Le mardi 15 juillet 2025

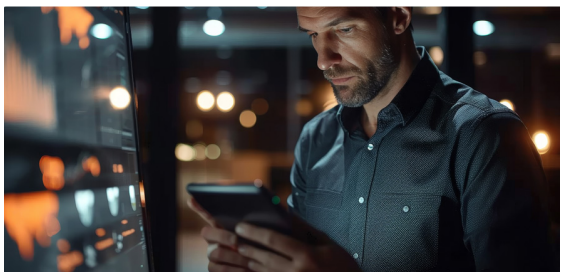
Renforcer la cybersécurité des entreprises et des collectivités locales

Breizh Cyber et ANOZR WAY publient la première étude sur le risque cyber humain

La start-up bretonne ANOZR WAY et Breizh Cyber, le centre de réponse aux incidents cyber (CSIRT) de la Région Bretagne, ont noué un partenariat pour mener la toute première étude d'analyse du risque cyber humain sur un échantillon d'entreprises bretonnes, de tailles diverses allant de la très petite entreprise (TPE) aux grands groupes industriels et appartenant à des secteurs variés en Bretagne.
Le risque cyber humain regroupe l'ensemble des comportements, actions ou omissions — volontaires ou involontaires — susceptibles de compromettre la sécurité informatique d'une organisation ou d'une personne : par exemple, diffuser son numéro de téléphone sur les réseaux sociaux, utiliser son adresse personnelle pour des usages professionnels… Ce « facteur humain » constitue la principale porte d'entrée pour les cybercriminels.

La méthode

L'étude, menée de février à juin 2025, se base sur un échantillon composé de **81 entités tant publiques que privées, allant de la TPE aux grands groupes industriels,** représentant 14 secteurs d'activité dont l'agroalimentaire, la comptabilité, la banques, la communication, la santé, etc. La méthode d'évaluation du risque humain développée par ANOZR WAY, comprend le croisement d'informations disponibles en sources ouvertes à celles issues des bases de données ayant fuité (détection des adresses ou téléphones pro ou perso, par exemple).



Les « empreintes numériques » de 17 988 personnes, des dirigeants aux salariés, ont été analysées.

Les résultats

Cette **étude inédite** sur le risque humain en cybersécurité apporte un éclairage précieux sous l'angle des métiers. Elle confirme les observations de terrain, notamment sur les dirigeants : près de 70 % des membres de comité exécutif (Comex) et comité directeur (Codir) présentent un niveau de risque élevé à très élevé. Cette étude révèle qu'**un dirigeant sur cinq a au moins une adresse email professionnelle compromise.**

L'enquête va plus loin en révélant que d'autres fonctions, souvent moins visibles mais fortement exposées, sont également vulnérables : les **métiers de la communication et du marketing** en première position (1 employé du secteur sur 4 est à très haut et haut risque) ainsi que les **métiers … de la sécurité informatique.**

Les enjeux

Si une adresse email ou un numéro de téléphone est compromis, cela **augmente le risque d'attaques par hameçonnage ou par ingénierie sociale.** Dans le second cas, une usurpation d'identité sophistiquée peut permettre à des cybercriminels de demander des paiements indus, de modifier des coordonnées bancaires, etc… De plus, si les pirates récupèrent des identifiants et mots de passe, ils peuvent **accéder au système informatique interne** de l'entreprise. Enfin, dévoiler son adresse postale personnelle peut conduire à des tentatives de **chantage** ou à des cambriolages.

À l'issue de l'étude, le constat est préoccupant dans la mesure où les attaques sont désormais largement automatisées et alimentées par les fuites massives de données, comme dans le cas de l'opérateur Free : les données de plus de 19 millions de clients ont « fuité », fin 2024.

… / …

Contacts
RÉGION BRETAGNE - Service presse - 02 99 27 13 54 - presse@bretagne.bzh
ANOZR WAY - Charline Jéhannin - 06 40 17 76 60 - charline.jehannin@anozrway.com

