Les cybercriminels utilisent aussi les Sous-domaines abandonnés

Les cybercriminels utilisent aussi les Sous-domaines abandonnés

Si la plupart des hackeurs tentent de contourner les mesures de sécurité mises en place sur les serveurs d'une entreprise, il est parfois plus simple de scruter l'architecture d'un site au global et les sous-domaines, notamment.

Spécialisée dans la sécurité, la société Detectify, propose un outil de scan en mode SaaS et annonce avoir mené une enquête concernant la vulnérabilité des sous-domaines. Ces derniers seraient largement laissés à l'abandon et constitueraient un vecteur d'attaques.
Un prestataire de services proposant de créer des comptes utilisateur en leur attribuant un sous-domaine peut lui-même créer son propre sous-domaine pour lancer un service ou une campagne promotionnelle pendant quelques semaines, voire quelques années. Par la suite, à la fin de cette campagne ou à la fermeture du service en question, Detectify explique que le prestataire n'efface pas systématiquement la redirection du sous-domaine pointant vers le service ou la campagne. Or, un internaute peut donc se créer un compte chez ce prestataire de service puis obtenir ce même sous-domaine et orchestrer une attaque de phishing, par exemple.
Cette manipulation est possible lorsque la société en question ne procède pas à la validation du détenteur de chaque sous-domaine. Et il en existerait un certain nombre parmi lesquels nous retrouvons Heroku, Github, Bitbucket, Squarespace, Shopify, Desk, Teamwork, Unbounce, Helpjuice, HelpScout, Pingdom, Tictail, Campaign Monitor, CargoCollective, StatusPage.io ou encore Tumblr.
« Nous avons également identifié 200 organisations qui s'en trouvent affectées. Dans beaucoup de cas, nous parlons de société listées au NASDAQ ou figurant dans le top 100 d'Alexa », ajoute Detectify.
Pour vérifier si une personne est bien le propriétaire d'un domaine ou d'un sous-domaine, quelques sociétés, comme Google demandent de transférer un ficher HTML via FTP ou d'ajouter une CNAME particulière dans le panneau de contrôle du nom de domaine.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://pro.clubic.com/it-business/securite-et-donnees/actualite-735061-domaine-abandonnes-vecteur-attaques-hackeurs.html?&xvc_mode=ML&xvc_campaign=NL_ClubicPro_New_25/10/2014&partner=-&xvc_position=71726460?&xvc_misc=-&crmID=639453874_71726460?&estat_url=http%3A%2F%2fpro.clubic.com%2Fit-business%2Fsecurite-et-donnees%2Factualite-735061-domaine-abandonnes-vecteur-attaques-hackeurs.html

---

Déclaration à la Cnil d'un dispositif de contrôle et moyen de preuve

Déclaration à la Cnil d'un dispositif de contrôle et moyen de preuve

Les informations collectées par un système automatisé de contrôle des données à caractère personnel avant sa déclaration à la Cnil constituent un moyen de preuve illicite.
Une salariée engagée en tant qu'assistante chargée de l'analyse financière des dossiers ayant fait un usage excessif de sa messagerie électronique à des fins personnelles, son employeur l'a licenciée pour cause réelle et sérieuse.
La cour d'appel a rejeté les demandes de dommages et intérêts de la salariée pour licenciement sans cause réelle et sérieuse et pour licenciement vexatoire, au motif que la déclaration tardive à la Cnil de la mise en place d'un dispositif de contrôle individuel des flux de la messagerie électronique ne rend pas ce système de contrôle illicite, alors que la salariée ne faisait pas un usage raisonnable de cet outil à des fins privées, durant son temps de travail.
La Cour de cassation censure cette position, dans un arrêt du 8 octobre 2014, et considère que les informations collectées par un système de traitement automatisé des données personnelles avant sa déclaration à la Cnil, constituent un moyen de preuve illicite. Les éléments de preuve obtenus à l'aide d'un tel système avant sa déclaration à la Cnil ne sont donc pas licites.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://actualitesdudroit.lamy.fr/Accueil/Articles/tabid/88/articleType/ArticleView/articleId/125297/Declaration-a-la-Cnil-dun-dispositif-de-controle-et-moyen-de-preuve.aspx

Une bague connectée pour mieux nous contrôler ?

