À partir de quel âge peut-on laisser les ados s’inscrire sur les réseaux sociaux ?

À partir de quel âge peut-on laisser les ados s’inscrire sur les réseaux sociaux ?

Les réseaux sociaux seront-ils bientôt interdits aux moins de 16 ans ? La nouvelle législation européenne sur la protection des données, approuvée le 17 décembre, entend relever l'âge minimum pour pouvoir s'inscrire sans consentement parental.

Bruxelles prévoit d'interdire l'accès aux réseaux sociaux aux adolescents de moins de 16 ans, qu'en est-il exactement ?

Pour le moment, il s'agit d'un accord de principe qui devra être soumis au vote du Parlement européen en 2016. Rien n'est donc fait. Cette disposition, ajoutée à la dernière minute au texte sur la protection des données personnelles, fixe à 16 ans l'âge minimum pour s'inscrire sur les réseaux en ligne. Mais chaque État peut ensuite déterminer ses propres limites entre 13 ans et 16 ans.

La règle n'est pas très contraignante, mais c'est tout de même un progrès puisque, à ce jour, aucune loi française ne fixe l'âge d'utilisation pour les mineurs. Actuellement, nous appliquons le droit américain avec la loi COPPA (Children's Online Privacy Protection Act) qui interdit aux sites de recueillir des données d'enfants de moins de 13 ans, sans consentement parental. Si outre-Atlantique, celle-ci est très contraignante, ce n'est pas le cas en France. Les jeunes peuvent s'inscrire en mentant sur leur âge sans conséquences.

À partir de quel âge peut-on les laisser s'inscrire ?

En dessous de 13 ans, ce n'est pas souhaitable car les enfants ne font pas la différence entre vie publique et vie privée. À partir de 13 ou 14 ans, en revanche, ils commencent à acquérir un esprit critique qui leur permet de prendre un peu de recul. Mais la question n'est pas tant l'âge auquel il faut les laisser s'inscrire sur les réseaux sociaux que celui auquel on leur donne un smartphone. Ces petits joujoux sont des réseaux sociaux à eux tout seuls, avec les SMS. Ils donnent en outre accès à tous les sites Internet. Or, la plupart des parents ne pensent pas à installer un contrôle parental.

Il faut donc retarder le plus possible l'acquisition du smartphone, à la fois pour protéger l'enfant des contenus inappropriés et pour qu'il comprenne qu'on peut s'en passer. Un tiers des élèves de CM1-CM2 que je rencontre lors de mes interventions dans les établissements scolaires possède un smartphone. Difficile dans ces conditions de ne pas devenir dépendant.

Smartphone ou ordinateur, comment accompagner les adolescents sur les réseaux sociaux ?

Il faut commencer par installer un contrôle parental, quel que soit le terminal. Les parents doivent ensuite expliquer à l'adolescent la stratégie de ces sites Internet qui revendent les données personnelles à des fins publicitaires. Les contenus sont gratuits, mais l'utilisateur devient en quelque sorte un produit commercial. Une fois cette dimension abordée, il faut l'accompagner dans la phase d'inscription en regardant avec lui les différents paramètres du site. Ainsi, il est primordial de limiter l'accès aux publications aux seuls amis, de même qu'il ne faut pas accepter d'inconnus ou de simples connaissances dans son réseau. Il est également essentiel de rappeler à l'adolescent qu'une fois en ligne, les contenus ne peuvent plus être supprimés, ou alors au prix de démarches complexes sans aucune garantie, puisque n'importe qui peut en faire une copie.

Certains réseaux sociaux sont un peu plus encadrés que d'autres. C'est le cas de Facebook, Instagram et WhatsAPP (qui appartiennent au premier) ainsi que Twitter. En revanche, je déconseille fortement Snapchat. Cette application, qui permet d'échanger des photos de manière instantanée et soi-disant éphémère, est beaucoup plus incontrôlable. Quel que soit le site ou l'application, les parents doivent toujours accompagner les adolescents et, a fortiori, les enfants dans l'univers numérique… comme ils le ferraient dans la rue ou sur la route.

Réagissez à cet article

Source : *À partir de quel âge peut-on laisser les ados s'inscrire sur les réseaux sociaux ? | La-Croix.com – Actualité*

Des organismes à l'abri des cyber-attaques grâce à une panoplie de normes sur la

sécurité

	**Des organismes à l'abri des cyber-attaques grâce à une panoplie de normes sur la sécurité**

Les cyber-attaques sont l'un des plus grands risques auxquels les organismes sont confrontés. Dans le monde numérique d'aujourd'hui, le besoin de normes et de systèmes pour protéger la sécurité des informations n'a jamais été aussi important. C'est pourquoi la famille de normes ISO/IEC 27000 sur les techniques de sécurité relatives aux technologies de l'information a été mise à jour, afin d'offrir aux organismes cette valeur ajoutée et ce surcroît de confiance.

Il ressort d'une étude mondiale menée par l'ISACA dans 129 pays, que seuls 38 % des organismes interrogés estiment être préparés à une cyber-attaque – même si 83 % d'entre eux sont malgré tout conscients que ce type d'intrusion constitue l'une des trois principales menaces pesant sur les organismes à l'heure actuelle. Compte tenu du volume de données personnelles et sensibles traitées électroniquement, il y a beaucoup à perdre en cas d'atteinte à la sécurité.

Le professeur Edward Humphreys, Animateur du groupe de travail de l'ISO chargé de l'élaboration des normes de systèmes de management de la sécurité des informations (SMSI) souligne que, « Pour garantir la sécurité dans le paysage numérique actuel, tous les organismes, quelle que soit leur taille, devraient mettre en place un cadre de management, à titre de préalable, pour gérer leurs cyber-risques.

