YOUR-IT
The smart choice

ÉTUDE DE CAS SUR LA GESTION DES RISQUES HUMAINS (GRH)

Un regard de terrain sur la façon dont la GRH a transformé le comportement des employés de cette entreprise en matière de sécurité.

OBJECTIFS DU CLIENT

- Identifier les employés qui risquent le plus d'être victimes d'une attaque de phishing.
- Obtenir un aperçu permanent des employés vulnérables aux attaques de phishing.
- Dispenser régulièrement des formations de sensibilisation à la sécurité qui aideront les utilisateurs à résister aux attaques de phishing et à améliorer leur comportement général en matière de sécurité.
- Démontrer la conformité de la clause 7.2.2 de l'ISO 27001

APPROCHE

Formation de sensibilisation à la sécurité

- Analysez les forces et les faiblesses actuelles de chaque utilisateur en matière de sécurité à l'aide d'un questionnaire d'évaluation initiale.
- Sur la base des résultats du quiz, chaque employé recevra toutes les quatre semaines un nouveau cours de sensibilisation à la sécurité, les cours étant classés par ordre de priorité afin de traiter en premier lieu les points les plus faibles.
- Des cours de conformité personnalisés seront également dispensés périodiquement.

Exercices de simulation de phishing

- Au moins une simulation de phishing sera lancée tous les six mois, afin de tester l'impact de la formation et d'identifier les utilisateurs à haut risque.
- Une formation de suivi instantanée sera déployée pour tous les employés qui compromettent leurs informations d'identification lors d'une simulation de phishing, afin de réduire les risques le plus rapidement possible.

Surveillance du Dark Web

- Une surveillance permanente du Dark Web sera mise en place afin d'identifier et d'éviter les attaques qui exploitent les informations d'identification volées des employés, comme les noms d'utilisateur et les mots de passe compromis.

PROFILE CLIENT

Industrie

- BTP

Nombre d'utilisateurs

- 250 Employés

Utilise la plateforme depuis

- Août 2021

DÉFIS/ FACTEURS CLÉS

- Un membre du personnel a été victime d'une attaque de phishing de type "carte cadeau".
- Les supports actuels de formation à la sensibilisation à la sécurité sont peu ludiques et inefficaces.
- L'approche actuelle de la formation à la sensibilisation à la sécurité prend trop de temps.

L'IMPACT - SCORE DE RISQUE

Afin de mesurer l'impact du programme de gestion des risques humains du client, des mesures de risques clés ont été prises au tout début du programme et après sept mois d'activité.

Ci-dessous, vous verrez le score de risque de l'entreprise (toutes les mesures de risque fusionnées), un score de risque sur la formation (une combinaison de notes de cours et de pourcentages d'achèvement de cours), un score de risque sur le phishing (les taux d'ouverture, de clics et de compromission recueillis lors de simulations de phishing) et un score de risque sur le dark web (basé sur la quantité de données sensibles de votre entreprise exposées sur le dark web).

