La cybersécurité un problème sous estimée par les chefs d’entreprises

	La cybersécurité un problème sous estimée par les chefs d’entreprises

Les entreprises se jugent souvent prêtes à résister aux cyber-attaques alors que la réalité est bien souvent moins reluisante.

Plusieurs études sorties récemment convergent pour montrer un tableau assez catastrophique de la cybersécurité des entreprises alors que la perception affichée par celles-ci est plutôt marquée par l'optimisme. Ou bien faut-il mieux parler d'inconscience ? Ainsi, 62% des entreprises ont déjà subi une tentative de fraude selon une étude de Sage. 12% en ont même subi au moins cinq. La fraude la plus courante reste la fameuse *fraude au président*(usurpation d'identité d'un dirigeant pour obtenir un virement à l'étranger) : 80% des entreprises affectées l'ont rencontrée. 18% ont été victimes d'un *test bancaire* et 14% d'une fraude interne (cas classique : substitution de RIB).

Les trois quarts des DAF craignent avant tout les fraudes d'origines externes. La*fraude au président* et la falsification de RIB sont largement cités avant des cyber-attaques sur des données financières (un quart seulement des répondants). Des processus métier ont été mis en place pour parer ces fraudes non-technologiques comme la séparation créateur/valideur d'un paiement, la double signature… Le respect des procédures et la vigilance interne ont suffi à détecter des fraudes dans de nombreux cas. Mais 30% des entreprises continuent de valider leurs virements par un simple fax ! Suivant les recommandations des organismes professionnels, la bascule vers les traitements informatisés (EBICS TS, via les portails bancaires, etc.) est malgré tout bien engagée.

Une méconnaissance des bonnes pratiques et des règles

Mais il n'en demeure pas moins que la méconnaissance des bonnes pratiques pour sécuriser l'information reste importante. Selon une étude Solucom/Conscio, 46% des collaborateurs ne sont pas préparés à réagir à de l'ingénierie sociale dont la *fraude au président* n'est qu'un exemple caricatural. Pourtant, selon les auteurs de l'étude, l'ingénierie sociale est la méthode principale pour s'introduire dans les systèmes d'information des entreprises ou réaliser des fraudes, notamment par usurpation d'identité ou de couple identifiant/mot de passe.

Si 88% des collaborateurs sont sensibilisés aux règles pour gérer les mots de passe, 47% seulement les adoptent. Un mécanisme technique est donc nécessaire pour obliger à respecter les bonnes pratiques. Enfin, la même étude mentionne que la réglementation sur les données personnelles est méconnue par la majorité des collaborateurs, entraînant de ce fait un important risque juridique pour leurs entreprises.

Bienvenue aux malwares

L'ingénierie sociale est décidément bien ancrée dans les pratiques des cyber-criminels. Cibler précisément les attaques permet notamment, selon l'étude publiée par Cisco, d'introduire des #ransomware. Ce type d'attaque génèrerait 34 millions de dollars par an et par campagne. Etre victime de tels pratiques est assez gênant, ce qui explique sans doute que seules 21% des entreprises informent leurs partenaires, 18% les autorités et 15% leur compagnie d'assurance.

Bien entendu, les fondamentaux du cybercrime sont toujours d'actualité avec des variantes pour les maintenir au goût du jour. La compromission de serveurs est ainsi un classique pour mener des attaques indirectes, notamment via des CMS mal mis à jour. La compromission de domaines WordPress a ainsi augmenté de 221% entre février et octobre 2015. Parmi les mauvaises pratiques qui se développent, la non-mise à jour des infrastructures est en croissance.

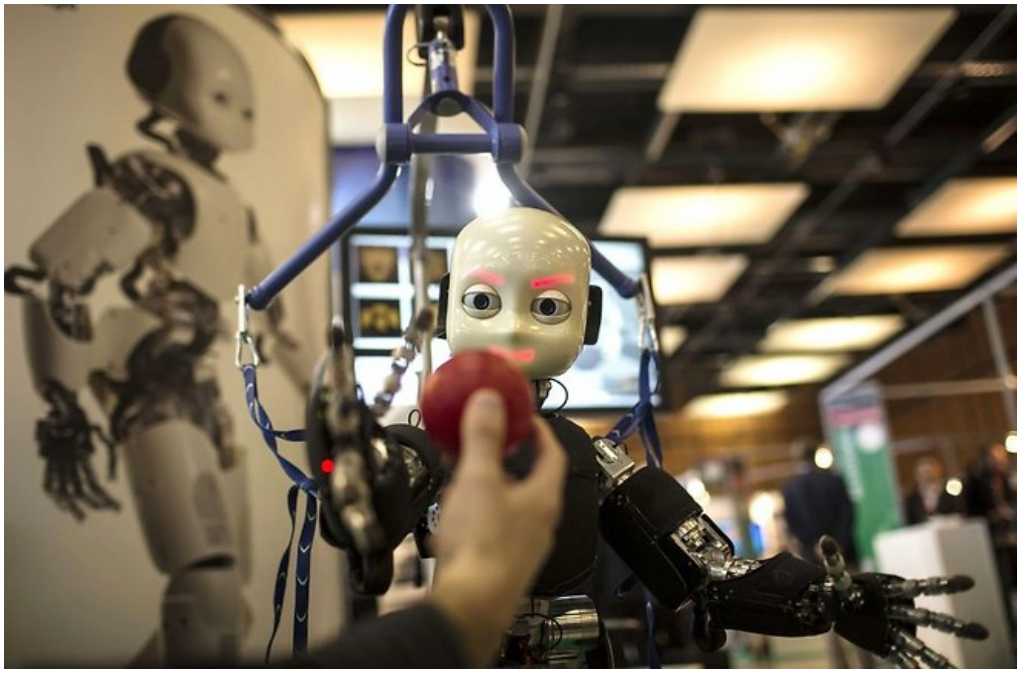
La fuite de données via les navigateurs, souvent négligée, est pourtant en pleine croissance : des extensions malveillantes affecteraient 85% des entreprises. Les attaques à base de DNS sont également en plein boum, d'autant que les experts DNS ne travaillent que rarement avec les experts en sécurité. Malgré tout, il est estimé que la rapidité de détection d'une intrusion a augmenté même si elle reste dans une fourchette de 100 à 200 jours.

