LA FORMATION DE SENSIBILISATION À LA SÉCURITÉ EST ROMPUE.

POURQUOI LA GESTION DES RISQUES HUMAINS (GRH) EST LA NOUVELLE SOLUTION POUR CRÉER UNE ÉQUIPE AVERTIE EN MATIÈRE DE SÉCURITÉ.

usecure

www.usecure.io

Intro

Ne soyez pas dupe...

Les entreprises investissent plus que jamais dans le renforcement de leur résilience humaine face à l'évolution des cybermenaces, mais un gros problème afflige toujours les PME et les entreprises de tous les secteurs : les violations de données liées aux utilisateurs.

Même avec de plus en plus d'entreprises déployant des mesures de formation à la sensibilisation à la sécurité, 85 % des violations de données impliquent toujours l'élément humain (Verizon, DBIR 2021).

Mais quelle en est la raison ?

Dans ce guide, nous examinons pourquoi la formation traditionnelle de sensibilisation à la sécurité n'est souvent pas suffisante pour transformer le comportement des utilisateurs et comment les entreprises peuvent véritablement créer une main-d'œuvre avertie en matière de sécurité grâce à la nouvelle classe de sécurité centrée sur l'utilisateur...

Contenu

Pourquoi les entreprises modernes doivent-elles gérer les cyber-risques humains ?

Les employés jouent un rôle important dans la sécurité des systèmes et des données sensibles qui, entre de mauvaises mains, peuvent causer de graves dommages financiers, opérationnels et de réputation.

La mauvaise nouvelle est que les employés font des erreurs, Verizon déclarant que 85% des violations de données impliquent toujours l'élément humain.

Voici trois raisons pour lesquelles la gestion du cyber-risque humain est si vitale pour les entreprises d'aujourd'hui...

#1 L'erreur humaine est un gros problème

Qu'il s'agisse de fautes de frappe ou d'oubli de mots de passe, des erreurs au travail se produisent tous les jours.

Malheureusement, de prétendues petites erreurs comme le téléchargement d'une pièce jointe provenant d'un expéditeur inconnu ou la mauvaise direction d'un e-mail un vendredi après-midi épuisé peuvent provoquer plus qu'un simple visage rouge - IBM signalant que l'erreur humaine est une cause majeure dans 95% de toutes les violations. .

Qu'il s'agisse d'un manque de sensibilisation ou d'un manque de jugement momentané, les entreprises doivent former leurs utilisateurs pour réduire les erreurs coûteuses.

#2 Les employés enfreignent les règles

Parfois, le non-respect des règles peut être commis avec une intention malveillante, comme un ancien employé mécontent qui vole des montagnes de données et les vend à des escrocs ou à quiconque est prêt à acheter.

Selon le rapport sur le vol d'initiés d'IBM, les menaces d'initiés (y compris le vol de données d'employés) ont coûté aux entreprises 11,45 millions de dollars et les incidents ont triplé depuis 2016.

D'autres fois, les employés peuvent simplement essayer de prendre des raccourcis pour se faciliter la vie, par exemple en réutilisant le même mot de passe pour plusieurs comptes.

#3 Votre pare-feu humain peut être exploité

De nombreuses cyberattaques d'aujourd'hui visent à manipuler les employés, souvent avec des criminels utilisant des attaques de phishing pour usurper l'identité de clients, collègues, sous-traitants et fournisseurs.

Le plus délicat, c'est qu'il suffit d'une erreur d'un employé pour avoir des répercussions - les escroqueries par hameçonnage coûtant aux entreprises américaines des pertes ajustées de plus de 54 millions de dollars (rapport IC3 du FBI).

Les attaques telles que Business Email Compromise (BEC) et le phishing ciblé ne cesseront de se multiplier, Google signalant récemment qu'il existe désormais 75 fois plus de sites de phishing que de sites malveillants sur Internet.

Pourquoi la formation traditionnelle de sensibilisation à la sécurité échoue-t-elle souvent ?