	Une bague connectée pour mieux nous contrôler ?

Un anneau pour les contrôler tous ? Au Japon, plusieurs sociétés planchent sur le concept de bague connectée, avec l'ambition de proposer reconnaissance de mouvements, clé sans contact, porte-monnaie électronique et système d'alerte au sein d'un seul et même petit appareil en forme de bijou.

Lunettes, montres ou vêtements, la tentation est grande de conférer des capacités informatiques à tous les objets du quotidien et beaucoup d'acteurs courent après la vision d'un accessoire à tout faire, fonctionnant en adéquation avec un smartphone. Parmi les différentes intégrations possibles, plusieurs se sont déjà intéressés à la bague. Un anneau se fait aisément oublier tout en restant accessible, et le doigt reste encore l'un des meilleurs moyens qu'a trouvés l'homme pour interagir avec son environnement. Jusqu'ici, les premières tentatives en matière d'anneaux connectés se sont toutefois révélées décevantes, en grande partie parce que les interactions proposées étaient à trop faible valeur ajoutée…

La donne va-t-elle changer ? La miniaturisation des composants permet désormais d'aller plus loin, comme en témoigne le projet développé par la start-up japonaise 16Lab. Celle-ci planche sur un anneau de titane qui, à terme, servirait aussi bien à la saisie de texte et de messages qu'à ouvrir la porte de sa voiture, payer ses courses ou alerter lors de la réception d'un message. Dans sa version actuelle, encore en cours de développement, la bague embarque deux petites surfaces tactiles qu'il suffit d'actionner du pouce pour « réveiller » l'appareil, qui émet alors une vibration de confirmation. Au centre de l'anneau, on trouve un composant développé par ALPS, qui propose, au sein d'une enveloppe de seulement 6 mm² une liaison Bluetooth 4.0, un accéléromètre et une boussole. Cette puce permet donc d'assurer la liaison avec le smartphone de l'utilisateur, mais aussi de mesurer la position de sa main dans l'espace ainsi que les mouvements de cette dernière.
D'après son concepteur, le dispositif est suffisamment précis pour envisager sérieusement d'écrire à main levée, en traçant simplement dans les airs les caractères. ALPS propose d'ailleurs des scénarios dans lesquels un démonstrateur contrôle une interface de télévision ou de téléphone grâce à des gestes capturés non pas par une caméra, mais par ce sensor network module.
16Lab admet toutefois sans ambages que la simple reconnaissance de mouvements ne justifierait sans doute pas l'achat et le port d'une telle bague. Il fallait donc chercher à enrichir cette dernière, ce qui passe par l'ajout de composants supplémentaires. Rapidement, le NFC s'est imposé comme une piste à étudier : les communications en champ proche, en plein essor, permettent en effet d'utiliser l'anneau comme une clé, capable d'actionner une serrure compatible, mais aussi comme un porte-monnaie électronique, à l'instar des déploiements en cours dans l'univers de la téléphonie mobile. Plutôt que de sortir son téléphone de sa poche, on n'aurait donc qu'à poser la main sur une surface dédiée au paiement. Dans tous ces scénarios, la bague fonctionne comme une interface rapprochée de la main, l'intelligence et la communication restant gérés au niveau du téléphone.
Alors, la bague sera-t-elle le parfait « raccourci » ? En attendant que le marché en décide, une autre start-up japonaise a justement fait de cette notion son slogan. Logbar Inc. développe également une bague à tout faire, avec une proposition de valeur similaire à celle qu'avance 16Lab. Sa bague s'appelle pour l'instant simplement Ring, et les développements reposent sur des fonds levés grâce au financement participatif. Bouclée en début d'année, la campagne Kickstarter de Logbar a débouché sur une enveloppe globale de 880 000 dollars, alors que la société avait fixé son objectif à 250 000 dollars. Le concept de bague connectée semble donc ne pas laisser indifférent. Reste à voir dans quelle mesure ces premiers essais seront transformés.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.clubic.com/technologies-d-avenir/ceatec/actu-une_bague_connectee_pour_les_controler_tous-731899.html

---

France Connect, pour simplifier l'administration

numérique

France Connect, pour simplifier l'administration numérique

Les administrations et les collectivités locales qui bénéficieront à court terme d'un support d'identification unifié.

