



Flash N° 15 – 6 mai 2015

Flash Ingérence Economique

Ce « flash » de l'ingérence économique relate un fait dont une entreprise française a récemment été victime. Ayant vocation à illustrer la diversité des situations et comportements auxquels nos acteurs économiques sont susceptibles d'être confrontés, 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, bien vouloir nous écrire à l'adresse :

securite-economique@interieur.gouv.fr

Rappel des droits et devoirs des salariés en entreprise en matière de sécurité informatique

Il n'est pas rare que des salariés soient surpris en train, au sein de leur entreprise, d'utiliser des outils de type Keylogger – permettant l'enregistrement des touches utilisées sur le clavier – et des logiciels visant à capter et à forcer les mots de passe de sessions de systèmes d'exploitation. Or, dans la majorité des cas, aucune sanction n'est prise par les employeurs, y compris lorsque les auteurs des faits sont animés d'intentions malveillantes et non simplement ludiques. Dans un raisonnement inspiré du droit du travail, l'employeur – arguant par exemple de ne pas disposer de charte de sécurité informatique spécifiant les comportements à respecter, ainsi que les sanctions applicables – estime qu'à défaut d'avoir porté par écrit à la connaissance de l'employé la réglementation en vigueur au sein de l'entreprise, celui-ci ne peut être légalement sanctionné.

Commentaire :

Il est important de rappeler que **le seul fait** de collecter des données à caractère personnel par un moyen frauduleux est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende (article 226-18 du Code pénal) et ce, quelles que soient les intentions du salarié. De même, le fait de s'introduire frauduleusement dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans de prison et de 30 000 euros d'amende (article 321-1 du même code). La loi est d'application directe et ne nécessite pas d'être citée dans une charte informatique pour en assurer le respect par les salariés. Les employeurs peuvent donc prendre immédiatement les sanctions afférentes à une telle faute.

En outre, la responsabilité de l'employeur peut se voir engagée par ce type d'agissements, sur la base de plusieurs fondements :

- la personne cible/victime des menées de son/ses collègues pourra, en cas de dommage, agir contre l'employeur, responsable de ses salariés. Il reviendra alors à la société de prouver que le mis en cause a agi « *hors des fonctions auxquelles il était employé, sans autorisation et à des fins étrangères à ses attributions* », ce qui est rarement admis en pratique.
- de par la jurisprudence « Sarenza c/ Jonathan » du 21 février 2013, le juge a précisé que la société devait supporter, à hauteur de 30%, son propre dommage, engendré par les lacunes dans la gestion des identifiants d'accès aux bases de données. Le juge a donc instauré l'obligation, pour l'employeur, de mettre en place des mesures de protection informatique efficaces, afin de prévenir l'installation de tout logiciel espion.

Enfin, la plupart des logiciels utilisés à ces fins proviennent de téléchargements, susceptibles de contenir des virus. Les réseaux internes des entreprises sont



régulièrement infectés par ce biais, ce qui facilite les intrusions informatiques et, partant, l'accès, l'utilisation, l'extraction, voire la destruction de données stratégiques pour l'entreprise.

Préconisations de la DGSI :

La DGSI recommande à toute entreprise :

- En priorité, d'établir une charte de sécurité informatique qui permettra de sensibiliser les salariés aux enjeux numériques, tout en les responsabilisant.
- D'organiser régulièrement des conférences de sensibilisation à destination de l'ensemble des collaborateurs, qui insisteront sur leurs droits et obligations à l'ère du tout-numérique et dispenseront des mises à jour sur les évolutions technologiques en cours.
- De mettre en place des mesures de protection efficaces afin de prévenir l'utilisation potentielle de logiciels et matériels espions. L'existence de tels dispositifs de sécurité informatique permettra à l'employeur de dégager sa responsabilité juridique et d'optimiser le bon fonctionnement de son entreprise en augmentant le niveau de protection.