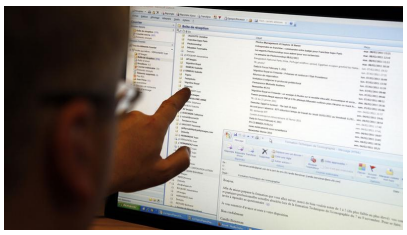
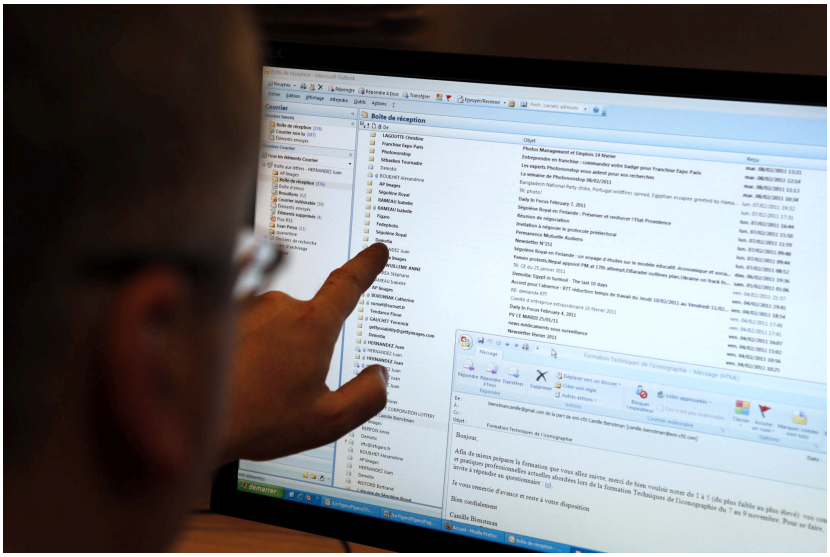
100 fois plus de victimes vol de données personnelles en deux ans en France



100 fois plus de victimes vol de données personnelles en deux ans en France

En 2015, cette pratique visant à dérober des informations personnelles par Internet ou par téléphone a fait plus de 2 millions de victimes en France. C'est cent fois plus qu'il y a deux ans.



Véritable piège pour les internautes, la pratique du phishing ne cesse de se répandre en France. Contraction de «fishing» (pêche) et «phreaking» (piratage de lignes téléphoniques), ce procédé malveillant vise à soutirer des données personnelles (mot de passe, identifiant de connexion, numéros de cartes bancaires). On parle également de «hameçonnage».

Sur la seule année 2015, plus de 2 millions de personnes auraient été victimes du phishing en France. C'est 100 fois plus qu'il y a deux ans, selon Europe 1 qui reprend un rapport de Phishing Initiative, site reconnu par les services de lutte contre la cybercriminalité. Le plus souvent, cette arnaque se manifeste par la réception d'un mail personnalisé provenant d'un organisme financier (banques), d'une entreprise (fournisseur d'Internet, EDF…) ou même d'une administration publique (CAF)… Du moins en apparence.

Car le message en question, aussi crédible et réaliste qu'il puisse paraître, vous invite en réalité à cliquer sur un lien, lequel vous redirige vers un site vous demandant de mettre à jour vos données personnelles. Dès lors, en se faisant passer pour des tiers, les cybercriminels à l'origine de ces mails frauduleux sont en mesure de récupérer vos informations personnelles. «L'augmentation des pratiques de phishing s'explique notamment par le nombre croissant de cybercriminels organisés en réseaux très structurés. D'autant que leurs méthodes sont de plus en plus sophistiquées. Auparavant, des fautes d'orthographe présentes dans les mails permettaient d'éveiller les soupçons. Désormais, c'est plus dur à déceler car ils paraissent davantage crédibles», explique Raphaël Renaud, spécialiste des questions liées au phishing.

