Découvrez les techniques de persuasion utilisées par les cybercriminels

3

	**Découvrez les techniques de persuasion utilisées par les cybercriminels**

L**e rapport « Piratage de l'OS humain » d'Intel Security réalisé avec Europol révèle les techniques de persuasion utilisées par les cybercriminels ainsi que les méthodes de manipulations des hackers pour rendre les collaborateurs d'entreprises complices/acteurs d'actes de cybercriminalité.**

A titre de repère, les deux tiers des emails dans le monde sont des spams qui visent à extorquer des informations personnelles et confidentielles ainsi que de l'argent. Avec un coût global de la cybercriminalité estimé à 392 milliards d'euros par an, Intel Security encourage les entreprises à éduquer leurs collaborateurs face aux six leviers d'influence utilisés par les hackers. Une démarche soutenue par Europol pour limiter l'influence des hackers en europe de l'ouest

Publié quelques jours après la révélation d'une cyberattaque qui a touché plus de 100 banques à travers le monde et causé aux alentours de 900 millions d'euros de dégâts, ce rapport démontre toute l'importance d'une prise de conscience collective et souligne la nécessité d'éduquer les collaborateurs aux méthodes de persuasion appliqués par les hackers dans le monde numérique. Dans l'exemple cité, les attaques de phishing ciblées ont permis l'ouverture de brèches au sein de ces réseaux bancaires, démontrant ainsi la faiblesse intrinsèque du « pare-feu humain ». A titre de comparaison, l'étude Threat Report d'Intel Security a permis, en septembre dernier, de révéler que 92 % des employés français n'étaient pas en mesure d'identifier un courriel de phishing sur sept.

« L'analyse de nombreux cas d'usurpation de données nous montre qu'aujourd'hui, le facteur humain est le plus souvent la clé qui permet aux hackers d'agir. En les manipulant, ils les incitent à prendre des mesures qui facilitent l'infection des systèmes par des logiciels malveillants », commente Raj Samani, Directeur Technique EMEA d'Intel Security (photo)et conseiller auprès du Centre européen de lutte contre la cybercriminalité d'Europol.

« Aujourd'hui, les cybercriminels n'ont pas nécessairement besoin de savoir-faire technique pour atteindre leurs objectifs. Certains logiciels malveillants peuvent infecter les ordinateurs en y accédant directement par emails. Ces attaques ciblées manipulent les victimes et les incitent à ouvrir des pièces jointes, prétendument légitimes, ou à cliquer sur un lien qui semble provenir d'une source sûre », indique Paul Gillen, directeur des opérations du Centre Européen de lutte contre la cybercriminalité.

Sur l'année 2014, McAfee Labs a répertorié une augmentation spectaculaire du nombre d'URL malveillantes soit plus de 30 millions de liens suspects. Cette augmentation peut être attribuée à la fois à une forte hausse du nombre de liens de phishing ainsi qu'à une utilisation plus commune des URL courts qui cachent, souvent, des sites Web malveillants. Cette tendance est d'autant plus inquiétante que 18 % des utilisateurs visés par un email de phishing cliquent sur ce lien malveillant et deviennent ainsi victimes de la cybercriminalité.

Le rapport des 500 chercheurs du McAfee Labs pointe du doigt le fait que deux tiers des emails mondiaux sont des spams qui visent à soutirer des informations et de l'argent à leurs destinataires. Face à ce constat, il est d'autant plus important que les consommateurs et les collaborateurs d'entreprises soient informés des techniques de phishing et d'escroquerie couramment utilisées dans le monde numérique.

« Aujourd'hui, les cybercriminels sont devenus de très bons psychologues, capables de jouer sur le subconscient des employés en s'appuyant notamment sur un grand nombre de tactiques de « vente » souvent utilisées dans la vie quotidienne. Pour garder une longueur d'avance sur les cybercriminels et réduire le risque d'être l'une des victimes de la cybercriminalité, les entreprises doivent non seulement optimiser leurs processus et compter sur la technologie mais aussi former leurs personnels pour pallier à la brèche dans ce qu'on nomme 'l'OS humain' », conclut Raj Samani.

