MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

FLASH INGÉRENCE ÉCONOMIQUE DGSI #106

Octobre 2024

VOLS DE DONNÉES PAR DES COLLABORATEURS INTERNES À LA SOCIÉTÉ

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

VOLS DE DONNÉES PAR DES COLLABORATEURS INTERNES À LA SOCIÉTÉ

Dans le cadre de leurs activités, les acteurs économiques et scientifiques sont souvent exposés au risque de vol de leurs données sensibles. Si ces vols sont majoritairement de nature crapuleuse, ils peuvent également viser certaines informations à des fins de captation ou d'espionnage industriel. Les acteurs malveillants vont notamment cibler des données relatives à la stratégie commerciale des entreprises, à leur savoir-faire et leurs développements technologiques, à leur organisation et fonctionnement interne, ou encore à la sécurité de leurs systèmes d'information. Les individus mal intentionnés peuvent également chercher à supprimer ces données, à les modifier ou à en empêcher l'accès.

Ces vols sont souvent commis par des personnels travaillant au sein des sociétés victimes, notamment les salariés en fin de contrat, les stagiaires ou même les prestataires de services. Si les vols surviennent généralement dans les locaux de l'entreprise, ils peuvent parfois être commis depuis l'extérieur, notamment dans le cadre du télétravail grâce aux accès à distance.

1 CAPTATION DE DONNÉES D'UNE ENTREPRISE PAR UN CADRE DÉMISSIONNAIRE

Une société a été victime d'un vol de données commis par un de ses employés ayant démissionné après avoir été recruté par une autre entreprise. L'individu, salarié du groupe depuis une quinzaine d'années, était responsable d'un programme sensible. Peu avant son départ, il a copié sur un disque dur externe plusieurs dizaines de milliers de fichiers depuis son ordinateur professionnel. La majorité correspondait à des données confidentielles, dont notamment un fichier relatif au programme sensible dont il avait la charge.

Un dispositif de surveillance informatique mis en place par l'entreprise durant la période de préavis du salarié a permis de constater le vol de données. La société a alors déposé plainte pour vol, conduisant à l'ouverture d'une enquête judiciaire.

Placé en garde à vue dans le cadre de cette enquête, l'individu a reconnu avoir copié des données liées à ses travaux professionnels mais uniquement à des fins personnelles. Il a toutefois reconnu que la transmission de ces informations à un concurrent était susceptible d'être préjudiciable pour son ancien employeur. Il a par la suite été convoqué au tribunal judiciaire pour une comparution sur reconnaissance préalable de culpabilité (CRPC).

2 VOL DE DONNÉES PAR UN SALARIÉ DE NATIONALITÉ ÉTRANGÈRE

Une société spécialisée dans les services a déposé plainte contre l'un de ses employés, un ingénieur de nationalité étrangère, pour « extraction frauduleuse de données dans un système de traitement automatisé », celui-ci ayant téléchargé frauduleusement plusieurs milliers de documents disponible sur le cloud de l'entreprise. Une grande partie de ces documents étaient particulièrement sensibles et portaient notamment sur l'organisation interne de la société, des sujets commerciaux et des projets conduits à l'étranger.

La plainte a abouti à l'interpellation de l'individu et à la perquisition de son domicile. Il a été ensuite incarcéré, puis placé sous contrôle judiciaire.

3 VOL DE DONNÉES D'UN INDUSTRIEL FRANÇAIS PAR UN EMPLOYÉ D'UN PRESTATAIRE DE SERVICE

Après avoir engagé une société spécialisée dans la transformation numérique, un industriel français a été victime d'un vol de données commis par l'un des ingénieurs du prestataire.

En poste depuis plus d'un an, celui-ci a copié sur une clé USB plus de 5 000 fichiers, dont 300 sans lien avec sa mission. Ces données portaient sur le fonctionnement du système d'information de l'entreprise, notamment sur les règles d'administration du réseau, et sur la politique de sécurité des systèmes d'information de l'entreprise. Détournées, celles-ci pourraient permettre à un acteur malveillant de s'introduire dans le système d'information de l'industriel français.

Après la découverte des faits, l'industriel a déposé plainte contre l'ingénieur qui a été interpellé, et son domicile perquisitionné. Jugé en comparution sur reconnaissance préalable de culpabilité, il a été condamné à une peine d'emprisonnement.

Commentaires

Le risque de vol par un collaborateur interne (employé, stagiaire, prestataire, etc.) est réel. Les auteurs de vols peuvent recourir à des captations pour de multiples raisons (revente, réutilisation pour le compte d'un nouvel employeur ou pour la création d'une entreprise concurrente, vengeance, etc.).
Or, la perte de données sensibles peut avoir d'importantes conséquences pour l'activité des entreprises victimes : perte de savoir-faire stratégique, préjudices financier ou commercial, atteinte à la réputation, perte de confiance des clients, coût des poursuites juridiques, etc.. De surcroît, ces vols sont souvent découverts tardivement par les entreprises, ce qui limite les actions de remédiation.
Dans ce contexte, il est déterminant que les sociétés victimes privilégient le dépôt de plainte en cas de vol de données. Cette démarche permet l'ouverture d'une enquête judiciaire, et constitue le meilleur moyen pour parvenir à sanctionner pénalement les auteurs.

PRÉCONISATIONS DE LA DGSI

Renforcer la protection de ses données sensibles pour prévenir les risques de vols

- **Classer les données en fonction de leur niveau de sensibilité.**
  Il s'agit d'identifier les données considérées comme sensibles pour l'entreprise, de les répertorier rigoureusement et d'adapter leur stockage en fonction de leur niveau de sensibilité.

- **Hiérarchiser les accès informatiques au sein de la société en fonction du profil et des fonctions des employés.**
  Il s'agit de limiter l'accès aux données de la société aux besoins précis de chaque salarié.

- **Renforcer la sécurité numérique des matériels hébergeant des données sensibles.**
  Tous les matériels informatiques hébergeant des données sensibles ou stratégiques pour l'entreprise doivent être protégés par des mots de passe robustes et un système de chiffrement. Les mots de passe doivent aussi être régulièrement actualisés.

- **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.

- **Contrôler le comportement des utilisateurs sur le réseau de l'entreprise en mettant en place des moniteurs de surveillance des bases de données.**
  Il est possible de mettre en place un outil pour examiner les accès des utilisateurs au réseau de l'entreprise. Ces outils aident notamment à identifier les salariés ayant accédé à certains types de données, à déterminer le nombre de fois où un utilisateur a essayé d'accéder à des dossiers, etc. de gouvernance de la sécurité des données.

- **Dans l'hypothèse du départ d'un salarié, s'assurer que celui-ci 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. Il conviendra ensuite de désactiver les accès de l'ancien salarié.

- **Adoption de clauses de non-concurrence.**
  Afin de protéger l'entreprise des débauchages ciblés de salariés, il est possible de mettre en place des clauses de non-concurrence post-contractuelles dans les contrats de travail.

Si un vol de données est constaté

- **Déposer plainte auprès des services de police ou de gendarmerie, ou directement auprès du procureur de la République.**
  Le dépôt de plainte est une procédure simple, rapide et gratuite. Il permet à la victime de se prévaloir de ce statut auprès des services de l'État et de pouvoir bénéficier d'un accompagnement adapté.

- **Rassembler tous les éléments de preuve et éléments de contexte qui seront transmis à l'autorité judiciaire lors du dépôt de plainte.**
  Il convient notamment de prendre note de la date et de l'heure des faits, du nom de la personne à l'origine de l'infraction, et de décrire précisément l'évènement et le préjudice subi.

- **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

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité