La sécurité selon Yahoo : chiffrement et mot de passe jetable | Le Net Expert Informatique

Yahoo a soumis sur GitHub le code d'un plugin permettant de chiffrer de bout-en-bout les courriels envoyés depuis son service de messagerie. La firme veut aussi faire disparaître le mot de passe et implémente un système OTP, un mot de passe à usage unique.

Depuis les révélations autour d'Edward Snowden concernant l'espionnage américain, la sécurité et la confidentialité des communications préoccupent nettement plus les fournisseurs de services en ligne, dont Yahoo et Google.
La firme de Marissa Mayer a ainsi notamment choisi d'adopter le chiffrement des échanges. Et dans ce cadre, Yahoo travaille à une solution de chiffrement de bout-en-bout de la messagerie par l'intermédiaire d'un plugin.

Stamos répond à la NSA avec un plugin
Afin de s'assurer de la robustesse de cette technologie, le directeur de la sécurité de Yahoo, Alex Stamos, fait appel à l'expertise de la communauté. Le code du plugin a été publié sur GitHub et disponible pour être audité et les vulnérabilités identifiées.
Yahoo a collaboré avec Google pour que leurs systèmes de messagerie soient compatibles avec le plugin de chiffrement, qui devrait être finalisé d'ici la fin de l'année et est basé sur le standard OpenPGP.
A noter que Yahoo, comme d'autres services Web, planche également sur la sécurisation de la phase d'authentification. Comment ? En proposant des méthodes alternatives au mot de passe classique, dont la vulnérabilité est établie.
Ainsi, Yahoo a implémenté un système OTP ou One Time Password. Après avoir activé la fonction et communiqué un numéro de téléphone mobile Yahoo, l'utilisateur n'a plus à mémoriser son mot de passe habituel.
Lors de la connexion, l'internaute n'a qu'à cliquer sur le bouton déclenchant l'envoi du mot de passe. Celui-ci parvient sous la forme d'un SMS comportant un code de 4 caractères. Il ne reste plus qu'à le saisir pour se connecter.

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

Source :
http://www.zdnet.fr/actualites/la-securite-selon-yahoo-chiffrement-et-mot-de-passe-jetable-39816374.htm

---

Biométrie sur le lieu de

travail : quelles limites ? | Le Net Expert Informatique

Biométrie sur le lieu de travail : quelles limites ?

En Suède, la société Epicenter a récemment pris la décision d'implanter une puce électronique à ses salariés, afin de remplacer le badge d'accès aux locaux de l'entreprise et de faire fonctionner la photocopieuse. Qu'en est-il en France ?

1/ Qu'est-ce que la biométrie ?
La biométrie peut être définie comme la technique d'identification d'une personne à partir de ses caractéristiques physiques (empreintes digitales, iris de l'œil,…) ou biologiques (sang, ADN,…).
Pour la CNIL, « la biométrie regroupe l'ensemble des techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales. »
La CNIL ajoute que les données biométriques sont des données à caractère personnel en que qu'elles permettent d'identifier une personne, ayant la particularité d'être uniques et permanentes.
Ainsi, elles permettent le traçage des individus, agissant comme un « identificateur unique. »
Sur le plan professionnel, la biométrie peut être utilisée à plusieurs fins, et notamment pour autoriser l'accès aux locaux de l'entreprise, contrôler le temps de travail ou allumer l'ordinateur de travail.
Ce dispositif de contrôle est cependant soumis à de nombreuses conditions, compte tenu des contraintes qu'il fait peser sur les libertés individuelles.

2/ Dans quels cas peut-elle être admise ?
La CNIL a défini un cadre applicable à certains dispositifs biométriques, permettant à l'employeur de bénéficier d'une procédure simplifiée en adressant à la CNIL une simple déclaration de conformité.
Ces dispositifs sont au nombre de trois et visent ceux reposant sur la reconnaissance :
• du contour de la main pour assurer le contrôle d'accès au restaurant scolaire (autorisation n°AU-009) ;
• du contour de la main pour assurer le contrôle d'accès aux locaux et à la restauration sur les lieux de travail (autorisation n°AU-007) ;
• de l'empreinte digitale exclusivement enregistrée sur un support individuel détenu par la personne concernée pour contrôler l'accès aux locaux professionnels (autorisation n°AU-008).