Thierry Mandon, le secrétaire d'Etat chargé de la réforme de l'Etat et de la simplification, s'est rendu le 2 octobre dans les locaux de la Dila pour visiter le plateau de développement du projet « France Connect ». France Connect est la « marque de fabrique » du futur système numérique national d'identification et d'authentification des usagers des services de l'administration.
Le dispositif, développé par le Secrétariat général pour la modernisation de l'action publique (SGMAP), cible les services publics de l'Etat, les administrations et les collectivités locales qui bénéficieront à court terme d'un support d'identification unifié, bon marché et relativement facile à implémenter dans leur propre système d'information.
Ce programme, qui sera déployé dès 2015 avec la bascule sur France Connect des trois millions de comptes du site portail « mon.service-public.fr », doit permettre à l'usager de fédérer tous ses comptes publics existants, puis d'établir ensuite de nouvelles connexions avec des administrations non encore dotées de leur propre système d'authentification, à condition d'adopter directement celui de France Connect.

La solution annule et remplace la carte d'identité électronique
La procédure qui s'apparente à celle déjà pratiquée par les réseaux sociaux comme « Facebook Connect » ou « Google+ Sign in » restera relativement simple à déployer. L'usager n'ayant pas encore de compte pourra s'enregistrer à partir d'une administration reconnue par le label et à laquelle il est numériquement affilié. Après avoir saisi ses identifiants d'origine, le site lui proposera en retour de fédérer son compte avec France Connect.
Après avoir donné son consentement, il disposera d'un compte national réutilisable sur de nombreux sites. Cette simplicité dans le mode d'enregistrement a d'ailleurs incité la DGFIP à proposer aux contribuables, dès la campagne 2016 de déclaration de revenus en ligne, de fédérer leur compte « impôts.gouv.fr » avec France Connect afin d'étendre rapidement le dispositif aux 10 millions d'utilisateurs dotés d'un compte fiscal.
France Connect ne se limite pas au seul composant unifié d'identification. A terme, il devrait permettre aux administrations et notamment aux collectivités d'effectuer des requêtes sur le niveau d'imposition ou sur la domiciliation de l'usager afin d'éviter l'étape coûteuse des demandes de justificatifs. Selon un expert ayant participé à la définition du projet, la nouvelle solution répondrait à 95% des besoins justifiant la création d'une carte d'identité électronique (CNIE) et l'économie réalisée sur la « non création » de cette carte avoisinerait le milliard d'euros.
France Connect devrait ainsi accélérer le développement de portails de téléservices couvrant la totalité des besoins transactionnels des collectivités avec les usagers et constituer également une brique essentielle de la mise en œuvre du programme « dites-le nous une fois » dans toutes les administrations. Autant dire qu'il constitue déjà à lui seul un levier essentiel pour les prochaine conquêtes de l'administration numérique.
Philippe Parmantier / EVS

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.localtis.info/cs/ContentServer?pagename=Localtis/LOCActu/ArticleActualite&cid=1250267813817

Après JP Morgan, 9 autres

banques auraient été piratées

Après JP Morgan, 9 autres banques auraient été piratées

Le groupe responsable du piratage de JP Morgan cet été aurait mené des attaques sur 9 autres établissements financiers. Comme la loi américaine n'oblige pas les banques à communiquer sur ce genre d'incident, l'ampleur exacte de la fuite potentielle de données reste inconnue.

JP Morgan serait loin d'être la seule banque à avoir été attaquée par ce groupe de pirates. Il s'agirait en réalité d'une vague d'intrusions, dont l'ampleur exacte reste inconnue.

Elle aurait permis aux assaillants « d'infiltrer environ 9 autres établissements financiers », explique le New York Times en s'appuyant sur des sources proches de l'enquête.