Les recommandations

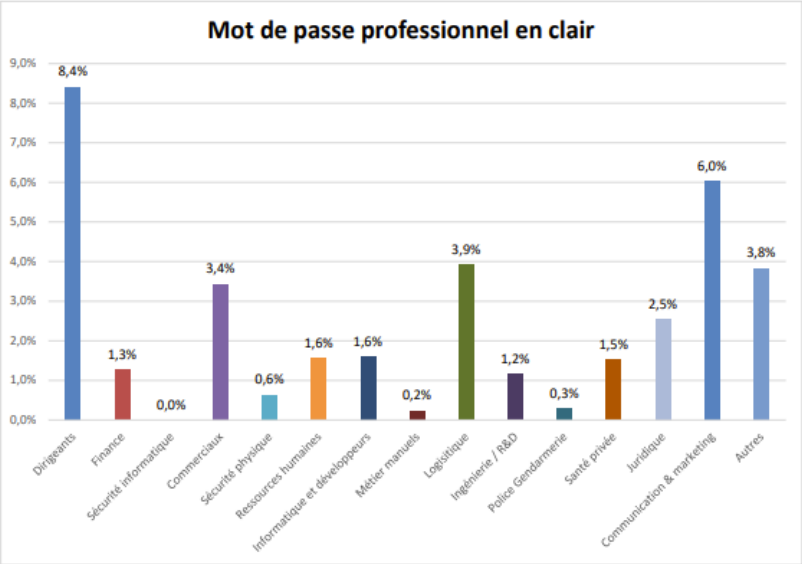
ANOZR WAY et Breizh Cyber formulent 4 recommandations à l'adresse des entreprises et collectivités.

> **Repenser les priorités de protection :** les profils les plus à risque ne sont pas forcément ceux que l'on imagine. Les fonctions support, les profils très exposés médiatiquement ou ceux en interaction fréquente avec l'extérieur peuvent présenter un niveau de vulnérabilité élevé.

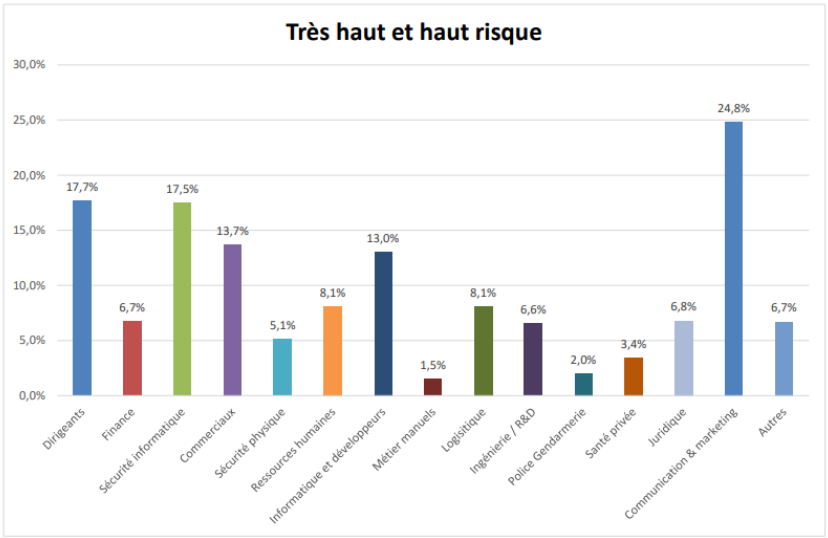
> **Quantifier le risque** avant de mettre en place un plan d'action cyber : cartographier l'exposition numérique individuelle à partir de données factuelles accessibles publiquement sur le web, les réseaux sociaux et le dark web.

> **Adapter les actions de sensibilisation** aux profils de risque : les messages doivent être ciblés et illustrés par des cas d'usages concrets qui parlent aux collaborateurs.

> **Diminuer le risque en corrigeant les failles :** rendre l'utilisateur acteur de sa propre protection, afin de diminuer son exposition numérique, et par ricochet le risque de l'organisation.



Détection des mots de passe ayant fuité, liés à une adresse email professionnelle, par catégories de métiers (en %)



Analyse du risque humain des catégories de métiers / fonctions étudiées (en %)

À propos d'ANOZR WAY

ANOZR WAY est un éditeur de logiciels breton dont la mission est de protéger les organisations, les dirigeants et les collaborateurs des attaques par ingénierie sociale : phishing, compromission de compte, usurpation d'identité... ANOZR WAY propose une suite logicielle de gestion des risques cyber humains et de protection des personnes, conçue pour contrer les menaces cyber ciblant les collaborateurs. ANOZR WAY a réalisé 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).

À propos de Breizh Cyber

Pour faire face à l'accroissement de la cybermenace, la Région Bretagne a créé, avec le soutien de l'État et de l'agence nationale de la sécurité des systèmes d'information (ANSSI), un centre de réponse aux incidents de sécurité informatique. A l'échelle régionale, Breizh Cyber accompagne les entreprises, associations et collectivités bretonnes dans la réponse aux attaques ou l'anticipation des menaces cyber.