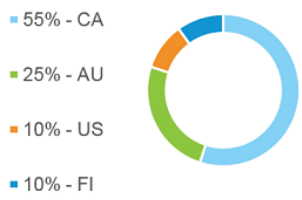
Le cheval de Troie Ramnit refait surface

Le cheval de Troie Ramnit refait surface

Ramnit refait surface moins d'un an après l'offensive d'Europol contre ses serveurs de contrôle Une première pour un botnet bancaire selon IBM



En février dernier, suite à une opération menée par plusieurs États ainsi que des acteurs privés (parmi lesquels Microsoft, Symantec et AnubisNetworks) qui a été coordonnée par le centre de lutte contre la cybercriminalité d'Europol, un réseau de serveurs de contrôle du botnet Ramnit a été démantelé. Trois cents domaines internet exploités par les pirates ont également été redirigés.
Détecté pour la première fois en 2010, le cheval de Troie Ramnit permettrait de gagner un accès distant aux ordinateurs Windows infectés et de subtiliser par la suite des données sensibles, comme des informations bancaires. Wil van Gemert, le directeur des opérations d'Europol, a salué le succès de l'opération : « cette opération réussie illustre l'importance pour les forces de l'ordre internationales de travailler de concert avec l'industrie privée afin de lutter contre la menace globale du cybercrime ».
Seulement, les chercheurs d'IBM ont mis la main sur une variante du cheval de Troie qui se base sur une infrastructure C&C différente de son prédécesseur et emploie un fichier de configuration plus court ainsi qu'un schéma d'injection web différent pour infecter les victimes. Plus de la moitié des infections a été observée au Canada. En seconde position sur la liste des pays les plus affectés viennent l'Australie qui compte à elle seule une infection sur quatre, puis les États-Unis.
Selon les chercheurs de la X-Force d'IBM, il semblerait que ce soit la première fois qu'un botnet de fraude bancaire refasse surface, ce qui a aiguisé leur curiosité puisque, jusqu'à présent, c'étaient plutôt les botnets de spams qui étaient souvent ramenés en circulation, les cybercriminels derrière les botnets de fraude bancaire préférant se contenter de l'argent déjà collecté et du fait qu'ils n'aient pas été arrêtés.
Les experts expliquent que « le cheval de Troie arborait un fichier de configuration lourd avec des déclencheurs d'URL qui lui indiquaient vers quelle banque, quelle transaction et quels sites de réseau social se tourner pour collecter des informations d'identification ». La configuration de Ramnit est orientée pour tenir les victimes éloignées d'une liste exhaustive d'outils de scans en ligne, de sites web d'antivirus, des sites d'information sur le cybercrime, mais également des blogs de sécurité. « Dans son ancienne configuration, la seule utilisation des mots « cybercriminalité » ou « police » de la part des victimes suffisait à déclencher un effet de redirection ».
Une autre trace laissée par les anciennes configurations est la liste relativement importante de sites de recrutements récoltant les informations d'identification, afin de viser ceux qui sont à la recherche d'un emploi et de les recruter. « Pour les victimes, cela pouvait être une lame à double tranchant étant donné que les opérateurs Ramnit pouvaient également obtenir toutes les informations qu'elles ont mises sur leur CV professionnel ».
La X-Force Threat Intelligence d'IBM n'a pas eu vent du fait que le code source de Ramnit ait été vendu ouvertement, partagé avec d'autres groupes de cybercriminels ou sur les forums dans le marché noir. Aussi, ils pensent qu'il y a de fortes chances qu'il s'agisse là du même groupe d'individus qui a remis cette nouvelle version en activité.

Réagissez à cet article

Source : *Ramnit refait surface moins d'un an après l'offensive d'Europol contre ses serveurs de contrôle, une première pour un botnet bancaire selon IBM*

La cybercriminalité en nette hausse en fin d’année

La cybercriminalité en nette hausse en fin d’année

« La cybercriminalité en nette hausse au cours du 3e trimestre 2015 » , titre le site www.developpez.com qui ajoute que « ces problématiques de sécurité constituent un prélude à des événements majeurs dont l’impact sera, selon Trend Micro, particulièrement fort en 2016 ».

Le site s’appuie sur une étude de Trend Micro intitulé « Hazards Ahead : Current Vulnerabilities Prelude Impending Attacks », qui revient longuement sur le bilan en forte progression des faits de délinquance informatique au 3e trimestre 2015, avant d’esquisser une perspective pour l’année 2016 qui sera aussi riche, selon l’étude, du fait notamment du développement des technologies mobiles et de l’internet des objets.
Pour un responsable de chez Trend Micro, interrogé par les auteurs de l’enquête de terrain, il est clair que « l’évolution des piratages commence à grever la rentabilité des entreprises et le quotidien de tout un chacun ».
L’intérêt de cette étude est qu’elle donne un aperçu sur les « dégâts » occasionnés par la délinquance informatique sur la vie privée de citoyens qui en sont victimes.
« Des cas de suicides ont d’ailleurs été recensés du fait des conséquences de cette attaque sur la vie privée des utilisateurs du site », relève le site qui évoque, en effet, une attaque massive, avec vol de données de quelque 30 millions d’utilisateurs contre Ashley Madison. Il s’agit, nous apprend l’encyclopédie en ligne Wikipedia d’un « site de rencontres en ligne et un réseau social canadien.
Le public visé est celui des internautes mariés, ou du moins vivant en couple, et souhaitant avoir une relation extraconjugale ».

