Ne donnez jamais une donnée personnelle de santé à un assureur

Ne donnez jamais une donnée personnelle de santé à un assureur

Quand il s'agit de données personnelles de santé, les Français ne doivent rien communiquer aux assureurs, aux banquiers ou aux employeurs. C'est le conseil de Philippe Douste Blazy, ancien ministre de la santé, et désormais créateur de la startup Honestica.

Les laboratoires pharmaceutiques à voir

Il a pris la parole lors de l'événement Keynote 2016 organisé par Maddyness le 20 janvier à Paris. "Il ne faut jamais donner de données personnelles aux assureurs, aux employeurs, aux banquiers," dit-il, "les laboratoires pharmaceutiques, il faut voir," ajoute-t-il.

Il parle alors de données personnelles. Il est plus ouvert pour l'usage de données de santé anonymisées. L'ancien ministre est revenu sur son expérience du dossier médical personnel. "Le DMP est le plus grand échec de ma vie quand j"étais ministre de la santé en 2004" déclare-t-il. Il croyait pourtant en ses vertus qu'il s'agisse d'accélérer les diagnostics, de détecter les risques liés à certains médicaments ou de réduire les coûts médicaux.

"En France, on dépense 30 milliards d'euros par an en examens redondants," pointe-t-il. "Vous vous blessez, on va vous faire faire une radio, et si vous devez aller à l'hôpital, on va refaire cette radio, on ne tient pas compte de la radio que vous avez faite dans le privé," illustre-t-il.

Mediator et sclérose en plaques

"Avec le DMP, on aurait vu en quelques mois et pas en années, que le Mediator créait des effets indésirables," souligne-t-il. "De plus, on avait dit que la vaccination contre l'hépatite B créait des risques de sclérose en plaques, on aurait vu que c'est faux grâce au DMP," martèle-t-il.

Depuis, il pense faire renaître ce dossier au sein de sa startup Honestica, où il est associé à Frank Le Ouay, l'un des cofondateurs de Criteo. "La création d'un dossier médical personnel a échoué chez les Américains parce qu'ils partent du patient, il faut partir du médecin, c'est lui qui dans le cadre de la relation de confiance avec le patient va pousser cette solution. Mais il faut lui vendre ce dossier médical comme un moyen de gagner du temps, une heure par jour, et pas comme de la paperasse supplémentaire," recommande-t-il.

Expérimentation en mars

Sa société va débuter l'expérimentation en mars prochain de sa solution auprès d'un hôpital toulousain. "Les comptes rendus de sortie de l'hôpital sont encore envoyés par la Poste," dit-il, "nous proposons de les gérer électroniquement." Et il mise sur les médecins hospitaliers pour faire le succès de ce dossier médical électronique.

Réagissez à cet article

Source : *Philippe Douste-Blazy : "ne donnez jamais une donnée personnelle de santé à un assureur" | La Revue du Digital*

Connaissez-vous les fichiers Prefetch ?

Que sont les fichiers Prefetch ?

Dans le cadre de ses analyses, le CERT-FR est régulièrement amené à analyser les fichiers Prefetch, si ceux-ci sont disponibles, afin de déterminer la date d'exécution d'un programme.

Un mot sur les fichiers Prefetch

Dans le cadre de ses analyses, le CERT-FR est régulièrement amené à analyser les fichiers Prefetch, si ceux-ci sont disponibles, afin de déterminer la date d'exécution d'un programme sur le système et éventuellement l'emplacement depuis lequel il a été exécuté.
Pour rappel, les fichiers Prefetch *.pf, introduits sous Windows XP et localisés dans %SystemRoot%Prefetch, sont utilisés par le système d'exploitation pour caractériser les applications exécutées par le système et l'utilisateur.
Cette fonctionnalité permet de déterminer les pages mémoires de code utilisées par un programme afin de les charger préalablement lors de l'exécution de ce dernier. L'objectif ainsi visé est d'éviter un maximum d'accès disque. Par défaut, le Prefetch est désactivé pour tous les programmes sur les environnements Windows Server.

