Sécurité Informatique

N°333
6 Juillet 2010
24ème année

PUBLI NEWS

Sécurité Informatique **souhaite de bonnes vacances à ses lecteurs et leur donne rendez-vous dans son numéro 334 daté du 24 août 2010**

SOMMAIRE

www.publi-news.fr

VIRUS

G Data Software AG : « Nos produits font preuve d'une détection de virus exceptionnelle »


Eddy Willems

Editeur à part dans un paysage « trusté » par des leaders d'origine américaine, l'Allemand G Data fait figure d'exception dans le monde des éditeurs de solutions antivirus. Avec une gamme de produits souvent classés dans le haut de gamme des tests techniques menés par des organismes indépendants, G Data tente de se frayer un chemin. En charge de la communication technique du G Data SecurityLabs, Eddy Willems, 'security evangelist' assure la représentation de l'éditeur de sécurité dans les évènements internationaux. Pendant plus de 20 ans, il a collaboré avec des instituts influents, tels que l'EICAR ou différentes associations CERT. Il a également travaillé chez NOXS ou Kaspersky Labs Benelux. Dans cette interview, il partage la vision de G Data sur les questions de sécurité.

- Dans de nombreux tests indépendants d'antivirus, les logiciels G Data obtiennent d'excellentes notes, voire les meilleures. C'est ,entre autres, le cas avec les tests de Virus Bulletin ou d'AV Comparatives. A quoi attribuez-vous ces résultats ?

Dans de nombreux tests indépendants, les solutions G Data font en effet preuve d'une détection de virus exceptionnelle. Ils montrent une capacité de réaction extrêmement rapide face aux nouveaux virus. Ils utilisent des méthodes modernes de détection de virus inconnus, basées sur l'analyse comportementale et heuristique ou encore le Cloud Security. L'une des clés de ces performances est l'utilisation de la technologie 'double scan' qui repose sur deux moteurs antivirus indépendants l'un de l'autre. Basée sur les moteurs d'Alwil Software et de BitDefender, cette technologie repose sur le principe selon lequel l'exploitation de deux moteurs d'analyse des virus permet de pallier les faiblesses éventuelles de l'un par l'autre. En permettant de contrecarrer la diffusion des virus le plus tôt possible, le double scan permet un taux de détection de plus de 99%. En cas de détection d'une charge virale, le fichier est traité (éradication, mise en quarantaine, etc.) et l'analyse reprend son cours. Le deuxième moteur ne s'active que si le premier n'a rien trouvé. Nous faisons évoluer cette technologie en permanence en termes d'optimisation et de rapidité grâce à la mise en cascade, la protection contre les coupures logicielles ou la restauration des anciennes signatures. La fonction préventive OutbreakShield assure une protection immédiate contre les nouveaux virus. Elle bloque les e-mails infectés et dont la signature virale est inconnue avant qu'ils n'atteignent le disque dur ou la mémoire du PC.
Dans les versions 2011 de nos produits, que nous venons d'annoncer, l'utilisation des technologies d'empreintes et des listes blanches intelligentes est encore plus poussée, la vitesse d'analyse a été optimisée, les besoins en mémoire réduits, d'où une protection accrue contre les virus, les logiciels espions et l'hameçonnage. Toutes les fonctions de protection s'exécutent de façon automatique en arrière plan.

- Comment expliquez-vous alors les mauvaises notes obtenues au dernier test de l'ESIEE ?

Ces tests ne correspondent pas à des situations réelles, c'est pourquoi les ingénieurs de cette école arrivent à contourner les moteurs de tous les logiciels AV du marché. Nous n'allons pas modifier nos produits pour prendre en compte les résultats de ce test. Nous estimons être bien placés dans la plupart des tests réels, y compris ceux de l'Amtso.org.

- Vos laboratoires ont procédé récemment à l'analyse du spam «pharmacie». Qu'en avez-vous retiré de significatif ?

Nous avons en effet analysé en avril dernier une vague de spam «pharmacie». Nous avons constaté que ce spam se cache de plus en plus derrière des sujets d'actualités. Et tous les sujets sont bons pour piéger l'in-

ternaute. Les activités du volcan islandais Eyjafjallajoekull étaient à la une des journaux. Elles faisaient aussi le bonheur du spam qui reprenait les titres les plus accrocheurs dans ses objets. Tous les sujets d'actualité sont aujourd'hui utilisés pour contourner les systèmes de filtrage. Ainsi, 900 spams en apparence différents se sont révélés finalement très proches. Le spam prend la forme d'une newsletter émise par MSN. Le corps du texte est identique et les adresses mails utilisées sont toutes russes (extension.ru). Les similitudes s'arrêtent là. Sur les 900 courriels collectés, aucun n'a le même objet. Et tous tournent autour de l'actualité. Les liens intégrés dans ces courriels pointent tous vers un même site, «Canadian Pharmacy». Plusieurs domaines sont utilisés. Tous ont été enregistrés il y a quelques jours par l'intermédiaire de 4 sociétés chinoises.

- Estimez-vous que l'internaute qui surfe exclusivement sur des sites français, ce qui est le cas le plus répandu, ne risque rien en fin de compte ?

Il est exact que beaucoup d'internautes francophones surfent exclusivement sur des sites en français et mettent automatiquement à la corbeille tous les courriels qu'ils reçoivent en langues étrangères. Pour définir quel risque réel prend ce type d'internaute lorsqu'il navigue sur Internet et reçoit des courriels, nous avons mené une étude sur trois mois et recensé les pages Internet dangereuses en langue française ou comportant dans leurs adresses l'extension.fr.

