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*

Les plus gros piratages de 2015 | Techniques de l'ingénieur

Les plus gros piratages de 2015 | Techniques de l'ingénieur

Année après année, c'est la même constat : quels que soient leur taille et leur secteur d'activité, les entreprises ne protègent pas assez efficacement leurs réseaux et les données personnelles ou sensibles qu'elles hébergent. Dans la majorité des cas, les attaques informatiques ont été facilitées par le non-respect de règles essentielles : mises à jour des logiciels, mots de passe faible, données sensibles pas chiffrées…

Janvier : 20 000 sites français piratés
Des mairies, des universités, des conseils généraux, des églises ou des PME… Après l'attentat contre Charlie Hebdo, de nombreux sites ont été victimes de pirates se réclamant du groupe État islamique. Dans la majorité des cas, ce piratage s'est limité à du « défacement » (modification de la page d'accueil notamment en remplaçant du texte par des revendications et/ou des images). Ce nombre élevé peut surprendre. En réalité, très peu de sites appliquent des règles élémentaires de sécurité.

Février, le « casse » du siècle
Selon l'éditeur russe d'antivirus Kaspersky, une centaine d'établissements bancaires d'une trentaine de pays auraient perdu entre 260 à 800 millions d'euros. Cette attaque massive aurait été organisée par des équipes russes et ukrainiennes.

Avril : mauvais vol chez Ryanair
Environ 4,5 millions d'euros ont été dérobés d'un des comptes de la compagnie aérienne à bas coûts Ryanair. Selon la société irlandaise, des pirates informatiques se seraient emparés de la somme par « un transfert

Juillet : des états civils plus privés
Des informations confidentielles sur la vie et l'état civil de près de 7% des américains ont été volées dans les serveurs de l'Office of Personnel Management, une agence du gouvernement fédéral des États-Unis qui gère notamment les demandes d'emploi dans la fonction publique. 22, 5 millions de personnes sont concernées par ce vol de données personnelles. Ce n'est pas la première fois que des administrations américaines sont victimes d'intrusion.

Juillet : des hackers au volant
Ne plus se plus se véhicules seront connectés d'ici quelques années. Les constructeurs devront renforcer la sécurité de leurs modèles sous peine de sortie de route ! Dans le Missouri, deux hackers ont en effet démontré qu'il était possible de prendre le contrôle à distance d'une Jeep Cherokee commercialisée par le groupe Fiat Chrysler. Situés à une quinzaine de kilomètres du véhicule, Charlie Miller et Chris Valasek (deux experts en sécurité, le premier étant connu notamment pour avoir révélé plusieurs failles dans l'iOS d'Apple) ont coupé le moteur pendant que la voiture roulait sur une autoroute. Ils ont également pris le contrôle des freins et du volant.

Août : des rencontres adultères… publiques
37 millions de comptes utilisateurs (dont des Français avec des adresses du ministère de l'Intérieur, de la Culture ou de plusieurs mairies) d'Ashley Madison ont été récupérés par un pirate. La base de données de cet important site de rencontres adultères comprend des informations très sensibles, comme les préférences sexuelles ou le numéro de téléphone. Pire, aux États-Unis, plus de 15 000 adresses email utilisées pour la création du compte provenaient de l'administration américaine ou de l'armée. De quoi lancer des opérations d'usurpation d'identité ou du chantage. Des sanctions disciplinaires et des peines de prison sont annoncées. Les conséquences sont parfois dramatiques. La police canadienne enquête sur deux suicides potentiellement liés au piratage de ce site géré par Avid Life Media, une société canadienne de Toronto.

Novembre : jouets en panne
Le fabricant de jouets Vtech a été victime du piratage d'une de ses bases de données. Des clients français, canadiens, ainsi que des ressortissants d'autres pays étaient enregistrés dans ce fichier d'environ 6 millions de données. Un internaute britannique de 21 ans a été arrêté le 17 décembre. Il ne serait pas le seul pirate à avoir pénétré ce serveur…

Réagissez à cet article

Source : *Les plus gros piratages de 2015 | Techniques de l'ingénieur*

Retard pour la plateforme nationale des interceptions judiciaires

Retard pour la plateforme nationale des interceptions judiciaires

plateforme nationale des interceptions judiciaires (PNIJ) a du plomb dans l'aile. Pour remédier au retard de son déploiement, le gouvernement a décidé de reporter l'abrogation du STIJ, le système de transmission des informations judiciaires qu'elle doit remplacer.

