L’UE parvient à un accord de principe sur la protection des données personnelles

L’UE parvient à un accord de principe sur la protection des données personnelles

Les États membres conservent toutefois à leur charge la question de déterminer l'âge minimum requis pour les mineurs sur les réseaux sociaux.

Après quatre ans d'âpres discussions, un accord de principe a finalement été trouvé mardi 15 décembre à Bruxelles, afin d'adapter la législation européenne sur la question de la protection des données personnelles à l'heure d'internet. Le texte a été validé à l'occasion d'une réunion associant le Parlement européen, la Commission et le Conseil, qui représente les Etats.
« L'UE aura désormais la législation la plus étendue de protection des données personnelles dans le monde », s'est réjouie l'eurodéputée Sophie in 't Veld (libérale). L'accord prend en compte la décision récente de la justice européenne qui a déclaré « invalide » le cadre juridique qui couvre le transfert par Facebook de données personnelles de l'UE vers les Etats-Unis, a-t-elle souligné.

Des entreprises inquiètes des sanctions

L'accord tente de faire la synthèse entre l'exigence de donner plus de moyens de contrôle aux citoyens quant à leurs informations personnelles et la nécessité d'harmoniser les législations des États membres afin de faciliter le travail des entreprises.
Parmi les autres points de discussion, figurait notamment le montant des amendes que devront payer les entreprises qui violent les règles européennes sur la protection des données. Au terme de l'accord, les géants d'internet pourraient se voir sanctionner à hauteur de 4% de leur chiffre d'affaires annuel mondial.
Quel âge minimum sur les réseaux sociaux?
Selon cet accord, les États membres pourront fixer librement « entre 13 et 16 ans » l'âge auquel un mineur peut s'inscrire sur des réseaux sociaux comme Facebook ou Snapchat, sans l'accord d'un parent, a indiqué l'Allemand Jan-Philipp Albrecht (Verts), rapporteur du Parlement européen sur la réglementation de la protection des données.
« Malheureusement, les États membres n'ont pas pu se mettre d'accord pour fixer une limite d'âge à 13 ans pour le consentement parental à l'utilisation de réseaux sociaux comme Facebook ou Instagram », a expliqué Jan-Philipp Albrecht, à l'issue d'une réunion associant le Parlement européen, la Commission et le Conseil, qui représente les Etats.
Le Parlement européen voulait fixer cette limite à 13 ans, soit l'âge minimum requis indiqué par Facebook, mais certains Etats membres s'y sont opposés.

Un accord contraignant

L'accord devra encore être confirmé par le Conseil européen et voté par le Parlement au début de l'année 2016. Il restera ensuite deux ans aux États membres pour le faire entrer en vigueur. L'accord, qui comprend un règlement et une directive, a vocation à s'imposer à tous les États membres.
En juin, les ministres européens de la Justice avaient déjà trouvé un accord sur la création d'un « guichet unique » compétent pour veiller à l'application des règles pour les transferts transfrontaliers de données personnelles collectées dans plusieurs pays de l'UE par des entreprises ou des plateformes internet comme Amazon, Google et Facebook.

Réagissez à cet article

Source : *Protection des données personnelles: l'UE parvient à un accord de principe*

Un tiers des salariés

communiquent des informations liées à son entreprise

Un tiers des salariés communiquent des informations liées à son entreprise

Les salariés prennent de plus en plus d'importance dans l'e-réputation RH de leur entreprise ! C'est ce que révèle l'infographie « Marque employeur : il est temps d'e-penser », produite par l'agence de marketing digital et éditorial Parlons RH, à partir de données croisées de différentes études.

33 % des salariés communiquent des informations liées à leur entreprise sur les réseaux sociaux.

Ce qui constitue une augmentation de 608 % en deux ans ! En tête des prises de parole par les salariés, 43 % des sondés communiquent des appréciations sur le management (+ 344 % en deux ans), 40 % discutent des appréciations sur la stratégie de l'entreprise (+ 640 % en deux ans) et 37 % portent des appréciations sur certains de leur collègues. Si les sentiments des salariés sont positifs ou neutres à 14 %, 6 % publient des avis négatifs sur l'entreprise.

Comment expliquer cette augmentation ? Les salariés possèdent une vie sociale virtuelle de plus en plus abondante. Surtout, seulement 29 % des salariés affirment qu'il existe une charte ou des règles internes sur l'usage des réseaux sociaux. 39 % des salariés affirment à l'inverse qu'il n'existe pas de charte ou de règles internes sur les réseaux sociaux, ou ne connaissent pas leur existence (34 %).

Pour plus de la moitié des sondés (60 %), les managers n'ont proposé aucune action concernant l'usage des réseaux sociaux. Seuls 21 % des managers ont proposé des formations, 9 % des réunions d'information, 6 % ont remis aux salariés un guide des bonnes pratiques et 4 % ont informé les salariés des risques pour l'entreprise.

Les avis influencent fortement les employés potentiels

Ces avis ont pourtant un fort impact sur la marque employeur, qui désigne la situation générale de l'e-réputation de l'entreprise pour ses salariés actuels, futurs et aux yeux de toutes les parties prenantes de l'entreprise. La marque employeur permet de rendre l'entreprise plus attrayante aux yeux de tous, et permet notamment de faciliter l'embauche.

