Cyberattaques : La prise de conscience n’est plus une option

Introduction

Le facteur humain est aujourd'hui l'élément le plus crucial de la cyber-sécurité, utilisé par la cybercriminalité pour s'infiltrer dans les organisations avec des stratégies offensives de plus en plus sophistiquées. En effet, ce sont précisément les utilisateurs, avec leurs comportements inadaptés à la complexité du défi, qui laissent inconsciemment le champ libre aux attaquants.

En analysant les différents rapports qui concernent l'état de la cyber-sécurité, la tendance qui émerge est que la croissance des cyberattaques semble imparable et que parmi les différentes techniques d'attaque utilisées, celles qui se caractérisent par une plus grande croissance s'appuient principalement sur le facteur humain.

La chronique est riche en cyberattaques réussies. Des attaques qui ont touché des organisations de tous les secteurs et de toutes les tailles. Des marques prestigieuses et d'autres moins connues ont vu leurs activités de production bloquées et leur réputation compromise. Il s'agit d'une véritable cyberguerre qui voit les attaquants dans une position d'avantage incontestable, d'autant plus que la première ligne de défense est constituée d'utilisateurs inconscients qui, dans la plupart des cas, n'ont même pas la perception d'être attaqués.

Lancer des programmes de sensibilisation à la cybersécurité efficaces et innovants, capables d'affecter les comportements humains et de transformer les utilisateurs en première ligne de défense des organisations, n'est plus une option.

L'objectif de la plateforme de sensibilisation à la cybersécurité de Cyber Guru est justement d'augmenter la résistance aux cyberattaques, à travers des parcours de formation permanente capables de développer chez les personnes la capacité à opérer avec des comportements sûrs guidés par une plus grande prise de conscience. Une plateforme constamment mise en œuvre qui utilise les technologies, les processus de production et les méthodologies pédagogiques les plus avancées pour assurer une implication maximale des utilisateurs et une protection contre les cyber-risques.

Michel Ruefenacht
VP Marketing

Le scénario

Les tendances relatives aux cyberattaques de ces dernières années montrent malheureusement une courbe en constante augmentation. Parmi les principales causes, il y a sans aucun doute l’utilisation accrue des technologies numériques, considérées comme le moteur d’une réelle croissance économique, à laquelle ne correspond cependant pas un niveau adéquat d’alphabétisation numérique des utilisateurs. Accélérer la tendance des effets de la pandémie, avec le recours massif au télétravail et à une utilisation accrue des applications et des services numériques.

Malheureusement, malgré les efforts considérables déployés par les organisations dans le domaine de la cybersécurité, il s’avère que le maillon faible de la chaîne de défense de toute organisation est encore aujourd’hui représenté par le facteur humain, et en particulier par les utilisateurs numériques. Il est désormais établi que plus de 90 % des cyberattaques peuvent être attribuées à une erreur humaine, à un comportement inapproprié.

90 % des cyberattaques commencent par un clic sur un mail malveillant

Barclays Bank

95 % des cyberattaques sont imputables à une erreur humaine

IBM Cyber Security Intelligence Index Report

Une chaîne est aussi forte que son maillon le plus faible

La résistance globale aux cyberattaques d’une organisation dépend donc de la résistance du facteur humain, aujourd’hui véritable maillon faible de la chaîne.

Le développement de la société numérique, avec ses risques, contraint toutes les organisations à s’étendre de manière cohérente sur le facteur humain, sur le niveau de conscience des personnes.

Un investissement devenu nécessaire pour combler le fossé culturel que les effets pandémiques et la transformation numérique rapide ont creusé.

En 2021, les violations de données ont coûté 45 milliards de dollars aux entreprises

Panda Security

Le nombre d’attaques de rançongiciels a augmenté de 13 % entre 2020 et 2021

Verizon Data Breach Investigations Report

Le coût mondial de la cybercriminalité atteindra 10,5 milliards de dollars d’ici 2025

Cybersecurity Ventures

La méthodologie

Lancer des programmes de sensibilisation à la cybersécurité efficaces et innovants, capables d’affecter les comportements humains pour transformer les utilisateurs en première ligne de défense des organisations, n’est plus une option.

La plateforme Cyber Guru a été conçue pour maximiser les processus d’apprentissage en développant 3 caractéristiques défensives de l’individu: la **connaissance**, la **perception du danger**, la **promptitude**.

Pour ce faire, des programmes de formation avancés, basés sur des méthodes innovantes de formation continue et d’engagement, sont nécessaires, afin de minimiser l’impact sur les fonctions de gestion de la formation du personnel et de la cybersécurité. Ce n’est qu’ainsi qu’il sera possible de suivre l’évolution constante des stratégies d’attaque de plus en plus sophistiquées.

