Quels changements anticiper ? Le règlement européen sur les données personnelles annoncé pour le printemps :

	Quels changements anticiper Le règlement européen sur les données personnelles annoncé pour le printemps : ?

Ce règlement, dont le premier projet remonte à 2012, est appelé à remplacer la directive de 1995 « relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ». Son objectif est d'uniformiser les règles en matière de protection des données personnelles en Europe, de garantir la libre circulation de ces données sur le territoire de l'Union et de simplifier l'exercice de leurs droits par les citoyens européens.

Après des débats parfois acharnés entre les acteurs en présence, que ce soit les CNIL européennes, les acteurs de l'internet et du Big-Data ou encore les représentants des consommateurs, une version consolidée a été arrêtée et diffusée le 15 décembre 2015.
De la loi du 6 janvier 1978 au futur règlement, la législation en matière de protection des données personnelles est allée dans le sens d'une complexité et d'une incertitude toujours plus grande. Les entreprises peuvent-elles attendre plus de sécurité juridique du futur règlement ? La réponse est contrastée.

Un projet de texte stabilisé… mais pas encore adopté
Il convient tout d'abord de tempérer l'enthousiasme affiché des institutions européennes : le texte définitif n'est pas encore adopté. Après un premier vote du Parlement européen en mars 2014, le Conseil de l'Union européenne donnait mandat au Luxembourg en juin 2015, dans le cadre de la présidence tournante de l'Union européenne, pour parvenir à un consensus sur le projet de règlement au plus tard fin décembre de la même année. Au terme de discussions intenses, Parlement et Conseil sont parvenus à un accord *in extremis* avant la trêve des confiseurs sur un document de pas moins de 200 pages…
Cet accord n'est pour le moment que politique, et la prochaine étape est un vote en deuxième lecture par le Parlement européen pour adoption définitive.
Le règlement européen sera ensuite applicable dans un délai de deux ans après son adoption. La différence essentielle par rapport à la directive de 1995 est que ce texte sera directement applicable au sein de l'Union européenne, sans que chacun des 27 états ne doive adopter des lois nationales de transposition, ce qui aurait nécessairement nui à l'objectif d'harmonisation. Les règles européennes nouvelles remplaceront donc automatiquement les règles nationales existantes incompatibles. Ainsi, pour ses 40 ans, la Loi française du 6 janvier 1978 dite « Informatique et Libertés » va se retrouver fortement vidée de sa substance.
Les entreprises ont donc encore un peu de temps devant elles pour se préparer à la mise en œuvre des nouvelles règles. Quels sont les changements majeurs à anticiper ?

***« Accountability »* et « *Privacy by Design* » sont des termes qui doivent devenir familiers**
Quelles données pourront être traitées ? Quelle durée de conservation appliquer ? Quels outils techniques installer ? Quelles formalités accomplir ?
Si le règlement uniformise la réponse à ses questions au sein de l'Union européenne… il ne les simplifie par nécessairement. Une large place sera faite à l'interprétation des dispositions nouvelles.

La **définition des données personnelles** ne change pas fondamentalement. Le règlement s'applique aux traitements des données identifiantes ou permettant d'identifier une personne, que ce soit directement ou indirectement. Le projet de règlement ajoute toutefois une série d'exemples de données qui permettent d'identifier une personne : son nom, mais également un numéro d'identification, une donnée de localisation, un identifiant d'un compte en ligne, ainsi que des références à des informations relatives à l'identité physique, génétique, mentale, économique, sociale ou culturelle d'une personne. Ces précisions sont dans la logique de la position actuelle des juridictions européennes et françaises.
S'agissant des **modalités de traitement** des données personnelles, il est abondamment fait référence dans le texte à la notion de *Privacy by Design*.
Qu'est-ce que cela signifie concrètement ? Les entreprises seront désormais tenues d'anticiper les sujets relatifs aux traitements de données dès les premières étapes de leurs projets informatiques, afin qu'il soit vérifié en amont que les développements à intervenir, où les logiciels à implémenter, seront conformes aux exigences imposées par le règlement.
Le responsable du traitement devra ainsi « *implémenter les mesures techniques et organisationnelles appropriées, telles que l'anonymisation, qui sont conçues pour mettre en œuvre les principes de protection des données, […] d'une manière effective et d'intégrer les protections nécessaires dans les traitements de manière à respecter les exigences du règlement et à protéger les droits des intéressés.* »
Une pondération devra en effet être faite entre coûts, état de l'art, contexte, finalités des traitements concernés, risques pour les droits et libertés des individus, etc. Autant de concepts dont la cohabitation laissera une grande place à une appréciation au cas par cas. Le règlement envisage qu'un mécanisme de certification soit mis en place, probablement afin de faciliter cette appréciation, bien que les procédures de certifications pèchent parfois par leur complexité.
Comme en l'état actuel de la législation, le règlement ne prévoit pas expressément de **durée de conservation des données**, et l'on peut le regretter. L'appréciation d'une durée de conservation des données sous une forme identifiante « *qui n'excède pas la durée nécessaire aux finalités pour lesquelles [les données] sont collectées et traitées* », place souvent le responsable de traitement dans une situation d'insécurité juridique. En revanche, dans sa dernière version, le projet de règlement prévoit que cette durée de conservation, ou *a minima* les critères retenus pour fixer cette durée, devront être portés à l'attention de la personne concernée dès la collecte. Les responsables de traitements devront donc apporter une attention particulière à ce sujet avant la mise en œuvre du traitement.
Les **formalités administratives** seront allégées : moins de notifications préalables aux autorités nationales, moins d'interlocuteurs. Un des objectifs principaux de ce texte est de garantir la libre circulation des données au sein de l'Union européenne. Ainsi, pour les groupes ayant des établissements dans plusieurs pays d'Europe, ou une activité ciblant plusieurs Etats-Membres, le principe du « guichet unique » permettra que les formalités requises ne soient effectuées qu'auprès de l'autorité de l'Etat Membre dans lequel le groupe a son établissement principal, les autorités des différents Etats Membres devant ensuite coopérer entre elles.
Les sociétés établies en dehors de l'Union européenne, mais ayant une activité ciblant le public européen, devront quant à elles désigner un représentant sur le territoire de l'Union, qui agira comme point de contact unique, tant pour les autorités que pour les personnes dont la société en question traite les données. A l'instar des pratiques en matière de fiscalité, cette dernière exigence incitera très probablement les grands acteurs du numérique non établis en Europe à désigner un représentant dans un Etat Membre dont l'autorité nationale de protection des données aura des règles réputées plus souples, ou disposera de moins de moyens pour diligenter des contrôles ou engager des procédures de sanction. Ces disparités devraient toutefois être tempérées par la coordination qu'assurera la nouvelle autorité européenne instaurée par le règlement.
En revanche, les **procédures internes seront quant à elles décuplées…** Un contrôleur à la protection des données devra être désigné dans les entités publiques et dans les entreprises traitant des données personnelles à une échelle importante. Il convient de souligner qu'il n'y a pas de seuil chiffré permettant à une entreprise de déterminer si elle doit ou non désigner une telle personne. Sa désignation est requise lorsque l'activité de l'entreprise implique le traitement de données personnelles de manière régulière et systématique sur une large échelle…
Le contrôleur pourra alternativement être salarié ou prestataire de service. Le responsable de traitement devra également tenir à jour des registres des traitements mis en œuvre sur le même modèle que ce qui existe actuellement pour les CIL. Dans la logique du principe d'« *accountability* », ces mesures devront permettre au responsable de traitement de démontrer que les traitements qu'il met en œuvre se font en conformité avec le règlement.
Afin de faciliter aux entreprises la mise en œuvre de telles procédures, et la démonstration de conformité du responsable de traitement à ses obligations, le règlement renvoie ici encore à un mécanisme de certification ou à des codes de conduite.

