MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

FLASH DGSI #94

MAI 2023

INGÉRENCE ÉCONOMIQUE

VOLS DE DONNÉES COMMIS PAR DES SALARIÉS EN FIN DE CONTRAT

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

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

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

FLASH DGSI #94

MAI 2023

INGÉRENCE ÉCONOMIQUE

VOLS DE DONNÉES COMMIS PAR DES SALARIÉS EN FIN DE CONTRAT

La fin d'une relation de travail, qui peut survenir à la suite d'un licenciement, d'une démission, d'une rupture conventionnelle, d'un départ à la retraite ou d'une fin de contrat, peut induire des vulnérabilités pour l'employeur. Qu'il soit volontaire ou imposé, anticipé ou imprévu, le départ d'un collaborateur peut conduire à des comportements condamnables visant à déstabiliser l'entité, notamment par le vol de données stratégiques.

Des salariés sur le départ peuvent dérober des données de leur ancienne entreprise pour de multiples raisons. Ils peuvent s'emparer d'informations critiques afin de les monétiser, de les utiliser pour le compte de leur nouvel employeur, pour le développement de leur carrière ou pour la création d'une d'entreprise concurrente ou bien par volonté de vengeance voire de dénonciation. D'autres vols s'apparentent à de l'opportunisme, le salarié voulant récupérer des éléments qu'il a produit sans véritable intention de nuire. Les informations ainsi obtenues ne sont plus protégées et sont plus facilement exposées à des risques de détournements par des acteurs malveillants.

PREMIER EXEMPLE :

Captation de données d'une société dans le domaine de la santé par un collaborateur étranger dont le contrat n'a pas été renouvelé. Au cours de la nuit précédant son dernier jour de contrat, un collaborateur de nationalité étrangère d'une société sensible du secteur de la santé a accédé à plusieurs dizaines de fichiers confidentiels depuis son domicile grâce à l'outil de contrôle à distance mis en place pour faciliter le télétravail. Confronté aux faits par sa hiérarchie le lendemain matin, alors qu'il venait rendre son badge d'accès, le salarié a reconnu avoir cherché des dossiers pour les exploiter dans le cadre de son futur emploi. Son contrat n'ayant pas été renouvelé, la société a soupçonné son salarié d'avoir agi par vengeance et a porté plainte pour captation de données.

DEUXIÈME EXEMPLE :

Peu avant son départ, un cadre d'une société française, débauché par un concurrent étranger, a procédé à un vol de données stratégiques. Un cadre de haut niveau, employé depuis 30 ans dans un

grand groupe industriel français, a mis fin à sa collaboration dans le cadre d'une rupture conventionnelle afin de rejoindre l'un de ses principaux concurrents étrangers. Lors de son départ, le salarié a procédé à la suppression de ses messages électroniques professionnels et de ses données hébergées sur son espace de travail, ainsi qu'au transfert de celles-ci vers un support de stockage externe. Propriétés de la société, ces données techniques et commerciales étaient considérées comme extrêmement sensibles et strictement confidentielles. En outre, elles recouvrent le périmètre sur lequel le salarié évolue désormais au sein de la société concurrente.

Le jour de son départ, le salarié a par ailleurs été surpris par un de ses supérieurs en train de charger dans son véhicule un grand nombre de dossiers en format papier comportant des données financières et juridiques. Interrompu dans cette opération, la société a récupéré l'intégralité de ces dossiers. Après avoir envoyé plusieurs courriers à l'ex-salarié et à son nouvel employeur, et avoir fait constater les faits par un huissier, la société française a déposé plainte.

TROISIÈME EXEMPLE :

Un employé en *freelance*, dont le contrat a été résilié prématurément, s'introduit dans le système d'information d'une société du secteur du numérique et télécharge des données sensibles. Un consultant employé en *freelance* depuis quelques mois par un groupe français du numérique a attiré l'attention de sa hiérarchie par des comportements suspects et des manipulations inhabituelles alors qu'il effectuait des missions au sein de la direction des systèmes d'information et bénéficiait de droits d'utilisateur étendus. Sa hiérarchie a alors pris la décision de rompre prématurément son contrat. Après sa résiliation, le salarié ne s'est pas présenté au rendez-vous fixé par son employeur afin de restituer son matériel informatique et son badge d'accès. La nuit suivante, bénéficiant de droits informatiques toujours valides, il a consulté des ressources internes et téléchargé des données particulièrement sensibles de la société. Celle-ci a porté plainte et va renforcer les mesures de protection (procédures d'habilitation, droits informatiques, sensibilisation) à l'égard du personnel temporaire et des sous-traitants.

