Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

INGERENCE ECONOMIQUE

Flash n° 60 – Février 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°60 Février 2020

Les risques liés à la divulgation d'informations stratégiques lors de déplacements professionnels à l'étranger

Afin de participer au développement et à la pérennisation des activités de leur société, de nombreux chefs d'entreprises et employés sont amenés à effectuer régulièrement des déplacements à l'étranger[1].

Certains pays extra-européens demandent aux voyageurs, via le téléchargement d'applications dédiées, la création d'une véritable identité numérique afin de profiter de contrôles plus rapides aux aéroports. De même, les questionnaires auxquels se soumettent les employés pour obtenir un visa d'entrée dans le pays visité peuvent être détournés à des fins d'intelligence économique.

Sous couvert d'impératifs de sécurité intérieure, ces dispositifs peuvent permettre à des services de renseignement étrangers d'identifier et de tracer des cadres d'entreprises sensibles et, le cas échéant, d'entraver leur activité commerciale.

PREMIER EXEMPLE

Certains pays proposent de télécharger une application mobile afin d'éviter les files d'attente à l'entrée de leur territoire. Le voyageur scanne lui-même son passeport et le programme génère une carte d'identité numérique. L'usager doit ensuite passer son téléphone au-dessus d'une borne et la fiche est automatiquement intégrée par les services de sécurité aux frontières.

Une fois installées, certaines de ces applications permettent d'accéder à d'autres fonctionnalités du téléphone telles que l'appareil photo, le contenu de la mémoire de stockage USB, le contrôle de la fonction « vibreur » ou la mise en veille de l'appareil, ce qui peut empêcher *de facto* le verrouillage du téléphone par un mot de passe.

Ainsi, ce genre d'applications téléchargeables peut constituer de véritables vulnérabilités pour les voyageurs.

[1] Cf. FI N°48 DECEMBRE « *Les risques de captation d'informations liés aux contrôles aéroportuaires* ».

Commentaires

Sous le prétexte légitime de la sécurité nationale, certains pays peuvent se servir des applications dédiées à la gestion de l'identité numérique des passagers comme des outils efficaces pour cibler et évaluer les profils professionnels des voyageurs arrivant ou transitant sur leur territoire.

Encore au stade de projet pilote, ces applications pourront à terme demander aux utilisateurs de fournir des informations très personnelles comme leurs études universitaires, leurs relevés de compte, leurs dossiers de vaccination ou leurs données biométriques dans le but de créer des profils numériques. Si ces derniers apparaissent comme une opportunité pour les voyageurs en leur permettant de bénéficier de contrôles accélérés aux aéroports, la création d'un tel profil implique également une perte de contrôle des informations personnelles collectées, transmises directement aux autorités du pays visité.

DEUXIEME EXEMPLE

Certains pays demandent aux personnes voyageant sur leur territoire de remplir des formulaires dans l'objectif de leur délivrer des visas d'entrée. Ces questionnaires, particulièrement détaillés et parfois même intrusifs, peuvent ainsi être utilisés à des fins d'intelligence économique.

En effet, certains de ces formulaires posent des questions particulièrement précises concernant des aspects aussi bien personnels (maladie physique ou mentale, addictions, comptes sur les réseaux sociaux, etc.) que professionnels (montant des revenus annuels, nom de l'employeur, poste occupé, nom du supérieur hiérarchique, etc.).

Commentaires

Certains États peuvent user de ce stratagème pour ralentir le développement et l'activité commerciale d'un concurrent français par exemple. En effet, des cadres d'entreprises se rendant dans certains pays extra-européens pour affaires peuvent se voir déboutés dans leur demande d'autorisation de visa dès lors qu'ils répondent positivement – ou négativement – à certaines questions du formulaire.
En outre, les précisions demandées sur l'environnement professionnel du voyageur permettent à ces Etats d'obtenir des informations stratégiques à moindre coût.

PRECONISATIONS DE LA DGSI

Face aux risques d'ingérence économique et de captation d'informations liés à l'ensemble des problématiques évoquées, la DGSI émet les préconisations suivantes :

→ Sensibiliser les personnels susceptibles d'effectuer des déplacements à l'étranger à ces problématiques.

→ Dans le cadre d'un déplacement, privilégier l'utilisation d'un téléphone dédié exclusivement à la mission. Cette pratique permet de limiter le stockage d'informations et de documents sensibles aux seuls besoin de la mission.

→ Avant de télécharger une application, vérifier sa provenance et ses droits d'accès aux données du téléphone.

→ Répondre le plus sincèrement possible aux questions posées dans les questionnaires destinés à établir un visa d'entrée dans le pays, tout en évitant d'entrer dans les détails.

→ Renoncer au stratagème consistant à dissimuler certains déplacements antérieurs (qui ne figureraient pas dans un nouveau passeport par exemple). En effet, une fausse déclaration ou une omission peuvent être lourdes de conséquences, compte tenu des capacités très importantes de recoupement et de croisement de données de certaines administrations étrangères.