Proofpoint Security Awareness Training

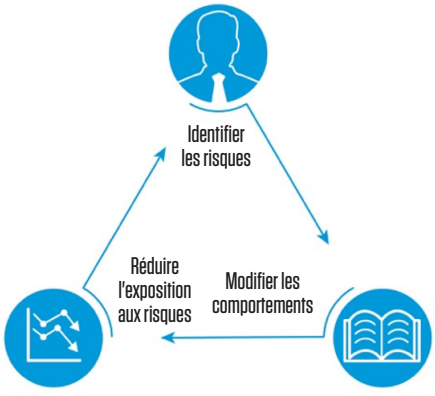
PRINCIPAUX AVANTAGES

- Réduisez les risques posés par les attaques de phishing et autres cyberattaques grâce à un changement de comportement des utilisateurs.
- Offrez des formations cohérentes dans plusieurs langues, partout dans le monde.
- Hiérarchisez et améliorez les interventions sur incident.
- Suivez les progrès accomplis grâce à la création de rapports dynamiques et à une API de gestion de résultats.
- Réduisez de 90 % le nombre d'attaques de phishing et d'infections de malwares.

Proofpoint Security Awareness Training vous permet de proposer la formation appropriée aux collaborateurs concernés au moment opportun. Cette solution transforme vos utilisateurs finaux en véritables piliers de défense capables de détecter les cyberattaques et de protéger votre entreprise.

Il faut savoir que plus de 90 % des cyberattaques ciblent les utilisateurs[1]. La formation des collaborateurs est donc un aspect critique de votre sécurité. Les technologies conçues pour détecter et bloquer les menaces avant qu'elles n'atteignent les utilisateurs ne peuvent pas neutraliser toutes les attaques. Vos collaborateurs doivent être conscients des dangers et savoir comment réagir de façon adéquate lorsqu'ils sont la cible de phishing et d'attaques par piratage de la messagerie en entreprise (BEC, Business Email Compromise). La solution vous aide à former vos collaborateurs à réagir correctement lors de cyberattaques de ce type. Nous vous aidons à différents égards :

- Identification des risques liés aux utilisateurs
- Modification des comportements des collaborateurs
- Réduction de l'exposition aux risques de l'entreprise



1 Verizon. « 2019 Data Breach Investigations Report » (Rapport d'enquête 2019 sur les compromissions de données). Juillet 2019.

IDENTIFIER LES RISQUES

Identifier les cibles des attaques et évaluer leur capacité à se protéger

Grâce aux rapports sur vos VAP (Very Attacked People™, ou personnes très attaquées), vous disposez d'une visibilité optimale sur les utilisateurs qui font l'objet d'attaques. Consultables dans le tableau de bord Proofpoint Targeted Attack Protection (TAP), ils contiennent des données pertinentes, telles que la personne visée par l'attaque et les types de menaces observées.

Les simulations d'attaques de phishing ThreatSim® vous aident à prendre la mesure de la vulnérabilité de votre entreprise face à un large échantillon d'attaques de phishing. Vous pouvez choisir parmi des milliers de modèles de phishing répartis dans 13 catégories pour évaluer le comportement des utilisateurs face à de multiples types de menaces, notamment :

- Pièces jointes malveillantes
- Liens intégrés
- Demandes de données personnelles

Chaque semaine, nous ajoutons de nouveaux modèles afin que les dernières tendances en matière d'attaques soient représentées. Ces simulations d'attaques de phishing comprennent des modèles dynamiques, fondés sur la threat intelligence recueillie par Proofpoint, ainsi que d'autres modèles inspirés des demandes de nos clients ou axés sur des thèmes saisonniers, afin de correspondre au mieux aux attaques réelles que pourraient subir les utilisateurs.

Les utilisateurs qui tombent dans le piège reçoivent immédiatement des explications et des conseils pour préciser les objectifs de la simulation, démontrer les dangers d'une attaque réelle et apprendre comment éviter de se laisser piéger à l'avenir. Vous pouvez également assigner automatiquement une formation à ceux qui échouent lors d'une simulation de phishing.

Il est également intéressant de savoir dans quelle mesure vos collaborateurs sont sensibilisés au problème des périphériques mémoire amovibles infectés. Les simulations d'attaques par clé USB ThreatSim forment vos collaborateurs aux dangers des clés USB infectées. Vous pouvez accéder aux simulations USB à tout moment et aussi souvent que vous le souhaitez. De plus, les utilisateurs qui tombent dans le piège de la simulation se voient immédiatement proposer des conseils et explications pertinents.

CyberStrength® est un outil Web puissant d'évaluation des connaissances. Il évalue les vulnérabilités des utilisateurs au-delà de la messagerie électronique et des lecteurs USB, couvrant un large éventail de problèmes de sécurité critiques, tels que l'emploi de terminaux mobiles, les attaques d'ingénierie sociale et la navigation Web. Vous pouvez choisir des évaluations prédéfinies dans une bibliothèque contenant des centaines de questions en plus de 35 langues et inscrire automatiquement les utilisateurs aux formations appropriées. Vous pouvez en outre créer des questions personnalisées pour évaluer la connaissance des règles et des procédures de votre entreprise. Une fois que vous avez établi une ligne de base des connaissances de vos utilisateurs, vous pouvez suivre les recommandations qui permettront de limiter les risques associés dans divers domaines.