Ainsi :

95 % des candidats se renseignent sur les entreprises avant de postuler.

4/5 des salariés ont déjà postulé après avoir lu des commentaires positifs en ligne sur une entreprise

1/3 des candidats refuserait un poste dans une entreprise à mauvaise réputation employeur.

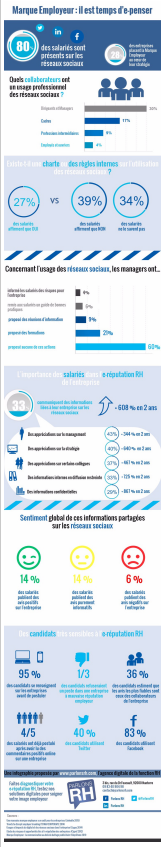
36 % des candidats estiment que les avis les plus fiables sur l'entreprise sont ceux des collaborateurs

Définir son identité et la diffuser efficacement sur lnternet permettraient ainsi d'embaucher plus facilement et d'avoir des salariés plus efficaces. Ce qui est important quand on sait qu'un recrutement raté coûterait entre 40 000 euros et 100 000 euros, selon Gwenaëlle Quénaon-Hervé, directrice générale adjointe du site Regionsjob.

Des outils et des méthodes existent pour l'utilisation des réseaux sociaux par les salariés

Même si des posts spontanés n'ont pas forcément objectif de nuire aux entreprises, les maitriser est aujourd'hui un enjeu de taille pour les sociétés afin d'éviter un bad buzz redoutable qui pourrait éloigner les meilleurs talents. Un point d'autant plus important que l'infographie explique que 80 % des salariés sont présents sur les réseaux sociaux.

D'où l'intérêt de sensibiliser et responsabiliser les employés pour en faire de véritables ambassadeurs pour les entreprises. Aux Etats-Unis, des programmes de sensibilisation des salariés se sont par exemple développés avec des fournisseurs de services et de logiciels qui aident les marques à responsabiliser les salariés dans les médias sociaux. Au programme : écoute ou surveillance des salariés, ou encore collaboration sociale, comme celle proposée par la société Jive.



Réagissez à cet article

Source : http://www.reputationvip.com/fr/blog/reseaux-sociaux-1-salarie-sur-3-communique-des-informations-liees-a-son-entreprise

Un pirate soupçonné du piratage de VTech arrêté

Un pirate soupçonné du piratage de VTech arrêté

Un jeune homme de 21 ans soupçonné d'être à l'origine du piratage des 6,4 millions de comptes d'enfants et 4,9 millions de comptes d'adultes, clients du fabricant de jouets VTech a été interpellé par la police britannique.

Suite au piratage des données personnelles de 11,3 millions de comptes clients du fabricant de jouet VTech, le plus grand vol de données concernant des enfants, la police anglaise indique avoir procédé à l'arrestation d'un jeune homme de 21 ans, soupçonné d'être à l'origine du délit. L'unité de cybercriminalité régionale du sud-est du Royaume-Uni a en effet indiqué dans un communiqué de presse ce mardi qu'elle avait arrêté un homme dans la ville de Bracknell, soupçonné d'avoir accédé sans autorisation aux serveurs et aux données de VTech. La ville, située à l'ouest de Londres, est un vivier pour les entreprises de haute technologie.
« Nous en sommes encore aux premiers stades de l'enquête et il y a encore beaucoup de travail à faire », indique Craig Jones, chef de l'unité de cybercriminalité régionale. Plusieurs équipements informatiques ont été saisis par la police.
Basée à Hong Kong, la société VTech est spécialisée dans les jeux ludo-éducatifs et propose depuis plusieurs années des tablettes tactiles adaptées aux enfants. Début décembre, elle avait été obligée de révéler que les données personnelles stockées dans les comptes de 6,4 millions d'enfants et 4,9 millions adultes avaient été copiées. Près de la moitié des victimes vivent en Europe.

Réagissez à cet article
Source : http://www.lemondeinformatique.fr/actualites/lire-la-police-britannique-a-arrete-le-hacker-presume-des-clients-vtech-63293.html

Safe Harbor : les CNIL

européennes doivent choisir entre force ou faiblesse

Safe Harbor : les CNIL européennes doivent choisir entre force ou faiblesse

Sans base légale mais en acceptant de prendre « un risque », les CNIL européennes ont donné jusqu'à fin janvier à l'Union européenne et aux États-Unis pour s'accorder sur un autre cadre permettant l'export de données personnelles vers les USA. Mais l'ultimatum ne sera visiblement pas respecté, et les autorités administratives hésitent sur l'attitude à adopter, entre diplomatie, force ou faiblesse.