Usurpées, les banques comme les grandes entreprises sont, elles aussi, directement concernées par le phishing. En modernisant leurs systèmes de sécurité, elles parviennent parfois à contrer les menaces. C'est le cas de Google qui a bloqué 7000 sites utilisés pour des attaques de phishing en 2015. De leur côté, les établissements bancaires assurent «un service de veille et donc une certaine publicité pour prévenir leurs clients, mais celle-ci est souvent insuffisante», remarque Serge Maître, secrétaire général de l'Association Française des Usagers des Banques (AFUB), avant de souligner que «le cryptogramme et le 3D Secure ont montré leurs limites face aux attaques de phishing.»

Comment réagir face au phishing?

S'il n'est pas encore trop tard, plusieurs méthodes permettent de contrer le phishing. Dans un premier temps, il est préférable de disposer d'un antivirus performant. Ensuite, «l'ultime chose à faire est de ne jamais cliquer dans un lien provenant d'un e-mail. Les services sérieux (banque, opérateurs téléphoniques, etc…) ne vous demandent jamais de changer un mot de passe de cette manière», explique Raphaël Richard avant d'ajouter «qu'il faut directement se connecter sur le site officiel pour ne pas avoir de doute». Enfin, certains sites tels que ou Phishing Initiative permettent de faire vérifier un mail en cas de soupçon mais également de signaler des adresses qui semblent suspectes.

En revanche, si un internaute vient d'être victime de phishing, il doit «déposer plainte si possible devant une brigade spécialisée dans les 48 heures car au-delà, cela devient plus compliqué. Il faut également contacter … [Lire la suite]

Réagissez à cet article

Source : *Données personnelles : le nombre de victimes de vol multiplié par 100 en deux ans en France*

[rappel] Les Anonymous s’en prennent au gouvernement français

[rappel] Les Anonymous s’en prennent au gouvernement français

---

Après avoir lancé une attaque par déni de service sur le site du Parti Socialiste hier, les Anonymous semblent aujourd'hui avoir pris pour cible les sites institutionnels du Sénat et de l'Assemblée nationale.

Les services informatiques de l'Assemblée nationale et du Sénat ont indiqué : « *Nous avons rencontré des problèmes de connexion et sommes en train d'en déterminer l'origine, qui pourrait en effet être une attaque DDoS. En tout cas, cela en a toutes les caractéristiques* ». Attaque ou pas, les auditions habituellement diffusées en direct n'ont pu être retransmises ce matin.

Hier, les Anonymous avait revendiqué une attaque similaire contre le site du Parti socialiste via la publication d'une vidéo sur YouTube. Dans cette dernière, le groupe d'« hacktivistes » fustigeait l'état d'urgence actuellement en cours dans notre pays, regrettant « *l'atteinte à la vie privée que pratique l'Etat français à l'égard de ses citoyens* » qu'il implique.

Une situation autorisée pour cause d'un terrorisme que les Anonymous considèrent comme « *excuse pour nous tromper, pour mieux nous surveiller, nous endormir et nous contrôler* ». Ils avaient hier menacé d'autres actions « *si l'état d'urgence n'est pas rectifié* », rappelant ne vouloir « aucunement faire de la politique » et ne viser que « *le site du Parti socialiste car il est le parti du dictateur Hollande.* ». Visiblement, ils auraient changé d'avis.

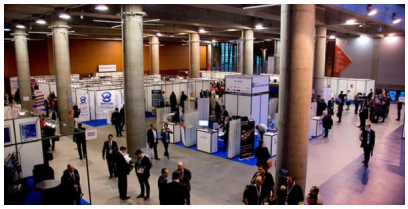
Mise à jour : après les sites du Sénat et celui de l'Assemblée, et après avoir souhaité la bienvenue au nouveau garde des Sceaux, Jean-Jacques Urvoas, en attaquant son blog, les Anonymous s'en sont pris ce matin aux sites des ministères de la Justice et de la Défense.

Si ce dernier est de nouveau sur pied à l'heure où nous écrivons ces lignes, il est toujours impossible de se rendre sur celui du ministère de la Justice. Les choses devraient toutefois revenir en ordre, les Anonymous étant désormais occupés avec les sites gouvernementaux du Burundi, dont la police a arrêté ce matin deux journalistes du *Monde*.