Un des premiers points à noter est le nombre croissant de sites Internet français hébergeant de l'hameçonnage et des malwares. 42 % des pages collectées sont liées à un site existant de langue française (adresses .fr). Il s'agit pour la plupart de sites de particuliers, d'associations, de clubs sportifs ou de petites entreprises. Gérés par des administrateurs non spécialisés, ces sites sont souvent mal sécurisés et représentent un terreau productif où les cybercriminels viennent semer leurs malwares. Par ailleurs, les pages d'hameçonnage en français constituent la plus grande part de la collecte (92 %). L'hameçonnage, qui avait longtemps épargné les internautes francophones, représente désormais la majorité des attaques. Les utilisateurs de PayPal sont la cible n° 1 des cybercriminels. Les courriels d'hameçonnage en français liés à PayPal sont en effet très courants. Les liens insérés dans ces courriels pointent vers de faux sites Internet. Dans le secteur de l'hameçonnage, les fausses pages prenant pour cible les utilisateurs francophones de PayPal représentent une écrasante majorité (67 %). Ces pages en langue française sont liées à des courriels d'hameçonnage. Ils invitent les utilisateurs à se connecter à leur compte pour effectuer diverses actions (vérification des débits suite à une «charge inhabituelle» sur la carte bancaire, réinitialisation des mots de passe…). Les coordonnées des comptes PayPal saisies sur ces fausses pages web sont automatiquement volées à leur propriétaire afin d'y récupérer l'argent stocké. Cette forte proportion de sites d'hameçonnage liés à PayPal s'explique par l'intérêt de ce type de système pour l'économie cybercriminelle. Un compte PayPal volé peut avoir de multiples usages, tels que le transfert d'argent ou l'escroquerie sur des sites de ventes aux enchères. Dans un registre équivalent, les faux sites eBay représentent 3 % des pages françaises dangereuses. Les sites eBay et PayPal, sont une combinaison idéale pour tout cybercriminel souhaitant escroquer des internautes. Bien sûr, les organismes français faisant l'objet d'usurpation (banques et organismes d'états) représentent 11 % des dangers susceptibles d'être rencontrés par des internautes francophones. Durant la période de l'étude, le site de la Caisse d'Allocation Familiale et celui de la Caisse d'Épargne ont connu une attaque d'hameçonnage

significative. Notons que les pages d'hameçonnage d'organismes français sont peu présentes sur des adresses .fr. Pour allonger le délai de blocage de ces pages frauduleuses et complexifier d'éventuelles enquêtes policières, le stockage de ces pages sur des sites étrangers est privilégié par les cybercriminels. C'est ainsi que 9 % des adresses recensées et comportant l'extension .fr renferment des pages d'hameçonnage étrangères.

- Avez-vous trouvé d'autres codes malveillants sur l'Internet francophone ?
Les pages Internet françaises infectées par des malwares représentent avec un taux de 8 % une faible part des dangers. Un point encourageant pour les internautes francophones, mais qui doit tout de même être relativisé, car les techniques d'infection utilisées rendent difficile une collecte exhaustive. Peu de cybercriminels optent en effet pour une insertion pure et simple de code malveillant dans les pages Internet. En pratique, une fois le serveur Web contrôlé, le chargement du code nuisible à partir d'un autre serveur (via IFRAME ou SCRIPT, par exemple) est souvent envisagé. Une autre possibilité consiste à modifier les publicités des pages Web. Ces pages généralement mises à jour via IFRAME sont détournées. Ces deux techniques d'infection sont plus difficilement détectables, car elles permettent d'infecter un site Internet de manière aléatoire. Comme une bannière classique, son contenu peut provenir de plusieurs serveurs. Il en résulte ainsi une alternance entre page saine et page infectée. Dans le panel étudié, 87 % des pages web infectées l'étaient par iFrame...

- Selon vous, la condamnation d'Albert Gonzales sonne-t-elle le glas du vol de données de cartes bancaires ?
Le trafic de fausses cartes bancaires est un marché très rentable pour les cybercriminels. Hélas, la lourde condamnation d'Albert Gonzales à 20 ans de prison pour vol de données de 130 millions de cartes de crédit ne met pas un terme à ce type de trafic. Techniquement, de telles attaques sont encore possibles. Les méthodes utilisées entre 2005 et 2008 par Albert Gonzalez sont encore très souvent exploitées par les cybercriminels. Ainsi, les réseaux Wi-Fi omniprésents dans les entreprises constituent des points d'attaques privilégiés : mal protégés, ils ne tiennent que quelques minutes face à une attaque. Quant à l'injection SQL, l'attaque de bases de données accessibles via Internet, elle reste une autre porte d'entrée très courante vers les réseaux des entreprises et leurs données clients. Si bien que, malgré de nombreux développements pour sécuriser les réseaux et les bases de données, il reste encore des possibilités pour lancer des attaques ciblées contre des entreprises qui conservent les coordonnées bancaires de leurs clients. Dans le cas d'une base de données SQL par exemple, une bonne protection est souvent le résultat de développements internes. Et dans ce cas, omissions et erreurs de programmations sont toujours possibles. Voilà pourquoi le marché de la carte bancaire volée continue d'attirer des hackers et qu'il s'organise autour de centaines de sites et de boutiques en ligne où tout le nécessaire au «carding» - la fraude à la carte bancaire - est disponible. Les données d'une carte se négocient entre 2 € et 300 €, prix fonction de la quantité d'information disponible avec la carte (date, coordonnées de l'utilisateur…).

