Memex : Moteur de recherche et nouvelle arme qui explore le Dark Web

Memex : Moteur de recherche et nouvelle arme qui explore le Dark Web

Cette nouvelle arme a permis aux autorités américaines de démanteler un réseau de prostitution. Memex, le moteur de recherche développé et présenté en février par la Darpa, la branche de l'armée américaine spécialisée dans les réseaux, est utilisé depuis plus d'un an par les forces de l'ordre des Etats-Unis pour traquer toutes sortes de criminels. Ce moteur de recherche a la particularité d'explorer les tréfonds de la Toile.

Le Web invisible, terrain de jeu des criminels

«Certains estiment que Google, Microsoft et Yahoo ne nous donnent accès qu'à 5% du contenu du Web», explique Chris White, ingénieur de la Darpa, dans une interview accordée à la chaîne américaine CBS. Memex inspecte la partie invisible de la Toile, appelée le «Deep Web», plus vaste encore que ce que des moteurs comme Google explorent.

Ce Web «invisible» contient les pages non indexées par les moteurs, comme des pages éphémères, à faible trafic, ou des pages protégées par un logiciel spécifique, comme les réseaux anonymes Tor, connu notamment par les pirates. Ces pages sont un des principaux outils des différents réseaux criminels qui auraient ainsi publié pas moins 60 millions de pages ces deux dernières années, selon la Darpa.

Memex est capable d'indexer ce Web invisible pour aider les enquêtes dans les activités illégales trafic de drogue, de prostitution ou encore de pédophilie. Il peut aussi comprendre les liens entre les différentes pages et présenter les informations obtenues sous formes de graphiques, cartes, frises, etc.

«Il s'agit d'un bel exemple de la manière dont le Big Data peut aider à protéger les personnes vulnérables», estime Barack Obama dans le cadre de son rapport sur le Big Data, publié en janvier.

Et la protection des données personnelles?

Memex est actuellement au service de l'armée, mais ses applications pourraient également aider le secteur de la santé, en repérant par exemple précisément l'évolution géographique d'une épidémie. De belles perspectives, mais aussi de plus sombres.

La Darpa précise que ce nouveau moteur de recherche ultra-puissant n'a pas l'intention de collecter des données personnelles. Il en est cependant potentiellement capable. N'oublions pas le scandale du programme de surveillance Prism, révélé par Edward Snowden.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.20minutes.fr/web/1539339-20150212-memex-moteur-recherche-explore-dark-web

La CNIL place un conseiller pour encadrer le blocage de sites terroristes

La CNIL place un conseiller pour encadrer le blocage de sites terroristes

Dans le but d'encadrer le blocage de sites faisant l'apologie du terrorisme, la CNIL a nommé un magistrat en tant que conseiller honoraire à la Cour de cassation.

Le blocage des sites internet faisant l'apologie du terrorisme est une mesure contestée par les défenseurs des libertés sur le net. C'est sa nature qui laisse penser à une censure du web, d'autant plus que ce dispositif administratif n'a pas besoin de l'intervention d'un juge, qui fait débat.
Pour replacer un représentant de la loi au centre de ce dispositif contesté, la Commission nationale de l'informatique et des libertés (CNIL) vient de nommer Alexandre Linden en tant que conseiller honoraire à la Cour de cassation. Le rôle de ce magistrat sera d'encadrer le blocage des sites internet faisant l'apologie du terrorisme, une manière détournée de placer un représentant de la loi pour juger de la pertinence de chaque mesure.
Alors qu'une première liste de 10 à 50 URL doit être soumise à l'Unité de coordination de la lutte antiterroriste, les décrets publiés le 6 février dernier précisent que l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) est chargé de mettre en œuvre la loi. Les fournisseurs d'accès auront 24 heures pour bloquer l'accès à ces sites suite à la décision de l'office.
Alexandre Linden aura donc son mot à dire dans ces décisions, mais reste à savoir les moyens qu'il aura à disposition pour agir.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.linformatique.org/la-cnil-place-un-conseiller-pour-encadrer-le-blocage-de-sites-terroristes/

Fuites subies par Anthem : une attaque lente et silencieuse

L'attaque menée contre Anthem, le second plus grand assureur aux États-Unis dans le domaine de la santé, qui a exposé les données personnelles identifiables de dizaines de millions d'assurés, n'était probablement pas un simple raid rapide mais plutôt un détournement continu et discret d'informations sur une période de plusieurs mois. L'attaque était conçue pour ne pas être détectée par les équipes informatiques et de sécurité de l'entreprise, et reposait sur un mécanisme d'infection par bot pour exfiltrer les données, explique Thierry Karsenti, Directeur Technique Europe de Check Point Software Technologies. Voici son analyse.

