Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

# INGERENCE ECONOMIQUE

Flash n° 32 – Avril 2017

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°32 Avril 2017

# Risques générés par le manque d'encadrement des stagiaires au sein des structures publiques et privées

Entreprises et laboratoires accueillent fréquemment des personnels temporaires étudiants (stagiaires ou alternants), présents dans leurs locaux pour une durée s'étalant parfois sur plusieurs mois.

Ce phénomène est accentué par l'internationalisation des échanges économiques et des savoirs, notamment par le biais d'échanges universitaires, favorisant l'accueil de stagiaires étrangers dans les structures publiques et privées françaises. Certains pays incitent d'ailleurs fortement leurs étudiants à privilégier un cursus universitaire à l'étranger, par le biais d'autorisations spécifiques et de soutiens officiels, notamment financiers. Ces étudiants se retrouvent ainsi dans des programmes de formation français requérant l'accomplissement d'un stage d'application.

Ces missions se déroulent parfois au sein d'entreprises ou de laboratoires de secteurs stratégiques ou innovants (industries de pointe, recherche, start-up innovantes). Certains stagiaires, totalement intégrés aux équipes, peuvent avoir accès à des informations sensibles, induisant une potentielle vulnérabilité si le périmètre d'accès et les droits de la personne n'ont pas été définis précisément en amont.

## 1er exemple

Un employé binational du secteur des fusions-acquisitions a copié des données d'un serveur chiffré, grâce notamment à une carte d'identification et à des codes d'accès appartenant à un stagiaire présent dans l'entreprise à ce moment-là. Après avoir récupéré les documents sur un serveur non-sécurisé, l'employé les a envoyés sur sa messagerie personnelle. Parmi les pièces copiées, figuraient des documents concernant des contrats de vente sensibles, co-traités avec une entreprise tierce, pour qui cette captation frauduleuse est également dommageable. Ces documents étaient tous strictement confidentiels.
Bien que les accès informatiques dans l'entreprise aient fait l'objet de cloisonnement, l'employé a pu accéder au serveur chiffré via les identifiants du stagiaire, car il était d'usage que les stagiaires les laissent à disposition des autres employés pour des raisons pratiques de connexion à certaines applications. Cette négligence concernant les droits informatiques a ainsi généré une vulnérabilité pour l'entreprise.

**2ème exemple**

Un élève ingénieur étranger, employé en tant qu'apprenti sur un site industriel de matières premières sur le territoire national, a quitté son lieu d'emploi en omettant de restituer le fichier informatique contenant le « plan de sécurisation » de l'unité pour laquelle il travaillait. Ce document intégrait les analyses des équipements et définissait leurs défaillances et points de vulnérabilité. Malgré les tentatives de récupération de la part de l'entreprise, l'ex stagiaire, qui n'a pu être contacté immédiatement, n'a restitué les documents que 4 mois après son départ, prétextant penser les avoir rendus en partant. Il a par ailleurs précisé être retourné dans son pays d'origine.

L'incident a fait prendre conscience au responsable sûreté du site des lacunes dans le suivi et l'encadrement des stagiaires concernant les supports informatiques dont ils sont détenteurs durant leur contrat.

**3ème exemple**

Une unité mixte de recherche médicale française, travaillant sur des sujets sensibles dans des domaines de pointe, a accueilli en son sein un stagiaire d'origine étrangère dans le cadre d'un programme universitaire d'échange. Son encadrement a rapidement identifié un décalage entre son curriculum vitae et son niveau de compétence réel, jugé faible. L'attitude de l'étudiant a, en outre, attiré l'attention du personnel du laboratoire, au regard de son tropisme marqué pour des domaines sans lien avec ses travaux. Il a en outre été surpris prenant des clichés photographiques de certaines zones du laboratoire, s'est intéressé aux disques durs de sauvegarde de la structure et a tenté de filmer une expérience résumant toutes les manipulations d'un personnel du laboratoire.

Après recherches, il est apparu que le stagiaire avait des intérêts dans plusieurs sociétés ou laboratoires concurrents de l'établissement français.