Et côté personnes physiques, quels droits ? Quelles protections nouvelles ?
Les personnes dont les données sont traitées devront bénéficier d'une **information plus large** sur les traitements qui les concernent. Outre les informations qui doivent déjà être fournies lors de la collecte de données en application de la Loi Informatique et Libertés, le responsable de traitement doit notamment préciser le fondement juridique du traitement, ainsi que la possibilité de déposer plainte auprès d'une autorité compétente d'un Etat Membre. Les mentions d'informations fournies par les responsables de traitement devront donc être ajustées.
Les personnes dont les données sont traitées bénéficieront d'un **droit à la portabilité de leurs données**. Les responsables de traitement devront donc être en mesure de restituer aux personnes dont les données sont traitées lesdites données, et ce dans un format standard et exploitable, afin qu'elles puissent être communiquées à un autre prestataire de services. Cette communication de données pourra même se faire directement au nouveau prestataire sur demande de la personne concernée.
Le projet de règlement prévoit des règles nouvelles encadrant **les traitements de données relatives aux enfants**. Ainsi, l'article 8 du projet de règlement prévoit une disposition visant à interdire aux services de la société de l'information destinés aux mineurs de 16 ans de recueillir leurs données personnelles sans autorisation préalable d'un titulaire de l'autorité parentale. Les Etats Membres pourront décider d'abaisser cette limite d'âge jusqu'à 13 ans. Le texte ajoute que le responsable de traitement devra fournir des efforts raisonnables, au regard des technologies disponibles, pour vérifier que le consentement est bien fourni par le titulaire de l'autorité parentale.
Les éléments détaillés ci-dessus ne sont que quelques points d'attention extraits parmi les 209 pages du projet de règlement dans sa dernière version. Les subtilités se cachent dans les détails et les 4 années de modifications et de reformulations du texte depuis sa première mouture ont pu altérer sa cohérence. Les deux années avant l'entrée en vigueur des dispositions nouvelles ne seront pas de trop pour permettre aux entreprises de se mettre en conformité. D'autant qu'en cas de manquement, les sanctions administratives pourront désormais aller jusqu'à 20 000 000 d'euros ou 4% du chiffre d'affaires mondial… ce qui est sans commune mesure avec les 150 000 euros d'amende que peut à ce jour prononcer la CNIL.

Réagissez à cet article

Source : *Le règlement européen sur les données personnelles annoncé pour le printemps : Quels changements anticiper ? – Féral-Schuhl Sainte-Marie*

La Cnil pourra infliger jusqu'à 20 millions d'euros d'amende

La Cnil pourra infliger jusqu'à 20 millions d'euros d'amende

Pourtant hostile au départ, le gouvernement est désormais favorable à un renforcement du pouvoir de sanction de la Cnil : jusqu'à 20 millions d'euros en cas de récidive. Et la portabilité des données ? « Ce sont les gros qui sont énervés » répond Axelle Lemaire.

Le projet de loi République numérique présenté par Axelle Lemaire est actuellement débattu par les députés. De nombreux amendements sont à l'étude, dont certains rejetés par le gouvernement. Celui-ci s'est en revanche rallié à une proposition des parlementaires en faveur d'un renforcement du pouvoir de sanction de la Cnil, l'autorité en charge de la protection des données personnelles.
Selon Les Echos, le gouvernement soutient donc désormais un amendement prévoyant, en cas de récidive, de permettre à la Cnil d'infliger une sanction pouvant atteindre jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires. A ce jour, en cas de récidive, la sanction ne peut pas dépasser les 300.000 euros.

Les « gros » sont « énervés »

Une autre mesure portant sur les données fait grincer des dents au sein de plusieurs organisations d'entreprises du numérique : la portabilité des données entre plateformes.
« Par son caractère large, il impose des contraintes extrêmement lourdes à des secteurs dans lesquels la portabilité n'apporte pas d'intérêt du point de vue des consommateurs et sur le plan de la concurrence. En l'état, il menace directement les investissements massifs réalisés par les entreprises du secteur afin d'améliorer leurs services » dénonçaient-elles notamment dans un communiqué du 14 janvier.
Message reçu au sein du gouvernement ? Difficile à dire puisque la ministre du numérique déclarait lundi 18 janvier sur RMC vouloir « protéger la concurrence ». « Ce sont les gros qui sont énervés, pas les petits » ajoutait-elle.

Réagissez à cet article

Source : *La Cnil pourra infliger jusqu’à 20 millions d’euros d’amende*

Mots de passe : nos conseils pour une sécurité maximum

	**Mots de passe : nos conseils pour une sécurité maximum**

---

password, admin, 123456, abcdef, qwerty, j'en passe et des meilleures… Voilà des mots de passe encore bien utilisés si l'on en croit le palmarès 2013 des 25 mots de passe les plus fréquents (publié par la société SplashData, éditrice de logiciels). Mais de véritables passoires en termes de sécurité ! A l'heure du cloud et des services Web qui numérisent toujours un peu plus nos vies, la vigilance ne saurait souffrir de négligences. De l'importance de sécuriser ses mots de passe, nous vous expliquons le pourquoi et le comment.

Paranoïa, quand tu nous gagnes…

On a beau être d'un naturel plutôt stoïque, la lecture du rapport P@$$1234: the end of strong password-only security publié en janvier 2013 par le cabinet d'expertise Deloitte donne tout de même quelques sueurs froides… Il s'appuie sur un travail intéressant de Mark Burnett (du site Xato.net), lequel a décortiqué une liste de 6 millions de duos login plus mot de passe uniques pour en extraire des statistiques.

- 98,8 % de cette base d'utilisateurs emploient les 10 000 mots de passe les plus fréquents ;
- 91 % se concentrent sur 1 000 mots de passe ;
- 40 % font avec 100 mots de passe ;
- 14 % (soit 840 000 personnes tout de même) piochent dans le top 10 !

Et le problème de ces mots de passe ultra bateau, dont « password » et « 123456 », c'est qu'ils représentent le degré zéro de sécurité, puisqu'ils seront les premiers à être testés par tout hacker qui se respecte. Le souci de sécurité n'est visiblement pas encore rentré dans toutes les têtes…

Pour mieux se protéger de l'ennemi, il faut tenter de le comprendre. Comment les hackeurs fonctionnent dans les grandes lignes ? Quatre scenarii sont à envisager : le piratage en direct, le vol de bases de données, le phishing (ou plus globalement le *social engineering* précise Paul Rascagnères, analyste malware chez l'éditeur d'antivirus G DATA) et les virus.

