Communiqué de presse
Le 3 décembre 2024

Ebook Anozr Way sur les Deepfakes : les entreprises en première ligne

Le nombre de deepfakes pourrait passer de 500 000 en 2023 à 8 millions en 2025[1]

Comme les autres attaques par ingénierie sociale, les deepfakes se nourrissent de l'empreinte numérique des individus : données en ligne, réseaux sociaux, vidéos, photos, infos émanant de l'entourage familial, amical et professionnel... Toutes ces données sont la matière première à partir de laquelle, grâce à l'IA, un hacker va pouvoir créer le double numérique d'un individu et fomenter un scénario d'attaque crédible. 2ème risque économique mondial, après le changement climatique[2], les deepfakes représentaient 500 000 tentatives de fraudes en 2023, soit une augmentation de 3000%[3]. Ce nombre pourrait atteindre 8 millions en 2025, selon Deepmedia. Les entreprises sont en première ligne : infobésité, exploitation des biais cognitifs des collaborateurs et difficultés à imaginer des mensonges émanant de sa hiérarchie.

La prévention, moyen le plus efficace pour lutter contre les deepfakes

La sensibilisation aux deepfakes est cruciale pour se protéger contre leurs effets néfastes. Comprendre leur fonctionnement et leur impact est le premier pas vers une meilleure défense.

Les technologies développées par ANOZR WAY permettent à chaque collaborateur d'avoir la visibilité sur ses propres informations professionnelles et personnelles qui circulent sur le web et le darkweb. Ils ont aussi la possibilité de corriger leurs vulnérabilités en temps réel.

Les deepfakes ou attaques par ingénierie sociale dopées à l'IA portent leur efficacité à un niveau inégalé. En 2019, leur impact sur l'économie mondiale s'élève à 78 milliards de dollars[4]. Les deepfakes s'appuient sur L'Open Source Intelligence (OSINT) pour collecter les informations sur leurs cibles, et sur la démocratisation de l'IA générative pour déployer plusieurs techniques de manipulation : imitations de voix, synchronisation labiale, génération de fausses images ou vidéos…

[1] Source : Deepmedia
[2] Source World Economic Forum 2024
[3] Source Onfido
[4] The Economic Cost of Bad Actors on the Internet : Fake News in 2019

Les dirigeants, cible privilégiée des deepfakes

En mai 2024, le PDG du plus grand groupe publicitaire mondial, Mark Read, a été la cible d'une tentative de fraude sophistiquée impliquant un deepfake vocal alimenté par intelligence artificielle. En créant un compte WhatsApp avec une photo publique de Mark Read, et en utilisant un clone vocal combiné à des séquences vidéo de YouTube, les fraudeurs ont organisé une réunion sur Microsoft Teams semblant impliquer le PDG et un autre dirigeant. Si la fraude a échoué, l'attaque montre le niveau d'exposition des dirigeants : les membres des Comex/ Codir font l'objet de 12 fois plus d'attaques cyber que les autres collaborateurs d'une entreprise.

2 dirigeants sur 3 disposent d'un ou de plusieurs comptes publics sur les réseaux sociaux et certains y sont même particulièrement actifs. Ils y publient des textes, mais aussi des photos, des podcasts, et des vidéos. Par recoupement, il devient alors très facile d'obtenir un maximum d'informations sur leur vie professionnelle, mais aussi personnelle. **1 dirigeant sur 2 est ainsi exposé à un risque élevé d'usurpation d'identité.** *"La meilleure prévention consiste à prendre conscience du niveau de risque auquel on est exposé en tant que dirigeant ou collaborateur. Cette prise de conscience permet de prendre les bonnes décisions et d'acquérir les bons réflexes pour se protéger soi-même, mais aussi l'entreprise et les équipes placées sous notre responsabilité." Philippe Luc, co-founder & CEO d'ANOZR WAY*

Quand les deepfakes jouent avec les émotions : le danger de la manipulation

Les deepfakes représentent une menace sérieuse pour notre perception de la réalité, car ils peuvent être utilisés pour manipuler l'esprit humain de manière insidieuse. Une série d'études révèle que même une simple imitation de voix peut avoir un impact profond sur les pensées et les émotions des auditeurs.