Il n'a jamais été plus important de former les individus à la sécurité et à la politique de leur entreprise en matière de protection des données. Paradoxalement, une étude récente publiée par Enterprise Management Associates1 a révélé que seulement 56 % des employés avaient suivi une formation à la politique de sécurité de l'entreprise. Pour mieux protéger les informations sensibles des consommateurs et des entreprises, le rapport « Piratage de l'OS humain » d'Intel Security détaille les techniques de persuasion le plus souvent utilisées par les cybercriminels :

Restez vigilent aux six leviers d'influence des cybercriminels dans le monde numérique :

Réciprocité des échanges : Les gens ont tendance à se sentir obligés de répondre une fois qu'ils reçoivent quelque chose.

Rareté de l'offre : Les individus sont motivés par l'obtention de ce qu'ils croient être une ressource rare ou une offre limitée dans le temps et peuvent ainsi s'exposer plus facilement au cybercrime. Par exemple, un faux courriel envoyé par une banque demandant à l'utilisateur d'accepter une demande suspecte afin d'éviter la désactivation de son compte dans les 24 heures peut avoir tendance à inciter au clic.

Cohérence des engagements : Une fois engagée dans une démarche, la victime choisit très souvent de tenir ses promesses pour rester cohérente et éviter de paraître peu voire non fiable. Par exemple, un pirate peut se présenter en tant qu'un membre de l'équipe SI de l'entreprise et, après avoir fait en sorte qu'un employé s'engager à respecter tous les processus de sécurité, lui demander d'effectuer une tâche suspecte sur son poste, qui semblerait être conforme aux exigences de sécurité.

Appréciation et amitié : Les tentatives d'hameçonnage sont plus productives lorsque le cybercriminel réussit à gagner la confiance de la victime. Pour endormir la méfiance, un pirate pourrait notamment essayer d'entrer en contact, soit par téléphone soit en ligne, et « charmer » au préalable sa victime potentielle.

Respect de l'autorité : Les gens ont tendance à se conformer à une figure d'autorité. Les directives dans un email prétendument envoyé de la part d'un PDG de l'entreprise sont plus susceptibles d'être suivies par un employé.

L'effet de masse : Les gens ont tendance à se conformer à la majorité. Par exemple, si un courriel de phishing est prétendument envoyé à un groupe de collègues, plutôt qu'à un seul destinataire, la victime potentielle de l'attaque se sent davantage rassurée et est plus susceptible de croire que l'email provient d'une source sûre.

Lire le rapport d'Intel Security : http://www.mcafee.com/us/resources/reports/rp-hacking-human-os.pdf

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

Source : http://www.informatiquenews.fr/les-techniques-de-persuasion-utilisees-par-les-cybercriminels-intel-security-30570
Par Enterprise Management Associates

Téléchargement illégal : un avertissement d’Hadopi, ça calme

Téléchargement illégal : un avertissement d’Hadopi, ça calme

Comme les années précédentes, la Hadopi estime, chiffres à l'appui, que la riposte graduée est efficace et agit sur les comportements – hormis l'achat de contenus légaux. Et non, les abonnés ne se sont pas réfugiés vers d'autres modes de téléchargement.

La question est posée depuis sa création – et l'était même avant : alors, Hadopi, efficace ou pas ? Et la réponse est toujours un peu la même. Durant un temps, l'Autorité a toutefois pu bénéficier du soutien – entier ou non – des ayants droit.
Désireux de voir le gouvernement durcir la législation à l'égard du téléchargement illicite, et de la transférer au CSA, ces derniers se montrent désormais plus acerbes quant aux résultats obtenus par la Hadopi et la riposte graduée. La toute récente étude de l'Alpa en est une bonne illustration.

10% des abonnés avertis une fois récidivent
Et celle qui défend le mieux le bilan de la Hadopi, c'est encore la Hadopi elle-même – sous une précédente majorité, elle pouvait en outre compter sur le soutien du ministre de la Culture. A l'occasion de la dernière publication des chiffres clés de la riposte graduée, la Haute Autorité en arrive donc cette année encore à la même conclusion : ça marche.
Ainsi sur les 8,9% de titulaires d'un abonnement à Internet ayant reçu un premier avertissement (entre octobre 2010 et juin 2014, soit plus de 3,2 millions d'emails envoyés), ils ne sont plus que 10,4% d'entre eux à avoir été avertis une deuxième fois – puis 0,4% à s'être retrouvés en phase 3.

