CGI | Business Consulting

Lettre d'information

Cybersécurité et Cybercriminalité

Numéro 9 – Octobre / Novembre 2013

Édito

Cette année, CGI est partenaire des Assises de la Sécurité et des Systèmes d'Information qui se dérouleront du 2 au 5 octobre prochain à Monaco. Cet évènement reste un incontournable pour les acteurs et utilisateurs finaux du système d'information ainsi que pour les décideurs — RSSI, DSI, DI, *risk managers*, CIL — qui souhaitent être au fait des dernières problématiques sécuritaires nationales et internationales et veulent anticiper les tendances et innovations de demain.

C'est dans ce cadre que les experts sécurité de CGI Business Consulting animeront un stand sur le thème de la cybersécurité. Notre équipe sera à votre disposition pour discuter avec vous des tendances que nous observons chez nos clients ainsi que des évolutions des normes et bonnes pratiques de la profession. Venez nombreux sur notre stand pour que nous puissions vous aider à construire les meilleures approches pour lutter efficacement contre les menaces aussi bien externes qu'internes.

À cette occasion, Jean Olive, Sénior Manager CGI Business Consulting, animera un atelier sur le thème « La politique de sécurité des SI : un référentiel de contrôle interne comme les autres ? », le 3 octobre 2013 de 17h00 à 17h45. Dans certaines organisations complexes, le pilotage et la mesure du niveau de sécurité des SI, bien qu'indispensables, sont des opérations actuellement difficiles et lourdes à mettre en œuvre. Au-delà du référentiel ISO 27002 et de l'analyse de risques préalable, un grand organisme du monde santé-social a fait le choix de transformer sa PSSI en véritable outil de contrôle interne, guidé et didactique. Celui-ci s'appuie sur une déclinaison « maison » de l'échelle de maturité CoBIT et un système de preuve explicite, garant de l'industrialisation de la démarche.

Pour en savoir plus, nous vous donnons rendez-vous dès le 2 octobre prochain à Monaco sur le stand n°8.

Parole d'expert

Après une phase de concertation et d'expérimentation de deux ans, l'ANSSI a publié en juin 2013 le référentiel d'exigences applicable aux Prestataires d'Audit de la Sécurité des Systèmes d'Information (PASSI). En attendant la publication des textes officiels (RGS V2) pour prétendre à la qualification de « Prestataire de Services de Confiance » (PSCo), LSTI est d'ores et déjà qualifiée pour délivrer des certifications à des sociétés. Elle est aujourd'hui la seule.

L'objet est de certifier une personne morale sur une partie ou toutes ses activités d'audit : 1) l'audit d'architecture, 2) l'audit de configuration, 3) l'audit de code source, 4) les tests d'intrusion et 5) l'audit organisationnel et physique.

Les exigences du référentiel portent 1) sur la société prestataire, et notamment la sécurité de son SI, 2) sur les auditeurs, leurs pratiques et leurs connaissances techniques, et enfin 3) sur la conduite des audits (cf. norme ISO 19011).

La certification sera délivrée suite à un audit sur site de la société prestataire, à l'observation d'audits de sécurité réalisés pour des clients et à la réussite d'évaluations écrites et orales des auditeurs.

Aucunement limitée à la sphère publique, cette certification « à la française » offre un outil d'aide aux donneurs d'ordre pour le choix de sociétés d'audit. Si les acteurs adhèrent, cette démarche amènerait qualité, professionnalisme et une meilleure traçabilité à un marché jusqu'alors sans contrôle. La démarche semble être à ses débuts, l'ANSSI ayant l'intention de poursuivre en ce sens notamment pour les prestations de détection d'incidents et d'investigation numérique.

Les prestations couvertes par cette certification sont au cœur de métier de la ligne de service « Cybersécurité » de CGI Business Consulting. C'est donc tout naturellement que nous avons décidé de postuler à la qualification PASSI.

Vincent Maret
Associé CGI Business Consulting

Menaces

Vous serez peut-être la prochaine victime de FRANCOPHONED !

Depuis plusieurs mois, les entreprises françaises sont la cible d'attaques d'ingénierie sociale particulièrement sophistiquées et très ciblées. Le message est d'autant plus crédible que les victimes sont contactées en parallèle, par e-mail et téléphone. Les attaquants parlent un français clair, sans accent et utilisent un ton autoritaire pour abuser leurs victimes. À la clé, des transferts de fonds vers des comptes *offshore*.
Lire

Un simple SMS peut suffire à compromettre votre ordinateur

Un expert sécurité américain a présenté au CanSecWest 2013 une faille impliquant les modems USB se connectant à un réseau GSM/DMA (clés 3G, par exemple). Les SMS seraient simplement lus et exécutés en superutilisateur. Il serait alors possible de s'introduire sur l'ordinateur en exécutant du code.
Lire

PRISM : quelles conséquences pour les entreprises européennes ?

