Flash N° 3 – 5 novembre 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

De l'importance de définir et protéger l'information stratégique.

Suite à la démission de l'un de ses employés, le dirigeant d'une PME innovante a découvert qu'il avait subtilisé de très nombreuses informations stratégiques depuis de nombreuses années. Employé depuis plus de vingt ans au sein de l'entreprise, le technicien mis en cause travaillait sur la plupart des produits développés et bénéficiait de la confiance de ses dirigeants.

Incités à poursuivre leur travail à domicile, les personnels étaient autorisés par la direction de l'entreprise à copier les informations sur leurs propres supports amovibles. L'employé démissionnaire avait donc pris l'habitude de cette pratique au point d'en oublier de sauvegarder également les informations sur le réseau de l'entreprise.

Fort de compétences en informatique, il intervenait également pour réparer les petites pannes du réseau de l'entreprise. A ce titre, il en détenait un accès administrateur alors que son activité professionnelle ne le justifiait pas. Cet accès lui a permis de copier sur un disque dur personnel d'autres informations relatives à l'entreprise depuis 1995, sans que ses collaborateurs ne s'en aperçoivent.

A la suite d'une plainte déposée auprès des autorités territorialement compétentes, la société a pu récupérer l'ensemble des données subtilisées.

Commentaire :

Connaissant de nombreux succès à l'export et travaillant pour de grands groupes industriels et des organismes de recherche de pointe, cette société française aurait pu connaître un préjudice important en raison de la sensibilité de ses clients, du caractère stratégique des documents dérobés, et de leur absence d'archivage.

Elle illustre la vulnérabilité des entreprises qui se sont progressivement développées dans un contexte familial, puis en totale confiance avec leurs collaborateurs et n'ont pas suffisamment pris en compte la gestion de leur documentation et la sécurité de celle-ci.

La confiance n'excluant pas le contrôle, il convient de définir rigoureusement les conditions d'application d'une politique de sécurité de l'information au sein de l'entreprise.

La DCRI préconise quelques mesures permettant de clarifier les responsabilités de chacun.

► Contractualisation sur les droits et obligations des personnels à accéder, détenir et utiliser les données de l'entreprise.

► Rédaction d'une charte informatique : La déconvenue subie par cette PME trouve également racine dans l'absence d'une gestion rigoureuse du réseau informatique. La société ne disposait en effet pas de charte informatique détaillant les règles, les obligations des utilisateurs, et les sanctions en cas de manquement. Il convient de rappeler que l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) fournit des préconisations sur son site web[1] relatives à la sécurité informatique dont les entreprises peuvent utilement s'inspirer pour la rédaction de leur charte informatique.

► Le cloisonnement de l'information doit être une règle de base, même dans les PME, dès lors qu'elles opèrent sur un secteur aussi stratégique que celui relatif à notre exemple. Ce principe est d'ailleurs partagé par les chefs d'entreprise de tout secteur, pour limiter les accès aux informations financières ou à la stratégie commerciale de l'entreprise.

► L'utilisation de support amovible connecté au réseau de l'entreprise doit être formalisé par un code de bonne pratique rigoureux tant elle ouvre des portes à toutes les vulnérabilités. Il conviendra de préférer l'utilisation de moyens informatiques (clefs USB, ordinateurs portables) propriété de l'entreprise afin de s'assurer de la bonne concordance des règles de sécurité, à l'intérieur comme à l'extérieur de l'entreprise.

► Vérifiez la politique de sauvegarde de l'information. Dans le cas présent, aucune copie n'avait été réalisée pendant des années. Faute de récupération des données lors de la procédure pénale, l'entreprise aurait été contrainte d'obtenir de ses clients des copies de sa production afin de procéder à des opérations de rétro ingénierie. A la perte de temps se serait ajouté un impact très négatif en termes d'image.

► L'affaire est toujours en cours. Elle pose la question de la protection de l'information au sein des entreprises, et de la qualification des faits commis par l'employé indélicat.

[1] www.ssi.gouv.fr

Que faire en cas d'incident ?

► Dans le cas présent, l'entreprise victime a eu le bon réflexe. Après avoir sollicité la restitution des informations, elle a rapidement déposé plainte en l'absence de réponse de son ancien collaborateur.

► Exiger la restitution des moyens mis à disposition de l'ex-salarié.
Si le support amovible n'est pas la propriété de l'entreprise, celle-ci ne peut en exiger la restitution. Il n'en est pas de même pour les moyens mis à disposition du salarié (voiture, ordinateur, téléphone, etc.) qui doivent être rendus au moment de la rupture de contrat. Dans le cas contraire, l'ex-salarié s'expose à des poursuites pour abus de confiance, après mise en demeure.

► Vérifier les informations auxquelles le salarié a accédé avant sa décision de quitter l'entreprise, afin de s'assurer de la conformité des accès avec sa mission et de se prémunir d'une soustraction d'informations stratégiques.