La norme ISO/IEC 27001 a été précisément conçue à cette fin. Cette norme fait figure de « langage commun » universel pour apprécier, traiter et gérer les risques de sécurité des informations. »

Les toutes dernières révisions et adjonctions à la famille de normes ISO/IEC 27000 présentées ci-dessous ont été publiées en 2015. Elles font partie de la « boîte à outils » ISO/IEC 27000 destinée à la maîtrise des cyber-risques.

Protéger les informations dans le Cloud (ISO/IEC 27017)

Un nouveau code pratique pour les contrôles de sécurité de l'information pour les services du nuage, ISO/IEC 27017, vient d'être publié. Le nuage, ou Cloud en anglais, est l'une des innovations les plus largement utilisées dans le monde trépidant du commerce et des affaires d'aujourd'hui. À mesure que ce service se généralise, les utilisateurs exigent des garanties quant à la sécurité du stockage et du traitement des données dans le Cloud.

Le marché des services de Cloud, par définition mondial, est caractérisé par la dispersion des fournisseurs sur de vastes secteurs géographiques et par le transfert régulier des données d'un pays à l'autre. Il est donc essentiel de pouvoir s'appuyer sur des directives internationales.

Selon Satoru Yamasaki, l'un des rédacteurs qui a travaillé sur la norme, « ISO/IEC 27017 aidera les fournisseurs de services à trouver un terrain d'entente avec leurs clients quant à l'adéquation des contrôles de sécurité et leurs recommandations de mise en œuvre.

Cette Norme internationale relative aux contrôles de sécurité pour le Cloud facilitera le développement et l'expansion de systèmes informatiques en nuage plus sûrs ».

Ces nouvelles lignes directrices sont le fruit d'une initiative commune des principales organisations élaboratrices de normes internationales – l'IEC, l'ISO, et l'UIT – afin de garantir un rayonnement maximal.

Des solutions intégrées pour les services (ISO/IEC 27013)

Un nombre croissant d'organismes choisissent de combiner leur système de management de la sécurité de l'information (ISO/IEC 27001) et leur système de management des services (ISO/IEC 20000-1). Un système intégré implique que l'organisme peut gérer efficacement la qualité de ses services, les retours d'information de ses clients et résoudre les problèmes tout en préservant la sécurité de ses données.

ISO/IEC 27013 propose une approche systématique pour faciliter l'intégration d'un système de management de la sécurité de l'information avec un système de management des services, ce qui permet de réduire les frais de mise en œuvre et d'éviter les activités à double, dans la mesure où un seul audit, au lieu de deux, est nécessaire pour l'obtention de la certification.

Communications intersectorielles et interorganisationnelles (ISO/IEC 27010)

Comment des organismes qui s'échangent des informations peuvent-ils s'assurer que leurs données sont protégées ? ISO/IEC 27010 est un complément sectoriel à la boîte à outils ISO/IEC 27000, qui établit des lignes directrices pour l'introduction, la mise en œuvre, la mise à jour et l'amélioration de la sécurité de l'information des communications intersectorielles et interorganisationnelles. Elle comprend des principes généraux sur les moyens à mettre en œuvre pour respecter les exigences spécifiées, en s'appuyant sur des méthodes de messagerie et d'autres techniques établies. Cette norme devrait encourager l'essor de communautés de partage d'informations à l'échelle mondiale.

Comme l'explique M. Mike Nash, l'un des rédacteurs de la norme, « ISO/IEC 27010 permet fondamentalement d'adapter et d'appliquer ISO/IEC 27001 et ISO/IEC 27002 aux communications entre organismes. La mise en place de cette norme leur apporte un surcroît de confiance dans le fait que les informations qu'ils partagent avec un autre organisme ne seront pas divulguées involontairement. » Cette norme est particulièrement pertinente pour la protection d'une infrastructure nationale cruciale, lorsque le partage sécurisé d'informations sensibles est primordial. Elle est aussi largement utilisée par les équipes chargées de réagir en cas d'incidents liés à la sécurité.

Détection et prévention des cyber-attaques (ISO/IEC 27039)

Comment un organisme peut-il détecter et prévenir une cyber-intrusion dans son réseau, ses systèmes ou ses applications ? Au vu des meilleures pratiques en la matière, un organisme devrait être capable de savoir si, quand et comment une intrusion est susceptible de se produire. Il devrait également être prêt à identifier quelle faille a été exploitée et quels contrôles devraient être mis en place pour que ce type d'incident ne se réitère pas. Il peut, pour ce faire, recourir à un système de détection et de prévention d'intrusion (IDPS).

ISO/IEC 27039 établit les lignes directrices relatives à la préparation et à la mise en place d'un IDPS, et couvre des aspects essentiels tels que la sélection, le déploiement et les opérations. Cette norme est particulièrement utile sur le marché actuel où un nombre important de produits et services IDPS basés sur différentes technologies et approches sont proposés, qu'ils soient commercialisés ou disponibles en source ouverte. ISO/IEC 27039 permet de guider les organismes tout au long du processus.

Audit et certification (ISO/IEC 27006)

De plus en plus d'organismes s'en remettent aux audits de certification par tierce partie pour démontrer qu'ils ont mis en place un système de management de la sécurité de l'information (SMSI) fiable, en conformité avec les exigences d'ISO/IEC 27001. ISO/IEC 27006 établit les exigences que les organismes procédant à l'audit et à la certification doivent remplir pour être accrédités, afin d'être en mesure d'offrir des services de certification selon ISO/IEC 27001.

