Une plateforme en ligne pour combattre le Phishing | Le Net Expert Informatique

	**Une plateforme en ligne pour combattre le Phishing**

Face à l'expansion du hameçonnage (phishing), la police judiciaire française a décidé de s'allier au privé. Une initiative « exceptionnelle », relate l'AFP, présente lors de la signature, le 4 novembre, d'une convention avec l'association privée Phishing Initiative. Cette plateforme, fondée par Microsoft, PayPal et Lexsi, offre aux internautes la possibilité de lutter contre ces menaces en dénonçant l'adresse d'un site – mais pas de mails.

Pour la PJ, il s'agit d'abord de mettre l'accent sur la prévention. C'est, d'un point de vue réaliste, sa seule façon d'agir contre ce phénomène trop complexe à appréhender. Catherine Chambon, sous-directrice de la lutte contre la cybercriminalité à la direction centrale de la PJ, a expliqué à l'agence de presse que les faits étaient le plus souvent « générés par un seul auteur, de l'étranger » ce qui rend les enquêtes « longues ».

Une menace grave

En 2014, 137 000 signalements ont été effectués sur la plateforme gouvernementale Pharos, dont un tiers concernait le phishing. Depuis le début 2015, Phishing Initiative a récolté pour sa part 60 000 signalements dont 35 000 relevaient du hameçonnage. Derrière ces faux e-mails envoyés par des usurpateurs se cachent parfois des attaques hypersophistiquées comme celle menée en février à l'encontre de cent grandes banques.

Pour la société dont l'identité a été volée (une banque, un assureur, un service en ligne…), les dégâts sont d'une autre nature. Elle, qui investit énormément en communication et en marketing, peut voir ruinée sa réputation en quelques heures à peine, selon l'expert Return Path, en raison d'une campagne de phishing.

Source :
http://pro.clubic.com/it-business/securite-et-donnees/actualite-785286-police-phishing.html

Phishing : Lexsi et Microsoft s’allient à la plateforme Pharos | Le Net Expert Informatique

	Phishing : Lexsi et Microsoft s’allient à la plateforme Pharos

Le phishing a la cote : cette technique de social engineering consiste, via l'envoi de mail frauduleux ou la création de faux sites web arborant les couleurs d'un service ou d'une administration, à soutirer des identifiants aux victimes qui pensent se connecter sur le site légitime. Simple, facile à automatiser, le phishing est une attaque de plus en plus courante comme le soulignent les chiffres de la plateforme : en 2015, la Phishing Initiative a ainsi repéré plus de 35.000 URL jugées malveillantes.

La plateforme Phishing Initiative a été lancée par des sociétés privées (Lexsi et Microsoft notamment, mais Google est aussi partenaire du projet) et annonce aujourd'hui un partenariat avec Pharos, la plateforme de signalement mise en place par l'OCLCTIC (Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication.)

« C'est un partenariat qui porte sur deux volets principaux » explique à ZDNet.fr Jérôme Robert, responsable marketing du groupe Lexsi « D'une part, le partenariat permettra de mettre en place un échange de données : quand un site de phishing sera signalé chez Pharos, ils nous transmettront leurs informations. A l'inverse, on leur transmettra également les informations que nous avons, bien que notre dispositif seul ne permette pas l'ouverture d'une plainte. D'autre part, on espère également pouvoir bénéficier d'une certaine visibilité à travers ce partenariat. »

Lutter contre le hameçonnage des particuliers

La plateforme Phishing Initiative s'adresse avant tout aux particuliers et permet de communiquer une URL jugée suspicieuse par l'utilisateur. Une fois l'URL transmise, des experts de Lexsi analysent le site afin d'écarter d'éventuels faux positifs. Si celle-ci est jugée malveillante, elle est transmise à Microsoft et Google qui peuvent l'ajouter à leurs listes noires de sites web, présentant un avertissement aux utilisateurs qui tentent de s'y connecter.

Des listes noires qui sont partagées par les principaux éditeurs de navigateur et qui permettent donc d'assurer une plus grande sécurité des internautes. En parallèle de cela, Lexsi se charge également de prendre des mesures afin de signaler le site et de le faire fermer.

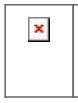
Le service est entièrement gratuit, destiné aux particuliers qui ont été redirigés ou confronté à un site malveillant. « On a remarqué que pas mal d'entreprises avaient également recours à notre service pour signaler des tentatives de phishing » poursuit Jérôme Robert « Ça ne nous dérange pas et on n'entend pas du tout limiter cela. Mais on permet aux entreprises qui le désirent de sponsoriser l'initiative à hauteur de 5000 euros par an, et on envisage de proposer des services additionnels aux entreprises, tels que la possibilité de soumettre des URL en masse pour 1500 euros. »

L'effort permettra également au groupe Phishing Initiative de nourrir différents rapports sur les tendances des la cybercriminalité en ligne.

