La fraude au Président n’arrive pas qu’aux autres

	La fraude au Président n’arrive pas qu’aux autres

Des millions d'euros envolés dans une escroquerie aux faux virements bancaires. Une entreprise Dunkerquoise découvre qu'elle vient de perdre plus de neuf millions d'euros dans la manipulation de ses informations bancaires.

Qu'ils sont fatigants ces gens qui savent toujours tout. Il y a quelques semaines, lors d'une conférence que m'avait demandé une collectivité locale, un responsable d'un bailleur social m'expliquait qu'il ne fallait pas trop exagérer sur les risques de piratage informatique, de fuites de données… J'expliquais alors comment des malveillants s'attaquaient aussi aux locataires de logements sociaux. Le monsieur expliquait alors, pour conforter ses dires « ***depuis que j'ai un antivirus et le firewall incorporé*** […] ***je n'ai plus jamais eu d'ennui avec mon ordinateur portable***« . Le monsieur travaillait pour un bailleur social de la région de Dunkerque (Nord de la France – 59). Et c'est justement à Dunkerque, chez un bailleur social, *Le Cottage social des Flandres*, qu'une nouvelle affaire de fraude au président vient de toucher la banlieue de la cité de Jean-Bart. Une manipulation des informations bancaires qui coûte 25% du chiffre d'affaires de la victime.

23 versements de 400.000 euros

Alors, cela n'arrive qu'aux autres ? L'entreprise Dunkerquoise n'est pas une structure à la Nestlé, Michelin, Total, Le Printemps. 140 employés, 6.000 locataires et un quelques 40 millions d'euros de chiffre d'affaires. Bref, une petite entreprise comme il en existe des dizaines de milliers en France. Le genre d'entité économique qui pense que les pirates informatiques, les escrocs ne s'intéresseront pas à elles. Erreur grave ! Pour *Le Cottage social des Flandres*, les professionnels de la Fraude au Président, la fraude au FoVI, se repartis avec 23 virements de plus de 400.000 euros. Bilan, 9,8 millions d'euros envolés dans les caisses d'une banque basée en Slovaquie. Autant dire que revoir l'argent revenir à la maison est peine perdue. D'autant plus que la fraude a couru du 7 avril au 23 mai. Piratage qui n'aura été découvert qu'un mois plus tard, au départ en vacances d'un dès comptable. Bref, en manquement évident de sérieux, et cela dans toutes les strates stratégiques de l'entreprise. Surtout à la lecture de la Voix du Nord : un responsable explique que l'arnaque était tellement bien montée que la société n'y a vu que du feu, et plus grave encore « ***On a les reins solides, on va pouvoir faire face***. » Après tout, 9,8 millions d'euros « ne » représente que 25% du CA de cette société (Sic !).

Méthode rodée mais simple à contrer

Un exploit que cette fraude ? Les adeptes du social engineering (l'étude de l'environnement d'une cible avant de s'attaquer à son univers informatique) savent très bien que non. Dans l'affaire Dunkerquoise, un compte mail piraté aurait permis le début de cette fraude au président. Détail troublant, les courriels arrivaient ailleurs que sur une adresse type adresse@Cottages.fr ? Car si piratage il y a eu, c'est l'ensemble des services couplés au domaine qui ont pu être corrompu. A moins que le responsable usurpé utilisait un gMail, Yahoo! ou tout autre compte webmail. Toujours est-il que le pirate a mis la main sur une adresse officielle et a pu ainsi manipuler les employés.

Parce que pour éviter un FoVI, c'est aussi simple que de protéger son argent personnel, normal. C'est d'ailleurs très certainement là où le bât blesse. Ce n'est pas mon argent, donc j'en prends soin, mais pas trop. Penser que cela n'arrive qu'aux autres est une grande erreur. Éduquer vos personnels, éduquez-vous, patrons, dirigeants…

Pour éviter un FoVI, contrôler ses informations bancaires

N'autoriser le transfert d'argent qu'après applications de mesures décidées en interne, et quelle que soit l'urgence de la demande de manipulation des informations bancaires. D'abord, la somme d'argent. Plafonner le montant. Si ce montant dépasse le chiffre convenu, obligation d'en référer à la hiérarchie. Un élément qui doit obligatoirement faire « tiquer » dans les bureaux : la demande d'un second transfert, d'une nouvelle modification des Le mot-clé principal « informations bancaires » n'apparait pas dans le titre SEO de la page par la même personne, même entité, doit également être indiquée à la hiérarchie. « ***Paulo, c'est normal de faire 23 versements de 400.000 euros en 2 mois ?*** » – « ***Oui ! Le boss achète des chouquettes en Slovénie. Il me l'a dit par mail !***« . La validation de transfert doit se faire par, au moins, deux personnes différentes, dont un supérieur hiérarchique.

Article original de Damien Bancal

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : ZATAZ Informations bancaires : la fraude au Président n'arrive pas qu'aux autres – ZATAZ