Les collégiens de plus en plus victimes de cyberviolences

Les collégiens de plus en plus victimes de cyberviolences

Selon une enquête de l'Éducation nationale dévoilée par RTL jeudi, 18% des élèves de collège déclarent avoir été insultés, humiliés ou victimes d'actions dévalorisantes par le biais de leur téléphone portable ou de leur ordinateur en 2013.

Souvent utiles, les outils numériques comme les téléphones portables, les tablettes ou les ordinateurs peuvent aussi se retourner contre leurs utilisateurs. Au grand dam parfois des plus jeunes, plus vulnérables face à ces nouvelles technologies. Commentaires désobligeants, insultes, photos publiées à leur insu… Depuis deux ans, la cyberviolence se développe dans des proportions inquiétantes dans les collèges.
18% des collégiens déclarent ainsi avoir été insultés, humiliés ou victimes d'actions dévalorisantes en 2013 par le biais des nouvelles technologies, selon une enquête de l'Éducation nationale dévoilée par RTL jeudi.
Parmi eux, 5% affirment avoir subi cette violence de façon répétée et être sujet au «cyberharcèlement». En comparaison, en 2011, seuls 9% des élèves de collège déclaraient avoir été insultés ou humiliés par textos ou internet. Mais à l'époque, l'enquête ne se basait pas sur les mêmes critères qu'aujourd'hui puisque les photos, agressions et «happy slapping» (agressions filmées, ndlr) n'étaient pas pris en compte.

La direction de l'évaluation, de la prospective et de la performance (Depp), la branche statistique du ministère de l'Éducation nationale qui est à l'origine de ce rapport alarmant, a constaté que ce phénomène touchait davantage les élèves de troisième et plus particulièrement les filles. Il n'est par ailleurs pas plus répandu dans les établissements difficiles qu'ailleurs.

Les enseignants aussi victimes de cyberharcèlement
Autre donnée statistique: les élèves victimes de cyberviolence sont en général plus touchés que leurs camarades par d'autres types d'agressions. Un collégien sur trois déclare ainsi avoir subi des coups en plus d'attaques sur la toile, contre un sur sept qui ne déclare pas de cyberviolence. Selon la note de la Depp, «les élèves touchés par la cyberviolence sont aussi deux à trois fois plus nombreux à avoir été épiés dans les toilettes». Ce nouveau type de violence reste toutefois difficile à quantifier, les jeunes victimes ayant souvent du mal à en parler. Si elles se laissent aller à des confidences, c'est le plus souvent en-dehors de leur établissement, à un ami ou un parent. Mais elles sont encore plus d'un tiers à ne pas réussir à en parler.

À une moindre échelle, les enseignants sont eux aussi parfois victimes de cyberharcèlement. Si le phénomène n'est pas nouveau et qu'il reste marginal au regard des autres formes de violences dont sont victimes les professeurs, il n'en reste pas moins en hausse. Les «préjudices informatiques» représentent 3,7 % des dossiers traités par les Autonomes de solidarité laïques (ASL) – qui assurent depuis plus de 110 ans la défense des personnels de l'enseignement public et privé laïque – et la Maif, bien loin derrière les agressions verbales, qui prédominent (75 %). Mais ces chiffres ne prennent en compte que les dossiers déclarés, selon l'assureur Maif, qui évoquait en avril auprès du Figaro une «omerta» autour du cyberharcèlement.

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

Source : http://www.lefigaro.fr/actualite-france/2014/11/27/01016-20141127ARTFIG00086-education-les-collegiens-de-plus-en-plus-victimes-de-cyberviolences.php

---

Coopération Internationale : Le Cap-Vert adhère à la

Convention sur la Cybercriminalité

Coopération Internationale : Le Cap-Vert adhère à la Convention sur la Cybercriminalité

Praia, Cap-Vert – Le Cap-Vert vient d'adhérer à la **Convention sur la cybercriminalité**, créant ainsi les conditions de doter l'archipel de législation nécessaire pour punir ce type de délit, a appris la PANA de source officielle.
Cette Convention était réclamée par les Cap-verdiens, vu l'absence de législation qui permet de punir la cybercriminalité, ce qui a fait que plusieurs personnes ont été victimes de calomnie et de diffamation sur Internet, à travers des commentaires sur les sites d'informations et de blogs online.

La Convention sur la cybercriminalité, approuvée à Budapest (Hongrie) en 2001, réserve à chaque État adhérant la possibilité de produire une législation pour classer les infractions par dommages relatifs à la suppression des données informatiques, au sabotage, à l'utilisation indue de données, à la pornographie infantile, entre autres pratiques illégales.
Elle préconise aussi des infractions concernant la violation du droit d'auteur et aussi les responsabilités et sanctions proportionnelles et dissuasives, dont les peines privatives de liberté.

Toutefois, dans le cas du Cap-Vert, le pays devra aussi créer les conditions pour que les autorités compétentes puissent conserver les données informatiques, dont celles stockées, surtout quant il y a de sérieux risques de perte ou d'altération.
Il est aussi de la responsabilité de l'État du Cap-Vert d'adopter des mesures législatives nécessaires pour permettre aux autorités compétentes d'effectuer des recherches et des saisies de données informatiques stockées.
La Convention sur la cybercriminalité stipule aussi que: "chaque partie devra adopter des mesures législatives nécessaires pour obliger un prestataire du service à garder la confidentialité'.

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

Source : http://www.afriquejet.com/afrique-ouest/13826-informatique-et-cybercriminalite-le-cap-vert-adhere-a-la-convention.html

---

Un logiciel malveillant caché dans le chargeur d'une cigarette électronique

Un logiciel malveillant caché dans le chargeur d'une cigarette électronique

Selon des experts interrogés par The Guardian, si le véhicule de l'attaque est inédit, l »anecdote » en elle-même n'a rien de surprenante : les différents supports USB sont fréquemment à l'origine de virus informatiques.