C'est dans une position délicate que la Cour de justice de l'Union européenne (CJUE) a plongé la CNIL et ses homologues du G29, lorsqu'elle a décidé le 6 octobre dernier d'invalider le Safe Harbor, qui permettait aux entreprises américaines comme Facebook d'importer chez elles les données des internautes européens. La plus haute juridiction de l'Union a de fait obligé les autorités de protection des données à choisir entre leur mission officielle de protection de la vie privée des citoyens, et leur contrainte officieuse de ne pas bloquer l'activité économique liée à l'exploitation des données personnelles.
Dans un arrêt protecteur des droits de l'homme tel que la CJUE les multiplie ces dernières années concernant Internet, la Cour a en effet jugé que les conditions n'étaient plus réunies pour être certain que les États-Unis respectent en droit et en fait la bonne protection des données personnelles des internautes européens traitées sur le sol américain. Elle a donc invalidé avec effet immédiat le Safe Habor qu'utilisaient des milliers d'entreprises américaines, dont Facebook, Google, ou Microsoft, ce qui aurait dû conduire à bloquer immédiatement tous les transferts de données vers les États-Unis, au moins le temps que les dossiers fondés sur d'autres mécanismes juridiques soient vérifiés et validés.

Or la CNIL et ses homologues ont décidé, sans aucune logique juridique mais par choix politique et pragmatique, d'octroyer aux États-Unis et à la Commission européenne un ultimatum fixé au 31 janvier 2016 pour négocier un nouveau Safe Harbor 2.0 assorti de nouvelles législations protectrices aux USA. « Quand nous avons appelé à une période de transition jusqu'en janvier, c'était un risque que nous avons pris ensemble. (…) Nous avons décidé de cette phase de transition afin de permettre à tous les acteurs du secteur de prendre leurs responsabilités », reconnaît aujourd'hui la présidente de la CNIL Isabelle Falque-Pierrotin, dans une interview à Euroactiv.

« Les transferts de données ne continueront pas à n'importe quel prix »

Mais les négociations traînent, et les États-Unis n'ont toujours pas proposé de législation qui permettrait notamment aux Européens de faire valoir leurs droits contre la NSA, lorsque celle-ci accède à leur données sans contrôle judiciaire. En principe, le Safe Harbor 2.0 (s'il aboutit) ne devrait donc pas être plus sécurisant que l'ancien, et n'aura aucune validité pour légaliser les transferts des données.

Interdire les transferts ? L'arme atomique

La menace de l'arme atomique de la suspension des transferts de données, brandie notamment en Allemagne, est donc théoriquement existante. Mais la CNIL peine à (se) convaincre d'une intention de l'utiliser, tant les enjeux économiques sont forts. « Nous souhaitons tous que les transferts de données continuent, parce qu'ils sont associés à des intérêts économiques et politiques très importants. Mais ils ne continueront pas à n'importe quel prix », prévient ainsi Mme Falque-Pierrotin.

Alors que le G29 avait demandé que des solutions juridiques soient trouvées avant la fin janvier 2016, le groupe se contente désormais d'exiger « un geste politique ».
« Je ne sais pas s'il sera possible de finaliser tout cela avant fin janvier, mais nous devons au moins recevoir un signe qu'ils ont compris le message des juges. Il ne s'agit pas de produire un Safe Harbor numéro deux. Il faut réellement tenir compte des arguments du juge, qui s'inquiète de la protection des données des citoyens européens aux États-Unis, quand les services de renseignement y ont accès », prévient la présidente du groupe des CNIL européennes.
Rendez-vous fin janvier pour voir quelles mesures seront effectivement prises.

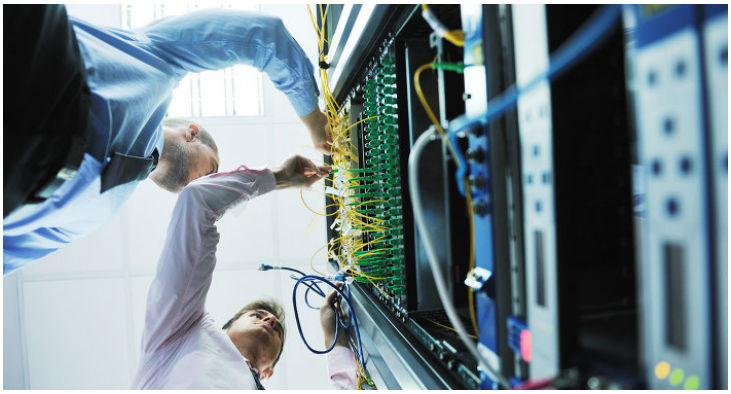
Réagissez à cet article
Source : http://www.numerama.com/politique/134571-cnil-europeennes-safe-harbor-diplomatie-faiblesse.html

La fin des cartes bancaires est-elle proche?

La fin des cartes bancaires est-elle proche?

D'ici 5 ans, selon les prévisions, il n'y aura plus ni argent liquide, ni cartes bancaires. Ces changements marqueront un tournant dans notre quotidien. De même que dans la cybercriminalité.

En 2015, les pertes de la Russie liées à la cybercriminalité s'élèveront à un milliard de dollars, a déclaré le vice-président de la direction de la banque russe Sberbank Lev Khassis, ajoutant que dans 5-7 ans la carte bancaire, telle qu'on la connaît aujourd'hui, n'existerait plus. Pour payer, on utilisera alors différents appareils mobiles.



