CGI | Business Consulting

vQice of CGI

LA LETTRE
CYBERSÉCURITÉ
Décembre 2018 / Janvier 2019
n°23

édito

Début octobre, lors des Assises de la sécurité de l'information, l'ANSSI a annoncé la publication de la nouvelle version de sa méthode de référence d'analyse des risques : EBIOS Risk Manager. Le maître-mot : anticiper pour ne plus subir. Des principes à contrepied de la version 2010 et une nouvelle approche. Visite guidée.

Uniquement les menaces intentionnelles ?
Première nouveauté, la méthode se focalise sur les menaces intentionnelles et ciblées. Plus précisément, elle concentre les efforts sur l'analyse des attaques ciblées, considérant les risques informatiques habituels comme traités par une approche par conformité. Il s'agit de ne plus perdre d'énergie et de temps à justifier par des risques la nécessité de la mise en place de règles d'hygiène de sécurité ou à réécrire la règlementation sous forme de mesures de sécurité.
Les conséquences sont immédiates et bienvenues : les mesures de sécurité résultats ne seront plus une redite de la PSSI ou une liste de bonnes pratiques déjà connues, mais bel et bien des objectifs de sécurité spécifiquement adaptés au système étudié et à son écosystème.

La fin de l'exhaustivité ?
Oui. La démarche proposée d'analyse des scénarios d'attaque ne recherche pas l'exhaustivité, mais l'efficacité. Dès lors que l'on sait qu'une mesure de sécurité viendra couvrir complètement plusieurs menaces, est-il bien nécessaire de lister tous les scénarios ?
Ici, **l'expertise de ceux qui contribuent à l'analyse de risque est absolument nécessaire** pour effectuer le meilleur choix des scénarios d'attaque. Il ne s'agit pas d'analyser des scénarios trop proches ou forcément les plus vraisemblables a priori, mais un panel de scénarios permettant de garantir la meilleure couverture possible. Des bases de connaissances seront d'ailleurs prochainement disponibles avec des indicateurs sur les attaques avérées.

Intégration de l'écosystème entourant le système à analyser
L'expérience montre une complexification des attaques. Les attaquants exploitent parfois des vulnérabilités annexes pour atteindre leur cible. La version RM intègre une modélisation des parties

prenantes qui interagissent avec le système : infogérants, fournisseurs, partenaires, directions supports, etc. avec pour objectif d'intégrer à la réflexion la menace que représentent ces parties prenantes et l'exposition qu'elle engendre pour la cible.

Une approche par graphe d'attaque
Vous pouvez dire adieu aux tableaux à rallonge et aux indicateurs chiffrés, réservés aux initiés. L'avenir est à la *kill chain* et à la représentation graphique des chemins d'attaque.
Une volonté forte de cette nouvelle méthode est d'impliquer davantage les métiers et interlocuteurs SI qui ne sont pas des experts de la sécurité. **Ces graphes,** au-delà d'illustrer les résultats, **facilitent la co-construction** et la prise de décision pour identifier les meilleures stratégies.

L'approfondissement successif
Alors que les précédentes méthodes demandaient de « dérouler » l'ensemble des modules pour obtenir risques et mesures, EBIOS RM a choisi une approche par approfondissement successif. À chaque fin d'étape, vous êtes en mesure de constituer des risques. Plus vous avancez dans la méthode, plus les risques seront détaillés. L'arrêt est possible à chaque étape, **ce qui permet de faciliter grandement l'adaptation du niveau de granularité des résultats.**

Ces nouveautés sont le fruit d'un long travail de recueil des retours terrain et de prise en compte des bonnes pratiques en matière d'analyse de risques et de modélisation de la menace.
Guillaume Poupard veut rendre l'analyse de risque « sexy ». Avec EBIOS RM, il a, avec certitude, gagné le pari du visuel et de l'efficacité*.

Si vous souhaitez en savoir plus sur la méthode EBIOS RM, n'hésitez pas à nous contacter directement.

