GoSecure

BROCHURE DE CAS D'UTILISATION

ÉDUCATION

LES CYBERATTAQUES SE MULTIPLIENT ET UN NOMBRE CROISSANT D'ÉCOLES EN SONT VICTIMES.

L'IMPACT DU HAMEÇONNAGE EN CHIFFRES :

29 %

Des attaques contre les établissements d'enseignement proviennent de l'exploitation de vulnérabilités et 30 % de campagnes de hameçonnage sur les écoles de la maternelle à la terminale en 2023.

53 MILLIARDS

Les attaques de rançongiciels contre l'enseignement primaire et secondaire et l'enseignement supérieur dans le monde ont causé plus de 53 milliards de dollars de coûts d'indisponibilité entre 2018 et la mi-septembre 2023.

6,7 MILLIONS

Ces attaques ont permis de brèche plus de 6,7 millions de dossiers personnels à travers 561 incidents.

Votre allié pour consolider, évoluer et prospérer

INFO@GOSECURE.AI

WWW.GOSECURE.AI

LES ATTAQUES D'HAMEÇONNAGE REPOSENT SUR L'ERREUR HUMAINE

Les statistiques suggèrent que si de nombreux éducateurs et membres du personnel respectent généralement les règles d'hygiène et d'utilisation sécurisée du courrier électronique, il y a toujours un petit nombre de personnes qui oublient ou négligent ces pratiques essentielles.

Un clic erroné sur un courriel suspect par un membre de votre école ou de votre district pourrait, sans le savoir, permettre à des cybercriminels d'accéder à votre réseau et à des informations sensibles.

Avec cet accès non autorisé, des acteurs malveillants pourraient voler les données des élèves et du personnel, perturber l'enseignement et les opérations administratives, ou nuire à la réputation de votre établissement.

Malgré les rappels fréquents en matière de sécurité informatique pour éviter de cliquer sur des courriels non sollicités, les pirates comptent sur la probabilité qu'au moins une personne de votre communauté éducative fasse confiance à une pièce jointe ou à un lien hypertexte d'apparence innocente.

RISQUES D'UN PLAN DE CYBERSÉCURITÉ FAIBLE :

- ATTAQUES PAR HAMEÇONNAGE
- COMPROMISSION DES COURRIELS D'ENTREPRISE
- LOGICIELS MALVEILLANTS AVANCÉS
- RANÇONGICIELS
- MENACES LIÉES À L'INGÉNIERIE SOCIALE
- FALSIFICATION DE MARQUE

Pire encore, les utilisateurs disposant de privilèges élevés pourraient par inadvertance donner aux attaquants les « clés du royaume ».

GoSecure

PROTÉGER L'ÉDUCATION AVEC GOSECURE

Grâce à des solutions sur mesure, à un engagement en faveur de l'innovation et à une compréhension approfondie des défis propres au secteur de l'éducation, GoSecure ouvre la voie en matière de protection des écoles et des institutions contre les cybermenaces.

DÉFIS

MANQUE DE RESSOURCES INFORMATIQUES

De nombreux établissements d'enseignement, en particulier les écoles primaires et secondaires, disposent souvent de budgets limités pour l'infrastructure et la sécurité informatiques. Ils sont donc vulnérables aux cyberattaques en raison de logiciels obsolètes, de pare-feu insuffisants ou d'un manque de personnel qualifié pour traiter les questions de sécurité.

AUGMENTATION DES ATTAQUES DE HAMEÇONNAGE ET DE RANÇONGICIELS

Les établissements d'enseignement sont de plus en plus ciblés par les escroqueries par hameçonnage et les rançongiciels. Les attaquants considèrent les écoles et les universités comme des cibles faciles en raison du volume élevé de communications numériques et de la sensibilisation souvent limitée du personnel et des étudiants à la cybersécurité.

PROTECTION DES DONNÉES SENSIBLES

Les écoles traitent des informations sensibles, notamment les données personnelles des élèves, du personnel et des parents. Veiller à ce que ces données soient stockées en toute sécurité et ne soient accessibles qu'au personnel autorisé est un défi permanent, d'autant plus que les systèmes deviennent de plus en plus complexes.

UN NOMBRE CROISSANT D'APPAREILS ET D'UTILISATEURS

Avec l'essor des outils d'apprentissage numériques, les élèves et le personnel accèdent aux réseaux scolaires à l'aide de plusieurs appareils personnels (ordinateurs portables, tablettes, téléphones intelligents, etc.). Gérer et sécuriser tous ces terminaux tout en empêchant les accès non autorisés est un défi majeur.