Il est facile de penser que le déploiement de cours de sensibilisation à la sécurité et l'envoi de quelques bulletins par courrier électronique de temps en temps suffisent pour que les employés se comportent de manière plus sécurisée.

Mais la formation informatique sur la sensibilisation à la sécurité et les cyber-conseils envoyés à tous ne suffisent souvent pas pour vraiment renforcer la résilience des utilisateurs et favoriser un comportement humain sécurisé.

Voici pourquoi les mesures traditionnelles de formation à la sensibilisation à la sécurité échouent souvent :

Trop concentré sur le fait de cocher les cases

La formation traditionnelle des utilisateurs a été fortement axée sur la recherche du contenu de la formation, la prestation de la formation, puis (peut-être) le test de ce que les utilisateurs ont appris. Cette approche simpliste met davantage l'accent sur la prestation de formation plutôt que sur la fourniture d'une solution pour lutter contre le risque humain.

La formation est trop irrégulière

On peut demander beaucoup aux employés lorsqu'ils organisent un atelier annuel d'une heure. Le personnel est censé comprendre l'information, la conserver puis l'utiliser. Le problème, c'est que nous oublions tous des choses et que de nouvelles techniques d'attaque apparaissent tout le temps.

La formation est trop générique

Certains employés sont très vulnérables au phishing mais prudents avec l'hygiène des mots de passe. Certains employés ont des mots de passe faibles qu'ils réutilisent, mais oublient rarement de se déconnecter de leurs appareils. Le fait est que chaque employé a un ensemble unique de zones à risque. Les cours de formation envoyés à tous ne comblent pas les lacunes de connaissances de chaque utilisateur.

L'impact n'est souvent pas mesuré

C'est un gros problème. Comme tout dans la vie, si nous ne mesurons pas les performances, comment savons-nous que les choses s'améliorent ? Une fois la formation dispensée, il est important de mesurer ce que les employés ont réellement retenu.

Les cyberréflexes ne sont souvent pas testés

Tout comme les athlètes, les gens peuvent avoir fière allure à l'entraînement, mais comment cela se traduit-il en un événement réel ? Le déploiement de tests pratiques, tels que des simulations d'hameçonnage, est un moyen efficace de mesurer l'impact de la formation et de comprendre les risques en cours pour les attaques dans le monde réel.

La source des problèmes n'est pas abordée

61% des violations impliquent des identifiants d'utilisateur volés - comme des noms d'utilisateur et des mots de passe - dont beaucoup sont exposés sur le dark web. Ces informations d'identification sont ensuite utilisées pour alimenter les attaques d'ingénierie sociale et de spear-phishing contre les utilisateurs. Les programmes de sensibilisation à la sécurité ne traitent souvent pas ce problème, même s'il s'agit d'un atout extrêmement populaire qui fournit des munitions pour de nombreuses attaques.

