CGI | Business Consulting

CYBERSÉCURITÉ
LA LETTRE

Numéro 21 - Mars / Avril 2018

ÉDITO

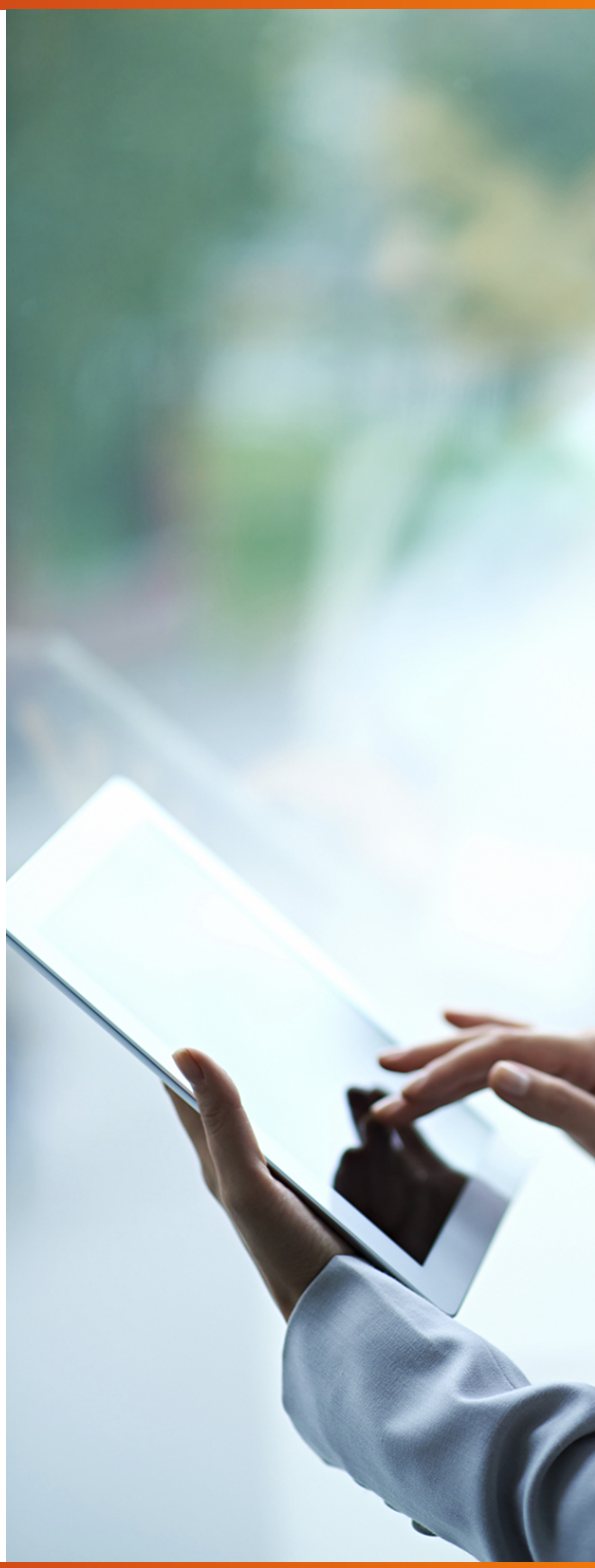
Le RPA : une technologie à mettre au service du RSSI et des fonctions de contrôle ?

Certains processus métiers sont encore composés de tâches répétitives qui sont exécutées manuellement, comme la compilation de données provenant de sources différentes. Pour les outiller, une solution d'automatisation traditionnelle, par développement de script ou d'une fonctionnalité dans une application du SI, n'est parfois pas flexible, intéressante économiquement ou adaptée aux besoins des métiers. Le RPA devient alors une solution intéressante.

RPA est l'acronyme de *Robotic Process Automation*. Il s'agit d'un ensemble de solutions proposant l'automatisation des tâches répétitives au sein des back-office métiers des entreprises par une approche *low code*, c'est-à-dire nécessitant peu ou pas de programmation. Les outils RPA se positionnent en concurrence des solutions classiques d'automatisation. Ils sont faciles à configurer, disposent d'une interface intuitive et d'une logique de workflow. En quelques heures, l'automatisation d'une tâche est réalisable, par le métier, seul.