Décidément, on ne peut plus se fier à rien de nos jours ! The Guardian rapporte l'histoire d'un cadre d'une grande entreprise qui s'est fait piéger par un logiciel malveillant codé dans son chargeur de cigarette électronique. »L'ordinateur d'un des cadres était infecté par un logiciel malveillant dont la source ne pouvait être déterminée. Le système était à jour, avait un antivirus et disposait de tous les dispositifs anti-malwares. […] Au final, après avoir cherché du côté de tous les moyens d'infection traditionnels, le service informatique a cherché d'autres possibilités. Ils ont demandé au cadre: « Y a-t-il des changements dans votre vie récemment? » Et le cadre a répondu: « oui, j'ai arrêté de fumer il y a deux semaines et me suis mis à la cigarette électronique », témoigne un membre du personnel informatique de l'entreprise en question sur le site Reddit.

Selon des experts interrogés par The Guardian, si le véhicule de l'attaque est inédit, l »anecdote » en elle-même n'a rien de surprenante : les différents supports USB sont fréquemment à l'origine de virus informatiques. Les clefs USB sont d'ailleurs plus difficiles à pirater que les périphériques USB. Pour Pierre-Yves Bonnetain, consultant sécurité informatique interrogé par France Info, il faudrait remonter l'ensemble de la chaîne de production des cigarettes électroniques pour en savoir plus. »La chaîne de fabrication est relativement complexe. A un moment ou à un autre, quelque part dans la chaîne, il est parfaitement possible qu'un des ces soust-traitants approvisionnent des composants qui ont déjà été frabriqués en étant malveillants », explique-t-il.

En août, deux chercheurs allemands, Karsten Nohl et Jakob Lell, ont réalisé une expérience pour montrer comment il est possible de transformer le code qui permet de faire fonctionner le périphérique USB pour installer un virus sur l'ordinateur. La faille, nommée Bad USB, permettait de mémoriser n'importe quelle saisie sur votre clavier : mots de passe, numéros de carte bancaire… Et à l'heure actuelle, il existe malheureusement très peu de solutions pour se protéger de ce type de virus. Morale de l'histoire : évitez d'acheter des contrefaçons qui circulent sur le net !

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

Source : http://www.atlantico.fr/atlantico-light/cyber-piratage-logiciel-malveillant-cache-dans-chargeur-cigarette-electronique-1874188.html

---

Du « Privacy by Design » aux Privacy Rules : accompagner et encadrer le développement

des usages autour de la biométrie – JDN Web & Tech

Du « Privacy by Design » aux Privacy Rules : accompagner et encadrer le développement des usages autour de la biométrie

On assiste, depuis quelques mois, à un développement de nouveaux usages de la biométrie, utilisée à des fins de sécurité, dans le cadre d'applications de paiement et de signature électronique, d'authentification en proximité et en ligne…

Cette utilisation de la biométrie s'inscrit dans une logique d'authentification permettant de vérifier que le possesseur du support personnel est « bien le bon titulaire ». Celle-ci se retrouve dans les recommandations émises dans le rapport sur l'avenir des moyens de paiement en France, et la nécessité d'«identifier les évolutions nécessaires des moyens de paiement existants et les innovations qui permettraient d'en créer de nouveaux afin de mieux satisfaire les besoins des consommateurs et des entreprises toutes en améliorant la sécurité et en réduisant les coûts pour l'ensemble des parties prenantes, et ce de manière équitable ».Il s'agit en effet de répondre aux besoins croissants d'une méthode d'authentification simple, universelle et sécurisée, qu'entrainent la dématérialisation croissante des transactions et la multiplication des canaux de distribution (automates bancaires, téléphones et tablettes…).

La frontière devient de plus en plus ténue entre moyen de paiement et moyen d'acceptation
Mais au-delà de la finalité, c'est l'implémentation qui permet de définir un certain niveau de sécurité, d'instaurer la confiance et donc l'appropriation de la technologie. Ainsi une implémentation à des fins de sécurité doit prendre en compte différents paramètres comme l'utilisation d'au moins 2 facteurs, dont un support personnel permettant à l'utilisateur « la maîtrise de sa donnée biométrique ». Ce support assurera le stockage sécurisé des données biométriques et l'exécution des applications (dont l'algorithme de comparaison et les applications reposant sur l'authentification).

Une implémentation appropriée de la biométrie permet d'en garantir l'intégrité et la sécurité et donc la protection de ses données personnelles. Natural Security qui a été distingué en 2013 « Privacy by Design ambassador », a inscrit les problématiques de protection des données personnelles et de la vie privée dés le commencement de ses travaux en 2008. Le PbD, sans être une norme, vise à instaurer un état d'esprit en s'appuyant sur un certain nombre de grands principes . Cette démarche est en parfaite cohérence avec une démarche de type Privacy Impact Assessment qui apparaît à ce regard plus formelle et va tendre à se généraliser en Europe.

La démarche de Privacy By Design trouve un écho tout particulier en Europe où, dés 2005, « les données biométriques qui sont uniquement utilisées à des fins de vérification devraient être stockées de préférence sur un support individuel sécurisé, par exemple, une carte à puce par exemple, que détiendrait la personne concernée ». Le standard définit par Natural Security repose sur des spécifications ouvertes à tous les industriels. Ce choix d'ouverture permet la mise en place d'un schéma d'évaluation et de certification permettant de vérifier que les implémentations ont été effectuées dans le respect des règles et des valeurs qui structurent ce standard. S'il s'agit de vérifier l'interopérabilité entre les différentes implémentations effectuées par les industriels, la démarche de certification vérifie quant à elle que les règles de sécurité et de protection des données personnelles ont bien été implantées.
Dans ce prolongement, des règles de conformité, les « Privacy Rules » viennent compléter le dispositif en engageant le responsable de traitement à une utilisation respectueuse de la protection des données personnelles, afin d'éviter, par exemple, la constitution de base de données biométriques.