© FOTOLIA/ .SHOCK
La NSA disposerait d'un nouveau logiciel espion

Les pays scandinaves ont déjà l'intention de tenir un référendum pour arrêter l'usage de billets de banque. Leur réponse positive débouchera sur la disparition des distributeurs de billets.
« Les changements n'auront pas lieu dans tous les pays à la fois, estime Evgueni Kaspersky, directeur général de Kaspersky Lab. L'argent liquide se maintiendra au cours des cinq prochaines années. Tour à tour, les pays pourraient en outre interdire l'usage des bitcoins en tant que crypto-monnaie », remarque-t-il.
La monnaie virtuelle (bitcoin) et l'argent liquide auront la même popularité auprès des escrocs, estime Kaspersky. Par exemple, les rançons pour piratage des systèmes informatiques sont exigées en cybermonnaie. En Russie, le bitcoin est interdit, ce qui ne signifie pas le refus de la technologie elle-même. Les institutions financières adoptent à l'heure actuelle la technologie qui est actuellement utilisée par les créateurs de la crypto-monnaie.

« C'est une technologie géniale. On peut l'utiliser pour les transactions intra-bancaires. Elle peut aussi être utilisée pour l'identification des internautes », dit Kaspersky.

© FLICKR/ BTC KEYCHAIN
Une nouvelle monnaie va voir le jour en Europe

Le retrait de la circulation du papier monnaie marquera un vrai tournant dans la cybercriminalité: les escrocs s'installeront désormais sur Internet et le nombre de cyberattaques va augmenter. En 2015, on en enregistrait déjà 300 en moyenne chaque jour.
Une autre tendance de l'année 2015 qui perdurera en 2016 est l'essor du nombre des bandes des cybercriminels prêtes à attaquer différents systèmes opérationnels pour voler de l'argent ou espionner la personne en téléchargeant l'information. « La législation sur la cybercriminalité est insuffisante », estime M. Khassis.

Réagissez à cet article
Source : http://fr.sputniknews.com/economie/20151210/1020180651/carte-bancaire-bitcoin-cybercriminalite.html

La face cachée du Web caché, le « dark Web »

	La face cachée du Web caché, le « dark Web »

Le «dark Web», dont les utilisateurs sont anonymes et intraçables, est utilisé, pour le pire et pour le meilleur, par des trafiquants d'armes autant que par des dissidents opprimés par les États totalitaire.

«Sur Internet, on peut acheter une kalachnikov en deux clics.» Pour qui n'y connaît rien, ce genre de phrases, entendues à la radio ou à la télévision, interroge.

Depuis les attentats de janvier notamment, Internet (1) est au cœur des préoccupations. «Dans quelle mesure, Internet et le Web profond sont-ils utilisés pour recruter, communiquer et préparer des actions criminelles?», interrogeait Nathalie Goulet, présidente de la commission d'enquête sénatoriale sur les réseaux djihadistes, lors d'une table ronde fin janvier.

Web profond, Web sombre ou dark Web… Tous ces termes renvoient à une même idée: il existerait un espace sombre, caché et donc suspect, dans lequel chacun pourrait, en quelques minutes, se procurer une arme ou de la drogue. De fait, à première vue, la chose n'est pas bien compliquée.

Pour commencer, il faut télécharger sur son ordinateur un navigateur personnalisé, libre et gratuit, comme TOR par exemple (pour The Onion Router). Ses paramètres permettent la connexion au réseau TOR. L'intérêt? Alors qu'habituellement, un utilisateur surfant sur Internet dispose d'une adresse IP, sorte de plaque d'immatriculation de son ordinateur, TOR brouille l'adresse IP de l'utilisateur.

«Les criminels ont recours à ce type de technologie pour anonymiser leurs échanges d'informations, ne pas être identifiés ni localisés, et de ce fait, ne pas être inquiétés par les forces de l'ordre, explique Solange Ghernaouti, directrice du Swiss Cybersecurity Advisory & Research Group, à l'Université de Lausanne. En rendant impossible la surveillance ou les filatures numériques, TOR permet l'anonymat et d'avancer masqué dans l'Internet.»

Une fois sur TOR, pas de moteur de recherche. Sur TOR, on ne trouve que ce que l'on sait chercher: il faut directement taper l'adresse du site souhaité dans la barre d'adresse. Pourquoi? Pour comprendre ce point, il faut s'imaginer Internet comme un iceberg. La partie immergée, la plus connue, est celle où nous avons l'habitude d'aller et dont les pages sont agrégées par des moteurs de recherche, comme Google. On y lit nos mails, on y achète des produits, on y fait des recherches… C'est l'Internet «surfacique», une petite partie d'Internet.

Sous la surface, on trouve le Web profond, qui contient les pages non indexées par les moteurs de recherche parce qu'elles sont mal conçues, non reliées, protégées par leur créateur… C'est le même Internet, mais en moins balisé.

Enfin vient le dark Web, ou plutôt les dark Nets, c'est-à-dire un ensemble de réseaux virtuels privés et décentralisés, constitués par des internautes qui se connectent entre eux.

Comment donc trouver une arme quand on n'y connaît rien? En récupérant des adresses de sites sur des forums, entre initiés. Ou grâce à des annuaires collaboratifs, référençant des adresses sous forme thématique, comme The Hidden Wiki (le «wiki» caché). Voulez-vous acheter un passeport? Rendez-vous à telle adresse. Des armes, de la drogue? Ce sera par là. Ainsi, on peut rapidement trouver un passeport français pour 600 € ou un pistolet SIG Sauer de calibre 9 mm pour 790 €.

