Mais à quoi sert Spaces, le nouveau service de Google ?

Mais à quoi sert Spaces, le nouveau service de Google ?

Google a sorti aujourd'hui son nouveau service nommé Spaces. Disponible sur le web, sur iOS et sur Android, cet outil est difficile à cerner : voici quelques pistes d'utilisation après un premier test à la rédaction.

Le monde découvre en ce moment un nouveau service Google : Spaces. Non, il ne s'agit pas du petit nom du programme spatial de Mountain View, mais d'une application qui vous permet de créer des groupes avec des amis / collègues / inconnus pour partager… des choses. Des liens, des images, des commentaires et des vidéos YouTube pour l'instant.
Mais à quoi cela sert ? Eh bien c'est assez difficile à dire pour l'instant. Nous nous sommes empressé de créer un groupe pour Humanoid et d'inviter nos collègues préférés à tester l'application qui se paie le luxe d'être multiplateformes, disponible sur le web, iOS et Android. Nous avons partagé quelques liens, modifié ce qui était modifiable. Nous sommes aussi passés à côté des premiers bugs : une phrase qui sort de l'écran (dommage, c'est celle qui présente le service) ou l'impossibilité d'utiliser un compte Gmail d'entreprise… alors qu'il est proposé au lancement de l'application… [Lire la suite]

Réagissez à cet article

Source : *Mais à quoi sert Spaces, le nouveau service de Google ? – Tech – Numerama*

Pourquoi 95% des distributeurs de billets sont encore vulnérables au piratage

Pourquoi 95% des distributeurs de billets sont encore vulnérables au piratage

---

Lorsque Microsoft a abandonné Windows XP en 2014, on pouvait alors découvrir que 95% des distributeurs de billets de banque tournaient encore sous cette version obsolète de l'OS, devenant ainsi vulnérables au piratage. En 2016, rien n'a changé et les banque comme les constructeurs ne semblent pas décidés à faire le nécessaire.

Lorsque Microsoft a abandonné Windows XP en 2014, la menace de piratage est devenue de plus en plus grande pour les distributeurs de billets. Pourtant, fin 2015, **95% d'entre eux** tournaient encore sous cette version obsolète du système d'exploitation. On dénombre d'ailleurs pas moins de 9000 risques de sécurité sur ces machines. Pourtant les banques semblent s'en laver les mains, pourquoi ?
Comme l'explique Alexey Osipov, ingénieur chez Kaspersky, les constructeurs de distributeurs automatiques ont très peu de concurrents et les banques sont sous contrat avec eux, ils ne font donc pas l'effort de prendre les mesures suffisantes pour sécuriser leurs machines.
Pour Olga Kochetova, également ingénieur chez Kaspersky après avoir travaillé plusieurs années sur le marché des distributeurs bancaires, la réponse est encore plus simple. Ces machines étant désormais trop vieilles pour faire tourner des versions plus récentes et sécurisées de Windows, elles nécessitent donc d'être remplacées, or « **l'investissement serait trop coûteux** ». En outre, ça impliquerait aussi d'embaucher un nouveau personnel mieux formé vis à vis des nouveaux risques de piratage.

Il faut dire que pour un hacker, pirater un distributeur de billet est d'une simplicité enfantine puisqu'il suffit d'acheter une clé sur internet pour se connecter physiquement aux machines. Ils prennent ainsi tout simplement le contrôle du DAB pour lui réclamer la somme qu'ils souhaitent. L'an dernier, une attaque massive baptisée « Carbanak » avait fait perdre plus de **10 millions de dollars** à différentes banques situées un peu partout dans le monde… [Lire la suite]

Réagissez à cet article

Source : *Pourquoi 95% des distributeurs de billets sont encore vulnérables au piratage*

Windows 10 Mobile acceptera l’empreinte digitale comme moyen d’authentification cet été

Windows 10 Mobile acceptera l’empreinte digitale comme moyen d’authentification cet été

La version mobile de Windows 10 gagnera bientôt la compatibilité avec les lecteurs d'empreinte digitale déjà exploités par Android et iOS.