« ISO/IEC 27006 est une référence en matière d'accréditation pour les organismes de certification qui proposent des services relatifs à ISO/IEC 27001 » explique M. Humphreys, qui ajoute que « cet aspect est important car l'accréditation des organismes de certification est un gage de confiance supplémentaire dans le processus d'audit, qui renforce la crédibilité du certificat qu'ils octroient ».

Réagissez à cet article

Source : *Des organismes à l'abri des cyber-attaques grâce à une boîte à outils de normes sur la sécurité (2015-12-17) – ISO*

Apple contre le projet de loi britannique sur le

renseignement !

	**Apple contre le projet de loi britannique sur le renseignement !**

Le monde semble actuellement « en guerre » contre les projets de loi sur le renseignement qui fleurissent un peu partout dans les pays développés. Et nombreux sont ceux qui prennent part à ces actions. Apple, par exemple, a clairement affiché ses objections face au projet de loi britannique.

Le monde semble actuellement « en guerre » contre les projets de loi sur le renseignement qui fleurissent un peu partout dans les pays développés. Et nombreux sont ceux qui prennent part à ces actions. Apple, par exemple, a clairement affiché ses objections face au projet de loi britannique.

Pour la firme de Cupertino, affaiblir les techniques de chiffrement, comme le souhaite le gouvernement britannique, reviendrait à diminuer la sécurité des « données personnelles de millions de citoyens respectueux des lois« . La création d'une porte dérobée présente, elle, un risque majeur : « une clef laissée sous le paillasson ne serait pas là uniquement pour les gentils. Les méchants sauraient la trouver également. » Voici en substance les points qu'Apple a voulu souligner à la commission en charge de ce projet de loi.

Autre point sensible : la modification du fonctionnement de iMessage pour pouvoir être écouté « placerait une entreprise comme Apple, dont la relation avec les clients est en partie construite sur un esprit de confiance quant à la confidentialité des données, dans une position très difficile« .

La commission saura-t-elle prendre en compte ce genre de considérations ? À suivre !

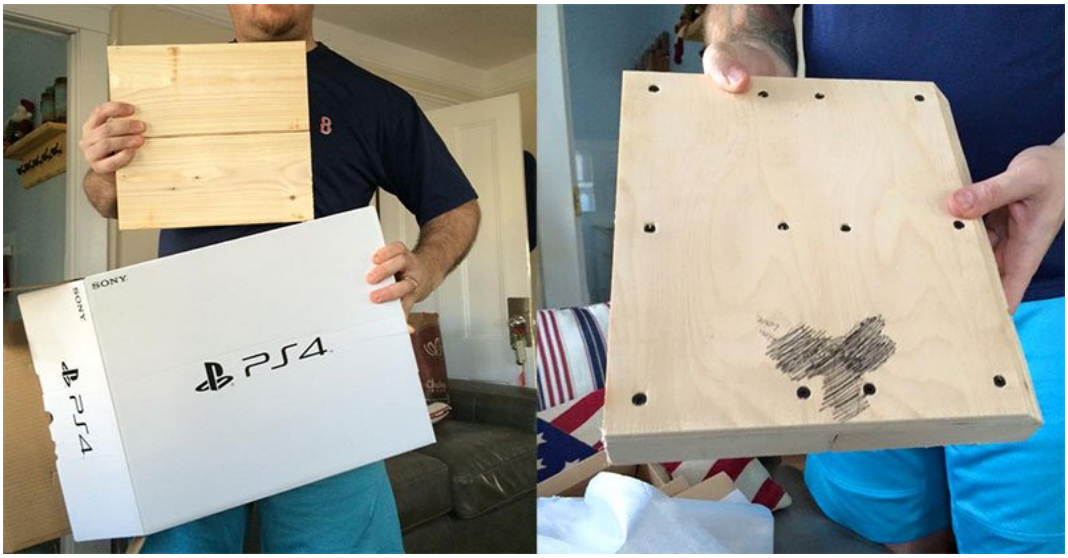
Réagissez à cet article

Source : *Apple contre le projet de loi britannique sur le renseignement !*

Il commande une PS4 pour Noël et reçoit à la place un morceau de bois

Il commande une PS4 pour Noël et reçoit à la place un morceau de bois

Un père de famille a fait l'acquisition d'une PS4 en boîte dans un magasin Target, en vue des fêtes de Noël. Lorsque son fils a déballé la console le 25 décembre, ils ont découvert un bloc de bois en forme de PS4 à l'intérieur.



Ah, la magie de Noël… parfois certains cadeaux laissent de marbre, tandis que d'autres font un carton. Par contre, la PlayStation 4 en bois était jusque-là inédite… jusqu'à ce que la famille Lundy, résidant dans le Massachusetts aux Etats-Unis, décide de faire l'acquisition d'une console dans le magasin Target de sa ville. Le cadeau est destiné à Scott Lundy, 9 ans. Fou de joie en découvrant son cadeau le 25 décembre, il demande à son père de l'installer sur la télévision. Seulement, au moment d'ouvrir la boite, Brian Lundy découvre à l'intérieur un bloc de bois taillé dans la même forme que la console.
Cerise sur le gâteau, un dessin sexuel, doublé d'un message insultant avait été rajouté sur la surface du bois par le voleur. On imagine assez facilement la déception du garçon de 9 ans, dont le Noël a été ruiné, mais également celle des parents qui ont dépensé plusieurs centaines de dollars pour un bout de bois assorti d'un dessin de pénis.
PS4 en bois
L'histoire s'est cependant bien terminée, puisque le magasin Target incriminé a échangé la fausse console contre une vraie, assortie de 100 dollars de bon d'achat et de la compilation Uncharted : The Nathan Drake Collection. Néanmoins, les responsables du magasin ont expliqué que « c'est quelque chose qui arrive de temps à autre ». Un voleur inventif et un peu de malchance peuvent « ruiner l'esprit de Noël », a résumé auprès de la chaîne Fox 25 la belle-mère de l'enfant. On peut malgré tout reconnaître que le faussaire a particulièrement soigné sa copie en bois : on est bien loin de la photo de la Xbox One qu'un père de famille avait reçu pour Noël 2013, après s'être fait avoir par une annonce frauduleuse sur eBay !