- Etes-vous présents sur le marché des entreprises ? Y avez-vous des références ?
Nos produits se démarquent de la concurrence par leur simplicité d'utilisation. Pour les petites entreprises, qui n'ont pas toujours les ressources d'un service informatique pour installer des outils antivirus et les administrer, c'est un avantage réel. Parmi nos clients dans ce cas de figure, nous comptons la Mutuelle Nationale des Sapeurs Pompiers (MNSP). Cette dernière a choisi G Data Antivirus Entreprise 9.0 pour remplacer sa précédente solution antivirale et sécuriser un parc hétérogène de 65 postes dont 10 serveurs et 6 postes itinérants. G Data Antivirus Entreprise intègre également les clients Linux, ce qui représentait une exigence de la part de la MNSP. Dès l'implémentation, nous avons détecté le ver Conficker et l'avons éradiqué. Le double moteur, les résultats lors des tests comparatifs et la simplicité d'utilisation ont été déterminants pour cette PME.
http://www.gdata.fr

Propos recueillis par Jo COHEN

GESTION DES RISQUES

Les entreprises évoluent mais trop lentement face à l'ampleur des risques, selon le Clusif

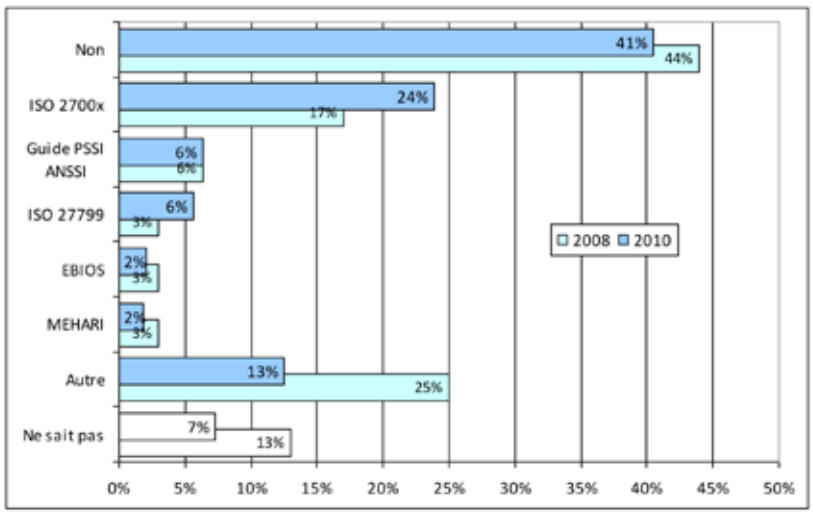
L'étude biennale du Clusif « Menaces informatiques et pratiques de sécurité » confirme une prise en compte progressive des enjeux de la sécurité informatique chez les acteurs économiques et dans une moindre mesure, chez les particuliers. Pour autant, des politiques globales de sécurité, décrétées au plus haut niveau de l'entreprise, restent à produire. Compte tenu du nombre et de la diversité des attaques, une riposte adaptée tarde toujours à venir. Les explications de Lionel Mourer en charge du pilotage de l'étude Clusif et responsable de la partie « Entreprises », et par ailleurs directeur du cabinet spécialisé ESR Consulting.

Enquête de référence réalisée tous les deux ans, par la taille et la représentativité des échantillons d'entreprises (350 entreprises ont répondu) et d'hôpitaux (151 établissements ont répondu) interrogés, le travail supervisé par les experts du Clusif, passe en revue l'ensemble des 11 thèmes de la norme ISO 27002 à la sécurité des systèmes d'information. Intérêt supplémentaire de cette année : l'étude comporte un volet consacré aux pratiques des particuliers utilisateurs d'Internet à domicile (1.000 répondants se sont exprimés sur le sujet). Premier aspect : la situation dans les entreprises françaises, de plus en plus souvent la cible d'attaques informatiques de types (virus, trojans avec une forte hausse des attaques dites man-in-the-middle) « Avec un sentiment de dépendance à l'informatique toujours en hausse, les entreprises continuent d'avancer dans la prise en compte de la sécurité des systèmes d'information, la SSI, explique Lionel Mourer en charge du pilotage de l'étude Clusif et responsable de la partie « Entreprises », et par ailleurs directeur du cabinet spécialisé ESR Consulting. Malgré des progrès bien réels, les changements concrets se font toujours selon la politique des petits pas. La prise en comptede la SSI est de plus en plus visible, tant dans la formalisation de la Politique de Sécurité des Systèmes d'Information (PSSI) (73%, + 14% vs 2008), l'existence de charte SSI (67%, +17% vs 2008) que dans l'évolution du nombre de Responsables de la SSI (RSSI) (49%, + 12% vs 2008). Et pourtant, il existe une baisse quant à son rattachement à la Direction Générale (34%, - 11% vs 2008), certainement liée au fait que les RSSI « récents » proviennent souvent de la Direction des Systèmes d'Information (DSI). ». Traduction : dans plusieurs entreprises, la RSSI, souvent perçue comme un centre de coûts reste une émanation de la DSI , les direction générales ayant un intérêt pour la sécurité informatique assez discontinu : une attaque fortement médiatisée remet l'attention sur la sécurité des infrastructures puis ensuite la vigilance retombe. Un travers onne peut plus humain. Comme dit la chanson : « j'y pense et puis j'oublie ».