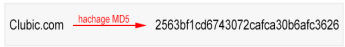
Le premier, qui consiste à tester tous les mots de passe possibles et imaginables dans une interface de connexion sur la base d'un identifiant connu, n'est plus possible aujourd'hui ou très rarement. Cela, parce que la grande majorité des sites sérieux bloquent les comptes au bout de quelques tentatives ratées, trop peu nombreuses même pour un mot de passe évident (quoique avec password et 123456…).

Non, le gros des dangers tient dans le vol, les virus et le *social engineering*. Pour ce dernier, une sorte de vol avec consentement non éclairé, la complexité d'un mot de passe n'a pas d'intérêt : le hackeur se fait passer pour quelqu'un d'autre (email, coup de fil ou faux site officiel), et s'il parvient à duper l'utilisateur, il en profite pour récupérer ses identifiants, en clair. La pratique est courante, les données sont ensuite utilisées ou revendues sur des marchés parallèles. Le seul remède dans ce cas, c'est la vigilance. Idem pour l'aspect virus, un malware avec keylogger peut intercepter vos saisies au clavier ou chiper les identifiants stockés dans le navigateur par exemple : votre ordinateur doit être protégé par un antivirus, à jour, et en programmant des analyses régulières.

? Un hash qui part d'autant plus vite en fumée que le mot de passe est simple ?

C'est en matière de vol qu'il est intéressant de comprendre les mécanismes. Tous les couples identifiants / mots de passe des services Web sont stockés sur les serveurs des entreprises respectives, et forment ainsi autant de bases de données. Ces vols sont assez ponctuels mais malheureusement massifs (par milliers voire millions d'entrées). Très rarement (et normalement pas en France puisque c'est illégal), ces bases de données sont stockées en clair. Si dérobade il y a, la complexité du mot de passe sera vaine.

Mais dans la majorité des cas, les identifiants et mots de passe sont hachés, c'est-à-dire brouillés par un algorithme. Quand quelqu'un veut se connecter à son service, le mot de passe qu'il entre est également haché en temps réel, puis comparé à celui stocké sur les serveurs. Les hackeurs qui se procurent pareilles bases de données vont devoir utiliser des logiciels spécifiques pour déterminer quelle fonction de hachage (hash en anglais) a été utilisée, après quoi ils peuvent automatiser les tests. Tests qui vont consister à choisir un mot, le hacher, le comparer à l'empreinte hachée de la base de données volée : s'il y a correspondance, le mot de passe est trouvé, sinon il faut tester un autre mot, etc. Un hash qui part d'autant plus vite en fumée que le mot de passe est simple.



En hachant un mot via un algorithme, on obtient une empreinte de ce type. Il existe plusieurs algorithmes, proposant des niveaux de sécurité plus ou moins élevés : MD5, SHA-1, SHA-2, etc…

Le hasard fait parfois bien les choses, mais les statistiques les font encore mieux. Pour éviter de tâtonner au doigt mouillé, les hackeurs recourent à des dictionnaires, ou mieux encore, à des listings de mots de passe qui ont été établis au fil des différents vols de données, comme la base du réseau communautaire RockYou.com et ses 32 millions d'entrées évaporées dans la nature en 2009. De vrais mots de passe, couramment employés, et qui ne changent pas beaucoup, comme en témoigne la constance des palmarès des mots de passe les plus fréquents, d'une année sur l'autre. Les cas de vols de données ne manquent pas : Ebay,Orange, Domino's Pizza ou encore Adobe pour les exemples les plus récents.

Vends forfait 4G pas cher, avec livraison à domicile. Seul moyen de paiement accepté : l'abonnement annuel.

Les listings contiennent des mots simples, les logiciels pirates proposent donc des règles complexes. Mais faciles à mettre en oeuvre d'après le journaliste Nat Anderson. Son expérience est instructive. En tentant de se mettre dans la peau d'un hacker, il a potassé le fonctionnement des logiciels pirates, et notamment de Hashcat, qui sont, sans surprise, très bien conçus.

En quelques clics, on peut étoffer la recherche, de sorte à ce que sur un mot de passe comme « clubic » (à tout hasard), le logiciel teste également des ajouts de chiffres ou de lettres (« clubic10 » ou « clubicz »), mais aussi l'ordre inversé (« cibulc »), les ajouts de préfixes et suffixes courants (man, 123, mad, me…), la version *leet*, c'est-à-dire avec des caractères alphanumériques ASCII (« (|_ |_| |3 | (») voire des inversions de lettres. De quoi multiplier les chances du malfaiteur d'arriver à ses fins.


Le logiciel Hashcat

? Un mot de passe à 8 caractères hacké en 5 h 30 ?

Plus efficace encore mais exigeante en ressources, la bonne vieille attaque de force brute. Sur une quantité donnée de caractères, mettons six, la technique un brin bourrine consiste à hacher et tester « aaaaaa », puis « aaaaab », etc. Sachant qu'un clavier français peut produire 142 caractères (avec tous les accents, la casse, les symboles, les chiffres, et encore 103 si on exclut les accents) et que la statistique est exponentielle, ça nous fait 8 198 418 170 944 de combinaisons possibles (8 200 milliards pour ceux qu'autant de chiffres perturberait). Dans l'exemple donné par l'étude du cabinet Deloitte, un mot de passe à 8 caractères (6,1 millions de milliards de possibilités sur un clavier américain à 94 caractères) pourrait être hacké en 5 h 30 par une configuration dédiée haut de gamme (estimée à 30 000 $ en 2012), mais en près d'un an avec un PC correct de 2011.

Représentation visuelle de ces chiffres astronomiques

Le petit point noir, c'est le nombre de combinaisons à 8 caractères, le gros point bleu c'est avec 10 caractères. Les joies de l'exponentiel !

Voilà donc la clef : plus un mot de passe est complexe (avec des caractères spéciaux, un séquençage aléatoire, etc.) et long, plus le hacker aura du fil à retordre. Rien qu'en passant à 10 caractères, courbe exponentielle oblige, on fait grimper les combinaisons sur un clavier français à 3 333 369 396 234 118 349 824 (3 333 milliards de milliards !!!). La même machine de compétition mettrait alors 343 ans pour tester toutes les combinaisons… A cette parade, les hacker répondent par le crowd-hacking : ils confient des fragments de calculs à faire à des milliers de PC normaux infectés (les fameux PC zombies). C'est supposé aller beaucoup plus vite ainsi, mais bon, les hackers préfèrent tout de même les mots de passe courts et basiques.

? nous peinerions à retenir plus de sept chiffres dans notre mémoire à court terme ?