De nombreux points à éclaircir
Peu de détails ont été révélés par les canaux officiels. D'ailleurs, le journal américain n'a pas pu obtenir les noms des établissements infiltrés et ignore toujours ce à quoi les pirates ont pu accéder.
JP Morgan, seule banque à avoir communiqué sur le sujet, affirme que les responsables n'ont pu accéder qu'aux noms des clients et à d'autres informations non-financières. Le personnel chargé de la sécurité de la banque aurait repéré l'attaque avant que les assaillants n'accèdent aux données sensibles. Ceci étant dit, l'intrusion n'aurait pas été entièrement arrêtée avant la mi-août alors qu'elle avait débuté en juillet.
Pour ce qui est de l'identité des pirates, les autorités en charge de l'enquête pencheraient pour un groupe opérant depuis la Russie. Ils auraient une « vague connexion » avec des membres du gouvernement de Moscou.
Les motivations des pirates restent, elles aussi, inconnues. Cependant, ces attaques pourraient avoir été menées en représailles aux sanctions visant la Russie dans le cadre de la crise ukrainienne, présument les services de renseignement américains.

Une brèche dans les systèmes mais aussi dans la loi ?
Outre l'aspect sécuritaire, l'attaque met en évidence une potentielle lacune dans la loi américaine. On apprend aujourd'hui que l'incident a bien plus d'ampleur qu'il n'y parait. Peut être qu'une meilleure information aurait permis de limiter l'intrusion ou d'aider à faire avancer l'enquête. Seulement, les banques en ligne ne sont pas obligées de communiquer sur les événements ayant pu compromettre les données des clients à moins qu'ils leur aient fait perdre de l'argent.

Dans certains Etats américains, les banques peuvent attendre jusqu'à un mois avant d'informer les autorités et les clients de ce type d'incident. La loi californienne, par exemple, impose simplement un délai « raisonnable », une définition sujette à interprétations. Il est alors difficile, dans un tel contexte, de lutter efficacement contre ce type de piratage.

La France n'est pas mieux lotie : les banques ne sont pas tenues d'informer les clients lors d'une fuite de données. Pour l'instant, seuls les fournisseurs d'accès et opérateurs ont l'obligation de notifier la CNIL ou les clients. Cependant, le régulateur français et ses équivalents européens cherchent à étendre ces exigences à l'ensemble des services en ligne.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://pro.clubic.com/it-business/securite-et-donnees/actualite-731231-jp-morgan-9-banques-attaquees-pirates.html

500 000 PC infectés à cause d’une faille Windows XP

500 000 PC infectés à cause d’une faille Windows XP

Selon les chercheurs en sécurité de Proofpoint, 52% des PC infectés par le botnet Qbot font tourner Windows XP. Exploitant une faille de Windows XP mais également de Seven et Vista, un groupe de cybercriminels russe a réussi à activer le botnet Qbot fort 500 000 PC zombies, essentiellement localisés aux Etats-Unis. Son objectif : Aspirer les identifiants bancaires des utilisateurs de ces PC corrompus.

Des pirates russes à l’origine du botnet Qbot ont construit une impressionnante armée de 500 000 PC zombies en exploitant des failles non corrigées dans des ordinateurs tournant sous Windows XP mais également Windows 7 et Vista. Des PC localisés principalement aux Etats-Unis, a fait savoir la société Proofpoint. Ces derniers temps, les hackers russes ont fait monter la pression avec des incursions sérieuses telle que l’attaque qui a visé la banque américaine JPMorgan Chase. Avec ce botnet, baptisé Qbot, les chercheurs de Proofpoint ont fait ressortir que le groupe qui est à l’origine de sa création l’a élaboré de façon méticuleuse à travers le temps, sans faire de vague, au point de rester sous les radars des sociétés de sécurité et donc de ne pas avoir attiré leur attention.