Selon les déclarations d'Anthem, les premiers signes de l'attaque sont apparus au milieu de la semaine dernière, lorsqu'un administrateur informatique a remarqué qu'une requête de base de données était exécutée à l'aide de son identifiant sans qu'il ne l'ait déclenchée. L'entreprise a déterminé qu'une attaque avait eu lieu, a informé le FBI et a engagé un consultant externe pour mener une enquête de sécurité.

Les enquêteurs ont constaté qu'un logiciel malveillant personnalisé a été utilisé pour infiltrer les réseaux d'Anthem et dérober des données. Le type exact de logiciel malveillant n'a pas été communiqué, mais il semble être une variante d'une famille connue d'outils de piratage. Un rapport de sécurité indépendant signale que l'attaque a pu commencer trois mois auparavant. Le consultant a remarqué une « activité de type botnet » dans des entreprises affiliées à Anthem en novembre 2014.
Ce n'est pas surprenant car les activités de bot à long terme sont courantes dans les entreprises. Le Rapport Sécurité 2014 de Check Point, basé sur la surveillance d'événements dans plus de 10 000 entreprises dans le monde entier, a constaté qu'au moins un bot a été détecté dans 73% des entreprises, contre 63% l'année précédente. 77% des bots étaient actifs pendant plus de quatre semaines, et communiquaient généralement avec leur « centre de commande et de contrôle » toutes les trois minutes.
Les bots sont capables d'échapper à toute détection car leurs développeurs utilisent des outils d'offuscation pour leur permettre de contourner les solutions antimalwares traditionnelles reposant sur des signatures. En tant que tel, l'émulation des menaces, également appelée « émulation en bac à sable », devrait être utilisée comme couche de défense supplémentaire pour stopper les bots avant qu'ils n'infectent les réseaux. Des solutions antibots devraient également être déployées pour faciliter la découverte des bots, et empêcher d'autres fuites en bloquant leurs communications.
Il est également important que les entreprises segmentent leur réseau, en séparant chaque segment par des couches de sécurité pour empêcher les infections de bot largement répandues. La segmentation peut restreindre les infections à une zone particulière du réseau pour atténuer les risques et empêcher les infections d'accéder à des données confidentielles dans d'autres segments du réseau.
Avec ces trois approches préventives, les entreprises peuvent réduire considérablement leur exposition au type d'attaque lente et furtive qui semble avoir frappé Anthem, et éviter de devenir la victime de fuites à grande échelle.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.itrmanager.com/articles/154049/fuites-subies-anthem-attaque-lente-silencieuse.html

Effet Charlie : explosion des signalements d’apologie du terrorisme en ligne

Effet Charlie : explosion des signalements d’apologie du terrorisme en ligne

Après les attentats de Paris, la plateforme de la police Pharos a recueilli en un mois 40.000 signalements de contenus illicites en ligne. Même explosion auprès de la plateforme des fournisseurs d’accès et de services Internet, pourtant après une forte baisse en 2014.

La fusillade meurtrière ayant ciblé « Charlie Hebdo » le 7 janvier à Paris, suivi du meurtre de la policière à Montrouge et de la prise d’otages sanglante à l’Hyper Cacher de la porte de Vincennes, ont provoqué un sursaut mais aussi un déferlement de haine sur Internet. Les chiffres officiels sont impressionnants : la plateforme de la police Pharos, qui permet à tout internaute de signaler un contenu illicite en ligne (internet-signalement.gouv.fr), a enregistré une explosion des notifications dans la foulée des attentats, comme l’avait évoqué Bernard Cazeneuve, le ministre de l’Intérieur, courant janvier.