Rémi Kouby
Consultant sécurité et gestion des risques
remi.kouby@cgi.com

* https://www.usinenouvelle.com/article/le-patron-de-l-anssi-veut-rendre-la-cybersecurite-plus-sexy.N737689

CYBERSÉCURITÉ SOUS-MARINE :
DES INFRASTRUCTURES VULNÉRABLES

Il semble surprenant de lier le monde des TIC à celui de l'environnement sous-marin. En effet, le fond de nos mers n'apparait pas d'emblée connecté au milieu extérieur. Mais, en réalité, le cyberespace et le milieu sous-marin présentent des similitudes.

Ces univers se ressemblent par leur nature de profonde liberté et d'interconnexion avec les populations. 95% des communications transitent par les câbles sous-marins à fibre optique. Cette colonne vertébrale du numérique qui relie des états et des continents est aujourd'hui investie par les GAFAM. Les géants du Big Data investissent le monde des abysses : propriétaires de câbles, poseurs de câbles ou… de datacenter immergé, comme le projet NATICK concrétisé en juin 2018 au large de l'Écosse par Microsoft et Naval Group. Or, les fonds marins ne sont pas du tout épargnés par les risques de cyberespionnage et cybersabotage sur les infrastructures qui y sont installées. Des dispositifs-espions de tapping peuvent être insérés dans les stations d'atterrissage des câbles. Les plateformes énergétiques offshores sont connectées à des postes de contrôle et sont exposées aux risques liés aux systèmes d'information industriels. Une fois le SCADA du système de contrôle industriel atteint, il est possible d'accéder au Programmable Logic Controller (PLC) et de prendre la main sur les contrôles automatisés. Les attaques peuvent permettre d'altérer le recueil des

données provenant des sondes, des senseurs, des capteurs posés sur les câbles et les pipelines, de pervertir les commandes d'un poste de contrôle réagissant aux données de ces capteurs, de bloquer le fonctionnement d'une sous-station électrique, ou d'une plateforme d'extraction. Les impacts peuvent être majeurs et les scénarios d'évènements redoutés protéiformes.

À côté des menaces classiques dont les SII de ces infrastructures peuvent être la cible, figurent des attaques plus spécifiques, par exemple de type « man in the middle » sur les liaisons satellitaires, ou par spoofing sur les GPS des drones de maintenance. D'autres modes opératoires inattendus émergent, avec des capacités potentielles de cybersabotage. Pour exemple : les attaques par ondes sonores permettent de rentrer dans le software en saturant le hardware par une pression acoustique. Elles peuvent permettre de prendre le contrôle d'un navire autonome ou d'un drone sous-marin en ciblant l'accéléromètre de son dispositif. Les ondes sonores peuvent circuler d'ailleurs, jusqu'à quatre fois plus vite dans l'eau que dans l'air. Le scénario d'un drone antimine équipé d'une charge explosive, dérouté et détourné sur une plateforme pétrolière devient alors vraisemblable…

Extraits d'un mémoire de recherche à l'attention de l'IRIS Sup'
Thomas Goudon, 2018

vOice of the client

La conférence Voice of Innovation du 13 novembre 2018, organisée avec Les Echos, a été une tribune pour CGI et ses clients, notamment pour échanger sur les enjeux et moyens de la cybersécurité. L'innovation se traduit par de nouvelles menaces qui - telles que les cryptominers - montent sur le podium et viennent s'ajouter aux menaces existantes (phishing, ransomware, etc.). Les intervenants ont mis en avant deux facteurs de réussite pour une cyberdéfense efficace. D'abord, une approche holistique de la cybersécurité incluant le top management permet l'appropriation, par le corps dirigeant, du risque encouru. Les directeurs sont alors plus enclins à libérer le budget nécessaire à l'effort de sécurisation. Enfin, il s'agit de remettre l'humain au cœur de la stratégie de cyberdéfense, en conduisant des campagnes de formation et de sensibilisation en continu.

Hervé Ysnel, vice-président en charge des activités cybersécurité chez CGI a participé à la table ronde sur la cybersécurité lors de l'évènement Voice of Innovation. Il répond à quelques-unes de nos questions.

Q1 : EN QUOI LA VIE PERSONNELLE DES SALARIÉS PEUT-ELLE AVOIR UN IMPACT SUR LA SÉCURITÉ DE L'ENTREPRISE ?

