Mutualiser nos forces,
assurer l'avenir

IA & Cybersécurité

02/09/2024

Enjeux de l'IA dans le monde de l'assurance

L'intelligence artificielle (IA) occupe une place de plus en plus importante chez Covéa. En tant que leader dans le secteur de l'assurance, Covéa s'engage à intégrer les technologies de pointe pour améliorer ses services et répondre aux besoins de ses clients. L'IA est au cœur de cette transformation, offrant des opportunités pour optimiser les opérations, anticiper les besoins et renforcer la sécurité.

Pourquoi l'IA est un axe métier stratégique pour Covéa (depuis 2022)?

- **Automatisation et accélération des processus internes :** l'automatisation de tâches telles que **la conclusion de contrats, la vérification de documents ou la gestion des sinistres** permet d'améliorer l'efficacité tout en réduisant les délais de traitement.
- **L'amélioration de l'expérience client :** une analyse des données historiques et l'utilisation de modèles prédictifs menées par l'IA permet d'affiner et de **personnaliser les offres de façon à s'approcher d'un modèle sur mesure** avec une approche plus proactive dans la conception des produits et une tarification plus précise permettant de fidéliser le client. Cela peut passer par l'utilisation **de chatbots alimentés par IA**, en mesure de répondre (en contextualisant l'échange) à une grande partie des interrogations et ce à toute heure.
- **La prévention des risques :** compte tenu de l'évolution de la société (usages, produits, mobilités) et des bouleversements climatiques, la prévention des risques est un enjeu majeur pour l'assurance. Les algorithmes sophistiqués des IA permettent aux compagnies de détecter les signaux faibles et les comportements suspects et donc de signaler ou non un potentiel danger (fraude, zone inondable d'ici quelques années…).

…. mais pas que!!

L'IA impacte de manière importante le monde de la cybersécurité, apportant son lot de risques significatifs de par des attaques de plus en plus sophistiquées (IA offensive) mais offrant également des opportunités de renforcement de la cybersécurité (IA défensive)

Rappel: la cybersécurité dans les banques et assurances; un enjeu majeur

1. Protection des données clients
2. Prévention des pertes financières
3. Préservation de la réputation
4. Un cadre réglementaire et législatif de plus en plus contraignant

Quelques prévisions (*source Gartner*):

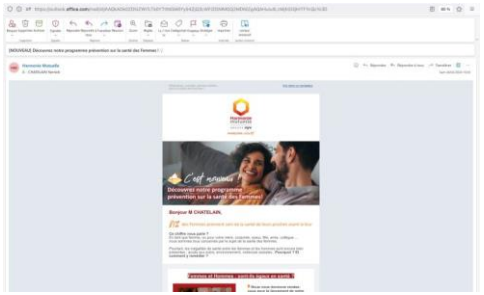
2026: suite aux attaques utilisant des deepfakes générés par l'IA sur la biométrie du visage, 30 % des entreprises ne considéreront plus ces solutions de vérification d'identité et d'authentification comme fiables de manière isolée
2028: l'IA multiagents dans la détection des menaces et la réponse aux incidents passera de 5 % à 70 % des implémentations d'IA pour principalement augmenter, et non remplacer, le personnel.

IA offensive

Une évolution constante de la menace

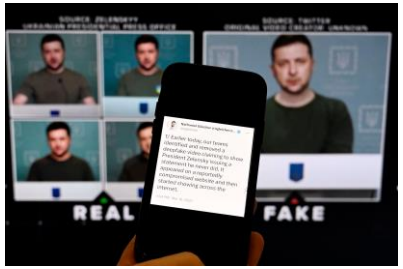
***Utilisation de systèmes d'intelligence artificielle pour assister ou exécuter des activités nuisibles**, automatiser l'exploitation de vulnérabilités et augmenter l'efficacité des opérations offensives, allant des cyberattaques aux campagnes de désinformation et à la manipulation de l'opinion publique*

Types d'attaques courantes/connues par le grand public



1 - Phishing (mail)/Vishing(message audio)/Smishing(attaques par SMS) « améliorés » (traductions, orthographe soignée, noms de domaine…) et « personnalisé » (reconnaissance du genre, de l'âge, de la situation socio économique) au travers de l'exploitation de données issues de l'OSINT (e.g phishing de Harmonie mutuelle en février 2023).