Source :

http://www.zdnet.fr/actualites/phishing-lexsi-et-microsoft-s-allient-a-la-plateforme-pharos-39827758.htm

La surveillance des communications internationales validée | Le Net Expert Informatique



La surveillance des communications internationales validée

Le Parlement a adopté un texte comblant un vide laissé par la loi renseignement. La surveillance des communications internationales impliquera moins de contrôles que celle des interceptions effectuées dans l'Hexagone.

Le débat est clos. Le Parlement a adopté définitivement jeudi 5 novembre par un dernier vote de l'Assemblée la proposition de loi destinée à légaliser la surveillance des communications internationales, qui resteront soumises à moins de contrôles que les interceptions effectuées en France.

Les députés ont voté le texte dans les mêmes termes que les sénateurs un peu plus tôt dans la journée.

Le législateur compétent

La proposition de loi a pour objet de pallier un vide juridique résultant de la censure par le Conseil constitutionnel d'une disposition de la loi renseignement. Celle-ci, qui légalise et encadre l'activité des services en France, était restée floue pour leurs activités à l'étranger, renvoyant cela à un décret en Conseil d'État.

Mais le Conseil constitutionnel a jugé que c'était au législateur d'agir dès lors que des libertés publiques étaient concernées.

Une autorisation du Premier ministre

Les auteurs du texte, les députés socialistes Patricia Adam et Philippe Nauche, respectivement présidente et vice-président de la commission de la Défense à l'Assemblée, ont proposé un cadre juridique spécifique en introduisant un nouveau chapitre dans le code de la sécurité intérieure.

Dès lors que « la défense et la promotion des intérêts fondamentaux de la Nation », qui comprennent notamment « les intérêts économiques, industriels et scientifiques majeurs » de la France, sont concernées, « la surveillance des communications qui sont émises ou reçues de l'étranger » est autorisée et le Premier ministre pourra « désigner les zones géographiques, les organisations ou les personnes objets de cette surveillance ».

Moins de contrôles

Ces interceptions à l'étranger seront nettement moins encadrées que celles effectuées en France. Le Premier ministre n'aura pas besoin de solliciter l'avis préalable de la nouvelle Commission nationale de contrôle des techniques de renseignement (CNCTR).

Sur proposition du Sénat, la commission mixte paritaire a retiré au Premier ministre la faculté de déléguer à un collaborateur la désignation des réseaux de communications électroniques internationales sur lesquels l'interception est autorisée.

Source :
http://www.latribune.fr/economie/france/la-surveillance-des-communications-internationales-validee-par-le-parlement-520191.html

Les moyens de preuves sur Internet | Le Net Expert Informatique

Les moyens de preuves sur Internet

La récente décision de la Cour d'appel de Paris du 9 octobre 2015 rappelle une fois de plus le caractère essentiel de constituer des preuves valables avant d'agir en justice, particulièrement sur Internet. En l'espèce, la société éditrice du site « Onvasortir.com » attaquait en parasitisme la société éditrice du site « dailyfriends.com » pour avoir copié le plan, la structure, les fonctionnalités, l'agencement des rubriques et le contenu de son site internet.

Afin de rendre sa décision, la Cour s'est appuyée sur des copies écran (des sites en question et d'un forum de discussion), dont la valeur probante était contestée par la partie adverse, mais que la Cour a jugé recevable dans la mesure où elles étaient « parfaitement nettes et datée ». En revanche, la Cour a rejeté un constat d'huissier du fait que l'officier ministériel avait dissimulé son identité lors de ses constats en se connectant aux sites via le compte de la société.
Que ce soit pour un site internet ou une application sur smartphone, la constitution de preuves, souvent difficiles à obtenir et pas toujours recevables, est pourtant essentielle à :
La caractérisation du délit (et donc la condamnation) ;
L'évaluation du préjudice (et donc des dommages-intérêts).

Si la preuve est libre en matière de concurrence déloyale ou de contrefaçon, toutes les preuves ne sont pas admissibles, comme en atteste cette décision, et leur force probante variable. Cet arrêt est donc l'occasion de revenir sur les règles en la matière, avec la particularité de la preuve sur Internet.