La cybersécurité sera le sujet de la Matinée Stratégique de CIO le 16 février 2016 : Cybersécurité : Les nouvelles menaces contre le système d'information. … [Lire la suite]

Réagissez à cet article

Source : *La cybersécurité reste une problématique sous estimée dans les entreprises – Le Monde Informatique*

Quand la machine pourra t-elle dépasser l’homme ?



Quand la machine pourra t-elle dépasser l’homme ?

Face aux progrès déroutants de l'intelligence artificielle, de nombreuses voix s'élèvent et alertent face à l'avènement d'une ère d'asservissement de l'Homme à la machine. En réalité, même si elle a réalisé d'impressionnants progrès, la technologie est encore loin de rivaliser avec l'Homme.

Il existe dans la communauté de l'intelligence artificielle une date qui symboliserait le passage d'une ère d'algorithmes soumis à l'Homme à une ère de machines dominatrices : la « singularité ». Cet instant théorique cristallise les inquiétudes, car les machines, une fois conscientes de leur environnement, seraient capables de se retourner vers leurs créateurs.
Cette panique est encouragée par des discours d'« évangélistes » de l'intelligence artificielle, comme ceux de la Singularity University créée avec le soutien de Google et de la Nasa. Ceux-ci s'attellent à dépasser le monde biologique en repoussant, par exemple, les limites de la mort. Ce transhumanisme prophétique illustre un regain de popularité du progrès technologique après le grand désamour qui avait succédé aux excès guerriers de son usage au début du siècle.

Une avancée sans précédent

L'intelligence artificielle est un des bras armés de la révolution technologique, et ses prouesses ne cessent de surprendre. Le récent « grand bond en avant » vient du passage de programmes aux instructions éditées par l'homme, à des programmes « apprenants » où la machine déduit à partir d'exemples les causes d'une conséquence.
Les utilisations commerciales de l'intelligence artificielle sont elles aussi de plus en plus perfectionnées et concernent tous les aspects de la vie d'entreprise. Des start-up proposent à présent des assistants personnels avec qui il est possible de communiquer pour consulter ou modifier un agenda. La voiture automatique de Google se déplace depuis plusieurs années sur les routes américaines et montre un taux d'accidents plus faible d'un conducteur humain .
D'autres algorithmes sont capables de proposer les meilleurs itinéraires en temps réel en prenant en compte la circulation actuelle, et enfin, l'intelligence artificielle s'est récemment illustrée en battant les plus grands joueurs de Go , considéré comme l'un des jeux les plus difficiles.

La limite de l'excellence

Ces impressionnantes performances cachent en réalité la plus grande limite de l'intelligence artificielle, son excellence à réaliser une tâche particulière, et non un ensemble de tâches. L'Homme, s'il ne peut exceller dans tous les domaines, doit cette imperfection à sa capacité d'adaptation.
Notre propension à faire des erreurs témoigne de notre capacité à nous adapter au monde qui nous entoure et à rechercher des solutions innovantes à chaque problème. Cette capacité d'adaptation à l'environnement manque aujourd'hui à l'intelligence artificielle.

Une autre des grandes limites du Machine Learning tient de sa nécessaire interaction avec l'Homme. Si la machine est aujourd'hui capable d'étudier les relations entre plusieurs variables, de choisir les paramètres les plus judicieux à la résolution d'un problème, elle n'est en revanche pas capable d'imaginer à priori quels éléments utiliser et de les rechercher de façon proactive.
Par exemple, la reconnaissance d'objets sur photos demande d'effectuer de nombreux tests et de comparer plusieurs modèles. Le rôle de l'Homme est ici de rechercher les variables explicatives (couleurs des pixels, interactions entre certains éléments de l'image, etc.) et de demander à l'algorithme d'évaluer leur importance statistique.

Une logique trop fidèle au cerveau humain

Un des freins au progrès sans fin de l'intelligence artificielle tient de sa méthode de conception. C'est souvent du fonctionnement du cerveau humain que les chercheurs s'inspirent pour résoudre les problèmes les plus complexes.
Or, il est difficile d'imaginer des méthodes de réflexions dépassant l'expérience que nous avons du raisonnement logique. De plus, le cerveau humain est à notre connaissance l'ordinateur le plus performant, et la technologie actuelle est à des lieux de pouvoir le recréer.
Sa capacité de stockage, souvent révisée, est aujourd'hui estimée à 1 petabyte, soit 1.000.000 de gigabytes, où la capacité d'environ 2.000 ordinateurs actuels. Sa vitesse de traitement d'opérations et elle aussi remarquable, et sa capacité d'adaptation est telle qu'il est impossible de l'imaginer d'un point de vue algorithmique.