Réagissez à cet article

Source : *[rappel] Les Anonymous s'en prennent au gouvernement français*

Fic 2016 : La sécurisation des objets connectés préoccupe enfin…

	Fic 2016 : La sécurisation des objets connectés préoccupe enfin…

Le 8e Forum international de la cybersécurité, qui s'est tenu à Lille les 25 et 26 janvier, a permis de découvrir des solutions qui émergent en France en termes de sécurisation des objets de communication et des systèmes d'information auxquels ils sont connectés. Certaines sont encore à construire comme la plateforme Scop, d'autres sont déjà opérationnelles comme le CERT-Ubik et le boitier Hardsploit.

La multiplication des objets communicants, les IoT en anglais pour Internet Of Things, est une excellente opportunité pour la cybercriminalité. Sachant qu'à chacun de ces objets correspond une adresse IP, leur diffusion rend les réseaux très perméables.

« On estime à plus 50 milliards leur nombre d'ici 2020, soit 7 objets connectés par personne sachant qu'il y aura 7,5 milliards d'habitants sur terre. Les hackers vont pouvoir profiter d'une perméabilité des systèmes d'informations jamais atteintes jusqu'à présent. Et si la sécurité était en réalité le principal enjeu de l'Internet des objets ? »

A cette question posée en introduction de son exposé lors du 8e Forum International de la Cybersécurité, Christophe Joly, le directeur sécurité de Cisco France, a bien sûr répondu par l'affirmatif en chiffrant à plus de 375 milliards de dollars le marché annuel du cybercrime qui se profile. Mais comme avec les voitures au début du vingtième siècle et avec Internet plus récemment, le législateur attendra sans doute qu'une catastrophe ait lieu avant de mettre en place des règles. En attendant, rien n'empêche de se protéger.

Sécuriser l'électronique embarquée

Pour Cisco, le leader mondial des technologies informatiques de connectivité, les moyens de le faire passent par une bonne connaissance de son infrastructure informatique et des objets qui s'y connectent. Mais cette approche ne suffit pas toujours, entre autres quand l'objet communique par radiofréquence. De plus, la sécurité des objets connectés ne porte pas uniquement sur les réseaux et les… *Lire la suite…*

Réagissez à cet article

Source : *Cybercriminalité: la sécurisation des objets connectés est en marche au FIC*

Des braqueurs confondent un coffre-fort… avec un Minitel

Des braqueurs confondent un coffre-fort… avec un Minitel

A Roubaix, des braqueurs visiblement très jeunes sont repartis avec un butin particulier et fort inutile. Les deux malfrats ont emporté un Minitel, qu'ils avaient pris pour un coffre-fort.

Ils pourront peut-être revendre leur butin sur un marché aux puces. Mercredi, deux braqueurs de Roubaix s'en sont pris à une librairie et sont repartis avec ce qu'ils pensaient être un coffre-fort. Manque de chance, ils ont confondu l'objet avec un Minitel, rapporte *La Voix du Nord*.

Les deux malfrats, visiblement débutants selon les quotidiens régionaux, sont arrivés dans le commerce et ont menacé le gérant avec une arme. Les personnes présentes se sont interposées, empêchant les braqueurs de s'emparer de la caisse enregistreuse.

Un gros objet cubique

Par dépit, les deux hommes se sont dirigés vers la réserve, « à la recherche d'un coffre », selon un témoin. Le duo est ressorti de la pièce avec un gros objet cubique. Un Minitel. « Ils ont dû le confondre avec un coffre », a raconté le gérant du magasin à *Nord Eclair*. Les deux braqueurs ont alors pris la fuite à pied avec leur maigre butin. Ils sont recherchés par la police.

