MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

FLASH DGSI #83

AVRIL 2022

INGÉRENCE ÉCONOMIQUE

LES RISQUES LIÉS AUX SOLLICITATIONS PAR DE FAUX PROFILS SUR LES RÉSEAUX SOCIAUX PROFESSIONNELS

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. Il est également disponible sur le site internet : www.dgsi.interieur.gouv.fr

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

LES RISQUES LIÉS AUX SOLLICITATIONS PAR DE FAUX PROFILS SUR LES RÉSEAUX SOCIAUX PROFESSIONNELS

Les réseaux sociaux professionnels ont vocation à permettre à leurs utilisateurs de se constituer un réseau et de partager du contenu en lien avec leurs activités professionnelles. Utilisés comme des plateformes de recrutement et comme des outils permettant la mise en relation de sociétés, les réseaux sociaux professionnels sont devenus des acteurs incontournables du monde du travail.

La possibilité d'y être démarché incite les utilisateurs à rendre leurs profils attractifs en détaillant leur formation, leurs compétences et les missions réalisées dans le cadre de leurs différents postes.

Des concurrents, des cabinets d'intelligence économique étrangers ou encore des individus malveillants exploitent régulièrement cette démarche de transparence. Après avoir identifié des professionnels occupant des postes sensibles dans les sociétés ciblées, ils peuvent se constituer des identités fictives ou usurper l'identité de salariés et prétendre appartenir à des sociétés réelles, afin de donner davantage de légitimité à leurs approches. Leurs démarches peuvent viser à capter des informations stratégiques sur une entreprise ou un marché, porter atteinte à la réputation de l'entreprise concernée, ou initier des attaques informatiques.

PREMIER EXEMPLE

Un salarié démarché par un faux partenaire de sa société afin d'obtenir des informations stratégiques. À la fin de l'année 2019, un membre d'un laboratoire pharmaceutique a été approché sur un important réseau social professionnel par le représentant d'une société prétendant réaliser une évaluation de la collaboration établie entre sa société et le laboratoire français.

L'étude du compte a permis d'identifier que la photo de profil utilisée provenait d'une banque d'images libres de droits et comportait en outre une adresse de société correspondant à celle d'un centre commercial localisé à l'étranger. La direction du laboratoire, informée de l'approche, ne connaissait pas cette société.

Après accord avec son entreprise, l'employé a accepté un entretien téléphonique avec l'individu. Lors de l'entretien, conduit en anglais, l'interlocuteur s'est montré particulièrement insistant sur les sujets d'étude du laboratoire et sur ses perspectives d'avenir.

Cette tentative d'acquisition d'informations coïncidait avec l'annonce par l'entreprise de plusieurs projets d'expansion internationale. La direction a depuis mis en place une sensibilisation auprès des équipes dans le but de systématiser le signalement de ce type de sollicitations.

DEUXIÈME EXEMPLE

Risque d'atteinte à la réputation d'une société dont le nom et le logo ont été usurpés par un faux profil. Au cours de l'année 2020, un employé d'une société spécialisée dans la sécurité informatique a signalé à son entreprise l'existence de plusieurs profils prétendant appartenir à la société, mais établis dans des villes étrangères dans lesquelles l'entreprise ne dispose d'aucune implantation. Usurpant le logo de l'entreprise, les noms utilisés par ces comptes ne correspondaient à aucun employé de la société et mentionnaient des fonctions fictives.

TROISIÈME EXEMPLE

Un groupe industriel victime d'une intrusion informatique à la suite d'approches répétées d'un faux recruteur auprès de ses collaborateurs. En 2021, plusieurs salariés d'un groupe industriel français ont été la cible d'approches malveillantes sur l'un des principaux réseaux sociaux destinés au monde de l'entreprise. Se faisant passer pour un recruteur, un individu ayant recours à un faux profil leur a proposé des opportunités professionnelles attrayantes.

Après avoir été contactés sur le réseau social, les salariés du groupe ont systématiquement été invités à poursuivre leurs échanges sur une autre application de messagerie, permettant au faux recruteur d'éviter la surveillance exercée par la plateforme. Il a ensuite fait parvenir à ses interlocuteurs une offre d'emploi contenue dans des documents à télécharger, en recommandant de les ouvrir depuis leur ordinateur professionnel. Le téléchargement de ces fichiers, qui contenaient un logiciel malveillant, a entraîné l'exfiltration de données sensibles. Une trentaine de collaborateurs aurait été touchée.

Un rappel des conduites à tenir face à ce type de sollicitations a été diffusé aux salariés et, afin d'éviter le téléchargement de virus sur les postes informatiques de la société, le groupe a décidé de bloquer l'accès aux réseaux sociaux professionnels depuis ses ordinateurs.

COMMENTAIRES

Les risques induits par ces campagnes d'approches de salariés initiées par des faux profils sont souvent sous-évalués. Des contacts sporadiques peuvent cacher une stratégie d'approche globale difficilement identifiable par une entreprise, compte tenu de la discrétion souvent recherchée par les salariés lorsqu'ils envisagent une mutation professionnelle. L'identification de ce type de campagnes repose donc sur la vigilance des employés ciblés et sur leur capacité à signaler toute approche qui leur paraît suspecte. Dans de nombreux cas, ces approches peuvent conduire à l'acquisition d'informations stratégiques par des concurrents.