H.Y : Il y a une continuité entre l'activité numérique du salarié et celle de l'individu dans sa vie personnelle. Nous avons déjà rencontré le cas où un collaborateur utilisait le même mot de passe pour un site de vente de pizzas et pour le SI de l'entreprise. On crée alors une faille de sécurité de l'entreprise qui peut engendrer une perte financière.

Q2 : QUELLE EST LA PLACE QUE L'ON DONNE À LA CYBERSÉCURITÉ DANS LES ENTREPRISES EN FRANCE ?

H.Y. : Une PME sur deux admet avoir été attaquée dans l'année ! Pourquoi ? Probablement n'ont-elles pas encore vécu de crise majeure de cybersécurité. Nous constatons en France, par le **baromètre CGI**, une différence notable de maturité entre petites et grandes entreprises. Ce que nous disent nos clients, c'est que :

- Nous ne testons pas assez nos dispositifs, lorsqu'ils existent, de gestion de crise et de gestion d'incidents SI.
- La supervision de la sécurité, via les SOC, n'est pas assez déployée dans les entreprises.

Pour revoir en intégralité la table ronde, c'est par **ici**

Q3 : EST-CE QUE LA CYBERSÉCURITÉ EST VRAIMENT TRAITÉE COMME UN SUJET STRATÉGIQUE ?

H.Y. : La cybersécurité est dans le top 3 des risques majeurs d'entreprises depuis trois ans, juste après les enjeux climatiques et les effets des armes de destruction massive. Notre enquête CGI Voice of Client, menée auprès de 1400 clients à travers le monde, le place même en seconde position, derrière l'enjeu de réussir sa transformation numérique. On voit qu'il s'agit d'un sujet stratégique pour les dirigeants, le COMEX ou dans les conseils d'administration des grandes entreprises. En revanche, on remarque un retard important pour les PME.

Q4: COMMENT PROTÉGER EFFICACEMENT SES SALARIÉS ?

H.Y. : Dans un premier temps, il faut mener de grands programmes de sensibilisation et de formation. Il faut diversifier les moyens (affichage, e-learning, formation...) et s'adapter aux rôles des personnes à sensibiliser. Ensuite, il est nécessaire de vérifier l'impact de ces programmes en planifiant des campagnes de phishing, et mettre à l'épreuve son dispositif de crise cyber avec, par exemple, un scénario basé sur un ransomware. Enfin, il faut garder en tête que protéger ses salariés, c'est protéger son entreprise, mais c'est aussi indirectement les protéger dans leur vie personnelle.

RETOUR EXPRESS DES ASSISES DE LA SÉCURITÉ DE L'INFORMATION

Nouvelle méthode EBIOS RM
« Un renoncement à l'exhaustivité des risques pour cibler les chemins d'attaque les plus pertinents, une analyse en se positionnant en tant qu'attaquant et intégrer les parties prenantes externes »,
Jean Olive,
Vice-Président cybersécurité, CGI.

La réalité des exercices de crise cyber
« S'appuyer sur les bons experts et des solutions de sécurité de pointe n'est pas suffisant. La capacité des dirigeants à prendre rapidement des décisions malgré l'incertitude propre à une attaque cyber est décisive. »,
Anthony Augereau,
Directeur cybersécurité, CGI.

« S'entrainer régulièrement à rebondir et ne pas avoir peur du caractère évolutif et non prédictif des crises cyber est absolument essentiel ! »
Aurélie André,
Consultante, CGI.

REVUE DE PRESSE
PAR ICI... ÇA FUITE !

Cyberattaques et fuites de données ont été au cœur de l'actualité ces derniers mois. Voici notre sélection, de la plus spectaculaire à la plus improbable, en passant par la plus dévastatrice. Bonne lecture !