Selon *Engadget*, Microsoft en a fait l'annonce aujourd'hui dans le cadre de la conférence WinHEC. Alors qu'il était déjà possible de déverrouiller son téléphone Windows grâce à la reconnaissance faciale du système, la lecture d'empreinte digitale pourra également être employée.

Pour en bénéficier, il faudra attendre que les fabricants de téléphones Windows ajoutent le lecteur en question.

Ainsi, Windows Hello gagnera cette fonctionnalité dans la mise à jour anniversaire de Windows 10 Mobile dont le déploiement est prévu pour juillet prochain.

Bien entendu, pour en bénéficier, il faudra attendre que les fabricants de téléphones Windows ajoutent le lecteur en question. Pour le moment, seul l'Elite X3 de HP – un téléphone Windows toujours en développement destiné pour le marché des affaires et promettant d'agir comme un ordinateur portable – intègre un lecteur d'empreinte digitale… [Lire la suite]

Réagissez à cet article

Source : *Windows 10 Mobile acceptera l'empreinte digitale comme moyen d'authentification cet été | Branchez-vous*

Laurent LASALLE

Retrouvrer les traces d’une attaque informatique peut s’avérer complexe et coûteuse

Retrouvrer les traces d’une attaque informatique peut s’avérer complexe et coûteuse

Selon l'un des principes fondamentaux de la police scientifique, sur une scène de crime, tout contact laisse une trace. Dans l'univers de la cybercriminalité, chercher les traces pour remonter le fil des événements jusqu'à l'auteur de l'attaque, se révèle souvent compliqué.

Lorsqu'un incident survient, il est généralement difficile pour l'entreprise de définir qui a accédé à son système d'information et ce que cette personne – ou groupe de personnes – a fait. La tâche se complique encore un peu plus lorsque cet incident provient d'utilisateurs internes bénéficiant d'un haut niveau de privilèges sur le système – voire même de la personne en charge de prévenir les attaques sur le réseau.
Que l'incident soit le résultat d'une action malveillante d'un utilisateur interne, d'une erreur humaine ou d'une faille, dès lors que l'entreprise n'est pas capable de remonter les informations, elle passe à côté de preuves cruciales, et rend l'enquête beaucoup plus longue et onéreuse.

Le facteur temps : la clé de la réussite
Dans toutes investigations post-incident de sécurité, le temps est un facteur crucial. Pour mener à bien une enquête, il est plus facile, plus précis et généralement moins couteux de conduire une analyse criminalistique, dite forensics, poussée immédiatement, plutôt que plusieurs semaines voire plusieurs mois après l'incident.
L'examen approfondi des logs : remonter les étapes d'une attaque
Lorsqu'une faille est avérée, l'entreprise dépend des logs générés par les terminaux et les applications sur le réseau, pour déterminer la cause initiale et remonter les étapes de l'attaque. En pratique, trier les informations peut prendre des jours – en d'autres termes, cela revient à chercher une aiguille dans une botte de foin.
L'intégrité des logs : le respect du standard des preuves
Si les logs ont été modifiés et qu'ils ne peuvent pas être présentés dans leur format original, l'intégrité des données de logs peut être remise en question lors d'une procédure légale. Les logs doivent respecter le standard légal des preuves, en étant collectés de manière inviolable. A contrario, les logs qui ont été modifiés ou qui n'ont pas été stockés de manière sécurisée, ne seront pas acceptés comme preuve légale dans une cour de justice.
Cependant, même pour les organisations qui ont implémenté des solutions fiables de collecte et de gestion des logs, l'information cruciale peut manquer et ce chainon manquant peut empêcher l'entreprise de reconstituer tout le cheminement de l'incident et ainsi de retrouver la source initiale du problème.