Que penser de l'arrivée de cette technologie pour les métiers de la sécurité et du contrôle ?

Il est tout d'abord essentiel de se pencher sur les risques. Le RPA met à la main d'utilisateurs métiers un moteur de scripts puissant, qui, mal utilisé, pourrait provoquer des dommages dans le système d'information (altération de bases de données, etc.). La formation des utilisateurs est donc essentielle, malgré l'apparente facilité d'utilisation de ces outils. L'authentification est également essentielle : lorsqu'il est utilisé directement par les utilisateurs finaux, le RPA peut se



connecter à des applications avec les identifiants et mots de passe de l'utilisateur pour réaliser des actions en masse. Ils sont donc enregistrés dans l'outil RPA, qui sans chiffrement robuste peut provoquer une fuite d'information incontrôlée.

Plus pernicieuse, une utilisation généralisée, voire systématique, du RPA pourrait générer des effets pervers, comme le report de projets d'évolutions du SI, ces derniers voyant leur ROI chuter, étant cannibalisés par cette automatisation low cost. À terme, une dette technique considérable pourrait s'accumuler. Enfin, il suffit d'un changement de version d'une application pour que les commandes doivent être mises à jour, voire revues complètement, dans le pire des cas. Une gouvernance stricte des opérations de maintenance doit donc être mise en place pour éviter un risque de désordre dans l'environnement IT.

Le RPA reste toutefois une opportunité, notamment pour les métiers de la sécurité et de la gestion des risques. Il existe déjà des applications éprouvées, par exemple dans la gestion des identités et des accès. En effet, grâce à son coût relativement faible, le RPA peut compléter une solution d'IAM existante pour provisionner des bases de comptes et de droits lorsqu'il est difficile économiquement ou techniquement de le faire. Un autre exemple en plein essor est l'automatisation des contrôles pour assister la fonction « contrôle interne » dans ses tâches chronophages. Le robot va chercher directement les exports de données dont il a besoin dans les applicatifs métiers, et calcule un taux de conformité ou un résultat de contrôle. Ce résultat est ensuite automatiquement renseigné dans l'outil GRC, tout en stockant la preuve de contrôle associée.

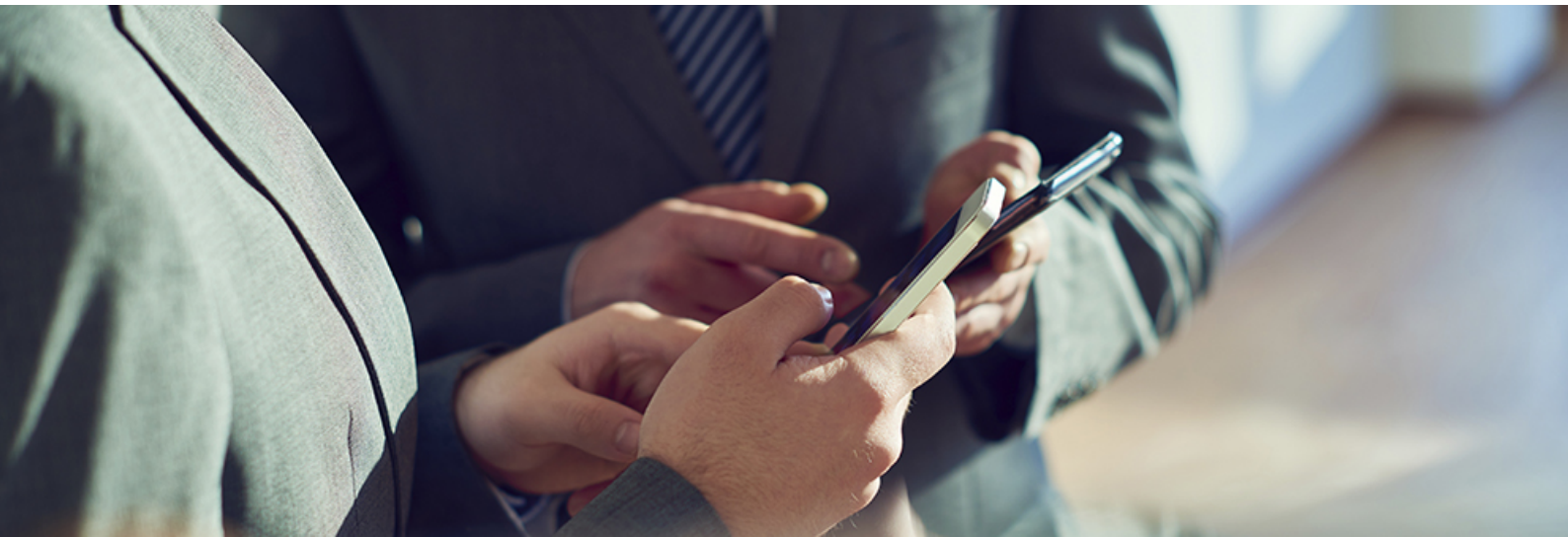
Faut-il donc s'intéresser au RPA ?