Réagissez à cet article

Source : *« La cybercriminalité en nette hausse au cours… – Horizons*

Cyber attaque arabe contre Israël

Cyber attaque arabe contre Israël

Un groupe de hackers arabes surnommé Kadmoun a annoncé qu'il avait entamé une série d'attaque massive contre 1 600 sites israéliens en ligne. Une semaine après la liquidation du terroriste Samir Kountar à Damas, attribuée à Israël, cette attaque n'a pas encore été repérée en Israël.

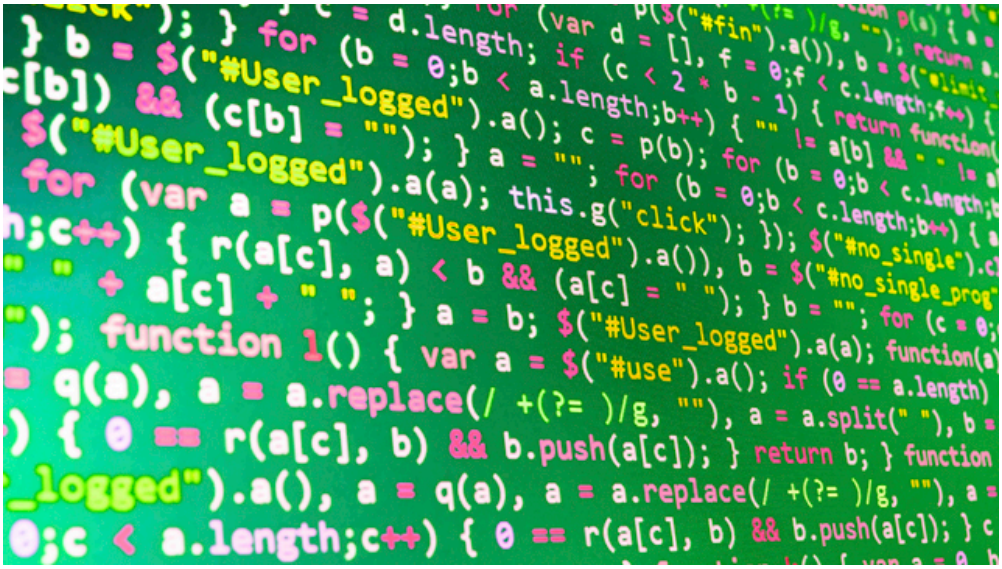
Réagissez à cet article

Source : *Cyber attaque arabe contre Israël | Coolamnews*

Code Erreur 451 en cas de site bloqué ou censuré par un organisme gouvernemental

Code Erreur 451 en cas de site bloqué ou censuré par un organisme gouvernemental

Les sites Web censurés sont désormais indiqués par un code « Error : 451 » de l'Internet Engineering Task Force.



L'Internet Engineering Task Force – IETF – vient d'officialiser un nouveau code d'erreur pour indiquer qu'un site est bloqué ou censuré par un organisme gouvernemental. Suite à ce vote, les internautes du monde entier vont désormais savoir quand un gouvernement veut leur interdire d'accéder à un site Internet. Le code en question – Error 451 (en anglais) – devient synonyme de censure sur Internet. Le code HTTP Erreur 404 est bien connu des internautes, tout comme le code Erreur 500 dans une moindre mesure – qui indique un problème de serveur. Ne doutons pas que l'**Erreur 451** va rapidement devenir l'un des codes d'erreur stars de la toile.

L'organisme de standardisation du Web a décidé d'indiquer dans un souci de transparence qu'un site Internet est interdit, bloqué ou censuré dès qu'un utilisateur tente de s'y connecter. L'IETF prévoit notamment que le gouvernement à l'origine de cette censure pourra accompagner le message d'erreur d'une explication sur les causes du blocage d'accès. L'origine du nombre « 451 » est une référence dans la plus pure tradition des geeks, puisque l'erreur 451 renvoie à l'ouvrage de science-fiction de Ray Bradbury « **Fahrenheit 451** » publié en 1953 et dont le thème central est la dénonciation de la censure et de toute forme de propagande. Le message universel de libre accès l'information sur Internet existe encore.

Réagissez à cet article

Source : *Le code Erreur 451 synonyme de censure*

Le site de la BBC victime d’une cyber-attaque

Le site de la BBC victime d’une cyber-attaque

Ce jeudi matin, tous les sites de la BBC étaient inaccessibles à cause d'une attaque par déni de service…

Une cyber-attaque de grande ampleur. Le fonctionnement du site Internet de la BBC a été perturbé jeudi matin par une attaque par déni de services, rendant la consultation des informations impossible, selon un article du groupe britannique d'audiovisuel public.