Créé par un décret du 30 juillet 2007, le fichier STIJ permet « *aux magistrats et aux officiers de police judiciaire de disposer des données de trafic des correspondances interceptées (numéros de téléphone, date, heure et durée de l'appel, etc.) ainsi que des contenus des messages (SMS, MMS) émis ou reçus par un numéro de téléphone dont la ligne est surveillée* » , résumait la CNIL en 2014.

Ce dispositif n'était que temporaire. Il devait être remplacé par la plateforme nationale des interceptions judiciaires six mois après l'entrée en vigueur de celle-ci et au plus tard au 31 décembre 2015. La PNIJ a en effet pour mission de centraliser le recueil des données de connexion et des interceptions de correspondances décidés par un juge. Elle tranche avec les pratiques jusqu'alors en vigueur « *où les dispositifs d'interception des communications électroniques et les réquisitions de données de connexion reposaient sur un système hétérogène et décentralisé* » dixit la CNIL.

Report d'un an

Seulement, il faut croire que le passage de relais ne se passe pas aussi bien que prévu. Hier, au Journal officiel, le gouvernement a en effet décidé de reporter l'abrogation du STIJ au 31 décembre 2016. Pour comprendre pourquoi, il faut lire la délibération de la CNIL publiée à cette occasion.

Selon la Commission, la version actuelle de la PNIJ « *ne permet pas techniquement de traiter les données prévues à l'article R. 40-46-2° du Code de procédure pénale* », c'est-à-dire les données faisant l'objet d'une mesure de géolocalisation en temps réel. Autre fonctionnalité en souffrance, dont la Commission révèle l'existence : « *la fonction de reconnaissance vocale du locuteur n'est pas disponible* ». Bref, de nouveaux développements sont nécessaires pour parfaire ce chantier, des travaux qui prendront plusieurs mois.

Un passage de relais délicat

Le basculement du STIJ à la PNIJ devra aussi être l'occasion d'un gros ménage puisque la CNIL a interdit que les données de l'un soient reprises par l'autre. Il faudra donc organiser un effacement, en tenant compte des différentes durées de conservation. Un exercice rendu d'autant plus complexe par l'éparpillement des informations sur les postes de travail des enquêteurs.

Rappelons que la plateforme nationale des interceptions judiciaires, située dans les locaux du géant Thales, est placée sous le contrôle d'une personnalité qualifiée (article R40-53 du Code de procédure pénale). C'est Mireille Imbert-Quaretta, l'ancienne présidente de la commission de protection des droits à la Hadopi, qui occupe désormais ce poste pour une durée de cinq ans. Elle devra établir un rapport annuel qu'elle adressera au garde des sceaux, ministre de la justice. Sur cette question, la CNIL a déploré ne pas être destinataire de ce rapport, mais le ministère de la justice lui a promis de lui en adresser un exemplaire.