Objectifs: usurper l'identité de la victime, prise de contrôle de l'appareil et vol de données et fichiers (ransomware, chantage), mise en place d'une arnaque financière.



2- Deepfake: utilisation de données audio (10-15 secondes suffisent) et/ou photo/vidéos permettant de simuler une interaction numérique auprès d'une victime ou d'un système de protection. Evolution de « l'arnaque au président » ayant dans certains cas permis le versement de forts montants (p.e transfert de US$ 25M à Hong Kong en février 2024 suite à une conférence vidéo entièrement créée et animée par une IA). Utilisation de technologies liées à l'IA sur du matériel vidéo permettant notamment de bypasser certains mécanismes d'authentification.

Objectifs: vols mais également usurpation d'identité. Très utilisé également pour de la désinformation et de la déstabilisation politique

Des vecteurs d'attaque multiples…

- Identification des vulnérabilités
- Automatisation de l'exploitation des failles
- Propagation rapide d'information/contenu à travers le réseau
- Eviction de la détection par changement de comportement
- Ciblage d'attaques sur parties spécifiques de l'infrastructure

…pour des cibles parfois un peu moins évidentes

- Ciblage de plateformes cloud possédant de très grosses quantités de données sensibles/personnelles (données de santés comme p.e hôpitaux)
- Acteurs de grand événements à forte audience (p.e JO, billetteries, hébergements,…)
- Moteurs d'IA générative plus éthiques afin de participer à du poisoning ou bien à du détournement d'information

IA défensive

Anticiper et apprendre pour rester à la pointe de la défense

***Utilisation de systèmes d'intelligence artificielle pour détecter, prévenir et répondre aux cybermenaces**, renforcer la sécurité des systèmes et automatiser les mesures de défense*

L'intelligence artificielle, un élément devenu central dans la cybersécurité

Une stratégie d'IA défensive a pour objectifs principaux l'agilité, la proactivité, l'anticipation et l'apprentissage. Elle contribue à l'amélioration continue de la sécurité, en complément des équipes existantes (SOC, exploitation), en agissant, entre autres, sur les aspects suivants:

- **Détection des menaces**

Utilisation d'algorithmes de Machine Learning (ML) au niveau des systèmes de gestion des informations de sécurité (SIEM) qui permettent **d'analyser les journaux et le trafic réseau en identifiant des indicateurs de compromission (IoC)** qui pourraient passer inaperçus par un traitement humain.

- **Prévention des attaques**

L'IA permet une approche proactive grâce aux analyses prédictives. Les algorithmes d'IA permettent aux équipes de cybersécurité **d'anticiper certains vecteurs d'attaque potentiels en analysant les données historiques** d'autres attaques en les enrichissant de flux de renseignements extérieurs.

- **Réponse automatique aux incidents**

L'automatisation pilotée par l'IA (via l'utilisation d'un SOAR) permet de **prioriser les alertes, déterminer la nature de la menace et même initier des actions de remédiation** sans aucune intervention humaine. Chez Covéa, les cas les plus fréquents concernent la détection potentielle de ransomwares ainsi que l'analyse des attaques de phishing.

- **Renforcement de la sécurité des données**

Les outils de DLP (Data Loss Prevention) sont maintenant capables **d'analyser et de reconnaitre des patterns associés à des informations à caractère personnel** (même au niveau des images) et sont en mesure d'analyser le bon usage qu'il en est fait au travers du système d'information de l'entreprise et ensuite d'identifier ou d'alerter les équipes en cas de suspicion de fuite d'informations.

- **Apprentissage continu et adaptation**

La capacité d'apprentissage adaptatif des systèmes d'IA en cybersécurité leur permet d'**affiner les stratégies de détection et de réponse aux menaces en mettant à jour leurs modèles de détection** basées sur les nouvelles tactiques, techniques et procédures (TTP) en utilisant des algorithmes de deep leaning et de reinforcement learning et ce en toute autonomie

Merci

Mutualiser nos forces,
assurer l'avenir