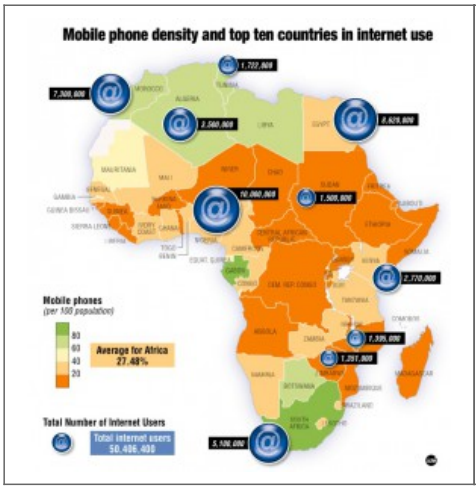
En Afrique la communication digitale s’impose en entreprise Le Net Expert Informatique



En Afrique la communication digitale s’impose en entreprise

Décidément, la communication digitale rivalise avec les outils du marketing classique, et grignote désormais une part importante du « budget communication » des entreprises, associations, organisations et institutions gouvernementales.

Au fur et à mesure de l'accroissement de l'utilisation d'Internet en Afrique, les différentes formes d'entreprises et institutions se tournent de plus en plus vers des experts en communication digitale pour renforcer leur présence sur le web.
« le nombre des utilisateurs d'Internet en Afrique devrait être multiplié par 3.5 d'ici 2015 pour que le nombre d'internautes atteigne près de 600 millions » Indique l'UIT

Quelques chiffres clés sur le digitale en Afrique
Selon le rapport annuel publié par l'UIT (Union Internationale des Télécommunications), en fin de l'année 2014, seulement 42% de la population mondiale soit 3,025 milliards de personnes utilisent le réseau internet. Sur l'ensemble du continent africain, le taux de pénétration d'Internet est estimé à 16% en 2014 soit 167 millions d'internautes, contre 110 millions en 2010, une croissance considérée relativement importante en une période de 4 ans. Selon la même source, le nombre des utilisateurs d'Internet en Afrique devrait être multiplié par 3.5 d'ici 2015 pour que le nombre d'internautes atteigne près de 600 millions.

Pénétration Internet et Mobiles dans les pays d'Afrique
La même année Google a également réalisé une étude statistique portant sur le comportement des internautes dans le monde notamment les Africains qui sont de plus en plus présents sur Internet dans l'objectif d'acheter quelque chose ou simplement consulter des produits sur le web. Cette étude chiffrée indique que l'augmentation des achats en ligne est de 33% au Kenya, 37% en Afrique du Sud et 49% au Nigeria.
Ces chiffres illustrent en partie l'évolution du comportement des Africains vis-à-vis du réseau internet.
Ces estimations indiquent également un avenir prometteur pour la communication digitale sur ce continent. Les pays les plus matures en matière de marketing digital sont certainement ceux ayant les taux de pénétration d'Internet les plus élevés, à citer le Nigeria, l'Afrique du Sud, l'Égypte, le Maroc et la Tunisie.

Rôle des agences de communication digitale ou webmarketing
Une présence proactive sur Internet permet non seulement de maîtriser l'e-réputation mais aussi de booster les ventes et conquérir de nouveaux marchés. Les agences de communication digitale utilisent aujourd'hui des techniques très avancées pour cibler efficacement les internautes et aussi suivre l'audience des sites web.
En exemple, l'Inbound marketing (ou marketing entrant), par opposition au marketing classique, consiste à faire venir le client vers l'entreprise. Cette forme de webmarketing, mettant en œuvre divers leviers du marketing digital, prouve depuis quelques temps son pourvoir et son mérite d'être un moyen de communication pertinent. Chaque site internet devient donc son propre média en diffusant en ligne des contenus attractifs, de bonne lisibilité et visibilité.

Le marketing digital ou webmarketing, est assez vaste qu'il devient difficile à cerner
Ce nouveau mode de communication touche divers domaines, de la création des sites internet au management de l'e-réputation en passant par le référencement, la gestion des contenus web et la diffusion d'informations via les réseaux sociaux, sans oublier les bannières, outil de publicité classique sur Internet.

L'un des avantages du marketing digital est qu'il permet de communiquer directement avec les clients et de suivre efficacement leur comportement, contrairement au marketing traditionnel. Cette forme de marketing permet également un certain degré de précision pour le ciblage des internautes par centres d'intérêt, âge, sexe ou encore par zones géographiques.

Source : http://www.info-afrique.com/5336-en-afrique-communication-digitale/
Par Thierry Barbaut avec l'Agence 360

Réunion de crise de 8 banques à cause d’attaques de hackers | Le Net Expert Informatique

Réunion de crise de 8 banques à cause d’attaques de hackers

De nos jours les attaques par des hackers font partie du quotidien. Souvent on reçoit des mails par des expéditeurs inconnus qui ont pour but de parvenir aux données personnelles des clients. Les banques sont souvent ciblées lors de tels envois: le système « multiline » offert par 8 banques du Grand-Duché est actuellement dans la ligne de mire.