Le remède est simple, sa mise en oeuvre plus délicate. D'après une étude de l'Université de Toronto que cite le rapport Deloitte, les êtres humains limités que nous sommes peinerions à retenir plus de sept chiffres dans notre mémoire à court terme, et même plus que cinq en prenant de l'âge. L'ajout de symboles, de lettres majuscules et minuscules produirait un mix encore moins aisé à retenir. Le rapport se fait plus accablant en ajoutant que la nature humaine a tendance à suivre des schémas de pensée limités par rapport aux possibilités offertes. La majuscule ? En première position dans les mots. Les chiffres ? À la fin. Des 32 symboles présents sur un clavier américain ? Une demi-douzaine seulement est utilisée. De quoi rendre l'aléa théorique plus prédictif pour les hackers. Rien de nouveau cependant. A moins que… le rapport ne pointe du doigt un nouveau frein, imputable aux usages mobiles. L'absence ou la moindre accessibilité des caractères spéciaux sur les claviers des smartphones amène le nomade à simplifier son mot de passe. Tout comme le temps de saisie supérieur qui inciterait un quart des personnes sondées à utiliser un mot de passe plus court pour gagner du temps. De 4 à 5 secondes pour taper un mot de passe de 10 caractères sur un clavier standard d'ordinateur, il faudrait entre 7 et 30 secondes pour faire la même chose depuis un smartphone tactile.

Réagissez à cet article

Source : *Mots de passe : nos conseils pour une sécurité maximum*

Alerte : Vulnérabilité zero-day qui affecte des millions de systèmes Linux et Android

Alerte : Vulnérabilité zero-day affecte des millions de systèmes Linux et Android

---

Le fournisseur en sécurité Perception Point a découvert une vulnérabilité zero-day présente dans le code source de Linux depuis 2012. Touchant des dizaines de millions de postes de travail et serveurs Linux 3 et 64-bit, mais également tous les terminaux Android 4.4 ou supérieurs, cette vulnérabilité sera corrigée sous peu.

Une nouvelle vulnérabilité zero-day a été découverte permettant à des applications Android ou Linux d'escalader des privilèges et d'avoir un accès root, d'après un rapport publié ce matin par le fournisseur de solutions de sécurité Perception Point. « Elle affecte tous les téléphones Android sous KitKat (4.4) ou supérieurs », a fait savoir Yevgeny Pats, co-fondateur et CEO de Perception Point.

Toutes les machines dotées d'un noyau Linux 3.8 (ou supérieur) sont vulnérables, incluant des dizaines de millions de PC et serveurs Linux, aussi bien 32 que 64 bits. En tirant parti de cette vulnérabilité, des attaquants sont en mesure de supprimer des fichiers, accéder à des informations personnelles, et installer divers programmes.

Des correctifs disponibles via des mises à jour automatiques

Cette vulnérabilité, présente dans le code source de Linux depuis 2012 mais découverte seulement maintenant par Perception Point, n'a pour l'heure pas été exploitée. L'équipe Linux a été prévenue et des correctifs devraient être disponibles sous peu et seront installés via des mises à jour automatiques. Selon Yevgeny Pats, cette vulnérabilité zero-day (CVE-2016-0728) concerne le service keyrings facility permettant aux drivers de sauvegarder dans le noyau de l'OS des données de sécurité ainsi que des clés d'authentification et de chiffrement.

Réagissez à cet article

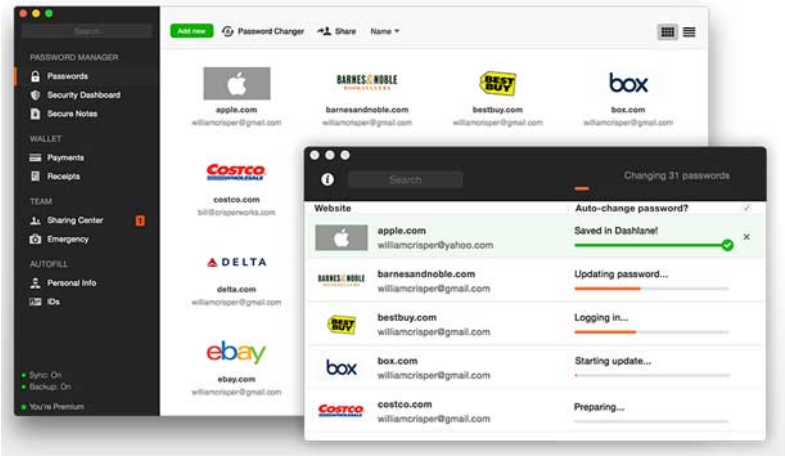
Source : *Une vulnérabilité zero-day affecte des millions de systèmes Linux et Android – Le Monde Informatique*

Article de Dominique Filippone avec IDG News Service

Dashlane : 500 mots de passe modifiés en un clin d’oeil

Dashlane : 500 mots de passe modifiés en un clin d’oeil

La nouvelle version de l'outil français des gestion des mots de passe propose d'automatiser la gestion des mots de passe. De quoi soulager des utilisateurs toujours plus sollicités sur le terrain de la sécurité.



La multiplication des services en ligne fait exploser le nombre de mots de passe utilisés par les professionnels. Au point de poser des problèmes de mémoires insolubles. Google réfléchit à les remplacer grâce au smartphone.

Dashlane propose le changement automatique de mot de passe pour 500 sites Web. (Source : Dashlane)

La pépite Dashlane propose elle une alternative au stockage manuel de plusieurs mots de passe en automatisant le stockage et la modification des mots de passe. Et la dernière version de l'outil permet de le faire pour 500 sites (au lieu de 75 jusqu'alors) et services web en un seul clic, avec la fonctionnalité Password Changer.

Banque et mot de passe

8 formats de documents sont désormais pris en charge : les applications, les bases de données, les documents financiers, les documents juridiques, les abonnements, les licences logicielles et les mots de passe Wi-Fi. Autres nouveautés de cette quatrièmes version de Dashlane, 7 langues différentes sont supportées et l'interface graphique a été revue de mnière à être identique quelque soit la plateforme (Mac, PC, iOS et Android). Autre amélioration, un moteur de recherche plus performant et un affichage des résultats sous divers formats.

Côté moyen de paiement, 618 nouvelles banques internationales peuvent être utilisées dans les moyens de paiement. A noter que la version de base de Dashlane est proposées gratuitement, et que la version Premium 39,99 euros/an) permet de synchroniser les données sur mobile (nombre illimité d'appareils) et de les sauvegarder en mode sécurisé.

Réagissez à cet article

Source : *Dashlane : 500 mots de passe modifiés en un clin d'oeil*

Wi-Fi dans les TGV : il faudra finalement attendre 2017

Wi-Fi dans les TGV : il faudra finalement attendre 2017

Une connexion gratuite devait être proposée sur certaines lignes dès le milieu de cette année, mais la SNCF et ses partenaires opérateurs semblent (encore) prendre du retard.

La présence d'un Wi-Fi fonctionnel et rapide dans les TGV relève de plus en plus de l'Arlésienne. En octobre 2014, Axelle Lemaire, la secrétaire d'Etat au Numérique s'agaçait comme beaucoup de l'absence de cette technologie. Alors que de nombreuses compagnies ferroviaires dans le monde proposent ce service, aujourd'hui considéré comme une commodité, le fleuron de la SNCF reste aveugle et muet. Alors bien sûr, il est toujours possible d'accrocher un réseau 3G ou 4G. Mais à grande vitesse, la qualité de service est rarement au rendez-vous et les coupures fréquentes.

