MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER

Liberté
Égalité
Fraternité

FLASH INGÉRENCE ÉCONOMIQUE DGSI #103

Mai 2024

PRÉVENIR LES VOLS DE MATÉRIELS SENSIBLES

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**

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

PRÉVENIR LES VOLS DE MATÉRIELS SENSIBLES

Les entreprises françaises sont régulièrement victimes de vols de matériels sensibles susceptibles de contenir des données relatives à leur stratégie commerciale, leurs clients, leurs développements technologiques ou encore leurs savoir-faire. Les matériels ciblés peuvent être des ordinateurs portables, des tablettes, des supports de stockage (clés USB, disques durs) mais aussi des téléphones portables connectés au réseau de l'entreprise ou encore des prototypes ou maquettes à caractère stratégique.

Ces vols peuvent être commis dans les locaux de l'entreprise et être facilités par des mesures de sécurité insuffisantes, ou être commis à l'extérieur des locaux, lors des déplacements habituels ou ponctuels des cadres et salariés. Dans une grande majorité des cas, ces vols exploitent des imprudences individuelles qui pourraient être évitées par la mise en place de mesures de précaution élémentaires.

Ils peuvent être ciblés et viser spécifiquement le contenu des matériels volés à des fins de captation d'information ou d'espionnage industriel, ou bien constituer des vols crapuleux motivés par la valeur marchande des matériels dérobés. Dans les deux cas, les données contenues dans ces supports sont susceptibles d'être détournées à des fins malveillantes.

1 UNE ENTREPRISE FRANÇAISE SE FAIT DÉROBER DES ORDINATEURS CONTENANT DES INFORMATIONS STRATÉGIQUES DANS DES LOCAUX QU'ELLE S'APPRÊTAIT À QUITTER

Un individu s'est introduit dans les locaux d'une entreprise stratégique française, quelques semaines avant la date prévue de déménagement de la société.

Un individu s'est introduit dans les locaux de l'entreprise, tôt le matin, avant l'arrivée des salariés. La porte principale ayant été laissée ouverte pour les personnels de ménage, l'individu a forcé une seconde porte donnant accès à l'accueil des locaux.

Manifestement familier des locaux et dissimulant son visage à l'approche des caméras de surveillance, l'individu a récupéré des badges d'accès laissés à l'accueil dans un emplacement non-sécurisé pour s'introduire dans les bureaux à l'étage. Il a alors volé plusieurs ordinateurs dont deux contenaient des informations stratégiques sur le lancement d'un nouveau projet majeur pour l'entreprise.

Les ordinateurs dérobés n'étant pas protégés par un système de chiffrement, l'entreprise a redouté que les informations contenues puissent être portées à la connaissance de l'un de ses concurrents. La société a déposé plainte et a mis en place des mesures de sûreté bâtimentaire renforcées dans ses nouveaux locaux afin de se prémunir de nouvelles intrusions.

2 UN GROUPE INDUSTRIEL FRANÇAIS A ÉTÉ VICTIME DE MULTIPLES VOLS DE MATÉRIELS SENSIBLES, DONT UN PROTOTYPE CONFIDENTIEL, EN L'ESPACE DE QUELQUES JOURS

Un groupe industriel français a eu recours à un transporteur pour acheminer un prototype confidentiel depuis son lieu de production vers le site dédié aux essais préalables au lancement de la commercialisation du produit l'année suivante.

Arrivé en fin de journée à proximité du site d'essai, le transporteur n'a toutefois pas pu livrer le prototype immédiatement en raison des horaires d'accueil du site. Il a donc été contraint de passer la nuit dans un hôtel et de stationner son véhicule sur le parking de cet établissement.

Le lendemain matin, le chauffeur a constaté que le prototype avait disparu de son véhicule, dont les portes avaient été manifestement forcées durant la nuit.

En parallèle, plusieurs ordinateurs portables contenant des données confidentielles sur des projets du groupe français ont été dérobés sur plusieurs sites de production. Des plaintes ont été déposées par le groupe industriel.

3 UN INGÉNIEUR D'UNE ENTREPRISE STRATÉGIQUE FRANÇAISE SE FAIT VOLER SON ORDINATEUR PORTABLE PROFESSIONNEL À L'EXTÉRIEUR DE L'ENTREPRISE

Placé temporairement en télétravail à temps complet, un ingénieur d'une entreprise stratégique française a pris l'habitude de se rendre avec son ordinateur portable professionnel dans un parc situé à proximité de son domicile.