Oui, sans aucun doute, mais à condition d'avoir bien évalué les cas d'usages et réfléchi à son mode de déploiement, d'exploitation et de maintenance. Les cas d'utilisation actuels du RPA les plus intéressants sont ceux où cette technologie est un complément aux autres solutions d'automatisation traditionnelles. À l'avenir, le RPA pourra permettre aux métiers d'accéder facilement et directement à des moteurs de décision plus complexes, notamment à base d'intelligence artificielle.

Pour en savoir plus, retrouvez dans notre livre blanc l'approche *lean cognitif* que nous proposons pour atteindre un premier résultat rapidement.

Lire le livre blanc RPA

PAUL COURSAULT
Consultant sécurité et gestion des risques
paul.coursault@cgi.com



RÈGLEMENTATION · BOÎTE À OUTILS RGPD

Comment ne pas évoquer le RGPD ? Son entrée en vigueur approchant, nous vous proposons une sélection d'outils pour vous accompagner et vous guider dans vos travaux de mise en conformité.

Le cahier technique de l'AMRAE pour une vision complète et détaillée

Le 8 février dernier, l'AMRAE, en collaboration avec notre cabinet CGI Business Consulting, a publié le cahier technique « RGPD - La protection des données du citoyen européen par l'entreprise ». Ce document didactique vous donne les clés de votre mise en conformité à cette nouvelle règlementation. Il passe en revue les principes de licéité du traitement des données personnelles, le renforcement des droits des personnes concernées ainsi que les acteurs impliqués et leurs responsabilités. Un dernier chapitre est consacré à la démarche de mise en conformité et aux facteurs clés de succès qui feront la réussite d'un tel projet.

Consulter le cahier technique AMRAE

Des cas pratiques de PIA

Le manuel « *Security of Personal Data Processing* » proposé par l'ENISA expose des cas pratiques d'analyses d'impact sur la vie privée (PIA). Présenté sous la forme de cas pratiques, ce guide vous donne des exemples concrets de PIA sur des traitements de données personnelles : recrutement, paie, achats, marketing ou encore gestion des badges. Une première approche très didactique du sujet !

Consulter le manuel de l'ENISA

Un outil signé de la CNIL pour accompagner vos démarches de PIA

La CNIL met à disposition un logiciel visant à faciliter la conduite et la formalisation d'analyses d'impact sur la vie privée tel que prévu par le RGPD. On attend encore l'intégration automatique des bases de connaissance, notamment de mesures et bonnes pratiques, directement dans l'outil.

Télécharger l'outil de PIA de la CNIL

Une vue globale du RGPD en une infographie

Depuis quelques mois, les infographies sur le RGPD se multiplient, mais une seule a retenu notre attention : celle du CLUSIF. Elle ne vous permettra pas de rentrer dans le sujet mais s'adresse plutôt à des initiés en proposant une synthèse efficace des différents articles et de leurs cas d'application.

Découvrir l'infographie du CLUSIF

Focus - Droit à l'oubli

Le droit à l'oubli prévu à l'article 17 du RGPD peut susciter quelques craintes. Est-ce justifié ? Pas si sûr ! « La Cour de cassation a, dans un arrêt rendu mi-février, marqué son opposition à toute injonction de déréférencement d'ordre général, dans le cadre du droit à l'oubli. Les juridictions doivent vérifier le bien-fondé des demandes et tenir compte de l'intérêt du public. » Cette décision, prise dans le cadre d'une demande de déréférencement faite par un particulier à l'encontre de Google, pourrait s'appliquer à toute autre demande de suppression.

