CGI | Business Consulting

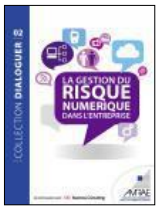
Lettre d'information

Cybersécurité et Cybercriminalité

Numéro 11 – Mars / Avril 2014

CyberÉdito

CGI Business Consulting publie avec l'AMRAE « La gestion du risque numérique dans l'entreprise »



Les DSI et RSSI ont compris depuis longtemps que le système d'information n'était pas seulement fait de technologie. Il est nécessaire de travailler avec les métiers et les autres fonctions support (RH, Achats, Juridique, Gestion des risques, …) pour assurer la sécurité du SI.

L'ouvrage (Lire) est le fruit des travaux de la commission Systèmes d'Information de l'AMRAE et de notre expérience. Il a pour ambition d'éclairer les acteurs de l'entreprise, et tout particulièrement le *risk manager*, sur les méthodes de gestion du risque numérique. Ce risque ne doit pas seulement être du domaine exclusif des experts techniques de la DSI mais inclus dans le management global des risques de l'entreprise.

Le dialogue proposé ici vise, d'une part, à permettre au *risk manager* de comprendre les risques numériques auxquels est exposée l'entreprise et de savoir si ceux-ci sont correctement appréhendés et traités par ceux qui en ont la charge. D'autre part, il permet au DSI, comme au RSSI, de bénéficier du support, tant méthodologique que d'expertise, du *risk manager*.

Cet ouvrage expose les méthodes de gestion du risque numérique dans l'entreprise et expose des applications dans les domaines de risques suivants : Cybercriminalité, Externalisation, Mobilité et BYOD, Cloud Computing, Réseaux Sociaux.

Hervé Ysnel - Associé CGI Business Consulting

Parole d'un CyberExpert

Pourquoi les aspects métier et organisationnels sont-ils nécessaires dans des audits ne relevant pourtant que des aspects techniques ?

Bien sûr, l'objectif des audits techniques est d'identifier des vulnérabilités techniques dans le périmètre défini et d'établir un plan de réduction de ces failles. Toutefois, l'expérience montre qu'un périmètre plus large doit être considéré.

Pour que la campagne d'audits soit une réussite et surtout que les plans d'action soient efficaces et pérennes, il est primordial de prendre conscience de l'origine des vulnérabilités découvertes. L'objectif sera de les corriger au plus proche de leur source. Ainsi, ce n'est pas seulement le périmètre audité qui bénéficiera des résultats de l'étude mais bien toute l'organisation.

Par exemple, lorsqu'il est découvert qu'un administrateur utilise un mot de passe faible sur un service, la correction la plus adaptée n'est pas toujours de remplacer le mot de passe. Il vaut mieux analyser la cause du choix qu'a fait cet administrateur et proposer une correction adaptée et personnalisée : il peut s'agir de sensibilisation, de mise en place de politique, de suggestion d'outils ou de processus, etc. Cette approche aura également le bénéfice d'éviter la reproduction de cette erreur dans la prochaine application déployée.

Pour cela, la relation avec les activités métier est indispensable. Chaque organisation est unique et ses enjeux spécifiques !

La prise en compte des risques métier permet de définir des scénarios d'attaque réalistes en se focalisant sur ceux engendrant les conséquences les plus critiques. La démarche consiste alors à apprécier les impacts de l'exploitation des failles. Les actions d'amélioration sont ensuite hiérarchisées sur la base de la criticité des risques induits.

Trouver des vulnérabilités sur un produit et établir un plan de correction technique limitent la population concernée par les résultats. Un audit bien mené doit mettre en relation les aspects organisationnels, techniques et les enjeux métier. Cette approche globale a un triple objectif : convaincre de l'importance des failles, de les corriger, y compris en recherchant des solutions non techniques, et de capitaliser les résultats pour éviter la réapparition de ces vulnérabilités.

Alors, tout le monde est gagnant !

Florent Cottey
Manager CGI Business Consulting

CyberMenaces

Panorama des menaces du CLUSIF

Comme il est désormais de coutume en début d'année, le CLUSIF publie son panorama des menaces 2014. Attaques *waterholing*, *ransomware*, et *malware* métier SAP sont les tendances de cette année.

Lire

Fuite d'informations sans précédent chez Orange

Difficile d'être passé à côté de la fuite massive d'informations qu'a subie Orange. La CNIL assure que l'opérateur s'est acquitté de ses obligations de notification mais déclare qu'il représente encore une exception. Qui sont les autres ?

Lire

Faites vous partie des sites les plus mal sécurisés ?

Cet article dresse la liste des sites de e-commerce les plus mal sécurisés. Au-delà du débat sur la pertinence des critères, c'est une réelle mauvaise publicité pour ces sociétés, l'article ayant été largement repris par la presse grand public.

Et si vous faisiez partie de cette liste !

Lire

Excel : une source de menace ?

Excel est largement déployé comme un outil anodin mais sa mauvaise utilisation peut devenir une source de risques. Cela met en évidence le risque induit par le contournement de la DSI.

Lire

Le bug de l'an 2014 : Windows XP

En avril 2014, Microsoft stoppera le support de Windows XP. Des « 0day » sont actuellement découvertes et attendent pour être diffusées et vendues les plus cher possibles.

Lire

Quels sont les ports les plus attaqués ?