D'autres dimensions de l'utilisation de la biométrie restent à discuter. Leur évaluation reste un point clé. On peut souligner le projet de la Biometrics Alliance Initiative , financé par des fonds européens, qui vise à développer un référentiel d'évaluation des technologies biométrique, dans le champ non-régalien afin de définir ce qu'on est en droit d'attendre en termes de performances, d'interopérabilité et de sécurité.

L'utilisation de la biométrie dans un contexte d'authentification constitue un des enjeux d'aujourd'hui pour l'accès aux services et la réalisation de transactions. La démarche de Privacy by Design est une invitation à intégrer la dimension sociale dans la conception d'une technologie. Elle devient dés lors une caractéristique à part entière « Not just good business, but good for business ».

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

Source : http://www.journaldunet.com/ebusiness/expert/59177/du–privacy-by-design–aux-privacy-rules–accompagner-et-encadrer-le-developpement-des-usages-autour-de-la-biometrie.shtml
Chronique de André Delaforge

Utilisation abusive de la messagerie électronique :

licenciement sans cause réelle et sérieuse en l’absence de déclaration préalable à la CNIL

	Utilisation abusive de la messagerie électronique : licenciement sans cause réelle et sérieuse en l’absence de déclaration préalable à la CNIL

Poursuivant sa construction jurisprudentielle extrêmement protectrice des droits personnels du salarié, la Cour de Cassation a rendu un nouvel Arrêt le 8 octobre 2014 (Cass. Soc 8 oct 2014 n° 13-14991) encadrant strictement le contrôle par l'employeur, de l'activité des salariés au travail.

En l'espèce, une salariée avait envoyé et reçu un peu plus de 1 200 mails personnels via sa messagerie professionnelle sur une période de deux mois.
L'employeur avait licenciée ladite salariée pour faute, au motif d'une utilisation excessive de sa messagerie professionnelle à des fins personnelles .

La jurisprudence bien établie de la Chambre Sociale de la Cour de Cassation considérait déjà qu'à défaut de déclaration à la CNIL d'un traitement automatisé d'information nominative en place dans l'entreprise, le licenciement fondé sur un tel grief est sans cause réelle et sérieuse.
Tel est le cas notamment du licenciement d'un salarié qui refuse d'utiliser le système de badge ou de pointeuse à l' entrée et sortie de l'entreprise: faute de déclaration préalable à la CNIL du système mis en place dans l'entreprise, l'employeur ne peut valablement sanctionner le salarié sur ce motif (Cass. Soc 6 avr. 2014 n° 01-45227)

Dans la présente espèce, l'employeur avait précisément réalisé cette déclaration à la CNIL.
Il avait toutefois déclaré le système de surveillance de la messagerie, non pas dès sa mise en service mais près de deux mois et demi après .
Or, ce dispositif avait servi, dès son installation, à mettre en lumière l'utilisation excessive par la salariée concernée de sa messagerie professionnelle à des fins professionnelles.
La Cour de Cassation a trouvé, dans cette espèce, l'occasion de durcir encore davantage sa jurisprudence en invalidant le licenciement de la salariée fondé sur une utilisation abusive de la messagerie électronique durant les deux mois ayant précédé la déclaration du dispositif de surveillance à la CNIL.
La Cour considérant que le système de surveillance étant antérieur à la déclaration à la CNIL, le moyen de preuve de l'employeur quant à la matérialité du motif de licenciement était donc illicite.

La Cour de Cassation indiquant précisément que :
« Constitue un moyen de preuve illicite les informations collectées par un système de traitement automatisé de données personnelles avant sa déclaration à la CNIL ».

Cet arrêt ne fait qu'ajouter à l'arsenal existant de protection des droits des salariés dans l'entreprise à commencer par l'art L1222-4 du Code du travail qui dispose qu'aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été préalablement porté à sa connaissance ou encore le fondamental art L1121-1 du Code du travail.

La Cour de Cassation s'estimant garante, en droit du travail, de la protection des droits fondamentaux des salariés poursuit sa jurisprudence protectrice des droits individuels du salarié qui ne s'arrêtent pas une fois la porte de l'entreprise franchie.
Par Me Sandrine PARIS-FEY
Avocat au Barreau de NANTES
Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.juritravail.com/Actualite/motifs-personnels-de-licenciement/Id/172011

Tout savoir sur votre identité numérique…

	**Tout savoir sur votre identité numérique…**

Vos données personnelles ne sont jamais à l'abri d'une fuite, ou d'un piratage. Derrière vous, vous laissez aussi nombre d'informations, très précieuses pour qui cherche à en tirer profit, pas toujours pour de bonnes raisons. D'où l'importance de faire un check-up de vos traces numériques.

Cet été, vous aurez sûrement suivi le feuilleton du Celebgate, cette fuite de données personnelles appartenant à des célébrités anglo-saxonnes. Ces photos, souvent intimes, provenaient des comptes iCloud des personnes visées, et pour mener à bien son vol de données, le hacker a utilisé deux méthodes : l'attaque par force brute, qui consiste à tester à la volée plusieurs milliers de mots de passe possibles, et l'ingénierie sociale, en cherchant sur le Web des informations lui servant à répondre aux « questions de sécurité » permettant ensuite d'obtenir un mot de passe « oublié ».
Bien souvent, nous choisissons par exemple le nom de notre chien, le nom de jeune fille de notre mère, ou encore le lieu où nous avons effectué nos études. Ces informations sont, dans de nombreux cas, facilement accessibles sur Internet. Il suffit de bien savoir chercher.

C'est le principe du « **Stalking** » : espionner l'autre (ses goûts, son parcours) sans être vu, en exploitant les traces (numériques) qu'il a laissées. En français, cela s'appelle la « **traque furtive** » – pas seulement le lot de certains déséquilibrés, « pervers » : beaucoup d'individus espionnent leur prochain, pour des raisons sentimentales ou professionnelles. Cette traque est possible parce que nous partageons des informations sur nous, sur les réseaux sociaux, sur des blogs, ou dans des forums de discussions, sans avoir conscience que nous ne nous adressons pas forcément qu'à un cercle restreint d'amis – mais aussi à des « amis d'amis d'amis », ou des « amis d'amis d'amis ».