Les normes aident à formaliser les stratégies de sécurité mais les financements tardent souvent

Par ailleurs, l'étude conforme que l'utilisation des « normes » est en hausse. « *On constate, depuis près de 4 ans maintenant, la mise en place d'une « organisation » et de « structures » de la SSI (RSSI, Correspondant Informatique et Libertés (CIL), PSSI, charte, etc.) sans que, toutefois, la mise en application concrète de ces stratégies ne*

La Politique de Sécurité de l'Information (PSI) de votre entreprise s'appuie-t-elle sur des « normes » de sécurité ?



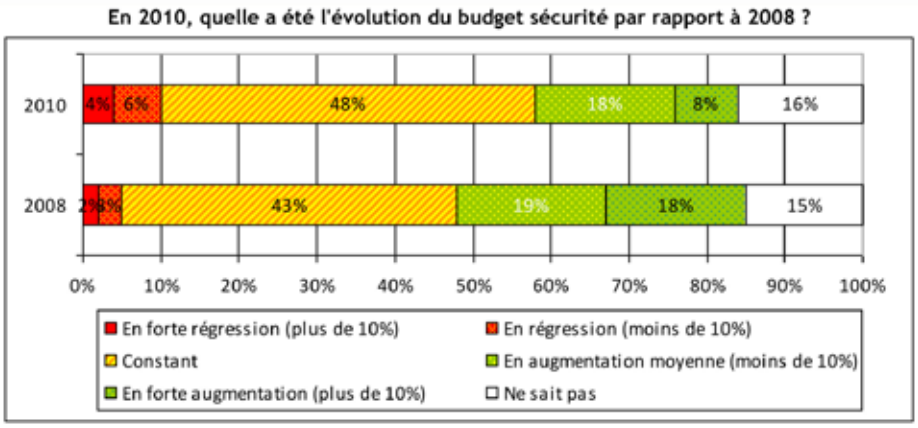
décolle réellement », note encore l'intéressé. Les budgets restent très serrés, parfois inexistants, et encore souvent réservés à la mise en oeuvre concrète de moyens techniques au détriment de la sensibilisation des utilisateurs (57% n'en font pas). Nouvel entrant cette année dans notre enquête, le thème ISO 27002 numéro 9 (sécurité physique), nous montre que pour 41% des entreprises, le responsable des « données papier » n'est pas clairement identifié. Peu de différences dans l'utilisation des technologies de sécurité, l'anti-virus, le pare-feu et l'anti-spam restent très largement en tête (respectivement 97%, 95% et 91%). Les IDS/IPS, technologies arrivées à maturité, progressent (34% et 27%, +11% vs 2008). Le chiffrement pour les utilisateurs évolue (17%, +7% vs 2008), mais reste « *à un niveau bien trop faible* », selon Lionel Mourer. Les technologies récentes (type NAC ou DLP) peinent à se déployer (respectivement 23% et 9%)… Seules 10% des entreprises ont placé leur SI sous infogérance et quand c'est le cas, près d'une sur trois ne met pas en place d'indicateurs de sécurité !

Des contrôles d'accès plus efficaces

Côté contrôle d'accès, le SSO et le Web-SSO décollent enfin (respectivement 21% et 8%, +14% et +5% vs 2008), signe d'une meilleure prise en compte de la simplification d'accès des utilisateurs. Cerise sur le gâteau, ce mécanisme permet également une meilleure traçabilité. Parmi les points positifs : la veille est de plus en plus réalisée, tant sur les vulnérabilités que sur les solutions de sécurité (34%, +13% vs 2008). Idem pour les procédures de déploiement de correctifs de sécurité ou patch management (64%, +16% vs 2008). Autre point positif, un mieux sur la gestion des incidents, avec une quantité d'incidents identifiée en hausse (26% déclare ne pas avoir eu d'incident, -19% vs 2008), certainement dû à des mécanismes d'alerte plus pertinents, pour un niveau de dépôt de plainte quasi identique à 2008 (5%, -1%). Reste que 33% (-7% vs 2008) des entreprises ne disposent toujours pas d'un plan de continuité d'activité pour traiter les crises majeures !… Enfin, les aspects « conformité », pour lesquels des progrès restent à faire, au travers :
- des « obligations CNIL » : en légère progression (68% « conforment», 20% « conforment pour leurs traitements sensibles », respectivement +4% et +1% vs 2008) ;
des audits de sécurité : 25% des entreprises n'en font toujours pas ;
du tableau de bord de la sécurité informatique : 34% seulement en dispose (malgré les +11%).