Alors que le scandale PRISM fait à nouveau planer le spectre de l'espionnage industriel, les entreprises doivent se poser les bonnes questions sur la valeur des informations qu'elles traitent et les méthodes de stockage.
Lire

Un dysfonctionnement d'utilisation d'un logiciel à l'hôpital entraine la mort d'une patiente

Dans les hôpitaux, les prescriptions sont de plus en plus dématérialisées. Les logiciels, comme tout autre code informatique, peuvent contenir des erreurs. La SSI prévient depuis longtemps d'un risque pour le patient mais c'est la première fois, malheureusement, que l'incident est avéré. Il concrétise le lien direct entre un risque informatique et le décès d'un patient. Dans le cas d'espèce, l'allergie d'une patiente à l'amoxicilline n'apparaissait pas dans le système informatique. Espérons que cet incident rendra plus vigilants les professionnels de santé.
Lire

Lettre d'information
Cybersécurité et Cybercriminalité
Numéro 9 – Octobre / Novembre 2013

Réponses aux menaces

Les injections SQL encore, les injections SQL toujours !

L'OWASP a publié son rapport des dix risques de sécurité applicatifs web les plus critiques. Les résultats varient de moins en moins d'une année sur l'autre. Il s'agit encore et toujours de l'injection (SQL ou autres), la violation de gestion d'authentification et de session et l'exploitation de failles XSS qui forment le trio de tête.
Lire

Un guide pour réaliser un plan de continuité d'activité

Ce guide du Secrétariat Général de la Défense et de la Sécurité Nationale présente la démarche méthodologique permettant l'élaboration concrète d'un PCA. Chaque étape est accompagnée d'une fiche dédiée sur laquelle vous retrouverez un ensemble de bonnes pratiques.
Lire

Évolution des attaques DDOS : comment s'en protéger ?

Alors que différentes études ont montré que les attaques DDOS proliféraient, seule une stratégie de sécurité appropriée épargnera aux entreprises les conséquences et les couts engendrés par ces attaques. Les trois étapes principales d'une stratégie reposant sur le maintien des services sont exposées dans cet article.
Lire

Êtes-vous au courant des mauvaises nouvelles ? Et votre directeur ?

Dans près de 50% des entreprises, les informations négatives ne remontent pas aux décideurs. Et il s'agit d'une seule des multiples raisons pour lesquelles la SSI ne parle pas à la direction générale.
Lire

La sensibilisation : Pourquoi ? Pour qui ? Comment ?

Ce livret fournit des pistes de réflexion et d'action qui vous permettront de mener à bien vos projets de sensibilisation. Il décrit notamment, au travers d'exemples concrets, les principales étapes et facteurs clés de succès de la démarche.
Lire

Brèves

ISO 22301 vs BS25999-2 : les différences en un coup d'œil

Cette infographie présente une vision synthétique des principales différences entre les normes de continuité d'activité que sont l'ISO 22301 et la norme BS 25999.
Lire

Le gouvernement va enfin suivre les conseils de l'ANSSI

Stop aux smartphones ! Les membres du gouvernement sont priés de ne plus utiliser autre chose que le matériel chiffré fourni par l'État pour leurs communications sensibles.
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

Les évolutions de PCI DSS 2014

PCI DSS 2014 devrait être prête vers novembre 2013. Les principaux changements à venir sont une plus grande implication et responsabilité demandée aux fournisseurs de services (*cloud computing* notamment), le renforcement des tests d'intrusion et plus de flexibilité accordée aux types de mots de passe dans le but de renforcer la protection globale. Enfin, il sera demandé des diagrammes de flux de données plus précis, une évaluation des menaces liées aux codes malveillants ainsi que d'autres éléments.
Lire

Une nouvelle téléprocédure pour les notifications de violation de données personnelles

Suite à la publication du règlement européen relatif aux failles de sécurité, la CNIL met en place une téléprocédure qui doit être utilisée par les entreprises concernées à partir du 25 aout 2013 pour notifier les violations de données dont elles ont fait l'objet.
Lire

Quelles nouveautés pour l'ISO 27001:2013 ?

Le 17 octobre prochain sortira la nouvelle norme ISO 27001:2013. Quel en sera l'impact sur les entreprises certifiées ? L'ISO dévoile les nouveautés.
Lire
En complément d'information, cet autre article analyse de manière approfondie le contenu de la nouvelle et de l'ancienne version de la norme. Lire

30

C'est en dollars le prix de 1000 « *like* » sur Facebook. À comparer aux 6 dollars pour 1000 numéros de carte de crédit.
Lire

Chez CGI Business Consulting

CGI Business Consulting participe au programme A400M

L'OCCAR (*Organisation Conjointe de Coordination en matière d'Armement)* a confié à CGI Business Consulting la réalisation d'analyses de risques, de spécifications et de procédures d'exploitation de sécurité en vue de l'homologation OTAN de l'A400M, avion de transport militaire. Ce projet s'étale sur 6 ans.

Recrutement

CGI Business Consulting fait face à une forte croissance de son activité sécurité. Notamment, nous recherchons des consultants très expérimentés en analyse de risques. Nous disposons également de nombreux postes de consultants sécurité qui sont à pourvoir. Envoyez votre candidature.

Formations EBIOS / IAM / Cybersécurité

Contactez-nous pour les dates des sessions de formation EBIOS 2010, IAM et Cybersécurité.

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

À ne pas manquer

Directeur de la rédaction Jean Olive
Comité de rédaction Guillaume Gandemer, Rémi Kouby, Vincent Maret
Contact jean.olive@cgi.com