« En moyenne, nous traitons 400 signalements par jour. Les attentats se sont traduits par un afflux de signalements : dans la semaine de 7 au 17 janvier, nous avons recueilli 29.000 signalements pour l’essentiel d’apologie du terrorisme et d’incitation à la haine raciale » a expliqué mardi Valérie Maldonado, chef de l’office central de la lutte contre la cybercriminalité liée aux technologies de l’information et de la communication (OCLCTIC).

Twitter beaucoup plus utilisé que Facebook

La commissaire divisionnaire, qui est également sous-directeur adjoint de la lutte contre la cybercriminalité de la Direction centrale de la police judiciaire, a relevé que « les attentats dans la vie physique ont eu un prolongement sur Internet avec ces propos de soutien en ligne. Twitter a été extrêmement utilisé, la plateforme la plus utilisée dans ce cadre, beaucoup plus que Facebook »

Julien Gauthier, le chef de la plateforme Pharos, a précisé que le nombre de signalements reçus entre le 7 janvier et le 7 février avait même atteint 40.000 à comparer aux 140.000 recueillis sur l’ensemble de 2014 ! Soit plus du quart du volume annuel en un mois seulement.

Ils intervenaient dans le cadre d’une présentation d’un bilan de l’année 2014 sur la suppression des contenus illicites en ligne, organisée par le service « Point de contact » de l’Association des fournisseurs d’accès et de services Internet (AFA), dont Orange, SFR, Bouygues Telecom, Google, Microsoft et Facebook sont membres, mais pas Free ni Numericable. Ce service, créé en 1998, permet à tout internaute par un formulaire simple et anonyme tout contenu choquant rencontré sur Internet. « Point de contact » a également relevé une explosion du nombre de signalements de contenus de propagande terroriste ayant reçu «pour le seul mois de janvier le volume de l’année 2014 dans cette catégorie. » Pourtant, le nombre de contenus de ce type dénoncés par formulaire avait été divisé par deux en un an (36 en 2014 et seulement 6 qualifiés comme tels).

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source :
http://www.latribune.fr/technos-medias/20150210trib83405d360/effet-charlie-explosion-des-signalements-d-apologies-du-terrorisme-en-ligne.html

Forum de la Cybersécurité à

Marrakech, appel à endiguer les menaces de la cybercriminalité en Afrique

Forum de la Cybersécurité à Marrakech, appel à endiguer les menaces de la cybercriminalité en Afrique

Les participants à la 6ème édition du « Marrakech Security Forum » ont appelé à faire front commun pour endiguer les menaces de la cybercriminalité en Afrique.

Face à des législations rudimentaires et un essor sans précédant des flux informatiques, les pays africains n'ont d'autre choix que de faire bloc aux niveaux institutionnel, juridique et technologique, pour contrer les menaces sécuritaires découlant de la cybercriminalité, ont-ils relevé lors d'une séance plénière sur « l'Afrique face à la cybercriminalité et au cyber-terrorisme ».
Selon le Directeur du Centre satellitaire de l'Union européenne, Pascal Legai, l'essor numérique débridé et la désuétude de l'arsenal juridique ont érigé l'Afrique en une terre de prédilection pour la cybercriminalité et son corolaire le cyber-terrorisme.
Protéiforme, le cyber-crime en Afrique mute, change en fonction des cibles et, pis encore, s'affranchit de toutes les juridictions, a-t-il fait remarquer, soulignant l'inéluctabilité « d'agir vite et de se coordonner » pour colmater les failles.
De par sa nature transfrontalière, la cybercriminalité est difficile à contrôler, d'où la nécessité, pour les Etats africains, d'harmoniser les politiques et législations nationales pour apporter une réponse normalisée aux menaces qui en découlent, a encore dit M. Legai.
De son côté, le directeur de l'Organe de coordination belge pour l'analyse de la menace (Belgique) Vandoren André a mis l'accent sur le risque que recèle le cyber-terrorisme comme étant un outil nouveau permettant aux groupes terroristes de repérer, d'incuber et d'enrôler des jeunes, « majoritairement paumés ».
La méthodologie de l'Etat islamique est une illustration on ne peut plus claire de la « propagande jihadiste » sur la toile, cette organisation ayant réussi à développer de nouveaux modus operandi, avec à l'appui une maitrise avérée de l'outil informatique et une armada de connaisseurs en la matière.
Placé sous le thème « L'Afrique face aux menaces transnationales et asymétriques », la 6ème édition du Marrakech Security Forum sert de tribune pour quelque 300 hauts responsables civils, militaires, sécuritaires, experts et représentants d'organisations internationales pour stimuler une meilleure compréhension de thématiques clés pour le devenir du continent africain.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://fr.starafrica.com/actualites/appel-a-endiguer-les-menaces-de-la-cybercriminalite-en-afrique.html
Par Atlasinfo