Réagissez à cet article

Source : *Des braqueurs confondent un coffre-fort… avec un Minitel*

Programme de la 6eme Edition IT Forum à Dakar au Senegal

Programme de la 6eme Edition IT Forum à Dakar au Senegal

Colloque, Rencontre, IT Forum pour les managers IT africains

PROGRAMME DU JEUDI 18 FEVRIER 2015
9h00-9h10 DISCOURS DE BIENVENUE
Par M. Mohamadou DIALLO, Directeur de la publication de Cio Mag
9h10-9h20 ALLOCUTION D'OUVERTURE
Approche nationale et régionale en matière de Cybercriminalité
Par M. Yaya Abdoul KANE, Ministre de la Poste et des Télécommunications
9h20-9h30 ALLOCUTION Pays Invité d'honneur
Lutte contre la cybercriminalité, la Côte d'Ivoire renforce son arsenal
Par M. Bruno N. KONE, Ministre de la Postes et des Technologies de la Communication de Côte d'Ivoire, Porte-parole du Gouvernement

9h30-9h50 KEYNOTE SPEAKER
Pas d'Economie Numérique sans cyber-sécurité : Comment faire face aux tendances du numérique tout en maitrisant les défis du Cyberespace ?
Par M. Thierry BRETON, Président Directeur Général d'ATOS
9h50-10h00 KEYNOTE SPEAKER
L'Arrivée des réseaux haut débit, un accélérateur ou un moyen efficace de lutter contre les cyberattaques
Session Introductive
9h50-10h30 2 POINTS DE VUE
– Cybersécurité et protection des données à caractère personnel
Par M. Mouhamadou LO, Président de la Commission de Protection des Données Personnelles (CDP) du Sénégal
– Cybercriminalité : un enjeu international
Par M. Ali Drissa BADIEL, Représentant de l'UIT (Union Internationale des Télécommunications) en Afrique de l'Ouest
Questions / Réponses

10h30-11h00 Pause café et visite des stands

11h00-12h00 Plénière 1
Cloud, Mobilité, big data, internet des objets, Byod : Comment intégrer les nouvelles tendances tout en maitrisant les nouveaux risques inhérents ?
Modérateur: Commandant Guelpechetchin OUATTARA, Directeur de l'informatique et des Traces Technologiques de Côte d'Ivoire
· Représentant opérateur (Orange/Tigo ou Expresso Télécom)
· M. Chris MORET, Responsable de la Global Business Line CyberSecurity d'Atos Big Data & Secrity
· Dr. Alioune DIONE, Directeur des Systèmes d'Information de la Douane
· Colonel Julien DECHANNET, Officier Cyber des Eléments français en Afrique de l'Ouest
· M. Jean-Paul PINTE, Expert International en Cybercriminalité,
· Alain DOLIUM, Co-fondateur et CEO EMEA North America de South Mobile Service,
Questions / Réponses

12h00-13h00 Plénière 2
Plan Numérique et Administration électronique : Quelles perspectives ?
Modérateur : M. Alain DUCASS, Expert en Transformation Digitale
· Présentation des grandes lignes du Plan stratégique pour le numérique (Côte d'Ivoire/Sénégal) Par M Euloge Kipeya SORO, Directeur Général de l'Agence Nationale du Service Universel des Télécommunications (ANSUT)
· M. Malick NDIAYE Directeur de Cabinet du Ministère des Poste et des Télécommunications du Sénégal
· M. Mouhamed Tidiane Seck, Directeur Associé Performances Management Consulting
· M. Cheikh BAKHOUM, Directeur Général de l'Agence de l'Informatique de l'Etat (ADIE)
. M. Brice DEMOGE, Directeur du développement Secteur Public et Afrique – GFI Informatique
Questions / Réponses

13h00-14h00
Pause Déjeuner

14h00-15h00 Plénière 3
Retours d'expériences : solutions
· Plan de Sauvegarde et réplication des donnée après un incidents
· SAP s'engage pour la préservation du Parc Niokolokoba
· Cloud, l'essentiel pour les entreprises
Par Opérateur (Orange/Tigo ou Expresso Télécom)
· Applications métiers en mode Cloud, GFI informatique / Cegid
– Big data et sécurité, M. Alain DOLIUM, CEO South Mobile Services
Questions / Réponses
15h00-16h00 Plénière 4
Quelles solutions face à l'internationalisation de la cybercriminalité ?
· Modérateur : M. Pape Assane TOURE, Magistrat, Secrétaire général adjoint du Gouvernement
· M. Pape GUEYE, Elève Commissaire de Police, Ancien Chef de la Brigade de lutte contre la cybercriminalité
· M. Jean-François BEUZE, Président Directeur Général de Sifaris
· · M. Ali El AZZOUZI, Président Directeur Général Data Protect
· M. Richard NOUNI, Directeur Général de CFAO Technologies
· Retour d'expériences du secteur bancaire
Questions / Réponses