L'usurpation de l'identité d'un employé d'une société ou le rattachement d'un faux profil à une société existante engendrent également des risques importants en termes de réputation.

Il est donc essentiel de sensibiliser régulièrement tous les salariés, notamment ceux occupant des postes stratégiques, aux risques liés à la mise en ligne d'informations détaillées sur les réseaux sociaux professionnels, afin qu'ils puissent adopter une posture de vigilance lorsqu'ils font l'objet de marques d'intérêt.

PRÉCONISATIONS DE LA DGSI

SENSIBILISER AUX RISQUES LIÉS À LA MISE EN LIGNE D'INFORMATIONS SUR LES RÉSEAUX SOCIAUX PROFESSIONNELS

- **Encourager ses salariés à un usage réfléchi et raisonné des réseaux sociaux professionnels.** Il est recommandé d'ajuster ses paramètres de sécurité et de confidentialité afin de restreindre l'accès du grand public aux informations du profil. Il est également déconseillé de partager des informations personnelles. Par ailleurs, lorsque les salariés occupent des postes stratégiques, des échanges avec leur hiérarchie quant à la présentation de leurs fonctions sur les réseaux sociaux peuvent permettre de limiter les risques de divulgation d'informations sensibles.
- **Effectuer de manière régulière des sensibilisations aux bonnes pratiques et aux règles d'hygiène informatique.** Des formations peuvent être animées en interne par le service chargé de la protection des systèmes d'information. Le personnel peut également être encouragé à suivre les modules numériques de l'Agence nationale en matière de sécurité et de défense des systèmes d'information (Anssi) dédiés à ces sujets.

DÉTECTER UN FAUX PROFIL

- **Prêter attention au taux de remplissage des informations personnelles et professionnelles du profil ainsi qu'à leur cohérence.** Un profil présentant peu d'informations personnelles et un parcours incomplet doit attirer l'attention. Un profil faisant état de plusieurs postes occupés simultanément, ou d'occupations professionnelles en inadéquation avec le lieu de résidence peut être révélateur d'une identité fictive.
- **Apprécier le degré d'interaction du profil.** Un profil ayant peu de relations, peu d'activités ou semblant avoir été créé récemment doit également être traité avec davantage de vigilance. Un profil de création récente faisant état de plusieurs centaines de relations professionnelles doit également faire l'objet d'une attention particulière.
- **Effectuer des vérifications élémentaires sur l'identité indiquée sur le profil.** Il s'agit notamment de s'assurer que le nom et le prénom indiqués sur le profil génèrent des résultats en ligne sur d'autres sites ou plateformes. La plupart des entreprises publient par exemple sur leur site internet les noms des cadres de leur organigramme. Une attention particulière doit également être portée à la photographie utilisée. Il est possible d'utiliser des outils de recherche d'images inversées afin de vérifier que celle-ci ne provient pas d'une banque d'image ou n'a pas été usurpée sur le profil d'une tierce personne.

- **Rester vigilant lors de la première entrée en relation.** Un faux profil réalisé par un individu cherchant à être crédible est difficile à détecter. Il peut s'avérer utile d'effectuer un premier contact, par téléphone ou en visio-conférence, tout en cherchant à confirmer la réputation de l'individu auprès d'autres membres de son réseau.
- **S'interroger sur la légitimité des informations demandées.** Lorsque des informations personnelles, sensibles ou semblant sans lien avec la fonction présentée par l'individu sur son profil sont demandées, cela doit systématiquement éveiller la suspicion de l'utilisateur. Enfin, le téléchargement de fichiers à la demande d'une personne dont l'identité n'a pas été confirmée doit être proscrit.

RÉAGIR FACE À UN FAUX PROFIL

- **Ignorer l'invitation à se connecter émanant d'un profil douteux.** Une demande de contact ignorée empêche le démarcheur d'envoyer de nouvelles invitations. En revanche, refuser une demande laisse l'opportunité au profil de la renouveler trois semaines plus tard.
- **Si la demande a déjà été acceptée, signaler le profil à son entreprise.** Le salarié ciblé est vivement encouragé à signaler l'approche au responsable sûreté ou à la direction de sa société. Celle-ci pourra ensuite chercher à évaluer s'il s'agit d'un cas isolé ou d'un démarchage global ciblant plusieurs salariés.
- **En cas de suspicion ou de détection d'un faux profil, la société concernée peut signaler le compte auprès du service d'assistance du réseau social.** Le service clientèle de principaux réseaux sociaux professionnels porte une attention particulière aux contenus douteux ou frauduleux et dispose d'une plateforme spécifiquement dédiée au signalement des faux profils.
- **Contacter la DGSI en cas d'approche par un faux profil.** Si une société détecte des approches suspectes, elle est invitée à prendre attache avec le Service, qui pourra l'accompagner dans ses démarches.