Concrètement, pour acheter sur le dark Net, il a fallu à peine plus de deux clics: rechercher des adresses sur un annuaire, télécharger TOR, le lancer puis rentrer l'adresse dans la barre de navigation.

De là à acheter le produit, il reste encore quelques pas… Sur le dark Net en effet, les prix sont donnés en euros, mais les achats se font en bitcoins, une monnaie virtuelle et chiffrée, échangée entre deux ordinateurs. Datant de 2009, ce système fonctionne sans les États et sans les banques. Il est possible d'acheter ou de vendre des bitcoins contre des devises ayant cours légal, sur des plates-formes en ligne. Payer en bitcoin permet donc d'effectuer des transactions de personne à personne dans le monde entier, sans intermédiaire et à moindres frais. Ces échanges sont publics mais anonymes. Une fois son porte-monnaie approvisionné, il reste à se créer un compte client, comme sur eBay ou Amazon.

Mais attention, comme sur le Web surfacique, les escroqueries prolifèrent: sans régulation, ni contrôle, difficile de savoir si l'on peut faire «confiance» à un vendeur. De plus, les adresses changent sans arrêt, pour des raisons pratiques, techniques ou de sécurité, les rendant rapidement obsolètes.

Au final, le dark Web reste donc le domaine des initiés et des mafieux. D'ailleurs, alors qu'Internet compte cinq milliards d'utilisateurs, TOR en compterait deux millions quotidiens. Parmi eux, plusieurs profils. Il y a, bien sûr, les délinquants, trafiquants, hors-la-loi, parfois les mêmes que l'on retrouve dans le monde réel. Pour eux, Internet est un «facilitateur de la performance criminelle», selon Solange Ghernaouti: «Internet reflète notre réalité sociale, économique, politique et criminelle, poursuit-elle. Il n'est ni pire ni meilleur, mais contribue à faciliter certaines actions, y compris le passage à l'acte criminel du fait de la dématérialisation – on agit caché derrière un écran – à distance.»

Mais on trouve aussi sur le dark Net tous ceux qui veulent communiquer à l'abri des regards, les «internautes soucieux de préserver leur vie privée et leur intimité numérique ou les cyberdissidents à des régimes non démocratiques», poursuit le professeur. Tout un volet positif du dark Net, mais dont on parle beaucoup moins.

———

LES MOTS POUR COMPRENDRE

Internet représente un réseau de télécommunication international reliant des ordinateurs à l'aide du protocole TCP/IP. Il sert de support à la transmission de données: pages Web, courriels, fichiers informatiques.

Une adresse IP (Internet Protocol) est un numéro d'identification attribué à chaque appareil connecté à un réseau informatique utilisant l'Internet Protocol. Une adresse IP est un numéro unique permettant à un ordinateur de communiquer dans un réseau.

Un moteur de recherche est un site Internet régi par une application sur lequel, en entrant des mots-clés, on obtient une liste de sites correspondant à la demande. Exemple: Google.

Un réseau virtuel privé est un passage ou un lien qui permet d'ouvrir un réseau local vers l'extérieur et de le connecter à un autre réseau local, grâce à une connexion Internet et avec une sécurité optimisée.

Le wiki est une application Web participative dont les internautes peuvent modifier les contenus.

Le terme bitcoin (de l'anglais « bit », unité d'information binaire, et « coin », pièce de monnaie) désigne à la fois un système de paiement virtuel et l'unité de compte utilisée par ce système.

Le chiffrement est une technique d'écriture en langage crypté ou codé. C'est une des disciplines de la cryptologie s'attachant à protéger des messages (assurant confidentialité, authenticité et intégrité) en s'aidant de clés.

Réagissez à cet article

Source : http://www.la-croix.com/Ethique/Sciences-Ethique/Sciences/La-face-cachee-du-dark-Web-2015-12-08-1390141

Donald Trump veut fermer Internet

	**Donald Trump veut fermer Internet**

Alors qu'il multiplie les prises de parole publiques, Donald Trump, candidat à la présidentielle des Etats-Unis pour 2016, a récemment tenu des propos assez radicaux vis-à-vis d'Internet.

Pour le milliardaire américain Donald Trump, tout est bon pour se faire remarquer. L'homme a l'ambition de remplacer Barack Obama à la tête des Etats-Unis et souhaite ainsi devenir le candidat du parti républicain. Si on n'abordera pas en détails les opinions conservatrices du milliardaire, ses propos sur Internet sont assez tranchés.

On a des enfants qui regardent Internet.(…) Et on se demande pourquoi on perd tous ces enfants qui partent la-bas (…) et qui veulent rejoindre l'Etat islamique (…) A cause d'Internet on a perdu beaucoup de gens.

On doit faire quelque chose. On doit aller voir Bill Gates et plusieurs autres personnes qui comprennent réellement ce qu'il se passe et leur demander de fermer Internet dans certains endroits. Les gens diront « liberté d'expression ! liberté d'expression ! ». Ces gens sont stupides. On a beaucoup de gens stupides. On doit faire quelque chose à propos d'Internet parce qu'ils recrutent des milliers de gens.