Face à la pression, la SNCF annonçait en février 2015 que le Wi-Fi gratuit serait opérationnel dans les trains, à partir de mi-2016. La ligne TGV Paris-Lyon sera équipée fin 2016. La ligne TGV Est et Paris-Bordeaux seront couvertes mi-2017. « Le dispositif sera testé et opéré de manière commerciale dès juin 2015. Il faut ensuite le temps d'équiper toutes les lignes », déclare Frédéric Burtz, responsable de l'innovation à la direction digitale SNCF.

Manque de bol, il faudra encore attendre un peu. « On va mettre en œuvre des systèmes dans les trains pour permettre d'avoir le Wi-Fi, en commençant par les trains à grande vitesse. En 2017, vous allez commencer à avoir ça », a indiqué sur BFM Business, Barbara Dallibard, la directrice générale de la branche SNCF voyageurs. Les lignes classiques suivront.

La 4G à la rescousse

Quelques mois supplémentaires de patience… Rappelons que techniquement, la SNCF n'utilisera plus le satellite pour acheminer les données mais la 4G aujourd'hui largement déployée. Ensuite, le W-Fi prendra le relai à l'intérieur des rames à grande vitesse. « Le choix du satellite, que nous avons fait il y a 5 ans n'était pas le meilleur. Le principal problème est son coût, d'environ 1 million d'euros par rame. Nous avons réalisé des essais notamment dans l'Est de la France mais de l'avis des clients, c'était superbof. Aujourd'hui on en tire les leçons », expliquait il y a quelques mois Guillaume Pépy, p-dg de la SNCF.

Pour mener à bien le projet, la SNCF s'attache donc avec les opérateurs mobiles à améliorer la couverture mobile 2G, 3G, 4G dans les trains classiques mais aussi les TGV. Il s'agit de déterminer quelles sont les zones blanches ou grises qui provoquent coupures et perte de réseau. « C'est la fin du renvoi de balle entre les opérateurs et la SNCF », a promis Guillaume Pépy.

Au total, la SNCF va consacrer un budget de 150 millions d'euros par an, au cours des trois ans qui viennent. Cela coûte « très cher en raison de la vitesse des trains et ce qui est fait sur Thalys (où les TGV sont équipés du Wi-Fi) est difficilement généralisable », précisait Axelle Lemaire. Le coût est évalué à 350.000 euros par rame. Reste la question du modèle économique : ce Wi-Fi gratuit sera-t-il financé par la publicité ?

Rappelons qu'en 2010, la société nationale annonçait fièrement que les usagers du TGV Est (12 millions de voyageurs par an) seraient les premiers à pouvoir disposer (en 1ère et 2ème classe) d'un accès Wi-Fi via le service Box TGV (facturé 4,99 euros par heure ou 9,99 euros pour toute la durée de leur voyage).

« On a fait la bêtise de le faire nous-mêmes », avait indiqué Guillaume Pepy. « Il y a dix ans, on a investi 30 ou 50 millions d'euros pour mettre le wifi dans le TGV Est et Thalys. Aujourd'hui, cet investissement est perdu ».

Réagissez à cet article

Source : *Wi-Fi dans les TGV : il faudra finalement attendre*

2017

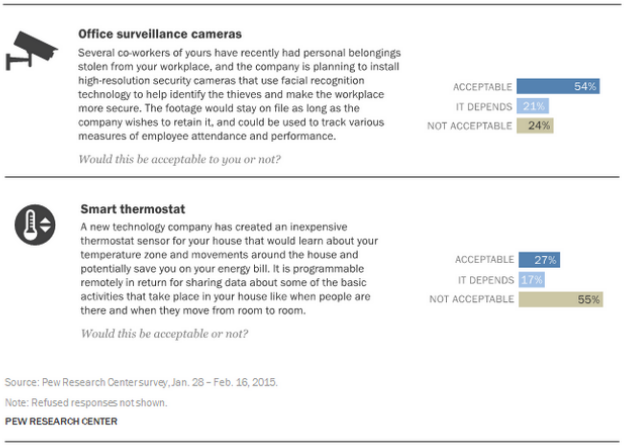
Données personnelles : les Américains sont prêts à faire des concessions

Données personnelles : les Américains sont prêts à faire des concessions

---

Selon une étude de Pew Research Center, une large proportion d'Américains est prête à dévoiler des informations personnelles en échange d'un bien ou d'un service. Du gagnant-gagnant ?

La protection de la vie privée serait un concept à géométrie variable pour les Américains, selon une étude menée par le **Pew Research Center**. Selon lui, une majorité d'Américains ne verraient pas d'inconvénient à partager avec des tiers leurs données personnels, en échange d'un produit, d'un service, ou pour d'autres bénéfices.
Ainsi, 54% d'entre eux estiment qu'il est acceptable pour un employeur d'installer des caméras de surveillance dans les locaux de l'entreprise, pour dissuader – officiellement- d'éventuels voleurs et 47% sont enclins à délivrer des infos personnels pour disposer d'une carte de fidélité.
Alors que, paradoxalement, 55% des personnes interrogées sont réticentes à l'idée d'utiliser au sein de leur foyer un thermostat connecté, susceptibles de relayer auprès de prestataires des informations sur les us et coutumes d'une maisonnée.



En outre, les Américains sondés sont aussi réfractaires aux sollicitations que ne leur « rapportent » rien en échange : ils n'apprécient ainsi que très peu les envois de spams et les demandes de contacts intempestives qui arrivent après avoir partagé avec une entreprises des données personnelles.
Les plus réfractaires au partage d'informations privées mettent surtout en exergue le fait qu'ils ne sont pas tenus au courant des types d'entreprises qui ont accès à ces données. L'anonymisation ne se fait qu'en un seul sens…
Ils s'interrogent aussi sur intentions qui motivent ce type d'entrepris, ravivant ainsi une certaine peur du « Big Brother ».

Crédit image : Gajus – Shutterstock.com

Réagissez à cet article

Source : *Données personnelles : les Américains sont prêts à faire des concessions | ITespresso.fr*

Panorama de la Cybercriminalité en 2015 : Attaques sur tous les fronts !

Panorama de la Cybercriminalité en 2015 : Attaques sur tous les fronts !

La nouvelle édition du panorama de la cybercriminalité du CLUSIF a fait la démonstration que la crise ne touche pas les pirates informatiques bien au contraire. Ils restent toujours aussi inventifs d'autant que leur terrain de jeu s'accroit grâce à l'introduction des nouvelles technologies dans de plus en plus de domaine entre autre avec les objets connectés. En parallèle, le cyber-terrorisme s'il n'est pas encore avéré au sens d'attaque visant à des détruire des entreprises ou des infrastructures critiques se sert du net pour tisser sa toile en recrutant des futurs terroristes, en menant des actions de communication, voir en servant de support pour monter des opération sur le terrain… cette année riche en actions malveillantes laisse augurer du pire pour 2016…

Après l'introduction par Lazaro Pejsachowicz, le président du CLUSIF qui a présenté les différentes activités de l'association, le panorama a débuté. En introduction il a rappelé que le cyber-crime se porte très bien. En outre, il a annoncé qu'en juin prochain aura lieu la conférence sur les résultats de l'enquête MIPS pour Menaces Informatiques et Pratiques de Sécurité.


