Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

INGERENCE ECONOMIQUE

Flash n° 48 – Décembre 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°48 Décembre 2018

Les risques de captation d'informations liés aux contrôles aéroportuaires

Les déplacements à l'étranger sont une étape incontournable de l'activité de nombreuses entreprises. Dans la grande majorité des cas, les employés voyagent avec des appareils nomades (ordinateur portable, tablette, téléphone) professionnels.

Les passages en douane et contrôles aéroportuaires peuvent être l'occasion, pour certains pays, de se livrer à des actes d'ingérence, notamment en accédant aux appareils électroniques des passagers.

PREMIER EXEMPLE

Empruntant un vol long-courrier à la suite d'un déplacement professionnel, depuis un pays étranger vers Paris, le directeur d'une entreprise française a mis son ordinateur dans son bagage en soute. L'intéressé a éteint l'ordinateur et l'a placé dans une enveloppe sécurisée.

En récupérant sa valise à Paris, il a constaté que l'enveloppe sécurisée avait été entièrement ouverte dans le sens de la longueur. Aucun autre effet n'avait changé de place.

L'absence de vol et le fait que seul l'ordinateur ait été manipulé rendent la piste crapuleuse peu probable, laissant planer l'éventualité d'une tentative de recueil des données informatiques de l'appareil, probablement orchestrée par les autorités du pays étranger où est par ailleurs implanté le seul et unique concurrent de l'entreprise française.

DEUXIEME EXEMPLE

Lors de l'enregistrement de ses bagages dans un aéroport étranger, le directeur général d'une société française spécialisée dans le domaine médical se voit remettre, par l'hôtesse, un titre d'embarquement différent de celui de ses collègues, marqué d'un trait de couleur.

Après avoir passé les contrôles de sécurité, il se rend en salle d'embarquement. Un agent de sécurité de l'aéroport lui demande alors de le suivre au motif que son ordinateur portable est suspecté de contenir des substances explosives. Cet agent est accompagné d'un policier en uniforme qui le conduit ensuite dans un local à l'écart des autres voyageurs.

Le directeur de la société tricolore se voit contraint d'allumer son ordinateur afin de prouver qu'il est en parfait état de fonctionnement. Il doit ensuite le remettre au policier qui, à force d'insistance, parvient à obtenir les mots de passe pour déverrouiller la session. L'agent se dirige ensuite vers un local isolé.

Le dirigeant français est ensuite interrogé sur les raisons de sa venue dans le pays, sur les personnes rencontrées et les raisons de ces entrevues. Au bout d'une heure, au terme de son interrogatoire, un policier entre dans le local d'audition pour lui remettre son ordinateur portable, qui, de toute évidence, a été manipulé. Il le récupère et monte, *in extremis*, dans son avion à destination de Paris.

Préalablement sensibilisé par la DGSI, le chef d'entreprise rend compte des événements dès son retour sur le sol français. Il reste persuadé que la marque réalisée sur son titre d'embarquement est un acte prémédité à son interpellation et aux vérifications faites sur son ordinateur portable.

Ce dernier contenait de nombreuses informations stratégiques : données clients, offres commerciales, plans du bureau d'étude, près de 4 000 courriels mais aussi le plan d'évolution de la société jusqu'en 2025. Le mot de passe était simplement composé de huit caractères et la machine n'était pas équipée d'une solution de chiffrement.

Sous un prétexte fallacieux, les autorités étrangères ont probablement mené une action ciblée pour capter des informations techniques et commerciales sur cette entreprise française.

COMMENTAIRES

Les autorités de certains pays procèdent régulièrement à l'inspection des appareils électroniques d'individus souhaitant entrer sur leur territoire. Ils peuvent parfois même faire une copie des données contenues dans les appareils s'ils estiment la démarche nécessaire, sans toutefois devoir donner plus de justifications au propriétaire de l'appareil.

Les autorités de certains États peuvent aussi légalement exiger les codes, mots de passe ou encore les clés de chiffrement pour débloquer les appareils électroniques et avoir ainsi accès aux données qu'ils contiennent.

En cas de refus, le passager concerné peut écoper d'une amende au montant non négligeable, voir ses appareils saisis et peut être refusé d'entrée dans le pays en question.

Ainsi, il faut garder à l'esprit que les contrôles aux frontières opérés dans les aéroports, bien que légitimes en principe, peuvent donner lieu à des captations d'informations. Certains États, sous

couvert de sécurité intérieure, peuvent en profiter pour cibler des employés ou des responsables d'entreprises françaises détenant des informations stratégiques.

PRECONISATIONS DE LA DGSI

Afin de limiter le risque de captation d'informations lors de contrôles aéroportuaires, la DGSI émet les préconisations suivantes :

- Privilégier l'utilisation d'appareils nomades dédiés exclusivement aux déplacements.

- Limiter les informations stockées sur les appareils électroniques aux seuls besoins de la mission.

- Garder ses appareils électroniques avec ses bagages à main, éviter de les mettre en soute. Si des appareils électroniques vont en soute, les mettre dans une enveloppe sécurisée.

- Marquer ses appareils d'un signe distinctif neutre afin de les surveiller et de s'assurer qu'il n'y a pas d'échange.

- Chiffrer les données sensibles grâce à des solutions de chiffrement.

- Faire analyser les appareils électroniques au retour de mission, avant de les connecter aux réseaux internes de l'entreprise.

- Faire remonter au directeur sécurité de son entreprise ainsi qu'à la DGSI tout problème constaté.

- Consulter le document « *Passeport de conseils aux voyageurs* »[1] édité par l'ANSSI qui présente des règles simples à mettre en œuvre lors des déplacements pour réduire les risques liés au nomadisme des données et des équipements.

[1] *Https://www.ssi.gouv.fr/guide/partir-en-mission-avec-son-telephone-sa-tablette-ou-son-ordinateur-portable/*