Donald Trump s'en est par ailleurs pris à Jeff Bezos, fondateur et PDG d'Amazon. Via trois messages publiés sur Twitter, l'homme estime que M. Bezos utilise le *Washington Post*, racheté en août 2013 et déficitaire, pour éviter de payer des taxes trop élevées. Face à ces agressions, Jeff Bezos a ironiquement répondu qu'il l'enverrait loin dans l'espace sur sa fusée Blue Origin.

Réagissez à cet article

Source : http://pro.clubic.com/technologie-et-politique/actualite-788798-donald-trump-gate.html##pid=22889469

Les tendances 2016 en cyber-sécurité

Les tendances 2016 en cyber-sécurité

Comme la plupart des professionnels de la sécurité informatique, je souhaite vraiment que mes prédictions ne se réalisent pas. Je préférerais que les entreprises ne soient ni piratées ni victimes de failles. Mais en prédisant la prochaine vague de menaces, nous espérons aider les entreprises à rester au fait de l'évolution des tactiques et des méthodes que les criminels vont utiliser pour les cibler. Voici dix menaces et tendances que nous devrions constater au cours de 2016 en matière de sécurité informatique.

Si une semaine peut sembler longue en politique, comme l'a observé l'ancien Premier ministre britannique Harold Wilson, une année dans le domaine de la cyber-sécurité peut ressembler à une éternité. Malgré les changements rapides, beaucoup de choses restent cependant constantes. Les trois principales menaces prévues par Check Point pour 2015 étaient la croissance rapide des logiciels malveillants inconnus, les menaces mobiles et les vulnérabilités critiques dans les plates-formes couramment utilisées (Android, iOS et autres). Ces prédictions se sont pleinement réalisées et ces menaces continueront certainement de poser nombreux problèmes. Le jeu du chat et de la souris qui a caractérisé la cyber-sécurité au cours des dernières années se poursuit. Les pirates tentent de trouver sans cesse de nouvelles manières d'attaquer les réseaux, comme le montrent les failles de cette année chez Anthem, Experian, Carphone Warehouse, Ashley Madison et TalkTalk.

Logiciels malveillants « sniper »
Les plus grandes failles de 2016 seront le résultat de logiciels malveillants conçus sur mesure pour franchir les défenses d'entreprises spécifiques, telles que lors des attaques menées contre TV5 Monde. Les attaques génériques à champ large continueront de menacer les utilisateurs individuels et les petites entreprises, et les pirates amélioreront leurs méthodes d'attaque contre les grandes entreprises qui disposent de postures de sécurité plus sophistiquées. Ils utiliseront des méthodes de phishing plus approfondies et plus sophistiquées, et d'autres astuces d'ingénierie sociale pour accéder aux systèmes et aux données qu'ils souhaitent.

Les terminaux mobiles en 1ère ligne des attaques
Le nombre d'attaques mobiles continue d'augmenter à mesure que les appareils mobiles prennent place dans l'entreprise et offrent aux pirates un accès direct et potentiellement lucratif aux données personnelles et professionnelles. D'après une étude que nous avons menée en 2015, 42% des entreprises ont subi des incidents de sécurité mobile leur coûtant plus de 200 000 €, et 82% s'attendent à une augmentation du nombre d'incidents. Cette année a également été le témoin de l'émergence de plusieurs vulnérabilités mobiles critiques, notamment Certifigate impactant des centaines de millions d'appareils Android, et XcodeGhost – première infection malveillante à grande échelle ciblant des appareils Apple iOS non jailbreakés. Nous nous attendons à d'importantes vulnérabilités mobiles similaires l'année prochaine.

La bataille contre les menaces les plus dangereuses
Dans la bataille continue entre les pirates et les professionnels de la sécurité, les agresseurs déploient des variantes personnalisées de logiciels malveillants existants et d'attaques encore inconnues (« zero-day ») de plus en plus sophistiquées, capables de contourner la technologie de sécurité traditionnelle. Ces nouveaux vecteurs d'attaque exigent des solutions plus proactives et plus avancées pour stopper ces logiciels malveillants. Des innovations comme le sandboxing au niveau du CPU, capable d'identifier les menaces les plus dangereuses avant qu'elles ne parviennent à échapper à la détection des outils traditionnels et infecter les réseaux, seront plus que jamais nécessaires en 2016 pour faire face à ces nouvelles menaces.

Les infrastructures critiques plus que jamais en ligne de mire
En décembre 2014, une aciérie en Allemagne a été frappée par des pirates qui ont réussi à accéder au réseau de production de l'usine et causer des dommages « massifs ». Le département américain de la sécurité intérieure a découvert que le Trojan « Havex » était parvenu à compromettre les systèmes de contrôle industriel de plus de 1 000 entreprises du secteur de l'énergie en Europe et en Amérique du Nord. Les cyber-attaques menées contre des services publics et des processus industriels clés se poursuivront, à l'aide de logiciels malveillants ciblant les systèmes SCADA qui contrôlent ces processus. Comme ces systèmes de contrôle sont de plus en plus connectés et offrent une surface d'attaque plus étendue, une meilleure protection sera nécessaire pour les défendre. Ces risques sur les infrastructures critiques sont particulièrement sensibles dans un contexte de menaces terroristes accrues.

