LA LETTRE D'INFORMATION

N°13 *Direction de la Sécurité Économique en Zone Paris*

EDITO

Cette 13e lettre d'information, qui inaugure l'année, est l'occasion pour moi de nous souhaiter une coopération aussi franche et efficace en 2017, que celle que nous connûmes par le passé. L'objectif que nous nous sommes fixé, en toute humilité, est de continuer à alimenter votre réflexion et perception des aspects les plus critiques de la sécurité économique au travers de ce support de communication

Ainsi, la présente édition met l'accent sur les données et les vulnérabilités induites .

En effet, lors de nos interventions à votre profit nous faisons régulièrement le constat que la protection physique est globalement comprise et traitée. Pour autant, et dans des structures de toutes tailles, l'identification, la qualification et finalement la gestion des données est encore trop souvent aléatoire. Permettez moi de souligner que dans ce domaine, qui relève aussi du périmètre des missions du Service, les équipes de la DSEZP sont vos interlocuteurs privilégiés.

Enfin, et toujours dans l'optique de renforcer notre coopération, j'ai le plaisir de vous inviter à la prochaine journée de formation complémentaire des OS qui se déroulera le 31 mai (cf page 4). Car je suis persuadé, comme le souligne M. Alain Juillet notre grand témoin, que les entreprises et les institutions doivent coopérer et se former pour anticiper les menaces.

Le directeur de la DSEZP

INTELLIGENCE ECONOMIQUE

La loi Sapin II : une avancée à suivre

Nombreuses sont les sociétés françaises soumises à des poursuites judiciaires aux Etats-Unis, notamment à travers des procédures négociées (*Deferred Prosecution Agreement*). Le droit américain est utilisé comme moyen d'affaiblir et éliminer les concurrents des entreprises américaines. En 2014, BNP Paribas est condamnée à payer 8.4 milliards d'euros et Alstom, à 730 millions d'euros alors que les entreprises américaines ont des amendes beaucoup moins importantes. D'après leur système judiciaire, plus les entreprises 'avouent' leur faute, moins les sanctions financières seront lourdes.

Une évolution à suivre est l'application par les juridictions françaises de la loi Sapin II, relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, promulguée le 9 décembre 2016.

La loi Sapin II introduit, calquée sur le modèle américain, le principe de l'extraterritorialité du droit français et les procédures négociées permettraient l'application du principe de *non bis in idem* (nul ne peut être poursuivi ni condamné deux fois pour les même faits).

Suivre le nouveau programme de compliance français ou entrer dans des procédures négociées françaises, établi par la loi Sapin II, associé à une 'dénonciation volontaire', pourrait permettre aux entreprises de se voir condamner par les juridictions françaises, et ainsi, potentiellement, échapper aux sanctions américaines.

Colloque CDSE

La DSEZP a assisté au **colloque annuel** du **Club des Directeurs de Sécurité et de Sûreté des Entreprise (CDSE)** le 16 décembre dernier (Paris, OCDE). Le thème abordé cette année fut **l'entreprise face au phénomène de radicalisation**. Les différentes tables rondes, ont permis de mettre en exergue les points communs au phénomène et qui méritent d'être soulignés.

- un fil rouge relie toutes ces menaces ; l'entreprise se trouve mise en difficultés face au phénomène de radicalisation, et par conséquent celui ci doit être considéré dans sa globalité (religieux, éco terrorisme, UG et UD, syndicats) ;
- face au phénomène de radicalisation, le droit du travail semble inadapté, le management souvent dépassé et la cohésion de l'entreprise affaiblie ;
- la prise en compte implique pour le management de connaitre, donc d'analyser les risques et de les intégrer dans le travail ;
- surtout, le besoin fondamental identifié par plusieurs intervenants est que devant le risque majeur qu'incarne la radicalisation, la coopération entre tous les acteurs (Etat et entreprise) est vitale.

Le président du CDSE, M. Alain JUILLET, a ouvert et clôturé ce colloque et insisté pour sa part sur le besoin d'anticipation, qui passe par la formation des cadres et un besoin de coopération accru entre l'ensemble des acteurs.

ENTRETIEN

Avec M. Alain JUILLET, président du CDSE

DSEZP : Monsieur, pouvez vous faire un point de situation de l'IE en France ? Quelle évolution voyez vous ?

M. JUILLET : En dépit d'une évolution positive, l'IE est dans une position très contrastée. Si on regarde le niveau européen, nous sommes, avec la Grande Bretagne et la Suède, les pays les plus avancés. Si on se compare avec le reste du monde, nous sommes en retard sur les Etats-Unis ou la Chine au niveau des moyens techniques utilisés et de la mobilisation de l'Etat. Si nous regardons le marché intérieur, l'IE a bien pénétré la plupart des grandes entreprises mais reste insuffisamment pratiquée par les ETI et les PME. Enfin, si l'on s'intéresse à l'Etat, on voit que sa prise en compte est très variable selon les administrations : le ministère de l'Intérieur est en pointe, la Défense sait l'utiliser, le Quai d'Orsay commence à se mobiliser et l'Economie fait trop cavalier seul. Quant aux services de renseignements ils sont essentiellement mobilisés sur l'anti-terrorisme.