Attention! N'ouvrez aucun fichier ou document émis par l'adresse email suivante: helpdesk@multiline.lu !
Ceci est un message obtenu directement lorsque qu'on se rend sur le site Multiline.

Multiline est un service dit « e-banking » pour professionnels et entreprises (pour leur gestion financière) proposé depuis 1992.
Bien que ce système paraisse assez sécurisé (collaboration avec Luxtrut et Cetrel) il a quand même fait l'objet de cyberattaques.
Les dégâts ont été tels que 8 banques utilisant ce système (BCEE, Banque de Luxembourg, Raiffeisen, BIL, Poste, BGL BNP Paribas, ING et Société Générale) se sont réunies en cellule de crise.
Il n'y a pas encore d'informations disponibles émanant de l'ABBL, de la Cetrel ou de Multiline.
Le situation serait sous contrôle, un communiqué officiel est attendu pour le mardi de pentecôte.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://5minutes.rtl.lu/fr/actualite/alaune/634917.html

Le Bundestag se montre incapable de surmonter une cyber-attaque | Le Net Expert Informatique

Le Bundestag se montre incapable de surmonter une cyber-attaque

Depuis quelques semaines le parlement allemand est victime d'attaques informatiques à répétition. Un phénomène qui inquiéte certains députés.

Le Bundestag est vulnérable. Depuis le début du mois de mai, les services informatiques du parlement allemand sont la cible de cyber-attaques répétées. Les députés ne sont plus en mesure de sécuriser leurs communications. Des données ont été piratées, sans qu'il soit possible d'en connaître la nature. Impossible pour l'heure de savoir si des documents confidentiels ont été volés. «Et ce n'est pas terminé», a déclaré un porte-parole, selon des propos rapportés par les médias allemands, comme Der Spiegel ou Die Zeit, qui ont notamment révélé l'affaire. Le «cheval de Troie» utilisé par les hackers n'a pas encore été neutralisé. Selon le quotidienSüddeutsche Zeitung, le BSI, chargé de la sécurité fédérale informatique, aurait même demandé une aide extérieure pour en venir à bout.
L'exaspération et l'inquiétude commencent à se répandre au Bundestag, principalement dans les rangs de l'opposition. Les députés Verts et Die Linke semblent davantage touchés par l'attaque. Mais la cible exacte des hackers reste encore inconnue. «L'incertitude demeure sur l'intensité de l'attaque et son ampleur», a expliqué le député Vert Konstantin von Notz, spécialiste des questions informatiques. «Il n'y avait encore jamais une telle attaque pendant plusieurs jours», a déploré la vice-présidente Petra Pau (Die linke). «Il y a une attente évidente pour que la protection des communications soient rétablies», a observé le responsable SPD Lars Klingbeil. Le Bundestag envisage la possibilité de devoir réinstaller totalement l'infrastructure du réseau, pour purger la menace. Toute l'activité informatique du Bundestag en serait interrompue. L'opération pourrait avoir lieu au moment des vacances parlementaires, en juillet.

20 tentatives d'intrusion par jour en 2014
Qui se cache derrière l'assaut? Pour l'instant, la seule piste connue mène vers Europe de l'Est, où sont situés des serveurs qui auraient infiltré au moins deux ordinateurs du Bundestag. Mais l'enquête de la Sécurité intérieure est toujours en cours. Toutefois, à écouter les experts, la complexité de l'attaque témoigne d'une capacité technologique dont seuls des services secrets peuvent disposer.
Il ne s'agit pas de la première attaque informatique dont est victime l'administration allemande, loin de là. Selon le BSI, les services internes du gouvernement auraient subi en moyenne 20 tentatives d'intrusion par jour l'année dernière. Des services de renseignement étrangers seraient à l'origine d'au moins une attaque quotidienne. Pour renforcer la sécurité informatique de l'Allemagne et notamment de ses entreprises, le gouvernement élabore un nouveau projet de loi. «Avec cette loi, une amélioration significative de la sécurité des communications informatiques devra être atteinte», promet le texte en préparation. Le Bundestag sera amené à en débattre.

Source : http://www.lefigaro.fr/international/2015/05/22/01003-20150522ARTFIG00173-le-bundestag-se-montre-incapable-de-surmonter-une-cyber-attaque.php

---

Comment s'assurer contre le cyber-risques ? | Le Net

Expert Informatique

Comment s’assurer contre le cyber-risques ?

Diverses études montrent que les entreprises sont mal préparées pour lutter contre le hacking. Les grands assureurs affinent leurs stratégies commerciales.

