MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

FLASH DGSI #6868

OCTOBRE 2020

INGÉRENCE ÉCONOMIQUE

les risques induits par les vols d'ordinateurS portableS

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.

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 INDUITS PAR LES VOLS D'ORDINATEURS PORTABLES

Les ordinateurs portables font partie intégrante de la vie en entreprise. Le caractère nomade de ces appareils permet à nombre de salariés, de dirigeants et d'indépendants de travailler à distance, depuis leur domicile ou lors de déplacements professionnels. Leur usage s'est révélé particulièrement utile lors du confinement, en permettant notamment la mise en place rapide de mesures de télétravail afin d'assurer la continuité de l'activité des entreprises. Dans le contexte de la crise sanitaire, le recours aux ordinateurs portables demeure privilégié par de nombreuses entités et offre une plus grande flexibilité aux salariés et collaborateurs qui peuvent travailler à distance, un ou plusieurs jours par semaine.

Les ordinateurs portables et autres supports informatiques nomades font, toutefois, régulièrement l'objet de vols crapuleux ou ciblés et peuvent donc fragiliser la société victime en cas de perte de données sensibles, techniques ou encore stratégiques. Cette menace est d'autant plus importante que de plus en plus de salariés sont amenés à se déplacer avec leur ordinateur portable dans le cadre professionnel.

PREMIER EXEMPLE

Un cadre d'une société française, participant à un important appel d'offres pour un marché public, a été victime du vol de son ordinateur portable et d'une clé USB, qu'il avait laissés à l'intérieur de son véhicule stationné à proximité d'un restaurant où la société organisait un évènement. Les autres objets de valeur présents dans le véhicule n'ont pas été dérobés, accréditant la thèse d'un vol ciblé.

Les deux supports contenaient des données sensibles sur le savoir-faire de l'entreprise, sur les spécificités de l'appel d'offres et sur le cahier des charges établi par l'entreprise. La possession de tels documents par une entreprise concurrente pourrait s'avérer très préjudiciable pour la société victime. Par ailleurs, si l'appel d'offres ou des documents afférents avaient fait l'objet d'une classification spécifique, la société française aurait également été confrontée à un important risque de compromission, délit puni par la loi.

DEUXIÈME EXEMPLE

Une société française, prestataire de services, a été victime du vol d'un ordinateur portable contenant des informations sensibles de son client. L'ordinateur a été dérobé durant la nuit, alors qu'il avait été laissé sans surveillance dans les locaux d'un espace de *coworking* loués pour plusieurs jours. Bien que la porte ait été fermée à clé, aucune trace d'effraction n'a toutefois été relevée. L'ordinateur, non chiffré et protégé par un simple mot de passe de session *Windows*, contenait notamment les plans détaillés d'une structure sensible du client.

Si aucun indice ne permet de conclure à un vol ciblé, la menace d'une utilisation malveillante des informations dérobées est bien réelle pour le client de la société française, confronté ainsi à la fragilisation de sa sûreté bâtimentaire. L'atteinte à l'image et la perte de confiance sont aussi des conséquences directes pour la société française victime du vol.

TROISIÈME EXEMPLE

L'ex-directeur d'une société française a été victime du vol de son ordinateur et de son téléphone portable à son domicile. Aucun autre objet de valeur n'ayant été dérobé, un vol ciblé est donc probable. Malgré son départ récent de la société, l'individu avait conservé dans son ordinateur des données techniques sensibles de l'entreprise relatives au développement, toujours en cours, de certains produits. La société estimait avoir plusieurs années d'avance sur ses principaux concurrents.

En conservant des données stratégiques de son ancienne entreprise sur son ordinateur portable, l'ex-directeur a exposé la société à des risques réels de captation de technologies et savoir-faire, notamment par une entité concurrente. En outre, l'impossibilité pour la victime d'identifier précisément les données dérobées empêche la société d'évaluer le préjudice subi.

COMMENTAIRES

Les vols d'ordinateurs professionnels représentent une menace sérieuse pour les entreprises françaises, particulièrement en raison des données sensibles, techniques ou stratégiques qui peuvent y être stockées. En cas de vol ciblé, ces données peuvent être exploitées par des concurrents, notamment étrangers, pour se positionner sur un marché, capter une technologie ou encore acquérir un savoir-faire.

Les vols d'ordinateurs sont majoritairement le fait d'erreurs d'inattention de la part des utilisateurs. Laisser, même un court instant, un ordinateur sans surveillance, manquer de vigilance dans les transports ou lieux publics, ne pas chiffrer son disque dur, ou négliger l'accompagnement et l'encadrement des salariés lors de leur départ de l'entreprise, sont autant de situations qui peuvent aisément être évitées.

PRÉCONISATIONS DE LA DGSI

FACE AUX RISQUES DE VOLS D'ORDINATEUR, LA DGSI EMET LES PRECONISATIONS SUIVANTES :

- Sensibiliser l'ensemble des collaborateurs, salariés et dirigeants, aux risques induits par l'utilisation d'appareils informatiques nomades ;
- Appliquer les mesures de sécurité informatique (sauvegarde externe de données, mots de passe complexes, chiffrement du disque dur, etc.) ;
- Ne pas laisser les matériels sans surveillance (véhicules, locaux temporaires de *coworking*, etc.) ;
- Connaître l'emplacement des données et classifier les documents selon leur niveau de sensibilité afin de mettre en place des règles visant à un meilleur contrôle et une meilleure sécurisation des informations de l'entité ;
- A l'occasion du départ d'un collaborateur, s'assurer du retour de l'intégralité du matériel informatique détenu ;
- Signaler toute disparition auprès de sa hiérarchie et du service informatique compétent ;
- En cas de vol, déposer rapidement plainte auprès des services de police ou de gendarmerie compétents, ou directement auprès du procureur de la République.

À l'occasion de déplacements professionnels, notamment à l'étranger :

- S'assurer que les matériels électroniques ne contiennent que les données strictement nécessaires au voyage et non sensibles pour l'entreprise ;
- Garder ses appareils à porter de main et ne pas les laisser sans surveillance, notamment lors du passage en douane et dans les hôtels ;
- Apposez un signe distinctif, de type pastille de couleur, sur les appareils pour s'assurer qu'il n'y a pas eu d'échange.