Forbes victime d’une vaste cyber-attaque chinoise

Forbes victime d’une vaste cyber-attaque chinoise

Les pirates traquaient tout spécialement des experts en défense et des sociétés financières grâce à la technique de hacking dite de « point d’eau ».

Un groupe de pirates informatiques basés en Chine a piégé fin 2014 le site internet du magazine américain Forbes, profitant notamment de failles d’un navigateur populaire pour transmettre des virus aux visiteurs, ont indiqué mardi des experts en cyber-sécurité. Selon les sociétés Invincea et iSight Partners, les pirates traquaient tout spécialement des experts en défense et des sociétés financières grâce à la technique de hacking dite de « point d’eau ».
Cette technique consiste généralement à infiltrer un site internet populaire, puis à le piéger avec des virus qui vont ensuite infecter les visiteurs. Lors de cette campagne de piratage menée en fin d’année dernière, Forbes et d’autres sites ont été visés, ont indiqué les experts. « Une menace chinoise avancée a compromis Forbes.com pour mettre en place une attaque de style +point d’eau+ visant la défense américaine et des sociétés de services financiers fin novembre 2014 », a expliqué Invincea dans un rapport publié sur son site, qualifiant cette attaque d’ »éhontée ».

Vaste portée
Les pirates ont notamment exploité les failles du navigateur Internet explorer et du programme Adobe Flash, qui ont depuis été réparées, a précisé la société. Cette campagne de cyber-espionnage n’aurait duré que quelques jours. De son côté, la société ISight a avancé que le groupe de pirates chinois Codoso, aussi appelé Sunshop, était à l’origine de cette attaque informatique concoctée pour cibler certains profils parmi les milliers de visiteurs du site.
Il aurait déjà à son actif des campagnes contre la défense américaine, des centres de réflexion, des services financiers, des entreprises énergétiques et des dissidents politiques, ont ajouté ces experts. Forbes.com est classé 61e site internet le plus populaire aux Etats-Unis et 168e mondial ; par conséquent la portée de la campagne de piratage pourrait être très vaste, estiment les experts.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lesechos.fr/tech-medias/hightech/0204150910405-forbes-victime-dune-vaste-cyber-attaque-chinoise-1092213.php
par AFP

Attaque informatique contre sony pictures : Les pirates s’appuient sur la naïveté des consommateurs

Attaque informatique contre sony pictures : Les pirates s’appuient sur la naïveté des consommateurs

Sony Pictures Entertainment a été victime, le 24 novembre 2014, d’une cyber attaque de grande envergure. Après avoir pénétré les systèmes informatiques de la société, des pirates ont publié des données volées qui comprenaient notamment des films, des scénarios (dont celui du prochain James Bond), des dossiers médicaux de salariés ou encore des e-mails internes.