Les comptes à privilèges : une cible fructueuse pour les cybercriminels
En ciblant les administrateurs du réseau et autres comptes à privilèges qui disposent de droits d'accès étendus, voire sans aucune restriction au système d'information, aux bases de données, et aux couches applicatives, les cybercriminels s'octroient le pouvoir de détruire, de manipuler ou de voler les données les plus sensibles de l'entreprise (financières, clients, personnelles, etc.).

L'analyse comportementale : un rempart nouveau pour les entreprises
Les nouvelles approches de sécurité basées sur la surveillance des utilisateurs et l'analyse comportementale permettent aux entreprises d'analyser l'activité de chacun des utilisateurs, et notamment les événements malveillants, dans l'intégralité du réseau étendu.
Ces nouvelles technologies permettent aux entreprises de tracer et de visualiser l'activité des utilisateurs en temps réel pour comprendre ce qu'il se passe sur leur réseau. Si l'entreprise est victime d'une coupure informatique imprévue, d'une fuite de données ou encore d'une manipulation malveillante de base de données, les circonstances de l'événement sont immédiatement disponibles dans le journal d'audit, et la cause de l'incident peut être identifiée rapidement.
Ces journaux d'audit, lorsqu'ils sont horodatés, chiffrés et signés, fournissent non seulement des preuves recevables légalement dans le cadre d'une procédure judiciaire, mais ils assurent à l'entreprise la possibilité d'identifier la cause d'un incident grâce à l'analyse des données de logs.
Lorsque ces journaux sont complétés par de l'analyse comportementale, cela offre à l'entreprise une capacité à mener des investigations forensics beaucoup plus rapidement et à moindre coût, tout en répondant pro activement aux dernières menaces en temps réel… [Lire la suite]

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Recouvrer les traces d'une attaque informatique : l'investigation peut s'avérer complexe et coûteuse – JDN*

Top 10 des arnaques sur Facebook en 2014

Top 10 des arnaques sur Facebook en 2014

Une étude des analystes antivirus Bitdefender révèle que Taylor Swift n'est plus aussi populaire que l'année dernière, lorsqu'une fausse vidéo à son sujet avait permis de répandre massivement un malware sur le réseau social. Chaque année, des millions d'utilisateurs tombent dans les pièges des arnaques diffusées sur Facebook. Voici le classement des 10 arnaques les plus répandues dans le monde, depuis le début de l'année 2014 !

1. **Qui a visité mon profil**– 30.20% (anglais – international)
2. **Changez la couleur de votre Facebook** – 7.38% (anglais – international)
3. **La sextape de Rihanna avec « son » petit-ami**– 4.76% (anglais – international)
4. **Consultez mon nouveau statut pour recevoir gratuitement un T-shirt officiel Facebook** – 4.21% (anglais – international)
5. **Dites au revoir au Facebook bleu**– 2.76% (français)
6. **Produits défilmés. Distribution gratuite**– 2.41% (anglais – international)
7. **Vérifiez si un ami vous a supprimé de sa liste** – 2.27% (anglais – international)
8. **Cliquez ici pour voir le top 10 des profils qui vous harcèlent le plus ! Vous serez étonné d'apprendre que votre ex visite toujours votre profil !** – 1.74% (anglais – international)
9. **Découvre comment voir qui visite ton profil, tu n'es pas au bout de tes surprises !** – 1.55% (espagnol)
10. **Je viens de modifier le thème de mon Facebook. C'est incroyable**– 1.50% (anglais – international)

Autres : 41.22%

Alors que Taylor Swift quitte le Top 10, **Rihanna reste la star la plus utilisée en tant qu'« appât »** par les scammers pour répandre un malware via Facebook.
L'arnaque des billets "gratuits" pour Disneyland sort aussi du classement alors qu'en juillet dernier, elle surclassait l'arnaque « Je peux vérifier qui regarde mon profil » qui avait fait des dizaines de milliers de victimes. Le scam « **Qui a visité mon profil » conserve quant à lui sa 1ère place**, représentant presque un tiers de la part totale des arnaques sur Facebook (30.20%).
Les arnaques du type « changez la couleur de votre Facebook » se sont internationalisées et représentent dorénavant **7,38 % de la part totale des scams sur Facebook** (vs 4.16% en 2013).

