Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

INGERENCE ECONOMIQUE

Flash n° 46 – Octobre 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°46 Octobre 2018

Les transports en commun, lieux propices à la captation d'informations

Les déplacements quotidiens en transports en commun, incontournables, souvent routiniers et prévisibles, peuvent être propices à la captation d'informations.

Qu'il s'agisse d'actes de malveillance ou de simple négligence, le vol ou la perte d'informations relatives à une entreprise peuvent se révéler préjudiciables pour cette dernière.

PREMIER EXEMPLE

Un cadre d'une entreprise du secteur de l'énergie effectue, chaque semaine aux mêmes horaires, un trajet en TGV pour se rendre sur un site de production qu'il supervise. Il emporte avec lui son ordinateur professionnel et profite, en toute logique, du temps de trajet pour avancer sur des dossiers en cours. Il travaille toutefois sur des documents hautement sensibles, comportant de nombreux schémas de prototypes stratégiques.

Le salarié a signalé récemment au responsable sûreté de sa société la présence régulière d'un individu sur le même trajet et aux mêmes horaires que lui. Cette personne prend chaque fois le soin de s'asseoir à proximité immédiate de l'intéressé.

Sans filtre de confidentialité, les informations sur lesquelles il travaille sont facilement accessibles aux passagers assis à proximité. Il est ainsi aisé pour une personne mal intentionnée de lire ou photographier des informations stratégiques visibles depuis l'ordinateur, à des fins de captation ou d'approche ultérieure du salarié.

DEUXIEME EXEMPLE

Le directeur du développement commercial d'une grande entreprise française attend le métro. Il pose, sur un siège inoccupé à côté de lui, une sacoche contenant un ordinateur portable professionnel. Ce n'est qu'une fois monté dans la rame du métro qu'il réalise l'avoir oublié sa sacoche sur le quai. Il descend à la station suivante, et reprend le métro en sens inverse afin de récupérer sa sacoche qui a disparu entretemps.

L'ordinateur portable contenait des données commerciales stratégiques avec une quinzaine de pays étrangers. Se trouvaient également à l'intérieur de la sacoche des documents relatifs à la

politique du groupe en direction de ces 15 pays, détaillant la stratégie microéconomique, c'est à dire les clients identifiés, les partenaires, ainsi que diverses données internes à l'entreprise.

Même si la probabilité d'un vol ciblé reste minime, la négligence dont a fait preuve ce responsable pourrait avoir d'importantes conséquences sur le développement international de l'entreprise.

TROISIEME EXEMPLE

Un chercheur en physique-chimie a été victime du vol de son ordinateur portable professionnel et de son sac à dos dans un aéroport français. Il devait se rendre dans un pays étranger pour y dispenser une conférence.

L'intéressé, après s'être installé dans le hall des départs, pose son sac ainsi que la sacoche de son ordinateur. Deux individus se rapprochent alors de lui et subtilisent habilement ses bagages.

Les vidéos de surveillance confirment que le vol a été effectué par une équipe chevronnée qui semble avoir réalisé des repérages en amont, et possiblement mené des surveillances sur la cible, éléments pouvant accréditer l'hypothèse d'un vol ciblé.

L'ordinateur contenait quatre années de recherche sur des sujets scientifiques à haute valeur stratégique. Le chercheur n'avait pas protégé particulièrement ses données (pas de solution de chiffrement, date de naissance comme mot de passe, utilisation d'une messagerie en ligne pour communiquer avec ses homologues, etc.).

En raison du motif de son déplacement et de sa connaissance de la sensibilité des données qu'il transportait, le scientifique aurait dû faire preuve de la plus grande vigilance concernant la protection de ses données professionnelles.

PRECONISATIONS DE LA DGSI

Afin de limiter les risques de compromission ou de captation informationnelle dans les transports en commun, la DGSI émet les préconisations suivantes :

- Installer un **filtre de confidentialité** sur les écrans des ordinateurs portables, des tablettes et des téléphones portables à usage professionnel.

- **Ne jamais laisser ses outils de travail**, comme son ordinateur professionnel, **sans surveillance.**

- **Choisir un mot de passe complexe** et **veiller à l'entrer discrètement**.

- **Eviter le plus possible de transporter des données sensibles** lors des déplacements quotidiens, notamment entre le domicile et le travail. Si cela est indispensable, utiliser une **clé USB sécurisée** et la conserver en permanence sur soi. Prévoir une **solution de chiffrement**.

- Faire preuve d'une **extrême vigilance** et d'une **grande attention** quand on se déplace avec des documents internes à son entreprise.

- **Rester discret concernant les sujets liés au travail.** Evoquer le moins possible les dossiers en cours, en personne ou par téléphone, dans les transports en commun.

- Eviter au maximum de **lire ostensiblement** des documents professionnels.

- Eviter de porter de façon visible son badge professionnel **en dehors de l'entreprise.**

- **Ne pas utiliser de WIFI public**[1] sans solution de sécurité de type VPN[2].

[1] *Cf. Flash Ingérence N°23 AVRIL 2016 – Les dangers liés aux Wifi publics*
[2] *VPN : Virtual Private Network*