Plus de détails

CYBER BRÈVES

Attaques, failles de sécurité, nouvelles règlementations, condamnations. Les actualités dans le domaine de la cybersécurité sont riches. Bien souvent des leçons peuvent en être tirées. Voici quelques faits divers à ne pas manquer.

La directive NIS enfin transposée

La directive européenne de 2016 dite *Network and Information Security*, souvent appelée directive NIS, a été transposé en droit Français.

Elle définit deux types d'acteurs : les opérateurs de services essentiels qui offrent des services essentiels au fonctionnement de la société ou de l'économie (banque, énergie, transport, eau, etc.) et les fournisseurs de services numérques que sont les places de marché en ligne, les moteurs de recherche et les services d'informatique *Cloud*. Cette directive fait peser de nouvelles contraintes et obligation sur ces acteurs : ils doivent mettre en oeuvre les mesures techniques et organisationnelles qui permettent de prévenir et réduire l'impact des incidents, identifier les risques de sécurité SI qui pèsent sur leurs activité et notifier à l'ANSSI les incidents de sécurité qu'ils subissent. Les acteurs devront également coopérer lors de contrôles avec l'ANSSI sous peine de sanctions pouvant atteindre 125000 euros.

Lire l'article

Chez FedEx, les données aussi s'envolent

Fin 2014, FedEx rachète Bongo International, spécialiste en technologies et solutions de commerce électronique.

Plusieurs services utilisés à l'origine par Bongo sont fermés. Enfin, presque tous... Parmi les oubliés, un serveur *Cloud* Amazon, contenant plus de cent-vingt-mille documents numérisés, y compris des passeports, des permis de conduire et des identifiants de sécurité. Laissés en déshérence, les services AWS de Bongo n'étaient plus maintenus ni surveillés, et donc à la merci de la première attaque venue. Finalement, début 2018, la société se voit dérober la totalité des données présentes sur le serveur. Une fuite qui aurait pu être évitée avec un audit sécurité rigoureux des actifs informatiques présents sur le *Cloud*.

Lire l'article

Quand objet connecté et géolocalisation ne font pas bon ménage !

En janvier dernier, l'application de fitness « Strava » dévoilait des itinéraires empruntés par des soldats français et américains autour de leurs bases militaires secrètes. L'affaire a été prise au sérieux par l'armée française, en rappelant à ses soldats de désactiver leurs fonctions de géolocalisation et de GPS. Certains agents de la DGSE ont toutefois pu être identifié car ils s'inscrivaient sous leur vrai noms à des compétitions officielles. Une simple corrélation des temps de parcours permet alors de retrouver les identités véritables des pseudos Strava.

Lire l'article

Pour de l'information en temps réel, retrouvez-vous nous sur twitter **@CGIsecurite**

Consulltez les précédents numéros de la lettre cybersécurité sur **https://www.cgi.fr/view/brochure**

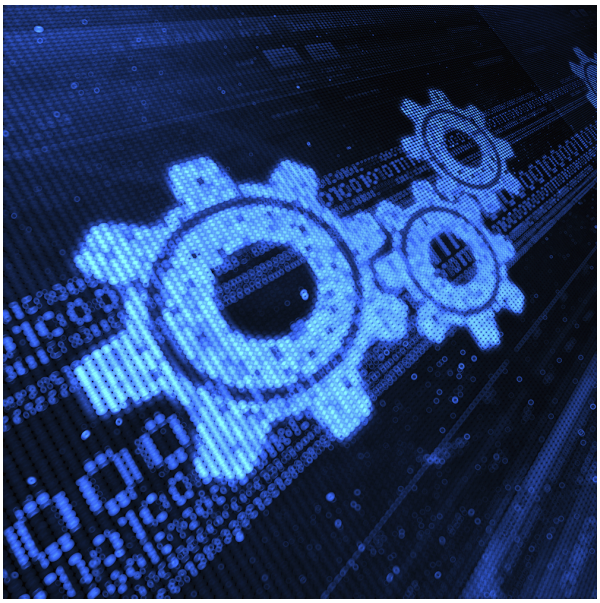
CRYPTOJACKING · LA NOUVELLE MENACE

Les *ransomware* deviennent *old school*. Place aux *cryptominer* ! Toujours plus discrètes, ces attaques rapportent encore plus d'argent. Explications.

