Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

INGERENCE ECONOMIQUE

Flash n° 26 - Septembre 2016

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.

Par souci 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°26 Septembre 2016

Certaines pratiques assurantielles peuvent induire des vulnérabilités en termes d'ingérence économique

En cas de sinistre, les assurances, qu'elles soient facultatives ou obligatoires, contribuent à préserver la pérennité des entreprises. Au-delà de la protection des actifs corporels, la gestion des risques, indissociable du processus assurantiel, aide les entreprises à adapter leurs prises de décision dans un environnement incertain.

Dresser la cartographie des risques de l'entreprise assurée nécessite l'acquisition d'une connaissance fine de son « business model » et un diagnostic précis de ses vulnérabilités. Or, ces informations, utiles dans une démarche d'assurance et de gestion des risques, relèvent de la stratégie de l'entreprise. En outre, face à l'émergence de risques nouveaux, certaines compagnies d'assurances n'hésitent pas, lors de la souscription, à effectuer des audits et à demander des informations très sensibles aux entreprises.

Ainsi, une vigilance particulière doit être portée au maintien de la confidentialité de ces informations, eu égard aux différents traitements dont elles pourraient faire l'objet.

Vous trouverez ci-dessous deux exemples représentatifs de scénarii de menaces :

Exemple 1 : Proposition d'externalisation de la gestion du risque entreprise

Une entreprise française en restructuration a récemment été démarchée, avec insistance, par un courtier en assurances qui proposait l'externalisation de la fonction gestion des risques, elle-même à la base de l'évaluation des besoins assurantiels de la société. Un engagement dans cette démarche aurait permis aux prestataires extérieurs d'avoir une connaissance approfondie de la société induisant, de fait, un risque de captation de ces informations stratégiques par des acteurs tiers.

Exemple 2 : Audits des réseaux informatiques lors de la souscription d'une « assurance-cyber »

Victime de plusieurs tentatives de faux ordres de virements bancaires déjouées, une entreprise française s'est récemment intéressée aux assurances nouvellement proposées contre les cyber-escroqueries. Elle constate cependant que sont exigés par les compagnies d'assurances, à l'appui de ces contrats, des audits poussés des réseaux informatiques des entreprises assurées. Ces dispositions inquiètent d'autant plus que les assureurs recommandent des audits effectués par des sociétés de services et d'équipements informatiques qui, pour beaucoup, sont étrangères.

Commentaire

Si le recours aux assurances est indispensable pour la pérennité de l'entreprise, notamment face à la montée de risques émergents, il convient de s'assurer du respect de la confidentialité des échanges et des données transmises.

Préconisations de la DGSI

- Prévoir avec soin le périmètre des données qui seront transmises et éventuellement protéger celles-ci par une clé de chiffrement connue seulement de l'entreprise ;
- S'enquérir des éventuelles transmissions externes de ces données que le prestataire de services pourrait être amené à faire ;
- Signer, avec l'appui du service juridique, un accord de confidentialité précisant les modalités d'accès et de traitement des données, assorti d'un état nominatif - et évolutif - des personnes autorisées ;
- S'assurer des conditions de stockage et de sécurité des données transmises ;
- Lorsqu'un audit est nécessaire, recourir à un Prestataire d'audit de la sécurité des systèmes d'information (PASSI) qualifié par l'ANSSI ou, a minima, à un prestataire n'ayant aucun lien avec une activité de vente de matériels ou de services informatiques.