurs internes.

SECTION 4

Mise en place d'un système de défense centré sur les personnes

Une approche centrée sur les personnes permet de protéger tous les utilisateurs en appliquant un niveau de contrôle adapté à leur niveau de risque. Elle est efficace sur toutes les plates-formes utilisées par le personnel, contre toutes les tactiques employées par les cybercriminels et sur tous les vecteurs de menaces pertinents.

Sécurité de base : la protection de tous les utilisateurs

Étant donné que les attaques par email prennent de nombreuses formes, vous avez besoin d'un système de défense capable de neutraliser tout le panel de menaces véhiculées par email.

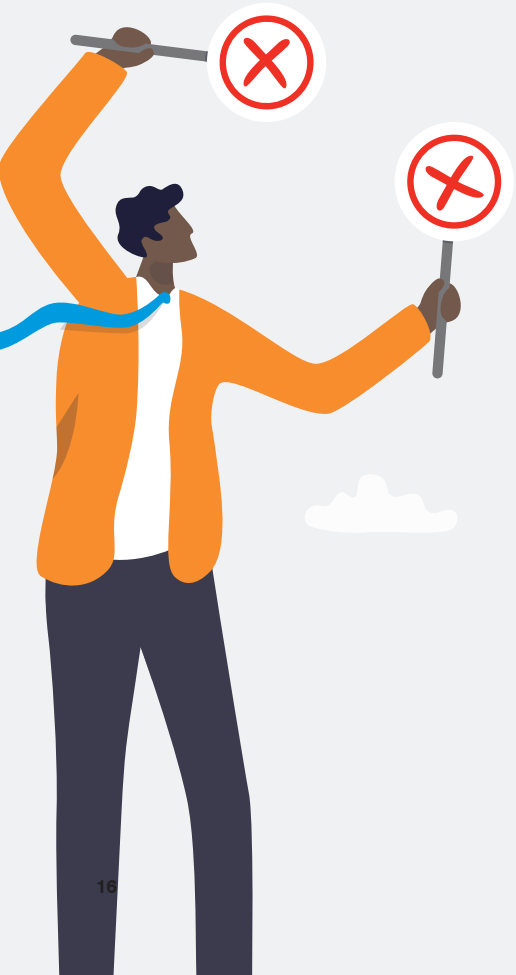
Voici les principales étapes à suivre pour la protection de la messagerie contre les menaces modernes :

- Neutralisez les pièces jointes malveillantes et les URL dangereuses avant qu'elles n'atteignent la boîte de réception des utilisateurs.
- Neutralisez les attaques d'imposteurs n'utilisant aucune charge virale, comme les attaques BEC et autres escroqueries, dont celles qui proviennent de comptes de messagerie compromis au sein de votre propre entreprise et chez des fournisseurs.
- Sécurisez la navigation Web et la messagerie personnelle des utilisateurs grâce à l'isolation du Web et de la messagerie personnelle.
- Renforcez la résilience des utilisateurs en mettant à leur disposition des formations de sensibilisation à la sécurité informatique et des informations contextuelles.
- Appliquez des contrôles tels que l'isolation du Web pour tenir les habitudes de navigation potentiellement dangereuses des utilisateurs à l'écart de votre environnement.
- Intégrez la protection des données à votre stratégie de protection de la messagerie.

Neutraliser les pièces jointes infectées et les URL malveillantes avant qu'elles n'atteignent la boîte de réception des utilisateurs

La plupart des cyberattaques requièrent une action de la part de la victime, le plus souvent ouvrir une pièce jointe ou cliquer sur une URL. Mais ces attaques qui s'exécutent suite à une action humaine ne peuvent réussir que si la victime voit le message.

C'est à cet égard qu'une solution avancée de protection de la messagerie donne toute sa mesure. En bloquant les charges virales malveillantes avant qu'elles n'atteignent la boîte de réception des utilisateurs, une solution efficace peut protéger votre entreprise contre un large éventail de malwares, notamment les ransomwares, les chevaux de Troie bancaires, les chevaux de Troie d'accès à distance, les voleurs d'informations, les téléchargeurs et les botnets.



Bloquer les menaces d'imposteurs difficiles à détecter

S'il est essentiel de neutraliser les malwares, certaines des attaques par email les plus dévastatrices n'ont recours à aucune charge virale. Elles s'appuient plutôt sur l'ingénierie sociale pour tromper les utilisateurs.