**4ème exemple**

Une entreprise française spécialisée dans la R&D pour la machinerie industrielle, travaille à un projet de joint-venture avec un intermédiaire étranger pour l'obtention d'un marché dans ce pays. Dans le cadre de ce projet, le PDG de l'entreprise étrangère a fortement « suggéré » de former de manière régulière deux ou trois étudiants originaires de son pays sur les sites hexagonaux de l'entreprise française, afin de les former et de les embaucher à terme dans la joint-venture. Le directeur de l'entreprise française s'est montré hostile à cette proposition, une salariée de son entreprise ayant surpris les stagiaires dans des parties de l'établissement qui leur étaient interdites, notamment les bureaux de R&D. Les stagiaires sont en outre apparus peu qualifié pour les tâches qui leur étaient demandées.

**5eme exemple**

Un stagiaire effectuant une mission dans le service SSI d'une administration et travaillant sur l'architecture dudit établissement, a sollicité l'aide d'un de ses enseignants afin de trouver la solution à un problème. Pour ce faire, il a envoyé à son professeur une copie de l'architecture concernée afin qu'il puisse l'aider dans sa recherche, exposant ainsi des données stratégiques pour l'établissement.

## Commentaires

La présence de stagiaires au sein d'entités françaises est inévitable et constitue un atout pour le rayonnement des établissements concernés.

Cependant, au regard des exemples cités, même s'il n'est pas toujours prouvé que la démarche des stagiaires ait été frauduleuse ou malveillante, leur présence n'en constitue pas moins une potentielle source de vulnérabilité pour le patrimoine de la structure hébergeante ou le potentiel scientifique et technique national.

En outre, certains concurrents ou pays tiers n'hésitent pas à « placer » des stagiaires dans le but de capter des informations ou de faire bénéficier ces derniers de formations à bon compte sur des technologies non maîtrisées.

Les manquements aux règlements de l'entité accueillante, ou l'accès à des données confidentielles, sont souvent favorisés par une politique d'accueil des stagiaires floue de la part des établissements. Le traitement de ces personnels temporaires est trop fréquemment négligé alors qu'ils devraient être informés et soumis aux mêmes obligations que l'ensemble du personnel de l'entreprise (émargement d'une charte informatique, clause de confidentialité…). Leurs accès physiques et informatiques doivent également être précisément déterminés et restreints aux seuls travaux de leur ressort. Par ailleurs, il est important de sensibiliser les référents du stagiaire à la nécessité d'informer de tout comportement anormal les personnes en charge de la sécurité.

Ajoutons qu'en cas de vol ou de fuite de données, **le Règlement général sur la protection des données[1] exposera les entreprises et administrations qui n'auront pas mis en œuvre toutes les mesures techniques et organisationnelles appropriées pour s'assurer de la protection des données à caractère personnel à de substantielles amendes** (2% à 4% du chiffre d'affaires annuel mondial pour les grands groupes, 10 à 20 millions d'euros pour les autres entités, publiques ou privées).

## Préconisations de la DGSI

Compte tenu de la présence de plus en plus fréquente de stagiaires étrangers dans les entreprises, la DGSI émet les préconisations suivantes :

- Identifier précisément le périmètre d'accès physique du stagiaire. Limiter si possible son accès à l'entreprise aux heures ouvrables afin d'éviter qu'il se trouve seul dans l'établissement
- Limiter les accès informatiques, notamment concernant des données sensibles ou stratégiques
- Faire signer au stagiaire la charte informatique de l'établissement (non partage des codes d'accès, identifiants, etc.)
- Faire signer un engagement de sécurité/confidentialité et avertir les stagiaires des sanctions en cas de non-respect des consignes internes à l'entreprise
- Sensibiliser le maître de stage/référent sur les risques potentiels afin que celui-ci reste vigilant quant à l'encadrement du stage et signale tout comportement suspect. Dans la même optique, sensibiliser les personnels de l'équipe d'accueil afin qu'ils respectent la politique de confidentialité des données

[1] Le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, abrogeant la directive 95/46/CE, entrera en application le 25 mai 2018.