INGERENCE ECONOMIQUE

Flash n° 65 – Avril 2020

Ce « flash » évoque des actions d'ingérence économique dont des sociétés françaises sont régulièrement victimes. Ayant vocation à illustrer la diversité des situations auxquelles les entreprises sont susceptibles d'être confrontées, il est mis à votre disposition pour vous accompagner dans la diffusion d'une culture de sécurité interne.

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 vous adresser à : securite-economique@interieur.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

Flash n°65 avril 2020

Les risques d'escroqueries liées au COVID-19 (suite des « flash » n°61 et 64)

Dans les précédents « *Flash* » consacrés aux actions d'ingérence économique, plusieurs exemples ont été cités concernant la multiplication des escroqueries dont sont victimes les sociétés privées et les institutions françaises dans le contexte de la crise sanitaire liée au COVID-19.

Les escroqueries aux faux ordres de virement internationaux (FOVI) se sont particulièrement développées ces dernières semaines. Dans certains cas, sans prendre en compte les frais de justice ni l'atteinte à l'image qui peut en découler, le montant du préjudice s'élève à plusieurs millions d'euros.

Alors que les sociétés françaises sont à la recherche de matériel sanitaire, soit pour répondre aux besoins de leurs clients soit pour pouvoir mettre en place des mesures d'hygiène permettant une reprise d'activité, des individus malveillants recourent à des modes opératoires divers et sophistiqués pour escroquer leurs victimes en se faisant passer pour des fournisseurs de matériel médical.

Profitant de la situation actuelle, ces individus n'hésitent pas non plus à se faire passer pour des fournisseurs de matières premières dans tous les secteurs d'activité, soit en usurpant l'identité d'un fournisseur historique soit en se faisant passer pour un potentiel nouveau partenaire commercial susceptible d'apporter une solution à une entreprise française qui a vu ces dernières semaines ses chaines de fournisseurs et de sous-traitants être particulièrement perturbées.

La réduction des effectifs et la modification en profondeur des habitudes de travail (télétravail, temps partiel, alternance des équipes, etc.) ont aussi créé des situations de vulnérabilité exploitées par des individus malveillants, usurpant l'identité de partenaires commerciaux ou d'institutions, afin d'obtenir des informations sensibles ou stratégiques. Un fonctionnement en mode « dégradé » peut ainsi entraîner une baisse de la vigilance.

Les procédures visant à allouer des aides publiques peuvent par ailleurs être détournées et falsifiées afin de capter des informations utilisées dans un second temps par des escrocs pour commettre d'autres actions malveillantes (revente de données sensibles à des concurrents, obtention d'aides publiques indues à la place de l'entreprise victime de l'arnaque, mise en place d'une escroquerie aux FOVI grâce aux données de l'entreprise, etc.).

Si la numérisation massive des données au sein de l'entreprise et l'utilisation des réseaux sociaux ont facilité la mise en œuvre de ce type d'escroqueries, leurs auteurs continuent également à recourir à des moyens classiques de manipulation (appel téléphonique, courrier, lettre recommandée, etc.), lesquels s'ajoutent aux outils numériques (falsification de site internet, piratage ou détournement d'adresse électronique, etc.)

PREMIER EXEMPLE

Au cours des dernières semaines, une entreprise française a commandé à l'un de ses fournisseurs chinois, avec lequel elle entretient des relations commerciales depuis plus de dix ans, une grande quantité de matériel de protection sanitaire. Quelques jours plus tard, la société française a reçu un courriel l'informant que la société chinoise avait changé ses coordonnées bancaires. Après avoir pris en compte ce changement, l'entreprise tricolore a effectué plusieurs virements pour honorer ses commandes. Toutefois, la société chinoise s'est rapidement inquiétée de ne pas recevoir de paiements pour les commandes passées. L'entreprise française a ainsi découvert que les coordonnées bancaires utilisées n'étaient pas celles de son fournisseur et qu'elle avait été escroquée de plusieurs millions d'euros.

DEUXIEME EXEMPLE

Dans le cadre d'une demande d'aides publiques, une entreprise française s'est tournée vers l'administration concernée et a fourni les documents requis. Par la suite, l'entreprise a reçu un courrier lui demandant de fournir des informations complémentaires, notamment des données confidentielles sur les activités de la société, afin que l'administration puisse statuer sur sa demande. Contactée par la société française, surprise par la demande, l'administration a pu indiquer à cette dernière qu'elle lui avait bien adressé un courrier mais qu'en aucun cas l'administration française lui avait demandé de fournir les éléments mentionnés dans la lettre reçue par la société française. Une étude attentive du document a ainsi pu révéler plusieurs anomalies et erreurs, attestant d'une falsification du courrier et une usurpation d'identité.