LA RÉPONSE DE GOSECURE

Les solutions avancées de détection des menaces de GoSecure peuvent surveiller les réseaux scolaires en temps réel, en identifiant les activités suspectes et en neutralisant les menaces avant qu'elles ne causent des dommages. Cette approche proactive aide les écoles à gérer les menaces de cybersécurité même avec des ressources internes limitées.

GoSecure offre de solides défenses contre les attaques de hameçonnage et de rançongiciels. Ses solutions de sécurité comprennent le filtrage des courriels et l'analyse des menaces pour détecter les messages et les liens suspects, ce qui permet d'éviter que le personnel et les étudiants ne soient victimes de ces stratagèmes.

GoSecure fournit des outils pour crypter les données sensibles et gérer les accès afin de s'assurer que seuls les utilisateurs autorisés peuvent accéder aux informations critiques. Cela permet de protéger les dossiers des étudiants, les informations personnelles et d'autres données confidentielles.

Avec davantage d'appareils accédant aux réseaux scolaires, GoSecure propose des solutions de sécurité des terminaux qui aident à protéger chaque appareil connecté au réseau. Cela réduit le risque de propagation des cyberattaques par le biais d'appareils vulnérables ou non protégés.

INFO@GOSECURE.AI

www.GOSECURE.AI

Votre allié pour consolider, évoluer et prospérer

Votre allié
pour consolider,
évoluer et prospérer

DÉTECTION ET RÉPONSE GÉRÉES ET ÉTENDUES GOSECURE TITAN[MC] (MXDR)

DÉTECTER ET ATTÉNUER PLUS RAPIDEMENT

La détection et réponse gérées et étendues GoSecure TitanMC (MXDR) offre le meilleur temps de réponse de sa catégorie, de la détection des menaces à l'atténuation, grâce à une solution qui identifie, bloque et signale les brèches potentielles.

Grâce à des alertes précoces, l'MXDR GoSecure TitanMC bloque de nombreuses attaques avant qu'elles n'aient un impact sur une organisation, tout en consolidant les données de sécurité critiques, en fournissant une visibilité inégalée et en offrant une protection éprouvée avec des vues personnalisables. Nous travaillons avec les équipes pour faire face à l'évolution des menaces, des technologies et des contraintes.

LES ATTAQUES DE HAMEÇONNAGE ÉTANT EN AUGMENTATION, LES EXPERTS ESTIMENT QUE PRÈS D'UN TIERS DES UTILISATEURS OUVRENT UN COURRIEL DE HAMEÇONNAGE ET QUE PLUS DE 10 % D'ENTRE EUX CLIQUERONT SUR UN LIEN OU OUVRIRONT UNE PIÈCE JOINTE

Inclus dans tous les offres MXDR GoSecure TitanMC, la Détection et réponse des boîtes de messagerie GoSecure TitanMC (IDR) offre aux utilisateurs un moyen plus rapide et plus facile de se débarrasser des messages douteux. Grâce à l'icône IDR GoSecure TitanMC toujours présente dans la barre d'outils de l'application Outlook, les utilisateurs se voient rappeler l'assistance disponible pour tout message qu'ils jugent un tant soit peu suspect.

Les messages sont examinés à la fois via des filtres d'apprentissage automatique et l'analyse experte de GoSecure afin que les utilisateurs puissent être assurés que le message est en sécurité à son retour ou qu'il soit supprimé en cas de menace.

Lorsqu'un statut de message est renvoyé à l'utilisateur en quelques minutes, sa conscience de la sécurité est renforcée et l'organisation est mieux protégée contre les violations. De plus, l'équipe de sécurité interne bénéficie d'une visibilité complète sur l'ensemble du processus sans lever le petit doigt.

En 2023, IDR GoSecure TitanMC a traité 123 745 courriels. Parmi ces courriels, 89 100 ont été considérés comme des menaces.

IDR GoSecure TitanMC permet aux utilisateurs de faire partie de la solution, tout en offrant le soutien dont les équipes internes ont besoin pour faire face à l'assaut des menaces par courrier électronique aujourd'hui. Grâce à une soumission facile depuis la boîte de réception, les utilisateurs bénéficient à la fois d'une analyse automatisée et d'une évaluation humaine professionnelle des messages douteux par l'équipe expérimentée de GoSecure.

UNE **FONDATION** SUR LAQUELLE VOUS POUVEZ FAIRE **CONFIANCE** ET SUR LAQUELLE VOUS POUVEZ **BÂTIR**

L'MXDR GoSecure TitanMC consolide les données de sécurité critiques, offre une visibilité inégalée et fournit une protection éprouvée avec des vues personnalisées. Nous travaillons avec les équipes pour faire face à l'évolution des menaces sophistiquées comme les rançongiciels et les attaques sans fichier, à l'évolution de la technologie et aux ressources limitées.

EN SAVOIR PLUS