Le succès des cryptomonnaies

Si le bitcoin est né il y a plus de 10 ans, ce n'est que depuis un an qu'il rencontre un vif succès auprès des entreprises et des particuliers.

Pour rappel, une cryptomonnaie repose sur un immense registre de toutes les transactions jamais effectuées : la *blockchain*. Cette dernière fonctionne comme un livre où sont ajoutées à intervalle régulier de nouvelles pages (blocs) sur lesquelles sont inscrites les dernières transactions. Ce travail d'écriture est réalisé par des machines, les mineurs, qui, en contrepartie, sont rémunérés en cryptomonnaie. Cependant, cette technique requiert une énergie et une puissance de traitement informatique considérable. Vous l'aurez compris, les cybercriminels n'ont donc pas pu résister à profiter du système. Comment ? En résolvant le problème de la quantité de ressources informatiques nécessaires pour faire tourner ce processus. Ce sont désormais les ordinateurs des utilisateurs qui sont réquisitionnés pour faire le travail.



Le cryptominer va-t-il remplacer le ransomware ?

Vous n'achetez pas de cryptomonnaie donc vous pensez être exempté de ce type d'attaque. Erreur ! Tout le monde peut être victime de minage de cryptomonnaie et cela porte un nom : le *cryptojacking*.

Il est loin le temps des campagnes de *ransomware* qui bloquaient les postes et demandaient une somme d'argent en échange d'une clé de déchiffrement. Avec le *cryptojacking*, les attaques évoluent. Vous naviguez librement sur des sites web, les publicités de vos marques préférées affluent, vous cliquez sur l'une d'entre elles et continuez vos activités.

Ces *malware* opèrent dans l'ombre. Aucun signe ne laisse penser que votre PC ou *smartphone* a été piraté. On vous explique.

Le site web infecté fait exécuter du code JavaScript pour faire tourner le *cryptominer*, en utilisant les ressources de toutes les machines qui le visite. De cette manière le mineur détourne votre CPU et redirige la puissance récupérée pour le calcul de transactions. De la même façon, les applications mobiles pourraient être utilisées pour miner de la cryptomonnaie à votre insu. Vous seriez alors en train de miner tout en jouant, par exemple, à votre jeu préféré. Autre technique, s'infiltrer dans le SI de l'entreprise, déposer des clients de minage sur des serveurs et se faire le plus discret possible. Là encore les ressources CPU mais aussi le réseau électrique sont exploités et ce sur la durée, les pertes financières peuvent être considérables. De plus, il se pourrait que le bon fonctionnement de certains programmes soit remis en cause.

Le *cryptojacking*, qui semblait jusqu'à présent cibler uniquement les particuliers, va devenir un enjeu de taille pour les entreprises. Outre la prévention qui passe par le blocage de l'exécution automatique de JavaScript, l'utilisation d'un antivirus ou la sensibilisation, la surveillance de l'utilisation de vos ressources doit plus que jamais faire partie de votre éventail de mesures de sécurité.

ESTELLE DE MONCHY
Consultante sécurité et gestion des risques
estelle.demonchy@cgi.com

LE RISQUE CYBER AU CŒUR DES PRÉOCCUPATIONS

Le risque cyber ne cesse d'être pointé du doigt par les entreprises, les collectivités, les particuliers et les médias. Les dernières études en la matière affichent clairement une montée en puissance qui semble aujourd'hui inévitable.

La cybermenace : une préoccupation majeure pour la sécurité nationale

Forte de ses 167 pages, la revue stratégique de cyberdéfense, publié par le secrétariat général de la défense et de la sécurité nationale, dresse un panorama des menaces actuelles, propose des actions d'amélioration pour le pays et ouvre des perspectives visant à mieux appréhender les enjeux liés à la sécurité de l'information.

Ce livre blanc de la cyberdéfense aide les entreprises à se préparer face aux attaques récentes, comme Wannacry et NotPetya. À ce titre, la loi de programmation militaire prévoit une enveloppe budgétaire consacrée à la cyberdéfense de 1,6 milliard d'euros pour la période 2019-2025 ainsi qu'une augmentation du personnel porté à 1000 personnes.

