Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

INGERENCE ECONOMIQUE

Flash n°56 – Octobre 2019

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°56 Octobre 2019

Les entretiens rémunérés, vecteurs de captation de l'information

En échange d'une compensation financière attractive, plusieurs employés d'entreprises et d'agences institutionnelles françaises ont récemment été contactés afin de participer à des entretiens visant à recueillir des informations précises relatives aux activités et à la stratégie commerciale de l'entreprise. Ces sollicitations émanent la plupart du temps de sociétés ou de cabinets de conseil étrangers.

Cette méthode permet en effet d'obtenir des informations à haute valeur ajoutée sur des filières d'importance, en ciblant notamment des acteurs stratégiques tricolores.

Véritable vecteur de captation d'informations, ce procédé peut faire perdre aux entités ciblées, via leurs collaborateurs, leur éventuel avantage concurrentiel et technologique.

PREMIER EXEMPLE

Un ingénieur, salarié d'une grande entreprise française, a été contacté sur son profil LinkedIn puis sur son mail personnel par une personne se disant mandatée par une société de conseil en management. Cette dernière demandait à l'intéressé de partager, par le biais d'une communication téléphonique, son expertise sur des sujets techniques et hautement stratégiques contre une rémunération importante. L'ingénieur français s'est également vu préciser qu'il serait rémunéré s'il parvenait à parrainer d'autres spécialistes capables de répondre à ce type de questions.

Le salarié visé n'a pas répondu favorablement à cette demande et a avisé immédiatement son service de sécurité, qui n'a néanmoins pas été en mesure d'appréhender l'amplitude de la campagne de démarchage.

Une communication interne a été diffusée au sein de toutes les filiales de l'entreprise afin de sensibiliser l'ensemble des collaborateurs à cette tentative d'ingérence caractérisée.

DEUXIEME EXEMPLE

Plusieurs employés d'une agence nationale française, opérateur d'importance vitale, ont été contactés sur leur boite mail professionnelle par un chargé de mission d'une entreprise

extra-européenne. Ce dernier leur proposait un entretien rémunéré, qui devait porter sur le descriptif complet de leurs fonctions au sein de l'agence.

Face à la multiplication des tentatives, la direction générale de l'agence concernée a envoyé un message au chargé de mission rappelant que ses agents étaient soumis au secret et à la discrétion professionnelle et en demandant d'arrêter immédiatement toute sollicitation.

TROISIEME EXEMPLE

Une dizaine d'ingénieurs R&D, travaillant pour une société développant des technologies de pointe, ont récemment été sollicités sur différents réseaux sociaux professionnels et personnels par des profils se présentant comme des ressortissantes extra-européennes. Ces dernières leur ont proposé de l'argent en échange d'informations confidentielles sur leur employeur.

La direction de la société tricolore n'ayant pas jugé utile d'alerter et de sensibiliser l'ensemble de son personnel sur ce type d'approche déloyale, il est possible que certains employés aient accepté et aient divulgué des informations stratégiques à une entreprise concurrente ou à un service de renseignement étranger.

PRECONISATIONS DE LA DGSI

Compte tenu du risque de captation d'informations, la DGSI émet les préconisations suivantes :

→ Sensibiliser et informer l'ensemble des salariés sur ce mode opératoire.

→ Sensibiliser les salariés à une utilisation responsable des réseaux sociaux personnels et professionnels, qui constituent une source précieuse d'informations pour des acteurs mal intentionnés. Leur indiquer de rester évasifs sur leurs fonctions précises et les thématiques ou projets sur lesquels ils travaillent.

→ Demander aux salariés de faire remonter systématiquement chaque sollicitation extérieure visant à recueillir des informations précises sur l'entreprise auprès de la Direction Sûreté - Sécurité et /ou contacter la DGSI en cas de découverte ou de suspicion d'ingérence.

→ Vérifier l'origine et la légitimité d'un émetteur extérieur avant de répondre à une demande de ce type.

→ Rester évasif en cas de sollicitations.

→ Effectuer une veille réglementaire, juridique, commerciale et technique régulière afin d'être en mesure d'identifier les secteurs ou les technologies susceptibles d'intéresser des entreprises concurrentes étrangères.