Communiqué de presse
A Rennes, le 20 juin 2023

Cybersécurité : 7 dirigeants français sur 10 dans la ligne de mire des hackers

ANOZR WAY, startup française éditrice de logiciel spécialiste de la protection des dirigeants et collaborateurs face aux risques cyber, dévoile une analyse de l'exposition cyber réelle des hauts cadres et dirigeants d'entreprises français (membres de COMEX-CODIR, tous secteurs confondus, ETI et Grands Groupes). Les constats principaux de l'étude :

- **La sphère personnelle des dirigeants est un vecteur critique de cyberattaques:** les hackers les ciblent directement ou s'en prennent à leur cercle de confiance (famille, amis, proches collaborateurs…) pour les atteindre eux et leur entreprise.
- **7 dirigeants sur 10 ont une exposition cyber à haut risque** mais qui pourrait être réduite de 68% s'ils identifiaient et maîtrisaient leurs données personnelles exposées sur Internet - données exposées sur les réseaux sociaux ou déjà fuitées sur le darkweb qui alimentent les hackers.

Un cumul et croisement d'informations dangereux

La sphère personnelle des dirigeants est particulièrement exploitée par les hackers pour atteindre leur entreprise. Plus facile d'accès, moins bien protégée, elle sort du périmètre de protection habituel de l'entreprise et offre aux hackers toute la matière pour mener des scénarios d'attaques personnalisés, donc crédibles. Selon l'étude ANOZR WAY issue de cas réels :

- **1 dirigeant sur 2 est à haut risque d'usurpation d'identité au regard de ses données exposées.**

- **70 % des décideurs font face à un risque élevé de phishing ciblé** – messages piégés contextualisés en se faisant couramment passer pour un proche.

- **66 % des dirigeants ont des réseaux sociaux personnels ouverts publiquement.** Les références aux centres d'intérêts et loisirs font partie des tactiques des hackers pour rendre leurs pièges attractifs.

- La menace dépasse même le cadre du virtuel : pour **72 % des dirigeants, l'adresse de leur domicile ou résidence secondaire est affichée sur le web, les exposant à des intrusions ou atteintes physiques.**

- **Pour 60 % des dirigeants, leurs cercles familial et amical sont facilement identifiables sur le web.** L'exposition de la vie privée est souvent l'angle mort des

dirigeants et les hackers misent sur l'émotionnel pour lancer des attaques particulièrement efficaces.

'Je suis peu actif sur les réseaux sociaux, je ne crains rien' est une phrase souvent prononcée par les dirigeants. Pourtant, comme l'explique Alban Ondrejeck le cofondateur et CTO d'ANOZR WAY : « **Une unique photo affichée sur son compte Facebook et 'likée' par son conjoint suffit pour vous atteindre**. En remontant au compte de ce dernier on y décèle : des photos des enfants, les établissements où ils sont scolarisés, l'adresse du domicile familial etc. **« De quoi appuyer là où ça fait mal »** souligne Alban Ondrejeck, permettant aussi de se faire passer pour un membre de la famille de façon crédible. « Pour 66% des dirigeants que nous accompagnons, leurs réseaux sociaux et ceux de leurs proches révélaient des informations qui mettaient sérieusement à mal leur sécurité avant de mettre en place les bons correctifs » ajoute le CTO d'ANOZR WAY.

Les hackers n'ont aussi aucune difficulté à basculer de la sphère personnelle à professionnelle, surtout quand les usages quotidiens des dirigeants le permettent :

- **1 dirigeant sur 2 a au moins un mot de passe fuité sur le darkweb**

- **80 % des dirigeants utilisent un seul et même mot de passe pour au moins 4 à 5 comptes différents, qu'ils soient professionnels ou personnels.** Utiliser un même mot de passe pour accéder au système informatique de son entreprise et ses comptes de réseaux sociaux ou e-commerces par exemple, alors que ces derniers se retrouvent facilement sur le darkweb, met en danger son entreprise. Surtout quand l'adresse email professionnelle est utilisée pour tout.