Un abonné averti rentrerait donc dans le rang et cesserait de partager illégalement des contenus sur les réseaux P2P. Et selon la Hadopi, un autre chiffre souligne « le caractère dissuasif de la riposte graduée » : la part d'abonnés avertis contactant l'autorité. Ce taux de contact est de 43,5% en phase 3 et de 4,2% après la 1ère recommandation. Un avertissement ça va, trois bonjour les dégâts.

Avertis, 70% diminuent leur consommation illicite
Alors convaincu ? Pas encore ? Pour convaincre les sceptiques (et les autres), la Hadopi a commandé un sondage CSA auprès de 1059 français. Sur ce panel, 47 ont effectivement reçu un 1er avertissement, soit environ 4,4% d'entre eux – donc moins que les 8,9% d'abonnés français à Internet déjà avertis une fois depuis 2010.
Or 70% des destinataires d'un premier avertissement affirment avoir diminué leur « consommation illicite de biens culturels dématérialisés ». Et cette part grimpe même à 88% parmi les 9 français de l'échantillon avertis deux fois. Le sondage n'a pas étudié si cette diminution du téléchargement illicite était oui pérenne ou seulement provisoire.

En revanche, la Hadopi s'est intéressée à une possible évolution des usages en matière de consommation illicite. La riposte graduée ne portant que sur le P2P, les abonnés, en particulier ceux destinataires d'un avertissement, ne seraient-ils pas tentés d'utiliser d'autres moyens, dont le streaming ?

Pas plus de consommateurs ?
D'après les résultats du sondage, la réponse est majoritairement non (73%). D'ailleurs, toujours pour la Hadopi, l'audience, plutôt en baisse des sites de téléchargement (P2P, DDL et streaming), confirmerait cette analyse.
Mais si les internautes ne cherchent a priori pas le moyen de continuer à consommer des contenus piratés, ils ne se précipitent pas non plus sur l'offre légale. Dommage puisqu'il s'agissait d'un des objectifs recherchés par la loi. Après un avertissement, ils sont 23% à déclarer se tourner vers une offre légale.

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

Source : http://www.zdnet.fr/actualites/telechargement-un-avertissement-d-hadopi-ca-calme-39803911.htm
Par Christophe Auffray

Panorama 2015 des menaces informatiques

	**Panorama 2015 des menaces informatiques**

McAfee, filiale d'Intel Security, publie son nouveau rapport annuel, intitulé '2015 Threats Prediction', qui met l'accent sur les principales menaces prévues pour l'année 2015. McAfee présente conjointement son rapport 'November 2014 Threat Report' relatif à l'analyse des menaces informatiques du dernier trimestre 2014.

Les prévisions 2015 de McAfee en matière de menaces :
1. Une fréquence accrue du cyber-espionnage. La fréquence des attaques de cyber-espionnage continuera d'augmenter. Les pirates actifs de longue date mettront en place des techniques de collecte des informations toujours plus furtives, tandis que les nouveaux venus chercheront des solutions pour subtiliser de l'argent et perturber les activités de leurs adversaires.
Les cyber-espions actifs de longue date travailleront à parfaire des méthodes toujours plus efficaces pour demeurer cachés sur les systèmes et les réseaux de leurs victimes. Les cybercriminels continueront à agir davantage comme des cyber-espions, en mettant l'accent sur les systèmes de surveillance et la collecte de renseignements sensibles relatifs aux individus, à la propriété intellectuelle et à l'intelligence opérationnelle. McAfee Labs prévoit que la cyberguerre sera davantage utilisée par les plus petits États et les groupes terroristes.