"Les deepfakes représentent une menace complexe qui ne se limite pas à la tromperie visuelle ou auditive, mais s'enracine profondément dans les biais cognitifs qui influencent notre perception du monde." Nathalie Granier, Threat Intelligence & Human Behavioral Researcher chez Anozr Way

L'une des raisons principales qui nous rendent vulnérables aux deepfakes réside dans notre tendance à surestimer notre capacité à identifier des mensonges sophistiqués, les êtres humains ayant une propension innée à faire confiance à ce qu'ils voient et entendent. **50 % des personnes exposées aux deepfakes ne reconnaissent pas qu'elles sont manipulées**[5]. A cela s'ajoute l'infobésité, sollicitant continuellement le cerveau humain et abaissant notre vigilance.

Enfin, les deepfakes, parfaits outils de manipulation, s'attaquent directement à notre système émotionnel. L'objectif est de créer en nous des émotions fortes : la colère, la peur, l'indignation ou l'admiration pour court-circuiter notre esprit critique.

[5] Nightingale, Wade, & Watson (2021)

Une recherche de Stanford University a démontré que **les vidéos qui provoquent des émotions fortes sont 35 % plus susceptibles d'être partagées**. Selon une autre étude de l'Université de Harvard, **75 % des gens partagent des informations qui suscitent des émotions fortes sans en vérifier la véracité**.

La reconnaissance des émotions, telles que le bonheur, la peur, la tristesse et la colère, est similaire entre les deepfakes et les vidéos originales[6]. Les deepfakes de la tête entière et les fakes de marionnettes, même entièrement synthétisés, suscitent des réponses comportementales comparables à celles des vidéos originales.

Cette nouvelle forme de manipulation peut toucher de nombreux aspects de la vie d'une entreprise, de la chute des actions en bourse à la perte de contrats, en passant par la démotivation des salariés.

« Il faut 20 ans pour construire une réputation et cinq minutes pour la ruiner.' Warren Buffet

Etude complète disponible sur demande : violaine.df@oxygen-rp.com / emmanuelle.c@oxygen-rp.com

À propos de Anozr Way

Anozr Way est une startup française spécialisée dans l'analyse des données exposées sur le web, dark web, et la protection des personnes face aux risques cyber. Fondée à Rennes en 2019 par Alban Ondrejeck, ancien officier des services de renseignement français, et Philippe Luc, ancien dirigeant dans le secteur de l'assurance, Anozr Way a développé une technologie propriétaire innovante souveraine. La solution Anozr Way est multi-récompensée : startup cyber du prix FIC 2023 et lauréate du Grand Défi Cyber 1 & 2 à titre d'exemples.

6 https://link.springer.com/article/10.3758/s13428-024-02443-y

Les solutions logicielles Anozr Way permettent aux dirigeants d'entreprises et à leurs collaborateurs de maîtriser leur empreinte numérique pour se protéger, eux et leur entreprise, face à des menaces d'ingénierie sociale, d'usurpation d'identité, d'espionnage, de ransomware, de vol de données, etc.
Avec une première levée de fonds de 2 M€ en 2021 (BPI, Breizh Up et BNP Développement), puis une seconde de 6 M€ début 2024 (Dentressangle), Anozr Way est en phase d'accélération avec une croissance de + 271 % et compte désormais 50 collaborateurs. La dernière levée de fonds et les recrutements récents vont stimuler et accélérer le développement de la startup notamment par des évolutions techniques prometteuses, puissantes et novatrices.

Contact presse
Agence oxygen
Violaine de Fontenilles - 06 59 28 82 71 - violaine.df@oxygen-rp.com
Emmanuelle Catheline - 06 79 06 36 11 - emmanuelle.c@oxygen-rp.com