CGI | Business Consulting

Lettre d'information

Cybersécurité et Cybercriminalité

Numéro 14 – Décembre 2014 / Janvier 2015

CyberÉdito

Vers un *big data* qui respecte vos droits

Les objets connectés envahissent, jour après jour, le quotidien des Français dont 61% déclarent, selon l'Ifop, être favorables à un partage des données [à caractère personnel] recueillies grâce à ces objets (Ifop). Ajoutés à la vague de la transformation digitale, les *big data* envahissent les entreprises. Si de nombreuses études et guides sur Internet décrivent les risques et recommandations de sécurisation de cette technologie, peu s'intéressent au respect des droits des personnes dans un tel contexte.

Qu'elles soient utilisées pour analyser les comportements, identifier des tendances ou détecter des incidents, les plateformes de *big data* s'appuient sur une architecture vendue comme fiable. Elles intègrent des mécanismes de contrôle d'intégrité et d'accès, de cloisonnement, et une architecture distribuée limitant les risques de fraude et de vol d'informations. Mais ces fonctions de sécurité suffisent-elles pour répondre complètement aux obligations de la loi ? Comment intégrer le consentement préalable de la personne, sans dispositif pour assurer les demandes de consultation, de rectification et contrôler la récolte volontaire de ces données ? En outre, pour respecter le droit à l'oubli des personnes, des fonctions d'anonymisation doivent être intégrées soit au moment de la collecte, soit au cours du cycle de vie des données. Au-delà de ces fonctionnalités, la sensibilisation des développeurs et *data scientists* est une action indispensable.

Les personnes, de plus en plus sensibilisées à la protection de leurs données personnelles, deviendront-elles plus vigilantes pour autant ? Quel que soit le point de vue, il s'agit d'un enjeu fondamental de la société de demain. Ce n'est qu'au prix d'une protection adéquate et d'une garantie de pouvoir disparaitre du système que les données personnelles doivent être collectées. Dès aujourd'hui, la *privacy by design* doit s'imposer dans ces nouveaux services sans attendre d'y être forcée par de futurs règlements européens.

Anthony Augereau — Manager CGI Business Consulting

Parole d'une CyberExperte

Les avancées technologiques en matière de stockage, de traitement et d'analyse de données font du *big data* l'un des plus grands changements dans le domaine de la sécurité. Là où les technologies traditionnelles de SIEM ont échoué, le *big data* réussira-t-il ? Dans tous les cas, il offre de nouvelles perspectives.

Les outils d'analyse traditionnels de SIEM supportent mal les ensembles de données hétérogènes ou non structurées. De plus, les infrastructures sont couteuses et obligent à des limitations. Le *big data* permet le stockage et l'analyse de grands ensembles de données hétérogènes à une vitesse et ampleur sans précédent. L'efficacité de cette approche vient de la combinaison de trois couches : des systèmes distribués et échelonnables pour la représentation des données, tels que Hadoop ; des outils d'interrogation en langage « naturel », comme Pig ou Hive ainsi que des algorithmes d'exploration de données ou d'apprentissage automatique comme Mahout ou RHadoop.

En divisant les temps habituels de recherche par un facteur allant de 7 à 20, les technologies *big data* permettent de réagir plus rapidement et d'élargir les champs de recherche. Elles peuvent être couplées à des SIEM classiques pour ne cibler que des trames réseau suspectes comme celles dont le domaine a déjà été identifié dans des *spam* récemment reçus, par exemple. Ces technologies permettent ainsi de parcourir l'ensemble colossal des données nécessaires pour filtrer les éléments suspects et appliquer des règles de recherche et ainsi, présenter des rapports synthétiques.

Attention ! Le *big data* ne vient pas du monde de la sécurité. Un effort de protection doit être entrepris. Il s'agit de s'assurer de l'authenticité et de l'intégrité des données manipulées. La fiabilité des sources des données doit être garantie, sans négliger la confidentialité des données analysées, de manière à encadrer la quantité d'informations qu'un utilisateur peut déduire des résultats des analyses.

Miriam Paiola – Consultante CGI Business Consulting

CyberMenaces

RSSI et *big data* : le rapprochement nécessaire

Avec la démocratisation de la numérisation et la montée en puissance du *big data* au sein des entreprises, une extension des périmètres de responsabilité est nécessaire. En effet, il apparait que les RSSI et leurs équipes sécurité ont tout intérêt à prendre le projet en main dès son lancement, de façon à pouvoir intégrer conformité et sécurité dans le *big data*.
Lire

Cyberattaque et chômage, un lien ?

C'est ce qui est arrivé à Sony Pictures. À la suite d'une attaque, aucun employé n'avait accès à son PC. La direction a invité ses salariés à rentrer chez eux le temps de résoudre une « panne informatique ».
Lire

Shellshock : les utilisations du bug en ligne de commande Bash

La vulnérabilité, découverte en septembre 2014, touche l'interpréteur de ligne de commande Unix et permet d'exécuter du code malveillant à distance. Cette faille permet de modifier des valeurs de variables d'environnement et conduit à des attaques très simples, automatisables et potentiellement dangereuses, comme on peut le voir dans les exemples illustrés.
Lire

Internet des objets : et si on attaquait votre bouilloire ?