2. Attaques fréquentes, profitables et sévères envers l'Internet des objets. A moins d'intégrer le contrôle de la sécurité dès la conception des produits, le fort déploiement de l'IdO devrait dépasser les priorités de sécurité et de confidentialité. La valeur croissante des données pouvant être recueillies, traitées et partagées par ces dispositifs devrait attirer leurs premières attaques en 2015.
La prolifération croissante des appareils connectés dans des environnements tels que la santé pourrait également fournir aux logiciels malveillants un accès à des données personnelles plus sensibles que les données relatives aux cartes de crédit. En effet, selon le rapport de McAfee Labs intitulé « Cybercrime Exposed : Cybercrime-as-a-Service », chacune de ces données représenterait un gain d'environ 10 $ pour un cybercriminel, soit 10 à 20 fois la valeur d'un numéro de carte de crédit américaine volé.

3. Les débats autour de la vie privée s'intensifient. La confidentialité des données sera toujours menacée, dans la mesure où les pouvoirs publics et les entreprises peinent à déterminer ce qui constitue un accès équitable et autorisé à des « informations personnelles » mal définies.

En 2015, les discussions vont se poursuivre pour définir ce que sont les « informations personnelles » et dans quelle mesure elles peuvent être accessibles et partagées par des acteurs étatiques ou privés. Nous allons voir une évolution de la portée et du contenu des règles de la protection des données ainsi que des lois de réglementation de l'utilisation de l'ensemble de données préalablement anonymes. L'Union Européenne, les pays d'Amérique latine, ainsi que l'Australie, le Japon, la Corée du Sud, le Canada et bien d'autres pays adopteront des lois et des règlements de protection des données plus strictes.

4. Les ransomwares évoluent dans le Cloud. Les logiciels de demande de rançon (ransomware) connaîtront une évolution dans leurs méthodes de propagation, de chiffrement et de cibles visées. McAfee Labs prévoit également que de plus en plus de terminaux mobiles essuieront des attaques.

Une nouvelle variante de ransomware capable de contourner les logiciels de sécurité devrait aussi faire son apparition. Elle ciblera spécifiquement les terminaux dotés de solutions de stockage dans le Cloud. Une fois l'ordinateur infecté, le ransomware tentera d'exploiter les informations de connexion de l'utilisateur pour ensuite infecter ses données sauvegardées dans le Cloud. La technique de ciblage du ransomware touchera également les terminaux qui s'abonnent à des solutions de stockage dans le Cloud. Après avoir infecté ces terminaux, les logiciels de ransomware tenteront d'exploiter les informations de connexion au Cloud. McAfee Labs s'attend à une hausse continue des ransomwares mobile, utilisant la monnaie virtuelle comme moyen de paiement de la rançon.

5. De nouvelles surfaces d'attaque mobiles. Les attaques mobiles continueront d'augmenter rapidement dans la mesure où les nouvelles technologies mobiles élargissent la surface d'attaque.
L'émergence de kits de génération de logiciels malveillants sur PC et la distribution de code source malveillant pour mobile permettront aux cybercriminels de désormais cibler ces appareils. Les app stores frauduleux continueront d'être une source importante de malwares sur mobile. Le trafic engendré par ces boutiques d'applications sera notamment conduit par le 'malvertising', qui s'est rapidement développé sur les plateformes mobiles.

6. Les attaques dirigés contre les points de vente augmentent et évoluent avec les paiements en ligne. Les attaques dirigées contre les points de vente demeureront lucratives et l'adoption croissante par le grand public des systèmes de paiement numérique sur appareils mobiles offrira aux cybercriminels de nouvelles surfaces d'attaque à exploiter.

Malgré les efforts des commerçants de déployer des cartes à puce et à code PIN, McAfee Labs prévoit pour 2015 une hausse significative des failles de sécurité liés aux points de vente. Cette prédiction est notamment basée sur le nombre de dispositifs de points de vente devant être upgradés en Amérique du Nord. La technologie de paiement sans contact (NFC) devrait devenir un nouveau terrain propice à de nouveaux types d'attaques, à moins que les utilisateurs ne soient formés au contrôle des fonctions NFC sur leurs appareils mobiles.

7. Logiciels malveillants au-delà de Windows. Les attaques de logiciels malveillants ciblant des systèmes d'exploitation autres que Windows exploseront en 2015, stimulées par la vulnérabilité Shellshock.