MODIFIER LES COMPORTEMENTS

Offrir une formation basée sur les menaces réelles, le comportement des utilisateurs et les lacunes au niveau des connaissances

Un contenu pertinent et étoffé est la clé d'une formation efficace, capable de modifier les comportements des utilisateurs. Grâce à notre Customization Center en libre-service, vous pouvez adapter le contenu à vos utilisateurs et en améliorer la pertinence. Vous pouvez par exemple personnaliser le texte, les images, les questions, les écrans, etc. des formations. La fonction Learning Science Evaluator vous guide en temps réel pour garantir l'efficacité de votre contenu personnalisé.

Les utilisateurs peuvent suivre les formations à tout moment, n'importe où, sur tout endpoint connecté. Chaque module dure de 5 à 15 minutes, ce qui évite de perturber le travail quotidien. Les modules interactifs Proofpoint sont conformes aux exigences de la section 508 et aux directives WCAG 2.0 AA (directives d'accessibilité des contenus Web).

Les modules de formation Proofpoint reposent sur des principes pédagogiques à l'efficacité reconnue. Ils couvrent un large éventail de risques de sécurité, allant des attaques de phishing aux menaces internes. Parmi les contenus disponibles :

- **Modules de formation** vidéo, interactifs et ludiques. Ils sont traduits dans plus de 35 langues et adaptés à la région où réside l'utilisateur.
  - Pour les formations spécifiquement axées sur la conformité et la confidentialité, du contenu spécialisé est proposé par notre partenaire, TeachPrivacy.
  - Notre acquisition de The Defence Works nous permet de proposer un contenu novateur et attrayant, afin de rendre notre offre encore plus variée.
- **Supports de sensibilisation à la sécurité** tels que vidéos, infographies, newsletters, articles, posters, images, etc. pour renforcer l'impact des formations.
- **Documentation sur le programme** à l'intention des administrateurs pour les aider à mettre en place un programme de formation efficace.

Vous pouvez également signaler aux utilisateurs les attaques et leurres les plus pertinents déterminés par la threat intelligence de Proofpoint. Notre série d'alertes Attack Spotlight fournit des informations claires et concises qui leur apprennent à identifier et à éviter les menaces actuelles.

RÉDUIRE L'EXPOSITION AUX RISQUES

Les utilisateurs avertis signalent les menaces potentielles, ce qui réduit la surface d'attaque

Le module d'extension du client de messagerie PhishAlarm® permet à vos collaborateurs de signaler des emails suspects d'un simple clic. Après avoir signalé un email, l'utilisateur reçoit un remerciement par message contextuel ou par email afin de renforcer immédiatement les comportements positifs. Grâce à ce module d'extension, il n'est pas nécessaire d'obtenir les en-têtes et pièces jointes des utilisateurs qui auraient transféré des emails dans une boîte email de signalement d'abus.

Grâce à PhishAlarm Analyzer, les messages signalés par vos utilisateurs sont automatiquement analysés et enrichis par divers systèmes de threat intelligence et de réputation de Proofpoint. Un rapport de synthèse sur la menace est ensuite généré, incluant notamment des informations détaillées sur le message et sa catégorie (malveillant, spam, etc.). Votre équipe de réponse aux incidents n'est plus tenue de rechercher et de hiérarchiser les messages, ce qui lui permet de gagner un temps précieux. Le système de threat intelligence de Proofpoint présente une couverture et une efficacité inégalées en matière d'informations sur les menaces. Plus de 100 chercheurs analysent plus d'un cinquième des emails B2B et B2C quotidiens, ainsi que les menaces liées au cloud et aux réseaux sociaux.

La solution automatisée CLEAR (Closed-Loop Email Analysis and Response) envoie les messages signalés vers TRAP (Threat Response Auto-Pull). Dans TRAP, ces messages peuvent être automatiquement mis en quarantaine, fermés ou envoyés aux équipes de réponse aux incidents. Les administrateurs peuvent définir des messages de réponse personnalisés qui seront envoyés aux utilisateurs, ce qui renforce les comportements positifs et vous aide à établir une culture de la sécurité.

ANALYSE DES RÉSULTATS GRÂCE À DES RAPPORTS COMPLETS

Nos rapports complets peuvent vous aider à estimer les progrès de vos utilisateurs. Intuitifs, ils vous aident à évaluer les progrès accomplis, à mesurer le retour sur investissement et à comparer et suivre les connaissances des utilisateurs. Grâce à une visibilité à la fois globale et granulaire, vous disposez d'un tableau complet de la situation. Vous pouvez par exemple observer les interactions de vos collaborateurs avec les évaluations, les simulations d'attaques et les attributions de formations. Les tableaux de bord permettent de filtrer les données, comparer les évaluations, modifier les facteurs de mesure, etc., en toute facilité.

Vous pouvez télécharger et exporter les rapports. Cela permet de partager des informations avec d'autres parties prenantes ou d'exécuter des analyses et comparaisons plus détaillées, en examinant par exemple certains indicateurs à la lumière d'autres événements de sécurité. Par ailleurs, vous pouvez automatiser la génération de rapports pour simplifier le processus. Vous pouvez planifier la remise automatique de rapports à vous-même et à d'autres parties prenantes.

Nous proposons également une API de gestion de résultats, qui vous permet d'accéder aux rapports et analyses relatifs aux formations, au phishing, à l'évaluation des connaissances, aux utilisateurs et aux emails. Vous pouvez ensuite intégrer ces informations dans des outils de veille stratégique ou dans un système de gestion des formations.

EN SAVOIR PLUS

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

À PROPOS DE PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) est une entreprise leader dans le domaine de la cybersécurité 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 plus de la moitié des entreprises de l'index Fortune 1000, 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.