TROISIEME EXEMPLE

En cherchant à obtenir le paiement d'une de ses factures, le dirigeant d'une entreprise française s'est vu répondre par son client que le virement avait déjà été effectué aux coordonnées bancaires que ce dernier avait fournies. Or, le dirigeant n'avait jamais transmis de telles informations à son client. L'analyse des ordinateurs de l'entreprise par le responsable de la sécurité des systèmes d'information (RSSI) n'a pas non plus révélé d'anomalies. Toutefois, il s'est avéré que le dirigeant de la société française utilisait parfois son adresse de messagerie personnelle, créée sur un site

gratuit et grand public, pour échanger avec ses partenaires commerciaux. Le client a, en outre, confirmé que les informations bancaires lui avaient été transmises depuis cette adresse électronique. Si, dans cet exemple, le piratage de la boite aux lettres électronique personnelle du dirigeant de l'entreprise française a permis aux pirates informatiques de mettre en place une escroquerie aux FOVI, ces derniers ont pu également avoir accès à d'éventuelles informations sensibles ou stratégiques concernant la société et ses partenaires commerciaux.

Commentaire :

Dans ces exemples, ou ceux cités dans les précédents « *Flash* », des indices permettaient d'éveiller l'attention afin de détecter les éventuelles tentatives d'escroqueries : une modification d'une lettre dans le nom d'une société (notamment lorsque la société est étrangère et que l'escroc tente de respecter la prononciation phonétique de l'entité), des erreurs dans les en-têtes, des incohérences dans les fonctions alléguées par les interlocuteurs, des changements étranges dans la police de caractère ou dans le style d'écriture, etc.

Sur Internet, d'autres éléments doivent également retenir l'attention : l'utilisation d'une nouvelle adresse de messagerie (notamment une adresse personnelle), des modifications dans l'adresse URL (nom de domaine, extension, protocole), etc.

En cette période marquée par la mise en place de nouvelles méthodes de travail, il s'agit de renforcer la vigilance, de sensibiliser régulièrement vos colorateurs, dirigeants et employés et de veiller au respect des procédures de vérifications, tout en maintenant à jour le système de sécurité informatique.

PRECONISATIONS DE LA DGSI

Face aux risques d'escroqueries pouvant fragiliser les sociétés françaises, la DGSI émet les préconisations suivantes :

→ De nombreuses sociétés françaises ont déjà été victimes d'escroqueries et de tentatives d'escroqueries. En cas de contact par une entreprise ou un individu, français ou étranger, jusqu'à présent inconnu, il est recommandé de faire preuve de méfiance, voire, dans le doute, de s'abstenir. Lorsque vous connaissez déjà votre interlocuteur, n'hésitez pas à lui demander de confirmer les informations qu'il vous fait parvenir en utilisant les moyens de communication déjà connus et qui ne sont pas susceptibles d'avoir été falsifiés.

→ En période de très forte demande mondiale de matériel médical de protection, voire dans certains cas de pénuries, il apparait peu probable qu'une entreprise de production de masques ou de gels ait besoin de faire de la prospection commerciale, par e-mail ou par téléphone, afin

d'écouler ses stocks. Un démarchage dans ce sens doit éveiller les soupçons sur une possible escroquerie.

→ Avant de procéder à tout paiement, il est important d'évaluer l'honorabilité d'un vendeur en se rapprochant de différentes entités : banques, autorités de santé (ministère, agence régionale de santé, hôpitaux), services de protection économique (ministère de l'Intérieur, ministère de l'économie et des finances), etc.

→ En cas de réussite de l'escroquerie, il convient de porter plainte immédiatement auprès des services de police et de gendarmerie. Gardez tous les éléments (e-mails, noms, etc.) pouvant contribuer à l'enquête. Des plateformes de signalements mises en place par les pouvoirs publics permettent également de dénoncer ces tentatives frauduleuses. Nous vous orientons plus particulièrement vers le site web du ministère de l'Intérieur : www.internet-signalement.gouv.fr