I – Les moyens de preuve irrecevables

Au préalable, il n'est pas inutile de rappeler que seules les preuves « légalement admissibles » pourront être retenues devant un tribunal.
Ainsi, il faut entendre par « légalement admissible », les preuves qui ne relèvent pas d'une obtention irrégulière telles que : les écoutes téléphoniques, la violation du secret des correspondances, la réalisation d'un constat en dehors des heures légales ou encore l'atteinte à un principe fondamental tel que la vie privée, le secret professionnel ou le secret de fabrique.
Ainsi, la Cour de cassation, par un arrêt de principe en son assemblé plénière du 7 janvier 2011 a énoncé que « l'enregistrement d'une communication téléphonique réalisé à l'insu de l'auteur des propos tenus constitue un procédé déloyal rendant irrecevable sa production à titre de preuve ».

C'est également sur ce fondement que dans sa décision la Cour d'appel a rejeté le constat dressé par l'huissier de justice qui n'a pas dévoilé son identité en se connectant au site mais a utilisé les identifiants de compte d'un tiers.

II – Les moyens de preuves sur Internet

Il existe plusieurs moyens de preuves visant à faire constater un usage sur Internet dont la force probante est plus ou moins importante.

A) Le constat d'huissier

Une fois établie et validée, cette preuve a une grande force probante.
Ainsi, l'huissier peut procéder à des constations sur Internet à la requête des particuliers. Il a cependant un rôle de simple observateur puisqu'il doit se borner à effectuer des constations purement matérielles.

Le constat sur Internet a cependant posé la question des limites de ce qu'il pouvait constater.
Constat d'un site internet ou d'une application sur smartphone : Sous réserve de respecter certaines conditions techniques (vider le dossier cache du navigateur, absence de serveur proxy…), l'huissier peut faire une description des sites internet accessibles au public, et notamment des produits argués de contrefaçon, et des captures écran des pages du site.

Constat d'achat sur internet : Cette pratique a posé certaines questions en cas de commande sur internet par l'huissier de produits litigieux.
Certains arrêts avaient admis qu'un huissier puisse commander un produit sur un site internet afin d'établir un constat d'achat aux vues de constituer une preuve de la contrefaçon. Cependant, des arrêts, plus récents [1] ont contesté la licéité de cette pratique au motif que l'huissier s'était engagé activement par l'ouverture d'un compte client et l'acquisition du produit litigieux, et avait ainsi outrepassé ses pouvoirs de simple constatation.

C'est en ce sens que va l'arrêt du 7 octobre 2015, qui a dénié toute validité au constat d'huissier qui n'avait indiqué ni sa qualité ni son identité en se connectant au site.
Pour acheter un produit sur internet, l'huissier doit impérativement et comme en matière de constat achat dans les magasins, décliner de manière claire et visible son identité et sa qualité avant de procéder à un acte d'achat. Certaines décisions ont cependant, admis que le seul fait de faire libeller la facture au nom de l'huissier était suffisant pour identifier l'huissier [2].

Sauf à y être expressément autorisé, l'huissier n'a pas le droit d'ouvrir un compte client et, d'acquérir à dessein, un produit allégué de contrefaçon [3].
Le site internet est assimilé à un magasin, comme un lieu privé et, sans autorisation du juge, l'huissier ne peut procéder à ses constatations que depuis la voie publique. Peut-être pourra-t-on procéder comme en matière de constat d'achat en magasin c'est-à-dire, faire procéder à l'ouverture d'un compte client par un tiers sous surveillance de l'huissier qui constatera les démarches effectuées dans le but d'acheter le produit incriminé ? Il faudra également que l'huissier soit présent lors de la réception du colis…ce qui complique les choses.

B) Le constat par un agent assermenté

Il consiste en la description par un agent assermenté d'un acte de contrefaçon. Il pourra être demandé à l'Agence pour la Protection des Programmes (APP) qui dispose d'agents assermentés.
Ce moyen de preuve est particulièrement utilisé en matière de droit d'auteur et de droits voisins et a été admis en matière de propriété industrielle. Ces constats peuvent servir à contourner la difficulté des achats sur internet effectués par un huissier.
Néanmoins, ces constats n'ont pas la force probante des constats effectués par un officier ministériel, et sont par conséquent soumis à l'appréciation souveraine du tribunal.

C) La copie-écran

Enfin, la copie-écran peut également être pertinente même si elle a une force probante moindre, elle représente une bonne solution pour étayer un constat d'huissier ou lorsqu'un constat d'huissier est invalidé comme dans la présente décision du 9 octobre 2015.

Il est donc impératif de connaître les limites d'investigations de l'huissier pour ne pas se voir déclarer irrecevable le constat. Le droit, à l'origine applicable à la vie réelle, essaie tant bien que mal de s'adapter aux contraintes et aux particularités du monde virtuel, et les constats d'huissier ne font pas exception. Attention donc à bien connaître ces spécificités avant d'intenter toute action au fond !

