Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

INGERENCE ECONOMIQUE

Flash n° 42 – Avril 2018

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°42 Avril 2018

Les manœuvres d'ingénierie sociale, une source de vulnérabilités pour les entreprises

L'ingénierie sociale est une pratique visant à manipuler psychologiquement un individu afin de récupérer des informations. Certaines victimes de manœuvres de cette nature peuvent ainsi être amenées à livrer des informations stratégiques/confidentielles ou à commettre un acte susceptible de porter atteinte à leur entreprise.

Il s'avère donc important de sensibiliser les entreprises et leurs salariés aux différentes techniques d'ingénierie sociale utilisées, et de rappeler les risques encourus par les acteurs économiques en termes d'escroquerie ou de captation de leurs savoirs et savoir-faire.

1er exemple

Une société a reçu la visite inopinée d'un auditeur prétendant travailler pour l'administration d'un pays étranger dans lequel l'entreprise tricolore commercialise ses produits. Si un audit était effectivement programmé, l'entreprise française s'est toutefois étonnée de ne pas avoir été prévenue de cette venue.

L'assurance de l'« auditeur », sa fermeté, son charisme et sa connaissance manifeste de l'entreprise ont convaincu les dirigeants, pourtant méfiants au départ, de lui autoriser l'accès au site. Cette personne extérieure a ainsi pu travailler librement une journée entière sur le système informatique et avoir accès à de nombreuses données stratégiques de la société.

A posteriori, l'entreprise s'est renseignée et a appris qu'un audit était bien prévu… mais quelques mois plus tard. Il est probable que le soi-disant auditeur travaillait pour une entreprise concurrente ou un service étranger. Le préjudice, en termes de captation informationnelle, a été considérable pour la société hexagonale.

2ème exemple

Le responsable juridique d'une entreprise française a reçu l'appel d'un individu se présentant comme officier de gendarmerie. Ce dernier souhaitait obtenir les coordonnées électroniques du PDG de la société afin de l'inviter à une cérémonie officielle. Après avoir obtenu facilement ce premier

renseignement, le pseudo officier a demandé l'adresse électronique du directeur financier afin qu'il soit également convié à la dite manifestation.

Le lendemain, le directeur financier recevait un courriel, envoyé depuis l'adresse mail du PDG, qui l'informait de l'acquisition, par le groupe, d'une société étrangère. Dans ce courriel, le « dirigeant » félicitait son interlocuteur pour ses qualités de discrétion et son professionnalisme, tout en lui indiquant que lui seul était en mesure de finaliser cette opération, par le biais d'un virement bancaire sur un compte inconnu de la société. Le correspondant demandait au directeur financier de ne pas informer, pour des questions de confidentialité, d'autres personnes de la direction.

Le directeur financier, étonné par les multiples précautions entourant cette demande, a toutefois pris contact avec le directeur juridique du groupe. Si la première démarche d'ingénierie sociale, qui consistait à récupérer les adresses mails des personnes ciblées, a fonctionné, les responsables juridique et financier se sont rendu compte, à temps, que l'adresse mail du PDG avait été usurpée et que la demande de virement bancaire était frauduleuse.

Si la tentative d'escroquerie n'avait pas été décelée, l'entreprise française aurait pu, faute de trésorerie pour rembourser la perte, être placée en liquidation judiciaire.

3ème exemple

La messagerie professionnelle d'un membre éminent d'une grande entreprise française a fait l'objet d'un piratage informatique par hameçonnage ciblé (« *spearphishing* »)[1].

L'utilisateur a reçu un mail, contenant une pièce jointe, qui semblait provenir de l'un des dirigeants de la société. L'objet du courriel, le contenu du message ainsi que l'intitulé de la pièce jointe n'ont pas éveillé sa suspicion, bien que l'adresse mail émettrice ait été différente de celle utilisée habituellement. L'employé a alors rentré ses identifiants professionnels afin de récupérer le document proposé en pièce jointe.

Plus de 3 000 mails, dont certains contenants des informations stratégiques et confidentielles, ont ensuite été détournés vers une boîte mail extérieure, dont le propriétaire n'a pas encore été identifié à l'heure actuelle.

[1] Utilisation d'un courriel d'apparence légitime pour obtenir du destinataire qu'il transmette ses coordonnées bancaires ou ses identifiants de connexion à des services financiers afin de lui dérober de l'argent (hameçonnage / *phishing*) ou, dans le cadre d'attaques plus ciblées (hameçonnage ciblé / *spearphishing*), un accès à son réseau professionnel (définition de l'ANSSI).

Commentaires

Comme le montrent les exemples présentés ci-dessus, l'ingénierie sociale peut se pratiquer par contact direct, courriel, lettre ou téléphone.

De nombreuses escroqueries ou tentatives d'escroqueries ont été relevées par le service ces dernières années, facilitées par l'essor de la numérisation au sein des entreprises, ainsi que par l'utilisation croissante des réseaux sociaux. Les auteurs de ces démarches malveillantes ont recours à plusieurs techniques, allant, entre autres, de la « **fraude au président** »[2] à l'« **l'hameçonnage** » (« *phishing* »), en passant par des **tentatives d'intrusion** sur des sites d'entreprises stratégiques, sous couvert d'un prétexte fallacieux ou au moyen d'une fausse identité.

L'ingénierie sociale repose en premier lieu sur l'exploitation de vulnérabilités d'origines humaine, technologique et organisationnelle. Ces techniques confirment que la sécurité d'une société repose sur l'implication de tous et sur une bonne sensibilisation des sociétés et de leurs personnels.

Préconisations de la DGSI

Compte tenu des évolutions et de la recrudescence de ces escroqueries et captations, la DGSI émet les préconisations suivantes :

- **Sensibiliser et informer l'ensemble des salariés sur les modes opératoires** de l'ingénierie sociale, les moments où elle est susceptible de se produire (veille de week-end, période de congés du dirigeant, période stratégique pour l'entreprise, etc.).

- **Mettre en place des procédures robustes de vérification** (chaîne de vérification fiable, désignation d'un interlocuteur habituel avec des coordonnées téléphoniques connues, techniques d'identification, etc.) avant de procéder à une quelconque opération de grande ampleur.

- **Sensibiliser les salariés, notamment ceux du service financier ou comptable,** à ces procédures de vérification.

- **Sensibiliser les salariés à une utilisation responsable des réseaux sociaux** personnels et professionnels, qui constituent une source précieuse d'informations pour les personnes malveillantes, soucieuses de parfaire la crédibilité de leur escroquerie.

[2] Usurpation de l'identité d'un haut dirigeant ou d'un sous-traitant afin de demander au service financier ou comptable de procéder, dans l'urgence, à un virement bancaire sur un compte situé en France où à l'étranger.

- **Définir des procédures strictes en matière de sécurité et se doter d'un référent sûreté**, vers lequel devront remonter tous les cas, avérés ou suspectés, d'ingérence (vols d'ordinateurs ou de téléphones portables, curiosité déplacée de visiteurs, tentatives de vols d'échantillon, stagiaire surpris seul un soir dans un service qui n'est pas le sien, etc.).

- Au besoin, **contacter la DGSI** en cas de découverte ou de suspicion d'un cas d'ingénierie sociale.