CGI | Business Consulting

Lettre d'information

Cybersécurité et Cybercriminalité

Numéro 15 – Mars / Avril / Mai 2015

CyberÉdito

Un effort de conformité ou une certification sécurité ?

Ces dernières semaines ont été riches en production de référentiels de sécurité. En particulier, un référentiel pour la gouvernance des informations à caractère personnel, publié par la CNIL, une nouvelle instruction interministérielle pour la protection des systèmes d'information sensibles par le SGDSN et un nouveau référentiel de l'ANSSI pour les services Cloud. Chacun de ces référentiels est associé à un label ou une qualification. Lorsque la règlementation ne l'impose pas, faut-il engager une démarche de certification ou rester dans une simple recherche de conformité ?

Certains diront : « La certification est chère ! ». Il faut se rendre à l'évidence : ce qui revient cher, ce sont surtout les efforts à faire pour respecter le référentiel et donc être conforme. D'autres diront : « La certification sécurité ne veut pas dire être sécurisé ». C'est vrai ! Mais c'est un premier pas vers plus de maturité. Les derniers avanceront que la certification peut également présenter des risques, notamment celui de perte du label. En théorie, cela peut paraitre gênant pour l'image de marque de l'entreprise mais l'histoire montre qu'aucune n'en a souffert, sauf une exception.

À l'inverse, force est de constater que les entreprises tirent, toutes, un réel avantage à « l'épreuve » de certification. Elles trouvent, tout d'abord, une obligation d'arriver à la cible à échéance. Elles remettent en question certaines mauvaises habitudes et profitent des efforts de formalisation jugés souvent non prioritaires et pourtant indispensables en SSI. Enfin, les équipes qui contribuent à ces travaux ont une réelle légitimité et sont motivées par la satisfaction d'obtenir un label et le RSSI obtient une visibilité plus importante auprès du comité exécutif de l'entreprise. Cerise sur le gâteau, l'organisme peut en faire la promotion pour améliorer la confiance de ses clients ou partenaires.

Notre constat est clair parmi nos clients ayant engagé des démarches depuis trois ans. La maturité en matière de sécurité des entreprises engagées dans une démarche de certification est bien supérieure à celles qui se sont limitées à une simple conformité.

Jean Olive — Manager CGI Business Consulting

Parole d'un CyberExpert

L'évolution des environnements IT (*Big Data*, *IoT*, *Cloud*, etc.) soulève de plus en plus d'inquiétudes. C'est un sondage réalisé par Symantec qui le révèle : près d'un français sur deux est inquiet du respect de sa vie privée. Au regard des enjeux et de la réforme du régime européen de protection des données à caractère personnel (DCP) qui se fait attendre, faut-il rester sans rien faire ?

La CNIL amène des éléments de réponse en publiant un guide qui s'affiche clairement comme la première étape de la mise en conformité au règlement européen. Elle propose aux organismes de labéliser « gouvernance Informatique et Libertés » leurs processus traitants de données personnelles. Markéting ou nouveau standard ?

Constitué de 25 mesures organisationnelles et techniques, ce référentiel renforce le positionnement stratégique du CIL : celui-ci doit être rattaché à un membre de la direction de l'organisme. Outre les actions de sensibilisation, d'audit et de contrôle régulier, il est également demandé au CIL de cartographier et de maintenir à jour tous les processus traitants des DCP et de réaliser une analyse de risques liés à la sécurité de ces données. En plus de définir et déployer des mesures adaptées aux risques identifiés, il est également demandé à l'organisme de mettre en place des moyens techniques concernant la bonne gestion des réclamations et incidents : enregistrement des traces d'évènements de sécurité sur une durée de 6 mois et notification dans un délai inférieur à 72h de toutes les personnes impactées en cas d'accès non autorisé par un tiers.

