Les résultats de votre campagne de phishing sont disponibles !

Cette simulation utilise des techniques de phishing réelles pour évaluer comment vos utilisateurs réagiraient à une attaque inévitable, notamment s'ils cliqueraient sur un lien nuisible, téléchargeraient un fichier malveillant et/ou compromettraient leurs informations d'identification.

Vous pouvez cliquer dans les cases pour comprendre des informations supplémentaires sur l'attaque de phishing.

Score de risques

Risque moyen

549

/900

Analyse du domaine

8	2	860	147
Domaines connectés	Services connectés	Domaines similaires	Applications connectées

Domaines et services connectés

Bien qu'il n'y ait pas de risque immédiat pour les domaines et services connectés eux-mêmes, ils aident les cybercriminels à comprendre comment votre entreprise est structurée. Grâce à ces informations, les cybercriminels sont libres de lancer une attaque très contextualisée qui a de fortes chances de réussir.

Les domaines laissés inactifs pendant un certain temps présentent également un risque, car ils offrent aux cybercriminels la possibilité d'utiliser des domaines semblables pour usurper l'identité d'une marque.

Domaines semblables

Un domaine semblable est presque identique à un domaine existant, mais avec une légère altération. Ils sont destinés à tromper la cible en la confondant avec le domaine original. Cela permet aux cybercriminels de se faire passer pour des marques légitimes et de commettre des fraudes. C'est pourquoi ils enregistrent des centaines de milliers de domaines similaires chaque année.

Applications connectées

Les cybercriminels sont curieux de connaître les applications utilisées dans votre entreprise. Grâce à ces informations, ils peuvent exploiter toute vulnérabilité connue dans les applications que vous utilisez afin de exposer vos données - ou se faire passer pour ces applications dans des attaques de phishing très ciblées contre des membres du personnel.

Analyse des brèches

24%	45%	0%
de vos utilisateurs apparaissent dans une ou plusieurs brèches à risque élevé	de vos utilisateurs apparaissent dans une ou plusieurs brèches à risque moyen	de vos utilisateurs apparaissent dans une ou plusieurs brèches à faible risque

Analyse du Dark Web

Une quantité modérée de données sur votre entreprise et vos employés est disponible sur l'Internet. Si un cybercriminel venait à acquérir ces informations, il pourrait les utiliser dans le cadre d'escroqueries par ingénierie sociale ou d'attaques de phishing très ciblées.

La présence de données de cette nature sur l'Internet montre que les employés ne respectent pas les bonnes pratiques en matière de sécurité des informations, comme le fait de garder leur e-mail professionnel privé et de ne l'utiliser que pour des services liés au travail.

Une attaque réussie pourrait causer des dommages importants à votre marque et à la réputation de votre entreprise, ainsi que des répercussions sur vos clients, vos partenaires et toute autre personne liée à votre réseau commercial.

Campagne de phishing

55%	44%	70%
E-mail ouvert	Page de destination visitée	Compromis

Simulation d'une cyber-attaque - Phishing

Les réactions de vos employés à l'attaque de phishing simulée montrent qu'une attaque de cette nature présente un risque modéré pour votre entreprise.

Le lien contenu dans l'e-mail de phishing simulé a été cliqué par un nombre modéré d'employés. Un e-mail similaire pourrait être utilisé par des cybercriminels pour diriger vos employés vers de faux sites web qui récolteront leurs identifiants de connexion ou infecteront leurs appareils avec des logiciels malveillants.

Les employés qui ont donné leurs informations d'identification sur la page de destination de la simulation sont susceptibles de transmettre des informations sensibles aux cybercriminels, laissant tout votre réseau d'entreprise ouvert à d'autres infiltrations.

Délai avant de subir une brèche

Le délai avant de subir une brèche est

1 heure 33 minutes

Le délai avant de subir une brèche est une estimation du temps qui s'écoule entre le moment où un attaquant commence à chercher une cible et celui où il réussit à pénétrer dans une organisation.

