



Flash N° 7 – 18 décembre 2013

Flash ingérence économique

Ce « flash » de l'ingérence économique relate un fait dont une entreprise française a récemment été victime. Ayant vocation à illustrer la diversité des comportements offensifs susceptibles de viser les sociétés, il est mis à votre disposition pour vous accompagner dans la diffusion d'une culture de sécurité au sein de votre entreprise.

Vous comprendrez que par mesure de discrétion, le récit ne comporte aucune mention permettant d'identifier l'entreprise visée.

Pour toute question relative à ce « flash » ou si vous souhaitez nous contacter, merci de nous écrire à l'adresse :

securite-economique@interieur.gouv.fr



Alerte aux escroqueries « SEPA »

L'harmonisation des moyens de paiement dans l'Union européenne génère des modifications informatiques au sein des entreprises françaises propices à la réalisation d'escroqueries.

Depuis la fin de l'été, la DCRI a eu connaissance de plusieurs escroqueries, sous couvert de vérification du bon fonctionnement du protocole de virement ou de mise aux normes.

Ces escroqueries sont réalisées dans le contexte de **l'harmonisation des moyens de paiement dans la zone SEPA** (Single Euro Paiement Area - Espace unique de paiements en euros) qui génère des changements informatiques au sein des entreprises, et qui prendra effet au 1^{er} février 2014.

Typiquement, un employé de votre service Comptabilité / Finances se voit proposer par un employé de votre banque de faire un test de transaction financière.

En l'espèce, après une phase de préparation visant à permettre à l'escroc d'avoir toute l'assurance requise au téléphone pour obtenir l'adhésion de sa victime, ce dernier se fait passer pour votre banque et avertit sa victime qu'elle recevra prochainement un appel du service informatique -toujours de votre banque- pour tester le nouveau protocole concernant les virements bancaires SEPA. Ce scénario ne vise naturellement qu'à gagner votre confiance.

Une fois le virement fait, et pour conserver la confiance de la victime, l'escroc rappelle pour confirmer que la banque étrangère a bien reçu l'argent, que le test est concluant, et que l'argent sera restitué tel jour à telle heure. Mais ce n'était pas votre banque au téléphone.

Commentaire :

Actuellement, les opérations bancaires aux formats nationaux et européens (virements et prélèvements) cohabitent. Mais à compter du 1er février 2014, seuls les moyens de paiement « SEPA » pourront être échangés.

Cette harmonisation va générer des changements informatiques au sein des entreprises :

- ✓ modification des formats de fichiers qui seront désormais échangés en XML et répondant à la norme ISO 20022 ;
- ✓ substitution de l'IBAN au RIB ;
- ✓ diverses autres modifications spécifiques aux prélèvements.



Ces escroqueries sont susceptibles de cibler davantage les entreprises de taille intermédiaire (ETI) et PME ayant une activité à l'international, que les grands groupes, les premières disposant moins de structures de contrôle ou de procédures écrites que les secondes. Par ailleurs, ces faits sont facilités par la possibilité de louer, auprès de sociétés sur Internet, des numéros de téléphone (en 01, 02, 03, 04, 05 et 08). Enfin, un appel masqué doit éveiller votre suspicion.

Parade à mettre en œuvre

La prévention de ces escroqueries ne peut se faire que par la sensibilisation de vos équipes comptables et financières.

Dans tous les cas, contacter votre conseiller bancaire habituel pour lui demander si de tels tests sont 1) effectivement prévus, 2) si Monsieur « X » est bien un employé du service chargé de procéder à ces tests, 3) si la banque et le numéro de compte/IBAN servant au test sont légitimes.

Nota : pour rappel, une vague d'escroqueries frappe, depuis 2011, de nombreuses sociétés, de tout secteur industriel, portant sur des virements bancaires internationaux (cf. Flash Ingérence n° 6 du 04.09.2013). Ces faits sont toujours d'actualité, indépendamment de l'escroquerie décrite ici.

Enfin, à l'instar des escroqueries aux virements bancaires internationaux, une escroquerie « SEPA » est susceptible de survenir une veille de weekend ou de jour férié, afin de retarder la découverte de la supercherie.

Parade complémentaire

Par ailleurs, une sensibilisation de vos employés aux manœuvres d'ingénierie sociale permettra d'y faire obstacle plus efficacement, cette technique étant utilisée pour obtenir les renseignements internes indispensables à la mise en confiance.

Est appelée « **manœuvre d'ingénierie sociale** » toute technique employée pour faire parler un individu *dans un but inavoué* et obtenir de lui les informations recherchées.

Enfin, toute difficulté à vérifier la qualité et l'identité de votre interlocuteur, et son numéro d'appel, doit éveiller une suspicion