Réagissez à cet article

Source : *Il achète une PS4 pour Noël et se retrouve avec un morceau de bois*

Augmentation de la cybercriminalité encore prévu pour 2016

	**Augmentation de la cybercriminalité encore prévu pour 2016**

Le nombre de piratages informatiques a substantiellement augmenté en 2015, une tendance qui devrait encore s'affirmer en 2016. Chefs d'Etat, groupes industriels, médias, banques, petites entreprises ou particuliers, personne n'est à l'abri de la menace.

Si les cyber-attaques (attaques informatiques, ndlr) ont augmenté durant l'année 2015 en France et dans le monde, la tendance ne semble pas près de s'atténuer en 2016. C'est la mise en garde prononcée par de nombreux organismes, dont le Cercle européen de la sécurité et des systèmes d'information. Cet organe, qui fédère les professionnels du secteur de la sécurité informatique, redoute un cyber-sabotage de grande ampleur en 2016.
Difficile cependant de cerner le danger car il vient de partout, emploie des formes diverses et peut toucher tout le monde, directement ou pas. A grande échelle, une attaque déclenchée à distance peut viser des objectifs affectant des bassins entiers de population : réseau électrique, distribution de l'eau, contrôle de la circulation, trafic aérien. Ou encore s'en prendre à des organismes gouvernementaux avec les conséquences que cela implique.

Des attaques en forte hausse

L'Allemagne a eu affaire à ces deux types d'attaques ces douze derniers mois: la mise hors service par deux fois d'un haut-fourneau dans la Sarre et le piratage de l'ordinateur personnel d'Angela Merkel. En France, l'exemple le plus spectaculaire remonte au printemps dernier quand la chaîne francophone TV5Monde (257 millions de foyers à travers le monde) a carrément cessé d'émettre durant plusieurs heures après une attaque perpétrée par Daech.

TV5 Monde avait été ouvertement ciblée par Daech. REUTERS/Benoit Tessier

A moyenne échelle, les malfaiteurs peuvent s'en prendre à une entreprise pour lui voler des données ou gripper son système informatique. Le cabinet PricewaterhouseCoopers révélait en octobre dernier que les cyber-attaques contre les entreprises avaient progressé de 38 % en un an dans le monde et de 51 % en France alors que les pertes financières s'élevaient à 3,7 millions d'euros par entreprise victime d'attaque en moyenne. Il faut noter que plus d'un tiers des sources d'incident provient d'employés de la compagnie attaquée.
A plus petite échelle, les particuliers sont touchés par des escroqueries en tout genre, à la carte de crédit par exemple. Ainsi, un rapport récent de Norton/Symantec révélait qu'un Français sur cinq s'était fait dérober ses données bancaires après un achat en ligne. Le phénomène est tellement répandu que les banques ont peut-être trouvé la parade, du moins provisoirement : le cryptogramme dynamique qui change toutes les 20 minutes, un identifiant qui va commencer à figurer au dos des cartes de crédit en 2016.

De plus en plus sophistiqués

Les hackers, remarquent les professionnels, utilisent des méthodes de plus en plus sophistiquées pour fracturer les systèmes informatiques de leurs cibles. Dans un rapport récent, l'entreprise de sécurité informatique roumaine Bitdefender identifiait des évolutions notables pour 2016. La première touchait aux systèmes de monétisation publicitaires et en particulier les systèmes de blocage de publicité qui pourraient être utilisés par les pirates informatiques pour développer de nouvelles souches de logiciels malveillants.
D'après Bitdefender, le monde de l'entreprise va être encore plus touché en 2016 à travers des attaques ciblées visant essentiellement le vol d'informations. Mais les individus aussi seront plus vulnérables, en partie du fait de la multiplication des objets connectés qui recèlent de nombreuses failles de sécurité exploitables par les cybercriminels. Même des systèmes d'exploitation réputés plus sûrs, comme le Mac OS X d'Apple, ne seraient plus à l'abri d'être percés par les malfaiteurs en ligne, selon Bitdefender.

Réagissez à cet article

Source : *La cybercriminalité devrait encore augmenter en 2016 – France – RFI*

Au bout du compte, combien de secondes fait gagner la high-tech ?

Au bout du compte, combien de secondes fait gagner la high-tech ?

Capteurs électroniques, fibre de carbone, combinaisons en polyuréthane, eyetracking… Jusqu'à quel point la technologie permet-elle aux sportifs de dépasser leurs limites… tout en restant humains ?

Quoi ? Vous vous êtes équipé des applications Nike + Running, STT Sport Tracker ou Micoach d'Adidas, et vous n'avez pas encore battu le record du 100 mètres ? C'est normal. Ces applications n'ont pas pour but de vous transformer en Usain Bolt, mais de vous permettre de mieux gérer vos efforts, et de mesurer vos progrès.

