CGI | Business Consulting

Lettre d'information

Cybersécurité et Cybercriminalité

Numéro 12 – Mai / Juin 2014

CyberÉdito

Axe majeur dans la maîtrise des risques, la cartographie du SI échappe pourtant au RSSI

« L'élaboration d'une cartographie du système d'information est le premier pas vers une meilleure connaissance du système d'information. » : voici la première règle du guide d'hygiène publié par l'ANSSI. En effet, comment imaginer maîtriser un système dont on ne connait pas les constituants : comment analyser efficacement une attaque sans savoir à quoi les équipements victimes ou les accès attaqués sont utilisés ? Comment déterminer la surface réelle d'une attaque sans connaître les relations d'approbation qui existent entre domaines d'administration ? Comment déterminer le niveau d'exposition du SI sans savoir où se trouvent les informations sensibles ou les points d'accès avec l'extérieur ?

Force est de constater que la maturité en matière d'inventaire patrimonial du SI des entreprises est à ce jour très faible. L'ampleur de la tâche est bien souvent un motif de découragement, sans compter sur la nécessaire dimension collaborative des travaux : métiers, urbanistes, techniciens et SSI doivent partager des visions communes. Les entreprises considèrent alors qu'il sera plus facile de réunir les experts en cas de besoin : encore faut-il les connaitre, qu'ils soient disponibles et rapidement mobilisables et que chacun ait une connaissance réellement opérationnelle des architectures.

Que peut faire le RSSI face à ce constat ? Convaincre la Direction et la DSI de s'engager dans un projet d'entreprise pour élaborer des cartographies du SI et s'inscrire comme client de cette démarche. De son côté, le RSSI peut commencer par se donner les moyens de pouvoir réunir rapidement les sachants en cas de besoin, se procurer l'inventaire des applications réellement exploitées (les plus sensibles et les plus exposées), et construire une vision exacte de l'architecture logique du SI (points d'accès externes, fonctions de filtrages et de routage, zones de confiance, fonctions des serveurs) et des périmètres d'administration. Pour chaque type d'inventaire, le RSSI doit définir le niveau de granularité adapté, issu du compromis entre capacité à maintenir à jour une information (volatilité, outils de recueil, qualité) et besoins liés aux interventions de cyberdéfense.

Jean Olive — Senior Manager CGI Business Consulting

Parole d'un CyberExpert

Gros temps pour SSL ! Que faire ?

Les implémentations du protocole TLS (ex SSL) ont montré ces derniers temps de véritables signaux de faiblesse.

En février, c'est la faille « *goto fail* » dans l'implémentation *made in Apple* qui est rendue publique. En mars, une vulnérabilité similaire est découverte : elle touche la gestion des codes erreurs dans l'implémentation GnuTLS. Enfin, en avril, c'est au tour d'OpenSSL, la bibliothèque la plus utilisée, d'être touchée. *Heartbleed* est une faille présente depuis deux ans qui permet de récupérer facilement des informations sensibles dans la mémoire (clés privées, mot de passe, etc.). Dès la publication de ces failles,, la chasse est ouverte et les attaquants ne se gênent pas pour les exploiter. Les conséquences sur les entreprises peuvent être ravageuses.

Que faire alors ? Bien évidemment, c'est la réactivité qui est ici de mise. Disposer d'une organisation qui permet de réagir le plus vite possible pour déployer les corrections. Encore faut-il connaître les éléments de son SI qui sont vulnérables ou exposés à l'Internet. Nos clients disposant d'un *footprint Internet* complet et à jour ont réussi à se procurer en moins de 48 h les résultats de *scan* de cette faille. Au grand étonnement de certains, en plus des sites internet, certains services tels que des VPN SSL étaient vulnérables.

Au-delà, la réflexion sur les licences doit être menée. Une entreprise qui utilise des implémentations gratuites doit-elle participer au financement des programmes de développement ? OpenSSL est utilisée par plus de la moitié des serveurs du monde. Pour autant, le code est maintenu en grande partie par des bénévoles. D'ailleurs, de grands acteurs américains et japonais, grands défenseurs du *closed source* pour certains, ont récemment formé le *Core Infrastructure Initiative* dans le but de financer des projets *open source* critiques. Ces projets pourront-ils rester indépendants ?

Rémi Kouby
Consultant sénior CGI Business Consulting

CyberMenaces

Bilan 2013 du CERT-IST

Le CERT-IST livre son bilan 2013 des menaces, failles et attaques. Les évolutions les plus marquantes de l'année passée sont les attaques matérielles de bas niveau, la sécurité offensive et les implications de l'« affaire Snowden ».
Lire

Une arme de précision ciblant les données stratégiques

« Careto », c'est le nom du nouveau virus de type APT développé à des fins d'espionnage ciblé de victimes stratégiques. La société Kaspersky le décrit comme étant le plus sophistiqué jamais décelé.
Lire

Les PME face au risque cybercriminel

La « fraude SEPA » est la dernière menace en date à laquelle sont confrontées les PME. Or, 80 % des risques cybercriminels des PME pourraient être évités par la mise en place de mesures simples.
Lire