C'est notamment le cas des attaques BEC, un type de fraude aux virements bancaires. Selon le FBI, des attaques BEC ont été signalées dans l'ensemble des 50 États américains et dans 177 pays, avec des virements frauduleux effectués vers au moins 140 pays[13].

Dans le cadre des attaques BEC et d'autres formes de fraude par email, un cyberescroc usurpe l'identité d'une personne de confiance et cible un destinataire à l'aide d'un compte de messagerie usurpé, compromis ou similaire. Sous cette fausse identité, le cybercriminel demande à la victime de procéder à une opération, comme virer des fonds sur un compte bancaire à l'étranger ou lui envoyer des fichiers sensibles.

13 FBI, « Internet Crime Report 2020 » (Rapport 2020 sur la cybercriminalité), mars 2021.

Les impostures sont un problème complexe aux multiples facettes. Pour les maîtriser, il vous faut un système de défense multicouche qui sécurise les emails entrants, sortants et internes de manière globale et cohérente.

Au-delà de la formation des utilisateurs et des autres mesures de sécurité mentionnées dans cette section, voici quelques aspects essentiels d'une stratégie de défense contre les emails d'imposteurs.

DMARC

Déployez le protocole DMARC (Domain-based Message Authentication, Reporting and Conformance) pour l'authentification des emails. Ce protocole Internet permet de vérifier que les expéditeurs des emails sont bien qui ils prétendent être et qu'ils sont autorisés à envoyer des messages au nom de l'entreprise.

Il vous offre une visibilité sur tous les emails envoyés via votre domaine de messagerie, notamment ceux d'expéditeurs tiers de confiance tels que Marketo et Salesforce. Grâce à cette visibilité, vous pouvez approuver tous les expéditeurs légitimes qui tentent d'envoyer des emails en votre nom, et bloquer quiconque utilise vos domaines de confiance pour dérober de l'argent ou porter atteinte à votre marque.

Classification dynamique

Si DMARC permet de bloquer les menaces qui usurpent votre domaine, les cybercriminels peuvent employer d'autres techniques pour piéger les utilisateurs. Pour cette raison, l'analyse et la classification dynamiques du contenu des emails constituent une autre étape importante de la lutte contre les menaces sans malwares. Cet aspect de la sécurité de la messagerie électronique consiste à analyser le contenu des emails, et pas seulement leur provenance. Votre solution de protection de la messagerie doit donc être capable de détecter les signes révélateurs de fraude, puis de neutraliser et d'analyser tout contenu suspect. La classification dynamique analyse et gère les emails en fonction de plusieurs facteurs :

- L'en-tête de l'email, l'adresse IP et la réputation de l'expéditeur
- L'analyse du contenu pilotée par l'apprentissage automatique permettant de détecter le détournement d'adresses de réponse, certains mots ou certaines expressions
- La relation entre l'expéditeur et le destinataire
- Les informations contextuelles sur l'expéditeur, p. ex. s'il semble usurper l'identité d'un fournisseur connu

Informations sur la protection des emails internes et les risques liés aux fournisseurs

Dans certains cas, les cybercriminels n'essaient même pas de maquiller leur adresse email et se contentent de prendre le contrôle d'un compte légitime appartenant à l'entreprise, à un fournisseur ou à un partenaire. La compromission de comptes de messagerie peut être utilisée dans un large éventail d'attaques, et constitue une technique d'imposture particulièrement efficace. En voici les raisons :

- La plupart des entreprises n'appliquent pas le même niveau de surveillance et les mêmes contrôles de sécurité aux emails en interne qu'aux emails provenant de l'extérieur.
- La majeure partie des utilisateurs font confiance aux emails émanant de personnes qu'ils connaissent.
- Les cybercriminels qui prennent le contrôle d'un compte ont accès à une mine d'informations sur l'utilisateur piraté : ses correspondants, les sujets abordés et même son style d'écriture. Toutes ces informations leur permettent de rendre l'usurpation extrêmement convaincante.

La protection des utilisateurs internes et la collecte d'informations contextuelles sur les risques liés aux fournisseurs sont indispensables pour assurer une protection efficace de la messagerie.

Renforcer la résilience des utilisateurs grâce à une formation de sensibilisation à la sécurité informatique

Les cybercriminels sont devenus redoutablement doués pour tirer parti des faiblesses de la nature humaine grâce à des techniques d'usurpation convaincantes, à des objets de message intrigants et à des appels à l'action auxquels il est difficile de résister. Bien souvent, le destinataire de ces emails n'est pas le seul à cliquer dessus, car ils sont transférés à d'autres personnes qui cliquent à leur tour.

