CGI | Business Consulting

Lettre d'information

Lutte contre la cybercriminalité

N°7 – avril – mai 2013

Édito

Le 28 février 2013, le gouvernement a présenté sa feuille de route dans le domaine du numérique (cf. cet article). Un exemple – s'il en fallait encore un – qu'il ne s'agit plus pour les entreprises de renforcer leurs systèmes, mais d'avoir mené en amont une analyse de risques qui garantie la protection de la vie privée. Ne soyons pas naïfs, c'est un mouvement de fond ! Désormais, ni la conformité à l'ISO 27002, ni la sacrosainte politique de sécurité des systèmes d'information ne sauraient protéger les dirigeants d'une éventuelle mise en cause pour négligence en cas de divulgation des données. Le *best effort* d'hier (tendre vers une conformité) suffisait peut-être, mais sous la pression de l'opinion, la tolérance zéro (maitrise des risques) est de rigueur. J'en veux pour preuve les nouvelles initiatives législatives et sectorielles ayant en commun la réalisation préalable d'analyses des risques : le RGS qui s'applique aux autorités administratives, le standard PCI-DSS qui s'impose dès qu'il s'agit des données de porteurs de cartes de paiement, ou encore le nouveau règlement européen sur la protection des données à caractère personnel, qui s'imposera à toute entreprise publique comme privée.

Le ton a été donné. Il n'est plus question seulement de vous imposer des moyens à mettre en place, mais bien d'exiger une maitrise des risques. Alors, face à cette nouvelle donne, comment un dirigeant (ou son RSSI) peut-il assumer sa responsabilité ? Le marché répond par une avalanche de catalogues (les 40 règles d'hygiènes de l'ANSSI, le guide de bonnes pratiques de la CNIL, le décret des hébergeurs de santé, etc.). Plus ou moins cohérents, ils sont voués à l'obsolescence compte tenu de la rapidité des évolutions technologiques et des menaces. EBIOS et Mehari peuvent aider à y voir plus clair visant une approche par les risques. Ces deux guides représentent des initiatives louables, mais ils leur manquent l'essentiel : la compétence et l'expérience.

Alors que faire ? Vous faire assister d'un professionnel de la gestion du risque me parait incontournable. Lui seul aura la légitimité et la vision globale. En interne, les *risk managers* ou les qualiticiens peuvent être de bons candidats. L'objectif est d'animer une démarche de gestion des risques dans une perspective d'ensemble, puis d'opérer un délicat arbitrage quant aux priorités, à l'utilisation des ressources de l'entreprise et aux conséquences potentielles de ne pas renforcer votre système.

Jean Olive
Senior Manager CGI Business Consulting

Parole d'expert

Le RSSI, en route vers la fonction de Risk Manager du SI

Les entreprises sont chaque jour un peu plus dépendantes de leur système d'information et de leur patrimoine informationnel. Elles se doivent de maitriser globalement les risques de la fonction SI.

Pour ce faire, le Risk manager (s'il existe), se tourne vers le DSI ou d'autres fonctions de la DSI afin obtenir une vision complète. Mais il est bien souvent mal à l'aise dans ce domaine d'experts SI.

Le RSSI, quant à lui, est le gestionnaire du risque lié à la sécurité du système d'information. Il est le gestionnaire du risque en amont des besoins de confidentialité, traçabilité, intégrité & disponibilité pesant sur le SI. Il ne couvre donc pas toute la problématique.

Le risque du métier de la DSI va au-delà de la sécurité de l'information. Il s'agit des risques opérationnels relatifs à tous les processus de la DSI : gouvernance, projet, production, processus supports… ou de risques plus stratégiques liés aux grandes orientations de la DSI : urbanisation, sourcing, alignement avec les besoins métiers, innovation, etc.

Aujourd'hui les normes (ISO 20000, COBIT, etc.) et les outils de GRC dédiés au risque SI permettent une prise en compte globale, cohérente et plus optimale de l'ensemble des risques SI. Le RSSI ne peut plus « traiter de ses risques dans sa tour d'ivoire » !

Cette mise en commun au sein de la DSI est une étape importante dans la marche vers une gestion des risques globale et partagée au sein de l'entreprise. Elle représente même une opportunité pour agrandir le terrain de jeu d'un RSSI devenu un véritable Risk Manager du SI.

Hervé Ysnel
Senior Manager CGI Business Consulting

Menaces

Bit9 livre les détails de son intrusion

La société de sécurité Bit9 a subi une intrusion et fait preuve de transparence. Elle livre dans cet article le détail de l'enchainement des évènements ainsi que l'ensemble des éléments techniques qui ont permis aux pirates de s'introduire dans le SI.
Lire

Un référentiel d'indicateurs sur des *malwares* et des APTs

La société Mandiant, au travers d'une enquête méticuleuse sur le fonctionnement d'un groupe de pirates basé en Chine, livre dans l'annexe du rapport un référentiel de plus de 3000 indicateurs de compromission, de contrôle et des détails sur les *malwares* utilisés.
Lire

Des informations médicales trouvées sur Internet. Encore !