L'hôpital va devoir se convertir à la culture de la sécurité

Autre thème central abordé par l'étude : le monde de la santé où les questions de sécurité deviennent essentielles en raison de l'informatisation galopante des infrastructures hospitalières. Avec la parution au Journal Officiel le 29 novembre 2009 des arrêtés actant la dissolution du GIP-CPS (Groupement d'Intérêt Public - Carte de Professionnel de Santé) et l'élargissement du périmètre des missions de l'Agence des Systèmes d'Information Partagés de santé (ASIP), une nouvelle étape a été franchie dans la réforme de la gouvernance des systèmes d'information de santé. Sur la page d'accueil de son site internet, l'ASIP affirme : « *Sécuriser les données de santé : une condition indispensable au développement du Dossier Médical Personnel (DMP) et de la télémédecine* ». Les directions informatiques des hôpitaux sont de plus en plus convaincues de la nécessité absolue du pilotage médical des projets et de la participation des soignants : la sécurité doit devenir une valeur à partager, d'où l'apparition dans les hôpitaux ou à un niveau régional de responsables sécurité des systèmes d'information (RSSI), qui cumulent souvent leur fonction avec celle



de Correspondant Informatique et Libertés (CIL). La mise en conformité des établissements avec le décret confidentialité relève aussi de leurs compétences. De huit membres en 2008, le club des RSSI hospitaliers est passé à une quinzaine en 2009. Les thèmes abordés sont notamment : l'identifiant patient (IP) et le problème des appareils biomédicaux. Par ailleurs, dans le cadre du projet de loi Hôpital Santé Patients Territoires (HPST), il a été décidé de regrouper la MAINH (Mission nationale d'Appui à l'Investissement Hospitalier, la MEAH (Mission nationale d'Expertises et d'Audites Hospitaliers) et le GMSIH (Groupement pour la Modernisation des Systèmes d'Information de Santé) au sein d'une nouvelle entité : l'Agence Nationale d'Appui à la Performance des établissements de santé et médico-sociaux (ANAP).

« *La Sécurité apparaît maintenant souvent comme une préoccupation de la gouvernance des hôpitaux (soutenue à 94% par la DG) : la montée en puissance des contraintes législatives et réglementaires n'est pas étrangère à cette tendance* », relate Lionel Mourer.

Depuis la dernière enquête en 2006, les hôpitaux ont adopté les chartes de sécurité (63%, +21% vs 2006) et mis en place des CIL (39%, +10%). Ils n'ont pas résisté au nomadisme, ni au développement des réseaux sans fil et de la téléphonie sur IP. En progression, la détection des incidents de sécurité : l'augmentation des vols de matériels informatiques (44%) et de la perte de services essentiels (46%) est forte, en raison de l'augmentation de la pénétration des Systèmes d'Information dans les actes médicaux. En retrait toujours : la sensibilisation générale des salariés à la sécurité de l'information (27%, +2% vs 2006), la mise en place de plans de continuité métiers (54% en tout ou partie, +18% vs 2006), les audits de sécurité (49% n'en font pas) et les tableaux de bord de suivi (7%, +1% vs 2006). Même si à travers cette enquête MIPS 2010 on peut constater quelques réponses discordantes, probablement dues à la subjectivité de l'observation sur des domaines difficilement quantifiables, ou au fait que la sécurité est encore dépendante de la culture de chaque établissement, il apparaît clairement que les défis à relever par les hôpitaux dans les prochaines années sont encore importants et multiples.

Les internautes plus confiants dans le paiement en ligne

D'une manière générale, la perception de la menace (spam, phishing, intrusion, virus, logiciel espion, etc.) résultant de la connexion à Internet est en très légère diminution par rapport à l'étude précédente (23% « risque important ou très important », vs 25% en 2008). En revanche, le sentiment de danger concernant la protection de la vie privée augmente (73% « mise en danger de la vie privée - fortement ou un peu », vs 60% en 2008). « *Les usages les répandus ont finalement assez peu évolué entre 2008 et 2010*, confirme L. Mourer. *Quelque 96% des utilisateurs stockent et manipulent des photos ou des vidéos, 90% traitent des documents personnels (courriers, comptabilité, etc.), seuls 42% traitent des documents professionnels (-7% vs 2008).* »

Signe encourageant pour les offreurs de solutions et autres sites marchands : le paiement d'achats en ligne est davantage accepté par la population internaute. « *Désormais environ 90% des internautes déclarent accepter de procéder à des paiements en lignes, confirme L. Mourer alors que 68% le font sous conditions (utilisation de https : 99% de confiance, notoriété de l'enseigne accédée : 72% de confiance ou utilisation d'une e-card : 68% de confiance), et 22% sans condition.* »

Prudence toutefois : la présence d'un pictogramme type cadenas sur une page web ne garantit pas une sécurité absolue. « Les internautes ne doivent donc pas se sentir à baisser la garde au point d'abandonner les règles élémentaires de la sécurité informatique. »Enfin et concernant les moyens et comportements de sécurité mis en oeuvre, on observe que les

SÉCURITÉ INFORMATIQUE
est éditée par PUBLI-NEWS s.a.
47, rue Aristide Briand 92300 Levallois-Perret
Tél : 01 41 49 93 60
Fax : 01 47 57 37 25
Email : i.lancry@publi-news.fr
Site Internet : www.publi-news.fr
Commission paritaire n°0214 I 84348
SIREN : 330 394 834
Impression : Un Point et Plus
74, rue Jules Guesde, 92300 Levallois-Perret
Lettre bi-mensuelle
Dépôt légal à parution
Prix au numéro : 39 € TTC

DIRECTEUR DE LA PUBLICATION/ RÉDACTEUR EN CHEF
Ange Galula

RÉDACTEUR EN CHEF ADJOINT
Gilles Prod'homme

RÉDACTION
Jo Cohen
Contact : 01.41.49.93.67
Fax rédaction : 01.41.49.93.71
E-mail : ange.galula@publi-news.fr

ordinateurs sont peu protégés par des mots de passe (5%) ou des contrôles biométriques (11%), mais aussi que les mises à jour de sécurité semblent être déployées régulièrement (+90%), qu'il s'agisse de déploiement automatique ou manuel. Les mesures de protection professionnelles sont très peu utilisées sur l'ordinateur familial : 80% n'utilisent pas de chiffrement, 88% n'ont pas d'antivol physique et 65% n'ont pas de protection de leur alimentation électrique. « *Au final, nous observons une banalisation de l'usage Internet, avec un sentiment de sécurité qui ne change pas grâce à une meilleure connaissance de l'outil informatique et de ses dangers* », conclut Lionel Mourer qui souligne que les « *questions autour de la protection et de la sécurité des données personnes préoccupe la plupart des internautes*. »