Les politiques sont négligées

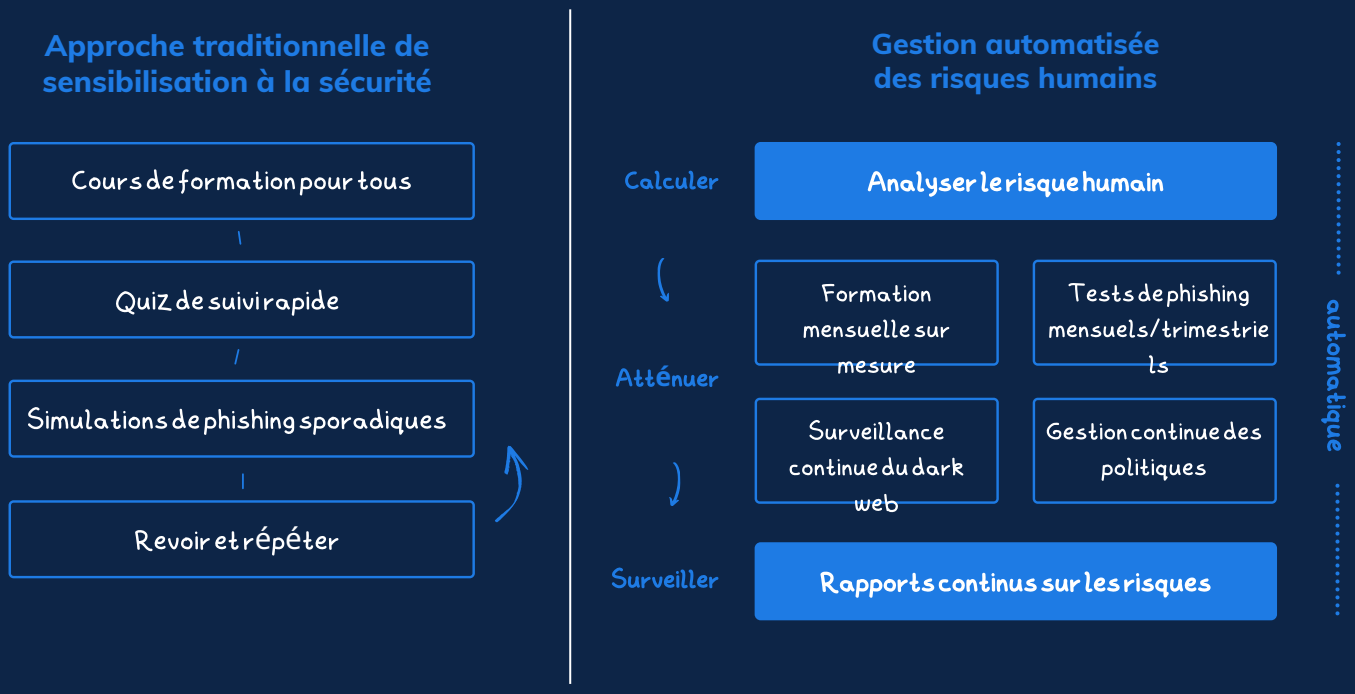
Parfois, les employés sont inconscients de leurs responsabilités en tant que rouage de sécurité clé de l'entreprise. Souvent, cela est dû à un manque de communication claire en ce qui concerne les politiques et les processus de sécurité. Les employés doivent comprendre quel comportement de sécurité est attendu d'eux et pourquoi cela est si important.

Comment la gestion des risques humains (GRH) fournit-elle la solution ?

> La gestion des risques humains est la nouvelle classe de sécurité centrée sur l'utilisateur qui permet aux entreprises de comprendre, de réduire et de surveiller les cyber-risques de leurs employés, sans avoir à sacrifier la productivité pour la protection.

Alors que les entreprises déploient généralement des programmes de formation à la sensibilisation à la sécurité pour réduire les risques des employés, GRH offre une solution complète pour transformer les humains en la meilleure défense d'une entreprise contre l'évolution des menaces.

Formation traditionnelle de sensibilisation à la sécurité VS la gestion des risques humains (GRH)



Comment fonctionne la GRH ?

La formation traditionnelle repose sur l'idée que l'humain est le « maillon le plus faible de la chaîne de la cybersécurité ». La gestion des risques humains repose sur la conviction que les humains constituent la meilleure ligne de défense d'une organisation contre les cybermenaces en constante évolution - votre entreprise a juste besoin des bons outils pour les y amener.

Les ingrédients clés pour faire fonctionner la GRH

Pour s'assurer que le cyber-risque des employés est continuellement traité, la plate-forme HRM d'usecure automatise les fonctionnalités suivantes :

Formation régulière de sensibilisation à la cybersécurité →
Des vidéos personnalisées et des programmes de formation interactifs sont créés pour chaque utilisateur, avec des cours de petite taille et des questionnaires de suivi envoyés automatiquement chaque mois.

Simulations de phishing périodiques des employés →
Des simulations de phishing régulières sont automatiquement déployées pour évaluer la vulnérabilité des utilisateurs à une gamme de techniques d'attaque. Des campagnes de phishing personnalisées peuvent être créées en quelques minutes.

Processus d'approbation des politiques clair →
Les politiques sont centralisées dans un endroit facilement accessible et le personnel est automatiquement informé de toute politique mise à jour qu'il doit signer, les signatures d'approbation du personnel étant suivies.