Lire la revue cyberdéfense

Numéro 1 des risques dans l'assurance

Suite à un sondage mené par la FFA auprès des directeurs des risques des 30 principales sociétés d'assurances en France, le verdict est tombé ! Le risque cyber obtient la première place du podium, devant les risques économiques, environnementaux ou politiques.

Ce baromètre va, pour la cinquième année consécutive, permettre d'intégrer les risques cyber au cœur du pilotage et de la stratégie de développement des entreprises.

Lire le baromètre des risques émergents

Un risque positionné juste derrière les risques environnementaux

Le WEF, *World Economic Forum*, une communauté d'experts et d'analystes, publie chaque année un rapport synthétisant les risques les plus probables auxquels le monde sera confronté pour les dix prochaines années.

En 2018, nous remarquons une évolution notable du risque cyber dans le classement par rapport à l'an dernier. Il trouve désormais sa place sur le podium des risques les plus probables et se classe 6e en gravité, juste derrière les risques environnementaux (évènements météo extrêmes, catastrophes naturelles et changements climatiques). Pour rappel, en 2017, il se positionnait sixième en matière de probabilité et en dehors du top 10 quant à son impact.

Cette montée en puissance s'explique en grande partie par une dépendance aux outils informatiques toujours plus importante, par la croissance des classes moyennes dans les économies émergentes et par un accroissement de la mobilité géographique.

Lire le rapport du WEF

1,6 milliard d'euros c'est l'enveloppe budgétaire prévue par la LPM pour la période 2019-2025, consacrée à la cyberdéfense.

LA BIBLIOTHÈQUE CYBER

Tous les deux mois, retrouvez notre sélection de guides, livres blancs, études ou tout autre document d'analyse ayant suscité notre intérêt. Bonne lecture !

Sécurité sur les médias sociaux

Hootsuit publie un guide sur les « Cinq étapes pour sécuriser votre présence sur les médias sociaux » qui doivent permettre à « votre directeur de la Communication ou votre responsable de Sécurité [de] souffler un peu ». Au menu, formation des salariés, centralisation des comptes, détection des activités suspectes et plus encore.

Cas concrets de PIA par l'ENISA

Les guides méthodologiques dédiés à la réalisation d'analyses d'impacts sur la protection des données sont nombreux et bien souvent longs et complexes à mettre en œuvre. Pour y remédier, l'ENISA a voulu proposer des cas concrets d'application de sa méthode d'évaluation des impacts.

Cybersécurité et IoT

Ce document, proposé par le « *Interagency International Cyber Security Working Group* », décrit les objectifs de sécurité de l'IoT, les principales menaces qui pèsent sur ce système ainsi que les principaux risques en résultant. Le livre blanc aborde les mesures et bonnes pratiques en matière de sécurité des objets connectés.

Revue cyberdéfense du SGDSN

« Véritable Livre blanc de la cyberdéfense, il est le premier grand exercice de synthèse stratégique dans ce domaine. Organisé en trois parties, il dresse un panorama de la cybermenace, formule des propositions d'amélioration de la cyberdéfense et ouvre des perspectives visant à améliorer la cybersécurité de la société française. »

Cahier technique AMRAE - RGPD

Déjà présenté dans notre boite à outils RGPD, ce cahier technique, proposé par l'AMRAE en collaboration avec CGI Business Consulting, vous apporte un éclairage sur les exigences posées par le RGPD et vous aidera dans votre de démarche de mise en conformité.

ENISA - Culture cybersecurité

Instaurer une culture cybersécurité dans l'entreprise est devenu un enjeu majeur. Selon une récente étude, il s'agirait même de la meilleure arme de défense contre les attaques. Alors qu'attendez-vous pour développer votre véritable pare-feu humain ? Suivez le guide de l'ENISA, il s'applique à tout type d'organisation, de structure, de secteur.

LA SÉLECTION DU CYSLAB

Cette section est alimentée par notre équipe d'experts du laboratoire de sécurité. Elle met en avant des sujets d'actualité et de veille dans les domaines de l'audit technique, de la détection et de la réponse à incident.