Gilles PROD'HOMME

SPAMMING

Les attaques de spams liés à la Coupe du monde de football s'intensifient depuis le début du tournoi

Dans l'édition de juin 2010 de son rapport MessageLabs Intelligence, Symantec note que depuis mars 2010, dans le contexte de la Coupe du monde de football 2010, le pourcentage des spams comportant des mos-clés liés au football et au soccer (appellation anglophone) approche 25 % du volume total des spams envoyés dans le monde. La Coupe du monde de la FIFA devient ainsi le dernier fait d'actualité exploité par les spammeurs. «*Les spammeurs profitent en ce moment de la vague d'enthousiasme que suscite généralement un événement de l'envergure de la Coupe du monde de football*, déclare Paul Wood, analyste senior de MessageLabs Intelligence. *Surfant sur cette vague, ils attirent l'attention de leurs victimes avec des produits à vendre ou en les encourageant à cliquer sur un lien. Il est fréquent que l'événement soit cité en objet de l'e-mail, mais que le corps du message évoque totalement autre chose.*»
Au début du mois de juin, MessageLabs Intelligence signalait de nouvelles attaques associées à la Coupe du monde de la FIFA. Dès le 2 juin, le laboratoire de Symantec interceptait ainsi 45 e-mails d'une même attaque ciblée à destination de cadres supérieurs et de dirigeants de sociétés brésiliennes des secteurs de la chimie, de la fabrication industrielle et de la finance. Ces e-mails employant le prétexte la Coupe du monde utilisaient l'ingénierie sociale pour compromettre les systèmes informatiques des sociétés afin d'accéder à leurs informations confidentielles via les destinataires. Pour multiplier ses chances de réussite, l'attaque était double : une pièce jointe au format PDF et un lien malveillant. Ainsi, si le fichier PDF venait à être supprimé par l'antivirus, le lien figurerait toujours dans l'e-mail « nettoyé » finalement transmis au destinataire par bon nombre de systèmes de filtrage d'e-mails.
En juin toujours, MessageLabs Intelligence a intercepté un spam lié à la thématique pharmaceutique utilisant en pièce jointe un code JavaScript masqué. Une fois de plus, la mention de la Coupe du monde en objet n'avait d'autre intention que de piquer la curiosité du destinataire afin qu'il ouvre le fichier html joint. Le code JavaScript masqué dans ce fichier redirigeait alors le navigateur du destinataire vers un autre site, lui-même falsifié. «*Les spammeurs, sûrement très compétents, se sont donné du mal pour maquiller le but véritable du code JavaScript*, explique M. Wood. *A savoir tromper les destinataires pour les inciter à ouvrir le message qui n'aura finalement aucun rapport avec ce à quoi ils s'attendaient. Une approche fréquemment utilisée par les malwares. Il faut s'attendre à ce que ces attaques se multiplient pendant toute la durée de la compétition*.»
http://www.symantec.com

Chine : jusqu'où Google mettra-il de l'eau dans son vin ?

Alors que la date d'expiration de sa licence d'exploitation en Chine approchait à grande vitesse, Google a tenté une manœuvre de la dernière chance dans le but évident de rester un acteur qui compte sur l'immense marché chinois, quitte à n'en détenir que le tiers face au moteur concurrent Baidu. La licence d'Internet Content Provider de Google venait à expirer en effet le 30 juin 2010 ! Afin de continuer à bénéficier de

son statut d'Internet Content Provider en Chine, le moteur de recherche a décidé d'assouplir ses positions et faire preuve ainsi de bonne volonté. Sur le blog de David Drummond, chef du département juridique chez Google, l'entreprise explique qu'elle a légèrement modifié sa politique afin de répondre au mieux aux exigences du gouvernement chinois, mais sans y perdre totalement son « âme ». L'idéal pour Google serait de proposer aux internautes chinois un moteur de recherche avec un minimum de filtrage. En pratique, dans le cadre de sa nouvelle politique, les demandes des internautes chinois ne sont plus systématiquement routées vers la plate-forme de Hong Kong, non soumise à la censure. Les internautes chinois qui souhaitent y accéder disposent à présent d'un lien sur lequel ils peuvent cliquer à cet effet. Dans le cas contraire, ils obtiennent des réponses filtrées selon les critères imposés au géant américain par le gouvernement de Pékin. Jusque-là, au plan technique, l'adresse web par défaut de Google en Chine dirigeait systématiquement les internautes vers le site de Google à Hong-Kong. Ce faisant, certains observateurs estiment que, loin d'avoir conforté ses positions, Google a carrément reculé devant l'intransigeance des autorités chinoises. «Sans une licence ICP, nous ne pouvons pas opérer un site commercial comme Google.cn - et donc Google serait totalement bouté hors de Chine» reconnaît David Drummond sur son blog. Or voilà que la veille de l'échéance fatidique, Google constate que son moteur de recherche est partiellement bloqué en Chine, la perte de perte de trafic fluctuant entre 10 et 66%. Voilà qui n'est pas de bon augure à quelques heures du renouvellement éventuel de sa licence d'ICP ! Bien que la redirection vers le site de Hong Kong ne soit plus systématique, les intransigeantes autorités chinoises ne semblent pas vouloir rechercher la voie du compromis. Elles y perdraient la face ! D'où la pression mise sur Google. Le sort de la société américaine, suspendu au renouvellement de sa licence en Chine, se joue dans la période qui s'ouvre. Selon un responsable chinois cité le 30 juin par l'agence officielle Chine nouvelle et repris par l'AFP, une réponse sera donnée ... très prochainement. «*Nous sommes dans l'attente d'une réponse du gouvernement*», a déclaré à l'AFP Jessica Powell, porte-parole du groupe basée à Tokyo. Reste que les médias officiels ont accusé le géant américain de vouloir jouer un double jeu. «*Google essaie d'obtenir un gain politique en Occident tout en retirant des bénéfices de l'économie chinoise*», a indiqué un article publié par l'édition destinée à l'étranger du Quotidien du Peuple, l'organe du Parti communiste. Jusqu'où la partie de bras de fer ira-t-elle ?