Si le dispositif biométrique obéit à l'une de ces trois finalités, l'employeur peut présenter une déclaration simplifiée auprès de la CNIL.

NB. L'utilisation de dispositifs de reconnaissance biométrique, pour la gestion des contrôles d'accès aux locaux, des horaires et de la restauration ne peut pas faire l'objet de cette demande d'autorisation.

Le recours à la biométrie n'est donc possible que dans des hypothèses très limitées, et ne saurait justifier un contrôle des horaires de travail.
Si le dispositif n'est pas conforme à l'une de ces autorisations uniques, il est possible de solliciter une autorisation spécifique auprès de la CNIL.
Cette dernière examine au cas par cas les demandes qui lui sont adressées afin de déterminer si, au regard des éléments du dossier, le dispositif est proportionné ou non à la finalité (CNIL.fr).
Cette exigence de la CNIL rejoint les dispositions de l'article L. 1121-1 du Code du travail selon lesquelles « 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. »

3/ Dans quelles conditions ?
Lorsqu'il est justifié, le recours à la biométrie est soumis à de nombreuses conditions de consultation et d'information.

3.1/ Information / consultation du comité d'entreprise
L'information / consultation du comité d'entreprise est requise sur le fondement de trois articles spécifiques :
– Article L. 2323-13 du Code du travail : « le comité d'entreprise est informé et consulté, préalablement à tout projet important d'introduction de nouvelles technologies, lorsque celles-ci sont susceptibles d'avoir des conséquences sur l'emploi, la qualification, la rémunération, la formation ou les conditions de travail. »
– Article L. 2323-32, alinéa 3 du Code du travail : « Il est aussi informé, préalablement à leur introduction dans l'entreprise, sur les traitements automatisés de gestion du personnel et sur toute modification de ceux-ci. »
– Article L. 2323-32, alinéa 3 du Code du travail : « 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. »

La consultation du comité d'entreprise doit permettre à ce dernier de donner son avis sur la pertinence et la proportionnalité entre l'utilisation de la biométrie et la finalité recherchée.

3.2/ Information / consultation du CHSCT
Le CHSCT doit également être informé et consulté sur le recours à la biométrie, en application de l'article L. 4612-8 du Code du travail.
Ce texte dispose en effet que « le comité d'hygiène, de sécurité et des conditions de travail est consulté avant toute décision d'aménagement important modifiant les conditions de santé et de sécurité ou les conditions de travail… »
La Cour d'appel de Paris (CA Paris 5 décembre 2007, n° 07-11402) a retenu cette solution concernant l'enregistrement automatique des communications des salariés.
Il y a lieu de considérer que la mise en place de la biométrie impose à l'employeur la saisine préalable du CHSCT, compte tenu des termes très larges de l'article L. 4612-8 du Code du travail.

3.3/ Information des salariés
Enfin, chaque salarié doit être informé, conformément à l'article L. 1222-4 du Code du travail selon lequel « aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance. »
Bien que le texte ne l'exige pas expressément, il est fortement conseillé de procéder à une information individuelle de chaque salarié, afin d'éviter toute contestation.

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

Source : http://www.village-justice.com/articles/Biometrie-sur-lieu-travail-quelles,18886.html

---

Comment rendre l'information infalsifiable ? Avec les blockchains | Le Net Expert Informatique

Comment rendre l'information infalsifiable ? Avec les blockchains

On sait maintenant réaliser des supports inscriptibles, partagés et infalsifiables. Ce qu'il est possible d'en faire est étonnant, formidable… et révolutionnaire.

Imaginez qu'à la place de la Concorde à Paris, à côté de l'obélisque, on installe un très grand cahier que, librement et gratuitement, tout le monde puisse lire, sur lequel chacun puisse écrire, mais qui soit impossible à modifier et indestructible. Cela serait-il utile ? Il semble que oui.

On pourrait y consigner des engagements, comme : « Je promets de donner ma maison à celui qui prouvera la conjecture de Riemann ; signé Jacques Dupont, 11 rue Martin à Paris. » On pourrait y déposer la description de ses découvertes, afin qu'il soit impossible d'en être dépossédé. On pourrait y laisser des reconnaissances de dettes, considérées valides tant que le prêteur n'est pas venu indiquer sur le cahier qu'il a été remboursé.

