Flash N° 1 – le 18 juillet 2012

Flash
ingérence économique

Ce « flash » de l'ingérence économique relate un fait dont une entreprise française a récemment été victime. Ayant vocation à illustrer la diversité des comportements offensifs susceptibles de viser les sociétés, il est mis à votre disposition pour vous accompagner dans la diffusion d'une culture de sécurité au sein de votre entreprise.

Vous comprendrez que par mesure de discrétion, le récit ne comporte aucune mention permettant d'identifier l'entreprise visée.

Pour toute question relative à ce « flash » ou si vous souhaitez nous contacter, merci de nous écrire à l'adresse :
securite-economique@interieur.gouv.fr

Opération de recueil de renseignement économique réalisée par des agents de sécurité d'entreprises étrangères

Un cadre d'une société française spécialisée dans les NTIC s'est vu demander son ordinateur portable professionnel par le service de sécurité d'une entreprise partenaire au cours d'un voyage d'affaires à l'étranger. Prétextant un contrôle de sécurité, des agents lui ont demandé son ordinateur portable lors de la sortie de l'entreprise.

Ces faits se sont reproduits dans une autre société du même pays à l'égard d'un cadre d'une société française différente. Dans cette seconde situation, la « victime », étonnée de la pratique, a décidé de rejoindre les agents au poste de sécurité. Il les a alors surpris en train de procéder au copiage de son support nomade à partir d'une clé USB. Déstabilisés par la présence du propriétaire de l'ordinateur, les agents lui ont immédiatement restitué son bien.

Commentaire :

Cette manœuvre est régulièrement commentée par la DCRI lors des conférences de sensibilisation à la sécurité économique.

Un périphérique externe (disque dur ou clef USB), doté de son propre système d'exploitation, est connecté à l'ordinateur avant son allumage**. Cette technique permet à l'attaquant d'avoir accès à l'ensemble du disque dur de l'ordinateur cible sans laisser de trace**. Elle est généralement mise en œuvre par les services de renseignement étrangers s'abritant derrière les contrôles de sécurité aéroportuaire ou lors de « visites » plus discrètes dans les chambres d'hôtel.

Cette situation, à laquelle ont été confrontés deux cadres français, confirme la prudence qu'il convient d'adopter lors de déplacements, en particulier à l'étranger, où le matériel informatique peut être retenu par des services officiels dans les aéroports pour des motifs liés à la sécurité. Ces deux cas d'espèces illustrent un aspect jusqu'alors demeuré discret de la politique offensive de recueil d'informations économiques menée directement par des industriels.

Il convient de définir au sein de chaque entreprise une politique de sécurité des systèmes d'information, afin de protéger efficacement les données contenues dans les ordinateurs lors de déplacements professionnels.

La DCRI dispose de plusieurs niveaux de préconisation pour la protection des supports nomades.

► La première consiste à utiliser une solution de chiffrement du disque dur. Des logiciels existent à différents coûts. Comme une assurance, le choix dépendra de la valeur et de l'importance stratégique de l'information à protéger.

► La seconde consiste à mettre en place quelques règles élémentaires de sécurité informatique : mot de passe à l'allumage de l'ordinateur (au « boot »), désactivation de la possibilité de « booter » sur un disque externe, etc.

► Dédier un ordinateur pour les déplacements à l'étranger. Celui-ci ne doit contenir que les informations en lien avec le motif du déplacement.

► Mettre les informations sensibles sur une clef USB chiffrée et la conserver lors du séjour.

Que faire en cas d'intrusion ?

► Avant tout, il est important de rendre compte de l'incident au sein de l'entreprise. Une évaluation à froid permet de bien analyser les conséquences pour l'entreprise de cette corruption d'informations : impact sur la stratégie commerciale, marketing, etc., sur les accords de confidentialité, sur l'image de la société ...

► Un dépôt de plainte doit être envisagé si la législation du pays comporte une disposition similaire à la notion française « d'intrusion dans un système de traitement automatisé de données ».