Les mêmes arnaques Facebook fonctionnent toujours

« Pourquoi les utilisateurs veulent-ils toujours savoir qui a jeté un coup d'œil à leur profil, malgré tous les avertissements de sécurité à ce sujet ? » déclare Catalin Cosoi, Responsable de la Stratégie de sécurité chez Bitdefender. *« Ils pensent certainement qu'il s'agit de vraies applications… C'est ce que l'on appelle de l'ingénierie sociale, et elle atteint alors son plus haut niveau – un jeu psychologique entre le cybercriminel et sa victime. Les appâts ont changé avec le temps – harceleurs, voyeurs, admirateurs, petites amies trop attachées et ex qui vous hantent, mais la raison pour laquelle ces arnaques fonctionnent est simple : la nature humaine. »*
Une offre de **T-shirts Facebook gratuits** fait son entrée dans le Top 10 (4.21 %). Les fans intéressés par des vêtements à l'effigie de la marque américaine se retrouvent à remplir de **fausses études ou à installer des add-ons malveillants** qui exploitent leurs données personnelles.
L'autre nouveauté de ce classement concerne des arnaques qui piègent les utilisateurs avec des **cadeaux publicitaires défilmés** (2,41 %).
Au cours de ces deux dernières années, les **arnaques sur Facebook se sont multipliées** en même temps que la plate-forme de réseau social s'est développée. L'étude Bitdefender montre aussi une augmentation du nombre d'arnaques via des **vidéos virales qui utilisent de façon abusive les *"like"*** Facebook et les options de partage. L'année passée, les sites frauduleux utilisant le **likejacking** (détournement de « *J'aime*«), **clickjacking** (détournement de liens) et **YouTube** ont proliféré en anglais mais aussi en allemand, chinois et en italien.
Pour éviter d'être détectés plus facilement, les scammers peuvent utiliser des caractères spéciaux et numéros dans la description de leur fausse application. Une **variante populaire du scam « Top profil visiteurs »** attire de nouvelles victimes avec ce message : *"Check 0ut n0w wh0 viewed ur profile"*.
Cette étude se base sur les données issues de l'outil Safego de Bitdefender, l'application Facebook gratuite qui scanne les timelines et alerte les utilisateurs en cas de posts malveillants et frauduleux. Pour plus d'informations sur la protection de vos comptes utilisateurs de médias sociaux, vous pouvez consulter le guide de sécurité de Bitdefender à ce sujet… [Lire la suite]

Source : *Fausses sextapes et arnaques diverses : le top 10 des scams en 2014 sur Facebook*

Denis JACOPINI participera au 8e IT-Forum à Abidjan les 2 et 3 juin 2016

Denis JACOPINI participera au 8e IT-Forum à Abidjan les 2 et 3 juin 2016

La 8e édition du IT-Forum (Forum des décideurs et acteurs des Technologies de l'Information) se déroulera les 2 et 3 juin prochain à Abidjan.