Réagissez à cet article

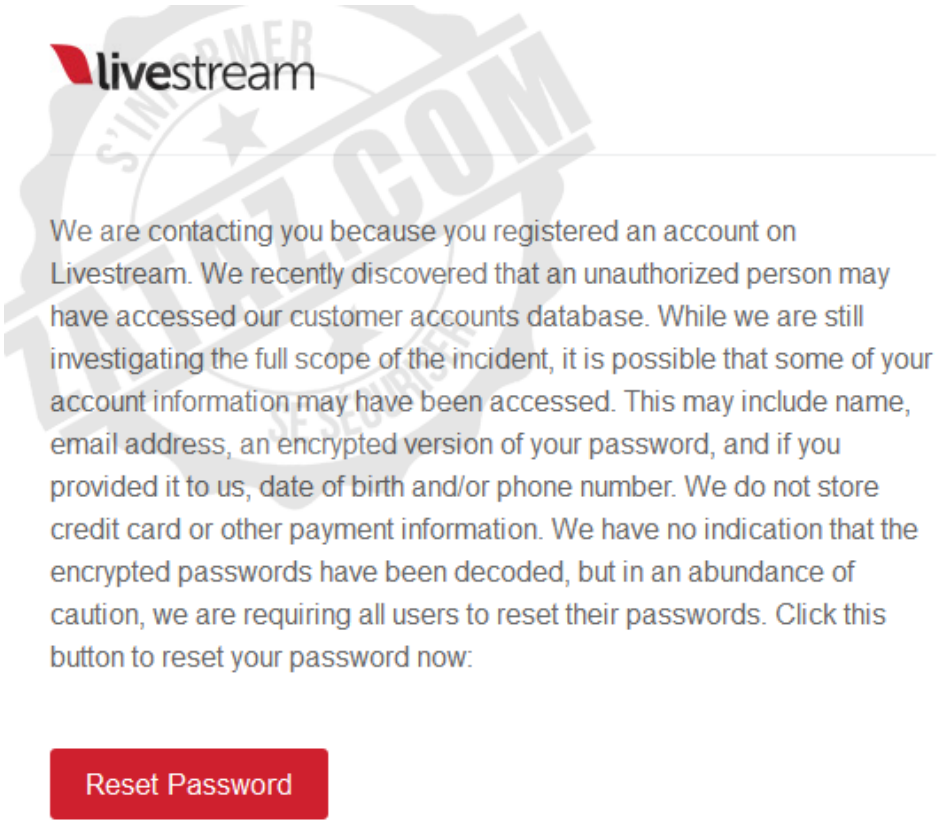
Source : *Du retard pour la plateforme nationale des interceptions judiciaires – Next INpact*

Alerte : livestream.com victime d'un vol de données

Alerte : livestream.com victime d'un vol de données

Le site Internet dédié aux concerts en live sur Internet, livestream.com, visé par un piratage informatique.

C'est via un courrier électronique laconique, envoyé après le réveillon de Noël, que le site Internet dédié aux concerts en live sur Internet, livestream.com, indique avoir été visé par un piratage informatique. « ***Nous vous contactons parce que vous avez enregistré un compte sur Livestream,*** explique la missive. ***Nous avons récemment découvert qu'une personne non autorisée a pu avoir accès à nos comptes clients.***«



Bilan, une faille qui a donné accès à la base de données et aux informations des utilisateurs. « ***Cela peut inclure le nom, l'adresse électronique, une version chiffrée de votre mot de passe.*** » Bref, toutes les informations que les clients ont pu sauvegarder. Aucunes données de carte de crédit ou autres informations de paiement ont pu être lues par le pirate, la base de données impactées ne concernées par ce secteur numérique de livestream.com. « ***Dans un souci de prudence, nous conseillons aux utilisateurs de réinitialiser leur mot de passe***« .

Réagissez à cet article

Source : *ZATAZ Magazine » Piratage de données pour livestream.com*

Et si les fuites de données sur Réseaux sociaux venaient de vos voisins ?

Et si les fuites de données sur Réseaux sociaux venaient de vos voisins ?

Selon une étude de l'université de Penn State aux Etats-Unis, les utilisateurs de réseaux sociaux se soucieraient bien moins de livrer des informations privées sur leur liste d'amis que de divulguer les leurs.

Quel internaute n'a jamais utilisé une application externe à Facebook qui demande d'accéder à sa date de naissance, à ses photographies et même aux informations personnelles de ses amis ? Les développeurs qui créent des applications tierces à lancer à partir des plateformes de réseaux sociaux demandent régulièrement l'accès à des données privées pas toujours nécessaires. En revanche, elles peuvent être revendues et cela constitue une source financière non négligeable pour ces développeurs.
Mais qu'en est-il des internautes ? A combien jugent-ils la valeur de leurs informations personnelles, et considèrent-ils la vie privée de leurs amis aussi précieuse que la leur ?