McAfee Labs prévoit que les conséquences de la vulnérabilité Shellshock seront ressenties au cours des années à venir par les environnements Unix, Linux et OS X, notamment exécutés par des routeurs, des téléviseurs, des systèmes de contrôle industriels, des systèmes de vol et des infrastructures critiques. En 2015, McAfee Labs s'attend à une hausse significative des logiciels malveillants non-Windows dans la mesure où les hackers chercheront à exploiter cette vulnérabilité.

8. Exploitation croissante des failles logicielles. Le nombre de failles décelées dans des logiciels populaires continuant d'augmenter, les vulnérabilités enregistreront une forte hausse.

McAfee Labs prévoit que l'utilisation de nouvelles techniques d'exploitation telles que la falsification de pile (stack pivoting), la programmation orientée retour (RDP, Return Oriented Programming) et la programmation orientée saut (JOP, Jump-Oriented Programming), combinées à une meilleure connaissance des logiciels 64 bits, favorisera l'augmentation du nombre de vulnérabilités détectées, suivi en cela par le nombre de logiciels malveillants exploitant ces nouvelles fonctionnalités.

9. De nouvelles tactiques d'évasion pour le sandboxing. Le contournement du sandbox deviendra un problème de sécurité informatique majeur.

Des vulnérabilités ont été identifiées dans les technologies d'analyse en environnement restreint (sandboxing) mises en œuvre avec les applications critiques et populaires. McAfee Labs prévoit une croissance du nombre de techniques visant à l'exploitation de ces vulnérabilités ainsi que le contournement des applications de sandboxing. Aujourd'hui, un nombre significatif de familles de logiciels malveillants parviennent à identifier les systèmes de détection de type sandbox et à les contourner. A ce jour, aucun logiciel malveillant en circulation n'est parvenu à exploiter des vulnérabilités de l'hyperviseur pour échapper à un système de sandbox indépendant. Il pourrait en être autrement en 2015.

Pour lire le rapport 'McAfee Labs – Threat Report' dans son intégralité, cliquez ici : http://mcaf.ee/ojbsz

Retour sur 2014
Durant le troisième trimestre 2014, McAfee Labs a détecté plus de 307 nouvelles menaces par minute, soit plus de 5 chaque seconde, avec une croissance des logiciels malveillants sur mobile en hausse de 16 % sur le trimestre, soit une croissance annuelle de 76 %. Les chercheurs de McAfee Labs ont également identifié de nouvelles tentatives visant à tirer profit des protocoles de sécurité Internet, notamment les vulnérabilités de protocoles SSL tels que Heartbleed et BERserk, ainsi que l'abus répété des signatures numériques pour masquer les malwares comme étant légitimes.

Pour 2015, McAfee Labs alerte sur les techniques de cyber-espionnage des pirates informatiques et prévoit que les hackers actifs de longue date mettront en place des techniques de collecte de données confidentielles toujours plus furtives au travers d'attaques ciblées étendues. Les chercheurs du Labs prévoient ainsi de mettre davantage d'efforts sur les vulnérabilités liées à l'identification d'applications, de systèmes d'exploitation et au réseau, ainsi que sur les limites technologiques du sandboxing, dans la mesure où les hackers tentent de se soustraire à l'application de détection par hyperviseur.

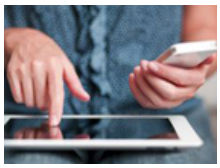
« L'année 2014 restera dans les mémoires comme l'année où la confiance en matière de sécurité informatique a été ébranlée », déclare David Grout, directeur Europe du Sud de McAfee, filiale d'Intel Security. « Les nombreux vols et pertes de données ont altéré la confiance de l'industrie envers le modèle d'Internet ainsi que celle des consommateurs dans la capacité des entreprises à protéger leurs données. La confiance des entreprises, ainsi que celle des organisations, ont également étaient impactées et les a poussé à s'interroger sur leur capacité à détecter et à détourner les attaques dont elles ont été la cible », poursuit David Grout. « En 2015, l'industrie d'Internet devra se renforcer pour restaurer cette confiance, mettre en place de nouvelles normes pour s'adapter au nouveau paysage des menaces et adopter de nouvelles stratégies de sécurité qui requièrent de moins en moins de temps dans la détection des menaces. Ainsi, nous devons tendre à un modèle de sécurité intégrée dès la conception de chaque appareil. »

