CGI | Business Consulting

Lettre d'information

Cybersécurité et Cybercriminalité

Numéro 19 – Mai / Juin 2016

CyberÉdito

Vous êtes RSSI. Vous voyez depuis quelques semaines un grand nombre d'articles sur les *bug bounties*. Ces programmes de cybersécurité sont mis en place par les entreprises elles-mêmes ou via des plateformes faisant l'intermédiaire comme bugcrowd.com ou le français bountyfactory.io récemment. Ces plateformes proposent de mutualiser les compétences d'experts sécurité *white-hat* afin d'offrir un service payé au résultat et non aux ressources ou moyens engagés pendant les tests d'intrusion. Outre les questions technicoéthiques qui ont été de nombreuses fois abordées sur le web, vous êtes séduit par le concept d'obligation de résultat et non de moyens. Vous vous lancez dans l'exercice et deux options s'offrent à vous :

- Option 1, lancer votre propre *bug bounty*. Il vous faut créer des règles, un processus de soumission de bugs, un accès sécurisé ouvert (paradoxalement …) aux contributeurs « hackers », ainsi qu'une équipe hautement qualifiée en sécurité capable d'analyser, qualifier et prioriser les soumissions et leur traitement. Attention également à superviser de près l'activité des « hackers ».
- Option 2, vous déléguez ces tâches à une plateforme externe. Cela signifie qu'un abonnement doit être payé avant même de devoir récompenser le moindre résultat. Vous devez choisir et négocier un modèle économique qui prévoit le cout d'un rapport signal à bruit trop faible dans les soumissions de bugs. Autre constat : la plateforme ne peut pas sérieusement qualifier les bugs sans prendre en compte les enjeux de votre métier ou avoir accès à du code sensible.

Quelques mois passent et votre programme *bug bounty* ne remonte aucune faille majeure. Votre SI est-il si bien sécurisé ou bien trop peu de « hackers » compétents sur le périmètre testé se sont intéressés à vos *bounties* ? Pire, il y a peut-être bien des failles, mais elles ont été divulguées à plus offrant, sur le marché noir des 0-day…

À la fin, le concept « payer au résultat » vous échappe. Le *bug bounty* est un outil intéressant, mais il ne remplace pas les audits et le conseil SSI et se rapproche de la mise en place de services de type SOC, l'assurance en moins.

Mouloud Aït-Kaci – Consultant sécurité et gestion des risques – CGI Business Consulting

Parole d'un CyberExpert

CDO et CISO : quelles places dans l'organisation ?

La transformation digitale implique une évolution du système d'information. Centré initialement sur les traitements, ce sont désormais les données qui y sont au cœur. Le besoin de gouvernance de la donnée au sein des entreprises prend aujourd'hui tout son sens. Il se matérialise par la création de nouvelles fonctions comme le CDO dont l'acronyme signifie aussi bien *Chief Data Officer* que *Chief Digital Officer* :

- le CDO *data* est chargé de mettre en place et de faire appliquer une stratégie de gouvernance des données ;
- le CDO *digital* a lui pour objectif de valoriser les données détenues par son organisation, en définissant de nouveaux services (*big data, open data, deep learning, etc.*). Cette activité ne peut s'exercer que si une gouvernance des données a été mise en place préalablement.

Aujourd'hui, le CISO assure la protection de ces données. Si nous prenons les besoins de classification et donc de protection de ses données, il existe des synergies potentielles entre CISO et CDO *data* sur ces activités. Le CISO est donc un client naturel, comme le CDO *digital,* des travaux réalisés par le CDO *data*.

Les fonctions de CISO et CDO *data* ne pourraient-elles pas être affectées à la même structure afin de faciliter la gouvernance dans l'entreprise ? Deux stratégies émergent :

- positionner le CISO en dehors de la DSI (métiers, fonctions *corporate*). Il peut dans ce cas couvrir les fonctions de CDO *data*. Il doit alors disposer de compétences dans la gouvernance des données et la transformation digitale ;
- positionner le CISO au sein de la DSI. Il a alors un rôle plus opérationnel et doit composer avec un autre acteur qui assurera la conformité sur l'usage des données dans l'entreprise.

Enfin, il existe des cas de CDO *digital* et *data*. Dans ce cas, les entreprises prennent le risque d'un problème de gouvernance en matière de conformité : on ne peut être à la fois juge et partie sur l'utilisation des données, notamment personnelles.

Thierry Jardin — Vice-président en charge des activités sécurité et gestion des risques

Spécial *Ransomware*

Ransomware : les attaques s'intensifient …

Plusieurs attaques par *ransomware* ont fait les gros titres ces derniers mois. Celles-ci ont démontré les difficultés des SI à répondre à ces menaces. Les attaques sont par ailleurs de plus en plus sophistiquées. Dernière évolution en date, le *ransomware* s'attaque désormais aux sauvegardes afin de contraindre les victimes à passer à la caisse.
Lire

Une infection par un *ransomware*, minute par minute, racontée par un RSSI

Afin de comprendre à quoi peut ressembler une attaque de ce genre, le RSSI de l'AFP, récemment victime d'un *ransomware*, raconte les faits, pas à pas.
Lire

Ransomware : comment s'en protéger ?

Cet article livre quelques bonnes pratiques pour se protéger des *ransomware* : appliquer une politique de segmentation réseau, procéder à des sauvegardes fréquentes et surtout, maitriser le processus de restauration en le testant régulièrement, former les employés à la détection des malware, maintenir à jour les équipements, utiliser des antimalware réputés, etc.
Lire

Comment réagir lorsque le mal est fait ?