16h00-16h30
Pause café et visite des stands

16h30-17h30 Plénière 5
Point d'Echange Internet et ouverture du marché des FAI : Vers une amélioration de la qualité de l'Internet au Sénégal ?
Modérateur : M. Mohamadou SAIBOU, Directeur de l'ESMT Dakar
· M. Cheikh BAKHOUM, Président de SENIX (Point d'Echange Sénégal)
· M. Tidjane DEME, Google Afrique
· M. Ali Drissa BADIEL, Représentant de l'UIT (Union Internationale des Télécommunications) en Afrique de l'Ouest
· M. Alex CORENTHIN, Président d'ISOC Sénégal
· Représentant de l'ARTP
Questions / Réponses

17h30-17h45
SDE/Sodeci (Société d'électricité et d'eau de Côte d'Ivoire) face aux enjeux de l'électronique
SEM Sylvestre, Directeur Général de GS2E (Groupement d'intérêt économique de CIE et SODECI).
Clôture

17h45-18h00
DISCOURS DE CLOTURE
Perspectives sur les enjeux du haut débit mobile au Sénégal avec l'arrivée de la 4G
Par M. Yaya Abdoul KANE, Ministre de la Poste et des Télécommunications
PRE-PROGRAMME DU VENDREDI 19 FEVRIER 2015
Réflexion sur les chantiers de Modernisation de l'administration publique – Trois cas
9h00-9h15 Ouverture
DISCOURS D'OUVERTURE
Par M. Alioune SARR, Ministre du Commerce, du Secteur informel, de la Consommation, de la Promotion des produits locaux et des PME du Sénégal
9h15-10h00 Plénière 1
CAS 1 – SIGIF (Système Intégré de Gestion des Informations financières)
Le SIGIF, un enjeu de modernisation et de transparence dans la gestion des comptes publics
· Gestion intégrée des finances publiques : Retour d'expériences de la Côte d'Ivoire
Par Nongolougo SORO, Directeur Général de la SNDI
· Direction Générale de la comptabilité publique et du Trésor
· M. Ibrahima FAYE, Chef de l'Equipe Projet SIGIF au Ministère de l'Economie des Finances et du Plan
· M. Frédéric MASSE, VP SAP
· M. Jean-Michel HUET, Associé BearingPoint
Questions / Réponses

10h00-11h00 Plénière 2
CAS 2 – GUICHET UNIQUE
Guichet unique et impact sur le Doing business
· Directeur du commerce au Ministère du commerce
· Ibrahima DIAGNE, DG de Gaindé 2000
· Représentant de l'Apix
· Dr. Alioune DIONE, DSI de la Douane Sénégalaise`
Questions / Réponses

11h00-11h20
Pause café et visite des stands

11h20-12h00 Plénière 3
CAS 3 – FICHIER D'ETAT CIVIL
Modernisation du Fichier d'état civil, quel enjeu pour la gouvernance locale ?
Modérateur: André GRISSONNANCHE, PDG Exense
– M. Frédéric Massé, VP SAP,
– Mme Emilie Scalier, GDexpert
– M. Mouhamed Tidiane Seck, Directeur Associé Performances Management Consulting
– Jean-Pierre La Hausse de la Louvière, CEO d'iSTEC
– ADIE
– Ministère de l'Intérieur
– Direction de l'état civil
Clôture

12h00-12h20
DISCOURS DE CLOTURE
Par M. Abdoulaye Diouf SARR, Ministre de la gouvernance locale, du développement et de l'aménagement du territoire du Sénégal
12h20
Cocktail déjeunatoire

Réagissez à cet article

Source : *Programme 6eme Edition IT Forum Senegal – Colloque, Rencontre, IT Forum pour les managers IT africains*