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

Source : http://www.globalsecuritymag.fr/McAfee-Labs-dresse-le-panorama,20141210,49364.html

---

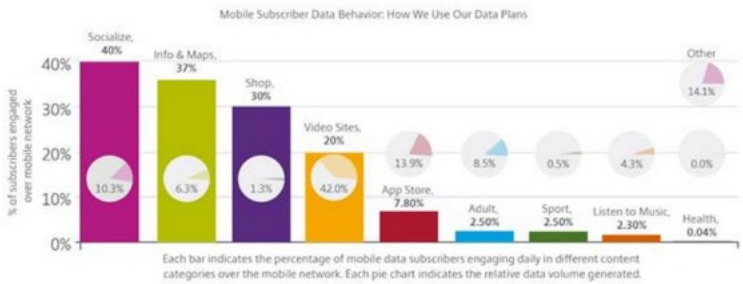
Le porno devient le 6e usage depuis un smartphone



Le porno devient le 6e usage depuis un smartphone

Si les réseaux sociaux et l'information sont en tête des usages, les contenus « pour adultes » se classent devant la musique et la santé, selon une étude de Citrix.

Une nouvelle étude sur les usages depuis un smartphone confirment les grandes tendances que l'on connaissait déjà. Ainsi, selon le dernier rapport de Citrix sur la question (basé sur le trafic 3G/4G dans le monde), les abonnés utilisent principalement leurs terminaux pour se connecter aux réseaux sociaux (40%), pour s'informer et consulter des cartes (37%) et réaliser des achats en ligne (30%).
Derrière ce trio inamovible, on trouve la consommation de vidéos (20%), les visites dans les app stores (7,8%) et désormais les contenus adultes qui se hissent à 2,5% des mobinautes, et qui passent devant la musique (2,3%).



Si cette part peut paraître marginale, le trafic généré l'est beaucoup moins. Toujours selon Citrix, le porno représente 8,5% du trafic, contre 4,3% pour la musique ou 13% pour le shopping. Dans ce domaine, la vidéo représente 42% des données mobiles générées.

Le spécialiste confirme également que le très haut débit mobile (4G) incite à consulter des contenus riches. « Il y a 1,5x plus de requêtes de vidéos sur les réseaux 4G que sur les réseaux 3G. La résolution des vidéos mobiles augmente de 20% sur les réseaux 4G par rapport à la 3G. Cela implique une augmentation du nombre de données générées, 5x plus élevé sur les réseaux 4G que sur la 3G », peut-on lire.

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

Source : http://www.zdnet.fr/actualites/le-porno-devient-le-6e-usage-depuis-un-smartphone-39805969.htm

---

Sécurité des données : Quid des risques liés aux nouveaux

usages ?

Sécurité des données : Quid des risques liés aux nouveaux usages ?

Une étude Hiscox/IFOP révèle que si 3/4 des actifs interrogés se considèrent bien sensibilisés à la protection des données professionnelles, une majorité d'entre eux ont toujours des pratiques risquées… Pourquoi ?

C'est un fait, les appareils mobiles sont complètement intégrés au sein des entreprises et les frontières entre le professionnel et le privé s'en trouvent fortement diminuées. Qu'en est-il de la sécurité des données des entreprises ? Hiscox s'est interrogé sur le sujet avec l'institut IFOP et les résultats sont pour le moins surprenants !

La sécurité des entreprises est exposée

Les salariés équipés d'au moins un appareil mobile professionnel sont les plus concernés par ces pratiques risquées puisqu'ils sont 77% à déclarer transporter des fichiers professionnels sur une clé USB ou un disque dur externe (contre 63% pour l'ensemble) et la moitié partage des fichiers en ligne via un service de cloud (contre 39% pour l'ensemble). 54% estiment que le partage de fichiers via le cloud n'a pas d'incidence sur la sécurité.
Si les salariés des petites structures sont les mieux équipés en appareils mobiles, ce sont ceux qui utilisent le plus leur matériel professionnel à titre personnel. 82% des salariés de ces entreprises se connectent à Internet au moins une fois par semaine pour des raisons personnelles à partir de leur appareil professionnel.