IT FORUM 8ème EDITION

Des conférences seront animées en plénières par des spécialistes, des Experts-Consultants et des Universitaires. Ce sera le lieu de faire des exposés, de partager des expériences, de former et d'informer les participants.
Les enjeux de la transformation numérique et plus globalement de l'appropriation des nouvelles technologies modifient considérablement notre mode de vie. La sécurisation des données et des dispositifs de paiement comporte des failles qu'il comporte d'améliorer pour apporter la confiance nécessaire au climat des affaires.
De nombreuses études viennent conforter ce constat et tendent à démontrer le potentiel de croissance du secteur.
En Côte d'Ivoire, les transactions mobiles s'élèvent à 15 milliards de FCFA par jour soit 22,5 millions d'Euros.
Des montants qui donnent le vertige et qui poussent les sites marchands notamment les opérateurs de télécommunications à prendre des mesures de sécurité de plus en plus importantes… mais qui montrent aussi rapidement leurs limites !
Au fil des années, la Côte d'Ivoire s'est imposée comme l'un des leaders naturels dans le domaine des transactions mobiles en Afrique.
En insistant sur la priorité à donner à la protection des données et des transactions (mobile banking, eCommerce),
Devenu un rendez-vous incontournable depuis une décennie, l'IT Forum s'impose aujourd'hui comme l'une des
rencontres les plus importantes.
QUAND
Jeudi 2 juin 2016 à 08:00 – Vendredi 3 juin 2016 à 18:00 (Heure : Côte d'Ivoire) – Ajouter au calendrier
LIEU
Maison de l'entreprise – CGECI (Confédération Générale des Entreprises de Côte d'Ivoire – Patronat ivoirien), Avenue Lamblin, Abidjan, Lagunes, Côte d'Ivoire, Abidjan, Plateau, Cote d'Ivoire –
PROGRAMME
http://www.ciomag-event.com/8eme-edition-it-forum-cote-d-ivoire

---

Réagissez à cet article

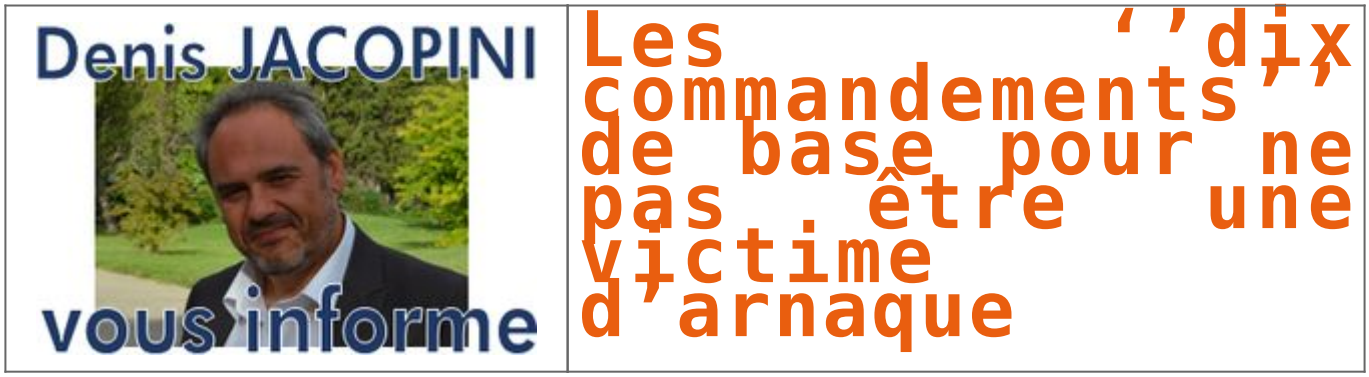
Sources :

IT-Forum 2016 – 8e édition du Forum des décideurs et acteurs des Technologies de l'Information

http://it-forum.ci

https://www.eventbrite.fr/e/inscription-it-forum-2016-8eme-edition-24951266911

Les ‘’dix commandements’’ de base pour ne pas être une victime d'arnaque



Les cybercriminels continuent de faire de nombreuses victimes à travers le monde. Si des moyens de répression de cette activité criminelle sont entrepris dans nos différents pays, l'un des moyens les plus efficaces de l'éradiquer reste la prévention.

Dans cet article, la Plateforme de lutte contre la cybercriminalité (PLCC) fait un rappel en 10 points des mesures à prendre pour naviguer sur la toile en toute sécurité.

1- Changer régulièrement vos mots de passe. (Un site = Un mot de passe unique)

2- Aucune autorité judiciaire, de police ne possède d'adresse mail gratuite de type Hotmail, Yahoo, Gmail…

3- Ne divulguez pas d'informations personnelles sur Internet. Prenez le temps de sécuriser vos comptes ainsi que ceux de vos enfants. Ne rendez pas visibles vos contacts sur Facebook ou autre réseau sociale.