Révélée le 14 décembre dernier lors de l'International Conference on Information Systems au Texas, une étude montre que les internautes sont plus soucieux de leurs données privées que de celles de leurs amis. En effet, lorsqu'on leur demandait d'évaluer en dollars la valeur de leurs propres informations quand une application tierce en avait besoin pour pouvoir fonctionner, la moyenne était de $2.31, alors que celles de leurs amis étaient évaluées à $1.56.
Les réseaux sociaux fonctionnent le plus souvent sur le modèle de l'interconnexion des données pour créer de la valeur. La vie que l'utilisateur affiche et qu'il veut voir rester privée est donc intrinsèquement liée à la confidentialité des informations des autres. A noter qu'en avril 2015, la société Facebook, régulièrement attaquée pour sa politique d'utilisation des données d'utilisateurs, a annoncé de sérieuses restrictions quant aux informations demandées par des applications tierces.

Réagissez à cet article

Source : *Réseaux sociaux : les données du voisin valent moins | L'Atelier : Accelerating Business*

AVG dévoile ses prévisions d’attaques informatiques et technologiques pour 2016

AVG dévoile ses prévisions d’attaques informatiques et technologiques pour 2016

L'apparition de voitures autonomes n'est pas le seul élément prouvant que les systèmes logiciels « intelligents » vont améliorer notre sécurité. D'autres indicateurs sont également visibles sur Internet.
Chez AVG, il nous a fallu des années pour concevoir nos récents algorithmes de détection des brèches et de réputation des fichiers. Pour notre tout dernier moteur antivirus, nous avons utilisé des techniques sophistiquées d'apprentissage neuronal et de collecte de données dans le cloud, qui ont été conçues pour intercepter les logiciels malveillants plus en amont, et de manière plus systématique.

En 2016, de nouvelles solutions de sécurité fondées sur l'intelligence artificielle vont faire leur apparition.
On peut donc espérer que la bataille engagée contre les mauvais génies d'Internet va connaître un regain d'énergie très attendu, et que les menaces seront encore plus vite contrées et éliminées. Les progrès de l'intelligence artificielle et des systèmes d'apprentissage profond (ou « deep learning ») sont devenus bien plus accessibles. C'est ce que l'on a pu voir récemment, par exemple, lorsque Google a ouvert le code source de l'outil Tensorflow mis au point au sein de la division chargée de l'intelligence artificielle chez Google.

Autorités de certification : une disparition annoncée
La nécessité de sécuriser tout le trafic HTTPS des sites Web via un mode de chiffrement prend de l'ampleur. En 2016, avec l'apparition de nouvelles normes ouvertes et le fait que les propriétaires de sites pourront plus facilement faire des choix, il se pourrait que cette réalité devienne globale. Certaines autorités de certification, qui par comparaison commencent à paraître un peu dépassées, risquent de connaître des moments difficiles.
Ces dernières années, certains cas d'erreurs de gestion des certificats, des incidents de sécurité et des brèches de données les ont mis sur la sellette et ont fragilisé la puissance de ces géants. La confiance dans les certificats SSL a également été ébranlée, notamment par le fait que des organismes d'état pourraient infiltrer, dans certains cas, nos communications Web prétendument sûres.
Traditionnellement, le rôle d'une autorité de certification est de confirmer l'identité du propriétaire légitime d'un site Web avant d'émettre un certificat SSL signé. Cela reste une bonne idée pour les entreprises qui peuvent se le permettre, et certaines protections et indemnités d'assurance sont également prévues. En revanche, pour un blogueur ou un propriétaire de site professionnel lambda, il est à la fois laborieux et inutile de payer une autorité de certification et se soumettre à ce qui peut sembler un processus laborieux de vérification et de confirmation. Dans ce contexte, les alternatives techniques telles que Let's Encrypt (actuellement en phase bêta) devraient prospérer.
En outre, l'identification des faux certificats SSL va se poursuivre dans le cadre du programme de transparence des certificats de Google, grâce à des systèmes de détection intégrés dans les navigateurs Web modernes. Google continue à demander aux autorités de certification d'assumer leurs responsabilités, afin que nous soyons tous mieux protégés.
Enfin, avec l'annonce d'autres solutions telles que le protocole DANE proposé par Internet Society, qui offre la possibilité à n'importe quel propriétaire de site Web de valider son propre certificat SSL et donc de se passer totalement d'une autorité de certification, l'année 2016 va nous réserver des nouveautés intéressantes !