Denis JACOPINI est Expert Informatique assermenté, consultant et formateur en sécurité informatique, en mise en conformité de vos déclarations à la CNIL et en cybercriminalité.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité, en accompagnement aux mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL et accompagnement de Correspondant Informatique et Libertés.
Contactez-nous

Source : http://www.village-justice.com/articles/Les-moyens-preuves-sur-Internet,20821.html
Colombe Dougnac – Conseil en Propriété Industrielle

Plus de 2 millions d’internautes victimes de phishing en 2015 | Le Net Expert Informatique

Plus de 2 millions d’internautes victimes de phishing en 2015

Pour renforcer la lutte contre le phishing, le Ministère de l'Intérieur a signé le 5 novembre, une convention de partenariat avec l'association Phishing Initiative, soutenue par Lexsi et Microsoft France. Cet accord vise à mutualiser les informations entre sa propre plateforme, PHAROS, et celle de Phishing Initiative qui a identifié de son côté plus de 150 000 adresses uniques de sites frauduleux visant la France depuis sa création en 2011.

Une convention commune pour renforcer la lutte contre le Phishing

En signant la convention de lutte anti-phishing, Catherine Chambon, sous-directeur de la lutte contre la cybercriminalité et Jérôme Robert, président de Phishing Initiative souhaitent renforcer la sensibilisation des internautes aux risques liés à cette malveillance majeure. « La complémentarité de nos actions rend évidente la nécessité d'un rapprochement et d'une coordination entre nos deux organisations », explique Jérôme Robert. « PHAROS et Phishing Initiative opèrent en effet tous deux des plateformes de signalement à destination du grand public. Il est par conséquent possible d'instaurer des conditions de partage de l'information de manière à optimiser d'une part, la recherche de données et d'autre part, la protection de l'internaute. »

Suite à la signature de cette convention et à l'engagement des parties prenantes, le Ministère de l'Intérieur et Phishing Initiative travailleront également à la rédaction d'un rapport commun et à l'élaboration d'un suivi des tendances au service de la protection des internautes.

Phishing Initiative et PHAROS : l'union des expertises

Elaborée et construite sous l'impulsion de Madame Catherine Chambon, Madame Valérie Maldonado, chef de l'OCLCTIC, Messieurs Jérôme Robert, Directeur Marketing, Vincent Hinderer, Expert Cybersécurité chez Lexsi, et Bernard Ourghanlian, directeur technique et sécurité de Microsoft, la convention a pour objectif d'augmenter le nombre d'URLs traitées et analysées. Avec respectivement 60 000 et 30 000 URLs traitées depuis début 2015, Phishing Initiative et PHAROS unissent leurs forces pour protéger les internautes et rendre le web plus sûr. « L'association de nos dispositifs de lutte contre la fraude sur Internet représente une avancée majeure dans la protection des particuliers comme des entreprises » précise Bernard Ourghanlian de Microsoft France. « Face à la malveillance et à la fraude organisée, chaque citoyen et chaque entreprise est acteur d'un Internet plus sûr au bénéfice de tous. » La Sous-Direction de la Lutte contre la Cybercriminalité (SDLC) a développé deux dispositifs destinés aux particuliers : la Plateforme d'Harmonisation d'Analyse et de Recoupement et d'Orientation des Signalements (PHAROS), lancée en janvier 2009, et Info-Escroqueries, une hotline téléphonique dédiée aux arnaques. PHAROS a notamment pour mission de recueillir et traiter les signalements de contenus et de comportements illicites détectés sur Internet.

Phishing Initiative, un programme de lutte européen

Cofinancé par le Programme de Prévention et de Lutte contre le Crime de l'Union Européenne, Phishing Initiative offre à tout internaute la possibilité de lutter contre les attaques d'hameçonnage en signalant de manière simple les liens lui paraissant suspects en un clic sur www.phishing-initiative.fr .

Chaque signalement fait l'objet d'une analyse par les experts Lexsi qui, s'il se révèle frauduleux, est transmis aux partenaires de Phishing Initiative, notamment Microsoft. Ces derniers enrichissent alors leurs listes noires, de sorte que le lien frauduleux est bloqué par les principaux navigateurs Web (Edge, Internet Explorer, Chrome, Firefox et Safari).

