# CYBERATTAQUES : CES NOUVELLES TECHNIQUES QUI VISENT TOUT LE MONDE

Vendredi 17 janvier 2025

AURYS

LE PROGRÈS

***Selon le dernier rapport annuel sur la gestion des cyber-risques de la compagnie d'assurances Hiscox, les cyberattaques contre les entreprises sont en hausse alarmante avec 67 % des sociétés touchées au cours de l'année écoulée. Cette tendance inquiétante met en lumière l'évolution constante des techniques utilisées par les cybercriminels, en particulier les fraudes sophistiquées comme celles aux faux conseillers bancaires et le spoofing de fournisseurs.***

## Qu'est-ce qu'une cyberattaque ?

« Une cyberattaque est une tentative malveillante d'exploiter les vulnérabilités des systèmes informatiques d'une entreprise pour voler des données, extorquer et/ou détourner de l'argent ou perturber les activités d'une entité. Ces attaques peuvent prendre diverses formes, allant du simple piratage de compte à des opérations plus complexes impliquant même l'intelligence artificielle générative. ».

## Quelles sont les techniques de cyberattaque les plus courantes ?

« Parmi les méthodes les plus répandues, on trouve notamment :

**1. Le phishing (hameçonnage)** qui consiste à envoyer des messages frauduleux pour obtenir des informations sensibles (code d'accès et mot de passe notamment) ;

**2. Les ransomwares (rançongiciels)** qui sont en fait des logiciels malveillants qui chiffrent les données afin d'exiger et obtenir une rançon ;

**3. Les attaques dites « DDoS »** qui ont pour objectif une submersion des serveurs d'une entreprise pour rendre les services d ' un site Internet inaccessibles ce qui peut être très préjudiciable pour un site marchand ;

**4. Le spoofing,** une usurpation d'identité d'un tiers vis-à-vis d'une cible. Cette technique utilise les outils issus de l'ingénierie sociale comme la manipulation psychologique et la crédulité de certaines victimes pour obtenir des informations confidentielles. On rencontre cette menace dans le cas des fraudes « au faux conseiller bancaire » et « au faux fournisseur ».

## Quels sont les nouveaux procédés employés ?

« Les cybercriminels innovent constamment. Deux techniques émergentes méritent une attention toute particulière de la part des chefs d'entreprise :

**1. La fraude au faux conseiller bancaire.** Dans ce cas, un escroc se fait passer pour un conseiller bancaire, gagne la confiance de la victime et l'incite à effectuer des transactions frauduleuses. Pour cela, les cybercriminels envoient fréquemment un SMS ou un mail avec un faux formulaire administratif afin de recueillir les informations de la victime (ou utilise le « Darknet » pour récupérer ces informations). Quelques jours après, l'escroc contacte la victime et se fait passer pour un conseiller bancaire en affichant le numéro de téléphone (voire le nom) de l'agence bancaire de la victime. Il la rassure en validant notamment son identité à l'aide des informations qu'il a recueillies sur elle au préalable grâce au formulaire ou via le « Darknet ». Une fois qu'il a gagné sa confiance, il l'invite à annuler les « soi-disant virements frauduleux » directement via son application bancaire. Mais en réalité, cela permet à l'escroc de valider les transactions frauduleuses qu'il est en train d'effectuer sur le compte de la victime.

**2. Le spoofing de fournisseur ou de prestataire de services ou de faux clients.** Dans ce cas, les fraudeurs se font passer pour des fournisseurs avec qui vous faites ou avez déjà fait affaire et demandent de modifier les coordonnées bancaires pour détourner les paiements. Ce type de fraude peut prendre différentes formes :

- **L'envoi de fausses factures** paraissant authentiques (coordonnées, numéros de compte et logos d'entreprise…) ou de vraies factures détournées et falsifiées pour notamment changer/modifier les coordonnées bancaires de paiement ;
- **L'achat de produits ou de services à votre entreprise en utilisant une fausse identité et de fausses informations de paiement et coordonnées de livraison.** Une fois les marchandises reçues, le fraudeur disparaît sans vous payer ! Autre technique utilisée : le fraudeur se présente comme un partenaire commercial potentiel proposant des opportunités d'investissement ou de partenariat. Il vous demande de verser des frais initiaux ou de lui communiquer des données confidentielles afin de lancer la négociation. Il disparaît ensuite, une fois les fonds transférés et les informations communiquées. »