GitHub et OVH tiennent bon face au DDoS

Le 28 février et le 1er mars 2018, GitHub et OVH ont subi la plus grosse attaque DDoS jamais recensée, dépassant les 1,3 Tbps. À la différence d'un DDoS « classique », l'attaque ne s'est pas appuyée sur un botnet, mais sur des serveurs de cache (memchached) mal configurés. Heureusement, il a fallu moins de 10 minutes à GitHub pour remettre son site web en service alors que pour OVH aucune interruption de service n'a été constatée. Malgré tout, répondre à cette attaque n'était pas de tout repos pour ces deux grands acteurs IT. OVH vous propose de revenir sur cette « semaine riche en émotions et en investigations… »

Lire l'article

Élévation de privilège avec SAML

L'équipe de recherche de Duo Security a récemment identifié une vulnérabilité affectant plusieurs applications qui reposent sur le protocole SAML (Shibboleth, OneLogin, etc.). Cette faille permet notamment de se faire passer pour un autre utilisateur avec des droits plus élevés. La description détaillée de cette brèche est disponible sur le blog de la société.

Lire l'article

Une vulnérabilité de Cisco maintenant exploitée !

Publiée par Cisco le 29 janvier dernier, la vulnérabilité CVE-2018-0101 affecte le parseur de XML de plusieurs équipements Cisco et permet d'exécuter du code arbitraire ou de faire un déni de service. En moins de 10 jours, des scripts d'exploitation commençaient à circuler sur Internet. Si ce n'est pas encore fait, patchez !

Lire l'article

Nouvelle version de Bettercap

Bettercap, le couteau suisse du bon *pentester* vient de passer en version 2.0. Pour rappel, Bettercap vous aide dans la réalisation d'attaque et la surveillance des réseaux : Man-in-the-Middle, spoofing, proxy, etc.

Lire l'article

LE CONSEIL DE ...

... José-Alexandre Mayan

Quand les entiers vous dépassent

Si vous avez déjà programmé en C, vous avez peut-être rencontré ce problème étrange où une addition ou une multiplication de deux nombres positifs donne un nombre négatif.

Ce phénomène s'appelle un « dépassement d'entier ». Il est dû au fait que les nombres entiers sont composés d'une série de 32 ou de 64 bits (0 ou 1) avec le premier bit déterminant le signe du nombre. Ceci est particulièrement gênant lorsque l'on gère des dates ou de l'argent !

En effet, pour représenter une date, les applications utilisent souvent l'intervalle de temps qui s'est écoulé depuis le 1er janvier 1970. De ce fait, en 2038, beaucoup de vieux logiciels risquent d'être affectés par le « bug de l'an 2038 ».

Pour votre prochaine opération sur des nombres entiers, posez-vous la question : « Ai-je une limite ? Que se passe-t-il si je la dépasse ? »

En savoir plus sur le bug de l'an 2038

À propos de **CGI**

CGI Business Consulting, cabinet de conseil en innovation et transformation, fait partie du Groupe CGI inc. Ses consultants associent expertises sectorielles, fonctionnelles et technologiques pour accompagner les plus grandes entreprises et organisations. Parce que chaque client est unique, CGI Business Consulting a créé des méthodes de travail spécifiques permettant à chacun de prendre part au management de sa transformation et garantissant une amélioration durable de ses performances.

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. CGI Business Consulting et son laboratoire de sécurité sont qualifiés « Prestataire d'audit de la sécurité des systèmes d'information » (PASSI) par l'ANSSI. Cette qualification atteste du haut niveau de qualité et d'expertise de nos prestations, ainsi que du traitement hautement sécurisé des informations de nos clients collectées lors des audits.

Fondée en 1976, CGI est l'une des plus importantes entreprises de services en technologie de l'information et en gestion des processus d'affaires au monde et offres de services-conseils en management ainsi que des services d'intégration de systèmes et de gestion déléguée de grande qualité.

Directeur de la publication
Rémi Kouby

Rédacteur en chef
Geoffroy Andrieu

Comité de rédaction
Geoffroy Andrieu, Kévin Bogo, Paul Coursault, Rémi Kouby, Arnaud Mangematin, Claudia Mendes, Estelle de Monchy, Jean Olive

Contact
remi.kouby@cgi.com

https://www.cgi.fr/conseil/cybersecurite