Ce paramètre est stocké dans la valeur suivante :
HKLMSYSTEMCurrentControlSetControlSession ManagerMemory Management
PrefetchParametersEnablePrefetcher
Windows Vista et SuperFetch

Introduit avec le noyau de Vista, SuperFetch est un procédé de gestion de la mémoire, à l'image du Prefetcher introduit sous XP. SuperFetch vise à améliorer les performances générales du système via un mécanisme de prédiction d'utilisation des pages mémoire de code en fonction de scénarios temporels (exécution en semaine ou week-end, utilisation entre 6 heures et midi, midi et 18h, 18h et minuit).
Prefetch ne se base que sur l'activité récente du système pour charger préalablement des données. Si une application utilise intensivement la mémoire, l'historique d'utilisation des pages sera faussé. SuperFetch tente d'optimiser ce modèle de gestion mémoire par le composant de rééquilibrage (rebalancer), qui permet de prioriser à nouveau la liste des pages mémoire en fonction de leur historique d'utilisation et des scénarios temporels établis.
Les fichiers Ag*.db constituent une base d'informations sur l'historique d'utilisation des programmes et de leurs pages mémoire de code. Par abus de langage, ils sont nommés fichiers SuperFetch, bien que ce terme englobe le procédé de gestion mémoire optimisé dans son ensemble. A l'instar des fichiers Prefetch, ils se trouvent dans le dossier %SystemRoot%Prefetch.
Comme pour Prefetcher, le SuperFetch est désactivé par défaut pour tous les programmes sur les environnements Windows Server.

Le paramètre est contenu dans la valeur suivante :
HKLMSYSTEMCurrentControlSetControlSession ManagerMemory Management
PrefetchParametersEnableSuperfetch

Initialement, enablePrefetcher et enableSuperfetch étaient désactivée par défaut sur Windows 7 sur les systèmes équipés de disques SSD, afin d'améliorer la durée de vie des premiers modèles de disque. L'option enablePrefetcher a été réactivée par défaut à partir de Windows 8, mais ce n'est pas le cas pour SuperFetch.

Utilité des artefacts d'exécution de programme

Dans le cadre d'une investigation lors d'un incident de sécurité informatique, l'analyste sera intéressé de savoir si un programme a été exécuté (le nombre de fois, la date, la fréquence et l'emplacement). Cela peut mettre en avant un comportement malveillant si une application suspecte est utilisée, ou déterminer la légitimité d'une autre par une étude statistique.

Les fichiers Prefetch peuvent être décodés avec les outils suivants :
Pf de TzWorks (payant) ;
CrowdResponse de CrowdStrike (gratuit) ;
Windows file analyzer de Mitec (gratuit) ;
le greffon prefetch de RegRipper (libre et gratuit) ;
Prefetch-parser de Airbus DS (libre et gratuit).

Les fichiers SuperFetch peuvent être partiellement décodés avec les outils suivants :
CrowdResponse de CrowdStrike (gratuit) ;
Superfetch-dumper de Rewolf (libre et gratuit).

Documentation
http://cert.ssi.gouv.fr/site/CERTFR-2014-ACT-037
http://cert.ssi.gouv.fr/site/CERTFR-2015-ACT-044
https://technet.microsoft.com/en-us/magazine/2007.03.vistakernel.aspx
https://www.crowdstrike.com/blog/crowdresponse-application-execution-modules-released
M. Russinovitch, D. Solomon, A. Ionescu. Windows Internals vol.2. Microsoft Press. p.338
https://github.com/libyal/libagdb/blob/master/documentation/Windows SuperFetch (DB) format.asciidoc

---

Réagissez à cet article

Source : *Bulletin d’actualité CERTFR-2015-ACT-051*

Un phishing et Lastpass s’en est allé

Un phishing et Lastpass s’en est allé

Lors de la conférence Shmoocon, un chercheur a présenté une attaque de phishing particulièrement convaincante visant les services du gestionnaire de mot de passe Lastpass. En réaction, les mesures de sécurité ont été rehaussées par l'éditeur du service.