4- Allez toujours sur une adresse commençant par https://, officielle et habituelle pour vous connecter à votre compte bancaire, à votre messagerie ou autres réseaux sociaux.

5- Evitez d'envoyer des photos ou vidéos, de vous, à caractère sexuelle ou tout autre position indélicate.

6- Ne versez jamais d'argent par Mandat Cash ou Western Union à une personne que vous ne connaissez pas, que vous n'avez jamais rencontrée physiquement.

7- Méfiez-vous des trop bonnes affaires. Ne cédez jamais à la précipitation. Les bases d'une transaction sont les mêmes dans la réalité et sur Internet. Une annonce trop alléchante cache souvent une arnaque. Renseignez-vous, comparez les prix et les produits avant d'acheter.

8- Cessez tout contact si votre interlocuteur (que vous ne connaissez pas) vous demande de l'argent sous prétexte de frais, de maladie, de transport…

9- Remettez vous souvent en question. Il n'y a pas de profil type de victime, personne n'est à l'abri sur Internet. Les cyberdélinquants jouent parfois sur notre confiance excessive en nos capacités.

10- Ayez un anti-virus efficace et à jour sur votre ordinateur.

Une fois de plus, la PLCC vous exhorte à la prudence !… [Lire la suite]

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Lutte contre la cybercriminalité: Voici les ‘’dix commandements’’ de base pour ne pas être une victime d’arnaque*

RGPG Règlement européen sur la protection des données : priorité au chiffrement, à l’authentification et aux contrôles d’accès

	**RGPD : Règlement européen sur la protection des données : priorité au chiffrement, à l’authentification et aux contrôles d’accès**

Philippe Carrère, directeur de la protection des données et de l'identité, Europe du Sud chez Gemalto revient sur le nouveau règlement européen sur la protection des données personnelles et ce qu'il implique pour les entreprises en termes de stratégie de sécurité et de relation client.

L'adoption récente du règlement européen sur la protection des données personnelles constitue un tournant pour les entreprises implantées dans l'Union Européenne. En effet, il exige des gestionnaires d'infrastructures et des fournisseurs de services numériques – tels qu'Amazon ou Google – de faire part d'éventuels vols de données et de mettre en place des mesures de sécurité adéquates. Les chefs d'entreprises devraient y voir là un avertissement et commencer dès à présent à évaluer leurs politiques de sécurité, avant que la proposition de loi ne soit approuvée par le Parlement et le Conseil européen.
Où en sont les entreprises européennes en termes de sécurité des données et quelles mesures doivent-elles prendre afin d'être conformes ? A l'heure actuelle, les pare-feu, les antivirus, le filtrage de contenu et la détection des menaces sont les principaux outils utilisés pour se prémunir des vols de données. Ces mesures sont, cependant, insuffisantes, les hackers pouvant franchir aisément ce premier périmètre de sécurité. Dès lors, l'adresse IP des entreprises ou encore les informations de leurs clients peuvent être compromises, comme ce fut le cas avec Volkswagen et la conception de sa Passat.
D'après le Breach Level Index réalisé pour l'année 2015 par Gemalto, plus de 707,5 millions de dossiers clients ont été volés ou perdus à la suite de 1 673 cyberattaques menées de par le monde. Un chiffre qui devrait faire l'effet d'un véritable électrochoc pour les responsables informatiques, d'autant que, fait encore plus inquiétant, 4 % des infractions ont impliqué des données sécurisées (chiffrées partiellement ou en totalité).
Les clients confient des données confidentielles, et ils doivent donc être assurés et convaincus de leur sécurité. Si le lien de confiance avec le client vient à être brisé, il peut être très difficile pour les entreprises de le renouer.
Une de nos récentes études a révélé que plus de la moitié des individus interrogés (57 %) ne traiterait jamais, ou très peu probablement, avec une société ayant perdu des données personnelles suite à une cyberattaque.