Sony, Home Depot, JP Morgan, TV5 Monde, Target… Le nombre d'entreprises victimes de cybercriminalité explose. Mais les couvertures d'assurance contre ce type de méfait ne font qu'émerger. Les vols de données, espionnages et autres attaques de systèmes informatiques coûtent pourtant 300 à 1000 milliards de dollars, selon la société de sécurité informatique McAfee.
La Suisse n'est pas épargnée. Dernier exemple en date: Implenia. Selon une étude récente de l'Université de Saint-Gall (https://www.alexandria.unisg.ch/Projekte/238276), plus de 90% des entreprises ont été touchées par des attaques de hackers, l'année passée. «Les PME se sentent, à tort, à l'abri. Leur protection est insuffisante», juge son auteur, Martin Eling.
Elles semblent effectivement ne pas être préparées, comme en témoigne le sondage de KPMG auprès de 64 entreprises, présenté mercredi à la presse. Son auteur, Matthias Bossardt, parle d'un «cycle de complaisance». **Plus de la moitié des sociétés interrogées croient que leur organisation est capable de détecter des attaques. Mais 45% n'ont pas de plan pour y répondre**. Même si celles-ci ne cessent de se transformer, 79% des entreprises interrogées n'ont pas changé leurs plans, ces 12 derniers mois. 7% d'entre elles n'ont même pas pris de mesure, après une attaque.

En moyenne, 229 jours s'écoulent jusqu'à la mauvaise surprise
Les entreprises ne découvrent que fort tard qu'elles sont piratées. «**En moyenne, 229 jours s'écoulent jusqu'à la mauvaise surprise**», explique Manuel Meier, directeur général de la division entreprises pour Zurich Insurance. Sur le plan global, le coût du cyber-risque correspond à celui des catastrophes naturelles. Mais sa complexité est supérieure. L'incendie ou l'effraction sont plus aisés à localiser et immédiatement visibles. «La cybercriminalité, dont l'origine est souvent étrangère, change la façon d'appréhender un sinistre», analyse l'assureur.
Le thème s'est imposé aux Etats-Unis, où «un tiers des entreprises ont déjà signé un contrat de cyberassurance», affirme Manuel Meier. Le marché américain est estimé à 1,3 milliard de dollars en 2013 par le rapport «Betterley», contre 150 millions d'euros en Europe continentale.
«Le cyber-risque nous préoccupe surtout depuis cinq ans», précise Carin Gantenbein, responsable de ce risque au sein de Zurich Insurance. L'importance du cyber-risque s'est accrue fortement à la suite de l'«obligation de notification», soit le devoir d'annoncer quand une infraction s'est produite, fait valoir Manuel Meier. Le client qui a été frappé par une attaque doit être averti, par exemple si les informations contenues sur sa carte de crédit ont été violées. Aux Etats-Unis, l'entreprise est pénalisée par un risque de publicité et par un coût d'information qui peut atteindre «plusieurs douzaines de millions de francs», explique Carin Gantenbein, responsable de ce risque au sein de Zurich Insurance. Son bénéfice est réduit d'autant. Les entreprises suisses actives aux Etats-Unis, ou ayant un client américain, sont directement touchées si la filiale américaine l'est, parce que l'obligation d'annonce la touche immédiatement.
A l'origine, les entreprises parlaient de sécurité «informatique». Parce que c'est le département du même nom qui était en charge du sujet. Mais elles se sont aperçues que tout leur personnel était concerné et qu'il ne suffisait plus d'avoir un pare-feu ni de changer leurs mots de passe régulièrement.
Si le hacking s'est aussi vite répandu, c'est parce que presque tous les objets sont connectés à Internet, de la voiture à la maison, multipliant les opportunités de piratages. Les risques d'intrusion dans les systèmes informatiques dépassent les produits de consommation et frappent aussi les hôpitaux et leur responsabilité civile en cas de vol de documents.
Les assurances peuvent offrir leur service habituel de transfert de risque. Mais ce dernier ne va jamais couvrir l'ensemble des cyber-risques, même s'il contribue à la réduction des coûts économiques. «Les coûts juridiques d'une attaque sont énormes», observe Manuel Meier. Une grande partie de la couverture d'assurance se concentre sur ceux-ci. «Il arrive que la couverture d'assurance soit entièrement utilisée pour les risques juridiques et qu'il ne reste rien pour la responsabilité civile», fait valoir Carine Gantenbein. L'assurance paie les coûts d'annonce et de rétablissement des données ainsi que l'interruption d'activité. Mais elle ne couvre pas les conséquences d'un piratage, comme l'absence de transaction ou la perte de confiance. Les entreprises peuvent décider de couvrir elles-mêmes les cyber-risques dans une filiale dite «captive» ou faire appel à un réassureur. La définition du prix pose toutefois problème. Il manque encore un historique. «Les assureurs sont dans une phase d'essais et d'erreurs», analyse Manuel Meier.
En outre, les risques d'interruption d'activité conduisent à des estimations compliquées, puisque tout est interconnecté. «Les clients utilisent les mêmes nuages (clouds). Si l'un d'entre eux est attaqué, certaines entreprises ne peuvent plus livrer leurs produits», explique Zurich Insurance.

Si ce marché se situe avant tout aux Etats-Unis, en raison des coûts juridiques, il devrait s'étendre à l'Europe. L'Union européenne débat aussi de l'introduction du devoir d'obligation», indique Manuel Meier. Le temps à cet effet est réduit, sous peine de sanctions supplémentaires. L'UE pourrait mettre en œuvre cette obligation en 2016. La sanction atteindrait 5% du chiffre d'affaires ou jusqu'à 100 millions d'euros.

Le marché suisse de la cyberassurance est encore minuscule, selon l'étude de l'Université de Saint-Gall, réalisée sur mandat du courtier Kessler. Il s'élève à 5 millions de francs. Mais Martin Eling est d'avis qu'il devrait décupler en cinq ans. Dans le monde, le marché devrait quintupler pour s'élever à 10 milliards de dollars.

Les assureurs répondent à ces défis en offrant une combinaison de services de prévention (pare-feu, logiciels) et de protection. C'est une chasse gardée des grands groupes internationaux. Les acteurs actifs dans ce domaine sont AIG Europe Limited, Allianz Global Corporate & Specialty AG (AGCS), Chubb Insurance Company of Europe SE, Zurich et Axa Winterthur. Les grands groupes suisses doivent souvent signer des accords de partenariat. Axa Winterthur travaille par exemple avec Nexos AG, tandis que Zurich Insurance collabore avec Kudelski.

Axa Winterthur offre des mesures de préventions et de couverture de sinistres spécifiques. Dans le cas d'une perte de données, Axa assume la réinstallation du système d'exploitation et des programmes ainsi que la récupération des données. En cas de perte de chiffre d'affaires, à l'image d'une boutique en ligne dont le système est bloqué à la suite d'une attaque et indisponible pendant trois jours, l'assureur verse le manque à gagner, déduit de la franchise.

Auprès de Zurich Insurance, l'assurance cyber-risque est définie selon le principe des modules. La composante de base est toujours la responsabilité civile, laquelle peut s'accompagner de la récupération des données et des coûts d'annonce, s'il y a des clients américains et dès 2016 européens. Elle offre aussi la couverture du risque de chantage. Le prix dépend du nombre de données sensibles et de la branche. Une petite banque est bien plus chère qu'une PME industrielle. Le tarif d'une couverture correspond à 0,6% du chiffre d'affaires, mais des changements sont fréquents. Les statistiques sont encore insuffisantes.

Au sein des entreprises, le travail de sensibilisation intègre chaque employé, selon Carin Gantenbein. Les PME n'ont pas les moyens d'établir de tels processus. L'assureur offre à ses clients des conseillers pour les sinistres, la communication et l'analyse des processus.

Pour les personnes privées, il existe une assurance cybermobbing pour les privés. L'assureur se charge d'éliminer certaines histoires répandues sur le Web. Un privé n'obtiendra pas satisfaction s'il téléphone à Google pour changer un site, explique Manuel Meier.

Et dans cinq ans? Si l'obligation de notification est introduite dans l'Union européenne, la Suisse suivra, promet le directeur de Zurich Insurance. Le marché en deviendra plus transparent. On en parlera davantage, la perception sera supérieure. Et l'offre d'assurance sera élargie.

Source : http://www.letemps.ch/Page/Uuid/01ccdc38-f4e7-11e4-bb1f-074820583190/Les_solutions_des_assureurs_face_au_cyber-risques
Par Emmanuel Garessus

L'employeur face au droit d'accès du salarié à ses

données informatiques | Le Net Expert Informatique

L’employeur face au droit d’accès du salarié à ses données informatiques

Pour Isabelle Renard, docteur ingénieur et avocate au barreau de Paris, la loi Informatique et libertés encadre encore de manière floue les relations employeurs/employés, notamment dans le cadre de l'accès au salarié à ses traces « informatiques ». Elle recommande aux entreprises d'encadrer de façon explicite et précise dans leur charte informatique les modalités de ce droit d'accès, pour éviter les demandes abusives de la part de leurs employés.

La loi Informatique et libertés prévoit que toute personne dont les données personnelles sont traitées peut demander au responsable de traitement d'accéder à celles-ci, dans des conditions qui sont précisées par l'article 39 du texte.
Aux termes de ces dispositions, chacun peut obtenir l'ensemble des renseignements qui caractérisent le traitement dont ses données font l'objet : quelles sont les données traitées, dans quel but, à qui sont-elles transmises, le responsable s'appuie-t-il sur ces informations pour prendre des décisions personnelles à l'égard de la personne concernée ?
Le responsable du traitement des data est tenu de répondre à ces interrogations, sauf si celles-ci procèdent d'un abus manifeste, par leur nombre ou leur répétition trop systématique.
Ces dispositions sont entièrement applicables aux relations entre salariés et employeurs qui, avec les nouvelles technologies, sont en possession de données personnelles de plus en plus nombreuses concernant leurs employés : données de connexion Internet, gestion centralisée des compétences, données des badgeuses, géolocalisation, enregistrements vidéos et vocaux…

UNE FICHE PRATIQUE DE LA CNIL
Les données des employés doivent être collectées licitement, ce qui suppose que les employeurs aient déclaré à la Commission nationale de l'informatique et des libertés (Cnil) les traitements afférents, selon la procédure applicable (déclaration simplifiée, normale, ou demande d'autorisation), selon qu'il existe – ou non – un correspondant informatique et libertés dans l'entreprise. En cas de non déclaration ou de déclaration partielle par l'employeur d'un fichier, les données recueillies ne peuvent pas être opposées au salarié pour fonder une procédure disciplinaire. Ce principe posé par le Cour de cassation est rappelé de façon constante par la jurisprudence.
Mais ce n'est pas tout. Encore faut-il que l'employeur soit en mesure de répondre aux demandes d'accès à leurs données exercées par les salariés. La Cnil, dans la fiche pratique numéro 3 de son guide « pour les employeurs et les salariés », donne une liste des informations auxquelles le salarié a le droit d'accéder, sur simple demande :
• recrutement
• historique de carrière
• rémunération
• évaluation des compétences professionnelles (entretiens d'évaluation, notations)
• dossier disciplinaire
De façon générale, le salarié doit pouvoir accéder à l'ensemble des données de gestion de ressources humaines le concernant, dès lors que celles-ci ont servi de base à une décision à son égard. Ce critère manque singulièrement de clarté, et semble ne concerner que les données de ressources humaines.
S'agissant des traces informatiques, la Cnil ne met aucune condition à leur droit d'accès par le salarié. Par exemple, pour les données de géolocalisation, elle a prononcé une sanction de 10 000 euros à l'encontre de la société Nord Picardie, qui a refusé de transmettre à un employé une copie de ses données de géolocalisation, dont il avait besoin pour prouver qu'un accident de la circulation dont il avait été victime avait un caractère professionnel. De la même façon, l'employeur est tenu de mettre à disposition d'un salarié en faisant la demande ses données de vidéosurveillance, ses écoutes téléphoniques ou ses données de navigation web.

UNE CHARTE INFORMATIQUE EXPLICITE
Confrontés à de telles requêtes l'employeur, même de bonne foi, a parfois du mal à savoir comment se positionner, surtout lorsque lesdites requêtes sont exercées par certains salariés uniquement par principe, pour obliger l'employeur à se plier à une exigence qu'ils estiment être de droit, et alors même que la fourniture de ces informations hors contexte peut se heurter à de réelles difficultés pratiques. Ne reste alors à l'employeur qu'à sortir le joker de la demande « manifestement abusive », et pour cela, il faut caractériser l'abus, ce qui n'est pas simple.
Le « droit d'accès » prévu de façon générale par la loi Informatique et libertés reste un sujet mal encadré dans les relations employeurs/employés, surtout s'agissant de l'accès au salarié à ses traces « informatiques », dont il est en tout état de cause informé de la collecte dès lors que celle-ci est clairement mentionnée dans la charte informatique. Le point n'est pas plus traité dans le projet de règlement européen sur la protection des données personnelles.
Faute d'attendre une amélioration des textes ou un positionnement de la Cnil, nous pensons que la meilleure façon pour les employeurs de se prévaloir de demandes abusives est d'encadrer de façon explicite et précise dans les chartes informatiques les modalités du droit d'accès, pour chaque type de trace « numérique », au lieu des dispositions génériques et floues qu'on y voit actuellement.

Source : http://www.usine-digitale.fr/article/l-employeur-face-au-droit-d-acces-du-salarie-a-ses-donnees-informatiques.N330908
Par Isabelle Renard, docteur ingénieur et avocate au barreau de Paris

Contrôle de la CNIL aujourd'hui à France Télévisions | Le Net Expert Informatique

Contrôle de la CNIL aujourd'hui à France Télévisions

L'Express l'a révélé ce jeudi matin: le siège de France Télévisions a été fouillé mercredi par la Commission nationale de l'informatique et des libertés. Le groupe audiovisuel est soupçonné d'avoir opéré un fichage illégal de ses salariés.

France Télévisions a subi mercredi un contrôle de la Commission nationale de l'informatique et des libertés (Cnil) pour vérifier l'existence de fichiers contenant notamment des données sur les opinions politiques et l'orientation sexuelle de ses salariés, a révélé L'Express ce jeudi matin.