3 PARCOURS DE FORMATION

Cognitif

La connaissance est gérée à travers un processus de formation cognitive basé sur une approche principalement didactique

Inductif

La perception du danger est stimulée par une formation inductive qui tend à agir sur la composante la plus émotionnelle de notre cerveau

Expérimental

Entraîner la préparation est essentiel pour agir rapidement en adoptant le bon comportement face à l’apparition d’un danger

Une plateforme complète de sensibilisation à la cybersécurité

La plateforme est conçue pour transformer les comportements de la main-d'œuvre de toute organisation publique ou privée, quelle que soit sa taille ou sa catégorie de produits, grâce à:

3 PARCOURS DE FORMATION FORTEMENT SYNERGIQUES ENTRE EUX

Cyber Guru Awareness

Un programme d'enseignement cognitif basé sur l'apprentissage en ligne qui garantit le développement progressif de la sensibilisation grâce à la connaissance des menaces du réseau et du schéma comportemental à adopter pour prévenir les attaques.

Cyber Guru Channel

Un programme de formation inductif qui génère de l'apprentissage grâce à la force de la narration et de la production vidéo. Suivant un schéma narratif typique des séries télévisées, l'apprenant apprend en s'identifiant dans les situations racontées dans les différents épisodes.

Cyber Guru Phishing

Un programme de formation expérientiel qui forme les individus à résister aux attaques d'hameçonnage dans leurs différents types. Le programme, automatique et adaptatif, permet à chacun de s'entraîner individuellement en fonction de ses expériences individuelles et de son niveau de résistance aux attaques.

Cyber Guru Awareness

Cyber Guru Awareness est conçu pour impliquer toute l'organisation dans un parcours d'apprentissage éducatif et stimulant, caractérisé par son approche « à libération constante et progressive » (Smart-School). Le parcours se compose de modules de formation auto-cohérents, chacun dédié à un sujet précis, avec une activation mensuelle pour une durée de 12/24/36 mois. Chaque module est à son tour composé de 3 courtes leçons vidéo de 5 minutes chacune. Les principales caractéristiques sont l'apprentissage cognitif efficace, l'implication maximale de l'apprenant et la supervision à impact zéro.

- **Modules de formation auto-cohérents avec activation mensuelle**
- **Engagement hebdomadaire minimal, compatible avec toutes les fonctions**
- **Micro-leçons vidéo au format multimédia**
- **Utilisation d'acteurs professionnels ayant des fonctions de coach**
- **Langage très vulgarisant**
- **Approche interactive avec une alternance continue entre les micro-leçons et les tests**
- **Questionnaire d'évaluation à choix multiples**
- **Méthodologie de ludification, avec organisation en équipe**
- **Plateforme multilingue**
- **Contenu supplémentaire et constamment mis à jour**

Cyber Guru Channel

La méthodologie inductive utilisée est basée sur l'immersion de l'utilisateur dans une situation réelle et sur un processus d'auto-identification avec la cybermenace, qui prend donc une forme concrète. L'utilisateur prend conscience non pas à travers une notion, mais à travers une narration, qui agit d'abord sur la perception du danger, puis sur l'élément conceptuel, en dépassant une arrière-pensée très dangereuse : « cela ne peut pas m'arriver ». Les trois principales caractéristiques sont l'apprentissage inductif efficace, l'implication maximale de l'apprenant et la supervision à impact zéro.

- **Formation continue**
- **Production vidéo avancée**
- **Plusieurs formats vidéo avec différentes narrations**
- **Épisodes courts**
- **Rythme narratif élevé**
- **Auto-identification dans des situations réalistes**
- **Approche Netflix-Like**
- **Documentation détaillée pour chaque épisode**
- **Reporting complet sur le niveau d'utilisation**
- **Fonctions de student caring automatique, pour motiver la participation**

Cyber Guru Phishing

Cyber Guru Phishing a été conçu pour former le personnel à résister aux attaques d'hameçonnage, par le biais de campagnes d'attaques simulées, personnalisées sur la base du profil comportemental de l'utilisateur individuel, grâce à l'utilisation d'un processus d'intelligence artificielle. L'apprenant augmente la résistance aux attaques par l'expérience, à la fois celle négative de l'erreur et celle positive de la reconnaissance de l'attaque. Les trois principales caractéristiques sont l'entraînement expérientiel efficace, l'entraînement personnalisé et la supervision sans impact.

- **Entraînement expérientiel efficace et continu**
- **Entraînement personnalisé par processus adaptatif**
- **Niveaux de difficulté et simulations personnalisées**
- **Campagnes d'attaque automatisées**
- **Erreur > Formation instantanée**
- **Procédure d'alerte**
- **Modèles préchargés**
- **Rapports analytiques et managériaux via un tableau de bord avancé**
- **Groupes à risque**
- **Politiques de remédiation**

Cyber Guru

Security Awareness Training That Works!

Suivez-nous sur LinkedIn | Youtube

En savoir plus sur Cyber Guru
cyberguru.it/fr/

Devenez notre partenaire
cyberguru.it/fr/partner/

Êtes-vous intéressé par une démonstration en direct de nos solutions ?

Réservez un rendez-vous de 30 minutes avec un Spécialiste de la formation sur la sensibilisation

RÉSERVEZ DÈS MAINTENANT