On pourrait y déposer des messages adressés à des personnes qu'on a perdues de vue, en espérant qu'elles viennent les lire et reprennent contact. On pourrait y consigner des faits que l'on voudrait rendre publics définitivement, pour que l'histoire les connaisse, pour aider une personne dont on souhaite défendre la réputation, pour se venger, etc.

Pour que cela soit commode et pour empêcher les tricheurs de prendre des engagements en votre nom ou écrire en se faisant passer pour vous, il faudrait que l'on puisse signer les messages déposés de telle façon que personne ne puisse se substituer à vous. Il serait utile aussi que l'instant précis où est inscrit un texte soit indiqué à chaque fois (horodatage).

Imaginons que tout cela soit possible et qu'un tel cahier soit mis en place, auquel s'ajouteraient autant de pages nouvelles que nécessaire. Testaments, contrats, certificats de propriétés, messages publics ou adressés à une personne particulière, attestations de priorité pour une découverte, etc., tout cela deviendrait facile sans notaire ni huissier. Un tel cahier public, s'il était permanent, infalsifiable, indestructible et qu'on puisse y écrire librement et gratuitement tout ce qu'on veut, aurait une multitude d'usages.

Public, infalsifiable et indestructible

Un tel objet serait plus qu'un cahier de doléance ou un livre d'or, qui peuvent être détruits. Plus qu'un tableau d'affichage offert à tous sur les murs d'une entreprise, d'une école ou d'une ville, eux aussi temporaires. Plus que des enveloppes déposées chez un huissier, coûteuses et dont la lecture n'est pas autorisée à tous. Plus qu'un registre de brevets, dont la permanence est assurée, mais sur lesquels il est difficile d'écrire. Plus que les pages d'un quotidien, indestructibles car multipliées en milliers d'exemplaires, mais auxquelles peu de gens ont accès et dont le contenu est très contraint.

Bien sûr, ce cahier localisé en un point géographique unique ne serait pas très commode pour ceux qui habitent loin de Paris. Bien sûr, ceux qui y rechercheraient des informations en tournant les pages se gêneraient les uns les autres et gêneraient ceux venus y inscrire de nouveaux messages. Bien sûr encore, faire des recherches pour savoir ce qui est écrit dans le cahier deviendrait impossible en pratique quand le cahier serait devenu trop gros et que ses utilisateurs se seraient multipliés.

Ces trois inconvénients majeurs – localisation unique rendant l'accès malcommode et coûteux, impossibilité d'y lire ou écrire en nombre au même instant, difficultés de manipuler un grand cahier – peuvent être contournés. L'informatique moderne, avec la puissance de ses machines, y compris les smartphones et ses réseaux de communication, est en mesure de les surmonter.

Cette idée d'un grand cahier informatique, partagé, infalsifiable et indestructible du fait même de sa conception est au cœur d'une nouvelle révolution, celle de la blockchain, ou plus explicitement et en français : la révolution de la programmation par un fichier partagé et infalsifiable.

Une idée mise en œuvre pour les bitcoins

Le terme blockchain vient du bitcoin, la monnaie cryptographique créée en janvier 2009 et qui a depuis connu un développement considérable et un succès réel, la valeur d'échange des bitcoins émis dépassant aujourd'hui deux milliards d'euros. Au cœur de cette monnaie, il y a effectivement un fichier informatique infalsifiable et ouvert. C'est celui de toutes les transactions, et son inventeur Satoshi…

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

Source : http://www.pourlascience.fr/ewb_pages/a/article-les-blockchains-clefs-d-apos-un-nouveau-monde-33873.php
Par Jean-Paul Delahaye et Philippe Boulanger

