Mouvement des Entreprises de France

Ingérence économique : Le dernier Flash de la DGSI Sécurité économique

Publié le 25 juin 2020

La DGSI Sécurité économique, publie régulièrement un « Flash Ingérence Économique » évoquant des actions dont des sociétés françaises sont régulièrement victimes. Ce flash apporte à la fois des témoignages et des réponses et parades. Le flash n° 66 vient de paraître Il traite des risques de vols de données stratégiques en cas de départ de collaborateurs.

Départs de collaborateurs : attention 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 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 de stage, démission ou débauchage par un concurrent, les départs de collaborateurs peuvent générer des situations complexes pour l'entreprise comme 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 peuvent également être motivés par exemple, par l'appât du gain généré par la revente des informations dérobées, ou par le souhait d'utiliser ces données pour lancer un projet concurrent.

Le flash Ingérence économique illustre ce cas par trois exemples

Les préconisations de la DGSI

Pour faire face à ces vols de données qui représentent pour l'entreprise un acte de nuisance pouvant être lourd de conséquences, 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. Plus généralement, une attention particulière doit être apportée à ce que l'ensemble des documents sensibles soit restitué.
- 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.

- 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.
- 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.

>> Télécharger le flash N° 66

>> Pour toute question s’adresser à : securite-economique@interieur.gouv.fr