CGI | Business Consulting

Lettre d'information

Cybersécurité et Cybercriminalité

Numéro 13 – Octobre / Novembre 2014

CyberÉdito

Enfin une PSSI de l'État : que faut-il en retenir ?

L'été a été riche pour la SSI : règlement européen sur la confiance numérique, nouveaux guides de l'ANSSI (Active Directory, RGS v2) et … la PSSI-E. Après plusieurs années de gestation, le 17 juillet 2014, le Premier ministre a publié une circulaire : la Politique SSI de l'État (PSSI-E). Elle s'adresse aux ministères, établissements publics sous tutelle, services déconcentrés et autorités administratives. Pour les autres, vous y trouverez des règles « d'hygiène ». Si vous appartenez aux entités visées par la PSSI-E et que vous êtes RSSI, il ne vous reste que **trois mois**, jusqu'au 1er janvier 2015, pour organiser la mise en conformité en produisant une politique adaptée et un plan d'action.

Côté bonnes nouvelles, il vous reste trois ans pour conduire les actions. Si vous possédez déjà une PSSI s'appuyant sur la norme ISO2700x et que vous appliquez le guide d'hygiène informatique, il devrait vous rester peu de choses à faire. Vérifiez quand même que vous n'hébergiez aucune donnée sensible hors de nos frontières, que vous interdisiez la connexion d'équipements non maitrisés comme les clés USB et la pratique du BYOD, que vous privilégiiez l'usage de cartes à puce pour l'authentification et que vous conserviez les logs pendant douze mois contrairement à la CNIL qui conseille une conservation ne devant pas excéder six mois. Relevant de l'organisation, vous y trouverez le cycle vertueux d'amélioration en insistant sur la conduite systématique d'analyses de risques, le maintien d'une cartographie de votre SI (cf. le précédent numéro), l'emploi de services et produits qualifiés, et l'organisation des moyens de détection et de réaction aux attaques et autres incidents.

Après avoir appliqué ces 183 règles, votre système d'information est-il protégé contre toute exfiltration de données confidentielles, atteinte à la vie privée, sabotage ou panne ? Pas si sûr ! Le préambule précise qu'il ne s'agit que d'un **socle minimal**. Dans ce socle, il est regrettable de ne pas faire référence aux nombreux guides publiés par l'ANSSI, de définition des niveaux de classification, de notion de la fédération d'identité, du *cloud*, des réseaux sociaux, du *big* et *open data*, ni des objets connectés. Mais espérons que les retours d'expérience permettront, comme rappelé dans l'article 6, à la PSSI-E « d'évoluer dans le temps ».

Jean Olive — Manager CGI Business Consulting

Parole d'un CyberExpert

Quand *digital* rime avec risque ?

Aujourd'hui, une majorité d'entreprises conduit des programmes de transformation *digitale*. Combien accompagnent le projet d'une gestion des risques propres à cette transformation ? Il est nécessaire d'inclure cette démarche, car c'est souvent au cours du premier incident de production qu'apparaissent les nouveaux risques.

Sur le plan technique, ces transformations s'accompagnent de nouvelles applications développées qui sont de plus en plus dépendantes de leur écosystème. En particulier elles sont tributaires de leur environnement d'exécution (navigateur, *smartphone*, OS) et de l'obsolescence de plus en plus rapide des technologies. Une révision des processus de développement et de qualification s'impose.

Sur le plan financier, les métiers ne mesurent souvent pas le cout que représentent le support et le maintien de nouveaux services sur un grand nombre de plateformes. Les bénéfices attendus sont parfois minimes pour certaines configurations quasi confidentielles. Une communication en avant-projet doit être établie.

Sur le plan juridique, la gestion de la *vie privée* devient un enjeu majeur (droit à l'information, droit à l'oubli, droit à la vie privée). Le développement des projets *big data* et le renforcement de la règlementation européenne *(privacy by design)* mettent en lumière la méconnaissance des entreprises sur ces sujets où aucun processus liant les acteurs techniques et juridiques n'est en place.

La gestion de crise devient aussi *digitale*. La maitrise de la communication multicanale (web, SMS, réseaux sociaux, *mailing*) est vitale alors que se multiplient les *community manager* dans les entreprises sans réelle coordination entre ces différents canaux.
Il convient donc de revoir, préalablement, l'analyse de risques de l'entreprise dans le cadre de ces projets, sous peine d'entrainer des conséquences graves.

Thierry Jardin — Directeur des activités sécurité et gestion des risques CGI Business Consulting

CyberMenaces

L'authentification à deux facteurs peut être compromise

L'opération « Emmental », très sophistiquée, montre les faiblesses des usages des moyens d'authentification, pourtant à deux facteurs, utilisés par les services bancaires. Découvrez le scénario d'attaque à deux étapes : un cheval de Troie et l'utilisation du canal SMS.
Lire

1,2 milliard de mots de passe dans la nature

Un groupe de pirates russes aurait amassé plus de 1,2 milliard de couples identifiants mot de passe, en utilisant un *botnet* qui teste des injections SQL sur les sites web. Vous y croyez ?
Lire

La mort d'un service due à son manque de sécurisation

Codespace, un service *cloud* de stockage de code source, a été victime d'un chantage. Assez banal me direz-vous ! Sauf, qu'en l'espèce, le service en est arrivé à complètement fermer. Évitez que cela vous arrive !
Lire

Qui veut les clefs ?