L'étude publiée sur les ports les plus scannés permet de mettre en lumière les centres d'intérêt des attaquants ainsi que les spécificités géographiques.

Lire

Attaque de Target

L'attaque des caisses enregistreuses de Target par des accès de télémaintenance de la climatisation.

Lire

Lettre d'information
Cybersécurité et Cybercriminalité
Numéro 11 – Mars / Avril 2014

Réponses aux CyberMenaces

Les guides 2014 : ANSSI, ENISA, Club EBIOS

En attendant le RGS v2 qui semble être imminent, l'ANSSI publie trois nouveaux guides dont l'excellent guide SCADA.
Lire SCADA, restriction logicielle, TOIP
L'ENISA n'est pas en reste : deux guides de qualité ont été publiés apportant des bonnes pratiques pour la mise en place d'un CERT ainsi que de Cloud gouvernementaux.
Lire Cloud gouvernementaux, CERT
Enfin, le club EBIOS publie une réflexion opérationnelle des risques pesant sur le BYOD.
Lire

Nouveau label CNIL pour les coffres-forts numériques

Désormais, les fournisseurs de coffres-forts numériques ont la possibilité de faire labelliser leurs offres.
Lire

Un SOC externalisé et gratuit. Ça vous tente ?

Pour protéger la vie privée, externalisez votre SOC ! C'est gratuit. Ou presque… Chaque accès à vos données vous sera facturé. Vous pourrez ainsi clamer votre bonne foi étant donné qu'aucune information ne sera détenue par l'entreprise.
Lire

Les 20 contrôles critiques de sécurité du SANS Institute

Les 20 contrôles critiques du SANS Institut pour RSSI et DSI pour lutter contre les cybermenaces. Dans le cadre du *Consortium for Cybersecurity Action*, les retours d'expérience sur cette stratégie.
Lire

État des lieux de la cybersécurité sur les SCADA

Au sommaire : problématiques et architectures en jeu, techniques d'attaque et de protection, normes et référentiels, faire face à une attaque, les perspectives et recherches (conférence C&sar 2013).
Lire

Lancement du Club ISO 22301, premier club dédié à la norme sortie en 2012

Lire

CyberBrèves

Les cyberréflexes

La Gendarmerie Nationale publie une fiche réflexe des mesures à mettre en œuvre pour lutter contre les cybermenaces.
Lire

Espionnez-vous vos employés sans le montrer ?

Suite à ce qui s'est passé au ministère des Finances, les proxy SSL sont mis en avant et dénoncés comme étant des outils d'espionnage des salariés.
Lire

R2GA : le nouveau référentiel des archives

La modification de la loi sur les archives est annoncée pour le début de l'année 2014. En attendant, un référentiel général de gestion des archives à l'attention des administrations a été publié. Huit chapitres viennent apporter des éléments de réponses aux administrations qui souhaitent faire de l'archivage.
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.

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 sécurité des Opérateurs d'Importance Vitale : une nouvelle législation

Le secrétariat général de la défense et de la sécurité nationale a publié en ce début d'année une nouvelle circulaire relative aux OIV.
Lire le texte de loi, FIC 2014

La loi de programmation militaire (LPM) a été promulguée

Désormais, la LPM autoriserait de tester la sécurité informatique de sites web et de logiciels. Cette brèche juridique pourrait se traduire par une vague d'attaques sans précédent et permettre à des organisations étrangères d'attaquer légalement les entreprises françaises pour « tester » leur sécurité (Lire). Toutefois, certains y voient l'opportunité d'améliorer la sécurité des sites web dont 80% sont criblés de failles (Lire).

Vers une évolution de la loi informatique et libertés

Au vu d'un règlement européen qui tarde à éclore, un débat parlementaire le 30 janvier dernier apporte un éclairage sur le projet de loi du gouvernement portant sur « la protection de la vie privée à l'heure de la surveillance numérique, commerciale et institutionnelle ».
Lire

Rappel de la législation sur l'usage des cookies

Vous utilisez des cookies sur votre site web ? Savez-vous quand vous êtes obligés de prévenir et d'obtenir le consentement de tous les visiteurs ? Quels sont les cookies exemptés de cette obligation de consentement ? Cet article de la CNIL apporte de nombreuses réponses de nature règlementaire.
Lire

La CNIL se dote de cyberpatrouilles

C'est désormais en ligne que la CNIL va effectuer ses contrôles. Alors qu'elle était dans l'obligation de se déplacer, un texte vient de l'autoriser à effectuer les contrôles à distance. Plus de contrôle et moins d'échappatoire !
Lire

Chez CGI Business Consulting

Intégrer la sécurité dans les SI de santé

CGI Business Consulting a participé à la rédaction du guide publié par le ministère de la Santé et intitulé « Introduction à la sécurité du Système d'Information ». Ce guide est composé de fiches pratiques et est à destination des petits et moyens établissements de santé cherchant à initier une démarche sécurité.
Lire

Le guide de l'AMRAE

Voir notre CyberÉdito. Ce livre est disponible auprès de nos consultants et sur le site de l'AMRAE.
Lire

Recrutement

CGI Business Consulting fait face à une forte croissance de son activité sécurité. Envoyez votre candidature.

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

Directeur de la rédaction Jean Olive
Comité de rédaction Florent Cottey, Guillaume Gandemer, Rémi Kouby, Hervé Ysnel
Contact jean.olive@cgi.com
© CGI Business Consulting 2014 - http://www.cgi.fr/conseil/securite