Kaspersky® Security Awareness

Le facteur humain est un enjeu majeur de la cybersécurité en entreprise

Au cours des dernières années, la plupart des organisations ont installé des filtres anti-phishing avancés et des pare-feu, et déployé des outils spécialisés pour atténuer les cybermenaces. Les cybercriminels se servent donc désormais des salariés comme point d'entrée initial dans les systèmes informatiques. L'exploitation des lacunes fréquentes dans les connaissances des utilisateurs est le moyen le plus simple de pénétrer dans l'infrastructure informatique d'une entreprise.

Selon l'enquête Kaspersky Lab et B2B International[1], **52 %** des entreprises admettent que les salariés, par négligence ou par ignorance, représentent le principal point faible de leur sécurité informatique et peuvent compromettre leur stratégie de sécurité.

Ce qui inquiète le plus ces organisations, ce sont les salariés qui partagent des informations inappropriées sur leurs appareils mobiles (47 %), la perte physique d'appareils mobiles mettant l'entreprise en danger (46 %) et l'utilisation inappropriée de ressources informatiques par les salariés (44 %).

En y regardant de plus près, les craintes concernant l'utilisation inappropriée de l'informatique par les salariés varient considérablement selon la taille de l'organisation et les très petites entreprises (1 à 49 salariés) se sentent plus exposées aux risques que les entreprises de plus de 1 000 salariés. Cela peut être dû à un certain nombre de facteurs, les grandes entreprises peuvent notamment avoir des politiques plus strictes et une formation plus poussée pour leurs salariés.

L'erreur humaine : principale source des cyberincidents

Selon l'indice relatif à la veille stratégique en matière de sécurité d'IBM, l'erreur humaine est impliquée dans plus de 90 % des incidents de sécurité (clic sur un lien de phishing, consultation d'un site Web suspect, activation de virus ou autres menaces persistantes avancées).

L'enquête réalisée en 2017 par Kaspersky Lab et B2B International[1] appuie ces conclusions. Selon ce rapport, l'utilisation inappropriée des ressources informatiques par les employés est à l'origine des attaques subies par 39 % des organisations mondiales sur une période de 12 mois.

L'augmentation du nombre de cyberincidents provoqués par des erreurs humaines est surtout perceptible dans le secteur des Très Petites Entreprises (TPE) : en un an seulement, le pourcentage de petites organisations (1 à 49 salariés) victimes d'une attaque impliquant une erreur humaine est passé de 25 à 32 %.

Plus préoccupant encore, près de la moitié des entreprises (entre 44 et 48 %) ne se sentent pas bien protégées contre la menace posée par l'ignorance, la naïveté et la malice de leurs propres salariés.

Les organisations désignent également les employés négligents ou mal informés comme la deuxième cause d'incident : 46 % des répondants estiment qu'il s'agit d'une source majeure d'incident. Il ne fait donc aucun doute que les salariés sont pour des pirates la principale porte d'entrée au sein d'une organisation. Néanmoins, un personnel bien entraîné, bien informé, conscient des risques et capable de respecter des normes de cyberhygiène peut également devenir votre première ligne de défense.

1 « Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within » (« Facteur humain dans la sécurité informatique : Comment les employés rendent les entreprises vulnérables de l'intérieur »), juin 2017

L'impact financier moyen des actions inappropriées des salariés négligents ou mal informés[1]

Pour les PME :

- Partage inapproprié de données - 88 000 $
- Perte matérielle d'appareils mobiles exposant l'organisation à des risques - 99 000 $
- Perte matérielle d'appareils ou de supports contenant des données - 81 000 $
- Utilisation inappropriée des ressources informatiques par un salarié - 68 000 $

Pour les entreprises :

- Incidents impliquant des appareils non informatiques connectés - 1,6 M$
- Perte matérielle d'appareils ou de supports contenant des données - 1,1 M$
- Utilisation inappropriée des ressources informatiques par un salarié - 581 000 $
- Partage inapproprié de données via des appareils mobiles - 464 000 $

Les violations de données en chiffres[2]

- 61 % des victimes de violation de données signalées dans le rapport 2017 sont des entreprises de moins de 1 000 salariés.
- 81 % des violations liées au piratage exploitent des mots de passe volés, faibles ou facilement devinables.
- 43 % des violations sont des attaques sociales.
- 66 % des programmes malveillants sont installés à partir de pièces jointes malveillantes.

1. « Rapport de l'enquête sur les risques informatiques mondiaux 2017 ». Kaspersky Lab et B2B International
2. « Rapport 2017 d'enquêtes sur la violation des données », Verizon

Sensibilisation efficace à la sécurité informatique

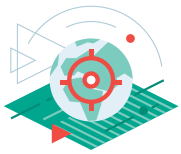
La formation du personnel est essentielle pour générer une prise de conscience des salariés et pour les motiver à être plus attentifs aux cybermenaces et aux contremesures, même s'ils estiment que cela ne fait pas partie des responsabilités liées à leur poste.

Malheureusement, de nombreux programmes de sensibilisation à la sécurité pèchent par manque d'efficacité. Les règles de sécurité sont en place, les informations les plus récentes sur les types de logiciels malveillants et de protection sont disponibles, les tactiques de protection pertinentes sont fournies, mais la formation ne produit pas les résultats escomptés. Quel est le problème ?

Pour les salariés, la sensibilisation à la sécurité est trop souvent synonyme de demi-journée devant un écran à faire semblant d'écouter une présentation PowerPoint tout en travaillant discrètement sur leur téléphone. Une telle formation est logiquement considérée comme une perte de temps et tout le monde continue d'agir comme avant.

