Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

INGERENCE ECONOMIQUE

Flash n° 50 – Février 2019

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. Néanmoins, les entreprises et administrations qui auraient constaté des modes opératoires identiques ou similaires sont invitées à contacter la DGSI.

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°50 Février 2019

Les risques générés par le manque d'encadrement des consultants extérieurs

De nombreuses entreprises ont recours à des consultants externes à l'entreprise aux fins de sous-traiter des missions de conseil dans des domaines spécifiques (ressources humaines, management, finances, RSSI, réorganisation, etc.).

Ces missions peuvent parfois se dérouler au sein de sociétés stratégiques ou innovantes. Certains consultants, totalement intégrés aux équipes et présents au sein de l'entreprise pendant plusieurs mois, voire parfois plusieurs années, peuvent néanmoins avoir accès à des informations sensibles, induisant une potentielle vulnérabilité pour le patrimoine informationnel de la structure hébergeante.

PREMIER EXEMPLE

Une entreprise spécialisée dans le transport de matières premières a déposé plainte contre un ingénieur consultant, prestataire pour le compte d'une société de conseil, pour avoir exfiltré des données confidentielles portant sur des technologies innovantes.

L'entreprise l'accuse en effet d'avoir transféré plus d'une soixantaine de courriels contenant des informations stratégiques, de son poste de travail vers sa messagerie privée et celle de sa supérieure hiérarchique au sein de la société prestataire de services.

L'enquête menée révèle une organisation défaillante et une négligence certaine de l'entreprise hébergeante, notamment dans le recrutement et l'encadrement des consultants extérieurs, pourtant chargés de travailler sur la R&D de l'entreprise.

DEUXIEME EXEMPLE

Un téléphone portable a été dérobé au sein d'une unité à accès règlementé d'une grande entreprise française. Cet appareil contenait, outre la traditionnelle carte SIM, une carte « micro SD » contenant des informations et des logiciels portant sur une technologie innovante de l'entreprise.

La consultation des vidéos de surveillance ainsi qu'une enquête interne ont permis de confirmer l'implication d'une consultante extérieure de nationalité étrangère, qui avait été la dernière à avoir manipulé l'appareil et attiré à plusieurs reprises l'attention de ses supérieurs du fait de son intérêt pour des sujets stratégiques étrangers à son domaine d'étude.

Selon l'entreprise tricolore, un concurrent étranger parvenant à entrer en possession du téléphone pourrait bénéficier d'une grande avancée technique en accédant aux données relatives à la technologie concernée. En outre, la technologie présente sur l'appareil n'est pas commercialisée dans le pays d'origine de la consultante, qui pourrait ainsi avoir été missionnée pour la dérober.

COMMENTAIRES

Les entreprises ne disposent pas toujours en interne de toutes les compétences nécessaires à leur développement, et font ainsi parfois faire appel à des spécialistes externes à des fins de conseil.

La présence de personnes extérieures à l'entreprise qui travaillent sur des domaines techniques, parfois à haute valeur ajoutée, constitue potentiellement une vulnérabilité pour le mandataire.

Comme pour l'accueil des stagiaires, le traitement de ces personnels temporaires et externes est trop fréquemment négligé, alors qu'ils devraient être sensibilisés et soumis aux mêmes règles que l'ensemble du personnel permanent[1].

PRECONISATIONS DE LA DGSI

Face au risque d'ingérence et aux pratiques de certains consultants, la DGSI émet les préconisations suivantes pour limiter les risques de captation du patrimoine informationnel des entreprises :

- S'assurer que les contrats de prestation de service comportent :
  - une clause de confidentialité ;
  - une clause permettant le changement du consultant en cas de suspicion de compromission ;
  - une clause précisant que le consultant est soumis aux règles de l'entreprise hébergeante (règlement intérieur, charte informatique, politique de sécurité des systèmes d'information, etc.) ;
  - le cas échéant, une clause éthique.

[1] *Cf. FI N°32 AVRIL – Risques générés par le manque d'encadrement des stagiaires au sein des structures publiques et privées.*

- S'agissant des prestations de services portant sur des actifs sensibles de la société émergente, demander régulièrement les preuves de la conformité du prestataire au contrat en ce qui concerne la protection des données de la société hébergeante.

- Inclure une clause de confidentialité dans le contrat passé entre l'entreprise et le consultant.

- Définir en amont avec l'équipe d'accueil du consultant les sujets qui pourront être abordés, les détails dévoilés et ceux qui devront restés confidentiels.

- Identifier précisément le périmètre d'accès physique du consultant. Limiter son accès aux locaux de l'entreprise aux heures ouvrables afin d'éviter qu'il se retrouve seul dans l'établissement.

- Limiter ses accès informatiques, notamment concernant les dossiers sur lesquels il ne travaille pas.

- Privilégier, dans la mesure du possible, des cabinets de consultants français, ou à défaut européens, dotés de personnels n'ayant pas travaillé pour un concurrent dans un passé proche et/ou n'ayant pas la nationalité d'un pays avec lequel l'entreprise a des intérêts opposés.

- Sensibiliser le personnel afin que tout comportement suspect soit signalé au responsable sécurité.

- Interdire le recours à des outils et matériels du consultants, qu'ils soient personnels ou fournis par son employeur (PC portable, plateforme collaborative, etc.).

- Contacter la DGSI en cas de découverte ou de suspicion de tentative de captation d'informations.