Dénoncé par une lettre anonyme, France Télévisions ficherait ses employés

Ce contrôle avait pour but de vérifier si, oui ou non, France Télévisions a illégalement fiché ses employés. D'après une lettre anonyme envoyée à la Cnil, le groupe audiovisuel aurait recueilli des données personnelles sur leurs opinions politiques, leur orientation sexuelle ou leur casier judiciaire.

Selon le procès-verbal de cette perquisition, les six agents de la CNIL dépêchés sur place ont effectué des recherches au sein des boîtes mails de la direction des ressources humaines du groupe audiovisuel public. D'après plusieurs sources syndicales, les enquêteurs n'auraient a priori pas trouvé « d'éléments probants » en fin de matinée, mais ils ont réalisé des copies de plusieurs fichiers internes. L'instruction, elle, « est toujours en cours ».

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.lexpress.fr/actualite/medias/soupcons-de-fichage-illegal-de-salaries-france-televisions-perquisitionne-par-la-cnil_1681974.html

E-marchands : faut-il confier vos données à Google et Facebook ? | Le Net Expert Informatique

Les deux plateformes risquent-elles de réutiliser vos données pour vos concurrents ? Quelles informations leurs fournissez-vous déjà ? Comment vous protéger à l'avenir ?
Google et Facebook ayant des modèles économiques avant tout publicitaires, ils sont amenés à collecter de plus en plus de données auprès de leurs clients annonceurs. Parmi les informations que les marchands leur transmettent déjà, la première est tout simplement ladite publicité, qui elle-même va générer plusieurs données : d'une part qui lui est exposé, d'autre part qui clique ou pas. « Ces données sont collectées par Google et Facebook, et l'annonceur doit négocier pour les obtenir » explique Thibaut Munier, cofondateur et DG de 1000mercis.

 Thibaut Munier, DG de 1000mercis © S. de P. 1000mercis

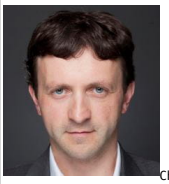
Par ailleurs, l'e-commerçant va communiquer des données de transformation à Google et Facebook, qui placent des tags sur les pages du site, tunnel de conversion compris. Mais si les deux plateformes essaient d'obtenir une meilleure vision de ce qui se passe chez les annonceurs, c'est dans le but de mieux les servir, assure Thibaut Munier.
Qui analyse : « C'est du donnant-donnant et le rapport de force se construit petit à petit, avec les avancées technologiques et les besoins des sites ».

D'autre part, le catalogue produit contient également des données importantes. Que Google les récupère en tant que données publiques sans demander leur avis aux marchands ou que ces derniers les transmettent, par exemple pour personnaliser leurs bannières publicitaires sur Facebook en fonction de leur catalogue, il s'agit encore d'un bloc de données supplémentaire dont les deux plateformes peuvent prendre possession. « Et pour les services de people-based marketing de plus en plus nombreux, comme les 'custom audiences' de Facebook, les marchands sont aussi amenés à charger non plus leurs produits mais leurs clients, afin de cibler soit leurs clients soit leurs non-clients », ajoute Thibaut Munier.

Négocier et ne pas tout donner
A quoi dès lors le marchand doit-il veiller ? D'abord, à bâtir un rapport de force lui permettant de récupérer auprès de Google et Facebook les données que génèrent ses publicités. Et bien sûr à les utiliser, idéalement en les déversant dans sa DMP, qu'il alimentera avec un maximum d'informations.

« Google et Facebook en savent plus que le marchand sur ses prospects »
« Entre les tags et les dispositifs d'identité unifiée comme Facebook Connect et Google+, Google et Facebook ont accès au parcours continu de l'internaute et savent même ce qu'il fait avant et après avoir visité un site marchand, remarque Christophe Camborde, cofondateur et PDG d'Ezakus. Ils en savent donc davantage que le marchand sur ses prospects. » Pour Thibaut Munier, raison de plus pour bien réfléchir à quels tags mettre sur son site. « Le pire est de tout taguer et de ne rien en faire. Si on met des tags, il faut les utiliser, faire des tests et se battre pour récupérer des informations dans l'autre sens », recommande-t-il. Conseil très similaire à propos du catalogue produit (et de la base clients) : se demander si on le charge ou pas et avec quelle granularité. Des questions à considérer aussi à l'aune du contexte concurrentiel plus ou moins sensible du marchand, bien sûr.

La valeur (et la marge) pourrait être transférée avec les données
Le marchand court-il le danger de perdre une partie de sa connaissance client au profit de Google et Facebook ? Christophe Camborde se veut d'abord rassurant : « Jamais ils n'utiliseront les données d'un Cdiscount pour fournir un meilleur service à un Rueducommerce. Garder un secret pareil serait impossible. » En outre, ce qui serait mauvais pour les marchands le serait à terme aussi pour Google et Facebook qui, s'ils « tuaient » leurs clients, n'auraient plus de revenus publicitaires à engranger.