Gare aux stalkers
L'ingénierie sociale, le stalking et le vol de données par les pirates informatiques, ont souvent des conséquences néfastes. Car vos données n'intéressent pas seulement la NSA, ou les entreprises, qui cherchent la plupart du temps à les revendre à des annonceurs publicitaires. Les méchants hackers – rappelons juste qu'à la base, les hackers sont des experts en sécurité, sans mauvaises intentions, et qu'il vaut mieux parler de pirates informatiques pour parler des méchants hackers – mais aussi les cybercriminels, et même votre ex et des personnes de votre entourage qui vous détestent, sont susceptibles de chercher à dénicher vos informations, en cherchant sur le Web, ou en essayant de vous pirater pour cela.

Des données qui vous échappent, et cela peut se traduire par la perte de grosses sommes d'argent, par la perte d'un emploi, par une réputation ternie, ou, pire, par l'usurpation de votre identité. Les cas d'hommes bien sous tous rapports qui, un jour, connaissent l'enfer parce que quelqu'un leur a volé leur identité, sont de plus en plus fréquents, et cela n'arrive pas qu'aux autres. Chaque année en France, plus de 200 000 personnes sont victimes d'usurpation d'identité. Pour les victimes, impossible de se marier, par exemple, parce que les usurpateurs se seront bien souvent déjà mariés sous leurs noms. L'usurpation n'est pas uniquement rendue possible par le fait de jeter à la poubelle des documents importants (factures, relevés bancaires…) : les informations que nous envoyons sur le Net sont aussi de véritables mines d'or.

Googlisez vous !
Pour éviter les mauvaises surprises, il suffit de prendre ses précautions, et de protéger ses données. D'abord, en trouvant les informations déjà en ligne qui pourraient vous compromettre, et les retirer. Gardez ainsi à l'esprit que quelqu'un désirant connaitre des informations personnelles sur vous a désormais toute une gamme d'outils à sa disposition. Et la plus grande aide vient de la personne qu'il veut pister elle même, car celle-ci laisse toute une série d'informations derrière elle, consciemment ou non. D'où l'importance de faire un check-up de votre vie privée online, afin de connaître l'importance des traces numériques que vous laissez derrière vous, puis d'agir en conséquence (en supprimant ces informations).

Vous pouvez (vous devez, même) faire le test : googlisez vous, autrement dit, cherchez votre nom sur Google. Vous trouverez des sites qui parlent de vous, ou des images de vous sur Google Images. Googlisez aussi votre numéro de téléphone, votre adresse de maison, votre numéro de sécurité sociale. Utilisez Google Reverse Image (effectuer une recherche Google à partir d'une photo), en envoyant sur Google des photos récentes de vous, que vous avez partagées sur le web. Cherchez aussi votre nom sur des agrégateurs de réseaux sociaux et de données tels que PeekYou ou Yasni, qui compilent toutes les informations partagées publiquement sur Facebook, Twitter, LinkedIn et autres.

Données sécurisées
Ce check-up, qui devrait être réalisé tous les trois mois pour être efficace, inclut donc votre numéro de téléphone, votre nom, votre adresse, vos comptes Facebook (car les paramètres de confidentialités changent souvent), Twitter et Google, vos comptes sur les sites marchands (Ebay, Amazon, Fnac), et vos comptes bancaires en ligne (afin de vérifier qu'il n'y a aucune transaction suspecte). Pour compléter ce check-up, vous pouvez aussi créer une Google Alerte : ainsi, vous recevrez une notification chaque fois que votre nom, votre adresse e-mail ou votre numéro de téléphone sera ajouté aux résultats de recherche de Google.

A moins que vous ne fassiez déjà attention aux traces que vous laissez derrière vous sur le Web, vous trouverez probablement des informations sur vous-même suite à ce check-up – des informations que vous ne pensiez peut-être pas avoir partagées. Pas de panique : ces informations sont simplement des données que vous avez confiées, un jour, à certains sites, blogs, forums ou réseaux sociaux, et elles peuvent être supprimées. Sans forcément faire appel à des sociétés spécialisées dans la suppression de traces numériques.

Faites le ménage
Une fois le check-up de votre vie privée effectué, place au ménage de printemps. Rendez-vous d'abord sur les réseaux sociaux. Sur Facebook, partez dans les options (cadenas en haut à droite), et rendez inaccessibles les informations que vous partagiez jusque là avec le public, ou avec les amis de vos amis. Créez ensuite des listes, afin de ne partager vos prochaines photos, vos prochains statuts et toutes vos prochaines informations, qu'avec vos amis proches.

Vous devez impérativement considérer le web comme un espace public. Où les informations que vous partagez, où vos communications, où tout ce que vous faites est potentiellement accessible par quelqu'un d'autre – parce que vous n'aurez pas suffisamment sécurisé vos données, le plus souvent. Souvenez-vous que tout ce que vous mettez en ligne peut potentiellement devenir public, quel que soit votre contrôle sur ces données. Dans cette situation, pas question pour vous de vous auto-censurer, car la vie privée est un droit (fondamental) : plutôt que de restreindre votre activité, mieux vaut agir en internaute averti, et apprendre à se protéger.

Sur les réseaux sociaux, à l'avenir, ne fournissez pas d'informations trop personnelles. Si vos amis ne se souviennent pas de votre date de naissance, tant pis pour eux : mieux vaut indiquer une fausse date. Mieux vaut aussi éviter de noter votre lieu de naissance, ainsi que votre lieu de domiciliation. Ensuite, évitez d'accepter comme « amis » d'illustres inconnus, ou des « amis d'amis » : il pourrait s'agir de personnes malintentionnées, guettant par exemple le moment où vous annoncerez votre départ en vacances, et le moment où votre maison sera disposée à être cambriolée.