« Une attaque par déni de service »

« Tous les sites Internet de la BBC étaient inaccessibles jeudi matin en raison d'une importante cyber-attaque », a indiqué la chaîne dans un article publié dans la section technologie de son site Internet attaqué qui était consultable par intermittence dans la matinée.
« Des sources au sein de la BBC ont indiqué que les sites étaient inaccessibles à cause d'une attaque par déni de service », ajoute l'article qui précise que l'attaque a porté sur le site et des services associés comme le service iPlayer pour revoir les émissions et l'application iPlayer Radio.

La situation est revenue à la normale

« Le site de la BBC est maintenant de retour et fonctionne normalement. Nous nous excusons pour le désagrément », a indiqué peu après 12h GMT une porte-parole de la chaîne dans un communiqué.
Ce type d'attaques a pour but de rendre un service indisponible en inondant un réseau ou en perturbant les connexions à un serveur.

La BBC déjà victime d'une cyber-attaque

En juillet 2014, une précédente attaque avait paralysé le service iPlayer de la BBC pendant un week-end entier, précise le groupe britannique d'audiovisuel public.
En septembre dernier, c'était le site Internet de l'Agence britannique de lutte contre le crime (NCA) qui avait été perturbé en raison d'une attaque équivalente, dans ce qui s'apparentait à une riposte d'un groupe de pirates après une série d'arrestations.
Selon la police, quelque 30 % des entreprises britanniques ont signalé avoir subi des attaques par déni de service en 2014.

Réagissez à cet article

Source : *Le site de la BBC victime d'une cyber-attaque*

Plus de 34 000 utilisateurs de Steam concernés par le piratage de données personnelles

Plus de 34 000 utilisateurs de Steam concernés par le piratage de données personnelles

Selon Valve, l'éditeur du service cloud de jeux vidéo Steam, c'est la combinaison d'une attaque par déni de service visant le Steam Store et d'un problème de cache qui est à l'origine de l'exposition des données personnelles de 34 000 clients.
Valve s'est finalement expliqué plus en détails sur ce qui s'est passé le jour de Noël sur sa plateforme Steam. Rappelons que des utilisateurs du service de distribution de jeux vidéo ont remarqué avoir accès depuis leurs comptes à des données personnelles d'autres utilisateurs, comme leurs adresses mail, leurs historiques d'achats, ou encore leurs numéros (incomplets) de cartes de crédit.

Dans un communiqué diffusé hier, Valve explique que ce bug est le résultat de deux facteurs : une attaque par déni de service qui a touché son magasin en ligne, le Steam Store, et une erreur dans le système de cache qui fut déployé pour la contrer. "Au cours de la deuxième vague de cette attaque, la seconde configuration de cache déployée a mal géré le trafic web en cache pour les utilisateurs authentifiés. Cette erreur de configuration s'est traduite pour certains utilisateurs capables de voir des réponses du Steam Store qui étaient générées pour d'autres usagers."

Valve a indiqué que les données personnelles de 34 000 clients ont ainsi été exposées. L'entreprise dit travailler avec son partenaire gérant la mise en cache afin d'identifier chaque client affecté pour pouvoir le contacter directement. (Eureka Presse)

Réagissez à cet article

Source : *Steam : plus de 30 000 utilisateurs concernés par le*

piratage de données

---

50 attaques informatiques qui ont marqué le web Français en 2015

50 attaques informatiques qui ont marqué le web Français en 2015

Pendant qu'il est possible de lire un peu partout sur le web le « top 5 », le « top 7 » des attaques informatiques dans le monde, ZATAZ préfère regarder du côté de VOS ordinateurs avec le top 50 des attaques informatiques qui ont touché la France et les internautes francophones. Des cas traités par ZATAZ.

Madison, Hacking Team, Hôtels Trump, Madisson, Vtech… les cas de piratage et de fuites de par le monde ont été pléthoriques, encore une fois, cette année. Revenir sur ces cas, pourquoi pas, mais il suffit d'en parler aux internautes francophones croisés sur la toile pour se rendre compte qu'ils ne se sentent pas concernés, et considères ces actes comme « drôles », ou « insignifiants » pour leur vie 2.0. Bilan, sur 1 475 personnes interrogées par ZATAZ (Âgés de 18 à 55 ans – entre le 22 décembre et le 30 décembre – 71% d'hommes – 43% évoluant dans le monde de l'informatique) seules 96 personnes interrogées avaient pris soins de modifier leurs mots de passe, car utilisés plusieurs fois dans des comptes différents (webmails, forums, …). 27 des interviewés confirmaient qu'ils regardaient plus souvent leur compte en banque. 339 avaient décidé, cette année, de faire un backup mensuel de leurs données (Je vous conseille fortement de pratiquer une sauvegarde, chaque jour, ndr).