Les formations de sensibilisation à la sécurité informatique, en particulier lorsqu'elles font partie intégrante d'une culture solide de la sécurité, peuvent transformer vos utilisateurs en véritables piliers de défense contre les cyberattaques. Mais elles doivent être ciblées et s'inscrire dans la durée pour être véritablement efficaces auprès des collaborateurs. Des formations annuelles génériques ne sont pas suffisantes pour modifier les comportements des utilisateurs ni instaurer une culture de la sécurité.

Les balises email qui fournissent des informations contextuelles aux utilisateurs sur la nature du message peuvent également les aider à détecter et à signaler des menaces potentielles. Par exemple, une balise qui informe l'utilisateur que l'email provient d'une adresse externe ou que le domaine de messagerie est étrangement similaire à celui d'une marque de confiance peut l'aider à détecter une tentative de phishing potentielle.

L'isolation du Web et de la messagerie permet de confiner et d'analyser automatiquement les clics liés à des messages qui peuvent rediriger vers de faux sites demandant la saisie d'identifiants de connexion, des pièces jointes ou des URL malveillantes qui contiennent des malwares ou d'autres menaces. Elle peut être appliquée aux utilisateurs les plus à risque, aux VIP ou à un groupe d'utilisateurs plus large en fonction du niveau de risque.

15,4 Mio $

de dommages par entreprise en 2021

Protéger les données contre les compromissions et les menaces internes

Aucune solution de protection de la messagerie ne permet à elle seule de bloquer toutes les menaces. Même parmi les collaborateurs les mieux formés, certains utilisateurs peuvent tomber dans le piège d'attaques d'ingénierie sociale ciblées.

C'est pour cette raison que chaque système de défense de la messagerie devrait intégrer des outils de prévention des fuites de données, notamment de chiffrement. En cas d'incident, la rapidité d'intervention et de prévention des fuites de données peut empêcher l'attaque de se propager et les cybercriminels de mettre la main sur vos données les plus sensibles.

La prévention des fuites de données assure également une protection efficace contre les menaces internes. Personne n'apprécie de devoir considérer ses collègues comme une menace potentielle. Mais les menaces internes, notamment les collaborateurs négligents, malveillants ou compromis, ont coûté à chaque entreprise en moyenne 15,4 millions de dollars de dommages en 2021[14].

Que les données soient exfiltrées de votre environnement par une compromission externe ou une attaque interne, la prévention des fuites de données permet de les protéger.

14 Ponemon Institute, « 2022 Cost of Insider Threats Global Report » (Rapport 2022 sur le coût des menaces internes à l'échelle mondiale), janvier 2022.

Sécurité adaptative : mise en place de contrôles adaptatifs pour les utilisateurs les plus à risque

Une approche centrée sur les personnes bien rodée tient compte du fait que certains utilisateurs ont besoin de couches et de contrôles de sécurité supplémentaires. Ces utilisateurs sont plus susceptibles d'être victimes d'attaques. Ils sont davantage ciblés par celles-ci. Ils disposent d'un accès avec privilèges élevés à des systèmes critiques et des données sensibles. Ou ils peuvent présenter ces trois caractéristiques, ce qui accroît d'autant leur niveau de risque global.

Voici l'arsenal à appliquer aux utilisateurs les plus à risque :

- Formation ciblée de sensibilisation à la sécurité informatique
- Protection adaptative selon les risques, telle que l'authentification renforcée et l'isolation du Web et des URL
- Protection contre les compromissions (prise de contrôle) de comptes cloud

Formation ciblée de sensibilisation à la sécurité informatique

Une formation de sensibilisation à la sécurité informatique assurée à l'échelle de l'entreprise permet d'identifier les vulnérabilités et de réduire votre surface d'attaque humaine. Au-delà de révéler des failles évidentes, une formation ciblée peut également constituer une mesure préventive efficace pour tous les utilisateurs à risque, pas seulement les plus vulnérables.

Les utilisateurs présentant un risque plus élevé en raison de leur profil d'attaque, par exemple, peuvent bénéficier d'une formation sur les menaces qui leur est spécifique. Les utilisateurs avec privilèges élevés, quant à eux, peuvent suivre une formation supplémentaire sur les campagnes d'attaques ciblant les données auxquelles ils ont accès.