VOL DE DONNÉES MASSIF CHEZ CATHAY PACIFIC

Après un vol de données touchant près de 9,4 millions de clients, la compagnie aérienne hongkongaise Cathay Pacific a été obligée de saisir les autorités de régulation et de publier un communiqué de presse pour informer les médias et ses passagers. Ce n'est pas moins de 860 000 numéros de passeports, 245 000 de cartes d'identité hongkongaises, 403 cartes de crédit expirées et de 27 cartes sans leur code CVV à trois chiffres qui auraient été visités par les pirates. Les clients de la compagnie n'ont été prévenus que tardivement : 6 mois après la découverte de l'incident. Rappelons que le RGPD, lorsqu'il est applicable, impose la notification dans les 72 heures suivant la découverte de l'incident.

> Lire l'article

NOUVEAU COUP DUR POUR LE GÉANT GOOGLE

Le réseau social de Google, Google+, a été affecté par une nouvelle faille de sécurité. La nouvelle a été rendue publique début octobre, six mois après la découverte de la faille par le groupe. Ce n'est pas moins d'un demi-million de comptes et 438 applications qui auraient été touchées par la faille. Pour le moment, Google assure qu'il ne détient aucune preuve que les données des clients ont été utilisées à des fins inappropriées. Mais pourquoi un tel silence depuis le mois de mars ? D'après le Wall Street Journal, les dirigeants redoutaient un traitement similaire à celui de Facebook suite au scandale Cambridge Analytica. Plusieurs enquêtes par des autorités de régulation sur la protection des données sont en cours. Quelles seront les sanctions ? Le verdict n'a plus qu'à tomber !
Pour rappel, en 2012, Google avait déjà été inquiété par la FTC et avait dû lui verser 22,5 millions de dollars dans le cadre du suivi non autorisé des internautes utilisant le navigateur web Safari.

> Lire l'article

Dernière minute : une nouvelle vulnérabilité accélère encore la fermeture de Google+ > Plus de détails

MARRIOTT HÔTEL, DU JAMAIS VU !

Sans hésitation, il s'agit d'une des plus grandes fuites connues de données de tous les temps. Les informations personnelles de **près de 500 millions de clients ayant fréquenté les hôtels au cours des quatre dernières années** ont été dérobées par des cybercriminels. W Hotels, St. Regis, Sheraton, Starwood, Westin, Element, Aloft, The Luxury Collection, Le Méridien ou encore Four Points. Au total, Starwood gérait plus de 6700 établissements. Au-delà de son ampleur, cette fuite inquiète les spécialistes par la durée de quatre ans sur laquelle elle s'est étendue.
Pour les personnes qui craignent d'être concernées par cet incident de cybersécurité, **Marriott a mis en place un site web et un centre d'appel.** Des notifications ont été envoyées aux victimes potentielles par email.

> Plus de détails

QUAND LE RGPD MET À MAL GOOGLE

Ce n'est pas moins de sept associations de consommateurs qui viennent de porter plainte contre Google. « En cause : l'historique de géolocalisation des utilisateurs de services Google sur smartphone ». C'est une enquête de l'Associated Press qui avait dénoncé, le 14 août dernier, que certains services de Google enregistraient la position de l'utilisateur, même si ce dernier avait désactivé l'option. Les associations jugent que l'utilisateur n'est donc pas suffisamment averti et sensibilisé sur ce service (au regard du RGPD) et qu'il est donc abusif et trompeur. Si Google est reconnu coupable, l'entreprise peut encourir une amende allant jusqu'à 4% de son chiffre d'affaire.

> Plus de détails

LE BILAN OFFICIEL DE LA CNIL, 6 MOIS APRÈS LE LANCEMENT DU RGPD

Les chiffres parlent d'eux-mêmes, les entreprises se sont bien évidemment lancées dans la course à la conformité au RGPD. 35000 entreprises ont désigné un DPO, 1000 notifications de violations de données ont été signalées et 130 000 téléchargements de l'outil PIA ont été comptabilisés. Du côté insécable des particuliers, on remarque que la sensibilité au sujet est en nette augmentation puisque la CNIL a reçu 9700 plaintes, soit + 34% par rapport à l'année précédente. Pour continuer à accompagner les professionnels, plusieurs référentiels de certification des compétences pour le DPO, ainsi qu'une dizaine de codes de conduite sont en cours de rédaction. Ils devraient voir le jour début 2019. Un MOOC est également en cours de réalisation.

