Les entreprises de la finance dans la tourmente du ransomware

PHILIPPE LUC,

CEO & Cofondateur ANOZR WAY, 12 ans chez Malakoff Médéric comme Directeur Commercial France et Directeur Marché

La cybermenace s'intensifie d'année en année, qu'il s'agisse de ransomware[1], de fraude au président, ou d'autres types d'attaques. **En 2022, les attaques par ransomware ont augmenté de 35% par rapport à 2021, soit 1 attaque revendiquée toutes les 3h dans le monde,** selon le Baromètre ANOZR WAY du Ransomware[2]. Les entreprises du secteur de la finance ne font pas exception : le secteur fait partie du top 10 des secteurs les plus visés en France en 2022.

8 attaques cyber sur 10 ciblent les dirigeants et collaborateurs

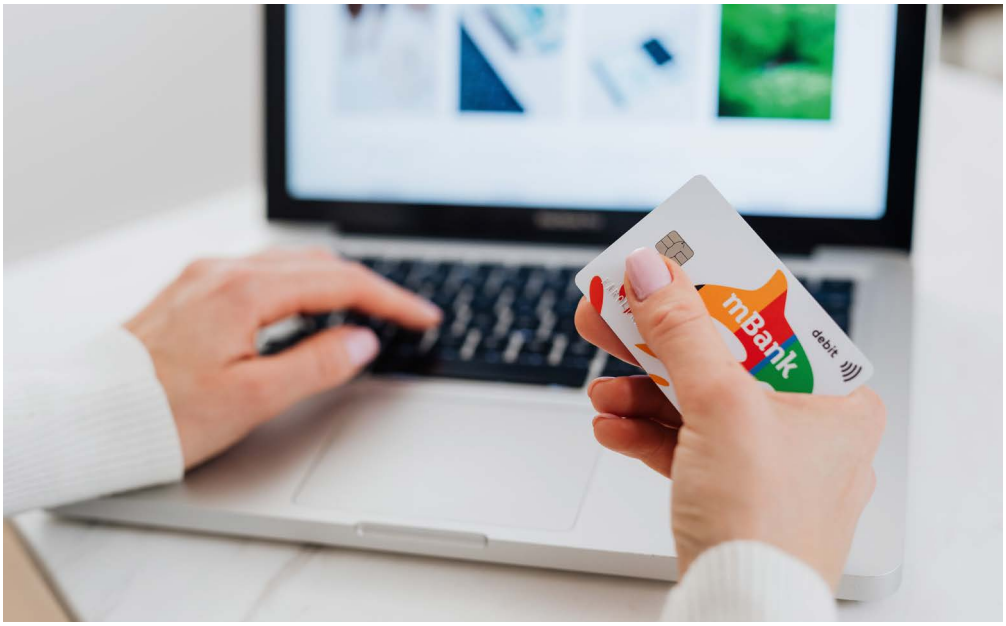
Les efforts sont souvent portés sur la sécurisation du système d'information. A juste titre, mais ce n'est malheureusement pas suffisant… Surtout quand l'on sait que **8 attaques cyber sur 10 ciblent les dirigeants et collaborateurs.** Cela signifie que les cybercriminels pour contourner les systèmes de sécurité techniques visent directement les personnes au sein de l'entreprise.

Les pirates ont bien compris que **l'humain était une porte d'entrée possible sur le système d'information.** Ils privilégient les messages piégés (hameçonnage/ phishing) personnalisés et ciblés. Pour cela, ils se renseignent en amont sur leur cible, en collectant toutes les informations disponibles sur le web, que ce soient les données publiques des profils de réseaux sociaux ou les données fuitées qui se trouvent sur le darkweb. Ils se font aussi passer pour un membre de votre entourage professionnel ou personnel pour maximiser les chances de réussir leurs attaques.

Les dirigeants et managers, cibles privilégiées

Plus d'1 dirigeant sur 3 a été victime d'escroqueries par hameçonnage en 2022, soit **12x plus que les autres collaborateurs**. Les dirigeants, membres du COMEX, CODIR, cadres, sont des cibles privilégiées pour les cybercriminels, de par leur statut et par leur accès à des documents confidentiels ou données sensibles.

A leur insu, **de nombreuses informations d'identité sont en libre accès sur le web et darkweb** à cause de fuites de



données issues d'autres cyberattaques (hôpitaux, collectivités, e-commerces, etc.) : documents d'identité, adresse du domicile, données bancaires, e-mails et mots de passe...

Les conséquences peuvent être multiples : usurpation d'identité, arnaque financière, etc. Une fois les données personnelles recueillies, la personne malveillante peut utiliser l'identité d'un dirigeant dans une "fraude au président", ou d'une personne du service comptabilité pour demander de réaliser un virement en urgence, autrement dit une "fraude au faux virement" (FOVI).

L'impact colossal des cyberattaques

Les attaques par ransomware peuvent être particulièrement destructrices pour les entreprises dans le secteur de la finance, particulièrement prises pour cibles en raison des informations sensibles et confidentielles qu'elles traitent. Cela entraîne ainsi **la perte de données sensibles concernant les clients, un impact sur le chiffre d'affaires, des pertes financières, une chute de la valorisation boursière et une atteinte à la réputation de l'entreprise.**

La perte de chiffre d'affaires annuel par entreprise consécutive à un ransomware est estimée en moyenne à 27%, hors paiement éventuel d'une rançon qui peut s'élever jusqu'à 128 000€ en moyenne par entreprise[3]. **Pour l'année 2022, l'impact économique est de 2,8 milliards d'euros de perte de chiffre d'affaires pour les entreprises françaises victimes de ransomware.**

Comment se prémunir des cyberattaques ?

Au-delà des mesures de sécurité techniques à mettre en place pour se protéger des cyberattaques (sauvegarde régulière, maintien des logiciels à jour...), **il est nécessaire de prendre en compte l'aspect humain.**

Il est important de sensibiliser les utilisateurs aux risques et de leur enseigner les bonnes pratiques de sécurité comme reconnaitre les pièges des e-mails de phishing.

En amont, pour qu'ils deviennent des cibles beaucoup plus difficiles à atteindre, il est nécessaire que chacun soit conscient de toutes les informations le concernant exposées en ligne. En maîtrisant cette empreinte numérique, on complexifie le travail des pirates lorsqu'ils se renseignent sur une entreprise et son personnel. Ils choisiront alors de passer leur chemin et de s'en prendre à une cible beaucoup moins complexe.

En étant informé, vigilant et en mettant en place des actions correctives, chacun contribue à la protection de son entreprise contre les cyberattaques. ■

[1] Ransomware : type de logiciel malveillant qui crypte les fichiers d'une victime. Les attaquants demandent ensuite une rançon à la victime pour rétablir l'accès aux fichiers moyennant paiement.

[2] Baromètre ANOZR WAY du Ransomware - Bilan 2022 & Prévisions 2023 https://anozrway.com/fr/barometre-ransomware/

[3] Hiscox