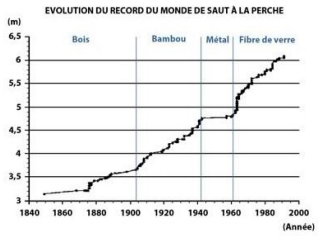
Reste que la technologie a toujours joué un rôle pour améliorer les performances sportives, et faire gagner des centimètres ou des secondes. C'est que la technologie peut améliorer les records grâce à trois facteurs : la mesure de la physiologie, les vêtements de sport et la tenue portée, et les matériaux utilisés.

« L'eyetracking » pour garder l'oeil sur les performances

Pour la mesure des performances corporelles, l'institut des sciences du sport de Berne utilise par exemple l'eyetracking pour étudier « le comportement du regard, ainsi que ses répercussions sur le comportement décisionnel en situations sportives ». Mais la mesure n'a pas de limite : développé par la NASA pour ses astronautes, la « pilule thermomètre » peut être ingérée pour prendre en permanence la température du sportif en plein effort – puis être ensuite restituée par les voies naturelles.

Des « vêtements dopants » ?

Même les vêtements et accessoires peuvent « doper » la performance : ainsi, les combinaisons de nageurs en polyuréthane ont-elles été interdites en 2009, du fait de leur trop grande efficacité. Les scientifiques ont évalué en 2008 que ces tenues permettaient de gagner 1 à 2% sur le chronomètre, et les chercheurs de l'Institut de recherche biomédicale et d'épidémiologie du sport (Irmes) ont estimé que deux tiers des records du monde de natation battus depuis 2000 l'ont été grâce aux combinaisons.



Fibre de carbone, aluminium, graphite…

Quant aux matériaux, ils jouent bien sûr un rôle essentiel dans les gains de performance. La preuve chiffrée en a été apportée de manière éclatante dans la discipline du saut à la perche. Comme le montre le graphique ci-dessous, les perches en bois permettaient à peine de dépasser 3,5 mètres. Avec le bambou, on atteint 4,5 mètres. Le métal permet de tutoyer les 5 mètres et, avec la fibre de carbone, les records explosent, jusqu'à dépasser les 6 mètres.

En 2010, le cycliste Fabian Cancellara a défrayé la chronique parce qu'il utilisait un pédalier optimisé (qui réduit les forces de frottement par un roulement à billes de graphite et huile) qui lui faisait gagner 2 secondes au kilomètre. Toujours dans le cyclisme, l'utilisation d'un cycloergomètre (vélo immobile servant à des mesures scientifiques) a montré que le plateau de type Harmonic permet une augmentation significative de la puissance maximale développée (+ 3%) lors d'un sprint ou d'une montée.

Bien entendu, les prothèses du coureur amputé Oscar Pistorius présentent un cas extrême. Non seulement elles lui permettaient de courir, mais elles furent accusées de lui offrir un avantage face à ses rivaux : une expertise a révélé que l'énergie restituée par les prothèses lors de la poussée était quasiment trois fois plus élevée que celle des chevilles humaines – au point qu'en janvier 2008, l'Association internationale des fédérations d'athlétisme lui a interdit de participer avec les valides aux jeux de Pékin.

La prochaine étape ? Sans doute des capteurs électroniques ou des régulateurs d'hormones greffés en permanence, qui brouilleront les frontières entre les sportifs et les cyborgs…

Réagissez à cet article

Source : *Big Data : La high-tech fait-elle gagner des secondes ?*

Plus fort que les cookies, découvrez les super-cookies

Plus fort que les cookies, découvrez les super-cookies

Dans un précédent bulletin d'actualité [1], était présenté comment les cookies HTTP (ou témoins de connexion), pouvaient être utilisés à des fins de profilage de l'utilisateur, dans le but notamment de pouvoir lui proposer du contenu ciblé. Après un bref rappel, cet article se propose de parcourir plus largement les mécanismes complémentaires existants à l'heure actuelle, à des fins de sensibilisation aux problématiques de vie privée sur l'Internet, et dans l'optique de permettre la prise des précautions d'usage adaptées à son utilisation au quotidien, dans un contexte professionnel comme personnel.

Techniques de pistage – Cookies – et évolutions

La technique la plus utilisée en matière de pistage d'utilisateurs sur l'Internet repose sur l'exploitation des cookies. Nous rappelons que le terme cookie désigne une variable utilisée par un serveur HTTP pour sauvegarder des informations sur la session HTTP courante. Il est composé d'une paire obligatoire nom/valeur, et d'attributs optionnels, comme la date d'expiration, le domaine et le chemin. Ces informations sont créées et mises à jour lors des échanges entre un serveur et un client Web grâce à des en-têtes dédiés du protocole HTTP (« Set-Cookie », « Cookie ») [2].
Le premier cas d'usage des cookies est tout à fait nécessaire à la navigation sur de nombreux sites Web, par exemple pour le maintien d'une session applicative ou la mémorisation d'un panier d'achats, on parle alors de « cookies de premier niveau ». Il existe cependant d'autres cas d'utilisations controversés sur le plan du respect de la vie privée. En particulier, l'usage de « cookies tiers » (ou « tierce partie ») [1], notamment dans l'optique d'établir des statistiques de consultation, peut permettre par exemple d'offrir des services de publicité ciblée. Ces cookies sont reconnaissables en particulier à leur domaine d'appartenance différent de celui de la page consultée, et peuvent parfois permettre d'identifier finement un utilisateur donné (par exemple cookies Google).