La page d'accueil de Google.cn offre la possibilité d'être routée vers Google.hk

MALWARE

Une faille non corrigée de Windows XP fait l'objet d'attaques

Selon l'éditeur Sophos, un programme malveillant exploite depuis peu une faille de Windows XP et Windows Server 2003. Cette faille a été découverte il y a une quinzaine de jours par un chercheur de Google. Microsoft estime que les attaques ciblant cette faille sont limitées, mais reconnaît qu'elles pourraient se développer. Le 5 juin dernier, Tavis Ormandy, ingénieur en sécurité chez Google divulguait l'existence d'une faille de sécurité dans le service Aide et Centre de support de Windows XP et Server 2003. Afin de démontrer la faisabilité d'une attaque, il publiait le 10 juin un exploit, soulevant l'indignation de Microsoft, l'éditeur estimant que le chercheur exposait ainsi les utilisateurs à des attaques. La crainte semble se confirmer puisque, dès le 15 juin, Sophos indiquait sur son blog avoir découvert des programmes malveillants exploitant cette faille de Windows. Selon Sophos, l'attaque se diffuserait par le biais de sites Web compromis. Ce malware, connu sous le nom de Sus/HcpExpl-A, provoquerait le téléchargement et l'exécution d'un code malveillant, un cheval

de Troie (Troj/Drop-FS), sur l'ordinateur vulnérable. Contacté par le site CNet.com, Jerry Bryant de Microsoft, déclare que l'exploitation de la faille reste à ce jour limitée. Il estime toutefois que ces attaques devraient se développer en raison de la divulgation publique de la vulnérabilité. Microsoft rappelle par ailleurs que seuls Windows XP et Windows Server 2003 sont affectés. Les autres versions du système d'exploitation ne comportent pas cette vulnérabilité. Afin de prévenir une attaque, Microsoft met à disposition des utilisateurs un correctif provisoire qui peut être téléchargé directement sur le site de l'éditeur.
http://www.sophos.com

Apple met à jour en toute discrétion l'anti-malware du Mac

Le pot aux roses a été révélé sur le blog de Graham Cluley de Sophos : le chercheur y explique comment Apple a discrètement mis à jour la protection anti-malware incluse dans Mac OS X. C'est à l'occasion du lancement de la nouvelle version diffusée en début de mois que cet ajout s'est opéré. Mac OS X 10.6.4 intègre en effet une protection limitée contre le cheval de Troie Pinhead-B. Bien que cette protection ne soit pas documentée par Apple, Mac OS X 10.6.4 comprend bien une protection limitée contre OSX/Pinhead-B (appelé HellRTS par Apple), un cheval de Troie qui permet aux pirates de prendre le contrôle d'un ordinateur Mac pour espionner son fonctionnement, dérober des identités ou diffuser du spam. Rappelons que Sophos a détecté OSX/Pinhead-B en avril dernier, lorsque le malware a commencé à se diffuser sous forme d'une populaire application iPhoto.
«C'est une bonne nouvelle qu'Apple ait mis à jour la protection de Mac OS X, car ce cheval de Troie peut donner aux pirates la possibilité d'envoyer du spam depuis l'ordinateur, d'effectuer des copies d'écran, d'accéder aux fichiers, etc., reconnaît Michel Lanaspèze, directeur marketing et communication de Sophos Europe du Sud, avant de s'étonner de la démarche. *Il est juste étrange que la société n'ait pas annoncé cette mise à jour dans la documentation ni dans les conseils de sécurité accompagnant cette nouvelle version. On pourrait presque penser qu'ils ne veulent pas reconnaître que des malwares puissent menacer Mac OS X.»* Du reste, Graham Cluley a révélé qu'Apple avait mis à jour un fichier nommé XProtect.list, qui contient une poignée de signatures élémentaires de menaces Mac, afin de détecter ''HellRST''.