Phishing Initiative en chiffres

A ce jour, plus de 400 000 adresses suspectes ont été signalées dans le cadre de la Phishing Initiative, dont plus de 300 000 uniques. Depuis le début de l'année 2015, 110 000 signalements ont déjà été transmis, représentant plus de 60 000 nouvelles adresses uniques. Parmi elles, plus de 35 000 URLs uniques ont été confirmées comme faisant partie d'une campagne de phishing, soit près de 120 adresses distinctes par jour. A noter que le temps médian nécessaire aux analystes pour catégoriser un nouveau cas signalé est de moins de 20 minutes. Microsoft rafraîchit sa liste noire toutes les 20 minutes au sein d'Internet Explorer et Edge, ce qui protège en moyenne les internautes en moins de 40 minutes suite à un signalement sur www.phishing-initiative.fr.

Des milliers d'internautes contribuent anonymement à ce projet chaque année et plusieurs centaines d'individus ont créé depuis la rentrée un compte personnel sur le site Phishing Initiative. Il leur permet désormais de signaler des URLs suspectes plus simplement et d'accéder à des informations, statistiques et services additionnels, relatifs notamment aux signalements effectués par leurs soins. Ces internautes peuvent, par exemple, suivre l'état du site en temps réel et demander à être prévenus du caractère frauduleux ou non d'une adresse ainsi soumise, mais surtout participer à la lutte anti-phishing et empêcher que d'autres internautes soient victimes de ce fléau.

A propos de Phishing Initiative

Créé sous l'impulsion conjointe du cabinet Lexsi, de Microsoft et de PayPal Europe en 2011, Phishing Initiative, association à but non lucratif, offre à tout internaute la possibilité de vérifier un site suspect et lutter contre les attaques de phishing. En signalant l'adresse d'un site suspecté d'héberger un cas de phishing francophone, vous contribuez à diminuer l'impact de cette cybercriminalité en évitant que d'autres internautes soient piégées par ces attaques. Chaque adresse différente fera en effet l'objet d'une vérification humaine et si confirmée comme frauduleuse d'un envoi pour blocage dans les listes noires des principaux navigateurs Plus d'informations sur : https://phishing-initiative.fr

---

Source : http://www.globalsecuritymag.fr/Plus-de-2-millions-d-internautes,20151105,57293.html

Kaspersky Decryptor : un outil pour décrypter les fichiers des ransomware Coinvault et Bitcryptor | Le Net Expert Informatique

Kaspersky Decryptor : un outil pour décrypter les fichiers des ransomware Coinvault et Bitcryptor

L'éditeur d'outils de sécurité a réussi à récupérer toutes les clés de décryptage de deux malwares qui corrompent les fichiers utilisateurs.

Kaspersky Decryptor : un outil pour décrypter les fichiers des ransomware Coinvault et Bitcryptor
Dans la liste des logiciels malveillants les ransomware font partie des plus redoutables pour extorquer de l'argent aux victimes. Kaspersky propose toutefois un outil pour venir à bout de deux d'entre eux tout en offrant la possibilité de décrypter les fichiers corrompus.

Coinvault et Bitcryptor sont deux malwares de type « ransomware ». Ils prennent place sur l'ordinateur en trompant l'utilisateur puis appliquent un chiffrement sur les fichiers de l'utilisateur qui deviennent inaccessibles sans clé de déverrouillage. Les malfaiteurs proposent de délivrer la clé contre le paiement d'une rançon, d'où le nom ransomware.

Ransomware Coinvault
Depuis plusieurs mois Kaspersky collabore avec les les forces de l'ordre néerlandaises pour récupérer des clés de décryptage. Après avoir récupéré quelques échantillons en début d'année, ils annoncent aujourd'hui que toutes les clés de décryptage, plus de 14000, sont à présent disponibles. Cela permettra aux utilisateurs infectés de se débarasser du logiciel malveillant tout en retrouvant l'accès à leurs fichiers.

Kaspersky Decryptor
La procédure (en anglais https://noransom.kaspersky.com/static/CoinVault-decrypt-howto.pdf) explique la marche à suivre. Le logiciel malveillant est tout d'abord éliminé en utilisant la suite Kaspersky Internet Security (http://www.cnetfrance.fr/telecharger/kaspersky-internet-security-39184140s.htm) puis le logiciel Kaspersky Ransomware Decryptor (https://noransom.kaspersky.com/) déchiffre les fichiers de l'ordinateur grâce à la liste qu'il récupère ou dans un dossier désigné par l'utilisateur.

Tous les logiciels malveillants agissant de cette façon ne sont toutefois pas concernés. Il est donc recommandé pour éviter tout problème de sauvegarder régulièrement ses fichiers personnels sur un support externe tel qu'un disque amovible ou un service de stockage en ligne.