## Quel rôle joue l'IA dans les cyberattaques ?

« L'intelligence artificielle devient un outil puissant pour les cybercriminels. Elle permet de créer des « Deepfakes » convaincants et d'améliorer la sophistication des attaques. Les modèles d'IA générative sont désormais utilisés pour produire des contenus vidéos et audios malveillants encore plus réalistes et très difficiles à détecter. Un exemple frappant de fraude par « Deepfake » contre une entreprise s'est produit à Hong Kong en 2024. Un employé d'une multinationale a été victime d'une arnaque sophistiquée impliquant une fausse visioconférence. Les escrocs ont utilisé la technologie « Deepfake » pour créer des vidéos réalistes de cadres supérieurs de l'entreprise, y compris le directeur financier basé au Royaume-Uni. Lors de cette visioconférence, l'employé a reçu l'ordre d'effectuer des transferts d'argent vers des comptes bancaires spécifiques. Croyant obéir à ses supérieurs, l'employé a effectué 15 transactions sur cinq comptes bancaires différents, pour un montant total de 200 millions de dollars hongkongais (environ 24 M€). Ce n'est qu'après avoir contacté ses vrais collègues que l'employé a réalisé qu'il avait été victime d'une fraude. Cette arnaque démontre le potentiel dangereux des « Deepfakes » dans le contexte professionnel, où la confiance et l'obéissance à la hiérarchie peuvent être exploitées par des criminels utilisant des technologies avancées d'intelligence artificielle. »

**Laurent Colas, expert-comptable dans l'Ain, détaille pour nous cette tendance.**

LE PROGRÈS

## Quel est l'impact pour les entreprises ?

« Pour une entreprise, les conséquences d'une cyberattaque peuvent être dévastatrices. On peut notamment citer :

- Pertes financières directes (détournement, paiement d'une rançon…) ;
- Atteinte à la réputation (dénigrement, perte de confiance des tiers…)
- Perturbation des activités (partielle dans le meilleur des cas et voire totale dans de nombreuses situations) ;
- Fuite de données sensibles (code d'accès, mot de passe, coordonnée bancaire…) ;
- Coûts de remise en état des systèmes qui sont trop souvent sous-estimés par les entreprises. »

## Comment faire face à ces menaces ?

« Pour se protéger, les entreprises doivent adopter une approche proactive :

- Former régulièrement les employés aux bonnes pratiques de cybersécurité ;
- Mettre en place des systèmes de sécurité robustes et les maintenir à jour ;
- Effectuer des audits de sécurité réguliers ;
- Établir un plan de réponse aux incidents ;
- Souscrire à une cyber-assurance adaptée ; dans tous les cas, il convient impérativement de :
- Vérifier systématiquement l'identité des interlocuteurs pour toutes les transactions financières, et ce, quel que soit le montant ;
- Mettre en place des procédures de vérification pour tout changement de coordonnées bancaires des fournisseurs.

Face à l'évolution rapide des menaces cybernétiques, la vigilance et l'adaptation constante des mesures de sécurité sont cruciales pour toute entreprise, quelle que soit sa taille. La cybersécurité n'est plus une option, mais une nécessité absolue dans le paysage entrepreneurial actuel. »

## Repère : Qui est visé ?

Quels profils d'entreprises sont visés ?
« Contrairement aux idées reçues, toutes les entreprises sont des cibles potentielles, souligne Laurent Colas. Cependant, les PME et TPE sont particulièrement vulnérables. Selon un des derniers rapports de la CNIL, les secteurs les plus touchés sont :

- Les activités spécialisées, scientifiques et techniques (21 %) ;
- La santé et l'action sociale (18 %) ;
- Les administrations publiques (12 %) ;
- Le secteur financier et de l'assurance (10 %). »