> Retrouvez le bilan complet, les chiffres, les infos ici

LA CYBERCRIMINALITÉ S'ENGOUFFRE DANS LES FAILLES DU RGPD

Europol publie une évaluation de la menace que représente la cybercriminalité organisée sur l'Internet (IOCTA) selon laquelle, notamment, les entreprises seraient plus enclines à payer une rançon aux attaquants plutôt que de voir révélée une fuite de données et donc s'exposer à une amende « plus élevée que la rançon », allant jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaire. Nous nous efforçons de toujours rappeler qu'il n'y a pas de raison valable de payer une rançon. En plus de financer la criminalité organisée, les atteintes à l'image de l'entreprise peuvent être très lourdes, si la fuite de données, et le fait que l'entreprise ait cherché à la dissimuler étaient révélés. Ce n'est définitivement pas un bon calcul de maitrise des risques que de payer une rançon.

> Ici le rapport d'Europol

L'IRAN FRAPPÉ PAR UN MALWARE PLUS VIOLENT QUE STUXNET ?

Le ver Stuxnet a trouvé plus fort que lui. « L'infrastructure iranienne et les réseaux stratégiques ont été attaqués ces derniers jours par un virus informatique similaire à Stuxnet mais plus violent, plus avancé et plus sophistiqué », annonçait le Time of Israël, début novembre. Le directeur de l'agence de défense civile iranienne a confirmé l'information, affirmant qu'une nouvelle génération de Stuxnet avait essayé de s'introduire dans leur système. Pour le moment, les impacts, s'il y en a, n'ont pas encore été dévoilés.

> Lire l'article

CLOUD ACT : L'ALLEMAGNE, SERA-T-ELLE LA PREMIÈRE VICTIME ?

Allons-nous vers une mainmise des États-Unis sur nos entreprises ? La mise en place du RGPD a-t-elle été suffisante pour faire barrage aux mastodontes économiques d'outre-Atlantique ? Avec l'adoption en catimini du Cloud Act, l'administration Trump renforce ses capacités d'extraterritorialité en imposant que les sociétés américaines, mais aussi leurs filiales à l'étranger, soient tenues de communiquer les données placées sous son contrôle « sans considération du lieu où elles se trouvent stockées », lorsqu'elles concernent un citoyen américain. Bon nombre de responsables politiques européens crient au scandale et redoutent un conflit de normes avec l'article 48 du RGPD, relatif au transfert et à la divulgation non autorisés de données. À titre d'exemple, Brainloop, société allemande qui protège les données de 70% des entreprises européennes telles que Adidas, Allianz, BMW, SUEZ, Crédit Suisse... a été l'objet, début août, d'une OPA par le groupe américain Diligent. Le danger est alors évident : Brainloop pourrait être contraint à communiquer ses données clients aux instances américaines.

> Plus de détails

LE CHIFFRE

7

C'est le nombre **quotidien** de notifications de violation de données que reçoit la CNIL.

REVUE DE PRESSE
LE COIN DES BONNES IDÉES

Parce qu'il n'y a pas eu que des attaques dans l'actualité cyber, on vous a dégoté quelques idées, astuces, conseils et informations pratiques. Mots de passe, formations des salariés, acquisition de nouvelles sociétés... Les sujets sont variés, c'est à prendre ou à laisser.

NE FAITES PLUS EXPIRER LES MOTS DE PASSE POUR RIEN !

Vos utilisateurs en ont assez de changer leurs mots de passe tous les 90 jours. Deal ! Imposez-leur uniquement si cela parait justifié.
Le changement des mots de passe a une limite : s'il ne vérifie pas la proximité entre le mot de passe précédent et le nouveau choisi, un grand nombre d'utilisateurs font le choix d'incrémenter un nombre en fin de mot de passe. La mesure devient alors inefficace face au modèle de menace qu'elle est censée contrer : la fuite du mot de passe en clair, car un attaquant pourra tester facilement un mot de passe dérivé de celui qu'il a obtenu.
Voici donc une autre approche, qui permet notamment de renforcer la complexité des mots de passe de manière globale dans l'entreprise : fixer la durée de validité du mot de passe en fonction de la complexité. Et ça marche : les utilisateurs tendent à utiliser des mots de passe de plus en plus forts pour éviter d'avoir à le changer trop souvent.