Safe Harbor 2 au point mort

A partir du 1er février, les sociétés privées transférant des données de citoyens européens vers les Etats-Unis sous le régime du « Safe Harbor » seront en infraction caractérisée. Ces sociétés bénéficiaient en effet d'une période de grâce, après l'annulation de cet accord international – mais la situation n'est toujours pas réglée.
Pendant quinze ans, « Safe Harbor » a permis à plus de quatre mille entreprises d'exporter des données vers les Etats-Unis, alors que les lois américaines n'offrent pas une protection suffisante au regard du droit européen.
Ce régime d'exception permanente a été aboli par la cour de justice de l'Union européenne (UE) en octobre 2015, à la suite d'une plainte déposée par un militant autrichien contre la filiale européenne de Facebook en Irlande, et aux révélations d'Edward Snowden sur les programmes de surveillance de masse des agences de renseignement américaines.

Blocage des négociations
Malgré l'urgence, les négociations pour la mise en place d'un Safe Harbor 2, qui serait plus respectueux des droits des Européens, n'ont pas encore abouti. L'une des exigences de l'UE est que les Etats-Unis autorisent les Européens à porter plainte devant les tribunaux américains au cas où leurs données personnelles seraient exploitées de façon abusive – une simple mesure de réciprocité, car les Américains possèdent déjà ce droit en Europe. Pour satisfaire cette demande, la Chambre des représentants américaine a voté en octobre 2015 une loi spéciale, baptisée Judicial Redress Act (JRA). Le Sénat aurait dû en faire autant le 20 janvier, mais le débat a été annulé au dernier moment, sans explications.
Ce blocage affecte aussi la mise en place d'un autre accord transatlantique, conclu en septembre 2015 : l'Umbrella Agreement (« accord parapluie »), qui encadre les échanges de données personnelles en matière de police et de justice, en limitant les droits des administrations américaines dans le traitement des données européennes. Tant que le JRA ne sera pas voté, l'Europe ne souhaite pas valider l'Umbrella Agreement.

Une loi attaquée de tous les côtés
En réalité, aux Etats-Unis, le JRA est attaqué de tous les côtés. D'une part, certains sénateurs conservateurs, suivant l'avis des agences de renseignement, estiment que les demandes européennes arrivent à contretemps : après les attentats de Paris, la lutte contre le terrorisme exige selon eux de renforcer la surveillance des données personnelles et d'allonger leur durée de rétention, et non pas de les réduire.
D'autre part, l'association américaine de défense des libertés sur Internet, l'Electronic Privacy Information Center (EPIC), estime au contraire que l'Umbrella Agreement ne protège pas assez les données des Européens, et exige que le département fédéral de la justice publie l'intégralité du texte de l'accord, pour s'assurer qu'il ne contient pas de clauses secrètes. EPIC a écrit aux sénateurs pour les inciter à voter contre le JRA dans sa version actuelle.
Le Safe Harbor 2 semble donc mal parti, du moins à court terme, sauf si l'Europe cède à nouveau aux exigences américaines. En coulisses, à Bruxelles et dans plusieurs capitales européennes, les grandes entreprises américaines et leurs associations professionnelles font un lobbying intense pour pousser l'Union européenne a accepter un nouvel accord, même si toutes ses demandes ne sont pas satisfaites.

Contrats bilatéraux pour contourner la loi
Le groupe de travail G29, qui regroupe les agences de protection de données européennes, doit se réunir le 2 février pour évaluer la situation et si possible proposer des solutions pour sortir de l'impasse.
Les entreprises fortement impliquées dans l'exportation de données sont parallèlement déjà en train de s'adapter. Selon le cabinet juridique américain Jones Day, qui possède un bureau à Paris, la situation actuelle est incertaine, mais pas aussi critique qu'on pourrait le croire. Pour rester dans la légalité, de nombreuses sociétés ont recours à un autre instrument juridique : un contrat bilatéral entre l'expéditeur et le destinataire des données (souvent la maison-mère américaine et sa filiale européenne) contenant des clauses types garantissant que les données européennes bénéficieront aux Etats-Unis d'une protection conforme au droit européen – une procédure plus complexe et plus coûteuse que le Safe Harbor, mais pas insurmontable.
En ce qui concerne les PME européennes qui font traiter leurs données aux Etats-Unis, elles sont prises en charge par leurs fournisseurs de service, c'est-à-dire les grandes entreprises de cloud américaines comme Amazon, Salesforce ou IBM, qui se chargent à leur place des formalités juridiques.