Fabien Cozic

Quelques astuces utilisés en 2015

Fabien Cozic, directeur d'enquêtes privées Read Team Investigation, a passé en revue quelques astuces utilisées par les pirates a commencé par la Yes Card qui a exercé ses activités en France et en Belgique. Le pirate était un ingénieur qui avait rajouté une petite puce de la carte bancaire qui permettait de valider les transactions en se substituant à la puce déjà installée.
Un groupe de pirate avait mis en place un système astucieux de déposé et de retrait des sommes. Puis une équipe en République Tchèque puis un second groupe effectuait des transactions aux Etats-Unis puis les annulait et récupérait ainsi de l'argent. Le préjudice se chiffrerait autour de 6 millions d'euros.
XCode Ghost qui a détourné le système de contrôle des applications d'Apple. Les pirates ont utilisé une faille humaine de ce système pour déposer des malwares afin de récupérer des informations
Le malwares Turla a utilisé des APT pour réaliser des écoutes en se servant des liaisons des satellites de communication.
Un malware a été conçu pour prendre le contrôle de la lunette de visé d'un fusil afin de déclencher le tir…
Pour conclure il a cité le détournement d'un jouet en utilisant le système de communication pour ouvrir les portes de garages. Ce malware a contribué à plusieurs cambriolages aux Etats-Unis.


Hervé Schauer

Le 0 Days un business juteux pour les entreprises

Loic Samain du CEIS représenté par Hervé Schauer a présenté l'évolution du business des 0 Days. La palme de l'année revient à un 0 Day sur IOS qui a été récompensé par 1 millions de $. Les systèmes de plateforme de 0 Day existent et se développent. Leurs clients sont tout d'abord les gouvernements qui veulent réaliser des écoutes, mener des attaques… Il a donné quelques exemples de prix comme par exemple 2000$ pour un 0 Day ciblant un site de ecommerce, pour Windows le prix est de 150000$… et pour IOS a atteint 1 million de $.
Le 20 mai 2015 la proposition Wassenaar sur les 0 Day a été publié et elle est déjà adopté par plusieurs pays. Une nouvelle proposition pour amender cette proposition devrait être faite en 2016. Aujourd'hui les primes aux 0 Days explosent avec des prix allant de 2000$ à plusieurs milliers de $. Ainsi, les entreprises de Bug Bounty voient leur valorisation exploser.
Ainsi, Vupen est devenu un grossiste en 0 Day et s'appelle aujourd'hui Zerodium. En janvier 2016 une faille de sécurité a été payée 100 000$ par cette entreprise pour la découverte d'une faille sur flash. Pour Hervé Schauer « 2015 est donc l'année de la professionnalisation de ce marché. »


Loïc Guezo

La cyber-diplomatie commence à émerger

Loïc Guezo, Strategist chez Trend Micro, a expliqué que l'on va vers une cyber-diplomatie avec entre autre la remise en cause de l'ICANN qui est au centre de très grandes manœuvres. On a de nombreux pays qui reconnaissent une capacité offensive sur Internet a commencé par les États-Unis, la Grande Bretagne, la Chine, la Russie et maintenant la France. En 2015, il a rappelé le cas du piratage OPM qui est une sorte de RH des agents des services spéciaux américains avec la récupération très personnel sur l'ensemble des collaborateurs. La Chine a été suspectée d'être l'auteur de ce piratage. Suite à cette accusation plusieurs arrestations ont eu lieu en Chine afin de faire diminuer les tensions entre ces deux pays. Aujourd'hui, le doute persiste sur la nature des personnes arrêtées. Le 31 décembre 2015 les autorités américaines ont ressortie une attaque sur 2009 ciblant Microsoft. Par contre Microsoft n'a pas alerté ces clients. Par ailleurs, la Russie a signé un pacte de non-agression avec la Chine mais ne signifie pas l'arrêt des opérations entre ces deux pays, il y a par contre une convergence de doctrine sur l'Internet autour de l'idée de souveraineté.
Quant à l'Iran et dans une moindre mesure à la Corée du Nord, ils ont été pointés par les Etat-Unis comme deux dangereux pays sources de piratages.
Par ailleurs, il a cité l'Accord Umbrella qui a été noté comme une grande avance en particulier Ui permet de facilité les procédures d'extradition. En France, il faut noter la publication de la Nouvelle Stratégie de la sécurité du numérique. A cette occasion, David Martinon a été nommé Ambassadeur pour la cyber-diplomatie et de l'économie digitale.
La cyber-diplomatie est devenue un élément clé de la vie politique dont l'influence géopolitique prévue dans cette nouvelle stratégie.

François Paget

Le Djiad Numérique : recrutement, endoctrinement…

François Paget a présenté pour sa part le Djiad Numérique. Lors du panorama 2004, il avait été évoqué l'utilisation d'Internet par les terroristes. Aujourd'hui, ils utilisent les réseaux sociaux et adressent plusieurs milliers de Tweet par jour. Daesh offre des conseils pour se dissimuler via par exemple les réseaux Tor, mais aussi Telegram. Ce dernier réseau social est dominant en Russie. Il permet de communiquer de façon chiffrée mais aussi de détruire les messages une fois lus. Les djihadistes se servent aussi du darknet, peut-être de Bitcoins… pour acheter des armes. Sans compter que les réseaux sociaux sont utilisés pour recruter des membres mais ce n'est pas le seul vecteur d'enrolement.
En novembre, les Anonymous se sont réveillés pour attaquer les djihadistes avec des actions parfois intéressantes, mais ils aussi ont réalisé des bévues qui ont parfois ralenties les actions des forces de police, voire aussi en attaquant des sites qui étaient en arabes mais sans aucun lien avec les terroristes.
En janvier dernier, il y a eu des défacements de sites surtout en janvier en particulier par Isis. Par contre, il y en a eu très peu après les attentats de novembre. Durant ces moments tragiques, Google a été particulièrement sollicité. Par contre, les réseaux sociaux ont servi à des élans de solidarité surtout en novembre. En revanche, Facebook a mis parfois beaucoup de temps pour fermer des sites malveillants. Quant à tweeter il a agi un peu plus rapidement, mais a laissé courir de nombreuses rumeurs. En ces périodes, il y eu de nombreuses fausses rumeurs qui ont circulé avec même des chevaux de Troie dissimulés dans certaines images.


Amélie Paget

Vers une limitation des libertés ?