Sur un réseau social, qu'il s'agisse de Facebook, Google + ou de Twitter, lorsque vous vous apprêtez à partager une photo ou autre chose, posez vous la question : ce que je partage donne-t-il des détails personnels sur moi, sur le lieu où je vis, sur mon travail, ou encore sur mon lieu de vie ? Des informations comme votre âge, votre lieu de naissance ou les lieux où vous avez étudié semblent anodines de prime abord, mais peuvent permettre à des personnes malintentionnées de créer un profil, leur permettant d'usurper votre identité.

Webcam
En ce qui concerne la visibilité de vos informations, vous pouvez vérifier, sur Facebook, comment les internautes qui ne sont pas vos amis voient votre profil, et ce qui est accessible publiquement (option aperçu du profil en tant que). Ensuite, l'on ne saurait vous conseiller que d'ajuster vos paramètres de confidentialité, même si cela peut prendre du temps. Choisissez donc avec qui vous voulez partager des infos, désactivez l'option qui permet à vos amis de vous taguer (identifier) sur une photo, sans votre accord, et privilégiez l'option « visible par moi uniquement » pour la plupart des informations que vous partagerez, afin de changer la visibilité plus tard.

C'est le même principe avec Google + : vérifiez ce qui est disponible sur votre profil public, car vos commentaires sur une vidéo YouTube peuvent par exemple figurer sur votre profil Google +, et cela, même si vous n'utilisez pas Google +, il vous suffit d'utiliser les services de Google pour avoir un compte… En haut de la page, il y a ainsi l'option « profil vu par », puis « moi » ou « tout le monde ». Choisissez « tout le monde », et vérifiez… Rendez-vous ensuite dans les paramètres de confidentialité, en cliquant sur votre compte Google, puis sur « paramètres » et paramètres Google+.

Pour ce qui est des informations sur vous qui ne sont pas sur les réseaux sociaux, vous devrez lister les adresses URL des sites, blogs ou forums qui en possèdent. Puis vous devrez contacter les responsables de ces sites (via la rubrique contact, ou via les mentions légales), et leur demander de supprimer ce qui vous porte préjudice. En cas de refus, vous pourrez adresser une plainte à la CNIL. Concernant les informations scannées et conservées par le moteur de recherche de Google (en cache, pendant plusieurs mois), vous pouvez remplir ce formulaire, mis en place récemment par l'entreprise.

Une fois que vous aurez fait le ménage, et supprimé vos traces, la clé sera d'adopter une certaine hygiène numérique, une attitude sur Internet qui permettra d'empêcher les stalkers et les pirates de vous atteindre. D'abord, utilisez des mots de passe complexes (que vous changerez souvent), en prenant garde à ne pas utiliser le même pour tous vos comptes. Un bon mot de passe est long, et se compose de chiffres, de majuscules et de minuscules.

Prudence est mère de sûreté
Ensuite, évitez d'envoyer par mail des informations sensibles (sauf si vous utilisez des moyens sûrs, comme le chiffrement de vos e-mails) : n'envoyez jamais le scan de votre carte d'identité par e-mail, par exemple. Si vous devez le faire, supprimez immédiatement le mail envoyé, et demandez au destinataire de supprimer votre message une fois le document récupéré, et mis en lieu sûr (dites-lui bien que garder votre scan de carte d'identité sur son bureau d'ordinateur, c'est un peu risqué).

En outre, apprenez à sécuriser vos appareils : utilisez des mots de passe pour votre ordinateur portable, votre tablette ou votre smartphone. En cas de vol, cela permet de rendre vos informations difficilement atteignables, sauf pour quelqu'un s'y connaissant en récupération de données. Ensuite, chiffrez vos données, pour les rendre inutilisables par quelqu'un d'autre que vous et vos destinataires, en utilisant des outils tels que RealCrypt, NCrypt, AxCrypt, ou AESCrypt pour le chiffrement de documents sur un ordinateur et GnuPG pour le chiffrement de vos mails (ce logiciel repose sur l'échange de clés publiques et privées). Enfin, logique, mais utilisez un antivirus, un pare-feu (firewall), mettez ensuite à jour régulièrement ces logiciels, et mettez aussi à jour votre système d'exploitation : quand des failles sont détectées, celles-ci ne sont corrigées que lorsque vous mettez à jour le service en question.

Pour surfer sur le Web sans que les entreprises ne collectent des informations sur vous et votre navigation (via les fichiers « cookies », qui permettent de retracer vos allées et venues sur le Web), utilisez aussi la « navigation privée » des navigateurs Web (Chrome, Firefox, Safari, Internet Explorer, Opera…) – cela se passe, pour tous les navigateurs, dans les options, en cliquant sur « fichier » puis « nouvelle fenêtre de navigation privée ».

Vol de données numériques
Enfin, un dernier conseil, qui vous paraîtra peut être un tantinet parano, mais qui prend tout son sens : mettez du scotch sur votre webcam, si vous possédez un ordinateur portable avec caméra intégrée. Car cette caméra est susceptible d'être hackée, et donc de servir d'instrument d'espionnage. Ce n'est pas une blague. Un hacker piratant votre ordinateur peut fort bien accéder aux images de votre webcam, même si vous ne l'avez pas activée.
Ce fut le cas il y a deux ans aux Etats-Unis, quand des loueurs d'ordinateurs utilisaient des logiciels espions pour espionner leurs clients, et l'année dernière, toujours aux USA, quand une ancienne Miss américaine, Cassidy Wolf, a découvert qu'un hacker avait piraté la webcam de son ordinateur portable, afin de la prendre en photo pendant une année entière, puis de la faire chanter. Le pirate informatique a depuis été arrêté par la police, et condamné à 18 mois de prison ferme, mais le mal a été fait.

Cette série de conseils qui vous permettront de vérifier les traces numériques laissées derrière vous, de les supprimer, et de ne plus en disséminer d'autres du même type, sont à suivre encore, et encore, et encore. Car la sécurité et la vie privée sont bel et bien une lutte constante.