Opération Anti Charlie

Janvier 2015, les attentats contre la rédaction de Charlie Hebdo et une supérette parisienne met en émoi le monde et le web. Les Anonymous décident de s'attaquer aux sites de djihadistes. Les participants s'attaquent à tout et n'importe quoi, dont des commerces de produits Hallal. En réponse, de jeunes internautes musulmans et plus d'une centaine de pirates du Maghreb et d'Asie lancent l'Opération Anti Charlie. Plus de 20 000 sites en .fr sont modifiés et/ou infiltrés. A noter que certains sites piratés, mais aussi infiltrés sans que la moindre trace du piratage n'apparaisse publiquement, ne sont toujours corrigés 11 mois plus tard. Une attaque informatique qui, sous l'excuse d'une cyber manifestation, était surtout menée et manipulée par des commerçants officiant dans le blackmarket. Dans la liste des espaces touchés : plusieurs centaines de sites du CNRS et des Restaurants du cœur, ainsi que 167 établissements scolaires d'Aquitaine ou encore de vieux espaces du Ministère de l'Intérieur et de la Défense.

TV5 Monde

Avril, le piratage de TV5 Monde fait grand bruit dans un contexte politique tendu. Au début du mois d'avril, la chaîne fait face à une cyberattaque d'ampleur. Ses différents comptes de réseaux sociaux sont piratés et diffusent de la propagande de la secte de Daesh. La diffusion des émissions de la chaîne sont coupées de l'antenne par la direction. Trend Micro évoque l'implication possible d'un groupe d'APT d'origine russe, Pawn Storm. Les autorités restent discrètes sur les différents éléments de l'affaire, si bien qu'encore aujourd'hui, on peine à se faire une idée de ce qu'il s'est vraiment passé dans le SI de France TV5 Monde. C'est surtout l'impact médiatique de cette attaque que l'on retiendra. Cinq mois après l'attaque, ZATAZ alertera l'ANSSI et TV5 Monde pour corriger d'autres failles informatiques découvertes sur les serveurs de la chaîne. A noter qu'un internaute est arrêté au mois d'août en Bulgarie. Des documents retrouvés dans son ordinateur son signé CyberCaliphate, le pseudonyme utilisé lors de l'attaque de TV5 Monde.
Un piratage qui fait ressortir que les media Français sont totalement dépassés par les potentialités malveillantes qui planent au-dessus de leurs claviers. Pour preuves, les différentes fuites de données et autres failles remontées par ZATAZ auprès de France Télévision [Fuite de données de téléspectateurs] ; du journal telecablesat.fr et 13 833 comptes clients volés.

Infiltrations

Les banques, les grands groupes Français sont visés, chaque jour, par des tentatives de piratage. Des attaques réussies ou non. Les clients ne sont jamais informés. Pendant ce temps, des millions d'informations appartenant aux Français sont pillés, copiés, revendues sur la toile. Par exemples, avec trois espaces de filiales de la BNP Paribas. Des sites retrouvés dans un espace pirate. Les malveillants s'échangeant les failles donnant accès à des bases de données. ; le pétrolier Total, et sa boutique, attaquée et pillée en janvier 2015. 29.657 clients d'un espace commercial grand public du pétrolier. Les pirates m'avouaient avoir vendu pour 500€ des informations de Français collectés dans cette BDD. Des fuites de données accessibles directement, ou via des tiers commerciaux, comme ce fût le cas pour TF1 et 1,9 millions de clients Français, abonnés à des journaux papiers ; Le site Internet La Boutique Officielle, spécialisé dans la vente de vêtements « Urban », visité par des pirates informatiques. Données des clients volées. L'entreprise ferme son espace numérique plusieurs jours ; de son côté, la CNIL contrôle 13 sites de rencontres français, 8 sont mis en demeure de mieux contrôler les informations de leurs « clients » ; En Mars, une faille informatique permettait à un pirate informatique de mettre la main sur les données d'un espace Orange Business.
Juin 2015, le portail Associations Sportives, qui répertorie plus de 240.000 clubs et associations françaises est infiltré. Le pirate diffuse un extrait de la base de données. Même sanction pour l'enseigne King jouet qui corrigera une fuite de données visant ses clients. Quinze ans de factures disponibles sur le web d'un simple clic de souris ; Un pirate informatique annonçait, en septembre, le vol des données appartenant au laboratoire Santé Beauté. Le groupe Santé Beauté regroupe des marques telles que « Barbara Gould », « Linéance », « Email diamant », « Batiste », « Nair », « Poupina » et « Femfresh ».
En octobre, le piratage de plusieurs espaces de la marque de lingerie ETAM était annoncé. Le jeune pirate diffusait plusieurs captures écrans qui ne laissent rien présager de bon pour la marque de textile.

Ransomwares

La grande mode des logiciels dédiés au chantage 2.0 (blocage de disque dur, chiffrement de données, NDR) aura frappé très fort en cette année 2015. ZATAZ a reçu pas moins de 3.022 mails de personnes et de PME piégés par ce genre d'attaque informatique. J'ai pu référencer plusieurs dizaines de mairies ou entités publiques malmenées par un ransomware, comme GDF Suez.