Amélie Paget, consultante juridique SI HCS by Deloitte a fait le point sur les deux nouvelles lois publié en 2015 pour renforcer les pouvoir de l'Etat : la loi sur le renseignement et l'Etat d'urgence. Pour ce qui concerne l'état d'urgence il a été prorogé jusqu'au 26 février 2016. Désormais, lors des perquisitions, les agents peuvent accéder aux données stockées sur les systèmes Informatiques ou l'équipement terminal ou accessible à partir du système initial. En outre, ils auront la possibilité de copier les donner et d'effectuer des saisies en cas d'infraction. Par ailleurs un projet de loi souhaite insérer à notre Constitution, un nouvel article consacré à l'état d'urgence.
En ce qui concerne la Loi sur le renseignement, elle donne des prérogatives pour accéder aux données de connexion en les demandant aux opérateurs, aux FAI et hébergeurs.. Les agents peuvent utiliser des outils de géolocalisation et demander en temps réel aux FAI des information et documents qui transite sur le réseau. Bien sûr toutes ces actions ne peuvent s'effectuer que pour protéger les intérêts fondamentaux de la Nation, notamment pour la prévention du terrorisme. Les agents peuvent collecter des informations en échangeant sur la toile. Quant au chiffrement les opérateurs auront 72 heures pour offrir un système de déchiffrement ou directement les documents en clair.


Gérôme Billois

Objets connectés : la sécurité doit être intégré by design

Gérôme Billois, Manager Sécurité de Solucom a traité des attaques sur les objets connectés en rappelant qu'en juillet dernier deux chercheurs ont pris le contrôle à distance d'une voiture connectée. En fait, les consoles de bords sont connectées à un premier Réseau dit de confort et un second pour la conduite comme celui qui gère le régulateur de vitesse, la boite de vitesse, le volant… En fait, la console de bord est assez facile à pirater et permet de prendre le contrôle de la console de confort. Par contre, la console de sécurité est plus difficile à pirater. Par contre, avec du temps et un peu de chance selon les dires de ces deux chercheurs, la prise de contrôle sur la console de sécurité est faisable. Cette démonstration a eu des impacts médiatiques mais aussi financiers pour les constructeurs avec l'envoi de clés USB aux utilisateurs pour faire des mises à jours, heureusement à ce jour, toujours pas d'attaque sur les voitures… Toutefois il est possible d'envisager la diffusion de ramsowares qui bloqueraient les voitures…
Au delà des voitures, les jouets connectés ont fait l'objet d'attaques plus ou moins amusants avec par exemple Barbie, les téléviseurs… Par contre, d'autres attaques seraient plus graves comme celle sur des pompes à insuline, des fusils, voir des avions…
En fait, en matière de sécurité des objets connectés il y a 4 dimensions à prendre compte : ceux qui les conçoivent, ceux qui les achètent, ceux qui les conseillent et tous ceux qui vont les accueillir en particulier dans les entreprises. Il faut donc réagir en intégrant la sécurité, en protégeant notre vie privée, sans oublier les spécificités de ces objets. Demain, nous allons voir arriver les objets autonomes qui vont demain faire partie de notre quotidien avec par exemple des robots qui vont être mis dans les boutiques Nespresso, à bord des bateaux de Costa Croisières… Cela pose, de nombreuses questions juridiques.


Garance Mathias

Objets connectés : les premiers procès à l'horizon 2016

Garance Mathias en préambule de son intervention explique que nous sommes tous concernés par les objets connectés car nous en avons tous. Le droit à déjà prévu le fait que l'on est responsable de nos objets. Un grand classique du droit est qu'il s'impose à tous les acteurs : le concepteur, l'utilisateur… Par exemple, le Cloud qui relie les objets connectés n'est qu'une externalisation avec toutes les contraintes liées.
Concernant les objets connectés, il faut aussi prendre en compte les analyses d'impacts d'où la nécessité pour les fabricants d'embarquer la sécurité y design. Elle a pris l'exemple de Vtech qui avait fait l'objet d'une plainte par « UFC Que Choisir » du fait de la non-prise en compte de la protection de la vie privée.


Le Colonel Éric Freyssinet

Téléphonie mobile : le protocole SS7 mis à mal…

Le Colonel Éric Freyssinet a évoqué en premier lieu la sécurité des téléphones mobiles. Fin 2014, une conférence lors du CCC a mis en lumière une vulnérabilité dans le protocole SS7 qui permettait de rediriger des communications et d'intercepter des SMS (chiffrés). En ce qui concerne les logiciels malveillants, il y a eu peu de nouveautés. Toutefois, parmi les nouveautés on trouve Pornbroid qui bloque le téléphone sous Android qui est un logiciel assez avancés capable de se relancer une fois désinstallé. Il a aussi cité Xcode qui exploite une vulnérabilité sur IOS.
… et des attaques aux effets collatéraux redoutables
Puis, le Colonel Eric Freyssinet a présenté les conséquences d'une attaque. Il a pris l'exemple de Target dont l'attaque a coûté environ 67 millions de $ avec Visa, la même somme avec MasterCard au final cette attaque devrait coûter environ 100 Millions de $ dont 90 sont pris par son assurance.
L'attaque contre OPM qui ciblait les personnels de l'état américain par la Chine a obligé la CIA a retiré des agents basés en Chine, sans compter la notification à plusieurs millions de personnes.
Hello Kity a aussi été visé par une attaque ciblée pour récupérées données Bancaires des parents.
TV 5 Monde a été une des premières véritables attaques pour détruire une entreprise. Au final l'impact sur le SI a été faible par contre les ventes de publicité se sont effondrées et son budget sécurité a été augmenté de façon conséquente. Son PDG a témoigné dans plusieurs conférences ce qui a un effet plutôt positif.
Ashley Madison est une affaire assez complexe. On a noté quelques retombées tragique comme le suicide d'un pasteur, des démissions, des chantages… De ce fait, la CNIL a demandé aux sites de rencontre français de renforcer leur sécurité.
Pour finir, il a recommandé de prévenir les risques, être capable de décréter la survenance d'un incident et être en mesure de maitriser leur impact.
François Paget a pour sa part rappelé que les forces de police rencontrent quelques succès en arrêtant des cybercriminels partout dans le monde.

Jean-Yves Latournerie

Nous passons à lutte anti-terroriste 2.0

La conclusion a été assurée par le cyber-préfet Jean-Yves Latournerie qui a félicité les intervenants et les organisateurs de ce panorama. Selon lui, il n'y a pas à ce jour d'actions en cyber-terrorisme à proprement parler. Par contre, le cyber joue un rôle très important dans la radicalisation, le recrutement et le passage à l'acte. Dans ces périodes tragiques, on apprend vite et on est en train de passer dans la lutte antiterroriste 2.0. Dans ce cadre le panorama du CLUSIF est important afin de mieux comprendre la nature de la menace de façon systémique et analytique et pouvoir ainsi anticiper les développements des actions terroristes. Il s'est félicité de voir le travail entre les forces de police et les entreprises privées se renforcer en particulier avec les principaux acteurs d l'Internet. Il note de réel progrès opérationnel entre janvier et novembre dernier. En effet, un travail méthodologique a été effectué entre ces deux périodes qui porte ces fruits aujourd'hui.
Il a conclu son intervention en rappelant que même s'il a quelques arrestations, le crime pour le moment sort le plus souvent des confrontations avec les forces de polices, toutefois, il semble que tous les acteurs d'Internet sont de plus en plus sensibiliser à ces attaques ce qui donne des espoirs pour améliorer cette situation.