La théorie généralement avancée est que le groupe responsable, Guardians of Peace, serait lié à la République populaire démocratique de Corée du Nord et que tout ce scénario-catastrophe serait en rapport avec la sortie d’une comédie potache hollywoodienne intitulée L’interview qui tue, ayant pour thème l’assassinat du dirigeant nord-coréen Kim Jong-Un.
Dans un communiqué, Tanguy de Coatpont, de Kaspersky Lab avoue : «Les avis sont partagés quant à savoir qui porte la responsabilité de l’attaque et le débat paraît devoir se prolonger. Or, dans le cas d’attaques ciblées, il est très difficile d’en identifier les auteurs, car il existe de nombreux moyens pour eux de masquer leurs traces. Malgré tout, deux éléments ont particulièrement retenu mon attention.»
Le premier concerne la sécurité de l’entreprise. Il est clair que Sony n’a pas su tirer les leçons de l’attaque qui avait frappé son réseau PlayStation Network au printemps 2011. La seconde observation porte sur les menaces proférées par les pirates (ou ceux revendiquant la responsabilité de l’attaque contre Sony), à savoir le risque d’attentats terroristes contre les cinémas projetant le film L’interview qui tue.
Cette menace d’une attaque physique contre la sécurité du grand public a de quoi alarmer. Nous vivons dans un monde connecté et des aspects de plus en plus nombreux de notre quotidien sont dématérialisés. Aucune entreprise, grande ou petite, n’est à l’abri d’une cyber attaque, que celle-ci soit ciblée ou le résultat de dommages collatéraux.
Toutefois, il est important de faire la différence entre le «hacking» et le «defacing» d’un site web. Si le premier peut avoir de graves conséquences en entraînant par exemple des vols de données importants, le deuxième vise surtout à occuper le terrain médiatique et véhiculer des messages politiques. Les antivirus classiques, qui constituent encore la seule ligne de défense de nombreuses sociétés, sont depuis longtemps inefficaces face aux nouveaux types d’attaque. Mais les pirates s’appuient aussi et surtout sur la naïveté des consommateurs, souvent peu au fait des dangers.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.elwatan.com/hebdo/multimedia/l-attaque-informatique-contre-sony-pictures-les-eclairages-de-kaspersky-lab-08-02-2015-286984_157.php

Voitures connectées faciles à hacker

Voitures connectées faciles à hacker

Les promesses de la voiture connectée font rêver : sans conducteur, intelligente,… mais visiblement, elle est aussi facile à pirater. Un hackeur en prend ici le contrôle, faisant du véhicule un danger pour ses passagers. Dans son émission « 60 minutes », CBS News consacre un dossier aux voitures connectées et à leurs failles de sécurité. Kathleen Fisher, experte de la DARPA (Defense Advanced Research Projects Agency) présente la voiture connectée comme un « ordinateur sur roues », soulignant de fait la possibilité de hacker le véhicule.

Démonstration à l'appui : il est en effet possible de contrôler la voiture à distance, à l'aide d'un simple ordinateur portable. Si déclencher les essuie-glaces ou le klaxon peut sembler « inoffensif », quand le hackeur prend contrôle des freins, c'est tout de suite plus inquiétant. Ici, il ne s'agit que de plots en plastique, mais on imagine rapidement les dégâts si une voiture connectée perdait les pédales « dans la vraie vie ».

Plus tôt cette semaine, le sénateur américain Edward J. Markey a sorti un rapport sur les dangers des voitures connectées. Il y compile les données fournies par 16 constructeurs automobiles dont BMW, Fiat Chrysler, Ford, General Motors, Nissan, Mitsubishi ou Mercedes-Benz après qu'il leur ait adressé une lettre et un questionnaire en décembre 2013. Certains constructeurs dont Tesla ont cependant refusé de lui répondre… Selon ses résultats, aucune mesure ne serait mise en place pour détecter et empêcher les tentatives de piratage ou les vols de données. Par ailleurs, outre la sécurité, le rapport revient aussi sur les problèmes de confidentialité des données : les propriétaires de voitures connectés ne seraient pas au courant de tout ce qui est enregistré à leur propos… De quoi faire réfléchir avant d'investir dans la voiture du futur.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.ladn.eu/actualites/pop-insight,voitures-connectees-faciles-hacker,74,24953.html

Cybercriminalité : un milliard de données volées en 2014 !

Cybercriminalité : un milliard de données volées en 2014 !

Selon l'étude Breach Level Index publié par le leader mondial de la sécurité numérique plus de 1 500 failles de données ont été enregistrées en 2014, entraînant le vol d'un milliard d'enregistrements de données. Par rapport à 2013, ces chiffres représentent une augmentation de 49 % du nombre de failles de données et de 78 % des enregistrements de données volées ou perdues.