Contrôles adaptatifs basés sur le niveau de risque

Appliquer en continu les contrôles de sécurité les plus rigoureux à l'ensemble des utilisateurs n'est pas pratique pour la plupart des entreprises. Cela pourrait même se retourner contre elles. En effet, des mesures strictes mais inutiles peuvent grever la productivité des utilisateurs et les inciter à les contourner pour exercer leurs fonctions.

Mais parfois, cette couche de sécurité supplémentaire est nécessaire. Un collaborateur en première ligne risque d'être plus particulièrement enclin à tomber dans le piège d'une attaque ciblant votre secteur d'activité. Un chercheur peut être ciblé par un cybercriminel extrêmement sophistiqué. Un PDG, compte tenu du poste qu'il occupe, peut avoir accès aux données les plus sensibles de l'entreprise.

Dans certains cas, il vous faudra peut-être renforcer l'authentification. Dans d'autres, il peut se révéler nécessaire de recourir à l'isolation du Web lorsqu'un utilisateur clique sur des URL présentes dans des emails reçus.

Quelle que soit leur forme, les protections adaptatives doivent offrir un aperçu en temps réel des facteurs de risque liés aux VAP et appliquer des contrôles adaptés à ces risques.

Protection des comptes cloud

Aux yeux des cybercriminels, un compte compromis est une invitation au vol.

Un compte compromis peut être exploité à différentes fins malveillantes. En prenant le contrôle de l'accès de l'utilisateur légitime, un cybercriminel peut se déplacer latéralement au sein de votre environnement, dérober des données ou duper vos partenaires commerciaux et vos clients. C'est la raison pour laquelle il est essentiel de protéger les comptes de messagerie, et plus particulièrement les comptes cloud.

Réponse : neutralisation plus rapide et plus efficace des menaces

Les incidents de sécurité sont inévitables, mais ils n'ont pas à être désastreux.

Lorsqu'une attaque réussit à franchir vos défenses, la rapidité avec laquelle vous êtes capable de limiter et de réparer les dommages peut faire la différence entre un incident bref et des dégâts durables. C'est la raison pour laquelle un cadre rigoureux de prise en charge des incidents constitue un aspect essentiel de toute stratégie de sécurité centrée sur les personnes.

Dans de nombreuses entreprises, la réponse aux incidents peut être lente et demander l'intervention de nombreux collaborateurs. Elle comprend les étapes suivantes :

- Investigation et vérification de l'incident
- Mise en quarantaine des emails dangereux
- Confinement de la menace
- Identification de l'origine et de la portée de l'attaque
- Remédiation des systèmes infectés

Toutes ces étapes sont primordiales pour une réponse efficace. Mais comme le savent les responsables de la sécurité, une prise en charge manuelle des menaces a ses limites. C'est là qu'intervient l'automatisation.

Une prise en charge efficace automatise les tâches demandant d'importantes interventions manuelles, telles que la mise en corrélation et l'analyse des alertes de sécurité, la vérification des indicateurs de compromission et la collecte des données d'investigation numérique. L'automatisation permet également d'optimiser la remédiation, comme la mise à jour des listes de blocage des pare-feu et des messageries électroniques, la suppression des emails malveillants des boîtes de réception et la restriction de l'accès aux comptes des utilisateurs affectés.

Utilisée de manière stratégique, l'automatisation accélère la réponse aux incidents et vous permet de réaffecter votre équipe de sécurité aux tâches pour lesquelles elle est le plus compétente. Plutôt que de réagir à un déluge de menaces, elle peut appliquer des mesures de protection proactives.

Atouts de l'intelligence artificielle et de l'apprentissage automatique

Les cybercriminels ciblent les personnes. Ils les exploitent. Et au bout du compte, ils sont eux aussi humains.

Pour les stopper, il faut des solutions modernes capables de s'adapter aux comportements humains. C'est la raison pour laquelle l'apprentissage automatique est une composante essentielle de toute stratégie de sécurité centrée sur les personnes.

L'apprentissage automatique est plus rapide et efficace que les analyses humaines manuelles. Et contrairement aux algorithmes traditionnels basés sur des règles, il peut s'adapter rapidement à l'évolution des menaces et des tendances.

L'apprentissage automatique dans la lutte contre les attaques BEC

Prenons l'exemple des attaques BEC. Les attaques BEC de fraude aux factures fournisseurs sont des tactiques sophistiquées et complexes visant à dérober de l'argent. Pour piéger les victimes, les cybercriminels leur présentent une facture frauduleuse comme légitime ou détournent un paiement vers un compte bancaire dont ils ont le contrôle.