> Lire l'article

BUG BOUNTY : CE QUE VOUS DEVEZ SAVOIR AVANT DE VOUS LANCER

Le *bug bounty* est complémentaire aux tests d'intrusion et doit être effectué sur des applications ayant subi un ou plusieurs tests d'intrusion.
Par ailleurs, la difficulté la plus souvent rencontrée dans les programmes de *bug bounty* est l'incapacité des entreprises à traiter les remontées de vulnérabilités des chasseurs de *bug*.
En effet, le niveau de maturité de la gestion des vulnérabilités doit être assez élevé de manière à être en mesure de qualifier, traiter les doublons et corriger toutes les remontées qui peuvent être parfois nombreuses.
Une fois cela compris et mis en place, la mise en place d'un programme de *bug bounty*, fait-maison ou via une plateforme spécialisée, apportera des résultats maximaux.

> Lire l'article

RENFORCEZ LES COMPÉTENCES DE VOS SALARIÉS EN CYBERSÉCURITÉ

Parce qu'il n'est jamais trop tard pour se former ou renforcer ses compétences professionnelles en sécurité du numérique, l'ANSSI lance son label SecNumedu-FC (formation continue), initié à titre expérimental en début d'année 2018. Aujourd'hui, le programme recense une quinzaine de formations qui portent sur la sécurité des systèmes industriels, de l'architecture, des réseaux ou encore sur les fondamentaux de la sécurité numérique. Ces formations, dédiées aux employés comme aux demandeurs d'emploi, ont été éprouvées et sont désormais dispensées à Paris comme en régions.

> Plus d'informations

LES TRÈS CHERS CERTIFICATS EV ONT-ILS ENCORE LA MOINDRE UTILITÉ ?

Apple a tranché. Sur iOS 12, Safari n'affichera à l'utilisateur qu'une différence mineure lors de l'utilisation d'un certificat EV : le nom de domaine en vert. Exit les informations sur le nom de l'entreprise.
De manière générale, les navigateurs optent pour un affichage limité de l'utilisation d'un certificat, qu'il soit EV ou non. Par exemple, dans chrome 69, la mention «Secure» pour les certificats va disparaitre. Les certificats EV seront donc les seuls à faire apparaître une mention de sécurité, mais pour encore combien de temps ?
À partir de là, investir dans un certificat EV semble de moins en moins évident, surtout face aux contraintes qui empêchent notamment d'utiliser un seul certificat *wildcard* pour plusieurs sous-domaines.

> Lire l'article

MANAGERS : ATTENTION AUX SANCTIONS !

Que ce soit en France ou à l'international, la menace d'une attaque cyber reste la préoccupation de tous les RSSI. Malgré l'ensemble des mesures et défenses déployées dans les organisations privées et publiques, certaines attaques, de par leur vélocité et modus opérandi, ont fortement marqué les esprits et « l'histoire » de la cyberdéfense. Dans de telles situations, qui sont ceux pointés du doigt, au sein des entreprises attaquées ? Ont-ils des représailles à craindre ? Une étude de B2B International pour Kaspersky, menée auprès de plus de 5 800 entreprises, nous informe, au travers de statistiques et données, des conséquences sur les managers opérationnels et techniques, suite à une faille de la sécurité des SI. D'ailleurs, nous nous souvenons tous de l'exemple de Target, qui avait subi un

LE COIN DES BONNES IDÉES

vol de données massif en 2014 et dont le PDG avait été remercié. Désormais, la non-résilience d'une organisation pourrait constituer pour son dirigeant *« une faute de gestion engageant » sa « responsabilité si un tel manquement impactait significativement les résultats, voire la pérennité de la société ».*

> Lire l'article

ACQUISITION DE SOCIÉTÉ : ATTENTION !

