KnowBe4

L'IA contre l'IA

Combattre les cybercriminels avec un programme de formation sur la sensibilisation à la sécurité alimenté par l'IA

L'IA contre l'IA : combattre les cybercriminels avec un programme de formation sur la sensibilisation à la sécurité alimenté par l'IA

✦ Sommaire

INTRODUCTION

L'IA offre aux cybercriminels une occasion rêvée de devenir encore plus dangereux. Des hypertrucages aux e-mails d'hameçonnage générés par l'IA et diffusés à grande échelle, cette technologie émergente est devenue une arme puissante qui fait désormais partie de l'arsenal des personnes malintentionnées du monde entier.

Heureusement, les professionnels de l'infosec comme vous disposent de plusieurs leviers pour agir. Vous appliquez sans doute déjà les puissants outils de l'IA à l'ensemble de vos technologies. Pourquoi ne pas utiliser aussi l'IA pour renforcer votre pare-feu humain ? La cybersécurité ne se réduit pas aux produits de sécurité que vous avez mis en place, mais englobe aussi les personnes qui les utilisent.

Le facteur humain joue un rôle essentiel pour la cybersécurité. Vous pouvez mettre à profit la puissance de l'IA pour impliquer les utilisateurs en leur dispensant des formations pertinentes et en les informant des évolutions des cyberattaques.

Ce document donne une vue d'ensemble des techniques utilisées par les personnes malintentionnées pour exploiter l'IA à leurs propres fins et présente les atouts qu'un programme solide de formation sur la sensibilisation à la sécurité et de simulation d'hameçonnage alimenté par l'IA peut apporter à une initiative de cybersécurité complète.

L'IA, NOUVELLE ARME D'UN PAYSAGE DES CYBERMENACES EN PLEINE ÉVOLUTION

À moins que vous n'ayez vécu ces dernières années totalement isolé du monde sur une île déserte, vous avez certainement lu des articles sur la myriade de méthodes élaborées par les cybercriminels pour exploiter l'IA générative et ses outils à des fins malveillantes.

L'IA est déjà utilisée pour promouvoir des campagnes de désinformation et de mésinformation, renforcer les attaques d'ingénierie sociale et automatiser des attaques multicouches et multifacettes à grande échelle, par des pirates informatiques qui ne possèdent parfois que très peu de compétences techniques.

Les leaders de l'infosec suivent cette actualité de très près. Selon un rapport récent de Netacea, entreprise spécialisée dans la détection des menaces, 93 % des professionnels de la sécurité interrogés pensent qu'ils seront confrontés à des attaques quotidiennes par IA dans les prochains six mois. À peine moins des deux tiers (65 %) pensent que l'IA offensive deviendra la norme.

✦ Comment l'IA booste les attaques par hameçonnage et l'ingénierie sociale

➔ Génération automatisée de contenus

- L'IA, notamment les modèles de traitement en langage naturel, est capable de générer des e-mails d'hameçonnage crédibles, corrects sur le plan grammatical et pertinents sur le plan du contexte. Les filtres antispam traditionnels peinent à les détecter comme malveillants.
- La recherche montre que les e-mails d'hameçonnage générés par l'IA ont un taux de réussite plus élevé que ceux rédigés manuellement. Un rapport de l'Agence de l'Union européenne pour la cybersécurité (ENISA) a ainsi révélé que l'IA peut générer à grande échelle des messages d'hameçonnage extrêmement personnalisés et cibler des personnes précises dont elle imite le style rédactionnel.

➔ Personnalisation du harponnage

- Les algorithmes d'IA sont capables d'analyser de grands volumes de données provenant des réseaux sociaux et d'autres sources en ligne pour recueillir des informations personnelles sur leurs cibles. Avec ces informations en main, les cybercriminels peuvent composer des e-mails de harponnage personnalisés et convaincants qui ont plus de chances d'induire leurs destinataires en erreur.
- Le rapport Data Breach Investigations Report (DBIR) de Verizon montre comment les attaques d'ingénierie sociale pilotées par l'IA peuvent exploiter des informations détaillées sur les centres d'intérêt, les relations et le comportement d'une personne pour améliorer leur taux de réussite.