Un danger organisationnel

Le futur de l'intelligence artificielle ne sera donc pas dans un asservissement de l'Homme par la machine, mais dans une plus grande association entre le créateur et son outil. Elle doit, en revanche, nous faire réfléchir à notre place dans la société et dans l'entreprise. Si les hommes ne sont aujourd'hui pas physiquement menacés par l'intelligence artificielle, son avènement entraînera une transformation radicale de l'organisation et de la répartition du travail.
De nombreux emplois et services seront remplacés par des algorithmes intelligents et autonomes. Ainsi, le plus grand défi de la société face à l'intelligence artificielle sera de repenser le rôle de chacun, et d'adapter tous les acteurs de l'économie à cette transformation.
Par **Jonathan Trevier**, fondateur de Sparkism

Réagissez à cet article

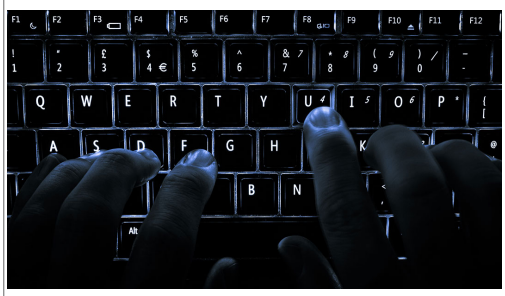
Source : *L'Homme dépassé par la machine, ce n'est pas pour demain, Le Cercle*

Comment les hackers font-ils pour pirater toutes vos données informatiques ?

	Comment les hackers font-ils pour pirater toutes vos données informatiques ?

Aujourd'hui, les informations sont partout avec le développement d'Internet. Il est donc important de savoir se prémunir contre les techniques employées pour nous pirater ou nous nuire. Surtout que les hackers, ces pirates du web, se développent de plus en plus et emploient des techniques toujours plus redoutables. SooCurious vous présente les techniques développées par ces génies malveillants de l'informatique.

Vous le savez certainement, le monde d'Internet est dangereux et est le terrain de jeu de personnes malveillantes. Ces gens sont appelés des hackers : ce sont des pirates informatiques qui se servent de leur ordinateur pour récupérer des informations privées ou pour infiltrer des serveurs de grosses entreprises. D'où l'importance de bien choisir ses mots de passe. Avant de pirater, le hacker va enquêter sur sa cible. Il va chercher tout ce qu'il peut savoir sur la personne, à savoir l'adresse IP, le type de logiciels installés sur l'ordinateur de la « victime ». Ils trouvent facilement ces informations grâce aux réseaux sociaux, aux forums en ligne. Une fois qu'ils ont récupéré ces données, le travail de piratage peut commencer.



Hacker n'est pas à la portée de tout le monde : il faut une maîtrise totale de l'informatique pour y parvenir. Ces pirates 2.0 ont plusieurs techniques pour parvenir à leurs fins. La première d'entre elles est le clickjacking. L'idée est de pousser l'internaute à fournir des informations confidentielles ou encore de prendre le contrôle de l'ordinateur en poussant l'internaute à cliquer sur des pages. Sous la page web se trouve un cadre invisible, comme un calque, qui pousse la personne à cliquer sur des liens cachés.
Par exemple, il existe des jeux flash où l'internaute doit cliquer sur des boutons pour marquer des points. Certains clics permettent au hacker d'activer la webcam.

Autre technique, peut-être plus courante, celle du phishing.
Appelée aussi l'hameçonnage, cette action opérée par le pirate vise à soutirer une information confidentielle comme les codes bancaires, les mots de passe ou des données plus privées. Pour récupérer un mot de passe, un hacker peut aussi lancer ce qu'on appelle « une attaque par force brute ». Il va tester une à une toutes les combinaisons possibles (cf. faire un test avec Fireforce) avec un logiciel de craquage. Si le mot de passe est trop simple, le hacker va rapidement pénétrer votre ordinateur. D'autre part, les hackers cherchent parfois à craquer les clés WEP, afin d'accéder à un réseau wi-fi. Encore une fois, si la clé est trop courte, le craquage est facile. Le hacking se développant, des techniques de plus en plus pointues se développent.

Vol des données bancaires via Shutterstock
Il existe maintenant des armées de hackers ou des groupes collaborant dans le but de faire tomber des grosses entreprises ou des banques. Début 2016, la banque internationale HSBC a été piratée. A cause de cela, leur site était totalement inaccessible, ce qui a créé la panique chez les clients de cette banque. Cet épisode n'est pas isolé. Il est même le dernier d'une longue série. Pour parvenir à semer la panique dans de grandes firmes, ils utilisent des techniques plus ou moins similaires à celles présentées ci-dessus, mais de plus grande envergure.

La technique du social engineering n'est pas une attaque directe.
C'est plutôt une méthode de persuasion permettant d'obtenir des informations auprès de personnes exerçant des postes clés. Les pirates vont cibler les failles humaines, plutôt que les failles techniques. Un exemple de social engineering serait l'appel fait à un administrateur réseau en se faisant passer pour une entreprise de sécurité afin d'obtenir des informations précieuses.

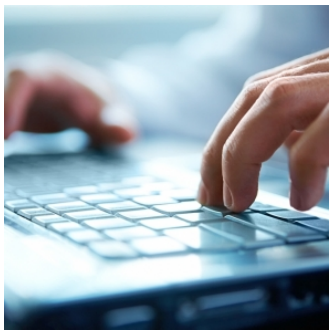
Autre méthode, celle du défaçage.
Cette dernière vise à modifier un site web en insérant du contenu non désiré par le propriétaire. Cette méthode est employée par les hackers militants qui veulent dénoncer les pratiques de certains gouvernements ou entreprises. Pour ce faire, le hacker exploite une faille de sécurité du serveur web hébergeant le site. Ensuite, il suffit de donner un maximum d'audience au détournement pour décrédibiliser la cible. En avril 2015, le site de Marine Le Pen a été victime de défaçage : des militants ont publié une photo de femme voilée avec un message dénonçant la stigmatisation des musulmanes par le FN.