Pourquoi ce règlement apparaît aujourd'hui comme une nécessité ?
La sécurité a toujours été un sujet d'actualité, mais suite aux récentes attaques, comme celle de Talk Talk, et le fait que de plus en plus de données personnelles sont collectées en ligne, assurer leur sécurité et maintenir une relation de confiance avec les clients n'a jamais été aussi primordial. A l'heure actuelle, les entreprises européennes ne sont pas tenues de signaler les brèches de données dont elles peuvent faire l'objet, et, de fait, grand nombre d'entre elles ne le font pas. Une fois la nouvelle réglementation en vigueur, elles seront dans l'obligation de révéler ces violations, sous peine de se voir infliger une amende pouvant aller jusqu'à 4 % de leur chiffre d'affaires. C'est pourquoi elles doivent dès à présent opérer un changement de stratégie.
Cependant, il ne s'agit pas là d'un fait nouveau. Cette pratique est déjà en place depuis plusieurs années aux Etats-Unis. C'est pourquoi nous entendons davantage parler des cyberattaques ayant lieu outre-Atlantique que celles se produisant près de chez nous.

Quels sont les principaux enseignements à en tirer ?
Au lieu de se concentrer uniquement sur la protection du périmètre de sécurité, les entreprises devraient plutôt adopter une approche segmentée, protégeant les données à tous les niveaux et barrant le passage aux hackers qui auraient franchi le 1er palier de défense. Cela signifie également que la priorité doit porter sur les données elles-mêmes et sur le fait qu'elles ne puissent être consultées ou utilisées par des personnes non autorisées. Protéger les données par des solutions de chiffrement de bout en bout, d'authentification et des contrôles d'accès permet d'ajouter un niveau de sécurité supplémentaire. En mettant en place des outils de chiffrement, les données subtilisées n'ont plus aucune valeur pour toute personne non autorisée. L'accès peut être sécurisé en utilisant des clés permettant aux personnes habilitées de consulter les informations. Ainsi, en cas d'attaque, les entreprises sont certaines de garantir la sécurité des données de leurs clients.

Informer les clients
Une fois ces mesures sécuritaires mises en place, il est important d'en informer les clients et de les rassurer quant à la pertinence des processus instaurés pour protéger leurs données. Si les entreprises peuvent démontrer qu'elles sont prêtes à se dépasser et à mettre toute leur énergie dans cette démarche, elles seront perçues comme innovantes et dignes de confiance.
La sécurité est un effort mutuel. S'il est important d'informer les clients sur le travail qui est fait pour assurer leur sécurité, il est tout aussi primordial qu'ils sachent comment se protéger eux-mêmes. De plus, s'adresser à un utilisateur averti permettra de lui proposer un meilleur service client.
L'adoption du nouveau règlement européen sur la protection des données donne aux entreprises la possibilité de prendre les devants et montrer dès à présent à leurs clients qu'elles prennent ce sujet très au sérieux. Elles ne doivent pas seulement se soucier d'être conformes ou pas, mais comprendre qu'il s'agit là d'une nécessité essentielle à leur réussite. Les utilisateurs sont de plus en plus conscients qu'ils confient des données sensibles aux entreprises, leur demandant, de fait, d'en être responsables. La montée en puissance de cette prise de conscience doit aller de pair avec un niveau d'exigence plus élevé vis-à-vis des structures hébergeant ces informations. Ne pas prendre ce sujet au sérieux pourrait non seulement être préjudiciable en cas d'attaque, mais également nuire à la confiance instaurée avec les clients. Perdre ce lien les incitera à se tourner vers des concurrents jugés plus fiables… [Lire la suite]

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Nouveau règlement européen sur la protection des données : priorité au chiffrement, à l'authentification et aux contrôles d'accès | Solutions Numériques*

Paypal ne protégera plus les transactions crowdfunding

	**Paypal ne protégera plus les transactions crowdfunding**

Trop d'arnaques au financement participatif ? Trop de remboursements pour des produits jamais livrés ? Paypal ne protégera plus les transactions crowdfunding à partir de la fin juin 2016.

