Lourds investissements par les banques pour ne pas se faire pirater

	Lourds investissements par les banques pour ne pas se faire pirater

Pour ne pas se faire pirater, les banques investissent massivement dans la cybersécurité, souligne le Wall Street Journal dans une enquête datée du 20 décembre. Elles essayent également d'instaurer de bonnes pratiques chez leurs employés, responsables de 30% des fuites de données.

Les banques dépensent sans compter pour se défendre contre une armée invisible de hackers, qui essayent par tous les moyens de récupérer des données sur leurs clients et les énormes quantités de fonds qu'elles stockent sur leurs comptes.
Le patron de Bank of America, Brian Moynihan, a déclaré lors d'une conférence au mois de novembre que le budget cybersécurité de son entreprise était illimité, comme le rapporte le Wall Street Journal.
JP MORGAN INVESTIT 500 MILLIONS DE DOLLARS EN 2016 DANS LA CYBERSÉCURITÉ
Même topo pour l'américaine Wells Fargo, première banque mondiale en terme de valorisation boursière : « Nous dépensons un océan d'argent » dans la cybersécurité, a expliqué son PDG John Stumpf dans une interview récente, reprise par le média américain. Un porte-parole de la société a refusé de donner plus de détails sur les montants investis.
J.P. Morgan Chase a été victime en 2014 d'un piratage massif de données : 76 millions de clients étaient concernés par cette fuite d'informations sensibles. La banque américaine a considérablement renforcé son dispositif de cybersécurité. Elle va investir 500 millions de dollars pour se protéger contre les hackers en 2016, soit environ deux fois plus qu'en 2014, détaille le Wall Street Journal.

LA VULNÉRABILITÉ NUMÉRO UN DES BANQUES : LEURS SALARIÉS
Souvent, les hackers jouent sur la vulnérabilité numéro un des banques pour récupérer des informations sensibles : les salariés. Ils envoient notamment des messages de phishing (hameçonnage), demandant à leurs destinataires de cliquer sur un lien. Cela leur permet d'installer dans les ordinateurs ciblés des logiciels espions. J.P. Morgan a envoyé un faux mail de phishing à ses salariés, pour les tester. Résultat ? 20% d'entre eux ont mordu à l'hameçon…
En moyenne, 30% des fuites de données dans les entreprises sont liées à une erreur d'un salarié, selon une enquête diffusée en décembre par l'Association of Corporate Counsel, une association professionnelle d'avocats américains. Pour limiter les dégâts, les banques interdisent donc à leur salariés d'utiliser des clefs USB venues de l'extérieur, d'utiliser leur adresse mail personnelle pour s'inscrire à des services sur Internet (site de e-commerce par exemple).

NE PAS ALLER JUSQU'AU « FLICAGE »
Elles leur demandent aussi d'être vigilants par rapport aux informations qu'ils postent sur les réseaux sociaux. « Mais jusqu'où les banques peuvent-elles aller dans le 'flicage' de leurs salariés sur ces sites ? », s'interrogent les experts du secteur.
Impossible de poursuivre un collaborateur qui poste des photos de ses vacances sur son profil Facebook, même si cela pourrait permettre à un pirate de s'introduire à son domicile et de voler son ordinateur professionnel. Alors que faire ? Cette réflexion délicate doit être conduite par les institutions financières si elles veulent protéger au mieux les données sensibles de leurs clients.

Réagissez à cet article

Source : *Cybersécurité : Les banques investissent « un océan d'argent » pour ne pas se faire pirater*

Lelia de MATHAREL