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

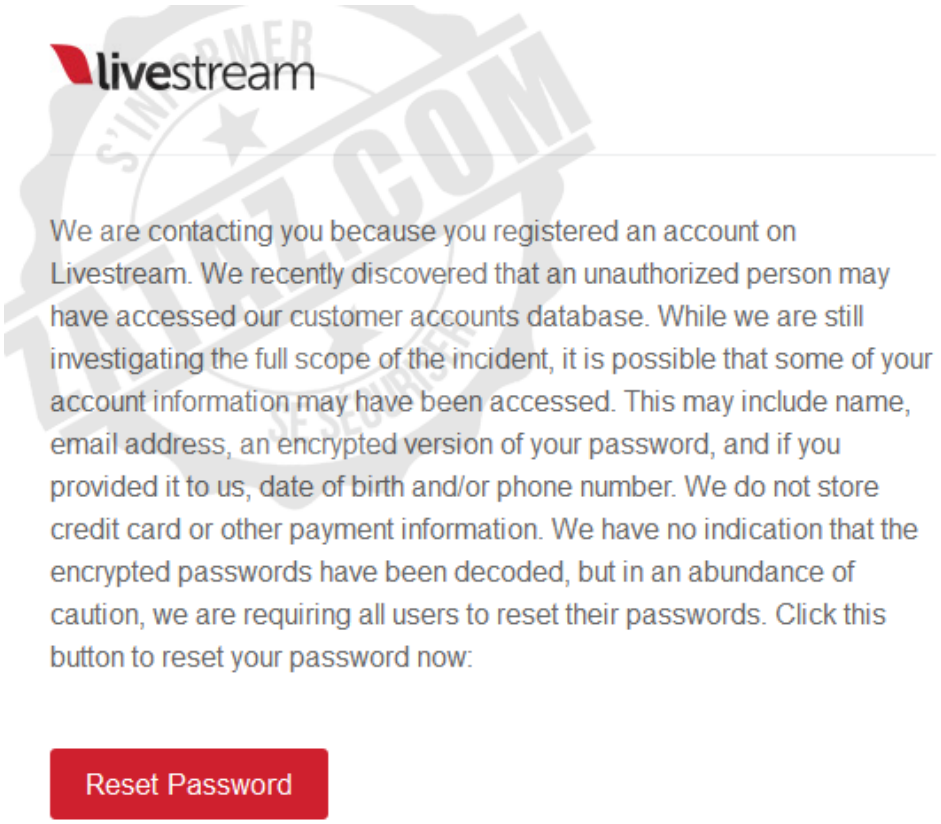
Source : *Du retard pour la plateforme nationale des interceptions judiciaires – Next INpact*

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*

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 !

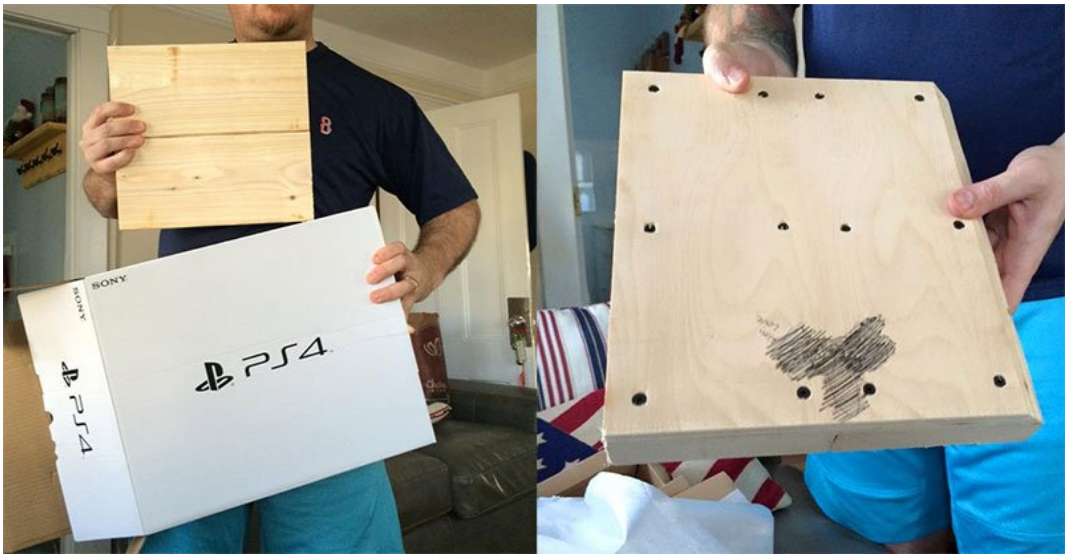
Réagissez à cet article

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*