Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

INGERENCE ECONOMIQUE

Flash n° 41 - Mars 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°41 Mars 2018

Les vulnérabilités induites par l'utilisation des réseaux sociaux

L'utilisation des réseaux sociaux, à titre personnel ou professionnel, peut constituer une source de vulnérabilités pour les entreprises.

En effet, des concurrents, des agents de services de renseignement étrangers missionnés par des institutions privées ou publiques, ou encore des activistes peuvent utiliser les informations mises en ligne sur ces réseaux afin de nuire aux établissements visés.

1er exemple

Un service de renseignement étranger a ciblé, via le réseau social professionnel LinkedIn, des entreprises spécialisées dans les énergies et la haute technologie.

Ce service a réussi à approcher, grâce à la création d'un faux profil, certains personnels spécialisés de ces sociétés. Après avoir échangé plusieurs mails afin de renforcer la crédibilité du faux profil, un lien leur a été envoyé, sous prétexte d'une offre d'emploi séduisante.

Le lien était en réalité un programme informatique malveillant qui, installé à l'insu des utilisateurs, a permis au service étranger d'infiltrer le réseau de plusieurs entreprises et de collecter un nombre important d'informations stratégiques sur leurs activités et projets en cours.

2ème exemple

Un prestataire de services informatiques pour des opérateurs d'importance vitale (OIV) dispose d'un compte Twitter « collaboratif », qui peut être utilisé par tous les employés de l'entreprise. Ce compte n'est verrouillé par aucun paramètre de confidentialité et peut donc être consulté par des utilisateurs externes à l'entreprise.

L'un des employés de la société a posté une photo sur laquelle on peut voir en arrière-plan la liste des matériels commandés, ainsi que l'emploi du temps de l'ensemble des agents, permettant ainsi à toute personne de collecter aisément des informations sur l'organisation de la société, l'identité de ses personnels et de ses clients.

Commentaires

Les réseaux sociaux constituent une source précieuse d'informations pour des acteurs malveillants qui chercheraient à entrer en contact avec des personnels travaillant dans des entreprises ciblées, première étape d'une démarche potentielle d'ingérence.

Par ailleurs, la publication de certaines informations sensibles internes à l'entreprise est susceptible de porter atteinte aux intérêts de la société, qu'ils soient économiques, sécuritaires ou réputationnels, et aux intérêts du salarié lui-même.

Aussi, il est important de définir et de rappeler les bonnes pratiques en matière d'utilisation de ces réseaux afin de sensibiliser les utilisateurs aux risques potentiels engendrés par leur utilisation.

Préconisations de la DGSI

La DGSI émet les préconisations suivantes :

Concernant les réseaux sociaux en règle générale :

- **Cloisonner ses comptes**. Ne pas faire mention sur son compte personnel de son appartenance à une entreprise et, inversement, ne pas donner de détails personnels sur un réseau social à vocation professionnelle.

- **Paramétrer sa confidentialité** :
  - limiter l'audience des publications et des différents comptes ;
  - vérifier les paramètres de confidentialité après chaque mise à jour.

- Utiliser des **mots de passe robustes et différents** suivant les comptes.

- Utiliser de préférence un **pseudonyme** et une **adresse mail non nominative**.

- Activer la **double authentification** pour éviter les piratages.

- **Rester discret, ne pas communiquer des informations professionnelles et personnelles trop précises,** comme par exemple le niveau d'habilitation au secret de la défense nationale.

- **Effectuer une veille active**, aussi bien pour les personnes physiques que morales, afin de maîtriser son image.

- **Rester vigilant et faire preuve d'une grande prudence** à l'égard des **courriels, liens et pièces jointes reçus** via les messageries des réseaux sociaux.

- Consulter **le site de la CNIL,** qui propose une série de bonnes pratiques en la matière.

Concernant les réseaux sociaux professionnels :

- **Rester vigilant** et **ne pas accepter** les demandes de contact provenant d'inconnu(e)s ou de profils suspects.

- Vérifier **si la photo de profil n'a pas été copiée-collée** depuis Internet, en utilisant les fonctions de recherche inversée par image de Google Images ou TinEye.

- Vérifier **si la description du profil n'a pas été dupliquée depuis un autre compte,** en effectuant une recherche partielle sur un moteur de recherche.

- Vérifier **si la personne existe vraiment** en recoupant les informations disponibles avec des recherches sur Internet avec ses nom, prénom et entreprise.

- Vérifier **si le parcours étudiant et professionnel du profil suspect semble cohérent** (dates, fonctions exercées, villes, etc.).