Le phishing n'est pas toujours un problème situé entre le clavier et la chaise. C'est en tout cas la thèse défendue par le chercheur Sean Cassidy, qui a présenté ce week-end lors de la conférence Shmoocon une attaque de cette catégorie particulièrement convaincante et capable de tromper les utilisateurs les plus aguerris du gestionnaire de mot de passe Lastpass.

L'attaque, baptisée « Lostpass » exploite plusieurs vulnérabilités présentes sur le service de gestion des mots de passe : il s'agit tout d'abord pour l'attaquant d'attirer l'utilisateur sur un site malicieux, puis d'afficher une notification indiquant à l'utilisateur que celui-ci a été déconnecté de Lastpass. Une fois celle-ci affichée, l'utilisateur est ensuite redirigé vers une page de login quasi identique à celle affichée par Lastpass en cas de déconnexion. L'attaquant peut exploiter un bug notamment présent dans Chromium afin de disposer d'un nom de domaine quasi similaire à celui utilisé pour les extensions chrome du même type que celles utilisées par Lastpass.

L'attaquant peut ensuite exploiter l'API ouverte de Lastpass pour vérifier si les identifiants entrés par l'utilisateur sont valides et pour savoir si celui-ci a activé un système d'identification à double facteur : si tel est le cas, l'attaquant peut également présenter une invite copiée sur celle proposée par le service de gestion de mot de passe et qui lui permet de récupérer par la même occasion le token généré par la double authentification. Une fois les identifiants récupérés, l'attaquant peut accéder au reste des mots de passe stockés par l'utilisateur, ou modifier les paramètres de sécurité du compte afin de faciliter d'éventuelles futures attaques.

Un problème entre la chaise et le clavier ?

Les équipes de Lastpass ont été mises au courant de ce scénario d'attaque au cours de l'été 2015 et ont depuis mis en place plusieurs mesures afin de protéger les utilisateurs. La société a ainsi mis en place un système de vérification par mail lorsque l'utilisateur se connecte depuis un appareil inconnu, ce qui permet selon Lastpass de réduire considérablement les attaques de ce type.

La société précise également revoir le fonctionnement de son extension :
celle-ci s'appuie en effet sur des notifications Viewport pour informer ses utilisateurs, une technique facile à imiter pour un attaquant qui souhaiterait tromper un utilisateur. Un comportement que Lastpass entend corriger afin de réduire un peu plus le risque de confusion entre véritables notifications et notifications malicieuses émanant du site visité.
Pour Sean Cassidy, le problème souligné par ce scénario est tout aussi critique qu'une vulnérabilité classique, mais celui-ci regrette que les attaques de type phishing soient trop souvent reléguées au simple rang des problèmes liés à l'utilisateur. Dans sa démonstration en effet, la différence entre les pages légitimes et les pages malicieuses utilisées par un attaquant est minime. Seule une infime différence de trois caractères dans une url et quelques différences typographiques séparent ici le vrai du faux, ce qui rend l'attaque bien plus inquiétante.

Réagissez à cet article

Source : *Lastpass : un phishing presque parfait*

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.

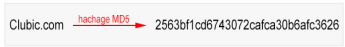
Le premier, qui consiste à tester tous les mots de passe possibles et imaginables dans une interface de connexion sur la base d'un identifiant connu, n'est plus possible aujourd'hui ou très rarement. Cela, parce que la grande majorité des sites sérieux bloquent les comptes au bout de quelques tentatives 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