Réagissez à cet article

Source : *Données personnelles : le projet « Safe Harbor 2 » dans l'impasse*

20 vulnérabilités critiques corrigées dans Magento

20 vulnérabilités critiques corrigées dans Magento

Magento, fournisseur de solutions e-commerce open source, a patché plusieurs vulnérabilités présentant un risque d'attaques dont certaines de type XSS. Plusieurs éditions des versions communautaire et entreprise sont concernées.

Les administrateurs de sites e-commerce sous Magento ont tout intérêt à faire preuve de grande vigilance. L'éditeur vient en effet de lancer plusieurs correctifs pour combler des vulnérabilités critiques dans plusieurs versions de ses produits. Parmi les failles recensées, l'une permet d'injecter du code Javascript dans un champ de mail pour mener des attaques de type cross-site scripting (XSS). Considérée par Magento comme critique, cette vulnérabilité permet de pirater le compte administrateur de la session. Elle affecte l'édition communautaire de Magento (antérieure à la v1.9.2.3), ainsi que l'édition entreprise (antérieure à la v1.14.2.3) de la solution e-commerce open source.

La salve de correctifs permet également de combler 19 autres failles (relatives notamment aux formulaires de commandes, headers des adresses IP client, téléchargement de fichiers, deni de service newsletter, contournement de captcha…) dont certaines concernent également les v2.x des versions communautaire et entreprise de Magento. Il s'agit des premières vulnérabilités de taille que Magento a rencontrées cette année. En 2015, l'éditeur avait dû faire face à plusieurs problèmes dont une vulnérabilité critique exploitée ayant affecté un grand nombre de sites e-commerce.

Réagissez à cet article

Loi sur le numérique adoptée quasiment sans voix contre

#Loi sur le numérique adoptée quasiment sans voix contre

La loi Pour une république numérique » vient d'être adoptée par l'Assemblée Nationale à 356 contre 1. Elle sera prochainement examinée au Sénat pour une seconde lecture.
La loi sur le numérique d'Axelle Lemaire vient d'être adoptée par une majorité de députés de l'Assemblée aujourd'hui. Sur 544 votants, 356 se sont prononcés en faveur de la nouvelle loi obtenant ainsi une large majorité.
Ainsi que la Secrétaire d'Etat chargée du Numérique l'avait énoncé devant l'Assemblée la semaine dernière, la loi est voulue construite selon la devise française, en trois axes :
• circulation des données et du savoir (liberté),
• protection dans la société numérique (égalité),
• l'accès des publics fragiles au numérique (fraternité).

Le gouvernement inscrit donc désormais dans le marbre législatif sa volonté de ne pas rater la vague de l'Open Data (Royaume-Uni, Danemark), tout en fournissant un nouveau cadre aux sites Internet et aux FAI (neutralité, loyauté des plates-formes).
Le vote a aussi permis de révéler que 187 votants se sont abstenus, la plupart des députés du groupe Les Républicains, avouant leur désapprobation de forme, et non de fond, du projet de loi dévoilé pour la première fois au début de l'été 2015.

Réagissez à cet article

Source : *La loi sur le numérique adoptée à 356 voix contre 1*

Fic 2016 : Etude d'impacts sur la vie privée : suivez la méthode de la CNIL

	**Fic 2016 : Etude d'impacts sur la vie privée : Suivre la méthode de la CNIL**

La CNIL publie sa méthode pour mener des PIA (Privacy Impact Assessment) pour aider les responsables de traitements dans leur démarche de mise en conformité et les fournisseurs dans la prise en compte de la vie privée dès la conception de leurs produits.