DSEZP : Quel est l'impact réel de l'IE sur le tissu industriel ? Quel apport et quel usage les entreprises ont-elles dans ce domaine ?

M. JUILLET : La recherche de compétitivité technique industrielle ou commerciale mettant tout le monde au même niveau, c'est par la capacité d'acquisition et de traitement de l'information qu'on peut se différencier. Celui qui sait peut anticiper, préparer des attaques ou des actions défensives au moindre coût tout en étant très efficace. Etre capable d'identifier les bons marchés, les produits adaptés et les bonnes approches stratégiques, vous rend plus performant avec des économies de gestion évaluées entre 2 et 3%. Malheureusement, une partie des grands groupes économise sur cette activité quand les résultats financiers sont insuffisants alors que ce devrait être le contraire.

DSEZP : Vous avez, lors du colloque du CDSE, évoqué la nécessaire coopération entre les organismes de l'Etat et les sociétés, quelle forme concrète peut prendre cette coopération ?

M. JUILLET : Dans la compétition mondiale les meilleures places vont aux plus rapides et aux plus forts. En dehors de quelques très grands groupes, personne n'a les moyens techniques et humains suffisants pour surveiller l'environnement, son évolution, le marché, les concurrents, les législations ou les normes. Atteindre le niveau requis exige une coopération étroite entre tous les acteurs pour chasser en meute. Les Allemands, les Américains ou les Chinois savent très bien le faire. Les Français sont encore pénalisés par ces relents de colbertisme qui opposent l'Etat et l'entreprise alors qu'aujourd'hui aucun ne peut vivre sans l'autre. Nous fonctionnons en silos verticaux alors qu'il faudrait agir en transversal et faire circuler l'information. C'est dommage car si nous cumulons les informations détenues par les uns et les autres nous sommes particulièrement bien informés.

DSEZP : Si l'on prend les exemples à l'étranger, notamment les *advocacy board* américains, voyez-vous des pistes pour des équivalents français ?

M. JUILLET : Hélas non et c'est très regrettable. La capacité américaine ou britannique de mobiliser tous les services de l'Etat pour contribuer à la réussite d'un contrat lui donne un formidable avantage concurrentiel et diminue sensiblement le risque d'échec. Il faut pour cela que chacun considère l'autre comme un associé aussi intelligent et capable que lui, et que l'échange soit ouvert et sans restriction avec mise en œuvre de tous les moyens disponibles et nécessaires. Il y a eu des tentatives mais elles ont échoué par notre difficulté à faire du multidisciplinaire, à échanger et à travailler ensemble

DSEZP : Merci, Monsieur, pour ces réponses et la mise en perspective que vous offrez à nos lecteurs.

Infos utiles:

CDSE:
Club des Directeurs de Sécurité et de sûreté des Entreprises

CDSE 6, place d'estienne d'Orves 75009 PARIS
01 72 317 318

www.cdse.fr

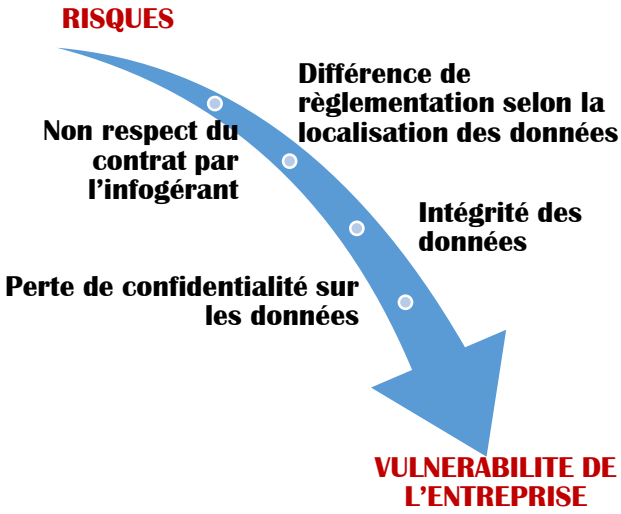
CYBER

INFOGERANCE

Externalisation des systèmes d'information

De nombreuses entreprises externalisent tout ou partie de leur système d'information afin de réduire des coûts de possession (TCO) et d'exploitation qu'elles savent ainsi parfaitement mesurer. Mais sont-elles en mesure d'évaluer les pertes financières occasionnées par la perte de contrats en raison de fuites d'informations financières ou commerciales ? Par une concurrence déloyale liée au vol de leur savoir-faire ? Par le débauchage de collaborateurs précieux dû à des fuites d'information sur leurs ressources humaines ?