Arnaques et autres fraudes

Des arnaques au ransomware qui oblige les « pirates » à payer pour récupérer leurs informations prises en otage. Des arnaques qui existent aussi sous d'autres formes, comme la fraude au président. KPMG, Michelin, le Printemps, LVMH, Vinci, Total, Brevini, Areva, le cabinet d'avocats Baker & McKenzie, Finder France, SAM, Abuba, Vallourec, Sonia Ryckiel, Dargaud, Seretram… quelques exemples d'entreprises qui ont versé de l'argent à des professionnels du social engineering. Des pirates qui avaient collecté un grand nombre d'informations sur l'entreprise. Des données qui vont permettre de convaincre les services comptables de verser des millions d'euros aux pirates. Ces derniers se faisant passer pour le patron, un client, un fournisseur. Les premières arrestations ont eu lieu en février 2015. Elles concernaient les pirates ayant jeté leurs dévolus sur le club de football de l'Olympique de Marseille (OM). Deux hommes (50 et 34 ans) seront été arrêtés à Tel-Aviv.
Autre chantage, autre arnaque, celle mise en place par Rex Mundi. Plus de 15 000 identités de patients d'un laboratoire de santé français diffusées par le pirate. Le maître chanteur réclamait 20.000€ contre son silence. Le laboratoire n'a pas payé. Les informations sensibles et privées des patients seront diffusées.
Des pirates informatiques qui se spécialisent, même dans les prénoms à l'image de cet arnaqueur qui ne visait que les « Jacquelines« . Un prénom que l'escroc considère comme étant celui de personnes âgées.
Le chômage et la « crise » économique profitent aux pirates. Comme avec le site Internet Crédit Financement Fiable qui cachait une escroquerie numérique ; ou encore avec plusieurs cas d'arnaques téléphoniques. Le pirate se faisant passer pour la FNAC, Conforama ou encore Darty ; Les hôteliers, les chambres d'hôtes ne sont malheureusement pas oubliés avec une vague massive de fausses réservations de séjours.

Universités et écoles

Piratage, spams massifs, infiltration par des pirates présumés Chinois et maintenant, la diffusion d'une base de données d'élèves. L'informatique de l'université de Lyon 3 était-elle devenue complétement folle en février 2015 ? Quelques mois plus tard, rebelote, avec de nouvelles fuites de données. D'autres grandes écoles seront visées par des fuites, comme l'extranet du groupe éducatif ESG fermé à la suite d'un piratage informatique ; ou encore le cas de milliers de documents privés, et pour certains sensibles, d'étudiants de l'EPITECH. Plus de 47 000 dossiers pour quatre ans de fuite.

Fuite de données d'adresses postales

En Mars 2015, via le site Internet Degrouptest, il était possible de trouver l'adresse postale collée à un numéro de téléphone. Même une ligne téléphonique sur liste rouge pouvait être démasquée ; Neuf mois plus tard, le même type de fuite touchait un site Bouygues Telecom. Ici aussi, il suffisait de rentrer un numéro de téléphone pour accéder aux adresses postales. Liste rouge comprise.
Des fuites de données que connaitra aussi la société Somfy (spécialiste de la domotique). Zataz.com a pu constater que l'un de ses espaces web, il était dédié au personnel de l'entreprise, avait été infiltré par de nombreux pirates informatiques. Des pirates qui s'étaient empressés d'installer des backdoors, des portes cachées, leur permettant de jouer, à loisir, avec le serveur et son contenu.
Fuite de données sous forme de CV aussi, comme ce fût le cas pour un site d'Ametix. Des milliers de CV sauvegardés directement dans un dossier du WordPress d'un site dédié à une opération marketing.

Viagra et baskets dans votre site web

Le Black Seo, l'utilisation malveillante du référencement de liens et pages pirates via un site légitime, aura permis à des escrocs d'installer de fausses pharmacies et autres boutiques de contrefaçons dans des centaines de sites Français. Des Mairies, des boutiques, des sites étatiques ; Sans parler des sites propres sur eux, capable d'attirer dans leurs filets des milliers de Français, comme la fausse boutique officielle Nike RBFIRM.
En juin, le site Internet officiel de la chambre des Huissiers de Justice de Paris est (le site diffuse toujours des liens malveillants, ndr) piraté et exploité par des vendeurs de viagra ; des attaques que zataz révélera aussi en août 2015 à l'encontre du site de la Haute Autorité de la Santé ; ou encore en septembre pour la Fédération nationale des associations d'accueil et de réinsertion sociale, pour le portail dédié à une étude médicale en France et l'Établissement de Préparation et de Réponse aux Urgences Sanitaires (APRUS).

DDoS

Bloquer un site Internet, un serveur, un streamer (joueur en ligne) … la grande mode des petits pirates, en 2015. Des attaques qui ont eu pour mission de bloquer un site, d'empêcher son bon fonctionnement. Cette année, le groupe de presse belge Rossel (Le soir, La Voix du Nord, …), mais aussi NRJ, BFM, l'Académie de Grenoble ou encore l'UMP ont été attaqués de la sorte.
Des attaques faciles à mettre en place pour le premier idiot qui passe. Les boutiques vendant du DDoS poussent comme les champignons à l'automne. A noter que durant ce mois de décembre 2015, de très nombreux amateurs de jeux en ligne, des streamers, se sont retrouvés menacer par un maître chanteur demandant de l'argent pour stopper ses blocages.