De l'application de bonnes pratiques de sécurité à une véritable mise en conformité

La Loi informatique et libertés (article 34), impose aux responsables de traitement de « prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données ».
Chaque responsable doit donc identifier les risques engendrés par son traitement avant de déterminer les moyens adéquats pour les réduire.
Pour aider les TPE et PME dans cette étude, la CNIL a publié en 2010 un premier guide sécurité. Celui-ci présente sous forme de fiches thématiques les précautions élémentaires à mettre en place pour améliorer la sécurité d'un traitement des données personnelles.
En juin 2012, la CNIL publiait un autre guide de gestion des risques sur la vie privée pour les traitements complexes ou aux risques élevés. Il aidait les responsables de traitements à avoir une vision objective des risques engendrés par leurs traitements, de manière à choisir les mesures de sécurité nécessaires et suffisantes.

Une méthode plus rapide, plus facile à appliquer et plus outillée

Ce guide a été révisé afin d'être plus en phase avec le projet de règlement européen sur la protection des données et les réflexions du G29 sur l'approche par les risques. Il tient aussi compte des retours d'expérience et des améliorations proposées par différents acteurs.
La CNIL propose ainsi une méthode encore plus efficace, qui se compose de deux guides : la démarche méthodologique et l'outillage (modèles et exemples). Ils sont complétés par le guide des bonnes pratiques pour traiter les risques, déjà publié sur le site web de la CNIL.

Un PIA (Privacy Impact Assessment) ou étude d'impacts sur la vie privée (EIVP) repose sur deux piliers :

les principes et droits fondamentaux, « non négociables », qui sont fixés par la loi et doivent être respectés. Ils ne peuvent faire l'objet d'aucune modulation, quels que soient la nature, la gravité et la vraisemblance des risques encourus ;
la gestion des risques sur la vie privée des personnes concernées, qui permet de déterminer les mesures techniques et d'organisation appropriées pour protéger les données personnelles.
Pour mettre en œuvre ces deux piliers, la démarche comprend 4 étapes :
• Étude du contexte : délimiter et décrire les traitements considérés, leur contexte et leurs enjeux ;
• Étude des mesures : identifier les mesures existantes ou prévues (d'une part pour respecter les exigences légales, d'autre part pour traiter les risques sur la vie privée) ;
• Étude des risques : apprécier les risques liés à la sécurité des données et qui pourraient avoir des impacts sur la vie privée des personnes concernées, afin de vérifier qu'ils sont traités de manière proportionnée ;
• Validation : décider de valider la manière dont il est prévu de respecter les exigences légales et de traiter les risques, ou bien refaire une itération des étapes précédentes.
L'application de cette méthode par les entreprises devrait ainsi leur permettre d'assurer une prise en compte optimale de la protection des données personnelles dans le cadre de leurs activités.

Denis JACOPINI EST FORMATEUR EN ETUDE D'IMPACT SUR LA VIE PRIVÉE

Réagissez à cet article

Source : *Etude d’impacts sur la vie privée : suivez la méthode de la CNIL – CNIL – Commission nationale de l’informatique et des libertés*

Fic 2016 : Orange a de grands projets pour la France

#Fic 2016 : Orange a de grands projets pour la France

Une introduction calibrée sur mesure pour Stéphane Richard, PDG d'Orange, qui a succédé à Xavier Bertrand et au général Favier, directeur général de la Gendarmerie Nationale, sur la scène du FIC.

Lundi 25 janvier 2016, au FIC (Forum International de la Cybersecurité) à Lille Grand Palais
« La politique de cybersécurité d'Orange a été boostée par des attaques et nous peinons à recruter des talents.
2600 postes sont aujourd'hui ouverts à Paris pour la cyberdéfense et il est difficile de les pourvoir.
Notre cyber SOC (security operation center) est installé à Rennes mais nous allons également nous positionner à Lille pour déployer des ressources capables de se projeter à Lille, Bruxelles et Paris », a assuré le PDG.
« Notre croissance – près de 20% par an – est aujourd'hui freinée car nous manquons de ressources », a ajouté Michel van den Bergue, directeur d'Orange Cyberdéfense. « Il est rageant de voir ce domaine avec une perspective énorme manquer de ressources ». Pour Lille, Orange va s'appuyer sur Euratechnologies et travailler avec le personnel de la compagnie qui désire évoluer vers les métiers de la cybersécurité pour répondre à des projets sur Paris, Londres et Bruxelles.

Réagissez à cet article