- **52 % des dirigeants ont leur numéro de téléphone personnel exposé sur le web ou fuité dans le darkweb**, offrant un contact direct et facilitant - grâce au cumul avec d'autres données récoltées - la prise de contrôle d'un portable pour contourner la double authentification par SMS et accéder aux comptes personnels et professionnels. Les dirigeants utilisant au quotidien leur téléphone mobile personnel pour le travail.

Toutes ces données exposées sur le web, auxquelles viennent s'ajouter les millions de données piratées et volées qui circulent chaque jour sur le darkweb, nourrissent les hackers. Par leur cumul et leur croisement, les cybercriminels reconstituent facilement toute l'empreinte numérique d'une personne et élaborent des attaques efficaces. Plus un hacker dispose d'informations sur sa cible, plus l'attaque sera personnalisée, crédible et aura des conséquences importantes pour l'entreprise : perte de données, de productivité, chute de valorisation boursière, perte de confiance des partenaires et clients. **Et surtout pour le dirigeant, la responsabilité d'avoir été la brèche pour que son entreprise soit piratée.** Si les très grandes entreprises parviennent généralement à se relever, au détriment de la réputation et la carrière du décideur pris pour cible, **1 PME sur 2 fait faillite dans les 18 mois suivants une cyberattaque.**

La réduction de la surface d'attaque personnelle des dirigeants est possible

Changer régulièrement de mot de passe, utiliser un mot de passe unique pour chaque compte, être vigilant et vérifier l'expéditeur avant de cliquer sur un lien reçu par message,

séparer ses usages personnels et professionnels, sont les premiers gestes à effectuer, mais généralement insuffisants. Une détection en temps réel et maîtrise de ses données exposées sur toutes les strates d'internet, sont aujourd'hui incontournables pour les dirigeants afin de devenir une cible plus complexe pour les hackers et ainsi prévenir les attaques. **ANOZR WAY a calculé qu'en moyenne, les dirigeants peuvent réduire leurs risques cyber de 68%.**

Méthodologie de l'étude :
Etude menée par la société ANOZR WAY sur des cas réels de 100 COMEX / CODIR d'ETI et Grands Groupes français dont l'exposition cyber a été diagnostiquée. Cette analyse a consisté à identifier les données professionnelles et personnelles des dirigeants exposées publiquement sur les différentes strates du web, darkweb. Puis à évaluer l'exposition réelle des dirigeants aux risques de cyberattaques en fonction des scénarios de menaces pratiqués actuellement par les cybercriminels (phishing ciblé, usurpation d'identité et de comptes etc.) au regard des données détectées.*

**Pour préserver leur anonymat, nous ne citons pas les noms, prénoms et entreprises des personnes concernées.*

Lien pour partage de l'étude au sein d'un article:
https://anozrway.com/fr/ressources/etude-vip/

Lien direct vers l'étude réservé aux journalistes:
https://eu1.hubs.ly/H048Sn50

À PROPOS D'ANOZR WAY
ANOZR WAY est une startup française de cybersécurité éditrice de logiciel dédiée à la protection des dirigeants et collaborateurs face aux risques cyber, pionnière de la prise en compte de l'humain en cybersécurité.
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 multi-récompensée – notamment lauréat du Prix du FIC 2023, du Grand Défi Cyber - à base d'Intelligence Artificielle.
La suite logicielle ANOZR WAY adresse :

- *les équipes de sécurité informatique de l'entreprise avec un tableau de bord d'évaluation et suivi des risques*
- *les dirigeants et collaborateurs avec une application qui leur donne le pouvoir de se protéger individuellement*

A la clé : permettre aux dirigeants d'entreprises et à leurs collaborateurs de maîtriser leur empreinte numérique pour se protéger face à des menaces d'ingénierie sociale, d'usurpation d'identité et de comptes, de phishing ciblé, d'espionnage, de ransomware et vol de données etc.
Avec une première levée de 2M€ en 2021, BPI, Breizh Up et BNP Développement sont au capital, ANOZR WAY est en phase d'accélération avec une croissance de +300% et compte 30 collaborateurs.
Plus d'infos : Site web, Linkedin, Twitter