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

Source : http://www.clubic.com/mag/trendy/actualite-740209-vie-privee-faites-check-up-complet.html?estat_svc=s%3D223023201608%26crmID%3D639453874_754265034
par Fabien Soyez

La protection des données personnelles largement ignorée par les professionnels européens de l’informatique

La protection des données personnelles largement ignorée par les professionnels européens de l’informatique

Vidéoprotection, contrôle d'accès…. la protection des données personnelles ne concerne pas que le eCommerce. Or selon un sondage récent, les acteurs européens ignorent l'arrivée imminente du Règlement général sur la protection des données dans le paysage réglementaire de 28 pays de l'Union d'ici à 2015. Malgré les fortes amendes que prévoit le dispositif envers les contrevenants…

Enquête en ligne menée par Ipswitch
sur un échantillon de 316 professionnels
de l'informatique. © Ipswitch

Selon une enquête d'Ipswitch, un éditeur américain de logiciels pour réseaux d'entreprise, une majorité de professionnels de l'informatique en Europe ne savent pas à quelle sauce ils vont être mangés en matière de gestion des données personnelles. En effet, les résultats semblent indiquer que les questions de réglementation et de conformité dans ce domaine sont largement méconnues. Un diagnostic qui s'applique tout particulièrement au Règlement général sur la protection des données (GDPR : General Data Protection Regulation), un texte qui devrait entrer en vigueur dans 28 pays de l'Union européenne entre la fin 2014 et le début de l'année 2015. Réalisée en ligne, en octobre 2014, l'enquête a recueilli la réponse de 316 internautes (104 du Royaume-Uni, 101 de France et 111 d'Allemagne).

Concrètement, plus de la moitié des personnes interrogées (56 %) n'ont pas pu identifier la signification du terme »GDPR ». De plus, 52 % d'entre elles ont admis qu'elles n'étaient pas préparées. Par ailleurs, plus d'un tiers (35 %) des sondés ignorent si les stratégies et processus informatiques mis en place au sein de leurs entreprises sont conformes à la nouvelle réglementation. À l'inverse, 13 % des personnes interrogées placent le GDPR dans leur liste des priorités et 12% seulement seraient prêtes au changement. L'enjeu est pourtant de taille alors que le GDPR prévoit de fortes amendes (jusqu'à 100 millions d'euros ou 5 % du chiffre d'affaires mondial) pour les organisations qui enfreindront les règles !

La France en milieu de podium

Par rapport à leurs homologues allemands et britanniques, les Français se placent dans la moyenne. Ils ne sont ni particulièrement en retard ni particulièrement en avance. D'un coté, les Britanniques se révèlent être les plus préoccupés par la sécurité des « images de nature personnelle » (7% contre seulement 3 % des Français et 2 % des Allemands). De l'autre, nos voisins germaniques semblent les mieux au courant de la problématique GDPR. En effet, près de la moitié d'entre eux (49 %) ont été capables de préciser la signification de l'acronyme. À l'inverse, seul 36 % des professionnels français a su l'indiquer contre un quart (26 %) des professionnels britanniques.

Les résultats de cette enquête doivent pourtant être utilisés avec précaution. En effet, Ipswitch passe sous silence bon nombre d'informations. Par exemple, la nature exacte des métiers exercés par les sondés n'a pas été précisée. Rappelons-le, la problématique des données personnelles touche en priorité les Directeurs et les Responsables de la sécurité des systèmes d'information (DSI et RSSI) des entreprises. Mais également les Centres de supervision urbains (CSU) qui opèrent les caméras de vidéosurveillance déployées en ville. Citons encore les entreprises qui sécurisent des accès physiques avec, par exemple, des équipements biométriques. Ainsi que toute organisation qui doit gérer de près ou de loin des informations d'identification (voir encadré : »Qu'est-ce-qu'une donnée personnelle? »). Avec l'explosion de l'informatique dans le nuage (Cloud Computing), nul doute que cette liste non exhaustive se rallongera de manière exponentielle dans les années à venir.

Qu'est-ce-qu'une donnée personnelle ?

En France, « constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. » (Loi du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel).

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

Source :
http://www.expoprotection.com/site/FR/L_actu_des_risques_malveillance__feu/Zoom_article,I1602,Zoom-e2460ddaaa1c99bf0e47ce05b66a4a7e.htm
par Guillaume Pierre

La reconnaissance juridique du vol de données

La reconnaissance juridique du vol de données

Pour assurer la protection des droits fondamentaux des citoyens, aussi bien les droits positifs que sa protection contre les abus, le Conseil d'Etat préconise 50 mesures à prendre d'urgence.

Le vol de données, une notion mal définie. On entend régulièrement parler dans la presse aussi bien de « vols de données personnelles » de clients, commis au détriment d'opérateurs ou de grandes entreprises, que de « vols de données confidentielles » qui s'apparentent plutôt à de l'espionnage industriel. Dans ces dossiers, le terme de « vol » est utilisé par commodité de langage, mais il n'est pas toujours la qualification retenue juridiquement. En effet, pour qu'il y ait vol, selon la définition du Code pénal (article 311-1), il faut constater la « soustraction frauduleuse de la chose d'autrui ». Or dans un vol de données, celles-ci ne sont pas « soustraites », mais recopiées ; elles demeurent à la disposition de leur légitime propriétaire qui ne peut donc pas déposer plainte pour « vol ».

Cette définition du vol par la « soustraction » date du Code Napoléon (1804). Remarquons que le droit romain était peut-être paradoxalement mieux adapté au vol de données, car les Institutes de l'empereur Justinien, publiées en 529, définissaient plus largement le vol (furtum) comme « contractatio rei fraudulosa » : la manipulation frauduleuse d'une chose (livre IV, titre I, 1). Et de préciser « furtum autem fit, non solum cum quis intercipiendi causa rem alienam amovet, sed generaliter cum quis alienam rem invito domino contractat » : il y a vol, non seulement quand on déplace la chose d'autrui pour la dérober, mais de manière générale quand on en dispose sans la volonté du propriétaire (IV, I, 6).

