CGI | Business Consulting

Lettre d'information

Cybersécurité et Cybercriminalité

Numéro 8 – Juin / Juillet 2013

Édito

SMSI et cybersécurité : deux approches qui tardent à converger

Le SMSI et la cybersécurité sont deux disciplines à priori assez dissemblables, pratiquées dans les entreprises par des populations encore souvent cloisonnées. Spécialistes de la gouvernance de la SSI, les responsables des SMSI se basent sur des processus formels et des approches d'amélioration continue, selon un cycle typiquement annuel. Le cœur de leur travail est d'analyser, d'évaluer, de documenter, de prioriser, de définir des plans d'actions visant la sécurité de l'information et d'en contrôler l'application. La cybersécurité, de son côté, s'intéresse aux menaces, attaques et moyens de défense, dans des domaines principalement technologiques. Les spécialistes de la cybersécurité font, au jour le jour, la chasse aux failles dans les systèmes, suivent l'évolution des menaces, surveillent les environnements, et réagissent en urgence aux attaques.

Ces deux mondes ont à apprendre l'un de l'autre. Le SMSI doit veiller à intégrer pleinement la très grande évolutivité des technologies, usages et menaces ainsi que la professionnalisation des attaquants. Il doit également considérer que les risques pour les entreprises dépassent la sécurité de l'information, et incluent la sécurité des SI industriels, ainsi que la sécurité dans les produits. De son côté, la cybersécurité devrait s'inspirer de la capacité du SMSI à relier les impacts métier aux scénarios de risque, à prioriser les actions, à impliquer le management, et à systématiser l'analyse des incidents.

La convergence de ces deux approches est indispensable à l'efficacité des fonctions sécurité des entreprises pour les années à venir. Cela nécessitera de synchroniser les démarches, mais aussi de faire dialoguer les personnes ainsi que les outils, comme les outils GRC et les outils de SIEM.

Vincent Maret
Associé CGI Business Consulting

Parole d'expert

La gestion des risques, où en sommes-nous ?

Depuis une petite dizaine d'années, la plupart des groupes français ont structuré progressivement leur approche et leur dispositif organisationnel. Concrètement, cela s'est souvent traduit par la mise en œuvre de démarches de cartographies des risques. Les *Risk Managers* se sont ainsi posés en acteurs incontournables de cet exercice, souvent annuel, qu'ils maîtrisent désormais parfaitement.

Cependant, les Directions Générales et les Administrateurs en attendent toujours plus. Cette attente légitime porte autant sur la mise en œuvre d'actions de sécurisation des activités que sur la démonstration de résultats tangibles.

Pour cela, le *Risk Manager* doit être en mesure de proposer une stratégie transverse de maitrise déclinée en actions concrètes, selon le profil de risque de l'organisation et ses priorités. Ainsi, cela peut se traduire par la mise en place d'un PCA, l'évaluation du risque de défaillance de fournisseurs-clés, le déploiement d'un programme de lutte contre la fraude interne et externe, la quantification de la gravité des risques du portefeuille de projets, etc. Mais il doit aussi proposer des outils de pilotage de la performance et du coût du risque, sur le plan des technologies, des activités, des processus ou des projets. Cette modélisation est souvent délicate, car les indicateurs sont à définir au cas par cas de chaque environnement organisationnel et économique.

Pourtant, c'est ce travail et ces fondamentaux qui permettront de positionner le *Risk Manager* comme un véritable *Business Partner* des différentes entités et activités de l'organisation, à même de challenger les hypothèses de son développement stratégique.

Florian Richard-Dap
Manager CGI Business Consulting

Menaces

Un exemple de *social engineering* étonnant

Ce sont 14 entreprises françaises qui ont été victimes de ces cyberattaques sur fond de *social engineering* toujours plus perfectionné. Appels téléphoniques à des personnes ciblées, mise en confiance, et e-mail infecté pour une intrusion sur un ordinateur stratégique.
Lire

Les applications mobiles sont curieuses

La CNIL et Inria livrent les résultats d'une étude menée pendant plus d'un an. Les applications que nous installons sur nos smartphones accèdent à bien plus de ressources (données, connexions, etc.) qu'elles en ont besoin. Les informations les plus récoltées sont l'identifiant unique Apple, le nom de l'appareil et les informations de géolocalisation.
Lire

Mettez à jour vos logiciels Oracle !

Oracle a publié un grand nombre de correctifs de sécurité en avril. Si vous ne les avez pas encore installés, c'est le moment ! MySQL, Database 11g, PeopleSoft, Solaris, etc. Il y en a pour tout le monde.
Lire

Internet ralenti par la plus grande attaque DDOS. Vraiment ?