Les objets connectés : futur terrain de jeu des hackers ?
L'Internet des objets en est encore à ses balbutiements, et il est peu probable qu'il ait un fort impact en 2016. Néanmoins, les entreprises doivent réfléchir à la manière dont elles peuvent protéger les appareils intelligents et se préparer à une plus vaste adoption de l'IoT. Les utilisateurs doivent se demander « où leurs données sont transmises » et « ce qui se passerait si quelqu'un mettait la main sur ces données ». L'année dernière, nous avons découvert une faille dans des routeurs équipant des TPE dans le monde entier, qui pourrait permettre à des pirates de les détourner pour lancer des attaques sur tous les appareils qui leur sont connectés. Nous nous attendons à plus de vulnérabilités similaires dans les appareils connectés.

Les wearables c'est beau … mais pas très sécurisé !
Les wearables tels que les montres intelligentes font leur entrée dans l'entreprise, présentant de nouveaux risques et défis pour la sécurité. Les données stockées dans les montres intelligentes et les autres appareils personnels intelligents sont vulnérables et pourraient même être utilisées par des pirates pour capturer de l'audio et de la vidéo via des Trojans d'accès à distance. Les entreprises qui autorisent l'utilisation de ces appareils doivent assurer leur protection via des mots de passe et des technologies de chiffrement renforcées.
Trains, avions et véhicules connectés… autant de portes d'entrée pour les hackers !

2015 est l'année de l'émergence du piratage de véhicules : leurs logiciels embarqués sont détournés afin de prendre le contrôle des véhicules. En juillet, Fiat Chrysler a rappelé 1,4 millions de véhicules Jeep Cherokee aux États-Unis après que des chercheurs aient découvert qu'ils pouvaient être piratés via le système de divertissement connecté. Avec plus de gadgets et de systèmes connectés que jamais dans les véhicules modernes, nous devons protéger ces systèmes. Il en va de même pour les systèmes complexes des avions de ligne, des trains et autres formes de transport public.

Véritable sécurité pour les environnements virtuels
La virtualisation a été rapidement adoptée par les entreprises au cours des dernières années, que ce soit via SDN, NFV ou le Cloud. Les environnements virtualisés sont complexes et créent de nouvelles couches réseau. C'est seulement maintenant que nous comprenons réellement comment protéger ces environnements. Lorsque les entreprises migrent vers des environnements virtualisés, la sécurité doit être conçue dès le départ pour offrir une protection efficace.

Nouveaux environnements, nouvelles menaces
2015 était également l'année du lancement de plusieurs nouveaux systèmes d'exploitation, tels que Windows 10 et iOS 9. La majeure partie des attaques menées contre les entreprises ces dernières années ciblaient Windows 7, en raison de la faible adoption de Windows 8. Mais avec Windows 10 et son offre de téléchargement gratuit, les cybercriminels vont donc tenter d'exploiter ce nouveau système d'exploitation. Ses mises à jour sont plus fréquentes et les utilisateurs maîtrisent moins son environnement.

La consolidation de la sécurité pour la simplifier !
Pour se protéger contre les menaces multiformes, les professionnels de la sécurité sont susceptibles de se tourner vers des solutions d'administration centralisée de la sécurité. Les grandes entreprises qui possèdent pléthore de différents produits de sécurité sur leur réseau verront la consolidation comme un moyen de réduire à la fois coût et complexité. La multitude de solutions et de produits individuels devient rapidement ingérable et peut effectivement entraver la sécurité plutôt que l'améliorer. La consolidation de la sécurité fournit un moyen efficace de réduire la complexité afin que les nouvelles menaces ne s'égarent pas entre les mailles des différents systèmes.

Réagissez à cet article
Source : http://www.globalsecuritymag.fr/La-cyber-securite-en-2016-Check,20151204,58072.html

---

Le Conseil de l'UE rend sa copie sur la directive cybersécurité

Le Conseil de l'UE rend sa copie sur la directive cybersécurité

Les députés et le Conseil des ministres de l'UE sont parvenus à un accord autour de la directive NIS (Network and Information Security.) Celle-ci entend harmoniser les exigences en matière de cybersécurité entre les 28 pays membres de l'UE.

L'Europe ouvre la voie à une gestion communautaire de la cybersécurité et annonce un accord entre le parlement et le Conseil de l'UE autour de la directive NIS.

Cette directive en négociation depuis plusieurs mois est chargée d'harmoniser le cadre légal des pays membres autour des dispositions relatives à la sécurité des systèmes jugés critiques. La directive était en discussion au conseil depuis le mois d'octobre 2014, après une validation du parlement et à l'époque, les négociations s'annonçaient serrées.

Le texte initial s'accordait sur la nécessité pour les opérateurs « critiques » de faire remonter auprès des responsables et autorités les incidents de sécurité qui pouvaient affecter leurs systèmes. Derrière ce terme, on retrouvait ceux qu'en France on place sous la catégorisation d'OIV (opérateurs d'importance vitale) depuis la loi de programmation militaire de 2013 : les acteurs majeurs du secteur de l'énergie, des transports, de la santé ou des marchés financiers par exemple.