➔ Automatisation des sites d'hameçonnage

- L'IA peut automatiser la création de faux sites web qui imitent les sites légitimes. Capables de s'adapter en temps réel pour ne pas être détectés et sembler plus authentiques, les faux sites augmentent ainsi leurs chances de voir les utilisateurs fournir leurs identifiants.
- Selon une étude publiée dans la revue Computers & Security, les sites d'hameçonnage alimentés par l'IA peuvent modifier leur apparence et leur comportement de façon dynamique, en fonction des interactions avec les utilisateurs et des données de renseignement sur les menaces afin d'échapper plus longtemps à la détection.

➔ Technologie des hypertrucages

- Les hypertrucages générés par l'IA peuvent créer des imitations audio et vidéo réalistes de personnes. Les cybercriminels les utilisent pour usurper l'identité de responsables ou de personnes de confiance, et convaincre leurs cibles de divulguer des informations sensibles ou d'autoriser des transactions.
- L'agence américaine de cybersécurité et de sécurité des infrastructures (Cybersecurity and Infrastructure Security Agency, CISA) a mis en garde contre le risque d'utilisation des hypertrucages dans les attaques d'ingénierie sociale, et observé leur sophistication croissante et les difficultés à les détecter.

L'IA est certes la nouvelle tendance du moment, mais elle n'est pour autant pas un vecteur d'attaque totalement inédit. Les pirates vont continuer d'utiliser l'hameçonnage généré par l'IA pour provoquer des réactions émotionnelles, la différence étant qu'ils vont agir à beaucoup plus grande échelle. Poussées par la peur, les victimes commettront des erreurs en effectuant des virements bancaires ou en introduisant des logiciels malveillants dans leurs systèmes. Enfin, le système de défense restera inchangé, c'est-à-dire qu'il continuera à surveiller les indices habituels d'une manœuvre d'ingénierie sociale.

Au vu des similitudes tactiques fondamentales des attaques, la puissance de l'IA se révèle vitale pour s'en défendre.

L'IA AU SERVICE DU BIEN : LES ROBOTS SONT NOS ALLIÉS

Face à des acteurs de la menace qui utilisent de plus en plus souvent l'IA à des fins malveillantes, les outils de cybersécurité s'adaptent pour tirer parti eux aussi de la puissance de l'IA.

L'un des domaines clés est la sécurité intelligente des e-mails. Le mode opératoire des filtres d'e-mail traditionnels consiste principalement à analyser les pièces jointes et à rechercher les signatures de logiciels malveillants connus. La sécurité des e-mails alimentée par l'IA va plus loin. Capable d'analyser le contenu des e-mails, elle évalue des schémas subtils et la sémantique pour identifier les tentatives sophistiquées d'ingénierie sociale.

L'IA et l'apprentissage automatique jouent également un rôle majeur dans la surveillance, l'analyse et la détection en temps réel des cybermenaces dans toute l'organisation. Les algorithmes d'IA peuvent ingérer et corréler en continu des volumes de données considérables provenant du trafic du réseau, des terminaux, des services cloud, etc. En d'autres termes, la détection optimisée par l'IA peut repérer très tôt les signes précurseurs de menaces et déclencher des alertes en temps réel, accélérant ainsi la réaction aux incidents.

Toutefois, l'aspect technique n'est qu'un des aspects de la lutte contre la cybercriminalité. L'IA doit et peut servir à renforcer votre surface d'attaque humaine.

L'IA À LA RENCONTRE DE L'HUMAIN : CRÉER UNE FORMATION INTELLIGENTE SUR LA SENSIBILISATION À LA SÉCURITÉ

Malgré les progrès de l'IA, l'infosec continue à se heurter à plusieurs défis :

- ➔ L'évolution rapide de la technologie de l'IA exige une vigilance constante de la part des utilisateurs.
- ➔ Les dispositifs de sécurité traditionnels peuvent s'avérer insuffisants face aux attaques alimentées par l'IA et nécessiter des tactiques de défense innovantes.
- ➔ Le manque de temps et de ressources des équipes de cybersécurité rend d'autant plus difficile de se tenir toujours au courant des menaces émergentes.