Paypal semble ne plus apprécier les transactions bancaires entre ses utilisateurs et les projets lancés sur les portails de crowdfunding. Trop d'arnaques au Crowdfunding ? Á partir du 26 juin 2016, le géant de la finance, ne protégera plus les transactions effectuées sur les sites de financement participatif.
Trop d'arnaques au transactions crowdfunding ? Trop d'argent envolé sans le moindre produit/projet finalisé ? Bref, des problèmes se posent des deux côtés – vendeurs et acheteurs. Paypal ne veut tout simplement plus faire partie d'une équation qui le place au milieu des conflits. Par conséquent, vous pourrez toujours payer via Paypal, mais la structure financière n'assurera plus cette transaction. Elle sera à vos risques et périls.

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *ZATAZ Paypal ne protégera plus les transactions crowdfunding – ZATAZ*

Liberté de la presse en Ukraine: journaliste = terroriste?

Liberté de la presse en Ukraine: journaliste = terroriste?

Alors que le métier des journalistes travaillant dans des zones sensibles reste difficile et dangereux, le site ukrainien Mirotvorets soutenu par le député ukrainien Anton Guerachtchenko, conseiller du ministre de l'Intérieur, les compare à des « terroristes accrédités ». Une comparaison qui n'a pas manqué de semer le malaise.

Sputnik a recueilli les propos d'une des journalistes faisant partie de la liste, à savoir d'Anne Nivat, politologue, journaliste et écrivaine française auteure de plusieurs livres, spécialisée depuis près de seize ans dans des zones sensibles, dont la Tchétchénie, l'Irak, l'Afghanistan etc., parfois même clandestinement.
« Traiter ces journalistes — dont je fais partie — de « complices de terroristes » est une ineptie qui, pour moi, n'a aucun sens », a déclaré Mme Nivat dans une interview à Sputnik.
Et d'ajouter: « En tant que reporter de guerre couvrant depuis près de 20 ans des zones de conflit (Balkans, Tchétchénie, Asie centrale, Irak, Syrie et Afghanistan) en toute indépendance, je continuerai à le faire y compris en Ukraine, cela va sans dire ».

Liberté de la presse: l' »Ukraine tend à ressembler à la Turquie »
Cette opinion de la journaliste est étayée par le Pacte onusien sur les droits civils et politiques, ou la Convention européenne des droits de l'Homme, selon laquelle les travailleurs des médias ne devraient pas être poursuivis pour l'exercice de leurs fonctions professionnelles.

Le Conseil de l'Europe accuse Kiev et Ankara d'intimider les médias
Un des points les plus problématiques est que la publication des noms des journalistes pourrait être lourde de conséquences, car leur sécurité est mise en question: c'est juste après la publication des données personnelles d'Oles Bouzina par le site Mirotvorets que le journaliste ukrainien avait été assassiné.
Selon la porte-parole de l'Organisation pour la sécurité et la coopération en Europe (OSCE) pour la liberté des médias Dunja Mijatovic, certains journalistes de la liste ont déjà commencé à recevoir des menaces.
S'étant fixé pour objectif de lutter contre les « ennemis de l'Ukraine », le site ukrainien Mirotvorets (« le faiseur de paix » en ukrainien) a publié les données personnelles (numéro de téléphone, e-mail, nom du service de presse) de milliers de journalistes, dont une cinquantaine de Français et un millier d'occidentaux.
Toutes sortes d'agences de presse sont concernées, de toutes nationalités: CNN, ABC, Al-Jazeera, AFP, Reuters, RT, ZDF, RTL, Europe 1… [Lire la suite]

Réagissez à cet article

Source : *Liberté de la presse en Ukraine: journaliste = terroriste?*