Les outils de sécurité traditionnels ont du mal à neutraliser les attaques de ce type, car elles sont très ciblées et ne contiennent aucune charge virale. L'apprentissage automatique peut analyser de manière dynamique un large éventail d'attributs, y compris les informations d'en-tête, le domaine et le corps du message, pour détecter une menace d'imposteur ou un fournisseur compromis.

Analyse du phishing d'identifiants de connexion

Nous aurions également pu prendre comme exemple les attaques de phishing d'identifiants de connexion. Ces attaques d'ingénierie sociale utilisent souvent de faux sites pour inciter les victimes à saisir leurs identifiants de connexion. Elles sont généralement si bien conçues que les utilisateurs ne savent pas faire la différence entre le faux site et le site légitime imité. En tirant parti de l'apprentissage automatique et de la vision par ordinateur pour analyser rapidement les URL, les outils de sécurité modernes peuvent détecter et bloquer tous les emails qui redirigent vers les sites frauduleux. L'apprentissage automatique peut détecter les URL dangereuses, même si leur enregistrement est récent, si elles sont hébergées par des sites de partage de fichiers ou si elles utilisent des techniques de contournement avancées telles que les CAPTCHA.

Concept GIGO (Garbage in, garbage out)

Contrairement aux systèmes logiciels standard basés sur des règles, l'apprentissage automatique s'appuie sur des données. Il n'est pas codé manuellement. Cela signifie que l'efficacité des systèmes d'apprentissage automatique dépend des personnes qui les entraînent et des données sur lesquelles ils s'appuient.

Lors de l'évaluation des fournisseurs qui vantent leurs fonctionnalités d'apprentissage automatique, recherchez des modèles basés sur l'apprentissage automatique entraînés avec de vastes ensembles de données sur les menaces. Les données doivent inclure des informations sur les menaces collectées auprès d'entreprises de premier plan des classements Fortune 100, Fortune 1000 et Fortune Global 2000, ainsi qu'auprès d'autant de fournisseurs de services Internet et de PME que possible. Ces données doivent couvrir de multiples vecteurs d'attaque, comme la messagerie, le cloud, le réseau et les réseaux sociaux. Ces canaux sont critiques, car les cybercriminels élargissent leur rayon d'action au-delà des emails.

Et n'oubliez pas le rôle des chercheurs spécialisés en menaces dans l'entraînement des modèles d'apprentissage automatique. Même les meilleurs scientifiques des données ne peuvent pas, à eux seuls, développer un modèle d'apprentissage automatique efficace. Ils ont besoin des compétences des professionnels forts d'une vaste expérience de l'analyse et de la recherche sur les menaces.

LISTE DE CONTRÔLE

Les fonctionnalités indispensables d'une solution de sécurité

La sécurité centrée sur les personnes n'est pas juste un terme marketing à la mode, mais une approche inédite des menaces et de leur neutralisation. Une approche adaptée doit également s'accompagner d'outils et de fonctionnalités efficaces.

Voici une liste de contrôle des fonctionnalités indispensables de toute solution de sécurité centrée sur les personnes.

Plate-forme unifiée, intégrée et évolutive

Une solution de sécurité centrée sur les personnes vaut plus que la somme de ses composantes. Les outils isolés peuvent résoudre certains aspects de votre problème de sécurité, mais la lutte contre les menaces modernes requiert une approche globale et intégrée qui tient compte de chaque tactique, outil et vecteur employé par les cybercriminels, sur tous les terminaux, toutes les plates-formes et tous les canaux utilisés par vos collaborateurs.

Les produits de sécurité non intégrés gérés via plusieurs consoles exigent plus de temps et de ressources en raison de leurs workflows complexes et redondants. Les équipes de sécurité bénéficient d'une vue fragmentée des menaces, se perdent dans des tâches inutiles et sont confrontées à une gestion complexe.

Privilégiez des solutions qui couvrent un large éventail de menaces et s'intègrent à votre écosystème de sécurité. En fonction de votre entreprise, ces solutions peuvent inclure des composants tels que des pare-feu de nouvelle génération, des systèmes de gestion des événements et des informations de sécurité (SIEM) et des outils de gestion de l'identité.

Protection efficace pour tous les utilisateurs

Le meilleur moyen de contrer les attaques par email est d'adopter une approche multicouche, comme le recommandent depuis longtemps Gartner et d'autres experts.