Mais notre Code pénal moderne lie le vol à la disparition matérielle. Ainsi en avait jugé récemment le tribunal de grande instance de Créteil (23 avril 2013), qui rappelait que « en l'absence de toute soustraction matérielle de documents (…), le simple fait d'avoir téléchargé et enregistré sur plusieurs supports des fichiers informatiques (du légitime propriétaire) qui n'en a jamais été dépossédée, puisque ces données, élément immatériel, demeuraient disponibles et accessibles à tous sur le serveur, ne peut constituer l'élément matériel du vol, la soustraction frauduleuse de la chose d'autrui, délit supposant, pour être constitué, l'appréhension d'une chose ».

Toutefois, la Cour d'appel de Paris a infirmé ce jugement (5 février 2014), et a considéré au contraire que le vol de données était bien caractérisé par le fait de réaliser « des copies de fichiers informatiques inaccessibles au public à des fins personnelles à l'insu et contre le gré de leur propriétaire ». Suite à ces appréciations divergentes de l'applicabilité de l'incrimination de vol, ce dossier se retrouve désormais devant la Cour de cassation, dont la mission est justement de dire comment on doit appliquer le droit.
Il est à noter que la même Cour de cassation avait validé le 9 septembre 2003 une condamnation pour vol, basée sur le fait « d'avoir en sa possession, à son domicile, après avoir démissionné de son emploi pour rejoindre une entreprise concurrente, le contenu informationnel d'une disquette support du logiciel Self Card, sans pouvoir justifier d'une autorisation de reproduction et d'usage du légitime propriétaire ». Elle a de nouveau validé le 4 mars 2008 une condamnation pour vol de données informatiques. Mais dans ces deux dossiers, la Cour n'a pas explicité comment l'incrimination de vol de données devait s'appliquer.

D'autres solutions juridiques
Lorsque l'on est victime d'un vol de données, d'autres solutions juridiques existent pour déposer plainte. Si les données copiées sont des données personnelles (relatives à des personnes identifiées ou identifiables), le recours à l'article 226-18 du code pénal (collecte frauduleuse de données personnelles) est possible.
Si le vol a été effectué via un accès frauduleux au système informatique (cas du hacking, du vol de mot de passe, du phishing…), l'article 323-1 du code pénal trouvera à s'appliquer.
Si c'est une base de données qui a été recopiée, son propriétaire peut réclamer la protection accordée par l'article L341-1 du code de la propriété intellectuelle, mais seulement si la constitution de la base a nécessité un investissement substantiel. La Cour de cassation a ainsi confirmé le 19 juin 2013 un arrêt refusant la protection d'une base de données en raison du caractère non substantiel des investissements réalisés.
Nouveaux éléments. L'arsenal juridique vient récemment de s'enrichir de deux nouveautés. Le 22 octobre 2014, dans une affaire de détournement de fichiers par un salarié, la Cour de cassation a validé la condamnation pour abus de confiance. Or l'article 314-1 du code pénal définit l'abus de confiance comme « le fait par une personne de détourner, au préjudice d'autrui, des fonds, des valeurs ou un bien quelconque qui lui ont été remis et qu'elle a acceptés à charge de les rendre, de les représenter ou d'en faire un usage déterminé ». N'étant pas des fonds ou des valeurs, on en déduit que pour la Cour de cassation les données sont des biens. Ce qui nous ramène à l'idée de vol : si les données sont des biens, la notion de vol de données devient plus naturelle.
Mais le législateur vient peut-être de rendre ces discussions inutiles. En effet, la loi antiterroriste du 13 novembre 2014 modifie l'article 323-3 du code pénal. Cet article, créé par la loi Godfrain de 1988, réprimait jusqu'ici l'introduction frauduleuse de données dans un système informatique, leur modification ou leur suppression. Désormais, sont également interdits les faits « d'extraire, de détenir, de reproduire ou de transmettre » frauduleusement des données. La sanction encourue est de cinq ans de prison et 75.000 euros d'amende, et est portée à sept ans et 100.000 euros s'il s'agit de données personnelles volées dans un système d'information de l'Etat.
La nouvelle rédaction de l'article 323-3 permet donc de réprimer efficacement à l'avenir les vols de données. Elle rend inutile le recours à l'article 311-1 et les débats sur son applicabilité, d'autant plus que la sanction du vol « traditionnel » n'est que de trois ans de prison et 45.000 euros d'amende (article 311-3), soit moins que ce qui est prévu par le nouvel article 323-3 consacré aux données.

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

Source : http://pro.01net.com/editorial/633857/vers-la-reconnaissance-juridique-du-vol-de-donnees/
par Fabrice Mattatia

La collaboration transfrontalière, clé de la lutte contre la cybercriminalité

La collaboration transfrontalière, clé de la lutte contre la cybercriminalité

Europol vient d'annoncer l'interpellation d'une quinzaine d'individus, dont six français, suspectés d'avoir utilisé des chevaux de Troie pour perpétrer différents types de cyber-attaque. L'opération, pilotée par la France, a été réalisée en collaboration avec différents pays européens.

