Flash n°6 – 04 septembre 2013

Flash
ingérence économique

Ce « flash » de l'ingérence économique relate des faits dont de nombreuses entreprises ont récemment été victimes. 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 les entreprises visées.

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

Prévention des escroqueries
aux virements bancaires internationaux

Le constat d'une recrudescence des escroqueries aux virements bancaires internationaux conduit à la nécessité de sensibiliser les employés sur des pratiques susceptibles de générer des préjudices de plusieurs centaines de milliers d'euros, voire davantage. Ces escroqueries sont toujours précédées d'une phase, le plus souvent téléphonique, de recherche de renseignements sur le collaborateur susceptible de procéder au virement (nom, fonction, carrière, etc.). Une bonne vigilance observée à ce stade permet de ne pas communiquer d'informations de nature à faciliter l'escroquerie.

1- Sur la phase de préparation

Ces recherches d'informations sont réalisées au moyen d'une technique communément appelée « ingénierie sociale ». Cette technique consiste pour l'escroc à obtenir des informations sur l'entreprise ciblée -ou l'individu ciblé- par fax, e-mail, téléphone, ou contact direct, en usurpant une qualité, en ayant recours à diverses manœuvres, menaces (de licenciement notamment), en adressant de faux questionnaires de satisfaction, etc.

La manipulation fonctionne d'autant mieux que son auteur a la capacité d'agir assez directement. Son assurance et son air de connivence n'incite pas en général à remettre en cause sa qualité ou la validité de sa démarche.

Cette phase de recueil de renseignement sur l'entreprise ciblée permet à l'escroc, ainsi documenté, de pouvoir se faire passer pour un membre de votre cercle le jour où il sollicitera le virement bancaire. Son aisance dans le contact, alliée à la connaissance de votre entreprise, lui permettra alors de gagner votre confiance.

2- Signaux qui doivent éveiller votre méfiance :

Les escroqueries constatées par la DCRI ont pour points communs :

a- l'usurpation d'identités de responsables de votre groupe (fondateur, P-DG, fils du P-DG, directeur financier, directeur marketing, etc.), de manière à intimider l'employé à qui il est demandé de réaliser le virement ;

b- un caractère d'urgence est avancé sous un prétexte quelconque (afin de ne pas laisser le temps de vérifier le bien-fondé de la demande de virement) ;

c- une totale discrétion est requise sous un faux prétexte (afin d'empêcher l'alerte d'un responsable hiérarchique en mesure de détecter l'escroquerie) ;

d- la demande de virement se fait au profit d'une banque généralement située hors de l'Union européenne (de manière à compliquer l'entraide judiciaire) ;

e- les victimes sont majoritairement -mais pas exclusivement- des employés de filiales étrangères de groupes français ;

f- ces escroqueries sont -en particulier, mais pas exclusivement- commises lorsqu'un weekend est suivi -ou précédé- d'un jour férié ou d'un pont engendré par un jour férié (ce délai permet de retarder la découverte du virement indu) ;

e- enfin, l'auteur de la supercherie prétextera le plus souvent être en déplacement pour ne pas laisser de coordonnées vérifiables.

3- La bonne démarche consiste :

a- en amont : à s'assurer de l'existence de procédures internes régissant les virements, à vérifier leur diffusion et leur application effective (contre-appel sur une ligne fixe, vérification que l'e-mail provient bien de la société (attention au nom de domaine), double signature requise au-delà d'un certain montant, etc.

A effectuer une communication interne en direction des équipes financières et comptables pour les sensibiliser, et plus largement à l'attention de tout employé exerçant une fonction de « filtre » = secrétaires, assistantes de direction, standardistes, etc. Ce personnel est en effet susceptible d'être contacté par l'escroc pour obtenir des informations sur votre entreprise dans le cadre de la phase préparatoire.

A ne pas rendre public votre organigramme sur votre site Internet. La connaissance de ce document interne est de nature à faciliter les repérages de l'escroc.

b- durant la phase active de l'opération : en cas de demande de virement faite hors formalisme habituel, exiger un écrit provenant d'une adresse mail professionnelle (et non personnelle), ainsi qu'un numéro de téléphone fixe (et non portable). Orienter votre interlocuteur vers la procédure régulière, et ne rien entreprendre sans aval hiérarchique.

Il a été constaté que, lorsque ces manœuvres échouent et que la supercherie n'a pas été détectée, l'échec est dû à la seconde signature requise pour les virements bancaires dépassant un certain montant.

Dans de petites structures où employés et dirigeants se connaissent bien, la supercherie a pu être déjouée, car l'employé ciblé n'a pas reconnu la voix de son prétendu patron.

c- après l'escroquerie : déposer plainte auprès de la section financière du Service Régional de Police Judiciaire (SRPJ) de votre ressort ;

4- En résumé

La prévention de ces escroqueries passe par le bon sens des personnes ciblées :

- au regard de votre position dans l'entreprise, serait-il logique que votre P-DG vous appelle, vous personnellement, pour solliciter un virement ?

- est-il logique que votre P-DG vous incite à déroger au formalisme en vigueur pour procéder à un virement bancaire ?

Dans tous les cas :

Retenez que les notions de
discrétion et d'urgence prétextées
doivent impérativement éveiller votre suspicion !