DDOS : une attaque peut en cacher une autre

Les DDOS sont une menace réelle. Toutefois, de plus en plus d'attaquants l'utilisent à des fins de diversion, dans le seul but de détourner les regards de l'équipe de sécurité informatique.
Lire

300 000 routeurs attaqués

Plus de 300 000 routeurs, principalement utilisés par de petites entreprises ou des particuliers, ont récemment été victimes d'une attaque. Les utilisateurs des routeurs en question doivent s'assurer que la configuration DNS de leur appareil n'a pas été modifiée.
Lire

Illustration du *shadow IT*

En Angleterre, le National Health Service (NHS) a vu des données médicales personnelles incluant notamment les dossiers médicaux, être chargées sur des serveurs Google par l'un de ses prestataires.
Lire

Réponses aux CyberMenaces

Les enjeux liés au *Cloud computing*

Sur la base d'une enquête réalisée dans le secteur bancaire et assurantiel, le SGACP livre les principaux enseignements liés à cette nouvelle offre technologique : apparition de nouveaux risques, appréciation des politiques de sécurité, des textes règlementaires et recueil des bonnes pratiques.
Lire

Modernisez vos chartes informatiques !

BYOD, services en lignes « personnels » (dropbox, evernote, etc.), géolocalisation, partage de connexion 3G, et bientôt Google Glass, et autres objets connectés. À quoi ont droit vos employés ? Sont-ils au courant ?
Lire

PCA : les facteurs à l'origine de la crise

La préparation des hommes qui seront amenés à devoir gérer la crise est l'aspect le plus important dans la mise en œuvre d'un PCA. Le Clusif et le Club de la Continuité d'Activité font le point sur les écueils et les bonnes pratiques en la matière.
Lire

Qui sont les *responders* ?

Dans cette entrevue, Cédric Pernet explique en détail le métier de la réponse aux incidents de sécurité. Il détaille en particulier comment est effectuée la résolution des incidents, quels outils sont utilisés et les interactions avec les SOC.
Lire

Quels sont les principaux risques encourus sur un poste de travail ou un réseau de taille modeste ?

Ce document présente les principales menaces pesant sur un poste de travail ou un réseau de taille modeste, les conséquences potentielles et les mesures simples permettant de réduire le risque.
Lire

Fin du support de Windows XP : quelles solutions ?

L'ANSSI publie sa recommandation suite à l'arrêt du support de Windows XP : migrez !
Lire

CyberBrèves

Le nouveau « Big Brother » français

Thalès est désormais en charge de la plateforme nationale des interceptions judiciaires. Au-delà de la rationalisation des couts et des procédures, c'est le recours à une entreprise privée qui pourrait elle-même faire l'objet de réquisitions judiciaires, qui interpelle.
Lire

Analyse de risques et *Business Impact Analysis* : quelles différences ?

L'analyse de risques et la *Business Impact Analysis* (BIA) sont des démarches proches. Toutefois, elles n'ont pas exactement le même objectif. L'analyse de risques donne une liste de risques et vise à les couvrir. La BIA sert principalement à déterminer les délais maximums acceptables de retour à la normale ainsi que les volumes maximums de perte de données acceptables.
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

Les risques juridiques liés aux SI sont mal appréhendés

C'est le constat dressé par l'IFACI. Les trois risques cités sont les suivants : non-respect de la protection des données personnelles, la cybercriminalité et la possibilité de divulgation d'informations de nature confidentielle et l'atteinte à l'image de l'entreprise sur les réseaux sociaux.
Lire

Le vol de fichiers informatiques est désormais une infraction

La Cour d'appel de Paris prend clairement position sur le vol de fichiers informatiques et reconnait que l'infraction de vol s'applique également aux biens incorporels. Cette décision devrait faire jurisprudence en attendant le projet de loi.
Lire

Jurisprudences : e-mail perso et différences d'utilisation de la preuve au pénal et au civil

Deux jurisprudences intéressantes : un e-mail envoyé sur une boite personnelle peut être considéré comme professionnel ; une preuve obtenue de manière illégitime (enregistrement à l'insu d'autrui par exemple) peut être retenue sur le plan pénal alors que ce n'est pas le cas sur le plan civil.
Lire et Lire

CNIL : nouvelles recommandations sur l'utilisation des cartes bancaires pour le paiement à distance

La CNIL anticipe sur les évolutions règlementaires à venir et élargit le périmètre de ses recommandations relatives à l'utilisation de la carte bancaire pour le paiement à distance.
Lire

Vigipirate : un guide d'hygiène musclé !

Dans le cadre du plan Vigipirate, l'ANSSI publie un guide de recommandations à destination des collectivités et des opérateurs non-OIV.
Lire

9

C'est le nombre de types d'attaques responsables de 92 % des incidents de sécurité.
Lire

Chez CGI Business Consulting

16 mai : Table ronde sur les cyberrisques

CGI Business Consulting et l'AMRAE vous invitent à un petit-déjeuner et à une table ronde sur le sujet « Cyberattaques sur les données de vos clients : quels risques ? quelles garanties ?
Un exemplaire du livre « La gestion du risque numérique » sera offert à tous les participants.
Pour vous inscrire gratuitement, écrivez à remi.kouby@cgi.com

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 Guillaume Gandemer, Rémi Kouby, Jean Olive
Contact jean.olive@cgi.com