D'autres mécanismes permettent la conservation de données utilisateur, qui exploitent d'autres modes de création et de stockage que les cookies HTTP. On regroupe généralement ceux-ci sous le terme « supercookie ». Ils s'appuient notamment sur l'utilisation :
• mécanismes de stockage local dédiés à des applications Web au-dessus du protocole HTTP, comme Adobe Flash (« Local Shared Objects », également appelés « cookies Flash »), Microsoft Silverlight (« Silverlight Isolated Storage ») ou encore HTML5 (« HTML5 storage ») ;
• d'objets dans le contenu des pages Web, comme la propriété « window.name » en JavaScript, qui peut être détournée pour stocker temporairement des informations ;
• du cache du navigateur et de l'historique de navigation, pour stocker sous forme encodée des informations ;
• de HSTS (« HTTP Strict Transport Security ») [3], mécanisme de politique de sécurité pour HTTP, permettant à un serveur de demander le passage vers HTTPS via un champ d'en-tête HTTP (« Strict-Transport-Security »), mais dont une utilisation détournée permet à tiers contrôlant plusieurs domaines d'identifier de façon unique un utilisateur [4].

Cette liste, non exhaustive, montre bien qu'il existe de nombreuses façons de stocker des données issues de la navigation Web, et qu'un simple nettoyage des cookies HTTP via le navigateur ne peut pas suffire à effacer proprement l'ensemble de celles-ci. D'ailleurs, on parle de « cookie zombie » pour désigner des cookies HTTP qui sont régénérés après leur suppression grâce à l'utilisation des supercookies. L'application Evercookie [5], par exemple, illustre cela, permettant la propagation des cookies HTTP dans autant que mécanisme de stockage que possible afin d'assurer la résilience de l'information.

Autres techniques
Si les cookies (et assimilés) permettent d'obtenir une masse d'informations très intéressante, ils ne sont pas pour autant la seule source considérée par les entités cherchant à pister l'utilisateur. Il existe en particulier de nombreuses autres méthodes permettant d'identifier de façon unique un utilisateur, parfois à la granularité du terminal utilisé (téléphone, ordinateur, téléviseur connecté, tablette, etc.).
Ces méthodes peuvent être classées en cinq catégories [6] :
• entification générée par le client : certains terminaux ou applications clientes génèrent un identifiant unique pouvant être accessible par les services tiers à des fins publicitaires (advertising identifiers).
• Identification via des éléments réseau : certains équipements réseau situés entre le client et le serveur insèrent des éléments permettant, volontairement ou non, d'identifier l'utilisateur. Par exemple, l'utilisation du champ « X-Forwarded-For » dans l'en-tête HTTP précise l'adresse IP d'origine d'un client se connectant à travers un serveur mandataire.
• Identification par le serveur : certains serveurs ajoutent des pixels-espions [7], images de très petite taille généralement non repérables par l'utilisateur, qui permettent la génération de cookies tiers.
• Identification unique : certains services permettent à l'utilisateur de s'authentifier pour accéder à un ensemble de ressources (sites, applications), induisant ainsi la création d'un identifiant unique, censé faciliter la navigation (unique portail d'authentification, gestion des préférences utilisateur, etc.). On peut citer par exemple Facebook Connect, Windows Live ID, Google Account, etc.
• Identification statistique : certaines données issues du navigateur, de l'application ou encore du système d'exploitation permettent le calcul d'une empreinte entraînant la capacité à singulariser l'utilisateur. Ce calcul peut par exemple s'appuyer sur le User-Agent, la valeur du champ HTTP Accept, la politique de gestion des cookies, la résolution de l'écran, ou encore les extensions installées [8].

La directive 2002/58 du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques [9][10] précise que l'utilisation de cookies est autorisée à condition que l'utilisateur se voie donner des informations claires et précises sur la finalité de ces cookies ainsi que les informations placées sur l'équipement terminal qu'il utilise. L'utilisateur pourra refuser l'utilisation de ces dispositifs, cependant cette disposition ne fait pas obstacle au stockage de données utilisées à des fins exclusivement techniques.
Techniquement, des solutions amont ont été proposées, comme l'en-tête HTTP « Do Not Track » (DNT, 2009), pour permettre d'indiquer à un site web qu'un utilisateur ne souhaite pas être tracé. Cependant, bien qu'intégré dans tous les navigateurs modernes, il est purement déclaratif et peut être ignoré par le site visité.
D'un point de vue pratique, une des solutions les plus simples afin de limiter ces traces est de bloquer les cookies tiers. Ces cookies ne sont généralement pas utiles pour la navigation et il est recommandé de les refuser par défaut [11].
Enfin, de nombreuses extensions pour navigateur permettent de limiter le suivi d'un utilisateur existant. Elles ont principalement pour effet :
• blocage des traceurs (DoNotTrackME, Disconnect, uBlock Origin, AdBlock),
• le blocage des scripts (NoScript, ScriptNo),
• la génération de fausses informations afin de brouiller le calcul des empreintes numériques (Random Agent Spoofer),
• le basculement automatique vers HTTPS si disponible (HTTPS Everywhere).

Références

Bulletin d'actualité CERTA-2010-ACT-005 (05 février 2010)
http://www.cert.ssi.gouv.fr/site/CERTA-2010-ACT-005/CERTA-2010-ACT-005.html
RFC 6265 (HTTP State Management Mechanism) (avril 2011)
https://www.rfc-editor.org/rfc/rfc6265.txt
RFC 6797 (HSTS) (novembre 2012)
https://tools.ietf.org/html/rfc6797##section-14.9
How HSTS supercookies make you choose between privacy or security (02 février 2015)
https://nakedsecurity.sophos.com/2015/02/02/anatomy-of-a-browser-dilemma-how-hsts-supercookies-make-you-choose-between-privacy-or-security/
Evercookie (github)
https://github.com/samyk/evercookie
IAB Cookie White Paper (janvier 2014)
http://www.iab.net/media/file/IABPostCookieWhitepaper.pdf
Web beacon (9 janvier 2014)
https://www.iab.net/wiki/index.php/Web_beacon
Browser uniqueness
https://panopticlick.eff.org/browser-uniqueness.pdf
Directive 2002/58/CE (12 juillet 2002)
http://eur-lex.europa.eu/legal-content/fr/TXT/?uri=CELEX:32002L0058
Sites web, cookies et autres traceurs (CNIL)
http://www.cnil.fr/vos-obligations/sites-web-cookies-et-autres-traceurs/que-dit-la-loi/
Conseils aux internautes (CNIL)
http://www.cnil.fr/vos-droits/vos-traces/les-cookies/conseils-aux-internautes/