Denis JACOPINI est Expert Informatique assermenté, consultant et formateur en sécurité informatique, en mise en conformité de vos déclarations à la CNIL et en cybercriminalité.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité, en accompagnement aux mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL et accompagnement de Correspondant Informatique et Libertés.
Contactez-nous

Source :
http://www.cnetfrance.fr/news/kaspersky-decryptor-un-outil-pour-decrypter-les-fichiers-des-ransomware-coinvault-et-bitcryptor-39827670.htm

---

Nouvelle réglementation Européenne sur la protection des données personnelles | Le

Net Expert Informatique

Nouvelle réglementation Européenne sur la protection des données personnelles

Comment être prêt à répondre aux exigences de la nouvelle réglementation européenne sur la protection des données personnelles ?

Les apports du projet de règlement UE sur la protection des données personnelles en matière de gestion de crise sont nombreux et les entreprises peuvent d'ores et déjà se préparer à plusieurs niveaux.
Vous êtes le dirigeant d'une entreprise de la grande distribution, vôtre RSSI vous informe que malgré les mesures de sécurité mises en œuvre, l'entreprise est victime d'un vol massif de données clients. Vous avez conscience que c'est impactant pour votre entreprise mais heureusement les législations européennes et françaises, en matière de violation des données à caractère personnel, ne visent que les fournisseurs de communication électronique. Vous êtes épargnés d'un point de vue réglementaire… Certes, mais plus pour longtemps.
Le projet de règlement sur la protection des données destiné à remplacer la Directive 95/46/CE doit actuellement repasser devant la Commission et son adoption ne saurait tarder. Le règlement vise désormais toutes les organisations traitant des données à caractère personnel et en lien avec l'UE (territorial, résidents UE…).
Celui-ci impose notamment, que si les conséquences de la compromission de données, constituent un risque élevé pour les droits et libertés des personnes physiques concernées, l'organisation doit les informer au plus vite. Elle doit aussi en informer les autorités compétentes en matière de protection des données à caractère personnel. Pour ce faire plusieurs actions doivent être réalisées en étroite collaboration avec le soutien du Data Privacy Officer (DPO) de l'organisation.

La qualification de l'incident
L'objectif est de déterminer si le risque est élevé pour les personnes concernées. Pour ce faire il convient en premier lieu de répondre à deux questions :
• Les données volées rendent-elles les personnes concernées identifiables ?
• Les personnes concernées peuvent-elles connaître des conséquences significatives voire irrémédiables (discrimination, vol/usurpation d'identité, perte financière, atteinte à la réputation) ?
A l'issue de cette première phase, si le risque est élevé pour les personnes concernées (données identifiables et conséquences majeures), il faudra procéder à la notification de l'autorité compétente et des personnes concernées.
L'organisation ne sera toutefois pas tenue de notifier les personnes concernées par la violation si :
• Le responsable du traitement a mis en œuvre des mesures de protection technologiques appropriées rendant les données incompréhensibles à toutes personnes non autorisées à y avoir accès (ex : chiffrement) ;
• Ou si la notification risque d'entrainer des mesures disproportionnées eu égard notamment au nombre de cas concernés ;
• Ou si la notification risque de porter atteinte à un intérêt public important.

La notification de l'incident
Pour la notification à l'autorité en charge de la protection des données, la CNIL en France, l'organisation victime de l'attaque dispose d'un délai de 72 heures. Cette notification devra notamment comporter les éléments suivants :
• La nature de la violation
• Le nombre approximatif de personnes et des enregistrements concernés
• La description des conséquences probables de la violation
• La description des mesures prises

Pour la notification aux personnes concernées, celles-ci doivent aussi être averties sans retard injustifié. Trois éléments principaux doivent être communiqués :
• La nature de la violation des données à caractère personnel
• Les mesures prises ou proposées pour remédier à la violation
• Les recommandations afin d'atténuer les effets négatifs de la violation

Durant toute la gestion de la crise ainsi que durant la sortie de crise, le responsable du traitement doit alimenter puis conserver une trace documentaire de la violation des données à caractère personnel en indiquant son contexte, ses effets et les mesures prises pour y remédier. Ce document aura valeur juridique et pourra être opposable.

En parallèle à ces actions, la gestion de la crise comporte également une gestion technique de l'attaque, une campagne de communication de crise afin de sauvegarder la réputation, ainsi qu'une démarche judiciaire et assurantielle notamment si l'organisation a adopté une cyber-assurance.

Le rôle du DPO
En temps de crise, le Data Privacy Officer (DPO) pourra veiller à ce que les mesures adaptées et la notification à l'autorité de contrôle et aux personnes concernées soient réalisées. Il pourra par ailleurs effectuer toutes les procédures requises auprès de la CNIL ainsi que suivre le dossier. En outre, les relations entre le CIL et la CNIL déjà établies en amont de la crise permettent d'alléger les procédures.