Malvertising et réseaux publicitaires : réagir ou disparaître
La publicité malveillante ou « malvertising » désigne ce qui se produit lorsque des visiteurs innocents sont la cible d'éléments malveillants, causés par des échanges avec des tiers douteux et une sécurité déficiente sur plusieurs réseaux publicitaires en ligne. En 2016, les réseaux publicitaires vont devoir réagir ou disparaître, avant qu'ils ne détruisent l'économie numérique qu'ils ont contribué à bâtir, et ne ruinent les résultats des sites Web dont la survie dépend des recettes publicitaires.
Ce problème a une cause principale : la « surface d'attaque » des scripts de publicité et de suivi toujours plus nombreux et complexes fournis par les réseaux publicitaires et intégrés par les éditeurs (souvent de façon transparente) sur leurs sites Web.
Sur mobile, plus de la moitié de la bande passante est utilisée pour la diffusion d'annonces publicitaires, beaucoup plus que pour le contenu même de la page !
S'il est associé avec des attaques réseau plus classiques, ce nouveau vecteur peut servir à infecter des milliers de victimes qui visitent des sites pourtant légitimes. Il faut aussi savoir que, même si beaucoup de grands réseaux publicitaires réagissent rapidement et arrêtent le flux de trafic lorsqu'un cas de malvertising se produit, quelques minutes suffisent pour toucher des centaines, voire des milliers de victimes. Toute personne ayant récemment installé un système de blocage publicitaire vous certifiera que ses sites Web préférés se chargent incroyablement plus vite, ce qui paradoxalement n'arrange rien.
Il faut malheureusement reconnaître qu'une grande partie des sites Web riches en contenu, pour qui les recettes publicitaires sont essentielles, se chargent lentement. En fait, une étude menée par le New York Times a montré que, pour la version mobile de nombreux sites d'actualité, plus de la moitié de la bande passante utilisée sert à la diffusion d'annonces publicitaires. Cela représente un volume de données (chargement des annonces, scripts et codes de suivi) supérieur au contenu effectivement affiché sur la page que vous lisez !
Toutefois, les systèmes de blocage de la publicité ne sont pas une solution à long terme à ce qui, finalement, est un problème de mise en œuvre. C'est encore plus vrai si vous convenez que la disparition du principe de monétisation actuellement en vigueur sur Internet pourrait avoir des conséquences économiques désastreuses. De plus, une récente déclaration de l'IAB (Interactive Advertising Bureau) confirme que les annonceurs « tiennent beaucoup moins compte de l'expérience utilisateur » dans leur manière d'élaborer des contenus.
Pour empêcher les systèmes de blocage d'annonces de se répandre, l'IAB a imaginé L.E.A.N. (de l'anglais Light, Encrypted, Ad Choice Supported and Non-Invasive), un programme basé sur des principes intervenant dans la prochaine phase des normes techniques publicitaires destinées à la chaîne d'approvisionnement publicitaire numérique globale. Quelle que soit la solution choisie, une chose est certaine : les réseaux publicitaires doivent réagir et régler les problèmes de sécurité, faute de quoi l'année 2016 pourrait bien être celle où la « vague scélérate » du malvertising aura emporté des millions d'entre nous.