Il est impossible d'envisager une acquisition d'une société sans se pencher sur la question de la cybersécurité. Qui voudrait se faire infecter par un rançongiciel sommeillant sur le SI d'une organisation fraichement acquise ou se voir dans l'obligation de payer une amende de la CNIL pour une non-conformité au RGPD ? Ainsi, la place du RSSI est d'autant plus importante dans ces phases que les conséquences peuvent être dévastatrices pour l'entité acheteuse. Un exemple très médiatisé fut par exemple l'acquisition de Yahoo par Verizon, à deux doigts d'être avortée, lors de la découverte d'une violation de données à grande échelle. Cette acquisition s'est finalement conclue avec une baisse du prix de 350 millions de dollars. Il est désormais essentiel de diligenter un audit de la société achetée avant son acquisition, afin de s'assurer de son niveau prétendu de sécurité.

assez élevé de manière à être en mesure de qualifier, traiter les doublons et corriger toutes les remontées, qui peuvent être parfois nombreuses.
Une fois cela compris et mis en place, la mise en place d'un programme de bug bounty, fait-maison ou via une plateforme spécialisée, apportera des résultats maximaux.

> Lire l'article

RGPD ET DROIT À LA PORTABILITÉ : L'EXEMPLE DU BONCOIN

Pour Damien Degremont, le DPO du Boncoin, c'est sans doute le droit à la portabilité porté par le RGPD qui a mené au plus gros chantier de mise en conformité pour l'entreprise. En effet, il a été décidé d'aller plus loin que la recommandation minimale, et d'ajouter une fonctionnalité sur le site internet pour récupérer toutes ses données. Mobilisant près de 20 personnes, dont des développeurs, ingénieurs et juristes, ce projet de grande envergure fut l'occasion d'obtenir une vue plus complète sur les données personnelles stockées dans les *datalakes* de l'organisation. Le principal levier de réussite de ce projet fut la mise en place d'un comité de pilotage hebdomadaire auquel assistait systématiquement le Directeur Général Adjoint du Boncoin.

> Lire l'article

LE CYBEROURAGAN DE L'INSTITUT MONTAIGNE

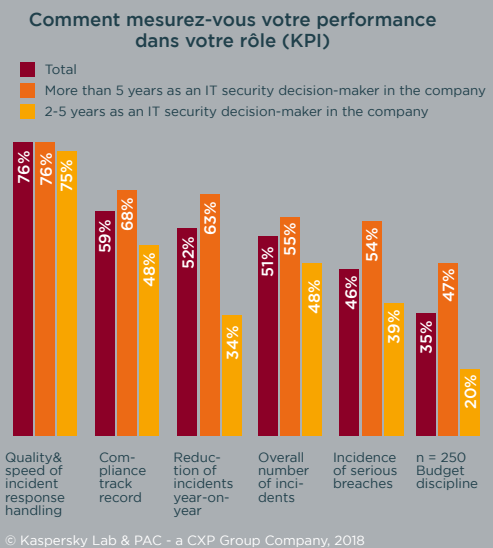
Le *think tank* vient de publier un rapport sur les dix mesures à observer pour renforcer les capacités du pays à faire face à une attaque cyber, qui prendrait la forme d'un « cyberouragan ». Le scénario est digne d'un film catastrophe. L'institut se base sur les récentes attaques de 2017 (Wannacry et NotPetya) et cible les faiblesses des infrastructures (interconnexions des systèmes IT, utilisation des technologies de l'information dans le quotidien des Français, utilisation exponentielle des objets connectés ...). Les auteurs invitent d'ailleurs les entreprises à réaliser de réels diagnostics de vulnérabilité afin de « couvrir les risques révélés ». Mais les grandes entreprises ne sont pas les seules à être ciblées par le rapport, les PME et l'État font également partie des recommandations de l'institut Montaigne.

> Lire l'article

RSSI : RÉSULTATS DES AUTOÉVALUATIONS DE VOS PERFORMANCES

Protéger l'entreprise des cybermenaces et de leur impact, réduire les vulnérabilités, résoudre les problèmes de conformité et maintenir les budgets dans le vert : voici des indicateurs de performance qui reflètent les priorités des RSSI. On remarque également que les RSSI qui sont en poste depuis 2 à 5 ans ont noté leurs performances de façon plus sévère que ceux en poste depuis plus de 5 années. (cf. indicateurs ci-contre).
En considérant la place cruciale que prend la cybersécurité dans l'entreprise, on s'attendait à ce qu'un responsable de la sécurité des systèmes d'information fasse partie des cadres dirigeants. Et pourtant, un quart seulement des RSSI interrogés font partie du COMEX. Les cas où l'on peut voir des RSSI au niveau COMEX concernent surtout les entreprises hautement numérisées, très sensibles, ou les très grosses organisations.