L'office de police intergouvernemental Europol, les forces de l'ordre françaises ainsi que six autres pays (Royaume-Uni, Estonie, Roumanie, Lettonie, Italie et Norvège) ont œuvré conjointement pour mettre la main sur quinze hackers. Jean-Pierre Carlin, directeur Europe du sud de LogRhythm, éditeur américain de logiciels de sécurité informatique basé dans le Colorado (Etats-Unis) et dont le siège social en France se trouve à Neuilly-sur-Seine (92), se félicite de cette collaboration transfrontalière. « Cette arrestation montre que nous sommes en train de rattraper notre retard sur les pirates informatiques, affirme-t-il. Nous disposons de davantage d'outils pour détecter l'origine des attaques et nous sommes capables de les tracer. Partager l'intelligence au-delà des frontières est la clé absolue. »

Coopération inégale

Car, jusqu'à présent, les forces de l'ordre détectaient les malware et les chevaux de Troie sans remonter à la source. Les hackers bénéficiaient donc d'un anonymat total. « Puis, la collaboration entre les pays s'est peu à peu tissée, ajoute Jean-Pierre Carlin. Mais tous les Etats ne coopèrent pas de la même façon. Les pays européens adhérents d'Europol travaillent main dans la main, mais pour les Etats-Unis et les états asiatiques, la donne est différente. »

Cependant, des opérations comme celles-ci ne peuvent être un succès que si les bonnes informations sont mises à disposition. Les organisations ont un rôle à jouer, celui d'assurer leur propre protection. « Toutes les entreprises doivent garantir la surveillance de la moindre activité sur leur réseau en temps réel, précise le directeur Europe du sud de LogRhythm. Avec une visibilité accrue, les comportements anormaux sont identifiés immédiatement et les informations collectées sont partagées avec les autorités pour arrêter les criminels. C'est la fonction de notre produit d'analyse LogRhythm Security Analytics. »

Caroline Albenois

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

Source : http://www.info.expoprotection.com/site/FR/L_actu_des_risques_malveillance__feu/Zoom_article,I1602,Zoom-1e13ba8f63fad9bbf651b6e811431989.htm

---

Sony Pictures victime d'une attaque informatique, les pirates ont publié certaines données sensibles après un chantage

Sony Pictures victime d'une attaque informatique, les pirates ont publié certaines données sensibles après un chantage

Les employés de la filiale du groupe japonais Sony Pictures Entertainment basée à Los Angeles ont eu une surprise des plus désagréables ce lundi 24 novembre 2014. En allumant leurs ordinateurs, une image représentant un squelette avec comme titre en rouge « Hacked By #GOP » (Gardians of Peace) apparaissait sur leurs écrans. Par la suite, les pirates passaient leur message : « nous vous avons déjà prévenu, et ceci n'est que le commencement. Nous continuerons jusqu'à ce que nos exigences soient satisfaites .» En cas de refus d'obtempérer, les pirates menacent de dévoiler à la face du monde des documents obtenus.

Depuis l'expiration de ce délai le 24 novembre 2014 à 23h GMT, plusieurs archives ont été publiées sur divers sites. Même si la plupart des liens ne fonctionnent pas, il est toujours possible de récupérer, sur Thammasatpress, un fichier au format zip de 207 Mo qui contient trois fichiers intitulés LIST1, LIST2 et « Readme ». Ce dernier se présente sous le format texte et contient des adresses électroniques. Pour les deux autres, ils semblent regrouper des documents financiers ainsi que des codes sources et des bases de données. Une analyse avec la commande GREP, dont le rôle est de rechercher un mot dans un fichier et d'afficher les lignes dans lesquelles ce mot a été trouvé, permet d'identifier des clés de chiffrement, mais aussi ce qui ressemble à des documents d'identité relatifs à certaines stars hollywoodiennes à l'instar d'Angelina Jolie.

La société n'était pas joignable pour commenter ces informations, mais un communiqué adressé au Hollywood Reporter indique que « Sony Pictures Entertainment a connu une perturbation de son réseau, et nous travaillons d'arrache-pied pour la résoudre ». Une source a confirmé « qu'un seul serveur a été compromis et l'attaque s'est propagée à partir de là ». Les employés ont été invités à rentrer chez eux après l'attaque : « nous allons tous travailler de la maison. Nous ne pouvons même pas aller sur internet » a déclaré un employé sous le couvert de l'anonymat. Ce dernier a confirmé que le département informatique de l'entreprise a demandé aux employés d'éteindre leurs ordinateurs et de désactiver le WiFi de leurs appareils mobiles, mais également qu'un message adressé aux employés a précisé que la résolution de cet incident pourrait prendre jusqu'à trois semaines.

Outre le blocage des ordinateurs de Sony Pictures, ce sont de nombreux comptes Twitter de Sony qui ont été provisoirement piratés afin de tweeter le même message sur le réseau social. L'entreprise a depuis repris le contrôle de ces comptes Twitter.

Cependant, le magazine spécialisé The Verge avance avoir reçu un courriel de la part des hackers responsables de cette attaque qui dit « nous voulons l'égalité [sic]. Sony ne le veut pas. C'est une bataille ascendante ». D'ailleurs un tweet cinglant de la part de GOP a été adressé à Michael Lynton, le PDG de Sony Entertainments, sur le compte de Starship Trooper's où lui et le reste du staff ont été traités de « criminels ».

Selon The Verge, les pirates ont affirmé avoir réussi à infiltrer la société en travaillant « avec d'autres employés ayant des intérêts similaires » parce que « Sony ne verrouille pas ses portes, physiquement, ». Pour The Verge, cela peut impliquer que les pirates ont réussi à pénétrer les serveurs de l'entreprise avec l'aide de personnes ayant accès aux serveurs internes de Sony.
Sony Pictures quant à lui a choisi de rester sobre dans sa communication en se contentant de dire que « nous enquêtons sur un incident informatique ».

En août dernier, les pirates ont affirmé être venus à bout de PlayStation Network via une attaque par déni de service qui a inondé le système de données réseau erronées. Toutefois, l'entreprise a tenu à rassurer les utilisateurs en affirmant qu'aucune des données personnelles des 53 millions d'utilisateurs de la plateforme PlayStation Network n'a été compromise suite à l'incident daté du 24 août. D'ailleurs, les ingénieurs ont pu à nouveau rendre l'accès disponible dès le lendemain. En 2011, une brèche dans la sécurité de la même plateforme exposait les identifiants (noms d'utilisateur et mots de passe) des utilisateurs.
Source : bloomberg, the verge

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

Source : http://www.developpez.com/actu/77586/Sony-Pictures-victime-d-une-attaque-informatique-les-pirates-ont-publie-certaines-donnees-sensibles-apres-un-chantage/