Selon Proofpoint, 75% des 500 000 PC infectés par le botnet Qbot sont situés aux Etats-Unis, sachant que parmi eux, 52% font tourner Windows XP, 39% Windows 7 et 7% Windows Vista. En Grande-Bretagne, la proportion de PC infectés est bien moindre, 15 000 postes environ. « Avec 500 000 clients infectés volant les identifiants des comptes bancaires en ligne des utilisateurs, le groupe de cybercriminels a le potentiel pour réaliser des bénéfices vertigineux », ont indiqué les chercheurs de la société de conseil en sécurité. Mais le botnet Qbot ne s’attaque pas seulement aux comptes bancaires, il compromet également les sites WordPress, soit en infectant le site lui-même ou bien en injectant des contenus corrompus dans leurs newsletters.
Article de Dominique Filippone

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.lemondeinformatique.fr/actualites/lire-500-000-pc-infectes-a-cause-d-une-faille-windows-xp-58878.html

Un nouveau malware vise les Mac, 17.000 machines affectées ?

Un nouveau malware vise les Mac, 17.000 machines affectées ?

Selon la firme russe Dr.Web un malware visant spécifiquement les possesseurs de Mac serait actuellement actif, affectant plus de 17.000 machines à travers le monde. Pas une première, mais ce malware possède quelques spécificités amusantes.

Pas la peine de se mentir, les produits Apple eux aussi sont parfois victimes de malwares. En 2011, le Trojan Flashback avait ainsi infecté des centaines de milliers d'ordinateurs Apple. Le malware détecté par Dr Web est en revanche bien moins diffusé : 17.000 utilisateurs seulement seraient infectés.
Ce malware se range sous la catégorie des Botnets, infectant l'ordinateur de l'utilisateur afin de permettre à l'attaquant de l'exploiter pour d'autres fonctions à l'insu de son utilisateur. Le malware a été baptisé, un peu rapidement, iWorm par Doctor Web, bien que le mode exact de propagation du virus reste encore peu clair.
La particularité qui a retenu l'attention des chercheurs, c'est la façon dont les ordinateurs infectés récupèrent les adresses IP des serveurs de command&control. Les machines du botnet vont ainsi chercher sur Reddit les adresses de leurs centre de command&control : celles-ci sont postées à intervalles régulier dans la section commentaire d'un sujet destiné à recenser des serveurs Minecraft via un compte tenu par les individus responsables de la propagation du malware.

Reddit est innocent !
Reddit n'a rien à se reprocher, le site n'a pas été altéré ou son utilisation n'a pas été techniquement détournée, mais cette approche originale mérite d'être notée. Comme le relève le chercheur Graham Cluley, même en supprimant le compte utilisé pour router vers ces adresses IP, cela n'empêcherait pas les pirates de recréer un compte et de continuer leur activité.
Comme souvent néanmoins, il convient de rester prudent avec les alertes lancées par les firmes spécialisées dans la vente d'antivirus. Dr.Web annonce ainsi 17.000 ordinateurs infectés à travers le monde, mais ne précise pas du tout quel mode de diffusion a été choisi pour propager le malware. Selon des sources anonymes, le principal mode d'infection se ferait via le téléchargement de logiciels Adobe et Microsoft piratés sur les plateformes de partage en P2P.
De la même manière, peu d'informations sont disponibles pour ceux qui souhaitent se prémunir de ce malware, si ce n'est la solution vendue par Dr.Web… Mais selon MacRumors, l'outil de protection maison proposé par Apple à ses clients Xprotect, a été mis à jour pour détecter et empêcher la propagation de cette menace.
Attention Livo !

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.zdnet.fr/actualites/un-nouveau-malware-vise-les-mac-17000-machines-affectees-39807339.htm
Par Louis Adam | Lundi 06 Octobre 2014

Que sont prêts à accepter les Français de leurs données personnelles ?

Que sont prêts à accepter les Français de leurs données personnelles ?

Havas Media Group France vient de publier les résultats d'une étude qui dresse l'état des lieux du rapport entre les Français et la Data. Des Français conscients et inquiets mais qui n'hésitent pas à donner leur données ; à condition d'obtenir des contreparties.

Des Français inquiets…

Havas Media a interrogé 1000 internautes représentatifs de la population française, agés de 15 à 64 ans. Le premier enseignement est qu'ils sont parfaitement conscients de la transmission de leurs données à des tiers. 93% savent qu'elles sont captées et 84% s'en inquiètent. Trois craintes se dégagent : 74% des internautes ont peur de l'usage frauduleux des données, 53% ont peur que des détails de leur vie intime soient révélés et 47% craignent la surveillance des autorités.