Enfin, les hackers se servent aussi du DDOS (déni de service distribué), qui sature un service pour le rendre inaccessible et du Buffer Overflow, qui provoque une défaillance dans le système pour le rendre vulnérable… [Lire la suite]

Réagissez à cet article

Source : *Comment les hackers font-ils pour pirater toutes vos données informatiques ? | SooCurious*

Big Data : gare à vos données personnelles !



Big Data : gare à vos données personnelles !

Les marques, enseignes et sites Web cherchent à capter un maximum d'informations sur leurs clients. Leur objectif ? Vous vendre plus en vous soumettant des offres et promotions personnalisées. À la clé, des bons plans ou du harcèlement ? Débat.

Renseigner votre mail pour participer à un jeu concours, indiquer votre numéro de portable pour ne rater aucune vente privée, ou encore remplir un formulaire pour intégrer un programme de fidélité : il ne se passe pas une semaine où un magasin ou une marque ne vous sollicitent pour obtenir des informations personnelles sur vous, votre famille et vos habitudes de consommation. Et sur le Web, même combat. Les sites Internet ont même un avantage puisqu'ils peuvent obtenir des informations via les fameux cookies et ainsi savoir quel site vous avez visité ou encore quels sont les produits que vous avez regardés sur la Toile.

Peut-être avez-vous déjà remarqué que le fameux ordinateur ou la paire de bottes que vous convoitez se retrouve dans un carré de pub les heures ou les jours suivants votre session de surf ?

Globalement, les Français communiquent facilement et de façon importante des informations sur eux. C'est ce que révèle l'enquête 2015 « Les Français et leurs données personnelles » réalisée par Ipsos pour Elia Consulting. Plus exactement, les résultats démontrent qu'il y a un décalage entre la méfiance grandissante des utilisateurs sans pour autant qu'ils changent leur comportement. Ainsi, paradoxalement, les Français renseignent fréquemment et en quantité leurs données personnelles, malgré leur opposition de principe à leur utilisation par les entreprises et la conscience des risques qui y sont associés. 74% déclarent partager régulièrement des données personnelles, ce qui s'explique souvent par la contrainte de fournir ces informations pour terminer un acte d'achat ou bénéficier d'un service (73% des Français renseignent leurs données personnelles pour terminer un acte d'achat). D'ailleurs, seul un internaute sur trois prend le temps de lire les conditions générales de vente ou de modifier les paramètres de sécurité de leurs réseaux sociaux et smartphones (33% dans les deux cas).

Des données pour quoi faire ?

Les Big Data, ou mégadonnées en français, désignent l'ensemble des informations que l'on peut capter et représentent le nouvel or noir des professionnels. En effet, l'objectif pour ces derniers consiste à bien cerner un client et lui glisser ainsi la bonne offre ou le bon service, au bon moment, et avec le bon prix. Amazon teste même un service aux États-Unis où le client reçoit un produit sans l'avoir commandé, en fonction de son historique d'achats. Libre à lui de le garder – dans ce cas, il sera débité dans les jours suivants – ou de le renvoyer si le produit ne lui convient pas.

En France, nous n'en sommes pas encore là. L'usage des mégadonnées reste encore peu développé, faute de moyens techniques et financiers à allouer à ce sujet. L'idée serait plutôt, dans le secteur du commerce, d'utiliser la « smart data », autrement dit celle qui fera la différence pour déclencher une intention d'achat chez le consommateur.

Pour illustrer l'usage des mégadonnées, prenons un cas pratique avec Monoprix par exemple. L'enseigne envoie à tous les porteurs de la carte de fidélité des bons de réduction. Or, ces fameux coupons nominatifs ont été définis en fonction des informations fournies initialement (genre, âge, situation matrimoniale, etc.) et des derniers achats effectués par le consommateur. Ainsi, un homme n'aura, en théorie, pas de réduction pour du maquillage. Et s'il consomme surtout des plats cuisinés, ces derniers se retrouveront dans ses bons de réductions.

Manque de transparence ?

Toujours selon l'enquête Ipsos, les Français sont parfaitement conscients que leurs données personnelles peuvent être utilisées. D'ailleurs, 9 sondés sur 10 (92%) pensent que les informations qu'ils renseignent peuvent être utilisées ou conservées pour un usage futur par le fournisseur de services. Mais dans la majorité des cas, les Français se sentent mal informés sur l'utilisation qui en est faite.

L'utilisation des données par les professionnels reste en réalité un jeu à double tranchant. En effet, si votre magasin d'électronique préféré vous envoie des promotions qui ne vous intéressent absolument pas, il y a fort à parier que vous allez vite couper toute relation avec lui. Pas forcément ne plus acheter chez lui, mais il ne pourra plus vous contacter pour vous inciter à venir en point de vente ou à vous rendre sur son site Web. Par ailleurs, même si les professionnels ont en leur possession de nombreuses données sur vous, ils font attention à ne pas devenir trop intrusifs. Imaginons que vous êtes en train de chercher un nouveau parfum et que la vendeuse vous lance : « Vous avez acheté depuis deux ans uniquement des fragrances sucrées, celui-ci est très différent ». D'un côté, vous bénéficieriez d'un conseil super personnalisé mais, d'un autre côté, vous réaliseriez que la dame en face de vous que vous ne connaissez pas sait beaucoup de choses sur vous…

Vigilance de mise

Si dans les faits, il devient presque impossible de ne fournir aucune donnée personnelle, il convient, néanmoins, de réfléchir à qui vous les donnez, de vérifier dans les petites lignes à quoi elles serviront, et d'identifier les gains que cela vous apportera. En effet, comme les professionnels veulent un maximum d'informations pour mieux vous cerner, ils proposent… [Lire la suite]

Réagissez à cet article

Source : *Big Data : gare à vos données personnelles !*

La CNIL attaque Facebook. Que lui reproche t-elle ?