La CIA aurait cherché à percer la sécurité de

l’iPhone | Le Net Expert Informatique

La #CIA aurait cherché à percer la sécurité de l’iPhone

C’est ce que révèlent de nouveaux documents transmis par Edward Snowden, et publiés par le site américain The Intercept.
Nouvelles révélations de nos confrères de The Intercept sur les pratiques d’espionnage des Etats-Unis. S’appuyant une nouvelle fois sur des documents transmis par Edward Snowden, le site américain fait état de l’existence d’une mission secrète de la CIA, initiée en 2006, visant à casser le système de chiffrement des terminaux iOS, iPhone et iPad.
L’agence américaine aurait notamment mis au point une version modifiée de l’environnement de développement Xcode : l’IDE conçu par Apple à destination des développeurs souhaitant créer des « apps natives » pour iOS. Cette édition modifiée permettrait d’aboutir à des applications dont les données seraient accessibles à la CIA, ces applications pouvant aussi servir de cheval de Troie sur le terminal – en désactivant ses fonctions de sécurité.
En revanche, aucune des pièces publiées par The Intercept ne tend à indiquer que l’opération a été un succès.
Les nouveaux documents d’Edward Snowden évoquent par ailleurs la tenu d’un événement secret survenu en 2012, le jamboree, lors duquel CIA et #NSA auraient partagé des informations. Le projet de hacking d’iOS y aurait notamment été présenté, lors d’une conférence titrée « Strawhorse: Attacking the MacOS and iOS Software Development ».

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

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

Source :
http://www.journaldunet.com/solutions/dsi/la-cia-aurait-cherche-a-casser-la-securite-de-l-iphone-0315.shtml?een=4a4b0e45c54d9fed8fc26819a6b6f84f&utm_source=greenarrow&utm_medium=mail&utm_campaign=ml49_6outilsdanalys

---

Limelight lance un service de détection de limitation de l’impact des attaques DDoS – Global Security Mag Online | Le Net Expert Informatique

Un service de détection de limitation de l'impact des attaques DDoS

Les menaces à la cyber sécurité connaissent une évolution croissante en termes de complexité, de rythme et d'échelle. Selon un enquête récente mondiale, menée en collaboration avec TechValidate, les clients sont le plus préoccupés par l'impact des cyberattaques de type DDoS sur la diffusion de contenu numérique [TVID : 957-39D-E29]. En outre, la majorité des clients interrogés croient que leur fournisseur de CDN est le mieux placés pour les aider à détecter et à limiter l'impact des attaques DDoS [TVID : 0B3-2FC-2FD].

Limelight Networks, Inc. annonce la disponibilité de sa solution DDoS Attack Interceptor, basée sur la plateforme Limelight OrchestrateTM (« Orchestrate »). Composante centrale du service Limelight Orchestrate Security, DDoS Attack Interceptor offre plusieurs lignes de défense pour la protection des clients : notification proactive en cas d'attaque, nettoyage du trafic et protection contre les coûts imprévus en raison des pics de trafic.

En accord avec cette préférence des clients, DDoS Attack Interceptor est directement intégrée dans le réseau CDN mondial de Limelight. Contrairement aux offres concurrentes, qui fonctionnent au niveau du routeur, la solution de Limelight place la détection directement dans le PoP du réseau CDN, offrant la seule détection en fonction de la situation accompagnée de technologies d'atténuation dans le Cloud. Le système de détection perfectionné de Limelight surveille en permanence le réseau pour détecter tout trafic malveillant. Allant au-delà des simples techniques de vérification des signatures, le moteur de détection utilise des techniques brevetées sur les comportements qui comparent la base de référence à partir du volume et des schémas et qui différencie de manière intelligente un bon trafic d'un trafic douteux.
Lorsqu'une attaque est détectée, le système détermine le centre de nettoyage distribué optimal dans le monde et y dirige le trafic, qui y sera alors filtré avant d'être retransmis à l'origine. Le service est entièrement fourni dans le Cloud via la plateforme Limelight Orchestrate, ce qui offre des performances élevées et une haute disponibilité, surtout en temps de sérénité, tout en offrant simultanément une détection continue. Les clients n'ont pas besoin d'acheter un matériel quelconque et aucune dépense d'investissement n'est nécessaire pour bénéficier de la totalité des fonctionnalités de cette offre.
Avec une capacité Egress de plus de 11 Tbit/s, la plateforme Orchestrate de Limelight gère plus de sept milliards de demandes utilisateurs par heure, garantissant la capacité de DDoS Attack Interceptor à gérer les plus grandes cyberattaques connues aujourd'hui. La solution offre un délai d'atténuation à la pointe de l'industrie, basculant rapidement en mode atténuation et offrant une base de référence coordonnée, une détection active et une atténuation rapide qui assurent le démarrage rapide du nettoyage, avec une très courte durée d'accélération, même pour les attaques plus difficiles à détecter.
Aujourd'hui, Limelight a également annoncé la disponibilité de Orchestrate 3.0, une plateforme complète conçue spécialement pour la diffusion de contenu numérique avec une qualité d'expérience (QoE) exceptionnelle. La plateforme Orchestrate 3.0 comprend le plus grand nombre d'améliorations jamais apportées par la société, que ce soit au niveau de l'infrastructure, de la suite logicielle ou de l'offre de services. Elle améliore ainsi pratiquement tous les aspects de l'expérience client et élargit l'offre de la société en incluant de nouveaux services axés sur la sécurité.