… mais opportunistes

Cependant, 46% des Français voient cette utilisation de leurs données comme une opportunité. 45% sont prêts à laisser les entreprises suivre leurs données, moyennant une contrepartie financière. Près de 42% des internautes interrogés sont prêts à l'accepter contre une contrepartie non-financière.

La typologie des Français vis-à-vis de leurs données personnelles

Grâce aux réponses fournies par l'échantillon interrogé, Havas Media a pu segmenter les internautes en cinq profils distincts. Chaque groupe a des comportements et des attentes spécifiques.

Data Natives – 24%. Une population plutôt jeune (15 à 25 ans), consciente de la captation des données personnelles mais peu inquiète. Pour eux, c'est normal, habituel, ils ne se protègent ni plus ni moins que les autres et n'attendent pas grand chose de la transmission des données.

Data Stratèges – 9%. Ils sont plus âgés (35 à 49 ans) et tout à fait conscients. Ils font plus attention aux données qu'ils fournissent et cherchent à obtenir des contreparties.

Data Fatalistes – 27%. Cette population est assez jeune, consciente, inquiète mais fataliste. Ils savent que leurs données sont captées mais ne maîtrisent pas vraiment la confidentialité de leurs données. Ils se protègent peu, par négligence.

Data Parano – 36%. Ils sont plus âgés, conscients et très inquiets. Ils ne voient aucun intérêt dans la captation de leurs données personnelles. Ils craignent tout : l'utilisation frauduleuse de leurs données, la surveillance généralisée et la diffusion de données privées. Ils ne comprennent pas tout mais cherchent à se protéger du mieux qu'ils peuvent.

Data Détendus – 4%. Cette population est indifférente au phénomène. Ces internautes sont peu conscients et donc peu inquiets. Ils pensent pouvoir tirer un bénéfice de la captation de leurs données mais restent passifs et fournissent de nombreuses données personnelles.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :

http://www.blogdumoderateur.com/etude-havas-media-francais-donnees-personnelles/

JP Morgan piraté : les données de 83 millions de clients exposées

JP Morgan piraté : les données de 83 millions de clients exposées

Cet été, JP Morgan a été victime d'une attaque informatique de grande envergure. La banque américaine admet que les données de 83 millions de clients ont pu être exposées. Toutefois, il ne s'agirait pas d'informations sensibles pour la porte-parole de la société.

76 millions de foyers et 7 millions de PME seraient concernés par ce qui pourrait être l'une des plus grandes fuites de données de l'histoire. Cet été, les systèmes informatiques de la banque JP Morgan ont été compromis par une attaque ayant permis aux pirates d'accéder aux noms, adresses, numéros de téléphone, et adresses e-mail de 83 millions de clients, annonce JP Morgan dans un document transmis à la SEC, le gendarme américain de la bourse.

La banque ajoute qu'il n'y a « pas de preuve » que des données sensibles comme les numéros de comptes, mots de passe, identifiants, dates de naissance ou numéros de sécurité sociale aient été compromises. Les responsables de l'attaque n'auraient pas eu accès à ce type de données sensibles, pense Patricia Wexler, porte-parole de JP Morgan. Il ne serait donc pas nécessaire que les clients changent leurs mots de passe.

Pour le moment, la banque n'aurait pas constaté de fraude relative à cet incident.
Mais l'attaque, très sophistiquée, aurait tout de même permis aux pirates d'accéder « au plus haut niveau des droits administrateurs » selon le New York Times qui s'appuie sur des sources proches du dossier. Puis, les informations exposées restent potentiellement utiles aux cyber criminels : « ils pourraient littéralement utiliser l'identité de ces 83 millions de personnes et entreprises », affirme Tal Klein, de la société de sécurité informatique Adallom, à l'agence Reuters.
La banque avait annoncé en août qu'elle enquêtait avec les autorités sur une attaque informatique. Le FBI soupçonnait des pirates russes en raison de la crise ukrainienne et des sanctions économiques à l'encontre du régime de Moscou. Le New York Times affirmait que JP Morgan n'était pas la seule banque concernée mais qu'en tout, cinq banques auraient été visées le même mois.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://pro.clubic.com/it-business/securite-et-donnees/actualite-730905-clients-jp-morgan-pirates.html

Cookies : ça y est, la Cnil commence à contrôler les sites français

	Cookies : ça y est, la Cnil commence à contrôler les sites français

Les contrôles de la Cnil commencent. La Commission va vérifier que les sites Internet français utilisant des cookies publicitaires ou de mesure d'audience invitent les visiteurs à leur consentement préalable.