Heureusement, les progrès récents en matière de sensibilisation à la sécurité et les stratégies de simulation d'hameçonnage laissent entrevoir des espoirs. Les progrès de l'IA ouvrent des perspectives majeures pour les initiatives existantes de formation sur la sensibilisation à la sécurité, notamment :

✦ Formation et perfectionnement automatisés

Les formations sur la sensibilisation à la sécurité alimentées par l'IA peuvent simplifier considérablement le travail de l'administrateur en charge de la formation. Imaginez un système d'apprentissage adaptatif géré par l'IA, capable d'affecter automatiquement des formations aux utilisateurs en fonction de tout leur historique d'apprentissage : l'efficacité des modules de formation précédents, les résultats des derniers exercices de sensibilisation à la sécurité et les préférences d'apprentissage personnelles, telles que le format du contenu (vidéos, quiz, animations, jeux) et la durée, sont tous pris en compte pour composer une expérience sur mesure pour chaque utilisateur.

Les formations sur la sensibilisation à la sécurité alimentées par l'IA peuvent simplifier considérablement le travail de l'administrateur en charge de la formation.

Cette approche soulage l'administrateur en lui évitant certaines tâches, tout en proposant une formation plus pertinente pour l'apprenant, bien plus susceptible de l'inciter à s'intéresser au contenu et à en mémoriser les notions.

Une fois la formation principale dispensée, l'IA permet aussi de générer automatiquement des quiz de formation afin de renforcer l'assimilation du contenu. Les quiz peuvent être créés à partir du contenu de la formation elle-même ou des politiques de l'organisation, l'IA générative se chargeant de la majeure partie des tâches. L'objectif est de répéter les principaux points à retenir et de s'assurer que les informations sur les politiques sont réellement enseignées aux utilisateurs finaux, et pas seulement présentées.

✦ Campagnes de simulation d'hameçonnage optimisées

Considérez le moteur de recommandations alimenté par l'IA comme votre propre assistant d'hameçonnage IA. Il choisira automatiquement le meilleur test d'hameçonnage pour chaque utilisateur à un moment précis. Imaginez que vous créez une campagne d'hameçonnage sur mesure pour chacun de vos utilisateurs, avec des tests de simulation d'hameçonnage parfaitement personnalisés pour le niveau de chacun.

Et pourquoi s'arrêter aux campagnes générées par l'IA ? Des outils d'IA générative peuvent être incorporés à la création de modèles d'hameçonnage afin de garantir la diversité des modèles et la possibilité de les appliquer à grande échelle dans toute votre organisation. La capacité à s'adapter aux menaces émergentes et à créer de nouveaux modèles d'hameçonnage pour y réagir est cruciale dans un contexte où les vecteurs de menace sont en constante évolution.

✦ Duo IA et veille collaborative

Un élément clé d'un programme robuste de formation sur la sensibilisation à la sécurité est la possibilité pour les utilisateurs de signaler à la fois les e-mails de simulation d'hameçonnages et les vrais e-mails reçus. Vos utilisateurs ont la volonté de lutter à vos côtés dans cette bataille de la cybersécurité : vous devez donc leur offrir les outils qui vont leur permettre de défendre proactivement votre environnement.

Des outils d'IA générative peuvent être incorporés à la création de modèles d'hameçonnage afin de garantir la diversité des modèles et la possibilité de les appliquer à grande échelle dans toute votre organisation.

Cette action collaborative permet aux utilisateurs de signaler ces campagnes d'hameçonnage plus rapidement qu'avec les méthodes conventionnelles. Associée à un outil de sécurité des e-mails alimenté par l'IA, la veille mutualisée améliore l'IA en donnant aux utilisateurs et aux équipes de sécurité les moyens d'identifier, de valider et de collecter de grandes quantités de données (dans ce cas précis, pour signaler des e-mails suspects et des e-mails malveillants).