Avant de subir les obligations et éventuelles sanctions prévues par le règlement européen, les organismes n'ont plus le choix. La démarche de mise en conformité doit être initiée. Et ce label constitue clairement une aide précieuse, car le travail effectué bénéficiera aux organismes qui seront alors en mesure de rassurer leurs usagers et partenaires en prouvant leur conformité en matière de traitement des DCP.

Emmanuel Petit – Manager CGI Business Consulting

CyberMenaces

2014 : l'année des failles ? 2015 : on continue !

Le CLUSIF a publié son traditionnel panorama des menaces de l'année 2014. Bien qu'il n'y pas de réelles nouveautés, les constats sont clairs. La sécurité des objets connectés est défaillante, le cybervandalisme se développe et les failles trouvées dans des bibliothèques libres ont de plus en plus d'impact.

Lire

Êtes-vous sûr de ne pas être une cible pour les cyberattaques ?

Beaucoup de dirigeants ne se sentent pas assez concernés par la sécurité de l'information, car ils ne pensent pas être des cibles dignes d'intérêt auprès des pirates. Il y a fort à parier que cela pouvait être le cas d'entreprises comme Target ou Sony Pictures qui ont perdu respectivement leur n°1 et n°2 suite à une attaque informatique.

Lire

Les tendances des malwares

Les malwares restent aujourd'hui une menace majeure à laquelle une entreprise doit savoir faire face. La meilleure protection ? Bien connaitre les tendances des malwares qui pointent à l'horizon !

Lire

Après Cryptolocker, voici Cryptowall 2.0 !

Cryptowall 2.0 chiffre les données stockées sur un ordinateur et force l'utilisateur à payer pour les récupérer déchiffrées. La nouveauté : ce *ransomware* utilise le réseau Tor pour communiquer avec les pirates et désactive les mécanismes de protection de Windows.

Lire

Gemalto : cible de choix pour la NSA

Une des principales raisons de l'interception des données de Gemalto par la NSA est le manque de protection des canaux d'échange d'information entre l'entreprise et ses partenaires. Et vous, échangez-vous encore en FTP avec l'externe ?

Lire

Lettre d'information
Cybersécurité et Cybercriminalité
Numéro 15 – Mars / Avril / Mai 2015

Réponses aux CyberMenaces

Le PIA, vous savez ce que c'est ?

La *Privacy Impact Analysis*, ou encore EIVP pour étude d'impact vie privée, est un type d'analyse de risques demandée par le règlement européen. Ce livre blanc présente de manière complète et détaillée tout ce que vous devez savoir. Comment définir le périmètre ? Comment mener l'étude ? Études de cas. Tout y est !
Lire

Si vous les comprenez, vous pouvez les convaincre !

Comment comprendre le fonctionnement du cerveau face aux investissements en matière de sécurité ? Une réponse vient de la théorie des perspectives : face à des pertes, la solution préférée est celle qui est la plus risquée et la moins couteuse !
Lire

Des certifications SSI pour les professionnels des SCADA ?

L'ENISA publie un rapport dans lequel elle pose le cadre de ce que devrait être le schéma de mise en place de certification pour les professionnels des SCADA.
Lire

Uhuru : l'antivirus souverain…

L'antimalware d'Uhuru a enfin vu le jour. Une version open source devrait être disponible courant premier semestre. Mais la France se donne-t-elle réellement les moyens de rivaliser avec les Kaspersky et autres Symantec ?
Lire

… et le smartphone sécurisé !