Une analyse doit être menée afin d'élaborer des mesures visant à abaisser ou supprimer les risques pesant sur le patrimoine immatériel de la société. Pour vous aider, l'ANSSI a publié sur son site Internet (*www.ssi.gouv.fr/bonnes-pratique/externalisation*) un document intitulé « maîtriser les risques de l'infogérance ».



Dans le cadre de votre entreprise, comment vous prémunir?

- **Exiger que les serveurs hébergeant les données soient localisés en France (application de la réglementation nationale)**
- **S'assurer de la réversibilité des données (possibilités de les recouvrer ou de les confier à un autre infogérant)**
- **S'assurer de la confidentialité des données en les chiffrant**
- **S'assurer du respect des clauses de sécurité du contrat d'infogérance par le prestataire et ses éventuels cotraitants et sous-traitants.**
- **Appliquer des règles de filtrage sur les flux d'infogérance**

Pour toute question supplémentaire veuillez contacter :
dpsd-dsezp-ssi.cds.fct@intradef.gouv.fr

PROTECTION

Les partenariats recherche

Les entreprises françaises, notamment de la sphère défense, mettent régulièrement en place des partenariats avec des laboratoires de recherche, soit nationaux soit internationaux. Ces opportunités sont aussi sources de vulnérabilités. En effet, la publication de travaux de recherche liés directement à des entreprises de la sphère défense peut amener à une dispersion des informations les plus sensibles de l'entreprise. Dans ce cas la création de ZRR, à la fois dans le laboratoire mais aussi au sein de la société, présente une solution intéressante, voire indispensable pour minimiser le risque de perte de l'information.
Références II 11155 (CD SF) et IM 298

Les objets connectés, quelles menaces?

Les objets connectés (OC) et l'internet des objets (IOT) connaissent un développement exponentiel (50 milliards d'OC en 2022, 15% de tous les objets seront connectés en 2020) offrant autant de portes d'entrée et de possibilités pour les attaques informatiques.
En effet, les OC ne sont que très peu protégés nativement et de plus en plus présents sur des infrastructures critiques ou sensibles (SCADA, réseaux industriels).

Les vulnérabilités de ces OC sont principalement la captation de données avec exportation vers les serveurs des fabricants et l'utilisation des OC, intégrés à des réseaux de machines fantômes (*botnet*), comme supports pour lancer des attaques informatiques (déni de service). Exemple du virus MIRAI qui infecte des dizaines de millions d'OC ensuite utilisés pour une attaque en déni de service (DDoS) de serveurs DNS.
Les mesures possibles/envisageables : analyser les flux, rétrofiter les OC et développer la sécurité *by design*.

Journée de formation complémentaire des OS du 1er semestre 2017

Après un premier galop d'essai en novembre 2016, qui, d'après les avis unanimes des premiers participants, a atteint ses objectifs, la DSEZP vous invite à vous inscrire pour la prochaine journée qui aura lieu le **31 mai 2017**.
L'objectif, en complément du stage CISIA 502, est de donner aux OS des informations pratiques et pragmatiques aux questions les plus fréquentes (ATAP ATAI, gestion des ISC, habilitations SOPHIA, etc.)
Les demandes de participation sont à adresser à la DSEZP via vos ISD référents.

Guide du fait religieux

Evoqué sous forme de projet dans la dernière lettre d'information (N°12), le guide du fait religieux dans l'entreprise publié par le ministère du travail est maintenant réalité. Il est disponible (employeurs) sous le lien suivant:
http://travail-emploi.gouv.fr/IMG/pdf/guide_employeurs_valide.pdf

Le conseil SOPHIA

La notice individuelle 94A est contractuelle. A ce titre, le candidat atteste et reconnaît être informé :

- de la définition de l'habilitation à laquelle il est candidat et de sa portée ;
- du caractère obligatoire des réponses qui lui sont demandées ;
- qu'il certifie l'exactitude des renseignements qu'il fournit et admet être informé qu'il s'expose, en cas d'altération frauduleuse de la vérité, à des sanctions prévues au code pénal.

Ainsi le CNHD relève un certain nombre d'erreurs récurrentes :

- mauvaise indication des dates (année d'arrivée en France, année d'acquisition de la nationalité française, date de naissance du conjoint absente …) ;
- nom de jeune fille suivi du nom d'épouse (intéressée, conjointe, mère et belle-mère) ;
- dernière page / cartouche 2 : bien renseigner les nom, prénom, date et lieu de naissance ;
- la photo est obligatoire (50 Ko max, de face, format pièce d'identité et non pas une photo de vacances !).

Une demande conforme est un préalable à un traitement dans les délais.