Réseau privé mondial Limelight
Le réseau mondial Limelight est l'un des réseaux privés de diffusion de contenu numérique les plus vastes au monde. Avec plus de 80 PoPs et 11 Tbps de capacité Egress, ce réseau a permis la diffusion sur Internet de quelques-uns des évènements les plus importants au monde. Le réseau Limelight assure la diffusion du contenu numérique tout en offrant une expérience d'une qualité irréprochable, quels que soient les pics de trafic et indépendamment des caprices de l'Internet public. Les autres améliorations que la version V3.0 apporte au réseau Limelight comprennent des mises à niveau des disques à circuits intégrés, une capacité supplémentaire de traitement, une bande passante plus large et une connectivité accrue, et de nouveaux points de présence dans le monde.

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

Source : http://www.globalsecuritymag.fr/Limelight-lance-un-service-de,20150312,51490.html

---

Trend Micro dresse le bilan de l'année écoulée dans son rapport annuel de sécurité | Le Net Expert Informatique

Trend Micro dresse le bilan de l'année écoulée dans son rapport annuel de sécurité

Les cyber-attaques réussies contre Sony, avec environ 100 Téraoctets de données piratées et des dommages estimés à près de 100 millions de dollars, sont venues couronner une année mémorable en termes de cyber-sécurité. Le rapport de sécurité annuel de Trend Micro, intitulé « The High Cost of Complacency » (Le coût élevé de la négligence), revient sur ce piratage ainsi que sur les événements de sécurité majeurs qui ont de nouveau illustré l'obstination des cybercriminels et la sophistication de leurs attaques en 2014.

« L'essentiel d'une stratégie de cyber-sécurité repose sur l'identification de ce qui est le plus important, le déploiement de technologies adéquates et la sensibilisation des utilisateurs », explique Raimund Genes, CTO de Trend Micro. « C'est le rôle de tout un chacun, pas seulement des informaticiens, que de préserver les données sensibles de l'entreprise. »
Les informations rassemblées au sein de ce rapport confirment notamment la prédiction formulée par Trend Micro fin 2013, selon laquelle un piratage majeur de données se produirait en moyenne une fois par mois. Pour les entreprises, le besoin de déployer des dispositifs de protection des réseaux et de détection des intrusions se fait d'autant plus sentir.
« A l'image du piratage de Sony, l'envergure et la portée des attaques perpétrées l'année dernière se sont avérées dramatiques », commente Tom Kellermann, Chief Cybersecurity Officer de Trend Micro. « Malheureusement, il ne s'agit sans doute que d'un aperçu de ce que l'avenir nous réserve. »

Parmi les principaux éléments traités dans ce rapport de sécurité 2014 :
Il ne faut négliger aucune menace, aussi minime soit-elle. Les pirates utilisent des méthodes simples pour déjouer la sécurité des entreprises et causer d'importants dégâts.
Les RAM scrapers, ces malware installés sur les terminaux de points de vente, sont presque devenus monnaie courante en 2014. Plusieurs cibles notables ont perdu des millions de données clients au profit des malfaiteurs tout au long de l'année.
De nouvelles attaques ont démontré qu'aucune application n'était invulnérable face à des pirates qui se diversifient.
La banque en ligne et mobile a connu ses plus importants défis de sécurité en 2014, notamment une sérieuse remise en question de l'authentification à deux facteurs comme garant de la sécurité des opérations sensibles.
Les ransomware ont gagné en puissance et en sophistication. Ils se sont étendus à de nouvelles régions du monde et à de nouvelles cibles. Ils vont désormais jusqu'à chiffrer les fichiers sur les systèmes infectés pour s'assurer du paiement de la rançon.