COMMENTAIRES

Agissant délibérément dans l'illégalité, certains employés sur le départ prennent le risque de voler des informations appartenant à leur employeur. Ces actions sont souvent synonymes de perte de savoir-faire pour les sociétés victimes ainsi que d'importants préjudices financiers et commerciaux.

Généralement découvert tardivement, à un stade où il n'est plus possible de collecter des preuves, le vol de données est particulièrement difficile à caractériser, ne permettant ainsi pas toujours aux actions en justice entreprises d'aboutir.

PRÉCONISATIONS DE LA DGSI

PRÉVENIR LE VOL DE DONNÉES SENSIBLES PAR DES SALARIÉS

- **Identifier les données sensibles à protéger.** Il est essentiel d'identifier de façon précise toutes les données considérées comme sensibles pour la préservation du savoir-faire de l'entreprise, notamment les documents en lien avec la propriété intellectuelle. Il s'agit de les répertorier, de les classer et de les stocker en fonction de leur niveau de sensibilité afin de limiter leur accès.
- **Hiérarchiser les accès informatiques au sein de la société en fonction de chaque profil de salarié.** Il s'agit de strictement limiter l'accès aux données de la société aux besoins précis de chaque salarié.
- **Adopter une politique de sécurité des données informatiques et veiller à son application.** Il est possible de mettre en place des règles strictes de sécurité informatique afin de limiter l'exfiltration de données, comme l'interdiction d'envoyer des informations sensibles à des comptes de messagerie personnels ou d'utiliser des dispositifs de stockage comme les clés USB. Le changement systématique des mots de passe des comptes partagés à chaque départ de collaborateurs est également à privilégier. L'Agence nationale de la sécurité des systèmes d'information (ANSSI) propose sur son site internet un cadre de gouvernance de la sécurité des données.
- **Surveiller le comportement des utilisateurs sur le réseau de l'entreprise en mettant en place des moniteurs de surveillance des bases de données.** La mise en place d'un outil d'audit doté de fonctionnalités de collecte de journaux et de production de rapports est indispensable pour maîtriser l'activité des utilisateurs. Ils aident notamment à identifier les salariés ayant accédé à certains types de données, à déterminer le nombre de fois où un utilisateur spécifique a essayé d'accéder à des dossiers, etc.

LORS DU DÉPART D'UN COLLABORATEUR

- **Le jour du départ, s'assurer que le salarié a restitué l'ensemble de ses clés d'accès et matériels.** La société peut prévoir une liste récapitulant les éléments que le salarié devra rendre lors de son départ afin de s'assurer que ce dernier n'a conservé aucun matériel de l'entreprise. Elle garantit ainsi la désactivation des accès de l'ancien salarié et la protection des données sensibles de la société.

EN CAS DE VOLS DE DONNÉES CONSTATÉS

- **Obtenir des preuves claires en collaboration avec l'équipe dédiée à la sécurité informatique de la société.** Le fait de voler les données de son entreprise est constitutif de plusieurs délits. Afin d'apporter des éléments qui pourront être utiles à l'enquête, des preuves tangibles peuvent être rassemblées notamment par le constat d'un huissier de justice.
- **Déposer plainte auprès des services de police ou de gendarmerie, ou directement auprès du procureur de la République.** En cas de vols de données dans des conditions suspectes, le dépôt

de plainte peut permettre d'établir la matérialité des faits et à la société d'obtenir réparation sous la forme de dommages et intérêts.

- **Contacter la DGSI afin de signaler l'incident.** Le service dispose d'une adresse électronique dédiée aux sujets de protection économique : securite-economique@interieur.gouv.fr.