Les mots de passe résistent
Les mots de passe sont un concept, pas une technologie, et la grande majorité d'entre nous va continuer à se servir de cet outil pour de nombreuses ressources, dans la vie privée comme dans la vie professionnelle. Alors certes, les mots de passe seront toujours utilisés en 2016, mais ils ne sont pas la panacée universelle, et vous avez donc intérêt à connaître certaines alternatives.
Cette année, Yahoo a annoncé le lancement d'une solution de sécurité qui utilise des périphériques mobiles plutôt qu'un mot de passe pour contrôler les accès, et nous avons même vu Google intégrer des fonctionnalités de verrouillage intelligent Smart Lock capables de déverrouiller votre smartphone en se servant des appareils présents à proximité.
Il existe des alternatives intéressantes aux mots de passe, même si ces derniers ont encore de beaux jours devant eux grâce à leur gratuité.
En matière de contrôle d'accès, la validation en deux étapes est un système efficace qui a tendance à se répandre et reste très utilisé chez de nombreux fournisseurs basés dans le cloud. Lorsqu'elle est proposée, vous avez tout intérêt à l'utiliser, surtout si vous n'êtes pas un spécialiste des mots de passe. Même s'il est interminable, le code de votre smartphone n'est pas inviolable, et le dispositif de lecture d'empreintes n'est peut-être pas si inutile.
Les mots de passe sont gratuits, et toutes les autres solutions ont généralement un coût, que ce soit sur le plan de la technologie ou de la complexité, ce qui explique que les mots de passe aient de beaux jours devant eux. Il est certain qu'en 2016, les problèmes liés aux mots de passe (réutilisation, stockage mal sécurisé, par exemple) ne risquent pas de disparaître. Espérons toutefois que nous saurons maintenir la vigilance des consommateurs et des entreprises !
L'Internet des objets : le principe de sécurité intégrée atteint le point d'ébullition Cela peut certes être amusant de posséder une de ces toutes nouvelles bouilloires WiFi, que vous pouvez allumer depuis votre smartphone, sans vous lever de votre fauteuil, mais ces objets normalement inoffensifs peuvent aussi révéler votre clé WiFi. Ceci n'est qu'un exemple de plus du problème existant au niveau de l'intégration de la sécurité.
S'ils ne sont pas protégés, chaque appareil périphérique, chaque téléviseur ou système stéréo intelligent, chaque système d'éclairage ou de sécurité domotique, et même ces nouveaux réfrigérateurs à la mode et ces voitures autonomes, bref tout ce qui est connecté à un réseau peut être la cible d'un hacker.
Les cybercriminels testent le matériel, analysent les ondes et recueillent mots de passe et autres données personnelles, quel que soit l'emplacement où ces informations sont conservées. Dans ce nouveau monde d'objets connectés, le danger augmente à mesure que la technologie vieillit.
Nous sommes nombreux à avoir paramétré nos ordinateurs et nos appareils mobiles de manière à ce qu'ils se mettent à jour automatiquement. En même temps, aucun d'entre nous ne pense à gérer la sécurité de ses appareils domestiques et à installer la dernière version logicielle.
Les objets connectés du quotidien peuvent réveler votre clé Wifi, et être la cible d'un hacker…Nous devons revoir notre façon de considérer ces appareils.
Dans certains cas, il est impossible de les mettre à jour. Nous devons considérer ces appareils et ces gadgets comme des ordinateurs déguisés, et les protéger aussi bien que nous le ferions pour notre PC et notre téléphone. Nous allons continuer à voir de nombreuses choses surprenantes connectées à Internet, et si aucun effort n'est fait pour y intégrer la sécurité, le problème risque d'empirer, car certains fabricants ne prennent pas le temps de mesurer les risques que courent les objets connectés au réseau.
Pour revenir un instant à l'analogie avec la bouilloire, rappelons que, dans une entreprise, si un employé achète une bouilloire intelligente, personne ne va s'en inquiéter et personne ne s'attendra à ce que le département informatique ait son mot à dire sur ce genre d'achat. Nous devons donc revoir entièrement notre façon de considérer ces appareils.

Mettre à jour : un élément vital !
Aujourd'hui plus que jamais, il est absolument essentiel que chaque logiciel, appareil, gadget ou équipement soit mis à jour.
Les constructeurs de voitures autonomes tels que Google annoncent déjà qu'ils assumeront la responsabilité des infractions au code de la route, et éventuellement des accidents ou des blessures corporelles dont leurs véhicules seraient responsables. Maigre consolation, avouons-le, si vous êtes victime d'un accident parce que vous avez oublié d'installer la dernière version du logiciel sur votre voiture … À mesure que les systèmes logiciels intelligents s'installent dans nos vies de multiples manières, ces mêmes logiciels pourraient décider de mettre votre vie en danger, il faut en être conscient.
Il va réellement devenir impératif que vous mettiez systématiquement vos logiciels à jour, en même temps que vos autres appareils. Un jour, cela vous sauvera peut-être la vie…

Réagissez à cet article

Source : *Cyber-Sécurité : AVG dévoile ses prévisions pour 2016 – Global Security Mag Online*

URGENT : Phishing Free Mobile, ne vous faites pas avoir !

URGENT : #Phishing Free Mobile, ne vous faites pas avoir !

Réagissez à cet article

Source : *URGENT : Phishing Free Mobile, ne vous faites pas avoir ! – Le Blog du Hacker*