D'après une étude de HP, la sécurité des objets connectés est insuffisante. Les appareils, même les plus anodins, ont des failles dont l'exploitation peut avoir des conséquences plus importantes. L'utilisation de mots de passe faibles et les interfaces non sécurisées sont autant de portes ouvertes sur votre réseau.
Lire

Lettre d'information
Cybersécurité et Cybercriminalité
Numéro 14 – Décembre 2014 / Janvier 2015

Réponses aux CyberMenaces

Cinq fausses idées reçues à propos de la sécurité de la virtualisation

Bien qu'elles améliorent la performance des projets applicatifs, les architectures virtualisées soulèvent des enjeux de sécurité supplémentaires. Sauriez-vous démontrer la fausseté des cinq idées reçues présentées dans cet article ?
Lire

Sécurité renforcée sur le *cloud*

Après le référentiel de l'ANSSI sur le *cloud*, voilà une nouvelle avancée de l'ISO : la norme ISO27018 donne des bonnes pratiques pour la protection des données personnelles. Il s'agit d'un outil de mise en conformité indispensable pour répondre aux exigences de sécurité et éviter d'être sanctionné par les autorités de contrôle.
Lire

France Connect : le SSO étatique est en marche

Après le succès plus que modéré de mon.service-public.fr, l'État ne se décourage pas et prépare une nouvelle version de sa solution de fédération d'identité.
Lire

Guide technique de l'ENISA pour la remontée d'incidents

L'Europe adopte l'équivalent du paquet télécom dans l'article 13a et impose la remontée des incidents détectés. Ce guide de l'ENISA donne des éléments pour la mise en place des mesures adéquates.
Lire

Le programme d'entrainement pour bien répondre aux incidents

Avoir un plan de réponse aux incidents ne suffit pas pour les traiter au mieux : il faut se tenir prêt à les gérer. Le meilleur moyen pour y être préparé ? Un entrainement quasi sportif de répétition et mémorisation.
Lire

CyberRèglementation

L'analyse des flux HTTPS : recommandations et analyse juridique

Le dernier guide de l'ANSSI donne une liste de recommandations sur l'analyse des flux HTTPS dans les entreprises. Lire
Si vous souhaitez mettre en œuvre cette analyse, n'oubliez pas les obligations légales. Lire

Faut-il respecter la loi informatique et liberté ?

Cette question pragmatique pose une question : les frais de mise en conformité ne sont-ils pas plus élevés que le cout d'une sanction CNIL, même si des risques pénaux existent ? Lire
Une illustration : Prisma Media récidive et se voit condamné, de nouveau, à subir de « sévères » sanctions. Lire

Le PIA du règlement européen expliqué en détail

Un excellent livre blanc vient d'être publié par SAGE sur le « qui ? », « quand ? », « quoi ? » et le « comment ? » réaliser une étude d'impact sur la vie privée telle que prochainement rendue obligatoire par l'article 33 du RGPD.
Lire

CGI Business Consulting fait partie du groupe CGI inc, 5e 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.

CyberBrèves

Les réalités de la localisation territoriale

Après le scandale PRISM, plusieurs États et entreprises ont pris des mesures de localisation territoriales de leurs données afin de mieux les protéger. Mais est-ce la bonne solution ?
Lire

Les alliés d'une gestion optimale des risques

Une démarche spécifique de gestion des risques permet d'augmenter le taux de détection des incidents, réduire les délais de réaction et apporter les solutions les mieux adaptées.
Lire

Apple, pas toujours si sûr !

80% des *malware* sur mobile ciblent Android ? Mais en voilà un qui touche bien iOS. Et il permet d'installer n'importe quelle application, sans passer par l'AppStore, en faisant simplement cliquer un utilisateur sur un lien ou une pub. Protégez-vous assez votre flotte d'iPhone ?
Lire

La surveillance des flux ne suffit pas !

En tout cas, pas pour ce mode de communication. Alors que l'on vous vante souvent l'analyse des signaux faibles, un mode de communication auquel vous n'aviez pas pensé peut être utilisé par les *malware* : le dossier « brouillon » d'une boite Gmail.
Lire

Fin du support de Windows Server 2003

Êtes-vous prêt à migrer ? En juillet 2015, le support de Windows Server 2003 se termine. Sans mises à jour ni correctifs, vos serveurs pourront être en danger.
Lire

250 M€

C'est ce qu'aura couté aux entreprises françaises l'arnaque au président entre 2010 et 2014.
Lire

Chez CGI Business Consulting

CGI est en cours de qualification PASSI

CGI Business Consulting est officiellement en cours de qualification de prestataire d'audit de la sécurité des systèmes d'information (PASSI) par l'ANSSI.
Lire

CGI protège les systèmes industriels

CGI Business Consulting propose des prestations d'audit de sécurité, de tests d'intrusion et d'*Internet footprint* sur les systèmes industriels (SCADA, etc.). Pour toute information complémentaire, n'hésitez pas à nous contacter.

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 Anthony Augereau, Julie Jeantot, Rémi Kouby, Jean Olive, Miriam Paiola
Contact jean.olive@cgi.com
© CGI Business Consulting 2014 - http://www.cgi.fr/conseil/securite