INGERENCE ECONOMIQUE

Flash n° 66 – Juin 2020

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°66 juin 2020

Les départs de collaborateurs, situation propice au vol de données stratégiques

La vie de l'entreprise est rythmée par les mouvements de salariés, stagiaires, collaborateurs, etc. Si les départs se déroulent le plus souvent dans de bonnes conditions, certaines situations particulières peuvent en compliquer les modalités, voire nuire à l'entreprise.

Quelle qu'en soit la raison (rupture conventionnelle, licenciement dans un contexte litigieux ou conflictuel, non-renouvellement de contrat, fin d'un stage, démission liée à un mécontentement ou dans le cadre d'un débauchage par un concurrent, etc.), les départs de collaborateurs peuvent générer des situations complexes pour l'entreprise tout en étant difficiles à vivre pour le salarié concerné, qui peut être amené à adopter des comportements visant à déstabiliser l'entité qu'il quitte. Parmi les comportements répréhensibles, la DGSI constate régulièrement le vol de données ou d'informations sensibles.

Le mécontentement ou la rancœur ne sont pas les seules motivations. Les collaborateurs malintentionnés sont également motivés par l'appât du gain généré par la revente des informations dérobées, le respect d'un engagement pris avec une société concurrente lors d'un débauchage, la volonté de proposer les données volées à une autre entreprise pour négocier un meilleur salaire dans le cadre d'un recrutement, le souhait d'utiliser ces données pour lancer un nouveau projet concurrent, etc.

PREMIER EXEMPLE

A la suite d'un licenciement dans un contexte conflictuel, une entreprise française particulièrement innovante est confrontée à la disparition de différents supports informatiques contenant des informations sensibles, incluant des brevets et les procédés de fabrication des produits de la société.

Alors que son licenciement venait de lui être notifié, qu'il lui était interdit de revenir au sein de la société et que ses accès informatiques étaient verrouillés, l'ancien employé est resté quelques heures dans les locaux de son ancien employeur, libre de ses déplacements et sans surveillance. Après son départ, le responsable de la sécurité des systèmes d'information (RSSI) à qui le matériel informatique a été restitué, constate la disparition d'un support de stockage. De très forts soupçons pèsent sur l'ancien employé.

Après de multiples tentatives infructueuses pour récupérer le disque dur manquant auprès de son ancien salarié, l'entreprise a été contrainte de déposer plainte.

L'exploitation des données volées pourrait nuire gravement à l'entreprise française.

DEUXIEME EXEMPLE

Un grand groupe français a fait l'objet d'une tentative de vol de documents confidentiels commis par un stagiaire chinois, étudiant dans une grande école de commerce française.

Lors de son dernier jour de stage dans un département sensible de l'entreprise, un ressortissant chinois a été surpris en train de remplir une valise avec de nombreux documents confidentiels. S'il n'avait pas été surpris, il aurait pu revendre ces informations ou les utiliser pour le compte de la société qui envisageait de le recruter à l'issue de son stage. Dans ce cas, aucun élément ne permet d'affirmer que le stagiaire chinois ait agi pour le compte de son futur employeur. Toutefois, cette société aurait pu, à son insu, s'appuyer sur les connaissances acquises illégalement par son nouvel employé.

TROISIEME EXEMPLE

Une société française, après s'être séparée à l'amiable de l'un de ses employés, a constaté une fuite de savoir-faire importante au bénéfice direct d'un concurrent étranger.

En dépit de déclarations évoquant une réorientation professionnelle pour justifier son départ de l'entreprise, l'ancien employé a en réalité été recruté par ce concurrent étranger.

Alors qu'il disposait de connaissances pointues sur les caractéristiques techniques des produits ainsi que sur l'environnement commercial de la société française, il est également soupçonné d'avoir emporté des données sensibles appartenant à son employeur lors de son départ. Il a réussi à maintenir un lien avec ses anciens collègues lui permettant d'organiser de nouveaux débauchages au profit de la société étrangère, tout en continuant à être informé des évolutions internes au sein de l'entreprise française.

COMMENTAIRE

Si chaque départ de collaborateur implique pour une entreprise une perte savoir-faire, le vol de données représente dans ces circonstances un véritable acte de déloyauté et de nuisance.

Il est important de souligner que les conséquences potentielles des vols de données commis par des anciens salariés au moment de leur départ sont rarement identifiables immédiatement pour l'entité visée. Le préjudice pour l'entreprise française se révèle le plus souvent plusieurs mois ou années après le vol.

L'exploitation des informations dérobées, leur revente à un concurrent ou encore leur destruction, lorsque la société française ne dispose pas de copies ou de sauvegardes, représente une menace majeure pour les entités victimes de ces vols de données de la part d'anciens collaborateurs sur le départ.

PRECONISATIONS DE LA DGSI

Face aux risques de vol de données induits par le départ de collaborateurs, la DGSI émet les préconisations suivantes :

→ Une charte doit être signée précisant les engagements du collaborateur vis-à-vis des règles de bonne conduite édictées par l'entreprise ou l'administration, y compris en cas de départ anticipé, voire contraint, de l'entreprise.

→ Le RSSI doit mettre en place une politique stricte encadrant le départ de tout employé, notamment la restitution anticipée et effective des matériels informatiques (ordinateurs, disques durs, smartphones, etc.), ainsi que le blocage immédiat des accès informatiques, notamment en cas de départ « à risques ». Plus généralement, une attention particulière doit être apportée à ce que l'ensemble des documents sensibles confiés soit restitué, ce qui implique de connaitre les documents, et leur classification, auxquels le collaborateur a eu accès.

→ Par précaution, et de manière systématique, il convient ainsi de classifier le niveau de sensibilité des informations au sein de l'entreprise et, au besoin, de renforcer le cloisonnement de l'information pour l'ensemble des collaborateurs. Il s'agit ainsi de limiter l'accès aux informations les plus sensibles aux seuls besoins des différentes missions confiées à chaque employé.

→ En cas d'utilisation d'outils numériques partagés et d'accès à distance à des logiciels et bases de données, s'assurer du changement des mots de passe dès qu'un collaborateur quitte le groupe de travail ou la structure d'accueil.

→ En amont des départs, notamment lorsque l'employé à eu accès à des données sensibles, mobiliser l'ensemble des services internes concourant à la protection de l'information dans l'entreprise afin d'évaluer le risque de fuite d'informations au cas par cas et, le cas échéant, mettre en place les mesures visant à minimiser le risque de perte ou la menace d'un vol de données.

→ Sensibiliser l'ensemble des salariés au cours de leur parcours professionnel.

→ Déposer plainte auprès des services de police ou de gendarmerie, ou directement auprès du procureur de la République, pour tous vols ou disparitions de données dans des conditions suspectes.