Après le scandale de Marseille, c'est un hôpital d'Ile-de-France qui se trouve impliqué dans une affaire de divulgation d'informations médicales. Le scénario est toujours le même : des négligences.
Lire

Les salariés emportent souvent des données confidentielles

C'est une réalité, les salariés qui quittent l'entreprise partent souvent avec des données confidentielles. Même s'ils n'ont pas (toujours) la volonté de nuire.
Lire

Cyber-attaque : un bon moyen pour diffuser un message

On voit souvent une cyberattaque comme une nuisance ciblée sur une entreprise ou une organisation. Mais les moyens de diffusion d'informations peuvent tout autant attirer les groupes de pirates.
Lire

Les risques du télétravail

Des réflexions refont surface dans un contexte où certains français ont été forcés de télé-travailler ce mois-ci, en raison des chutes de neige. Au programme : VPN, chiffrement et BYOD. Lire

Lettre d'information
Lutte contre la cybercriminalité
N°7 – avril – mai 2013

Réponses aux menaces

Le gouvernement Obama et le service du Premier ministre français s'attaquent à la cybersécurité

Aux États-Unis, après avoir officialisé son équipe de cyberoffensive (Lire) et déclaré que les cyberattaques deviendront à court terme la première menace devant le terrorisme (Lire), l'administration tient des réunions avec les patrons d'entreprises sur la cybersécurité. (Lire). En France, le sujet inquiète tout autant : Lire

Security as a service, la solution contre la cybercriminalité ?

Alors que de nombreuses entreprises font déjà appel à des SOC externalisés pour leur gestion de la sécurité des infrastructures, de nouvelles offres « *as a service* » telles que l'IAM ou le DLP font surface. La fonction SSI de l'entreprise va-t-elle devenir un simple *broker* de prestations externalisées ?
Lire

L'assurance : la solution face à vos risques résiduels

Beazley, en partenariat avec CGI, propose des polices d'assurance contre la perte ou la divulgation de données personnelles. Ces assurances proposent ainsi un accès privilégié aux services de consultants informatiques expérimentés.
Lire

L'AMRAE publie à nouveau son panorama des logiciels de gestion des risques

C'est la cinquième édition de ce panorama qui est publiée cette année. On peut noter que les solutions standardisées arrivent à maturation et que des solutions plus spécialisées commencent à émerger.
Lire

La PSSI « ISO 27002 » n'est plus suffisante

Cet article relate le témoignage d'un RSSI qui devrait parler à tous ses pairs. La PSSI ISO 27002 ne peut plus suffire à assurer la sécurité, au sens large, de votre système d'information. Les analyses de risques et les contrôles sont indispensables.
Lire

Brèves

Quand les actionnaires demandent des comptes aux RSSI

Vous vous inquiétez pour la sécurité de vos données ? Vos futurs actionnaires également. Cette étude montre notamment que la plupart des investisseurs sont regardants sur la manière dont une entreprise réagi en cas de compromission d'information.
Lire

Une clé USB pour passer outre la protection de Windows

Cette faille a récemment été corrigée par Microsoft mais elle permettait d'accéder aux données d'un ordinateur verrouillé, par simple branchement d'une clé USB contenant un code malveillant. Combien d'autres failles du genre reste-t-il à corriger ?
Lire

CGI Business Consulting fait partie du groupe CGI inc, 4e plus importante entreprise indépendante de services en technologie de l'information et en gestion des processus d'affaire au monde.

Cabinet de conseil en transformation et innovation, CGI Business Consulting est le partenaire privilégié de la croissance profitable et durable de l'entreprise.
Chaque jour, nos 3500 consultants mobilisent leur savoir-faire et leur créativité pour accompagner nos clients dans la réussite de leurs projets.

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.

Règlementation

La protection des données personnelles est décrétée priorité nationale

Au cours du séminaire gouvernemental sur le numérique, le Premier ministre a affirmé sa volonté de voir la protection des données personnelles devenir une priorité de l'action publique. Dans ce sens, la CNIL sera au premier plan pour jouer ses rôles de sensibilisation et de sanction.
Lire

Tous les incidents de sécurité seront-ils notifiés ?

Alors que les yeux sont rivés sur le futur règlement européen, un nouveau projet de directive qui propose d' « assurer un niveau élevé de sécurité des réseaux et de l'information ». Et pour atteindre cet objectif louable, des audits des éditeurs de logiciels sont prévus ainsi que l'obligation de notifier les incidents de sécurité (et pas seulement ceux qui concernent une divulgation de données à caractère personnel comme le propose le règlement européen).
Lire

210000

C'est le nombre de victimes d'usurpation d'identité en France en 2012. Un chiffre dont le taux d'augmentation est de 40% tous les ans. Lire

Chez CGI Business Consulting

Analyse des risques « données personnelles » et « entreprise »

Au cours d'une interview pour le cabinet Bensoussan, Jean Olive met en lumière les différences entre les analyses de risques d'entreprises et celles traitant de données à caractère personnel.
Lire

FedRAMP certifie CGI

Le *Federal Risk and Authorization Management Program* a certifié les services dans le *cloud* de CGI. Aujourd'hui, CGI fait partie des deux seules sociétés au monde à être certifiées *Secure Cloud Service Provider* par ce programme.
Lire

CGI animait un atelier à l'AMRAE

Hubert Chenut, consultant sénior de l'équipe cybersécurité de CGI Business Consulting a animé à l'AMRAE un atelier sur le thème « Cyber résilience : Protéger ses données et celles de ses clients ».
Lire

Prestataire d'audit de sécurité des SI : CGI va postuler

En tant qu'offreur de prestations d'audits de sécurité, CGI Business Consulting a engagé tous les travaux pour se porter candidat à la qualification des prestataires de sécurité dès l'ouverture de la procédure par l'ANSSI.
Lire

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

À ne pas manquer

Directeur de la rédaction Jean Olive
Comité de rédaction Louis Bavent, Rémi Kouby, Hervé Ysnel
Contact jean.olive@cgi.com