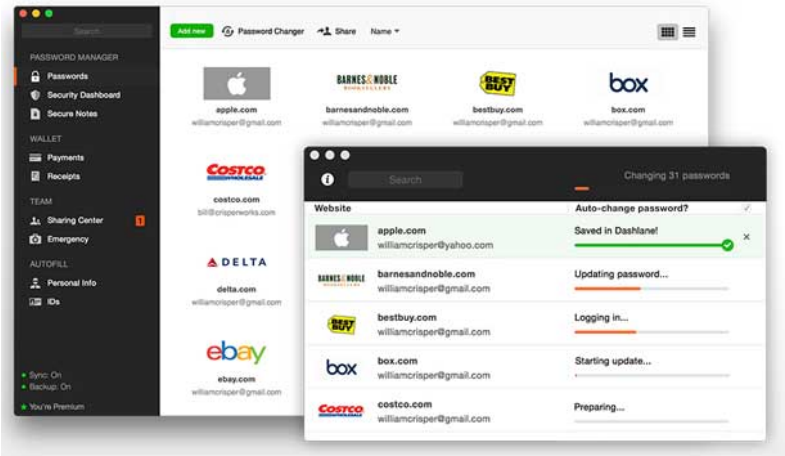
Source : *Une vulnérabilité zero-day affecte des millions de systèmes Linux et Android – Le Monde Informatique*

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

Les principales tendances en 2016 du Big data

Les principales tendances en 2016 du Big data

La nouvelle année verra le Big Data prendre de l'ampleur et de la vitesse. L'évolution des usages des données va progresser. Les entreprises ne pourront pas ignorer la généralisation des analyses en libre-service et l'adoption à grand échelle du cloud et de Hadoop, ainsi que les nouvelles technologies venant compléter ce framework, entraînant de nombreux changements.

1. Montée en puissance du NoSQL

Dans nos prévisions des tendances du Big Data de l'année dernière, nous avions noté une accentuation de l'adoption des technologies NoSQL, qui sont généralement associées aux données non structurées. Dorénavant, les bases de données NoSQL commenceront à occuper une place centrale dans le paysage IT des entreprises, tandis que les avantages des bases de données sans schéma seront de plus en plus notables. Pour s'en convaincre, il suffit de consulter le Magic Quadrant de Gartner consacré aux systèmes de gestion de bases de données opérationnelles. Par le passé, Oracle, IBM, Microsoft et SAP dominaient le classement. Aujourd'hui, ce Magic Quadrant fait la part belle aux prestataires de solutions NoSQL, comme MongoDB, DataStax, Redis Labs, MarkLogic et Amazon Web Services (avec DynamoDB), qui viennent supplanter les fournisseurs traditionnels dans la catégorie des leaders.

2. Apache Spark révolutionne le Big Data

De simple composant de l'écosystème Hadoop, Apache Spark est devenu une référence en matière de plate-forme Big Data pour de nombreuses entreprises. Spark offre une rapidité de traitement bien supérieure à Hadoop et constitue désormais le plus important projet Big Data open source, selon son créateur Matei Zaharia, également cofondateur de Databricks. Les exemples convaincants de mises en œuvre de Spark en milieu professionnel sont de plus en plus nombreux, à l'instar de Goldman Sachs qui en a fait sa solution de choix pour ses analyses du Big Data.

3. Les projets Hadoop arrivent à maturité et les entreprises passent à l'environnement de production

Selon une enquête récente menée auprès de 2 200 clients Hadoop, seuls 3 % d'entre eux envisagent de moins s'appuyer sur ce framework au cours des 12 prochains mois. 76 % des sondés prévoient de recourir davantage à Hadoop au cours des 3 prochains mois, et enfin près de 50 % des entreprises qui n'ont pas déployé Hadoop déclarent avoir l'intention de le faire dans les 12 prochains mois. Cette enquête révèle également que Tableau est le principal outil d'aide à la décision pour les entreprises utilisant Hadoop ou prévoyant de l'utiliser, ainsi que pour celles qui ont déjà parfaitement intégré ce framework à leurs projets.