Assurez-vous que vos cyberdéfenses peuvent neutraliser les menaces suivantes :

- Spam et emails indésirables à diffusion massive
- Attaques qui utilisent des pièces jointes et des URL malveillantes
- Attaques n'impliquant pas de charge virale telles que les attaques BEC
- Compromissions de comptes de messagerie et prises de contrôle de comptes cloud

Les utilisateurs jouent un rôle déterminant dans les attaques par email d'aujourd'hui. C'est pourquoi vous devez intégrer une formation de sensibilisation à la sécurité informatique à votre stratégie de protection de la messagerie électronique. Assurez-vous que votre programme de formation inclut les éléments suivants :

- Formations courtes pour favoriser l'engagement et des changements de comportement
- Simulations d'attaques de phishing inspirées par des campagnes réelles afin que les utilisateurs se familiarisent avec les menaces auxquelles ils sont susceptibles d'être confrontés
- Formations régulières basées sur des données pour les utilisateurs vulnérables ciblés par des cybercriminels ou qui interagissent avec des messages de phishing réels
- Balises email qui attirent l'attention des collaborateurs sur les messages suspects, avec mécanismes de signalement intégrés et envoi d'un feedback aux utilisateurs

Pour protéger les données volées, partagées accidentellement ou divulguées volontairement par un utilisateur interne, il est primordial de faire appel au chiffrement et à d'autres mesures de prévention des fuites de données. Une solution efficace de prévention des fuites de données permet de réaliser les tâches suivantes :

- Analyser et classer le contenu en détail et, si nécessaire, bloquer son envoi par email, son transfert dans le cloud ou son chargement sur une clé USB
- Identifier les utilisateurs malveillants, négligents ou compromis et aider les équipes informatique, RH, juridique et de sécurité à prendre les mesures appropriées pour éviter des dommages durables
- Identifier et protéger toutes les formes standard de contenu soumis à des réglementations, telles que les normes PCI et FINRA et la loi HIPAA
- Réacheminer, chiffrer ou rejeter automatiquement les emails qui transgressent les règles de sécurité et autres, et en avertir les personnes appropriées au sein de votre entreprise

Contrôles adaptatifs pour les utilisateurs les plus à risque

Les utilisateurs les plus à risque (en fonction de leur vulnérabilité, de leur profil d'attaque et de leurs privilèges) nécessitent des contrôles de sécurité supplémentaires. Une solution de protection de la messagerie électronique centrée sur les personnes vous aide à identifier ces VAP et à les protéger grâce à des couches de sécurité supplémentaires. Optez pour une solution offrant les avantages suivants :

- Visibilité décisionnelle sur vos VAP grâce à des informations de cyberveille riches et pertinentes et à une analyse détaillée du profil de risque des utilisateurs
- Outils de reporting simplifiant l'analyse et la communication du niveau de vulnérabilité, du profil d'attaque et des privilèges des utilisateurs, avec des comparatifs entre les différents départements et secteurs d'activité
- Réponse automatique à l'évolution du profil de risque des utilisateurs grâce au renforcement de l'authentification, à la réduction des privilèges, à l'isolation des URL, etc.

Réponse rapide et efficace en cas d'incident

L'automatisation des étapes clés de la prise en charge des incidents permet d'optimiser les tâches critiques mobilisant des ressources importantes en personnel. Ceci permet de réaffecter les équipes de sécurité à des tâches pour lesquelles elles sont plus compétentes. Optez pour des outils automatisés de réponse offrant les avantages suivants :

- Vérification des menaces, identification des utilisateurs impactés et collecte d'éléments contextuels et de données d'investigation numérique les concernant
- Enrichissement des alertes à l'aide d'informations pertinentes de cyberveille
- Confinement et neutralisation des menaces au sein de l'environnement, dans le cloud et sur site ; mesures correctives automatisées pouvant inclure l'analyse des emails signalés par les utilisateurs, l'extraction des menaces vérifiées de la boîte de réception des collaborateurs et la réinitialisation des mots de passe des comptes compromis

EN SAVOIR PLUS

Pour plus d'informations, visitez notre site à l'adresse : **proofpoint.com/fr**.

À PROPOS DE PROOFPOINT

Proofpoint, Inc. est une entreprise leader dans le domaine de la cybersécurité et de la conformité qui protège les ressources les plus importantes et les plus à risques des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, Proofpoint aide les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris 75 % des entreprises de l'index Fortune 100, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les personnes, pour diminuer leurs risques les plus critiques via les emails, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur **www.proofpoint.com/fr**.

proofpoint.

0301-001-01-03 03/22