Cartes Bancaires

La fraude à la carte bancaire se porte bien ! La police de Toulouse, et plus précisément la SRPJ, a mis la main sur trois cinéphiles pas comme les autres au mois d'avril 2015. Les individus avaient piégé un distributeur de billets installé dans le cinéma Gaumont Wilson ; En Juin, la banque postale déposé plainte après que des distributeurs de billets soient piégés par des skimmeur, du matériel pirate capable d'intercepter les données inscrites sur une carte bancaires ; Des cartes bancaires qui sont devenues causantes, en mode sans fil. Bilan, même le CNRS a tiré la sonnette d'alerte en indiquant que les cartes de paiement sans contact comportent de graves lacunes de sécurité ; du sans fil qui attire, en novembre, les Frotteurs 2.0 dans le bus, le métro et autres lieux publiques ; du matériel pirate que l'on a retrouvé, entre autre, au mois d'août 2015, dans un parking proche de la gare Montparnasse (Paris). Et les arrestations se succèdent, comme à Tours, et de la prison ferme (7 mois) pour l'un de ces pirates.

Objets connectés

En Mai, je vous expliquais que pour moins de 40 euros, des voleurs de voiture s'invitaient dans les véhicules que les propriétaires pensaient avoir fermé. Même le Ministère de l'Intérieur Français s'en inquiètera quelques jours plus tard ; des panneaux d'affichage seront attaqués, modifiés (Lille, Paris…). De la geek security attitude qui démontre aussi et surtout la faiblesse des villes connectées. La partie immergée d'un problème qui pourrait être bien plus dramatique.

Swatting

Le swatting, une mode venue des Etats-Unis. L'idée du pirate, envoyer les forces de l'ordre au domicile d'un joueur en ligne. En juillet, un second cas de swatting touchait la France. Domingo est un jeune Youtuber/Streamer. Un de ces jeunes professionnels du jeu en ligne qui diffuse ses parties, en direct. Il s'est retrouvé nez-à-nez avec la police après ce genre de mauvaise blague ; Le premier cas, en février 2015, BibixHD. L'action de la police, à son domicile, sera diffusé en directe alors qu'il était en train de jouer au jeu DayZ. Un inquiétant jeu qui amuse des adolescents en mal de repères. Certains vendant des possibilités de swatting pour quelques euros comme je le révélais au moins d'août !

Phreaking

Le piratage téléphonique, le phreaking, un acte numérique qui ne connait pas la crise. Mission du pirate, mettre la main sur une ligne téléphonique qu'il pourra commercialiser, surtout les minutes disponibles d'appels. Par exemples, en juillet, 5.288€ de détournement téléphonique pour la Maison de la Jeunesse de Nancy. En novembre, 43 000€ d'appels téléphoniques détournés pour le département des Deux-Sèvres.

Heartbleed

En juillet, la faille Heartbleed refaisait surface dans mes recherches. Une vulnérabilité datant d'avril 2014. Plusieurs centaines d'importants serveurs Français étaient toujours faillibles, 16 mois plus tard.

Scientologie

Des Anonymous se sont attaqués à plusieurs sites Français de la secte de la scientologie. Les manifestants 2.0 ont voulu rappeler l'affaire de Gloria Lopez, une ancienne scientologue retrouvée morte en 2006.

Box

Cette année, nous aurons connu chez ZATAZ cinq cas, dont deux considérés comme sérieux. Numéricâble, et Bouygues. Ce dernier avait son option Playin'TV particulièrement sensible. Plusieurs problèmes qui auraient pu servir à des actions malveillantes.

Réagissez à cet article

Source : *ZATAZ Magazine » Les 50 attaques informatiques qui ont marqué le web Français en 2015*

Impact sur les entreprises du règlement général sur la protection des données

Impact sur les entreprises du règlement général sur la protection des données

---

Dans un autre article, j'ai insisté sur le fait que l'impact du Règlement général sur la protection des données était lourdement sous-estimé. Dans cet article, j'explique pourquoi la conformité est essentielle, et je passe en revue les étapes à suivre pour s'assurer de la conformité au Règlement. Il ne s'agit pas d'une liste de tâches à accomplir, mais d'un virage fondamental dans la mise en place de la conformité.

Pour commencer, il existe de nombreuses définitions de la conformité, mais deux principes clés se dégagent :

Le permis d'exploitation : si votre organisation est une banque, un hôpital ou un service public en particulier, sa mission est de se conformer au respect de la vie privée, surtout si elle manipule des données sensibles sur les citoyens. Ce genre d'organisations est toujours exposé à des lois. Il est donc important d'intégrer les processus sans délai, au quotidien ; il ne peut pas s'agir d'un exercice qu'on effectue une fois par an.