Spamhaus a subit une attaque DDOS comme il n'en n'avait jamais été constatée. La presse s'affole et annonce un ralentissement de l'Internet mondial. Ce sensationnalisme recherché par la presse ne décrédibilise-t-il pas la menace, qui reste pourtant bien réelle ?
Lire

Une attaque peut en cacher d'autres

Les investigations sur une cyberattaque contre l'opérateur norvégien Telenor ont révélé un réseau indien de cybercriminalité beaucoup plus vaste. Ce rapport détaillé en dit beaucoup plus.
Lire

Lettre d'information
Cybersécurité et Cybercriminalité
Numéro 8 – Juin / Juillet 2013

Réponses aux menaces

Les guides de l'ANSSI des derniers mois

Ces derniers mois, l'ANSSI a publié plusieurs guides de recommandations sur la sécurité (dans l'ordre de parution) :

- Réseaux Wifi - Lire
- Définition d'une politique de filtrage réseau d'un pare-feu - Lire
- Usage sécurisé d'(Open)SSH - Lire
- Environnements d'exécution Java sur Windows - Lire
- Sécurisation des sites Web - Lire
- Sécurité relative aux smartphones - Lire

Mettez à l'épreuve la sécurité de vos systèmes

Cherchez vous-même les faiblesses et vulnérabilités de votre système d'information pour vous préparer à faire face aux incidents. N'attendez pas que l'incident se produise pour trouver des solutions. Si vous en avez les moyens, faites-le.
Lire

Stratégie de l'État en matière d'Identité Numérique

Plus qu'une lecture très intéressante, c'est un appel à consultation que le SGMAP (Secrétariat Général de Modernisation de l'Action Publique) propose. Un point de vue bien développé sur le sujet.
Lire

Un guide sur les systèmes d'information de santé

L'ANAP et l'ASIP Santé publient un guide sur la mutualisation et l'externalisation des SI en santé. Ce guide, à destination des décideurs, aborde les principaux concepts des systèmes d'information de manière claire et met en avant les opportunités et risques de la mutualisation et de l'externalisation des SI de santé.
Lire

L'assurance au secours des défaillances SSI des hôpitaux

L'assureur Beazley accompagne plus de 50 hôpitaux français dans leur lutte contre la cybercriminalité et les cyber-risques. Une réponse aux récents incidents de divulgation de dossiers médicaux.
Lire

Formation à la sécurité IT : des outils gratuits

Sophos, éditeur de solutions de sécurité, a mis en ligne des outils de formation et de sensibilisation à la sécurité informatique. Le tout gratuit et téléchargeable.
Lire
Et un guide faisant une bonne synthèse de la sensibilisation à la sécurité de l'information : Lire

Guide « *Cloud Computing* et protection des données »

En attendant le futur référentiel d'exigences en cours d'élaboration par l'ANSSI, ce guide pratique à l'attention des directions présente, avec des exemples concrets, les enjeux de protection des données pour ceux qui souhaitent souscrire à un service en mode *Cloud*. Il est signé par le CIGREF, l'IFACI et l'AFAI.
Lire

Règlementation

La loi CISPA : un nouvel élément de réflexion avant de transférer ses données dans le *Cloud* États-Unien

Si Barack Obama n'appose pas son véto, cette loi sera adoptée aux États-Unis. Après le *Patriot Act*, cette loi permet au gouvernement et à toutes ses agences l'accès aux bases de données hébergées dans le pays, sans aucun besoin de mandat de perquisition.
Lire

Brèves

La cybersécurité dans la stratégie de défense de la France

Le livre blanc sur la défense et la sécurité de la France a été rendu publique ce 29 avril. Plus de moyens, plus de formation d'experts, une protection accrue et une capacité de réaction, tels sont les thèmes principaux de cette stratégie de cybersécurité.
Lire

Il est temps de doper la cybersécurité des OIV

Les Opérateurs d'Importance Vitale (OIV) sont des organismes ou des entreprises stratégiques dans le cadre de la protection des intérêts de l'État. Le gouvernement se penche sur un projet de loi visant à l'obligation d'amélioration du niveau de cybersécurité de ces OIV. Une action préconisée dans le livre blanc sur la défense et la sécurité nationale.
Lire

La sécurité des systèmes industriels par le CLUSIF

Le CLUSIF constitue un groupe de travail pour se positionner sur la sécurité des systèmes industriels, dont les spécificités (interconnexion, protocoles, etc.) font qu'ils ne peuvent s'inscrire dans les approches classiques de sécurisation.
Lire

135

C'est le nombre d'infections de terminaux connectés à Internet par un botnet en 1 minute. Lire

Chez CGI Business Consulting

CGI aide ses clients à lutter contre la cybercriminalité

Président et chef de la direction, Michael E. Roach fait part de son point de vue lors d'une entrevue avec Howard Green. Il explique comment CGI aide ses clients à se protéger contre les incidents en matière de cybersécurité.
Regarder la vidéo

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 Louis Bavent, Rémi Kouby, Vincent Maret, Florian Richard-Dap
Contact jean.olive@cgi.com