Selon les données recensées dans l'indice BLI initialement réalisé par SafeNet pour l'année 2014, les cybercriminels sont principalement intéressés par le vol d'identité, 54 % des failles y étant rattachées, soit davantage que toute autre catégorie de failles y compris l'accès aux données financières. De plus, les infractions concernant les vols d'identité représentent également un tiers des failles de données les plus graves selon la notation du BLI (« catastrophique » pour une note comprise entre 9,0 et 10, ou « sévère » pour une note comprise entre 7,0 à 8,9). Les failles sécurisées, c'est-à-dire les failles de sécurité périmétrique où les données sont totalement ou partiellement cryptées, ont progressé de 1 % à 4 %.
« Nous assistons sans l'ombre d'un doute à un tournant dans la tactique abordée par les cybercriminels, le vol d'identité à long terme se substituant de plus en plus à l'immédiateté qui caractérise le vol des numéros de cartes de crédit », affirme Tsion Gonen, Vice-président en charge de la stratégie, Identity & Data Protection, Gemalto. « Le vol d'identité peut entraîner l'ouverture de nouveaux comptes de crédit frauduleux, la création de fausses identités à des fins criminelles, ainsi que d'autres activités d'une grande gravité. Les failles de données sont de plus en plus personnalisées, et il apparaît que pour l'utilisateur lambda, l'exposition aux risques est de plus en plus forte ».
Outre cette évolution vers le vol d'identité, les failles ont également augmenté en gravité en 2014, deux tiers des 50 failles les plus importantes selon leur score BLI ayant eu lieu l'année dernière. De plus, le nombre de failles de données impliquant plus de 100 millions d'enregistrements de données a doublé par rapport à 2013.
« Non seulement le volume des failles de données est en hausse, mais leur gravité est également de plus en plus importante. La question n'est plus de savoir « si » vous allez être victime d'un vol de données, mais « quand ». ajoute Tsion Gonen. La prévention des failles et la surveillance des menaces s'arrêtent là et ne sont pas toujours suffisantes pour repousser les cybercriminels. Les entreprises doivent adopter une vision des menaces numériques « centrée sur les données » en commençant par la mise en œuvre de meilleures techniques de gestion des identités et de contrôle d'accès, telles que l'authentification multi-facteurs, le chiffrement ou la gestion des clés pour sécuriser les données sensibles. Ces outils rendent les données subtilisées par les voleurs parfaitement inutilisables », précice-t-il.
En ce qui concerne les secteurs touchés, les services financiers et la grande distribution ont connu en 2014 les évolutions les plus significatives par rapport à d'autres segments industriels. La grande distribution est en légère augmentation par rapport à l'an dernier, avec 11 % de l'ensemble des failles de données enregistrées en 2014. Cependant, par le nombre d'enregistrements de données touchées, ce secteur est passé de 29 % en 2013 à 55 % en 2014 et ce, en raison de l'augmentation du nombre d'attaques visant les terminaux point de vente (TPV). Pour le secteur des services financiers, si le nombre de failles de données est resté relativement stable d'une année sur l'autre, le nombre moyen de dossiers perdus par faille a été multiplié par dix, passant de 112 000 en 2013 à 1,1 million en 2014.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://afriqueinside.com/cybercriminalite-milliard-donnees-volees-en-2014-12022015/

Safe Harbor et CNIL : des régulateurs allemands dénoncent le laxisme de la Federal Trade Commission (FTC)

Safe Harbor et CNIL : des régulateurs allemands dénoncent le laxisme de la Federal Trade Commission (FTC)

Des commissaires de la Cnil allemande ont lancé pour la première fois des procédure administratives contre deux transferts de données vers les Etats-Unis réalisés par des entreprises américaines sur la base de l'accord «Safe Harbor».