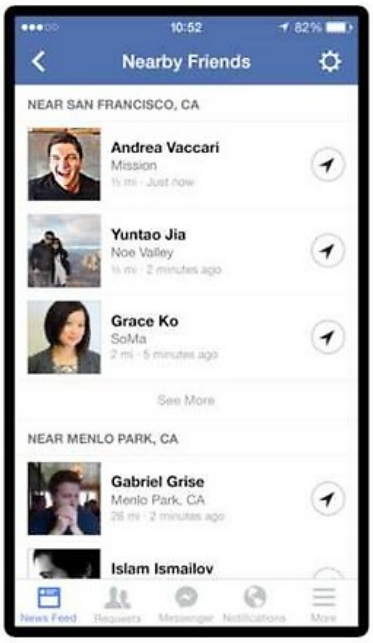
L'existence du CIL dans les entreprises peut être ainsi un élément favorisant l'adoption de réponses adaptées en temps de crise et pouvant réduire le montant de la sanction administrative dans le cas où la responsabilité du responsable de traitement ou du sous-traitant est démontrée.

Comme tout professionnel de l'informatique et de l'Internet, il est de mon devoir de vous informer que vous devez mettre en conformité et déclarer à la CNIL tous vos traitement de données à caractère personnel (factures, contacts, emails…).
Même si remplir un formulaire de déclaration à la CNIL est simple et gratuit, il vous engage cependant, par la signature que vous apposez, à respecter point par point la loi Informatique et Libertés. Cette démarche doit commencer par une analyse précise et confidentielle de l'ensemble de vos systèmes de traitements de données. Nous pouvons vous accompagner pour vous mettre en conformité avec la CNIL, former ou accompagner un C.I.L. (correspondant CNIL) ou sensibiliser les agents et salariés à l'hygiène informatique.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

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

Source : http://www.itpro.fr/a/nouvelle-reglementation-ue-sur-protection-donnees-personnelles/
Par Francesca Serio – Consultante spécialisée en Gestion de crise et Continuité d'Activité – Provadys

Avec Facebook, on peut désormais savoir quand nos amis sont à proximité.. et lui aussi ! | Le Net Expert Informatique



Avec Facebook, on peut désormais savoir quand nos amis sont à proximité… et lui aussi !

Le réseau social propose ce mardi sur son application mobile une option baptisée « Nearby Friends » qui envoie une notification quand un ami se trouve à proximité.

Facebook veut savoir où nous sommes et souhaite également que nos amis le sachent. A partir de ce mardi, une nouvelle option apparaît sur le réseau social : « Nearby Friends », soit une bonne méthode pour scruter les activités de vos amis. L'application va ainsi envoyer une notification quand un ami de l'utilisateur se trouve à côté de lui.

Option désactivée par défaut

Les réseaux sociaux ne laissent donc plus de place aux mensonges. Impossible d'éviter un ami encombrant : « Lorsque vous allez au cinéma, 'Friends Nearby' vous dit si des amis à vous sont proches pour que vous alliez voir le film ensemble ou pour vous retrouver ensuite », indique Facebook.

Pour l'instant, il s'agit d'une option non-obligatoire, c'est à dire qu'elle est désactivée par défaut. En revanche, il est impossible de savoir à partir de combien de kilomètres Facebook considérera qu'un ami se trouve « à proximité ».

Avec cette option, le réseau social pourrait également franchir une nouvelle étape dans la collecte des données personnelles, alors que la nouvelle application débarque au lendemain d'une injonction de la justice belge . Cette dernière a ordonné Facebook d'arrêter de tracer tous les internautes, dont ceux qui ne sont pas connectés au réseau social.

Nouvelle tendance

La nouvelle option Facebook semble s'inscrire dans une nouvelle tendance. Il y a quelques jours, c'est Google qui annonçait le lancement d'une nouvelle application indiquant aux amis d'un utilisateur si celui-ci est disponible pour sortir manger, boire un verre, etc. Baptisée « Who's Down », l'option n'est disponible qu'aux Etats-Unis et constitue un premier test pour Google. Pour Facebook en revanche, cette phase a déjà été réalisée : l'option « Nearby Friends » a été l'ancée dès 2014 chez les anglo-saxons.

Facebook Messenger intègre la reconnaissance faciale

En Australie, le réseau social va encore plus loin en proposant une nouvelle application sur Facebook Messenger. Baptisée « Photo Magic », il s'agit d'un outil permettant de partager facilement des photos où apparaissent les personnes avec lesquelles on discute. Facebook utilise pour cela la reconnaissance faciale et scanne toutes les photos stockées sur le téléphone de l'utilisateur. Si un ami Facebook est détecté sur l'une des photos, l'application propose de la partager à la personne identifiée. Pour l'instant la fonctionnalité est optionnelle et ne devrait pas arriver tout de suite en France. Facebook a en effet cessé la reconnaissance faciale en Europe pour respecter la législation sur la protection des données personnelles.