Le comportement et la culture de l'organisation : la conformité doit faire partie de l'ADN de toute l'entreprise, et être le catalyseur d'un changement du comportement des employés, même si les initiatives liées à la conformité émanent du Comité de Direction. Si la Direction est la seule à imposer les changements, les appels à la conformité porteront leurs fruits trois ou quatre fois, mais le processus peut se déliter à la cinquième fois.

Étant donné le caractère vital de la conformité, il est important de ne pas prendre en compte les seuls processus technologiques, mais aussi leur intégration aux processus business et à la mise à disposition d'informations. Voici quelques conseils de base pour aider les organisations à appliquer le futur Règlement général sur la protection des données.

Comprendre la gouvernance des données.

Avant de s'engager dans un projet de conformité, il est important d'avoir des données de qualité, de comprendre leur origine, le système ou l'application où elles sont stockées, et si les informations sont exactes et complètes. Si des tiers sont impliqués, assurez-vous de l'existence d'accords contractuels relatifs à la conservation et à la propriété de ces données.

Faire une analyse des écarts. Les organisations ont généralement déjà mis en place des contrôles concernant la vie privée. Cependant, lorsqu'un nouvel élément législatif tel que le règlement général sur la protection des données entre en vigueur, il est important de déterminer quels contrôles seront suffisants pour appliquer la législation et d'examiner quels points de contrôles doivent être étendus.

Concevoir et développer des contrôles. Après avoir identifié les faiblesses de votre processus de conformité, par exemple au niveau des ressources humaines ou des finances, il vous faudra définir et mettre en place de nouveaux contrôles pour pallier ces manques.

Installer des logiciels de chiffrement. Afin de garantir le transfert sécurisé des données individuelles, qu'elles concernent un client, un fournisseur ou un employé. Il existe toujours un risque potentiel lié à la vie privée, si ces données sont utilisées à des fins non autorisées.

Prouver la conformité et la traçabilité des informations. Il est important que toutes les données soient en place pour répondre aux questions des auditeurs. Il est envisageable d'avoir recours à un tiers pour exercer une fonction d'assurance qualité avant l'arrivée des auditeurs. Nous aidons les entreprises internationales à faire la preuve de leur conformité, informations précises et exhaustives à l'appui.

De plus en plus, le respect de la vie privée devient une préoccupation. Les organisations doivent avoir une vision complète des données en leur possession, de manière à apporter la preuve solide de leur conformité et à établir une relation de confiance avec les fournisseurs, les clients et les citoyens. Le Règlement général sur la protection des données entrera bientôt en vigueur. Il est désormais temps d'évaluer la gouvernance de vos données et les pratiques de sécurité et de confidentialité qui leur sont appliquées.

Réagissez à cet article

Source : *Appliquer le Règlement général sur la protection des données – Abbas Shahim, Atos Consulting*

Infractions aux données personnelles : les associations pourraient se porter partie civile –

Politique — Numerama

	Infractions aux données personnelles : les associations pourraient se porter partie civile — Politique — Numerama

Les députés ont ajouté dans le projet de loi Lemaire la possibilité pour certaines associations de se porter partie civile lorsque le parquet poursuit des infractions pénales liées à la protection des données personnelles.

Le gouvernement estimant urgent d'attendre l'adoption du règlement européen sur les données personnelles, qui ne laissera selon Axelle Lemaire « *aucune marge de manœuvre* » aux États, les députés ont rejeté jeudi un amendement qui aurait permis de muscler très sensiblement les sanctions que peut prononcer la CNIL lors d'infractions à la législation sur la protection des données personnelles. Il aurait mis fin à ces situations ridicules qui font que Google, pris la main dans une confiture très grasse, ne se voit infliger qu'une amende équivalente à 2 minutes de chiffre d'affaires.
Mais en attendant, les députés ont tout de même fait ajouter au projet de loi d'Axelle Lemaire une disposition qui autoriserait les associations à se porter civile, et donc à réclamer des dommages et intérêts, lorsque des individus ou des entreprises commettent des infractions pénales liées aux données personnelles.

Des dommages et intérêts

Le texte dispose en effet que « *toute association régulièrement déclarée depuis au moins deux ans à la date des faits, se proposant, par ses statuts, de protéger les données personnelles ou la vie privée peut exercer les droits reconnus à la partie civile en ce qui concerne les infractions prévues aux articles 226-16 à 226-24 du code pénal* », réunies sous le titre des « *atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques* ».
Parmi ces dernières figure notamment l'irrespect des préconisations légales imposées par la loi CNIL, le défaut de sécurisation dans les traitements de données personnelles, la conservation hors délai des données, la constitution sans autorisation de certains fichiers de données sensibles, ou encore l'obtention de données par fraude.
L'amendement adopté précise que « *quand l'infraction aura été commise envers des personnes considérées individuellement, l'association ne sera recevable dans son action que si elle justifie avoir reçu l'accord de ces personnes* »… Lire la suite

---

Réagissez à cet article

Source : *Infractions aux données personnelles : les associations pourraient se porter partie civile – Politique – Numerama*

Auteur : Guillaume Champeau

Propriété des données personnelles dans la loi Lemaire

	Propriété des données personnelles dans la loi Lemaire

L'article 26 de la loi Lemaire inscrit le droit à la libre disposition de ses données personnelles dans la loi du 6 janvier 1978 dite « informatique et libertés ». Bien que s'en défendant explicitement dans son exposé des motifs, la loi pour une République numérique introduit en droit français la propriété des données personnelles. Pour le meilleur et, surtout, pour le pire.