4. Le Big Data prend de l'ampleur : Hadoop s'ajoute aux normes de l'entreprise

Hadoop occupe une place de plus en plus importante dans le paysage de l'IT. L'augmentation des investissements dans les éléments gravitant autour des systèmes professionnels, comme la sécurité, viendra corroborer cette tendance. Apache Sentry procure un système granulaire et basé sur des rôles pour gérer les autorisations d'accès aux données et métadonnées stockées sur un cluster Hadoop. Il s'agit là d'exemples de ce que les clients attendent de leur plate-forme de gestion de bases de données relationnelles. Ces fonctionnalités se retrouvent désormais à l'avant-garde des nouvelles technologies en matière de Big Data, ce qui simplifie d'autant plus l'adoption de telles solutions en entreprise.

5. Le Big Data prend de la vitesse : Hadoop aussi

À mesure que Hadoop gagne en importance dans les entreprises, les utilisateurs attendent de plus en plus des fonctions d'exploration de données aussi rapides que celles proposées par les entrepôts de données traditionnels. En réponse à cette demande grandissante, nous assistons à une adoption croissante de technologies telles que Cloudera Impala, AtScale, Actian Vector et Jethro Data, qui favorisent la compatibilité de Hadoop avec les cubes OLAP et simplifient d'autant plus le rapprochement entre solutions traditionnelles d'aide à la décision et Big Data.

6. Le nombre croissant d'outils de préparation des données favorise la découverte d'informations

Les outils de préparation de données en libre-service gagnent en popularité. Cette explosion est due en partie à l'adoption d'outils de découverte de données générées par les utilisateurs métiers, tels que Tableau, qui permettent d'accélérer les analyses. Désormais, ces utilisateurs souhaitent également réduire le temps nécessaire à la préparation des données et la complexité d'une telle opération, ce qui revêt une importance toute particulière pour le Big Data qui implique une multiplicité de types et de formats de données. Nous avons pu assister à de nombreuses innovations en matière de préparation de données pour le Big Data de la part de prestataires comme Alteryx, Trifacta, Paxata ou Lavastorm. Les leaders traditionnels en matière de solutions ETL, comme Informatica, qui développe Rev, ne sont pas en reste et réalisent d'importants investissements en la matière.

7. Les entrepôts de données à traitement MPP se tournent vers le cloud

Même si la croissance du segment des entrepôts de données ralentit, ces solutions ne sont pas pour autant en passe de disparaître. Cette technologie opère actuellement sa transition vers le cloud, avec en tête Amazon Redshift, un entrepôt de données à la demande dans le cloud. Redshift est le service AWS qui a connu la croissance la plus rapide, mais il doit désormais faire face à la concurrence de Google et sa solution BigQuery, d'autres acteurs bien établis sur le marché comme Microsoft (avec Azure SQL Data Warehouse) ou Teradata, ou encore de nouveaux prestataires tels que Snowflake, lauréat du Strata + Hadoop World 2015 Startup Showcase, qui connaissent un succès grandissant dans le secteur. Les analystes estiment que 90 % des entreprises qui ont adopté Hadoop conserveront également leurs entrepôts de données. De plus, grâce aux nouvelles offres cloud, ces entreprises peuvent augmenter ou diminuer la capacité de stockage et la puissance de calcul de leurs entrepôts en fonction du volume d'informations stockées dans leur lac de données Hadoop.

8. Convergence de l'IoT, du cloud et du Big Data

Même si l'IoT n'en est encore qu'à ses balbutiements, les pétaoctets de données générées par les différents objets connectés vont favoriser l'explosion des solutions cloud. Dans cette optique, les leaders en la matière, comme Google, Amazon Web Services et Microsoft proposent désormais des services d'IoT pour transférer en toute transparence ces données vers leurs moteurs analytiques dans le cloud.

Si ces tendances et ces évolutions peuvent sembler disparates, elles sont toutes liées par une même nécessité : exploiter les données rapidement et confortablement. Alors que le Big Data continue d'évoluer et que de nouvelles manières d'exploiter ces données voient le jour, une seule chose ne change pas : l'analyse de données est désormais à la portée de tous, et nous avons hâte de nous y mettre.

Réagissez à cet article

Source : *Big data : les principales tendances de 2016*