Ainsi, la veille sur les menaces d'hameçonnage étayée par une analyse basée sur l'IA permet de protéger votre organisation contre les attaques par hameçonnage de nouvelle génération. Cette méthode permet de réagir plus rapidement et de façon proactive à la vague des toutes dernières attaques d'hameçonnage visant votre organisation.

RÉSULTAT : L'IA, UNE RÉALITÉ INCONTOURNABLE

L'impact de l'IA sur la société ne relève plus de la théorie. Elle est désormais une réalité. Il ne s'agit plus de savoir si vous devez l'intégrer à vos initiatives de cybersécurité et de formation sur la sensibilisation à la sécurité**,** mais *quand* vous devez le faire.

Les organisations doivent combattre le feu par le feu. En incorporant la puissance de l'IA à leurs programmes de formation sur la sensibilisation à la sécurité, les entreprises peuvent gérer leur risque humain et garder une longueur d'avance sur les cybercriminels.

Enfin, investir dans la sensibilisation à la sécurité optimisée par l'IA, c'est choisir une stratégie essentielle pour entretenir une culture solide de la sécurité et se défendre contre les redoutables cybermenaces d'aujourd'hui et de demain.

EN SAVOIR PLUS → **Découvrez l'approche de KnowBe4 en matière de sensibilisation à la sécurité alimentée par l'IA**

Ressources supplémentaires

Test de sécurité gratuit relatif à l'hameçonnage
Découvrez le pourcentage de Phish-Prone (pourcentage de vulnérabilité à l'hameçonnage) de vos employés, en profitant de votre test de sécurité gratuit relatif à l'hameçonnage.

Aperçu gratuit de la formation
Découvrez notre bibliothèque complète de contenus sur la sensibilisation à la sécurité, avec des options de consultation et de recherche par titre, catégorie, langue ou contenu.

Programme automatisé de sensibilisation à la sécurité gratuit
Créez un programme de sensibilisation à la sécurité, personnalisé pour votre organisation.

Outil Phish Alert Button gratuit
Un seul clic suffit désormais à vos employés pour signaler les attaques par hameçonnage de manière sécurisée.

Outil Domain Spoof Test gratuit
Déterminez si les pirates peuvent usurper une adresse e-mail de votre domaine.

À propos de KnowBe4

KnowBe4 offre à votre personnel les moyens de prendre au quotidien des décisions plus éclairées en matière de sécurité. Des dizaines de milliers d'organisations dans le monde font confiance à la plateforme KnowBe4 pour renforcer leur culture de la sécurité et réduire le risque humain. KnowBe4 crée une couche dite « humaine » de défense afin que les organisations puissent renforcer les comportements des utilisateurs en les sensibilisant à la sécurité de façon inédite, et en les formant à la conformité.

Le déploiement de KnowBe4 rend les utilisateurs vigilants et attentifs aux dommages causés par l'hameçonnage, les rançongiciels et les autres menaces découlant de l'ingénierie sociale. La plateforme comprend une suite complète de programmes de sensibilisation et de formation à la conformité, un coaching des utilisateurs en temps réel, une simulation d'ingénierie sociale optimisée par l'IA et une défense anti-hameçonnage basée sur des actions collaboratives.

Offrant du contenu en plus de 35 langues, KnowBe4 fournit la plus grande bibliothèque au monde, toujours actualisée avec du contenu engageant vous permettant de renforcer votre pare-feu humain.

Pour en savoir plus, consultez la page www.KnowBe4.com

KnowBe4

KnowBe4 NL, BV | Central Park, Stadsplateau 27-29, 3521 AZ Utrecht, Pays-Bas
Tél. : +31 (0)30 7996074 | www.KnowBe4.com | E-mail : Sales@KnowBe4.com

© 2024 KnowBe4, Inc. Tous droits réservés. Les autres noms de produits et de sociétés mentionnés dans ce document peuvent être des marques commerciales et/ou des marques déposées de leurs entreprises respectives.

08E06K01