Réagissez à cet article

Source : *Panorama 2015 de la Cybercriminalité du CLUSIF : Attaques sur tous les fronts ! – Global Security Mag Online*

Astuces pour une meilleure gestion de l’e-réputation – Annuaire +1 Annuaire +1

Astuces pour une meilleure gestion de l’e-réputation – Annuaire +1 Annuaire +1

L’e-réputation ne concerne plus les entreprises et les organisations de marque. Tout le monde peut disposer d’une image sur internet. En effet, avec ou sans permission, des sujets peuvent parler d’une personne notamment via des discussions, des images ou des vidéos. Or, dans ces discours et mauvaises appréhensions ne restent pas dans le monde virtuel. En fait, cela peut impacter la vie quotidienne, détruire des relations et même des carrières professionnelles. Heureusement que ce n’est pas une fatalité. L’e-réputation peut être géré et même utilisé à bon escient. Comment faire ?

Ajouter de l’importance à son image
Quels que soient les documents ou fichiers qu’il faut mettre en ligne, il faut les prendre en conscience. CV, photos ou des commentaires faits sur les plateformes sociales, ils contribuent tous à l’e-réputation d’une personne. Bien que quelque peut inévitable, ces contenus sont les vitrines d’une personne, alors autant qu’elle lui ressemble. La meilleure façon est de ne jamais négliger son e-réputation. Tout ce qui est sur internet reste sur internet ! Telle est la règle.

Avoir un bon aspect de l’état des lieux
Le mieux est d’évaluer son e-réputation le plus tôt possible. C’est très simple, il n’y a pas besoin de faire appel à une agence e-réputation pour avoir une idée de son e-réputation. Pour ce faire, il suffit de taper une requête sur la barre de recherche des moteurs de recherche. De porter une analyse sur au moins les deux premières pages (au lieu de rester sur la première). La suite consiste à vérifier s’ils coïncident avec l’image voulue, s’ils peuvent être lus publiquement…

Penser à son avenir
Les réseaux sociaux constituent en fait une bonne alternative pour constituer un réseau professionnel. Il y a également les sites dédiés avec qui, il faut prendre à l’avance des précautions. En fait, pour une candidature donnée les recruteurs ne s’arrêtent pas sur leur site. Ils peuvent étendre (et c’est bien compréhensible) leur recherche sur les autres plateformes sociales et même sur la totalité des moteurs de recherche.
De même pour les amis Facebook par exemple, ce sont les personnes les plus susceptibles de devenir un danger pour un internaute. La situation n’est pas toujours délibérément provoquée, par contre une identification sur une photo relatant une soirée vertigineuse entre élève et prof employer et employeur ne fait pas bon ménage. Pour éviter cette situation, il est indispensable de bien maitriser les paramètres (ce que peu de gens font également).
Après les constatations, les actions ! Quelle que soit la plateforme, il faut toujours vérifier les paramètres. Entreprendre des petites actions peut permettre à aider des problèmes plus graves. Comme le classement des amis par rapport au lien et relation partagée. Par exemple pour Facebook, cliquer sur rubrique confidentialité et choisir option « examiner les publications dans lesquelles vos amis vous identifient avant qu’elles n’apparaissent sur votre journal ».

Apparaitre ou ne pas apparaitre ?
Telle est la question ! En premier lieu, demander le droit de ne faire aucune publication sur internet ! C’est toujours possible à faire, mais il faut prendre en compte les autres internautes qui peuvent toujours influer l’e-réputation. L’inconvénient réside alors dans le fait qu’il n’y aura que du mauvais contenu à l’encontre de la personne en question. Un autre inconvénient est que les recruteurs n’aiment pas trop les candidats qui sont trop discrets sur le web.
Du coup, autant prendre le mal par les cornes ! Avoir le pouvoir de supprimer les contenus indésirables en contactant Google ou en faisant appel à une agence e-réputation.

Réagissez à cet article

Source : *Astuces pour une meilleure gestion de l’e-réputation – Annuaire +1 Annuaire +1*

La Cour de cassation confirme la sanction de 10.000 €

contre un employeur qui utilisait abusivement la vidéosurveillance sur le lieu de travail des salariés !

	**La Cour de cassation confirme la sanction de 10.000 € contre un employeur qui utilisait abusivement la vidéosurveillance sur le lieu de travail des salariés !**

La commission restreinte de la Commission nationale de l'informatique et des libertés avait relevé que la société avait manqué à l'obligation de proportionnalité en plaçant et maintenant sous surveillance l'un au moins de ses salariés bien au-delà du délai de mise en conformité fixé par la mise en demeure.

L'arrêt N°371196 du Conseil d'État du 18 novembre 2015 a confirmé la sanction pécuniaire prise par la CNIL – Commission Nationale Informatique et Liberté – d'un montant de 10.000 € avec la publication de la décision sur le site internet de la CNIL et sur le site Légifrance, à l'encontre d'une entreprise qui avait installé un système de vidéosurveillance intrusif sur le lieu de travail des salariés.

Dans ce litige, la Cour de cassation a considéré que les données à caractère personnel collectées par un responsable de traitement doivent être " *adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées ainsi et de leurs traitements ultérieurs* ". De plus, aux termes de l'article L1121-1 du Code du travail : " *Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché* ".

La surveillance des salariés par l'employeur

L'employeur a le droit de contrôler et de surveiller l'activité de ses salariés pendant le temps de travail.

Toutefois, l'article L1222-4 du Code du Travail indique qu'aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance.

De plus, l'article L2323-32 du même Code précise que le comité d'entreprise est informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés.

L'arrêt N°10-23482 de la Cour de Cassation du 10 janvier 2012 a indiqué qu'un employeur qui utilise la vidéosurveillance pour contrôler ses salariés doit les prévenir préalablement.

Ainsi, un employeur n'est pas autorisé à utiliser, comme mode de preuve licite, les enregistrements d'un système de vidéo-surveillance installé pour permettre le contrôle de leur activité et de leurs horaires d'arrivée et de départ, si les salariés et le comité d'entreprise n'ont pas été préalablement informés.

Le respect à la vie privée des salariés au travail

La délibération 2012-475 du 3 janvier 2013 de la CNIL avait déjà indiqué sa position sur la vidéosurveillance des salariés d'une entreprise en interdisant de surveiller en permanence des salariés sur leurs lieux de travail sauf circonstances particulières.

La CNIL, conformément à l'article L1121-1 du Code du Travail, précise que : " *Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché* ".

Ainsi, il est interdit de filmer les salariés en continu sur les lieux de travail sauf circonstances particulières, par exemple en cas de personnes exposées à un risque d'une particulière gravité.

Toutefois, la sanction pécuniaire prise par la CNIL – Commission Nationale Informatique et Liberté – d'un montant de 10.000 € avec la publication de la décision sur le site internet de la CNIL et sur le site Légifrance, est justifiée à l'encontre d'une entreprise qui avait installé un système de vidéosurveillance intrusif sur le lieu de travail des salariés.

Réagissez à cet article

Source : *CNIL : La Cour de cassation confirme la sanction de*

10.000 € contre un employeur qui utilisait abusivement la vidéosurveillance sur le lieu de travail des salariés ! | Infos Droits