L'article 26 de la loi pour une République numérique consacre la libre disposition des données personnelles, ce qui recouvre « le droit à la libre disposition de ses données, c'est-à-dire le droit de l'individu de décider de contrôler l'usage qui est fait de ses données à caractère personnel ». Cela revient ni plus ni moins qu'à reconnaître un droit de propriété sur ses données personnelles. Pourquoi ? Parce que vient d'être consacré le dernier des trois éléments du droit de propriété sur les données personnelles, qui ne l'était pas encore.

En effet, l'article 544 du Code civil définit la propriété comme « le droit de jouir et de disposer des choses de la manière la plus absolue, pourvu qu'on n'en fasse pas un usage prohibé par les lois ou par les règlements ». Les juristes ont, de longue date, distingué trois composantes de ce droit de propriété : l'usus – la faculté d'usage –, le fructus – le droit de percevoir les fruits de sa propriété – et l'abusus – le droit de disposer, incluant celui de mettre fin à sa propriété. À titre d'exemple, le propriétaire d'un appartement peut donc l'utiliser pour soit en l'habitant (usus), en tirer les revenus qu'il peut engendrer de par sa mise en location (fructus) ou tout simplement le vendre (abusus).
Et les données personnelles ? Avant l'article 26 précité, chaque personne en était simplement usufruitière. La loi ne lui reconnaissait tacitement que l'usus et le fructus, proscrivant tout aussi tacitement l'abusus. Une personne pouvait ainsi utiliser ses données personnelles (par exemple fournir ses coordonnées pour la réalisation d'un contrat et/ou d'une prestation de service) et en retirer les fruits (obtenir un compte mail en apparence gratuit en échange de la « location » de ses données personnelles). Elle ne pouvait toutefois pas s'en séparer, par exemple en les vendant.
La raison d'une telle limitation réside dans l'existence d'un principe structurant au sein de la loi dite « informatique et libertés » : celui de finalité. Il subordonne l'emploi de tout usage non strictement intime de données personnelles à l'existence d'une finalité considérée comme légitime par le législateur. À défaut de quoi, le traitement est illicite. C'est ce qui lui permet d'assurer les équilibres voulus par le législateur, à savoir concilier l'usage le plus étendu possible de l'informatique avec la protection de valeurs nécessaires à la vie en société.

Au premier rang desquels les droits et libertés fondamentales de la personne humaine, y incluant la protection de sa liberté et de sa vie privée. Sans leur respect effectif, nous ne sommes plus dans une démocratie libérale – qui implique une liberté effective de choisir ses gouvernants, donc l'existence d'une sphère privée pour nourrir et étayer cette liberté –, mais dans un régime à la 1984 de George Orwell. La question de la protection des données personnelles, à rebours d'une conception traditionnellement individualiste, est donc éminemment politique.
Il est donc formellement vrai que la loi Lemaire ne consacre pas le droit de propriété sur ses données personnelles étant donné qu'il existait avant cela une patrimonialité limitée à l'usus et au fructus. L'article 26 de cette loi se contente, de manière en apparence anodine, de consacrer sur les données personnelles le seul élément du droit de propriété qui ne leur était pas encore reconnu : l'abusus. Or, la libre disposition des données personnelles entre en contradiction avec le principe de finalité. En effet, disposer de ses données signifie pouvoir en perdre de vue l'utilisation, qui peut alors être réalisée pour une finalité ultérieure non déterminable au moment du transfert.
C'est là qu'est le cadeau empoisonné : le pouvoir de contrôle défini par l'article 26 de cette loi n'est qu'une faculté reconnue à la personne fichée, faculté qui vient se substituer au contrôle obligatoire de la CNIL. Or, il existe un décalage considérable entre l'innocuité apparente d'un transfert de données personnelles et la technicité extrême de l'encadrement de cette question par le droit. Pour donner un ordre d'idée, le dernier projet de règlement européen en la matière, qui devrait être adopté au printemps 2016, fait dans sa dernière version 209 pages. Est-il réaliste de croire que chaque personne fichée maîtrise sur le bout des doigts chacune de ces pages ?
Remplacer le contrôle obligatoire de la CNIL par le contrôle facultatif de tout un chacun, non spécialiste du droit des données personnelles, apparaît donc comme séduisant de prime abord. Mais cela n'aboutit qu'à donner à toute personne fichée les clefs d'une servitude accrue, en lui permettant d'entériner, par son consentement, le contournement des équilibres autrefois obligatoires de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. La libre disposition des données personnelles rend possible la propriété des données personnelles et ouvre la voie à une servitude accrue de la personne fichée. Merci Mme Lemaire.

Réagissez à cet article

Source : *La propriété des données personnelles : ce cadeau empoisonné de la loi Lemaire, Le Cercle*