Surveillance continue des violations du dark web →
La surveillance continue du dark web détecte lorsque des données sensibles de l'entreprise (par exemple, les noms d'utilisateur et les mots de passe) sont apparues dans une violation de données, ce qui pourrait être utilisé pour des attaques ciblées.

Surveillance des risques humains →
Le risque humain est suivi en permanence, avec des rapports riches en informations et une notation du risque humain. Explorez en profondeur les performances d'entraînement et les tendances de phishing directement depuis votre tableau de bord.

Comment la GRH crée une main-d'œuvre avertie en matière de sécurité

Entraînement régulier de la taille d'une bouchée

Les micro-cours de formation sont automatiquement dispensés à chaque utilisateur chaque mois pour maintenir des formations fréquentes sans nuire à la productivité.

Formation personnalisée pour chaque utilisateur

Pour commencer, les lacunes dans les connaissances de base de chaque utilisateur en matière de sécurité sont évaluées lors d'un rapide quiz d'analyse des écarts de 10 minutes, puis, à partir de leurs réponses, un programme de formation continue et personnalisé est déployé avec des cours hiérarchisés.

Comprendre facilement le risque en cours

Avant de lancer votre programme de GRH, usecure calculera le score de risque humain de votre organisation pour donner une référence de la posture de sécurité de vos employés. Ensuite, plusieurs métriques (y compris le phishing, la formation et les résultats du dark web) sont fusionnées pour donner un aperçu de l'évolution du risque utilisateur au fil du temps.

Les utilisateurs sont testés contre les attaques du monde réel

Des simulations de phishing régulières sont automatisées pour aider à surveiller la vulnérabilité de chaque utilisateur à une gamme de techniques d'attaque en évolution.

Tenir les utilisateurs au courant de leurs responsabilités

La gestion des politiques et les communications sont simplifiées grâce à une bibliothèque de documents facile à parcourir et à un suivi automatisé des approbations de signature électronique qui élimine le temps et les tracas liés à la recherche des signatures du personnel.

Détectez les menaces des utilisateurs à un stade précoce

La surveillance continue du Web sombre détecte lorsque les informations d'identification des employés sont compromises et disponibles sur le Web sombre, avec des informations supplémentaires sur le service qui a conduit à la violation et le type de données exposées.

Comment usecure simplifie-t-il la GRH ?

Cela peut sembler un peu intimidant lorsqu'on pense au lancement, à la gestion et à l'évaluation d'une solution de gestion des risques.

C'est pourquoi la plate-forme de gestion des risques humains d'usecure utilise une approche automatisée et simplifiée qui facilite le déploiement et l'administration. Voilà comment cela fonctionne:

Ajouter les utilisateurs

Importez des utilisateurs et des groupes en quelques minutes grâce à des **intégrations faciles** et à de **simples téléchargements CSV.**

Calculer les risques

La vulnérabilité des utilisateurs est évaluée au moyen d'une **simulation de phishing** et d'une **analyse des brèches du dark web**, ainsi qu'au moyen **d'un questionnaire d'évaluation initiale de 10 minutes** qui met en évidence leurs faiblesses en matière de sécurité.

Réduire les risques

À l'aide des résultats de l'évaluation initiale de vos utilisateurs, des **programmes personnalisés de formation à la cybersensibilisation** sont déployés pour chaque utilisateur, les cours étant classés par ordre de priorité en fonction des zones à haut risque.

Surveiller les risques

Les mesures relatives au phishing, à la formation et aux brèches sont suivies en permanence et fusionnées dans un score holistique de risque humain, accompagné de communications sur les chartes informatiques afin de clarifier les responsabilités des utilisateurs.

Voir usecure en action

Regardez des démos miniatures pour découvrir comment usecure s'attaque au cyber-risque humain.

Regarder une démo»

Commencer aujourd'hui

Commencez à calculer le cyber-risque humain dès aujourd'hui

Regardez des petites démos pour découvrir comment usecure peut transformer le cyber-risque humain de votre organisation.

Commencer »

www.usecure.io