Afin de pouvoir répondre à un appel téléphonique alors qu'il travaillait dans le parc, l'ingénieur a posé à côté de lui l'ordinateur équipé d'une carte d'accès à l'espace de travail de l'entreprise et sans en verrouiller la session. Laissé sans surveillance durant quelques minutes, son ordinateur a été dérobé. Il contenait des quantités importantes de données techniques sur une activité sensible de l'entreprise ainsi que sur des négociations avec un important prospect étranger.

L'ingénieur a immédiatement prévenu l'officier de sécurité de l'entreprise du vol de son ordinateur et a demandé au service informatique de désactiver à distance l'ordinateur et la carte d'accès. Il a par ailleurs également déposé plainte le jour même.

Commentaires

Le préjudice d'un vol de matériel contenant des données sensibles de l'entreprise ne se limite pas au seul coût de son remplacement mais inclut également la prise en compte des conséquences potentielles d'une fuite ou d'une perte de données.

Les incidences des captations d'informations liées à des développements technologiques s'évaluent souvent sur le temps long. Il peut s'écouler plusieurs années avant qu'une entreprise victime soit en mesure de percevoir qu'un vol a eu pour conséquence la montée en puissance d'un concurrent ou la mise sur le marché d'un produit similaire au sien.

Dans le cas de vols crapuleux non-ciblés, leur auteur peut par ailleurs chercher à revendre les données dérobées, après avoir découvert l'entreprise qui en est propriétaire, identifier la sensibilité de son activité et le caractère stratégique de ces informations.

Prévenir les risques de vol de matériel sensible

- **Sensibiliser les salariés aux risques de vol de matériels sensibles à l'intérieur et à l'extérieur de l'entreprise.**
  Il s'agit notamment de ne pas laisser sans protection ni surveillance les équipements électroniques contenant des données particulièrement sensibles ou encore des produits innovants comme des prototypes lors de leur transport. Il convient également de rappeler à l'ensemble des salariés et prestataires les consignes de sécurité en vigueur et la nécessité de signaler tout événement ou comportement suspect, même le plus anodin, survenant dans les locaux de l'entreprise.

- **Renforcer les contrôles d'accès pour les locaux hébergeant les matériels les plus sensibles de l'entreprise.**
  La mise en place de systèmes d'accès par badge permet de limiter les risques de vol. Un tel dispositif ne pourra cependant être efficace que si les badges ne sont pas en accès libre et rangés dans des emplacements sécurisés, accessibles uniquement aux personnels chargés de leur attribution. Les matériels sensibles doivent également être conservés de manière sécurisée, a minima dans des emplacements fermés à clé ou dans des armoires fortes.

- **Renforcer la sécurité numérique des matériels hébergeant des données sensibles afin de limiter les risques en cas de vol.**
  Tous les matériels informatiques hébergeant des données sensibles ou stratégiques pour l'entreprise doivent être protégés par des mots de passe, régulièrement actualisés, et un système de chiffrement.

- **Solliciter la DGSI pour des prestations de sûreté bâtimentaire ou des conférences de sensibilisation collectives.**
  Ces prestations visent à diffuser une culture de sécurité au sein des entreprises et à prévenir toute forme de malveillance, notamment les vols de matériels et de données sensibles.

Réagir à la suite d'un vol de matériel sensible

- **Évaluer rapidement la nature et la sensibilité des informations de l'entreprise compromises par le vol.**
  Il s'agit prioritairement d'anticiper tout risque de fuite de données stratégiques. Tout salarié doit signaler dans les meilleurs délais à son employeur le vol d'un matériel sensible qui était placé sous sa responsabilité et lister la nature et la sensibilité des données qu'il contenait. Le RSSI doit également être informé.
- **Effectuer systématiquement un retour d'expérience interne sur les circonstances du vol.**
  Ce retour d'expérience doit permettre d'une part, de rappeler à tous les autres salariés les risques auxquels ils peuvent être exposés et, d'autre part, de mettre en place des mesures préventives afin d'éviter la réitération d'un vol dans des circonstances similaires.

- **Mettre en place une veille active afin d'anticiper une possible mise en vente du matériel volé sur Internet.**
  La surveillance peut notamment porter sur les plateformes d'échanges de biens et services entre particuliers ou sur les plateformes de vente de produits en ligne.

- **Déposer plainte auprès des services de police ou de gendarmerie.**

- **Contacter la DGSI afin de signaler l'incident et de réduire l'exposition de l'entreprise à de nouveaux vols.**
  Le service dispose d'une adresse électronique dédiée aux ingérences économiques :
  securite-economique@interieur.gouv.fr

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER

Liberté
Égalité
Fraternité