 Christophe Camborde, PDG d'Ezakus © S. de P. Ezakus
« En revanche, une dépendance très forte des marchands va se créer envers Google et Facebook, qui finiront par mieux connaître leurs clients qu'eux, anticipe le PDG d'Ezakus. Lequel prend l'exemple de BigQuery. Cet équivalent de Google Analytics en big data est déjà capable de répondre à une requête du type : montre-moi mes clients qui ont dépensé plus de 200 euros ces quatre derniers mois. « Pour un marchand, pourquoi ne pas utiliser cela plutôt que son CRM interne ? Or avec chaque nouveau service fourni par les deux plateformes, avec chaque morceau de connaissance client et donc de valeur qui se transfère chez elles, c'est une partie de la marge du marchand qui partira aussi chez elles », souligne Christophe Camborde.
Raison pour laquelle il est urgent de monter en expertise sur ces sujets, répond Thibaut Munier. Le marchand est obligé de fournir des données, mais il doit être conscient de ce qu'il donne et de ce qu'il en retire. Pour le DG de 1000mercis, « il faut savoir quelles données ont quelle valeur et comment être pertinent dans leur utilisation. Et éventuellement se doter d'outils pour cela, au premier rang desquels une DMP, meilleure façon pour l'annonceur de protéger ses données. A ces conditions, il est possible d'en retirer des bénéfices. » Le dirigeant établit ainsi un parallèle avec les marketplaces. Certains marchands y commercialisent tout leur catalogue et transmettent leur valeur à Amazon, certains refusent tout en bloc et se privent d'un apport de revenus… et d'autres ne donnent pas tous leurs meilleurs prix, pas tout leur catalogue, et jouent sur plusieurs paramètres afin d'en sortir gagnants.

« On ne peut confier son CRM ou sa DMP à Google ou Facebook »
D'autant que pour Christophe Camborde, pas moyen de faire sans Google et Facebook. « C'est une fatalité, les marchands sont obligés d'y aller. Ceux qui bénéficient d'une clientèle très fidèle, sur une niche, pourront s'en passer. Pas les gros généralistes. »

Se renforcer pour mieux se protéger
Un plan d'action se dégage donc : répartir ses investissements pour ne pas dépendre d'une seule plateforme et travailler la fidélisation et le lien direct avec les consommateurs. « Un fan n'est pas un client », insiste Thibaut Munier, considérant pour sa part qu'on ne peut confier son CRM ou sa DMP à Google ou Facebook. « L'actif du marchand, c'est sa base de clients, sa DMP et son expertise dans ses investissements publicitaires. » Et de marteler : « il existe beaucoup de manières d'être exigeant dans sa relation avec Google et Facebook et beaucoup de manières d'être actif pour tester des choses nouvelles et mesurer ce qu'on en retire. »
Le nombre extrêmement restreint de marchands français disposant d'une DMP montre toutefois que même s'ils sentent qu'il leur faut organiser et protéger leurs données, ils n'investissent encore que très peu dans la data et misent en majeure partie sur le court terme : la publicité. La Redoute a une DMP, selon nos informations Carrefour et Voyages-Sncf.com y travaillent… et Cdiscount et la Fnac y ont réfléchi. La barrière de protection data des e-commerçants français n'est pas encore en place.

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

Source : http://www.journaldunet.com/ebusiness/commerce/donnees-e-commerce.shtml?een=4a4b0e45c54d9fed8fc26819a6b6f84f&utm_source=greenarrow&utm_medium=mail&utm_campaign=ml50_e-marchandsetle

87% des actes cybercriminels commis en France sont du fait de hackers made in France | Le Net Expert Informatique

87% des actes cybercriminels commis en France sont du fait de hackers made in France

Une étude révèle que 87% des actes cybercriminels commis en France sont du fait de hackers made in France. Russes, Africains, Chinois ou Coréens seraient moins offensifs qu'on ne le pense.

La dernière étude de ThreatMetrix va secouer les idées reçues sur la cybercriminalité en France. Selon ce rapport, qui porte sur le 1er trimestre 2015, « la plus grande cyber-menace ayant pesé sur les entreprises françaises durant cette période aurait pour origine l'hexagone ».