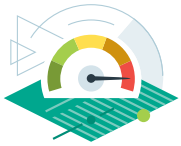
La sensibilisation à la sécurité est par ailleurs tout aussi inefficace lorsque les employés reçoivent une telle quantité d'informations qu'ils ne parviennent tout simplement pas à les absorber et adoptent en conséquence une attitude défaitiste.

Un programme de formation de sensibilisation à la sécurité efficace doit respecter 4 éléments clés :



Définir des objectifs de formation et justifier un programme

- Établir des objectifs mesurés par rapport à des repères
- Trouver un juste équilibre entre le niveau de compétence visé pour chaque groupe de salariés et le temps total d'apprentissage nécessaire pour les amener à ce niveau



Veiller à ce que tous les salariés atteignent au minimum leur niveau cible

- Utiliser l'apprentissage automatisé pour permettre à chaque salarié d'atteindre le niveau de compétence correspondant à son profil de risque
- Renforcer les compétences acquises afin qu'elles soient conservées
- Former les personnes individuellement, à leur propre rythme

Surveiller les progrès effectués grâce à des rapports exploitables et à des analyses

- Suivre en direct les données, les tendances et les prévisions
- Utiliser les prévisions en temps réel pour atteindre les objectifs de formation annuels
- Répondre aux questions avant qu'elles ne deviennent des problèmes (en identifiant les secteurs de l'organisation qui méritent davantage d'attention)
- Réaliser une analyse comparative des résultats provisoires

Garantir l'appréciation de la formation et, par conséquent, son efficacité

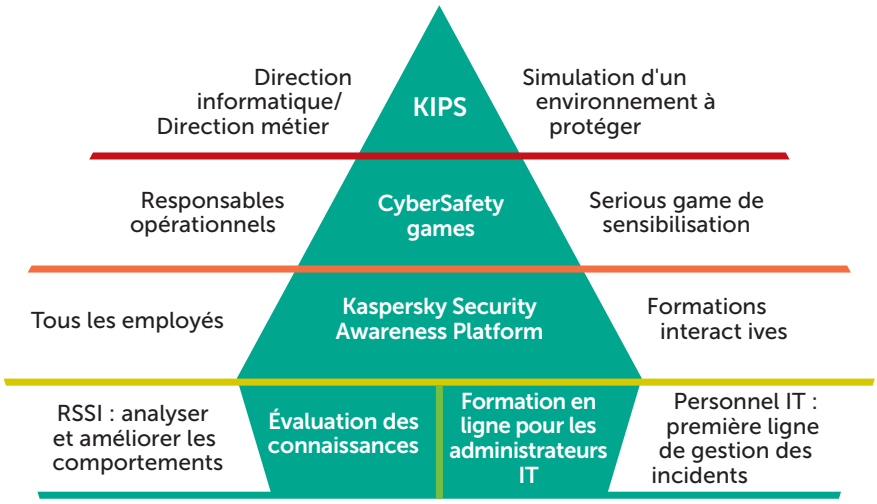
- Faire participer les salariés à la formation grâce à l'apprentissage ludique et l'émulation
- S'assurer que la formation est pertinente au quotidien
- Offrir la possibilité de comparer les résultats individuels avec d'autres résultats
- Éviter la surcharge d'informations

Comprendre comment fonctionne un processus d'apprentissage et d'enseignement permet de bâtir un programme d'enseignement efficace.

Kaspersky Lab propose des produits de formation sur ordinateur qui utilisent les techniques d'apprentissage les plus récentes et conviennent à tous les niveaux de la structure de l'entreprise. Non seulement nos programmes apportent des connaissances, mais plus important encore, ils contribuent à la formation des comportements nouveaux qui sont le véritable objectif de toute sensibilisation.

L'approche intégrale choisie par Kaspersky Lab est basée sur des techniques d'apprentissage modernes qui combinent le jeu, l'apprentissage par la pratique, la dynamique de groupe et le renforcement. Parmi ces techniques, l'apprentissage par le jeu est la plus importante car, en créant des liens émotionnels forts, elle permet de redéfinir les attitudes et d'établir de nouveaux modèles comportementaux qui renforcent l'envie d'apprendre.

Programmes pédagogiques de sensibilisation à la sécurité Kaspersky Lab



Une approche qui offre des résultats prouvés

Jusqu'à

90 %

de réduction du nombre total d'incidents

Au moins

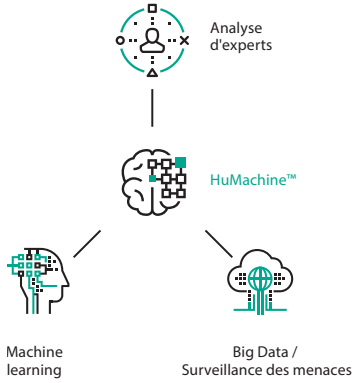
50 %

de réduction de l'impact financier des incidents

Une proportion exceptionnelle de

86 %

des participants recommandant le programme



Kaspersky Lab
pour les entreprises : **https://www.kaspersky.fr/enterprise-security**
Actualités des cybermenaces : **www.viruslist.fr**
Actualités de la sécurité informatique : **https://www.kaspersky.fr/blog/**
Kaspersky Security Awareness :
https://www.kaspersky.fr/enterprise-security/security-awareness

#truecybersecurity
#HuMachine

www.kaspersky.fr