Et lorsqu'un *ransomware* affecte votre SI ? Il faut réagir rapidement pour en limiter la diffusion et les dégâts !
Lire

Ransomware : faut-il payer la rançon ?

Dans tous les cas, il est hors question de payer la rançon aux cybercriminels, comme indiqué par Guillaume Poupard, directeur de l'ANSSI. La meilleure solution reste les protections évoquées dans les articles ci-dessus : antimalware et sauvegardes régulières.
Lire

Lettre d'information
Cybersécurité et Cybercriminalité
Numéro 19 – Mai / Juin 2016

CyberMenaces

Wordpress encore accusé à tort

Des installateurs de Linux Mint infectés, modifiés par un pirate, ont été déployés sur le site officiel. Une porte dérobée a pu être installée en raison de mauvaises permissions sur les dossiers de l'hébergement. Le fameux CMS, bien trop souvent pointé du doigt, est encore une fois hors de cause.
Lire

Une simple imprimante 2D peut avoir raison d'un lecteur d'empreintes de *smartphone*

Le capteur biométrique, porte d'entrée du *smartphone*, se popularise. Il devient une cible privilégiée pour contourner la sécurité. Des chercheurs ont découvert qu'il était possible de tromper un capteur en lui présentant une impression de l'empreinte digitale du détenteur de l'appareil.
Lire

Réponses aux CyberMenaces

Mise en production : suivez les commandements !

Une *checklist* qui reprend les éléments de sécurité basiques à vérifier impérativement, avec les commandes shell associées : ce dont vous avez toujours rêvé pour vous assurer des mises en production sereines.
Lire

ANSSI : des exigences de sécurité pour les prestataires d'intégration et de maintenance de SCADA

Une aide pour vos cahiers des charges : l'ANSSI a publié un nouveau référentiel d'exigences de sécurité pour les prestataires d'intégration et de maintenance des systèmes industriels.
Lire

CyberRèglementation

Le règlement européen sur la protection des données personnelles a été approuvé

Au programme : accord explicite de l'utilisateur, portabilité des donnés, droit à l'oubli, notification des fuites d'informations et amendes dissuasives. Ces mesures entreront en vigueur en avril 2018.
Lire

CNIL : 100 000 euros d'amende pour Google

Google refuse le déréférencement des liens du moteur de recherche pour les domaines non européens. La présidente de la CNIL avait mis en demeure Google en mai 2015, qui avait alors proposé un filtrage selon le pays de l'utilisateur. Cette solution n'a pas convaincu la formation restreinte de la CNIL.
Lire

La pseudonymisation au secours de la protection des DCP

Le règlement européen relatif à la protection des données à caractère personnel a introduit le principe de pseudonymisation.
Lire
Pour mettre en place des mécanismes de peudonymisation, il est possible de s'appuyer sur la norme ISO/TS 25237:2008, qui établit un certain nombre de principes et d'exigences en matière de protection des DCP à l'aide de services de pseudonymisation.
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

Mise en demeure de Facebook par la CNIL

Facebook ayant un établissement en France, la CNIL a estimé que la loi de 1978 lui était applicable. Début 2015, des contrôles ont été effectués et plusieurs manquements ont été relevés : ciblage publicitaire sans consentement, faible sécurité des mots de passe, conservation disproportionnée de données face à la finalité ou encore absence de demande d'accord à l'installation de cookies.
Lire

Mots de passe : simplifiez la vie de l'utilisateur !

Une récente étude commanditée par le gouvernement britannique a mis en évidence que l'utilisation de mots de passe complexes n'améliorait pas nécessairement la sécurité d'un SI. Au contraire ! Le dessin humoristique d'xkcd sera-t-il enfin suivi d'effets ?
Lire

SCADA : retour sur l'attaque du réseau électrique ukrainien

L'attaque du réseau électrique ukrainien ayant provoqué une immense panne de courant le 23 décembre 2015 et privant ainsi 225 000 foyers d'électricité a finalement pu être élucidée. Les analystes sont formels : l'attaque a été longuement préparée : campagne de *phishing* ciblée, prolifération de malware, vol de données d'identification, déni de service du système téléphonique et suppression des traces.
Lire

Sigfox : et si on n'oubliait pas la sécurité en construisant un nouveau réseau ?

Une étude de sécurité menée par un consultant a mis en évidence certaines faiblesses du réseau Sigfox. Sont pointées du doigt l'absence de chiffrement des échanges et la possibilité d'usurpation d'identité. Selon le vice-président innovation de la start-up, Sigfox a pris le parti de laisser la responsabilité du chiffrement (applicatif) au client, comme cela peut être le cas pour le réseau Internet. Néanmoins, des améliorations semblent être envisagées pour limiter les risques d'usurpation d'identité.
Lire

20%

C'est la proportion d'employés prêts à vendre leur mot de passe.

Lire

Chez CGI Business Consulting

La cybersécurité vue par les patrons des plus importantes entreprises britanniques

Après avoir interrogé plus de 150 membres de direction et comités exécutifs des plus grandes entreprises britanniques, CGI publie les résultats de ses recherches.
Lire

Recrutement

L'activité sécurité de CGI Business Consulting est à la recherche de nombreux talents pour répondre aux besoins grandissants de nouveaux clients. Envoyez votre candidature.

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

Directeur de la rédaction Rémi Kouby
Comité de rédaction Mouloud Aït-Kaci, Geoffroy Andrieu, Rémi Kouby, Thierry Jardin, Jean Olive, Miriam Paiola
Contact remi.kouby@cgi.com