Vulnérabilités critiques au sein de Juniper ScreenOS

Contexte

Le 18/12/2015, le CERT-FR a émis l'alerte CERTFR-2015-ALE-014 [1] concernant plusieurs vulnérabilités critiques impactant le système ScreenOS des équipements Juniper. D'après le bulletin de sécurité publié par Juniper [2], ces vulnérabilités ont été découvertes suite à un audit de code interne et auraient été introduites volontairement pour affaiblir la sécurité de ScreenOS. Il s'agit en l'occurrence de deux portes dérobées qui permettent de :
– contourner le mécanisme d'authentification en place au niveau des services SSH et Telnet,
– déchiffrer les communications entre un client et le service VPN d'un équipement Juniper vulnérable.

Marqueurs de détection

La société Fox-It propose des signatures au format Snort afin d'identifier toute tentative de connexion à un équipement Juniper vulnérable via la porte dérobée. Ces signatures sont cependant limitées au service Telnet. De plus, la vulnérabilité liée au service VPN étant exploitable après une interception passive du trafic chiffré, il n'est pas possible de détecter son exploitation.
Versions affectées
La porte dérobée permettant d'accéder à l'interface d'administration de l'équipement via le protocole Telnet ou SSH impacte le logiciel Juniper ScreenOS de la version 6.3.0r17 à 6.3.0r20.
La vulnérabilité permettant de déchiffrer les communications réseau liées au service VPN impacte le logiciel Juniper ScreenOS versions 6.2.0r15 à 6.2.0r18 et les versions 6.3.0r12 à 6.3.0r20.
Ces vulnérabilités permettant un accès illégitime sont respectivement référencées par les identifiants CVE-2015-7755 et CVE-2015-7756.

Description des portes dérobées

CVE-2015-7755
La porte dérobée permettant d'accéder à l'interface d'administration d'un équipement Juniper vulnérable est localisée au sein du code de vérification des identifiants de connexion. Ce code compare le mot de passe saisie par l'utilisateur avec une chaîne de caractère codée en dur dans le système ScreenOS. Si elles sont identiques, l'accès est autorisé.
CVE-2015-7756
La seconde porte dérobée reposait sur une faiblesse du générateur de nombres aléatoires utilisé par l'algorithme de chiffrement et permettait à un attaquant d'accéder au contenu des communications VPN, obtenues à partir d'une écoute passive du trafic réseau.

Corrections

Le CERT-FR recommande d'appliquer les mesures préconisées dans le bulletin d'alerte CERTFR-2015-ALE-014.

Documentation

1
Bulletin d'alerte du CERT-FR :
http://cert.ssi.gouv.fr/site/CERTFR-2015-ALE-014/index.html
2
Bulletin de sécurité de l'éditeur :
http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10713&cat=SIRT_1&actp=LIST
3
Versions de ScreenOS vulnérable :
https://isc.sans.edu/diary/Infocon+Yellow%3A+Juniper+Backdoor+(CVE-2015-7755+and+CVE-2015-7756)/20521
1 – Rappel des avis émis
Dans la période du 21 au 27 décembre 2015, le CERT-FR a émis les publications suivantes :
CERTFR-2015-ALE-015 : Campagne de messages électroniques non sollicités de type TeslaCrypt
CERTFR-2015-AVI-554 : Multiples vulnérabilités dans le noyau Linux de Debian
CERTFR-2015-AVI-555 : Vulnérabilité dans VMWare
CERTFR-2015-AVI-556 : Multiples vulnérabilités dans Citrix XenServer
CERTFR-2015-AVI-557 : Multiples vulnérabilités dans Cisco IOS et IOS XE
CERTFR-2015-AVI-558 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
CERTFR-2015-AVI-559 : Vulnérabilité dans Xen
CERTFR-2015-AVI-560 : Vulnérabilité dans Cisco IOS XE
CERTFR-2015-AVI-561 : Multiples vulnérabilités dans le noyau Linux de Fedora
CERTFR-2015-AVI-562 : Multiples vulnérabilités dans ISC Bind
CERTFR-2015-AVI-563 : Multiples vulnérabilités dans le noyau Linux de SUSE
Durant la même période, les publications suivantes ont été mises à jour :
CERTFR-2015-ALE-014-1 : Vulnérabilité dans Juniper ScreenOS (ajout de règles Snort dans les contournements provisoires.)
Gestion détaillée du document
28 décembre 2015 version initiale.
Dernière version de ce document : http://cert.ssi.gouv.fr/site/CERTFR-2015-ACT-052
CERT-FR
2015-12-28

Réagissez à cet article

Source : *Bulletin d’actualité CERTFR-2015-ACT-052*

Lourds investissements par les banques pour ne pas se faire pirater

	**Lourds investissements par les banques pour ne pas se faire pirater**

Pour ne pas se faire pirater, les banques investissent massivement dans la cybersécurité, souligne le Wall Street Journal dans une enquête datée du 20 décembre. Elles essayent également d'instaurer de bonnes pratiques chez leurs employés, responsables de 30% des fuites de données.