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

Source : http://www.globalsecuritymag.fr/Trend-Micro-dresse-le-bilan-de-l,20150309,51375.html

Vote électronique : Confidentialité et sécurité des données a confirmé le Conseil d’Etat | Le Net Expert Informatique

Vote électronique : Confidentialité et sécurité des données a confirmé le Conseil d’Etat

Le Conseil d'Etat a été amené, dans un arrêt du 11 mars 2015 n° 368748, à se prononcer sur la confidentialité et la sécurité des données à l'occasion de l'organisation d'un vote électronique pour les élections professionnelles de délégués du personnel.

En l'espèce, la CNIL, saisie d'une plainte d'un syndicat, prononce un avertissement à l'encontre d'une société n'ayant pas pris toutes précautions utiles pour préserver la sécurité et la confidentialité des données à caractère personnel lors de l'élection des délégués du personnel organisée par voie électronique avec recours aux services d'un prestataire extérieur. La société et le prestataire forment un recours en annulation de cette délibération devant le Conseil d'Etat.

Le Conseil d'Etat rejette la requête et retient qu'il résulte des dispositions du Code du travail, « dont l'objectif est de garantir la sincérité des opérations électorales par voie électronique, que l'utilisation d'un système de vote électronique pour l'élection des délégués du personnel est subordonnée à la réalisation d'une expertise indépendante lors de la conception initiale du système utilisé, à chaque fois qu'il est procédé à une modification de la conception de ce système ainsi que préalablement à chaque scrutin recourant au vote électronique ».

Dès lors, « à supposer même que le système de vote électronique en litige n'ai fait l'objet d'aucune modification de sa conception depuis sa précédente utilisation par l'entreprise, […] une expertise indépendante était requise préalablement à sa mise en place pour les élections professionnelles organisées par la société requérante ».

Par ailleurs, « il résulte de [l'article R. 2324-5 du Code du travail sur la confidentialité des données transmises] que la transmission aux électeurs des identifiants et mots de passe leur permettant de participer au vote doit faire l'objet de mesures de sécurité spécifiques permettant de s'assurer que les électeurs en sont les seuls destinataires ». Ainsi, « c'est à bon droit que la CNIL a estimé que la transmission par simple courriel de ces données aux électeurs méconnaissait les obligations » découlant de ce même article.

En outre, le Conseil d'Etat rappelle, conformément à un arrêté ministériel du 25 avril 2007, que « le respect de ces dispositions implique nécessairement que le chiffrement des bulletins de vote soit ininterrompu », et ce dès l'émission du vote sur le poste de l'électeur jusqu'à sa transmission au fichier dénommé « contenu de l'urne électronique ».

Enfin, si l'employeur a recours à un prestataire extérieur pour l'organisation du vote électronique, il reste malgré tout responsable de ce traitement de données. Le Conseil d'Etat précise ainsi que « la circonstance que des opérations de traitement de données soient confiées à des sous-traitants ne décharge pas le responsable de traitement de la responsabilité qui lui incombe de préserver la sécurité des données ». Cela ne méconnaît pas « le principe constitutionnel de responsabilité personnelle, dès lors que ces sous-traitants ont agi sur instruction du responsable de traitement ».

Le Conseil d'Etat a ainsi estimé que la sanction de la CNIL visant à rendre public l'avertissement était proportionnée au regard de la nature et de la gravité des manquements constatés, et sa publication appropriée « à la recherche de l'exemplarité ».

[block id="24761" title="Pied de page HAUT"]

A Lire aussi :
Nouveautés dans l'organisation des votes électroniques pour les élections professionnelles
3 points à retenir pour vos élections par Vote électronique
Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique
Modalités de recours au vote électronique pour les Entreprises
L'Expert Informatique obligatoire pour valider les systèmes de vote électronique
Dispositif de vote électronique : que faire ?
La CNIL sanctionne un employeur pour défaut de sécurité du vote électronique pendant une élection professionnelle
Notre sélection d'articles sur le vote électronique

Source : http://www.snaless.org/vote-electronique-confidentialite-et-securite-des-donnees_juri_2855.php

---

Les experts de la sécurité se penchent sur la Watch d’Apple | Le Net Expert Informatique

Les experts de la sécurité se penchent sur la Watch d’Apple

La firme de Cupertino a donc lancé officiellement sa montre connectée, la Watch, le 9 mars 2015 hier soir. Tout a été dit sur ce gadget déclinable en plusieurs versions dont une luxueuse au prix stratosphérique de 11 000 euros. Mais cette annonce a aiguisé la curiosité des experts en sécurité qui se sont penchés sur les faiblesses de la tocante numérique.