L'étude précise que 87% des attaques sont commises depuis la France. Pour les auteurs du rapport, il ne s'agit pas de pointer la performance de la cyberdélinquance made in France, mais de noter que désormais, les attaques menées dans chaque pays sont pilotées dans leur frontière. Ce constat est « en rupture avec les tendances dominantes où la grande majorité des cyberattaques avaient pour origine la Russie, l'Asie ou l'Afrique. »
Ainsi, la France n'est donc pas une exception, mais elle exprime une véritable tendance. En Grande-Bretagne, 75% des actes cybercriminels proviennent d'Irlande ou d'Angleterre, 81% en Allemagne, 54% aux Pays-Bas, 94% en Italie et 85% en Russie.
Sur les attaques, ThreatMetrix a constaté que l'usurpation d'identité (spoofing) est devenue la plus courante. Lors des fêtes de Noël, le cabinet a dénombré 11.4 millions de tentatives de transactions frauduleuses.

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://bfmbusiness.bfmtv.com/entreprise/les-hackers-francais-sont-les-rois-du-cybercrime-en-france-888210.html
Par Pascal Samama

Les opérateurs télécoms nous espionnent-ils ? | Le Net Expert Informatique

Les opérateurs télécoms nous espionnent-ils ?

Votre téléphone est-il sur écoute ? Depuis plusieurs semaines, une affaire secoue le milieu des télécoms suite à la révélation du journal arabophone Al Massae quant à l'utilisation d'un logiciel «d'espionnage des données personnelles» par un opérateur télécoms de la place. Il s'agit du LCS, un logiciel en principe prohibé en Europe et aux États-Unis, qui permet de surveiller l'activité des utilisateurs en dehors de tout cadre légal.

La question qui se pose aujourd'hui : les opérateurs télécoms ont-il le droit d'utiliser les outils qu'ils ont pour contrôler et accéder aux informations et aux données des utilisateurs ? «Il s'agit d'un système permettant de retracer toutes les actions d'un utilisateur sur sa ligne téléphonique et d'effectuer les perquisitions numériques, explique Carlo Lando, un expert italien en sécurité des télécoms.

«En principe, les opérateurs téléphoniques doivent avoir des autorisations du tribunal pour utiliser cette technologie de système sur les réseaux, notamment pour les enquêtes», précise l'expert. Interpellé, le DG de l'Agence nationale de régulation des télécoms (ANRT), Azeddine Mountassir Billah, dit tout ignorer de cette affaire et refuse de la commenter.

En revanche, à la Commission nationale de contrôle de la protection des données à caractère personnel (CNDP), on apprend qu'une réunion aura lieu cette semaine, avec à l'ordre du jour, entre autres, cette affaire de «logiciel LCS». Le président du CNDP, Saïd Ihrai, a déclaré que la commission n'a pas encore été saisie sur ce type de «procédé prohibé» permettant de surveiller et de contrôler les données personnelles des utilisateurs.

Source : http://www.leseco.ma/maroc/30623-donnees-personnelles-les-operateurs-telecoms-nous-espionnent-ils.html
Par NAIMA CHERII

L’immatriculation des drones, solution à toutes les craintes ? | Le Net Expert Informatique

L’immatriculation des drones, la la solution à toutes les craintes ?

L’immatriculation des drones de loisir est-elle une solution efficace pour responsabiliser leurs propriétaires ? À vous de juger !

Doter les drones de loisir de plaques d’immatriculation : c’est l’une des pistes de réforme envisagées par le gouvernement pour éviter les survols intempestifs de ces petits robots volants au-dessus de la capitale et aux abords de centrales nucléaires. La soixantaine d’incidents recensés ces derniers mois a en effet révélé les lacunes de la réglementation et des systèmes de détection et d’interception existants.

Deux projets ont été sélectionnés par l’Agence nationale de la recherche (ANR) en vue de relever le défi que ces engins provocateurs lancent aux autorités. Des systèmes de captation de signaux entre le pilote et l’appareil et de brouillage GPS forçant le drone à atterrir sont en cours d’expérimentation. Il est aussi question de doter ces appareils de puces d’identification.

La dissuasion passe également par des sanctions plus lourdes que celles encourues actuellement pour le non-respect des règles de sécurité, à savoir un an d’emprisonnement et 75 000 euros d’amende, outre les peines encourues pour mise en danger de la vie d’autrui. Car les drones présentent des risques, peuvent blesser des gens, s’écraser sur une route ou sur une piste d’aéroport. Une collision avait été évitée de justesse entre un A320 et un drone à l’aéroport de Heathrow en juillet 2014…
Faut-il obliger les propriétaires de drones à les faire immatriculer à leurs frais comme le font les propriétaires d’aéronefs civils ? À vous de juger – et de voter après avoir regardé nos deux expertes, Myriam Quéméner et Christiane Féral-Schuhl, plaider le « pour » et le « contre » en… trois minutes !

Faut-il immatriculer les drones ? *par LePoint*

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.lepoint.fr/justice-internet/au-tribunal-de-l-internet-faut-il-immatriculer-les-drones-18-05-2015-1929083_2081.php
Par Laurence NEUER ET Anne-Sophie JAHN