> Lire l'article



BIBLIOTHÈQUE

Retrouvez notre sélection de guides, ouvrages, romans... à lire attentivement ou à feuilleter. C'est vous qui choisissez !

SÉCURITÉ DES OBJETS CONNECTÉS

Le NIST a publié un framework relativement synthétique des risques et mesures de sécurité des objets connectés. C'est encore un draft mais déjà une excellente base de travail pour tout ceux qui travaillent sur la sécurité des objets connectés. Il vient compléter et intègre les résultats du document un peu plus ancien, publié par l'ENISA.

« GUIDE DE CARTOGRAPHIE DU SYSTÈME D'INFORMATION »

Le chapitre II du guide d'hygiène de l'ANSSI incite fortement à connaitre sur le bout des doigts son système d'information et à en réaliser une cartographie.
L'ANSSI vient de publier un guide de la cartographie qui permet de préciser une méthode pour le faire !

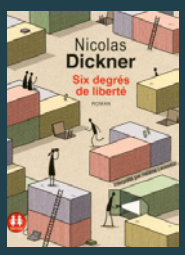
« AGILITÉ ET SÉCURITÉ NUMÉRIQUES : MÉTHODE ET OUTILS À L'USAGE DES ÉQUIPES PROJET »

L'Agence nationale pour la sécurité des systèmes d'information (ANSSI) et la Direction interministérielle des systèmes d'information et de communication de l'État (DINSIC) ont corédigé un guide explicitant comment l'agilité et la sécurité concourent au développement sécurisé des projets et à la gestion du risque numérique. Le guide rappelle les enjeux auxquels sont confrontées les équipes chargées de livrer un produit ou un service dans un temps contraint. La démarche repose sur l'organisation d'ateliers d'appréciation des risques qui préparent efficacement à l'homologation des services numériques et produits. Ce guide propose un accompagnement progressif, atelier après atelier avec des exemples concrets à l'appui, le tout enrichi de fiches méthodes.

ARRÊTÉ DU 14 SEPTEMBRE 2018

Publication au JORF du 29 septembre de l'Arrêté du 14 septembre 2018 fixant les règles de sécurité et les délais mentionnés à l'article 10 du décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique.

SIX DEGRÉS DE LIBERTÉ



Une spécialiste de la gendarmerie canadienne recherche un container qui a disparu des écrans radars. Une de ses collègues spécialiste des réseaux informatiques où elle traque les anomalies comptables va peu à peu s'intéresser à cette étrange disparition.

Ce roman a obtenu le prix du gouverneur général, soit l'équivalent du Goncourt au Canada. Il étonne d'abord par sa maitrise et par la capacité de l'auteur à tenir le lecteur en haleine. Un roman très documenté sur l'industrie des containers et sur les réseaux informatiques, qui mêle à la fois cyber polar et schémas romanesques plus classiques.

NOUS RECRUTONS !

En ce début d'année 2019, CGI Business Consulting fait face à une forte croissance de son activité.

Nous recrutons constamment des consultants sécurité.

> Envoyez votre candidature

RÉSEAUX SOCIAUX

Pour de l'information en temps réel, retrouvez-nous sur twitter

@CGIsecurite

Consulltez les précédents numéros de la lettre cybersécurité sur :

https://www.cgi.fr/view/brochure

À PROPOS DE CGI

CGI | Business Consulting

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.

vQice of innovation

transformer,
accélérer,
performer

Directeur de la publication
Rémi Kouby

Rédactrice en chef
Estelle de Monchy

Comité de rédaction
Antonin Deneux
Rémi Kouby
Arnaud Mangematin
Estelle de Monchy
Yoann Parronnaud