Nos confrères de The Register ont interrogé plusieurs spécialistes de la sécurité sur ce sujet. Ainsi, Ken Westin, chercheur chez Tripwire a indiqué que « le fait que le dispositif soit à la fois WiFi et Bluetooth va faciliter le développement des fonctionnalités supplémentaires à la montre et de s'interopérer avec d'autres équipements. Mais cela va également augmenter la surface d'attaque de l'appareil ». Pour lui, il ne fait aucun doute que « les chercheurs et les hackers ont été émoustillés pour trouver de nouvelles vulnérabilités et s'appuyer sur des attaques existantes qui profitent des faiblesses du WiFi et du Bluetooth ».

Problème de confidentialité des données
Un autre aspect de sécurité selon l'expert réside dans la confidentialité des données. « Avec ces connectivités, il sera intéressant de voir comment les données peuvent être utilisées pour suivre les personnes dans espaces physiques. Cela peut avoir un impact pour un cyberattaquant, tout comme pour des campagnes publicitaires trop ciblés ». L'arrivée d'applications tierces n'est pas faite pour rassurer le spécialiste qui y voit un risque supplémentaire pour la sécurité et la vie privée.

La fraude au paiement
En disposant d'une capacité NFC, l'Apple Watch peut servir pour le paiement mobile. Les risques de fraudes existent donc. Une récente étude de Drop Labs montre que le niveau de fraude sur les paiements avec Apple Pay est de 6% contre 1% en moyenne pour les transactions par carte bancaire. Pour la défense d'Apple, le problème vient surtout d'un niveau d'authentification faible de la part des banques. Une affaire récente a démontré ce risque. Certains spécialistes s'interrogent sur la fiabilité de la technologie NFC avec la capacité de la contourner.

Une révision des politiques de BYOD ?
Phil Barnett, directeur général EMEA de Good Technology, préfère souligner les menaces que les montres connectées et plus généralement les « wearables technology » impliquent dans le monde du travail. Elles s'inscrivent dans les politiques de BYOD (Bring Your Own Device) qui selon lui doivent être révisées. « Le BYOD a déjà connu les smartphones et des tablettes, les accessoires connectés arrivent comme les prochains véhicules de la donnée. Ils représentent une immense opportunité pour la productivité, mais ils nécessitent avant leur arrivée en entreprise de les sécuriser. »
Cela passe pour lui par plusieurs axes : « Chiffrement des données transitant sur le Bluetooth et la conteneurisation des données de l'entreprise. Par ailleurs, un contrôle plus granulaire des politiques de sécurité devrait permettre de trouver un équilibre entre risques et productivité. » A condition qu'il n'y ait pas de défaut dans la cuirasse, comme le montre la faille Freak qui affaiblissait le chiffrement des navigateurs Apple et Android. La firme de Cupertino vient d'ailleurs de publier iOS 8.2 qui règle ce problème.

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

Source : http://www.silicon.fr/les-experts-de-la-securite-se-penchent-sur-la-watch-dapple-110567.html

Tendances et prévisions en cybercriminalité pour 2015 | Le Net Expert Informatique

Tendances et prévisions en cybercriminalité pour 2015

Augmentation des attaques ciblées En 2015, les attaques ciblées deviennent encore plus sophistiquées. Souvent appelées APT (Advanced Persistant Threats), elles sont différentes des cyberattaques traditionnelles. Conçues pour attaquer des victimes spécifiques et pour être silencieuses, les attaques ciblées peuvent être cachées et non détectées dans des réseaux insuffisamment sécurisés.
"Le vecteur des attaques ciblées profite généralement des attaques d'ingénierie sociale", explique Pablo Ramos, chef du laboratoire de recherche ESET en Amérique Latine. "C'est alors que la manipulation psychologique est utilisée pour pousser les victimes potentielles à commettre certaines actions ou à divulguer des informations confidentielles. Les attaques peuvent également prendre l'apparence d'exploits jour-zéro, où elles profitent de vulnérabilités nouvellement découvertes dans un système d'exploitation ou une application particulière."
Au cours de 2014, le blog WeLiveSecurity d'ESET a publié un certain nombre d'analyses approfondies concernant les attaques ciblées, telles que BlackEnergy campaign et Operation Windigo .