Les banques dépensent sans compter pour se défendre contre une armée invisible de hackers, qui essayent par tous les moyens de récupérer des données sur leurs clients et les énormes quantités de fonds qu'elles stockent sur leurs comptes.
Le patron de Bank of America, Brian Moynihan, a déclaré lors d'une conférence au mois de novembre que le budget cybersécurité de son entreprise était illimité, comme le rapporte le Wall Street Journal.
JP MORGAN INVESTIT 500 MILLIONS DE DOLLARS EN 2016 DANS LA CYBERSÉCURITÉ
Même topo pour l'américaine Wells Fargo, première banque mondiale en terme de valorisation boursière : « Nous dépensons un océan d'argent » dans la cybersécurité, a expliqué son PDG John Stumpf dans une interview récente, reprise par le média américain. Un porte-parole de la société a refusé de donner plus de détails sur les montants investis.
J.P. Morgan Chase a été victime en 2014 d'un piratage massif de données : 76 millions de clients étaient concernés par cette fuite d'informations sensibles. La banque américaine a considérablement renforcé son dispositif de cybersécurité. Elle va investir 500 millions de dollars pour se protéger contre les hackers en 2016, soit environ deux fois plus qu'en 2014, détaille le Wall Street Journal.

LA VULNÉRABILITÉ NUMÉRO UN DES BANQUES : LEURS SALARIÉS
Souvent, les hackers jouent sur la vulnérabilité numéro un des banques pour récupérer des informations sensibles : les salariés. Ils envoient notamment des messages de phishing (hameçonnage), demandant à leurs destinataires de cliquer sur un lien. Cela leur permet d'installer dans les ordinateurs ciblés des logiciels espions. J.P. Morgan a envoyé un faux mail de phishing à ses salariés, pour les tester. Résultat ? 20% d'entre eux ont mordu à l'hameçon…
En moyenne, 30% des fuites de données dans les entreprises sont liées à une erreur d'un salarié, selon une enquête diffusée en décembre par l'Association of Corporate Counsel, une association professionnelle d'avocats américains. Pour limiter les dégâts, les banques interdisent donc à leur salariés d'utiliser des clefs USB venues de l'extérieur, d'utiliser leur adresse mail personnelle pour s'inscrire à des services sur Internet (site de e-commerce par exemple).

NE PAS ALLER JUSQU'AU « FLICAGE »
Elles leur demandent aussi d'être vigilants par rapport aux informations qu'ils postent sur les réseaux sociaux. « Mais jusqu'où les banques peuvent-elles aller dans le 'flicage' de leurs salariés sur ces sites ? », s'interrogent les experts du secteur.
Impossible de poursuivre un collaborateur qui poste des photos de ses vacances sur son profil Facebook, même si cela pourrait permettre à un pirate de s'introduire à son domicile et de voler son ordinateur professionnel. Alors que faire ? Cette réflexion délicate doit être conduite par les institutions financières si elles veulent protéger au mieux les données sensibles de leurs clients.

Réagissez à cet article

Source : *Cybersécurité : Les banques investissent « un océan d'argent » pour ne pas se faire pirater*

Lelia de MATHAREL

L’histoire interdite du piratage informatique (Documentaire)

L’histoire interdite du piratage informatique (Documentaire)

Hacker
C’est au cours des années 80 que ce mot a été utilisé pour catégoriser les personnes impliquées dans le piratage de jeux vidéos, en désamorçant les protections de ces derniers, puis en en revendant des copies.
Aujourd’hui ce mot est souvent utilisé à tort pour désigner les personnes s’introduisant dans les systèmes informatiques.

Réagissez à cet article

Source : *[Documentaire] L’histoire interdite du piratage informatique – TrLoad.net | Download Info | Video | Global Music Video | Top Videos, Artist, Songs, Free Mobile Music Download*

Arnaques et usurpation de vos données personnelles sur internet au Burkina Faso

Arnaques et usurpation de vos données personnelles sur internet au Burkina Faso

Face à la multiplication des plaintes pour piratage de comptes mails, usurpation d'identités sur les réseaux sociaux, Facebook notamment, suivi d'arnaques ou de chantage, enregistrées par la Commission de l'Informatique et des Libertés (CIL), il me plaît de rappeler quelques bonnes pratiques à adopter pour éviter de tomber dans le piège des cyberdélinquants.

Ainsi, il convient de prendre les précautions suivantes :

• Ne pas répondre à un courrier électronique (mail) ou à un message dans lequel votre mot de passe, votre adresse mail, votre numéro de compte bancaire, etc. sont demandés pour quelque raison que ce soit ;

• Eviter de saisir ou communiquer ses informations personnelles confidentielles (mot de passe, coordonnées financières…) sur un ordinateur dont on n'a pas l'assurance qu'il est sécurisé ;

• Eviter d'accepter les invitations d'inconnus sur les réseaux sociaux, Facebook notamment ;

• Eviter d'échanger des contenus inappropriés (photos, vidéos intimes) sur les réseaux sociaux en général et sur Facebook en particulier ;

• Eviter de se connecter aux réseaux internet public (wifi ouvert, des aéroports, des salles de conférences…) ;

• Utiliser un logiciel anti-virus, activer le pare-feu pour un minimum de protection de vos ordinateurs personnels, veiller à leurs mises à jour.

La protection de vos données personnelles, notre préoccupation.
LA PRESIDENTE

Réagissez à cet article

Source : *Arnaques et usurpation de vos données personnelles sur internet : conseils (…) – leFaso.net, l'actualité au Burkina Faso*