Mais le texte revu et corrigé par le Conseil de l'UE va plus loin et propose d'étendre la régulation des plateformes en ligne à l'instar de Google, Amazon ou Ebay. Ces plateformes en ligne devront donc également se plier à des exigences de reporting en matière de cybersécurité, mais celles-ci seront moins lourdes que les exigences envisagées pour les opérateurs critiques. Seuls les incidents graves devront être signalés.

Les États membres auront pour rôle d'identifier les acteurs et plateformes jugés « indispensables pour la société et l'économie » en amont, mais le texte prend soin d'exclure les micro et petites entreprises du numérique, qui jouiront d'une exemption.

Mieux vaut prévenir que subir

Le texte prévoit également la création d'un « réseau d'équipes d'intervention en cas d'incident lié à la sécurité informatique » établi dans chaque état membre afin de traiter et de répondre aux incidents transfrontaliers et « identifier des réponses coordonnées.

Reuters avait déjà publié en août un article relatant l'évolution des négociations en ce sens, une information qui avait suscité les inquiétudes de l'Afdel et de l'Asic. Les associations d'éditeurs en ligne craignaient en effet une loi trop pesante venant désavantager les entreprises et plateformes web européennes face à leurs concurrents étrangers.

Le texte doit encore être approuvé par la commission du marché intérieur du Parlement et par le comité des représentants permanents du Conseil avant d'être appliqué. En l'état actuel du texte, force est de reconnaître que cela ne devrait pas changer fondamentalement la donne en France : le reporting des incidents affectant les OIV était déjà l'une des mesures phares de la loi de Programmation Militaire de 2013 tandis que l'Anssi assume de fait le rôle d'équipe d'intervention en cas d'incident.

Mais la mention des plateformes web parmi les acteurs concernés pourrait en revanche amener le gouvernement à élargir la liste des OIV à placer sous la coupe de la LPM afin de se mettre en harmonie avec la directive européenne.

Réagissez à cet article

Source : http://www.zdnet.fr/actualites/le-conseil-de-l-ue-rend-sa-copie-sur-la-directive-cybersecurite-39829484.htm

---

Le FBI et Microsoft font

trembler le botnet DorkboOscar Barthe

Le FBI et Microsoft font trembler le botnet Dorkbot

En partenariat avec les forces de l'ordre de plusieurs pays comme le FBI et Interpol ainsi que d'autres acteurs IT et télécoms comme Eset, Microsoft a mené une attaque contre les infrastructures du botnet Dorkbot. Le but de l'attaque était, à défaut de l'éradiquer, de perturber son fonctionnement.

Le botnet Dorkbot permet à ses utilisateurs de récupérer les identifiants de connexion de différents services comme Gmail, Facebook, Twitter ou encore Steam.
En partenariat avec les forces de l'ordre de plusieurs pays comme le FBI et Interpol ainsi que d'autres acteurs IT et télécoms comme Eset, Microsoft a mené une attaque contre les infrastructures du botnet Dorkbot. Le but de l'attaque était, à défaut de l'éradiquer, de perturber son fonctionnement.
Microsoft a fait sa bonne action. La firme de Redmond a déclaré jeudi avoir collaboré avec les autorités de plusieurs régions pour perturber le fonctionnement du botnet Dorkbot.
Découvert il y a quatre ans, ce dernier a infecté aujourd'hui plus d'un millions de machine. Il est utilisée pour récupérer les identifiants de connexion de différents services comme Gmail, Facebook, Netflix, PayPal, Steam ou encore eBay. La firme de Redmond ne s'est toutefois pas lancée seule dans l'attaque contre Dorkbot, et a travaillé ainsi avec le fournisseur de solution de sécurité Eset, le Cert polonais Polska, la commission canadienne de Radio-télévision et de télécommunications, l'agence de sûreté américaine, le FBI, Interpol, Europol et la police montée du Canada.
Les utilisateurs sont pour la majeure partie d'entre eux infectés lors de leur navigation sur internet sur des sites pas forcément bien protégés. Dorkbot exploite la moindre faille logicielle via un exploit kit ou les spam. Il peut aussi utiliser un système de ver pour se diffuser à travers les réseaux sociaux, les services de messagerie ou les clés USB.

Une attaque efficace mais pas durable
Microsoft n'a toutefois pas détaillé comment il s'y était pris pour perturber les infrastructures de Dorkbot. Ce n'est d'ailleurs pas la première fois que la firme collabore avec les autorités dans ce genre de situation. Les actions coordonnées visant à déconnecter les serveurs hébergeant les botnet ont souvent un impact immédiat mais les bénéfices ne durent pas. Souvent, les cybercriminels remettent rapidement sur pied une nouvelle infrastructure et s'attaque à la reconstruction du botnet en infectant d'autres ordinateurs.
La situation autour de Dorkbot devenait critique. Ses créateurs ont diffusé un kit permettant d'utiliser le botnet comme base pour en construire d'autres, plus puissants. Baptisé NgrBot, il était en vente sur le deep web.

Réagissez à cet article
Source : http://www.lemondeinformatique.fr/actualites/lire-le-fbi-et-microsoft-font-trembler-le-botnet-dorkbot-63185.html
Par Oscar Barthe