	La CNIL attaque Facebook. Que lui reproche t-elle ?

La Commission nationale informatique et liberté (CNIL), l'autorité chargée de la protection des données personnelles, a annoncé avoir mis en demeure Facebook, lundi 8 février, lui reprochant de nombreux manquements à la loi française sur la protection des données personnelles. Un long réquisitoire, contre la manière dont Facebook collecte et exploite les données de ses 30 millions d'utilisateurs français, que la CNIL a décidé de publier.

Que reproche-t-elle à Facebook ? La liste est longue.

UNE CHARGE CONTRE LA PUBLICITÉ CIBLÉE

La CNIL estime que Facebook combine les données personnelles de ses usagers pour proposer de la publicité ciblée sans aucune base légale. Pour la CNIL, aucun consentement direct n'est donné par l'internaute, contrairement à ce qu'exige la loi française. La question de la combinaison des données personnelles en vue de la publicité est bien évoquée dans les conditions d'utilisation du réseau social, ce texte qui définit ce que peut faire ce dernier avec les données. Pour la CNIL, c'est insuffisant : la combinaison de différentes données n'est pas strictement prévue par ce « contrat » entre l'usager et le réseau social, et nécessite donc une approbation distincte de l'internaute.

La CNIL remarque que Facebook pourrait s'affranchir de ce consentement explicite en arguant, conformément à la loi, que l'affichage de publicité est fait dans l'intérêt de l'usager. Selon la CNIL, cet intérêt est trop faible et la collecte de données trop intrusive pour que Facebook se dispense d'un consentement.

DES DONNÉES COLLECTÉES TROP SENSIBLES

Dans certains cas, Facebook réclame des copies de documents permettant d'identifier l'utilisateur (afin, notamment, d'éviter qu'il se fasse passer pour quelqu'un d'autre). Parmi ces pièces, l'internaute peut soumettre un dossier médical : la CNIL estime que ce document est trop sensible et que le réseau social ne doit plus l'accepter.

Tout utilisateur de Facebook peut aussi renseigner, sur son profil, sa sympathie politique et ses préférences sexuelles. La CNIL juge que pour se conformer à la loi, Facebook devrait indiquer précisément ce qu'il compte faire de ces informations, compte tenu de leur sensibilité et de leur nature particulière que leur confère la loi française.

UN MANQUE DE TRANSPARENCE

La CNIL critique aussi vertement la manière dont Facebook explique à ses utilisateurs ce qui va être fait de leurs données personnelles. Pour la Commission, il faudrait que le réseau social les informe clairement dès le formulaire d'inscription à Facebook, conformément aux textes français, et non pas dans un texte séparé.

La CNIL juge aussi que les utilisateurs de Facebook ne sont pas suffisamment informés sur le fait que leurs données sont transférées aux USA.

UTILISATION ILLICITE DU SAFE HARBOR

Au sujet du transfert des données vers les Etats-Unis, la CNIL reproche aussi à Facebook de s'appuyer sur l'accord Safe Harbor. Ce dernier prévoyait que les données puissent librement être transférées, par des entreprisescomme Facebook, vers les Etats-Unis, au motif que ce pays apportait des garanties suffisantes en matière de protection des données. En octobre, la Cour de justice de l'Union européenne en a décidé autrement et l'a invalidé, au motif notamment que les Etats-Unis ne protégeaient pas suffisamment les données des Européens. La CNIL demande donc à Facebook de cesser de se baser sur cet accord pour transférer de l'autre côté de l'Atlantique les données de ses utilisateurs français.

PROBLÈMES DE COOKIES

Comme son homologue belge et la justice de Bruxelles avant elle, la CNIL reproche à Facebook son utilisation du cookie « datr ».

Lire aussi : La Belgique ordonne à Facebook de cesser de tracer les internautes non membres

Un cookie est un fichier qui peut être stocké sur l'ordinateur ou le téléphone d'un internaute lorsqu'il visite un site Web : il sert à mémoriser certaines informations (comme un mot de passe par exemple) ou à le reconnaître lorsqu'il visite à nouveau le même site. Facebook dépose le cookie « datr » y compris sur les appareils d'internautes qui n'ont pas de compte Facebook, lorsque ces derniers se rendent sur des pages Facebook accessibles à tous. De plus, le cookie mémorise toutes les visites de l'internaute sur les pages Web dotées par exemple du bouton « J'aime », soit la majeure partie des sites Web communément visités par les internautes français.

Facebook a fait valoir auprès la CNIL les mêmes arguments qu'il avait opposés aux autorités belges : ce cookie est destiné à reconnaître les utilisateurs « normaux » de Facebook — pour notamment empêcher le spam ou la création massive de compte — et aucun « pistage » des internautes non-inscrits à Facebook n'est effectué. Pour la CNIL, cette raison, valable, n'est pas suffisante : elle réclame à Facebook de mieux informer les utilisateurs de l'utilisation de ce cookie et des données qu'il mémorise.

La CNIL reproche aussi à Facebook de stocker trop longtemps les adresses IP — un numéro qui identifie la connexion utilisée par l'internaute pour se connecter à Internet — de ses utilisateurs.

La Commission, dans sa mise en demeure, fait de la loi de 1978 sur les données personnelles une lecture très littérale. Elle estime par exemple que Facebook y déroge en ne réclamant pas à ses utilisateurs, lorsqu'il s'inscrit, de mot de passe suffisamment compliqué. La Commission pointe qu'elle a pu s'inscrire sur le réseau social avec le mot de passe « 123456a », particulièrement faible car facile à deviner. Pour la Commission la loi impose à Facebook de prendre toutes les mesures pour protéger les données de ses membres, y compris, donc, en réclamant des mots de passe sûrs. Cette application pointilleuse devrait inquiéter de nombreuses entreprises du Web dont les pratiques sont similaires à celle du plus grand réseau social du monde.