Uhuru, c'est aussi le nom du smartphone sécurisé made in France ! Ce mobile contient l'antivirus Uhuru-AM et chiffre intégralement son contenu.
Lire

Sécuriser les tâches d'administration et déployer Firefox

L'ANSSI publie un nouveau guide afin de sécuriser les pratiques d'administration. Au programme : cloisonnement des environnements d'administration, charte informatique et hygiène des postes de travail.
Lire
L'agence a publié un nouveau guide concernant le déploiement sécurisé de Firefox.
Lire

CyberBrèves

TF1 sous les projecteurs pour le piratage d'un de ses sous-traitants

Des pirates ont volé des données à caractère personnel de 1,9 million de personnes sur le site de TF1. Cette information a largement été reprise dans les journaux alors que l'espace « abonnement presse » qui a été visé était géré par un sous-traitant.
Lire

La stratégie de cybersécurité de la Gendarmerie nationale

À l'occasion du FIC 2015, la gendarmerie nationale a publié sa revue sur le thème de la stratégie pour la cybersécurité. Au programme, cyberdéfense, objets connectés et droit à l'oubli.
Lire

CGI Business Consulting fait partie du groupe CGI inc, 5e plus importante entreprise indépendante de services en technologie de l'information et en gestion des processus d'affaire au monde.

CGI Business Consulting dispose notamment d'une équipe d'experts spécialisée dans le conseil aux entreprises et aux organismes publics pour les assister à lutter efficacement et globalement contre toutes les formes de cybercriminalité.

CyberRèglementation

La PSSI-E renforcée

L'ANSSI vient de publier une instruction interministérielle relative à la protection des systèmes d'information sensibles qui précise (enfin) les mesures à mettre en place sur les systèmes d'information traitant d'informations portant la mention « Diffusion Restreinte ».
Lire

Vol de données : l'abus de confiance peut être caractérisé

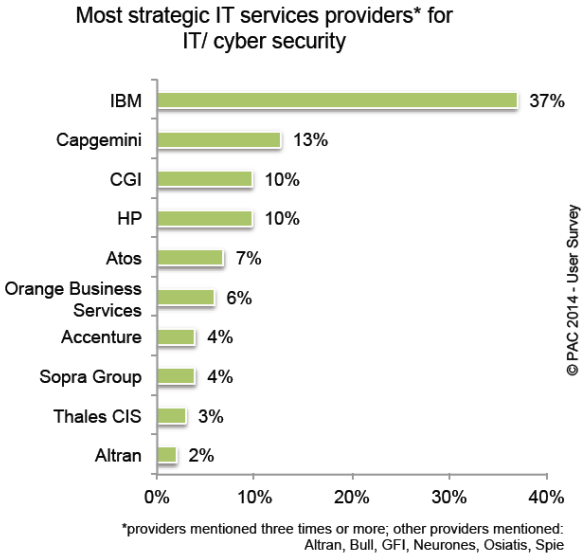
Beaucoup de questions ont été posées autour du vol de données. Est-ce un vol alors que le propriétaire peut toujours en faire usage ? En tout cas, la Cour de cassation vient de valider l'utilisation du délit d'abus de confiance dans le cadre d'utilisation de données volées par un employé démissionnaire.
Lire

Première condamnation pour usurpation d'identité numérique

Est-ce qu'un piratage informatique peut donner lieu à une usurpation d'identité ? Pour le TGI de Paris, il n'y a aucun doute : une utilisation frauduleuse d'un site internet qui atteint à l'image d'une personne peut constituer le délit d'usurpation d'identité numérique.
Lire

Chez CGI Business Consulting

CGI, numéro 3 des acteurs stratégiques en cybersécurité



D'après l'étude *PAC 2014 - IT Supplier Evaluation Market - Insight France*, « la sécurité des systèmes d'information est jugée stratégique par les DSI qui doivent s'entourer de prestataires de confiance. CGI s'est hissé dans le top 3 de ces acteurs stratégiques en ayant développé une offre dédiée et en se basant sur les *best practices* pour la France, issues des projets internationaux où la SSI est essentielle ». Cette étude a été réalisée auprès de 181 CxO d'entreprises de plus de 1000 employés en France.

Pour de l'information en temps réel, @CGIsecurite est sur Twitter

Directeur de la rédaction Jean Olive
Comité de rédaction Rémi Kouby, Jean Olive, Miriam Paiola, Emmanuel Petit
Contact jean.olive@cgi.com