Des techniques de sécurisation non adaptées

Mais ce n'est pas tout ! Pour assurer leur protection, 9 entreprises sur 10 s'appuient sur un mot de passe. Et là, tout commence, 18% des actifs doivent changer leur mot de passe tous les mois alors que 34% déclarent devoir le changer moins de 2 fois par an. Quant à l'élaboration du mot de passe, 70% des entreprises imposent au moins une règle à leurs salariés pour le choix du mot de passe, on arrive à 51% dans les structures de moins de 10 salariés.
Parmi les autres techniques, 35% des actifs interrogés déclarent disposer d'outils de cryptage des données mais 22% ne savent pas s'ils peuvent bénéficier de cette technique dans leur entreprise.

Enfin, 63% laissent leur ordinateur allumé lorsqu'ils quittent le bureau en fin de journée ou ne le verrouillent pas en quittant leur poste.

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

Source : http://www.itpro.fr/n/securite-donnees-quid-risques-lies-nouveaux-usages-20899/

Le nombre d’incidents de sécurité informatique a augmenté de 48% en 2014 !

Le nombre d’incidents de sécurité informatique a augmenté de 48% en 2014 !

D’après l’enquête The Global State of Information Security Survey, le nombre d’incidents de sécurité informatique dans le monde a augmenté de 48 % cette année.

C’est à l’instigation de PwC, CIO et CSO que le sondage The Global State of Information Security Survey a été réalisé auprès 9700 chefs de direction et gestionnaires en finances, en informatique et en sécurité informatique dans le monde, 35% en Amérique du Nord, 34% en Europe, 14% de l’Asie-Pacifique, 13% d’Amérique du Sud et 4% du Moyen-Orient et d’Afrique.

Publiés ce jeudi, les résultats sont que le nombre d’incidents de sécurité informatique à l’échelle internationale a augmenté de 48% en 2014 pour atteindre près de 43 millions d’incidents, soit un peu plus de 117 000 attaques par jour.

Alors que ce chiffre donne déjà des frissons, il est estimé que plus de 70% des incidents informatiques ne sont pas détectés en raison des méthodes de plus en plus sophistiquées qui sont utilisées par leurs auteurs.
Ce constat a vraiment de quoi inquiété vu qu’il est estimé que le coût global de la cybercriminalité cette année dépasse les 23 milliards de dollars, et cela uniquement pour les incidents détectés. Le coût global réel des atteintes à la sécurité informatique est « impossible à établir » selon les auteurs de l’enquête. En soulignant qu’il est particulièrement difficile de chiffrer la valeur de certains types d’informations, par exemple la propriété intellectuelle et les secrets commerciaux.
L’enquête révèle par ailleurs qu’un tiers des incidents sont imputables aux employés, un autre tiers aux ex-employés et un quart aux pirates informatiques. Les attaques des États, le crime organisé et de la concurrence font partie des incidents les moins fréquents.

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

Source : http://www.linformatique.org/le-nombre-dincidents-de-securite-informatique-augmente-de-48-en-2014/

Les e-commerçants ciblés par les attaques des cybercriminels

Les e-commerçants ciblés par les attaques des cybercriminels

Selon un rapport d'Imperva réalisé en octobre 2014, les e-commerçants sont les plus souvent ciblés par les cyber-attaques. Les attaques seraient plus nombreuses, mais également plus longues. 48 % des attaques cibleraient directement des applications web des e-commerçants, mais les institutions financières sont également concernées.

Les données des e-commerçants visées par les hackers

Les chiffres sont issus du rapport Web Application Attack Report (WAAR), réalisé par l'Application Defense Center (ADC) d'Imperva. Selon l'équipe du spécialiste de la sécurité informatique, près d'une attaque sur deux cible les e-commerçants, et notamment leurs applications web. 40 % des attaques par injection SQL et 64 % des campagnes de trafic http malveillant concernent les sites de commerce en ligne.