Le réseau social dispose désormais de trois mois pour pallier les manquements repérés par la CNIL, ou demander une extension de ce délai. À l'issue de cette période, la CNIL pourra, si elle estime que Facebook n'a pas suffisamment modifié ses pratiques, entamer une procédure de sanction. … [Lire la suite]

Réagissez à cet article

Source : *Données personnelles : le virulent réquisitoire de la CNIL contre Facebook*

Le site Internet des Pays de la Loire piraté

Le #site Internet des Pays de la Loire piraté

Après le site web du Parti Socialiste, les Anonymous ont attaqué celui du conseil régional des Pays de la Loire pour protester contre une pétition demandant l'évacuation de la ZAD de Notre-Dame des Landes.

Le site Internet du Conseil régional des Pays de la Loire a été altéré suite à une attaque dans la nuit de dimanche à lundi revendiquée par les Anonymous selon France Bleu. Le groupe d'activistes entend protester contre le projet d'aéroport à Notre-Dame des Landes et plus précisément contre la pétition en ligne demandant l'évacuation de la ZAD (Zone d'aménagement différée) à l'initiative de Bruno Retailleau, président du conseil régional. Le site est toujours bloqué avec une page indiquant simplement : « Cette page est introuvable. Merci de revenir un peu plus tard. »

Dans un communiqué, le groupuscule indique que « grâce au piratage du site du Conseil régional nous entendons démontrer à tous et toutes comment les citoyens ont été délibérément trompés et manipulés par Bruno Retailleau ». Les activistes, qui assurent avoir récupéré le listing des votants, contestent en effet l'organisation de cette pétition : « Nous avons pu constater que certains mails sont comptabilisés plusieurs dizaines de fois, et les mêmes adresses IP ont pu inscrire des dizaines d'adresses mails à la suite, sans aucune vérification, poursuivent les Anonymous. N'importe quelle adresse mail peut ainsi s'enregistrer sans aucune preuve de son authenticité. Au total, près de 40 % des signatures seraient à décompter. »

Aucune donnée dérobée

Ce n'est pas la première fois que les Anonymous s'intéressent au projet d'aéroport de Notre-Dame des Landes. Le 26 janvier dernier, ils avaient déjà lancé une attaque de type DDoS contre le site web du Parti Socialiste pour protester pêle-mêle contre l'instauration de l'État d'urgence, les perquisitions et les arrestations non-fondées qui ont notamment touché les opposants à l'aéroport de Notre-Dame des Landes. Le groupe avait précisé qu'il envisageait d'autres actions « si l'état d'urgence n'était pas rectifié ». C'est désormais chose faite avec le blocage du site des Pays de la Loire qui n'est toujours pas revenu à cette. Le Conseil général, qui s'active toujours avec ses prestataires pour remettre sa vitrine, a indiqué … [Lire la suite]

Réagissez à cet article

Source : *Les Anonymous piratent le site des Pays de la Loire – Le Monde Informatique*

Privacy Shield : attente des détails

	#Privacy Shield : attente des détails

Le groupe de l'article 29 a accueilli favorablement la conclusion de l'accord « EU-US Privacy Shield ».

Cependant, en dépit des efforts réalisés par les Etats-Unis, il réitère ses préoccupations concernant les nécessaires garanties à apporter.
Ainsi, dans son communiqué de presse en date du 3 février 2016 (1), le groupe de travail de l'article 29 rappelle, sur le fondement de la jurisprudence européenne, que quatre garanties essentielles devront être apportées pour encadrer notamment les activités de renseignement, à savoir que :
• le traitement doit être fondé sur des règles claires, précises et accessibles, de telle sorte que toute personne raisonnablement informée puisse savoir comment ses données sont traitées en cas de transfert ;
• un juste équilibre doit être trouvé entre les finalités pour lesquelles les données sont collectées et traitées et les droits des individus ;
• un système indépendant doit être mis en place pour assurer de manière effective et impartiale les contrôles nécessaires ;
• des voies de recours devant des juridictions indépendantes doivent être créées.

Le groupe de l'article 29 est dans l'attente de recevoir l'intégralité de la documentation du « Privacy Shield » afin de pouvoir analyser en détail son contenu.
Le groupe de l'article 29 appréciera alors si le Privacy Shield peut apporter les garanties nécessaires pour assurer un niveau de protection adéquat des données à caractère personnel, niveau qui n'est plus assuré par le Safe Harbor et a été remis en cause dans le cadre de l'affaire Schrems.
En particulier, le groupe de l'article 29 va apprécier dans quelle mesure ce nouvel accord va apporter des réponses quant à la validité des autres mécanismes de transfert.
Le groupe de l'article 29 appelle donc la Commission à lui communiquer tous les documents relatifs au « Privacy Shield » d'ici la fin du mois de février. Il sera alors en mesure de finaliser son analyse des transferts de données vers les Etats-Unis, à l'occasion d'une assemblée plénière qui sera organisée dans les semaines à venir.
A l'issue de ce délai, le groupe de l'article 29 se prononcera sur le sort des Clauses contractuelles types et des Règles Internes d'Entreprise. Dans cette attente, le groupe de travail de l'article 29 considère … [Lire la suite]

Réagissez à cet article

Source : *Le groupe de l'article 29 attend la communication du Privacy Shield*

Transfert de données personnelles entre l’UE et les Etats-Unis : Accord politique trouvé

Transfert de données personnelles entre l’UE et les Etats-Unis : Accord politique trouvé

Bruxelles – L'UE et les Etats-Unis sont parvenus la semaine dernière à un « accord politique » censé mettre fin à l'insécurité juridique dans laquelle sont plongées depuis des mois les entreprises transférant des données personnelles de l'Europe vers les Etats-Unis.