La fourchette est déterminée par les données que nous avons recueillies lors de la création de votre rapport de risque, combinées à certaines estimations basées sur les données du secteur.

Résumé

Votre entreprise est vulnérable à une brèche.

D'après les conclusions du rapport, le risque que vos employés représentent actuellement pour l'entreprise est moyen. Toute cyberattaque visant votre entreprise a une chance moyenne de réussir.

Il est possible de réduire les risques dans votre entreprise en déployant de nouveaux processus et technologies. Cependant, les cybercriminels cherchent souvent à exploiter les employés, qui constituent un point faible courant dans la défense d'une entreprise.

Une brèche pourrait avoir un impact important sur la réputation et la marque, et entraîner des amendes de la part des organes directeurs s'il s'avère que vous n'avez pas mis en place le niveau de sécurité nécessaire pour réduire les risques de brèche.

Ce qu'il faut faire maintenant

Commencez à aborder le cyber-risque humain

Votre entreprise risque d'être victime d'une brèche dans une cyberattaque.

Afin de réduire la menace d'incidents de sécurité liés aux utilisateurs, de pertes de données sensibles et de dommages financiers, nous proposons fortement de déployer le programme de remédiation des risques humains suivant, composé de **quatre éléments fondamentaux** :

Former les employés aux meilleures pratiques de cyber-sécurité

Afin de réduire les menaces internes, de renforcer la résilience face à une inévitable cyberattaque et de se conformer aux normes de sécurité de l'information, les marques de connaissances de vos employés en matière de cyber-sécurité seront évaluées et des formations régulières de sensibilisation à la cyber-sécurité seront déployées.

Une formation assistée par ordinateur sera organisée et mesurée chaque mois, sous la forme de cours courts et attrayants, conçus pour maximiser la rétention des connaissances et le changement de comportement sans perturber l'efficacité du travail, et couvrant les compétences essentielles des meilleures pratiques en matière de sécurité informatique.

Mettre en œuvre des chartes informatiques en matière de sécurité des informations et des données

La mise en œuvre de chartes informatiques et de procédures de sécurité de l'information et des données réduira le risque humain de votre entreprise en définissant clairement les normes du comportement attendu, ainsi que des conseils sur la manière dont les employés peuvent atteindre ces normes.

Les principales chartes informatiques seront mises en œuvre et envoyées à vos employés pour leur approbation. Afin de s'assurer que vos chartes sont respectées, les approbations par signature électronique des employés seront automatiquement suivies et accessibles pour un audit facile.

Effectuer des évaluations régulières du phishing

Les techniques de phishing et d'ingénierie sociale évoluent quotidiennement, ce qui augmente la probabilité que vos employés compromettent des données sensibles lors d'une attaque sophistiquée.

Afin d'évaluer et de surveiller la sensibilité de vos employés aux attaques nouvelles et diverses, des simulations régulières de phishing seront automatiquement déployées et suivies, ce qui vous donnera une visibilité totale des ouvertures, des clics et des compromissions. Si un utilisateur échoue à une simulation de phishing, il sera automatiquement inscrit à un court cours de sensibilisation au phishing afin de limiter les risques futurs.

Surveiller le Dark Web à la recherche d'informations d'identification d'utilisateurs exposées.

Chaque année, des millions d'informations d'identification sont exposées lors de brèches dans les données. Il est donc probable que vos employés voient à un moment ou à un autre leurs données sensibles compromises sur le Dark Web. Ces données sont ensuite utilisées pour mener des attaques de type "compromission de l'adresse email professionnelle" (BEC) et d'ingénierie sociale.

Afin de réduire la probabilité de ces attaques et de protéger vos utilisateurs exposés, des analyses régulières seront effectuées sur le Dark Web et à travers des milliers de sites tels que Pastebin, et votre entreprise serait alertée lorsque des données exposées sont détectées dans une brèche.