Source : http://www.lesechos.fr/tech-medias/hightech/021468123566-grace-a-facebook-on-peut-desormais-savoir-quand-nos-amis-sont-a-proximite-1174043.php

---

La CDP malienne venue s'inspirer de l'expérience

sénégalaise | Le Net Expert Informatique

	La CDP malienne venue s'inspi08rer de l'expérience sénégalaise

La Commission de Protection des Données Personnelles du Sénégal (CDP) a reçue la visite du 02 au 04 Novembre 2015 de son homologue malien, l'Autorité de Protection des Données à caractère Personnel (APDP), venu s'inspirer de son expérience et de sa pratique. Cette visite s'inscrit en effet dans le cadre du renforcement de la coopération et des échanges d'expériences entre les deux institutions qui ont en charge la protection des données à caractère personnel.

La délégation de l'Autorité malienne, avec à sa tête son Président, M. Oumarou A.G Mouhamed Ibrahim AIDARA, était composé de cinq personnes. Cette visite s'explique selon le Président de l'autorité malienne par la volonté de s'imprégner de l'expérience enregistrée par le Sénégal depuis quelques années en matière de protection des données personnelles. Elle se justifie également par les ressemblances constatées dans les deux pays.

M. Oumarou A.G Mouhamed Ibrahim AIDARA a remercié les autorités sénégalaises de leur accueil chaleureux et précisé qu'ils étaient venus pour apprendre du Sénégal.

De son côté, le Président de la CDP, le Dr Mouhamadou LO, a magnifié le début d'une fructueuse collaboration entre les deux institutions, tout en invitant ses responsables à œuvrer pour que le respect de la vie privée des personnes entre dans les habitudes quotidiennes des Maliens. Les deux autorités de protection ont émis le souhait de nouer une collaboration étroite et un appui mutuel dans le cadre de la lutte contre la violation de la vie privée au sein des deux pays.

Comme tout professionnel de l'informatique et de l'Internet, il est de mon devoir de vous informer que vous devez mettre en conformité et déclarer à la CNIL tous vos traitement de données à caractère personnel (factures, contacts, emails…).
Même si remplir un formulaire de déclaration à la CNIL est simple et gratuit, il vous engage cependant, par la signature que vous apposez, à respecter point par point la loi Informatique et Libertés. Cette démarche doit commencer par une analyse précise et confidentielle de l'ensemble de vos systèmes de traitements de données. Nous pouvons vous accompagner pour vous mettre en conformité avec la CNIL, former ou accompagner un C.I.L. (correspondant CNIL) ou sensibiliser les agents et salariés à l'hygiène informatique.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Source : http://www.dakaractu.com/Protection-des-Donnees-Personnelles-La-CDP-malienne-venue-s-inspirer-de-l-experience-senegalaise_a100379.html

---

Un rançongiciel Linux

s’attaque aux webmasters, en chiffrant les données des répertoires contenant les pages web | Le Net Expert Informatique

Un rançongiciel Linux s’attaque aux webmasters, en chiffrant les données des répertoires contenant les pages web

Un nouveau rançongiciel s’attaque aux machines Linux et cible en particulier les dossiers contenant les pages web. Le procédé du logiciel malveillant appelé Linux.Encoder est simple. Le rançongiciel crypte les répertoires de MySQL, Apache ainsi que le répertoire home/root. Le système demande alors de payer un seul bitcoin pour déverrouiller les fichiers.

Une fois que la rançon est payée, le système reçoit une instruction lui faisant parcourir les répertoires pour déchiffrer leurs contenus. Pour s’exécuter, la ransomware a besoin des privilèges d’administrateur et éventuellement d’une autorisation de la part d’un administrateur système pour qu’un tel programme puisse s’exécuter sans restriction. Selon le site drweb.com, une fois que le rançongiciel est lancé avec les privilèges d’administrateur, le logiciel télécharge le contenu des dossiers ciblés et crée un ficher contenant le lien vers une clé RSA publique. Le rançongiciel commence alors à supprimer les fichiers originaux et la clé RSA est utilisée pour générer une clé AES qui sera utilisée pour chiffrer les fichiers sur l’ordinateur infecté.

Source : Dr.WEB

Source :
http://www.developpez.com/actu/92220/Un-rancongiciel-Linux-s-attaque-aux-webmasters-en-chiffrant-les-donnees-des-repertoires-contenant-les-pages-web/