Fruit d' »intenses négociations », le nouveau cadre annoncé mardi par la Commission européenne est destiné aux transferts transatlantiques de données personnelles entre entreprises, et doit remplacer celui qui a été invalidé en octobre dernier par la justice européenne.
Salué par les milieux économiques concernés, l'accord a cependant déjà fait l'objet de vives critiques, notamment de députés européens doutant de sa portée juridique.

Dans un arrêt retentissant concernant le réseau social Facebook mais de portée générale la Cour de justice de l'UE avait exigé de meilleures garanties pour la confidentialité des données des Européens sur le sol américain.

Les données personnelles en question englobent toutes les informations permettant d'identifier un individu, de manière directe (nom, prénom ou photo) ou indirecte (numéro de sécurité sociale ou même numéro de client).

Nouveau « bouclier »
Les précédentes règles, connues sous le nom de « Safe Harbor », régissaient depuis quinze ans les transferts transatlantiques de données. Sa remise en cause a provoqué un séisme pour des milliers d'entreprises, des géants comme Facebook aux nombreuses petites et moyennes entreprises traitant aux Etats-Unis des données recueillies en Europe.
Depuis plusieurs mois, elles attendaient un cadre juridique de substitution, que la Commission européenne, plutôt que « Safe Harbor 2 », a préféré rebaptiser mardi « Bouclier de confidentialité UE-USA ».

Il protégera les « droits fondamentaux » des Européens, a assuré la commissaire européenne chargée de la Justice, Vera Jourova, et donnera aux entreprises « la sécurité juridique dont elles ont besoin », a appuyé son collègue Andrus Ansip, responsable du numérique, lors d'une conférence de presse à Strasbourg.
Pour répondre aux demandes de la justice européenne, l'exécutif bruxellois a assuré que ce nouveau système serait « vivant », avec des révisions annuelles, alors que « Safe Harbor » avait fait l'objet d'un accord unique en 2000.
« Pour la première fois, les Etats-Unis ont donné à l'UE des garanties contraignantes que l'accès » aux données des Européens par les autorités américaines « feront l'objet de limites claires, de garde-fous et de mécanismes de supervision », a assuré la Commission.

Un « ombudsman » (médiateur) sera établi au sein du Département d'Etat américain, pour suivre les éventuelles plaintes et requêtes de citoyens européens concernant un accès à leurs données pour des questions de sécurité nationale.

Réagissez à cet article

Source : *Transferts de données personnelles: « Accord politique » entre l'UE et les Etats-Unis – L'Express*

Des données personnelles de

développeurs trouvés dans des caméras de surveillance

Des données personnelles de développeurs trouvés dans des caméras de surveillance

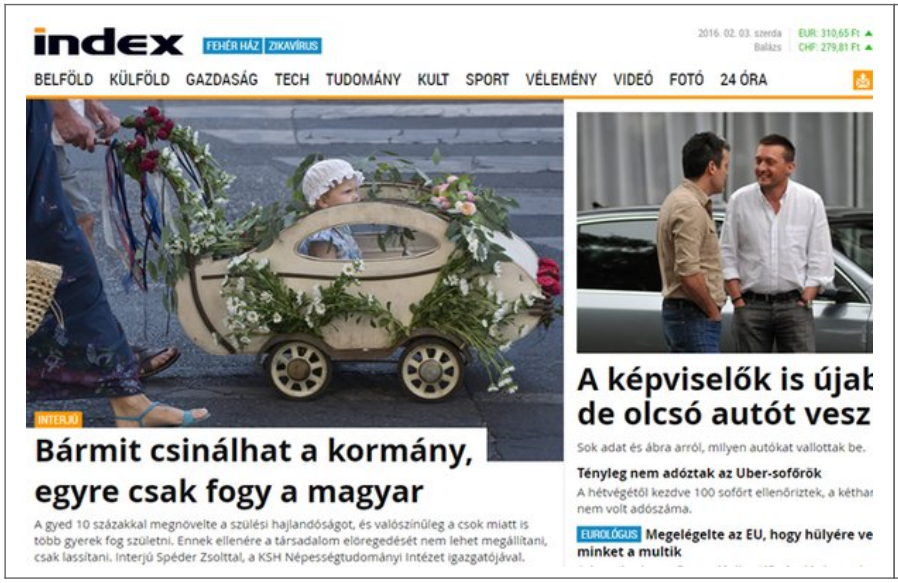
Gmail, Dropbox et comptes FTP, voici ce qu'ont laissé des développeurs dans les entrailles des caméras sur lesquelles ils travaillaient. Des informations personnelles qui montrent le manque de vigilance de ces techniciens, ayant utilisés leurs comptes privés lors du développement de ces caméras… Une affaire qui pourrait faire tâche sur les CV de ces indélicats !