SCORE DE RISQUE

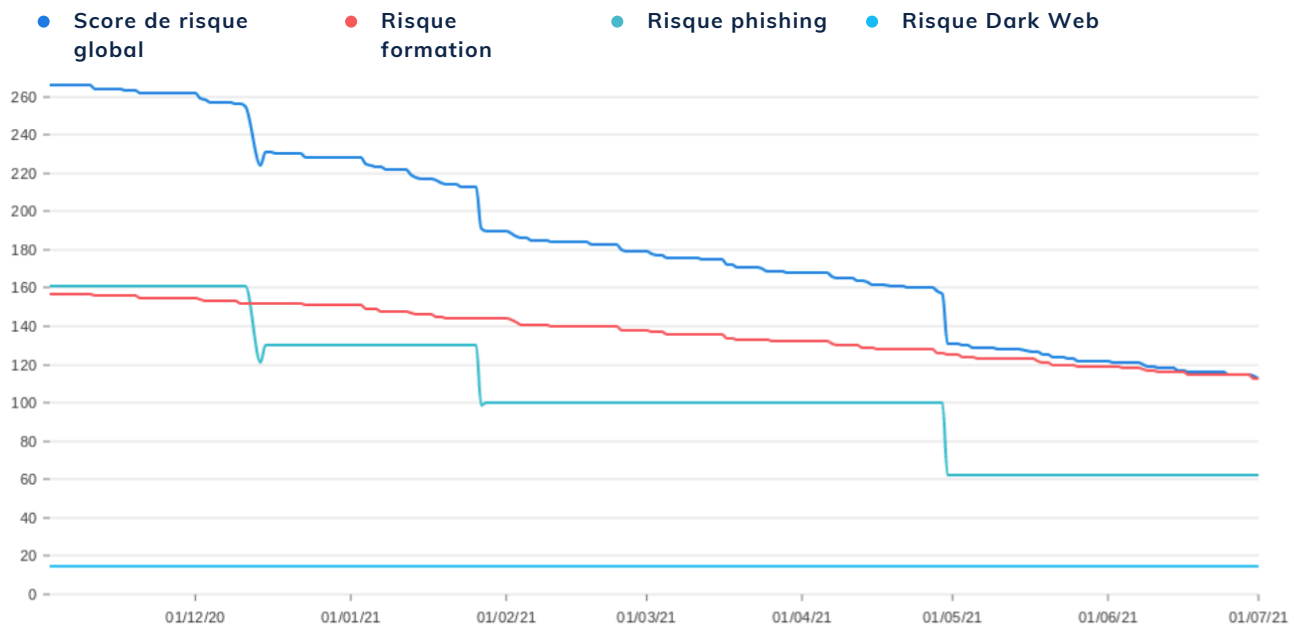
Après sept mois de formation de sensibilisation à la sécurité, de simulations périodiques d'hameçonnage et d'analyse des brèches sur le dark web, le score global de risque humain du client a été réduit de 152 points, passant d'un risque "moyen" à un risque "faible".

Le risque de phishing au sein de l'entreprise a considérablement diminué de 100 points, ce qui signifie que les employés étaient beaucoup plus aptes à repérer, éviter et signaler les attaques suspectes.

SCORE DE RISQUE INITIAL		SCORE DE RISQUE APRES 7 MOIS
270/900	»	**118**/900
Moyen		Faible

DONNEES CLES

- RISQUE GLOBAL | -152
- RISQUE FORMATION | -40
- RISQUE PHISHING | -100
- RISQUE DARK WEB | IDENTIQUE



L'IMPACT - FORMATION ET RÉSULTATS DU PHISHING

Afin de réduire le cyber-risque humain, il était important de s'assurer que les employés terminent leurs cours de sensibilisation à la sécurité dès que possible et atteignent le score minimum de 80% dans leurs questionnaires de suivi.

Pour ce faire, le taux d'achèvement et les notes des cours ont été suivis pour chaque employé, et des e-mails de rappel automatique ont été envoyés à tous les membres du personnel qui n'avaient pas terminé leur cours dans les jours ouvrables.

Les résultats de la simulation de phishing en cours ont également été suivis pour s'assurer que les cours de sensibilisation à la sécurité avaient l'impact souhaité.

RÉSULTATS DES FORMATIONS

Temps moyen pour terminer un cours	Cours débutés	Cours terminés	Note moyenne aux cours
3 jours	97 %	97 %	92 %

PERFORMANCE AUX SIMULATIONS DE PHISHING

	Envoyé	Ouvert	Vitisité	Compromis
1ère simulation	146	74	40	9
2e simulation	172	34 -74%	4 -163%	2 -127%

Sur les 250 membres du personnel, 97 % ont commencé et terminé leur cours, prenant en moyenne seulement trois jours pour terminer leur cours après l'inscription, tout en obtenant une note moyenne de 92 %.

Comme le montre le tableau des performances des simulations de phishing, les employés étaient beaucoup moins susceptibles d'ouvrir, de cliquer ou d'être compromis par une simulation de phishing.