L'étude annuelle du CLUSIF montre que près d'une entreprise sur deux n'a pas mené d'analyse de risques selon une méthode ou un référentiel éprouvés. Et une entreprise sur trois n'a aucun indicateur de sécurité pour contrôler les prestations d'infogérance du SI.
Lire

Les ports USB : nouveau vecteur d'attaque

Nous connaissions le risque des documents contenus sur les clés USB. Un bon antivirus ou mieux une suppression des fichiers et la menace disparait. Mais saviez-vous qu'un dispositif USB (clavier, souris) peut cacher un code malveillant ailleurs ? Dans le *firmware*. Il est alors impossible de le détecter ou de le supprimer par les moyens habituels… Seule solution : la signature des *firmware* de tous les dispositifs.
Lire

Lettre d'information
Cybersécurité et Cybercriminalité
Numéro 13 – Octobre / Novembre 2014

Réponses aux CyberMenaces

Guide de l'ANSSI : homologation de sécurité

L'homologation de sécurité d'un système informatique est recommandée de longue date par l'ANSSI. Aujourd'hui, l'agence apporte un guide clair en neuf étapes à destination des prétendants.
Lire

Sécurisez votre Active Directory !

Un nouveau guide de l'ANSSI qui vient donner les bonnes pratiques de sécurité à mettre en œuvre pour les administrateurs d'Active Directory. Comment modifier l'étendue de groupes, comment gérer l'historique des SID, comment réaliser des extensions de schéma ? Lisez le guide !
Lire

Charte informatique : de la rédaction au déploiement

La charte informatique, document incontournable dans les sociétés, n'a pas un contenu anodin. Il doit respecter des principes. Ce guide proposé par Olféo et le cabinet Bensoussan décrit en détail tout ce que vous devez savoir avant de vous lancer dans sa rédaction.
Lire

Cyberattaques : un marché aussi important que celui des catastrophes naturelles

Les récentes fuites d'Orange, DHL, Domino's Pizza combinées à la multiplication et sophistication des menaces incitent inévitablement les entreprises à se tourner vers les solutions de « cyberassurance ». À terme, le marché pourrait atteindre en volume celui des catastrophes naturelles.
Lire

CyberRèglementation

Les sanctions de la CNIL

La CNIL sanctionne ! Ces derniers mois les publications sont nombreuses (Foncia, Orange, CIC, etc.). Le cas d'Orange pour non-sécurisation des données est particulièrement emblématique. Attention à vos mots de passe, vos flux et vos zones commentaires.
Lire
Guide de la CNIL sur les zones de commentaires

Le RGS v2 est entré en vigueur le 1er juillet 2014

Au programme : une simplification d'ensemble, des évolutions dans l'usage des certificats, des références aux guides de l'ANSSI et la qualification des PASSI.
Lire

Qu'est-ce que le règlement européen eIDAS ?

Le 23 juillet 2014, le règlement européen eIDAS a été adopté. Il traite des services de confiance en particulier de la reconnaissance mutuelle des moyens d'identification.
Lire

La loi « secret des affaires »

Une proposition de loi a été déposée début juillet. Son but : protéger le patrimoine des entreprises. Sera-t-elle adoptée ?
Lire

CyberBrèves

5 manières infaillibles de se faire condamner par la CNIL

Ce document présente par l'exemple les cinq comportements à éviter absolument pour éviter une condamnation.
Lire … et 7 astuces pour vous mettre en conformité Lire

Prestataire américain et *datacenter* en Europe : le bon mix ?

On pourrait y croire. Et pourtant, après l'affaire Microsoft, un juge vient de confirmer le droit de l'administration américaine d'accéder aux informations se trouvant dans des *datacenter* européens de Gmail. La preuve que la localisation n'est pas une protection !
Lire

Un prestataire de téléphonie condamné pour défaut de sécurisation

Dans le cadre de l'attaque d'un réseau téléphonique d'une entreprise, le prestataire fournissant le service de téléphonie peut être mis en cause, notamment s'il n'a pas suivi les bonnes pratiques de sécurité. C'est ce qui s'est passé dans cette affaire, où les appareils disposaient toujours du mot de passe par défaut et où des obligations du contrat de maintenance n'avaient pas été respectées.
Lire

Appel à commentaire sur le référentiel d'exigences pour les prestataires sécurité *cloud*

Vous avez encore un mois pour apporter vos commentaires à l'ANSSI sur ce référentiel.
Lire

Le Patriot Act bientôt réformé ?

À la suite des révélations d'Edward Snowden, l'administration américaine pense à revoir le contenu du Patriot Act.
Lire

38%

Selon le CLUSIF, c'est le pourcentage d'entreprises ne disposant pas encore de RSSI et pourtant les incidents repartent à la hausse. Lire

Chez CGI Business Consulting

Du 1 au 3 octobre : Assises de la sécurité

CGI Business Consulting sera présent aux Assises de la sécurité à Monaco. Passez nous voir ! Stand 36, au centre du forum !
Nous animerons, avec le concours de l'AGPM, un atelier : « fuite de données : devons-nous continuer à subir ? ». L'occasion de revenir sur les usages des SI qui favorisent l'exploitation des informations sans discernement et les solutions qui réussissent.

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 Thierry Jardin, Rémi Kouby, Jean Olive
Contact jean.olive@cgi.com