Les systèmes de paiement en ligne attirent plus de malware
Alors que toujours plus de personnes adoptent les systèmes de paiement en ligne pour des biens et des services, ces systèmes deviennent encore plus attrayants pour les concepteurs de malware intéressés par les gains financiers.
2014 a vu la plus grande attaque connue à ce jour en matière de paiement digital, quand un pirate a récolté plus de 600.000 dollars US en Bitcoins et Dogecoins en utilisant un réseau de machines infectées.
ESET a signalé les attaques effectuées en mai contre Dogevault site , où les utilisateurs du très populaire portefeuille électronique ont signalé des retraits non autorisés de leurs comptes avant que le site ne soit obligé d'être déconnecté suite à la destruction des données du site par les attaquants. On estime que 56.000 dollars US ont été volés aux utilisateurs du portefeuille en ligne.
Nous avons aussi vu des attaques de force brute telles que Win32/BrutPOS , qui ont essayé d'accéder aux comptes protégés par un mot de passe en les bombardant de mots de passe populaires afin d'avoir un accès à distance – un rappel général en faveur de l'utilisation de mots de passe forts et uniques.

L'internet des choses – nouveaux jouets pour pirates
Alors que de nouveaux appareils se connectent à internet et stockent plus de données, ils deviennent un vecteur d'attaque attrayant pour les cybercriminels. Au cours de 2014, nous avons trouvé plus de preuves de la hausse de cette tendance. Lors de la conférence Defcon, on a vu les attaques sur les voitures en utilisant le dispositif ECU, ou sur la voiture Tesla qui a été piratée afin d'en ouvrir les portes alors qu'elle roulait.
Des attaques et des concepts ont aussi été montrés dans le secteur de la télévision sur différents systèmes, systèmes biométriques sur smartphones, routeurs – pour ne pas mentionner Google glasses.
C'est un domaine émergent pour la cybercriminalité et il restera un secteur de concentration pour l'industrie de la sécurité. Alors que cela pourrait prendre des années avant de devenir une menace grave, il faut agir dès à présent afin de mieux prévenir ce type d'attaques.
Plus d'information
Le rapport complet est disponible sur WeLiveSecurity.com.

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

Source : https://mail.google.com/mail/u/0/?hl=fr&shva=1#inbox/14be54fe5faeb40f?compose=14be53ae312f08d7

Windows concerné aussi par la Faille SSL Freak | Le Net Expert Informatique

Windows concerné aussi par la Faille SSL Freak

Sécurité : Microsoft a révélé que Windows était également touché par la faille de sécurité nommée Freak qui permet de pratiquer une attaque type « man in the middle » sur les connexions sécurisées https.

En début semaine, nous apprenions l'existence d'une nouvelle faille de sécurité portant sur les protocoles SSL et TLS. Baptisée Freak (Factoring RSA Export Keys), elle permettrait à un assaillant de lancer une attaque contre une connexion https afin de la forcer à activer une clé de chiffrement moins puissante qui peut ensuite être cassée en quelques heures. Cette faille a été découverte par une équipe de spécialistes européens, parmi les lesquels des français de l'Inria et des experts de Microsoft Research. Or, Microsoft vient d'annoncer que Windows était finalement lui aussi concerné par Freak. Une information qui n'avait pas été communiquée immédiatement au moment de la présentation des conclusions de cette étude.

Un correctif en préparation

Dans un bulletin de sécurité diffusé hier, l'éditeur indique que Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows 8, 8.1, Windows Server 2012 et Windows RT sont affectés. Microsoft indique qu'il a engagé une enquête technique qui pourrait déboucher sur la diffusion d'un correctif.

Selon les dernières estimations des chercheurs qui ont découvert Freak, voici la liste des navigateurs Internet concernés : Internet Explorer, la version Android de Chrome, le navigateur par défaut d'Android, Safari sur iOS et Mac OS X, le navigateur BlackBerry ainsi qu'Opera sur Mac OS X et Linux.

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

Source : http://www.zdnet.fr/actualites/faille-ssl-freak-windows-est-aussi-concerne-39815920.htm
Par Eureka Presse