Selon un article de Forbes, des développeurs ayant travaillé sur la création du software pour les caméras Motorola Focus 73 ont fait preuve d'un manque de vigilance flagrant au moment de finaliser leur travail, juste avant la commercialisation de ce modèle. Des experts de « Context Information Security » sont parvenus à accéder aux entrailles des caméras, et on pu en extraire plusieurs informations suprenantes. Les développeurs y avaient laissé trainer leurs identifiants Gmail, Dropbox et FTP d'entreprise.
Les caméra, facilement piratées et contrôlables à distance pour quiconque ayant un minimum de connaissance dans le domaine, ont apporté la preuve de la négligence de ces développeurs, comma l'a expliqué le responsable de Context Information Security :
Les comptes laissés dans le firmware sont apparus comme étant des comptes de développeurs partagés, utilisés pour recevoir les alertes de mouvement et les extraits de vidéo pour leurs tests. Nous n'avons pas accédé à ces comptes pour des raisons légales, mais nous avions tout ce qu'il nous fallait pour le faire. (…) On ne s'attend pas à ce qu'une entreprise de développement utilise ce type de comptes pour ce genre d'activité et ils n'auraient certainement pas du être laissés dans le firmware final.
Un constat d'autant plus affligeant que les mots de passe utilisés pour la sécurité des caméras et ces comptes Gmail sont plus que décevants : « 000000 » ou « 123456 ».

Réagissez à cet article

Source : *Gmail : des données personnelles de développeurs trouvés dans des caméras de surveillance – 1001Web*

Propos injurieux ou diffamatoires sur Internet : Quelle est la responsabilité des sites Internet ?



Propos injurieux ou diffamatoires sur Internet : Quelle est la responsabilité des sites Internet ?

La Cour européenne des droits de l'homme (CEDH) considère qu'un site d'information hongrois n'était pas responsable des propos injurieux laissés sur son forum. La Justice du pays l'avait pourtant condamné à verser une indemnisation au plaignant.

Dans un arrêt rendu hier par la CEDH, la Hongrie est condamnée à verser 5 100 euros au portail d'information hongrois Index.hu, pour violation de l'article 10 (liberté d'expression) de la Convention européenne des droits de l'homme. Suite à un verdict de la Justice hongroise accusant le site d'avoir laissé des commentaires insultants sur leur forum, Index.hu avait saisi la Cour européenne.

La plainte est à l'origine déposée par un site d'annonces immobilières, qui s'insurge contre des propos laissés sur Index.hu mettant clairement en cause leur honnêteté commerciale. Le portail d'information avait d'abord dénoncé leur offre « gratuite pendant 30 jours », sans en même temps stipuler que l'inscription devenait automatiquement payante ensuite. Choqués, des internautes avaient vivement réagi sur le forum d'Index.hu, laissant des commentaires franchement injurieux.

La Justice hongroise avait donné raison au site immobilier, considérant que le portail d'information était responsable des propos publiés sur leur site. Mais pour la Cour européenne des droits de l'homme, les juges hongrois « n'ont absolument pas mis en balance l'intérêt à préserver la liberté d'expression sur Internet ».

Le portail d'information hongrois « Index.hu »

Le premier jugement revendiquait l'atteinte au respect de la réputation commerciale, mais la CEDH met en avant qu'Index.hu avait pris en amont des mesures louables comme la publication d'une clause de déni responsabilité et la mise en place d'un système de retrait sur notification.

Où s'arrête la liberté d'expression

Le point crucial du nouveau verdict réside dans la substance même des commentaires publiés : il s'agissait de propos certes « injurieux » et « grossiers » mais ne constituaient pas des « déclarations de faits diffamatoires ». L'arrêté précise que la simple expression de jugements de valeur ou d'opinions ne peut être condamnable car elle est protégée par l'article 10 de la Convention sur la liberté d'expression.

Mais il y a un précédent européen dans ce même type d'affaire, exprimé en juin par la Cour européenne, qui à l'inverse condamnait le site d'information estonien Delfi pour des raisons similaires. Mais la CEDH invoque une différence notable dans la nature des propos relatifs aux deux dossiers : dans le cas de Delfi, il y avait « discours de haine et l'incitation à la violence ».

Pourtant dans l'affaire Index.hu , la minimisation des propos tenus peut faire débat. Exprimer le souhait que les salariés du site immobilier décèdent semblent se rapprocher de la définition donnée d'incitation à la violence. Au final, la différence qu'ont fait les juges entre ces deux dossiers est très subtile et pourrait résider dans le fait que dans le cas Delfi, les menaces étaient plus nombreuses, plus claires et moins assimilables à des railleries de mauvais goût, en plus d'être dirigées à l'encontre d'un seul homme (et non d'un groupe), en l'occurrence monsieur L., actionnaire unique ou majoritaire de la société dont il était question dans l'article, également membre de son conseil de surveillance.

Le document de la Cour Delfi AS c. Estonie contient 22 pages de désaccords, exprimés par les juges Sajo et Tsotsoria.

Responsabilité du modérateur

L'article 93-3 de la loi française du 29 juillet 1982 sur la communication audiovisuelle, dégageant la responsabilité des modérateurs dans ce genre de cas, avait été réexaminé en 2011 par Le Conseil constitutionnel et jugé conforme à la Constitution.

Le droit français établit donc que le modérateur ou directeur de publication ne peut pas être condamné pour des propos illicites publiés sur un forum, s'il est établi qu'il n'en avait pas connaissance avant sa publication (modération a posteriori), et s'il les retire au plus tard dans les 48 heures après qu'une demande ait été émise par le plaignant.

Pour la Cour européenne, l'article 10 de la Convention sur la Liberté d'expression est le seul référent, ce qui implique une appréciation aiguë des contenus à l'origine du litige. Cet article admet que des « restrictions » au champ de la liberté d'expression peuvent être envisagées, tout en laissant aux procureurs la marge d'appréciation de leur application.

Ce verdict rendu hier suite à l'affaire du site hongrois contribue donc à créer une jurisprudence européenne autour du domaine particulièrement délicat de la liberté d'expression en ligne.

Réagissez à cet article

Source : *Propos injurieux : les sites ne sont pas responsables*