D'après l'équipe ADC, le système de gestion de contenu WordPress est également souvent visé par les attaques. Pour Imperva, l'audience des sites est un critère de choix pour les hackers : « quand une application web ou une plateforme devient populaire, les hackers savent que le retour sur investissement d'une attaque sur ces supports sera intéressant pour eux, ils passent donc plus de temps à les explorer, soit pour voler des données soit pour utiliser les systèmes comme bots », estime le rapport WAAR.
Selon l'enquête d'Imperva, les sites de commerce en ligne sont attaqués deux fois plus souvent que des sites plus classiques. Les attaques durent aussi plus longtemps : près de deux fois plus longtemps qu'en 2013.
« Les e-commerçants doivent prendre ces menaces de cyber-attaque très au sérieux », soutient Amichai Schulman, directeur de la technologique pour Imperva, qui évoquent le verrouillage des bases de données et leur cryptage.
En France, la Fevad (Fédération du e-commerce et de la vente à distance) et Médiamétrie estiment que les consommateurs vont se tourner en masse vers les achats en ligne pour Noël 2014. 68% des internautes envisagent un achat sur internet d'ici la fin de l'année.

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

Source : http://www.commentcamarche.net/news/5865731-les-e-commercants-cibles-par-les-attaques-des-cybercriminels

---

Il y a désormais plus d'un

milliard de sites Web en ligne…

Il y a désormais plus d’un milliard de sites Web en ligne…

Chiffre symbolique, le Web qui a fêté ses 25 ans en mars viendrait de passer le cap du milliard de sites Web en ligne. En revanche, on ne sait pas combien sont à l’abandon…

Il y a eu les pages perso, puis les blogs, puis les Myspace, Tumblr et autres espaces personnalisés, petits bouts de 0 et de 1, colonisés à la sueur du clavier. Le Net et le Web sont des espaces d’expression jamais vus auparavant et leur succès est colossal, à l’échelle de l’humanité.

25 ans et toutes ses dents

Selon le site spécialisé Internet Live Stats, il y a désormais plus d’un milliard de sites Web, et ce chiffre augmente en permanence, selon les derniers relevés établis en temps réel mardi. Le Web a fêté ses 25 ans en début d’année et le compteur d’internetlivestats.com indiquait que la toile comptait plus d’1,06 milliard de sites mercredi peu avant minuit.

L’idée du Web, interface « graphique » du Net, a été développée dans les années 1980 par le Britannique Tim Berners-Lee, qui n’était alors qu’un jeune ingénieur en informatique dans un laboratoire de physique en Suisse. Il a présenté son idée par écrit le 12 mars 1989, un jour en général considéré comme la date de naissance du Web. Les militaires américains avaient étudié l’idée de connecter des ordinateurs en réseau dans les années 1950, et avaient lancé Arpanet en 1969, une sorte de précurseur d’Internet.

Le Web a gagné son premier milliard à seulement 25 ans…

Explosion de l’information

Mais grâce au système de « Sir Tim », aujourd’hui âgé de 59 ans, les gens ont été en mesure de publier ce qu’ils souhaitaient sur des ordinateurs reliés entre eux par internet, ouvrant la porte à un gigantesque partage d’informations et à une explosion du nombre de sites.

Des moteurs de recherche comme Yahoo! ou Google ont ensuite été créés pour aider les internautes à trouver les pages qui les intéressaient parmi la profusion d’informations postées. Ainsi, rien que pour la journée du mardi 16 septembre 2014, Google a enregistré plus de 3,1 milliards de recherches sur ses serveurs selon internetlivestats.com. Et près de 170 milliards d’e-mails avaient aussi été envoyés au cours des dernières 24 heures.

Tout n’est pas vert…

Toujours selon le compteur d’internetlivestats.com, la barre des 3 milliards d’internautes devrait aussi être franchie prochainement. Le revers de la médaille est que l’électricité consommée pour faire fonctionner internet a généré au moins 2,17 millions de tonnes de dioxyde de carbone (CO2) rejetées dans l’atmosphère rien que pour la journée de mardi, selon internetlivestats.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :

http://www.01net.com/editorial/626966/il-y-a-desormais-plus-d-un-milliard-de-site-web-en-ligne/#?xtor=EPR-1-NL-01net-Actus-20140917