« En utilisant ce site, vous acceptez l'utilisation de cookies permettant de vous proposer des contenus et des services adaptés à vos centres d'intérêts. » Le message a fleuri le Web français depuis décembre 2013. Il est la conséquence directe d'une recommandation de la Cnil découlant d'une directive européenne de 2011.

Celle-ci explique que « les traceurs (cookies ou autres) nécessitant un recueil du consentement ne peuvent (pas) être déposés ou lus sur son terminal, tant que la personne n'a pas donné son consentement ».

A partir de ce mois d'octobre, la Commission va procéder à des contrôles. Tout acteur contrevenant à cette obligation s'expose à une amende pouvant atteindre 150 000 euros. Voici un rappel pour être conforme :

Mettre son site Web en conformité. Qui est concerné par cette obligation ?
Les responsables de sites, éditeurs d'applications mobiles, régies publicitaires, réseaux sociaux et éditeurs de solutions de mesure d'audience.

Quels sont les cookies concernés par la loi ?
Les cookies liés aux opérations publicitaires, comme le traçage comportemental, les cookies des réseaux sociaux générés par les boutons de partage ainsi que certains cookies de mesure d'audience.

Quelles sont les obligations légales ?
Informer les internautes de la finalité des cookies, obtenir leur consentement et leur fournir un moyen de les refuser. A noter que la durée de validité de ce consentement est de 13 mois maximum.

Quels sont les cookies exemptés ?
Les cookies utilisés pour un panier d'achat de site marchand, l'identification pour la durée d'une session, l'authentification, la lecture de fichiers multimédias, l'équilibrage de charge, l'analyse d'audience (dans certains cas) ou encore la personnalisation de l'interface utilisateur.

Consciente que la mise en conformité avec ces dispositions présente, selon les cas, une certaine complexité, la Cnil consacre désormais une partie de son site Web à ce sujet. Elle explique quelles sont les façons de mesurer l'audience afin d'être exempté du message de consentement préalable. La Commission explique aussi comment recueillir ce consentement pour les outils comme Google Analytics ou Universal Analytics. La Cnil dispose enfin de solutions pour les boutons de partage sociaux ou pour les sites multipliant les cookies.

Préparer un contrôle de la Cnil
Il faut tout d'abord savoir que la décision de procéder à une vérification est prise par le président de la Cnil, sur la proposition du service des contrôles. La décision de prévenir, ou non, le responsable du site Web qui va faire l'objet de cette visite est « prise en opportunité », ce qui signifie qu'elle ne sera pas systématique. La Cnil peut aussi exiger la fourniture de documents en amont de sa visite. Voici le déroulé d'un contrôle :
Une mission de contrôle vise prioritairement à obtenir copie du maximum d'informations, techniques et juridiques, pour apprécier les conditions dans lesquelles sont mis en œuvre des traitements informatiques.
La délégation de la Cnil peut demander communication de tous documents nécessaires à l'accomplissement de sa mission, quel qu'en soit le support, et en prendre copie.
Les contrôleurs peuvent accéder aux programmes informatiques et aux données, et en demander la transcription pour les besoins du contrôle.
La délégation peut demander copie de : contrats (ex.: contrats de location de fichiers, contrats de sous-traitance informatique), formulaires, dossiers papiers, bases de données, etc.
Un procès-verbal de fin de mission est établi à l'issue du contrôle, pour préciser notamment la liste des documents dont une copie a été effectuée.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://pro.clubic.com/legislation-loi-internet/cnil/actualite-730529-cnil-controles-rappel-commercants.html