« La légitimité de l'accord est de plus en plus remise en question » a déclaré le commissaire Johannes Caspar (Hambourg) la semaine dernière lors d'un évènement consacré à la protection des données et organisé à Berlin. La frustration des commissaires les plus en pointe sur ce dossier vient du fait que cet accord n'a connu aucune réforme de fond suite aux révélations d'Edouard Snowden mentionnant que la NSA surveillait les données privées des citoyens allemands.
Dernier épisode en date, deux procédures administratives ont donc été initiées contre des entreprises américaines dans les landers de Berlin et de Brême.
Le programme Safe Harbor est un accord crucial pour les entreprises américaines. Google, Facebook ou encore Twitter peuvent en vertu de cet accord transférer légalement des données commerciales de l'Union européenne vers les États-Unis s'ils acceptent de respecter la loi applicable à la protection des données des citoyens des pays de l'UE. Cette loi porte essentiellement sur la collecte et le traitement des données.
C'est la FTC américaine qui doit vérifier que les exigences du Safe Harbor sont bien respectées par les entreprises américaines. Si l'accord venait à être dénoncé, cela aurait un impact important sur les activités des GAFA dans l'Union européenne.

Quel impact en cas de suspension du Safe Harbor ?
Suite au scandale d'espionnage de la NSA, de nombreuses voix européennes se sont élevées pour demander la suspension du programme Safe Harbor. Au lieu de suspendre l'accord, cependant, en novembre 2013, la Commission européenne a envoyé aux États-Unis une liste de 13 réformes qu'elle souhaite voir apporter au Safe Harbor. Le gouvernement américain n'a toujours pas pleinement répondu à la demande, même s'il avait promis de le faire pour l'été 2014. Tout cela pourrait être réglé en mai prochain, aux dernières nouvelles.
Reste que nul ne sait quel serait l'impact réel de la suspension du programme Safe Harbor. N'étant plus autorisés à transférer des données hors de l'UE, des entreprises comme Twitter, dont tous les serveurs sont aux Etats-Unis, auraient des difficultés majeures pour faire fonctionner leur activité européenne. Pour les entreprises qui ont des serveurs en Europe, cela affecterait néanmoins leur activité back-office, les données locales pouvant être transférées outre Atlantique pour subir un traitement algorithmique à des fins de profilage ou de détection des fraudes.
Mais la fin du Safe Harbor pourrait également porter préjudice à des entreprises européennes qui opèrent des données ailleurs qu'en Europe. Siemens, SAP et même BMW pour ne citer que les allemands, ont tout intérêt à expédier leurs données aux Etats-Unis quand cela est nécessaire d'un point de vue business.

5 000 membres de Safe Harbor
Plus de 5 000 sociétés sont membre de Safe Harbor, dont en plus des sociétés citées précédemment Amazon, Hewlett-Packard, IBM ou encore Microsoft. Ces entreprises affirment se conformer à un niveau 'adéquat' au exigences de protection des données personnelles de l'Union européenne.
Mais les inspections, réalisées par la FTC (Federal Trade Commission) des Etats-Unis, sont sporadiques, et les sanctions peuvent difficilement être appliquées. « De mon point de vue, la charge de la preuve n'est pas du ressort des entreprises américaines » a dit cependant Holger Lutz, associé chez Baker & McKenzie à DataGuidance. « C'est plus du ressort de l'autorité compétente en matière de protection des données ».
Les principes du Safe Harbor sont basés sur ceux de la Directive 95/46 du 24 octobre 1995 affirme la Cnil.
Les domaines couverts concernent l'information des personnes sur la collecte de données, la possibilité accordée à la personne concernée de s'opposer à un transfert à des tiers ou à une utilisation des données pour des finalités différentes, le consentement explicite des personnes pour le recueil de données sensibles, le droit d'accès, de rectification et enfin la sécurité.
« Le Safe Harbor permet donc d'assurer une protection adéquate pour les transferts de données en provenance de l'Union européenne vers des entreprises établies aux Etats-Unis » assure la Cnil, qui précise que la liste des entreprises ayant adhéré aux principes du Safe Harbor se trouve sur le site du Département du Commerce américain.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.zdnet.fr/actualites/safe-harbor-des-regulateurs-allemands-denoncent-le-laxisme-de-la-ftc-39814338.htm
Par Guillaume Serries