«Il est exact que les programmes malveillants visant les Mac sont beaucoup moins nombreux que ceux qui ciblent Windows, mais cela ne signifie pas que le problème soit inexistant, poursuit Michel Lanaspèze. *Malheureusement, un grand nombre d'utilisateurs de Mac semblent complètement ignorer que de telles menaces peuvent atteindre leur ordinateur, même si Apple intègre désormais une protection minimale dans son système. Cette situation ne s'arrangera pas si Apple effectue ses mises à jour de sécurité secrètement, sans en informer le public.»* De trop nombreux utilisateurs de Mac négligent encore d'installer un logiciel antivirus sur leur ordinateur, ce qui pourrait à l'avenir en faire des proies faciles pour les pirates.
http://www.sophos.com/blogs/gc/g/2010/06/18/apple-secretly-updates

PIRATAGE

Le «pirate» français de Twitter condamné à 5 mois avec sursis

Agé de 23 ans, le «pirate» français accusé d'avoir infiltré le réseau social Twitter et tenté de corrompre le compte du président Obama (voir nos précédentes éditions) vient d'être condamné par le Tribunal de Clermont Ferrand à cinq mois de prison avec sursis alors qu'il encourait jusqu'à deux ans de prison ferme. Ni Twitter, à l'origine du dépôt de plainte, ni les autorités américaines, ni les détenteurs des messageries électroniques piratées ne se sont constitués partie civile, expliquant dans une large mesure la clémence du jugement. Soulagé, le jeune autodidacte, plus connu sous son pseudonyme ''Hacker-Croll'', a accueilli la sentence avec le sourire ! Interpellé le 24 mars

dernier au terme d'une enquête pilotée par le FBI, le jeune homme avait été relâché peu après. L'Agence France Presse rapporte qu'à la sortie du tribunal, ses parents, entourés de leurs cinq autres enfants, ont estimé que le jugement était clément et que leur fils ne ferait donc pas appel. Le jeune homme s'est défendu d'être un hacker dans la mesure où il n'a rien détruit et qu'il n'a nui à quiconque. Il n'a escroqué personne. Il a juste voulu montrer, dans une démarche préventive autant que pédagogique, que le maillon faible n'était pas le matériel, mais l'humain. Le jeune homme était parvenu à obtenir les codes administrateurs de Twitter et pouvait y naviguer à sa guise. Par défi, il estime être entré dans une maison dont la porte était restée ouverte. Vrai ou faux, son action aura sans doute sensibilisé les abonnés de Twitter sur l'importance du choix de leurs mots de passe. L'avocat de la défense, maître Jean-François Canis, a poussé le bouchon encore plus loin en affirmant que cette affaire avait été profitable à Twitter. Le réseau social a pu en effet mettre en place de nouvelles procédures de sécurité. L'avocat a conclu que la démarche était somme toute assez morale «*de la part d'un gentil garçon, discret, qui a fait sa vie autour de l'informatique et qui a plus d'amis virtuels que réels*». Il est tout de même parvenu à trouver les mots de passe des comptes Twitter ouverts au nom du président américain ou de la chanteuse Britney Spears, des compétences qui lui ont valu d'être embauché par une société d'informatique pour effectuer de la surveillance de marques !

Tel est pris qui croyait prendre ou comment déjouer les attaques des hackers en utilisant les failles des codes malicieux !

A la conférence SyScan consacrée à la sécurité qui s'est tenue les 17 et 18 juin derniers à Singapour, le chercheur français Laurent Oudot a fait sensation en montrant que les failles des codes malicieux utilisés pour contaminer des sites Internet et infiltrer des PC, vendus sur la Toile au marché noir, pouvaient être mise à profit pour neutraliser les sites piégés par des réseaux de hackers et, dans certains cas, de remonter jusqu'aux commanditaires des attaques. C'est la version moderne de l'histoire du chasseur chassé… sauf qu'ici la méthode n'a rien de légal à l'heure qu'il est. Cela n'a pas empêché Laurent Oudot, ancien du ministère de la Défense et du Commissariat à l'énergie atomique de lancer sa société de conseil en sécurité au début de l'année. Son nom : Tehtri-Security. La société compte déjà des références dans la Défense et dans les milieux bancaires. En vente libre sur la Toile, des kits d'attaque tels que MPack ou Neon, conçus et développés en Russie, se vendent plusieurs centaines de dollars. Ils contaminent les internautes et enrôlent leurs PC dans des réseaux de botnets contrôlés à distance. Or, la gestion et la mise à jour de ces kits nécessitent de se connecter régulièrement à une interface d'administration qui révèle de nombreuses failles de sécurité. Il n'est pas difficile alors d'infiltrer ces kits et d'identifier les adresses IP des assaillants ou encore d'effacer les statistiques des ordinateurs contaminés. Il serait même possible de détruire les logiciels malveillants implantés dans les sites Internet. Même si la loi interdit ce genre de pratiques, la faisabilité technique vient d'en être démontrée par le chercheur français. Il estime que les états et les entreprises devraient faire usage de tels outils contre les pirates. C'est une évolution naturelle de la cyberguerre estime en substance le patron de Tehtri-Security, convaincu que la mésaventure qui est arrivée à Google devrait aider à une prise de conscience en faveur de telles techniques.

PHISHING

".be" dans le Top 5 des extensions exploitées frauduleusement

Selon les chiffres présentés par l'Anti Phishing Working Group au dernier Icann Meeting à Bruxelles, l'extension web «.be» serait parmi les plus recherchées par les pirates. Au niveau mondial, la Belgique se retrouverait ainsi derrière la Thaïlande, la Corée et l'Irlande. Sur le terrain, 4,6 noms de domaines enregistrés sous l'extension «.be» sur 10.000 seraient donc utilisés à des fins criminelles. Autre statistique inquiétante : 11,5 sites sur 10.000 abriteraient de faux sites destinés à pirater les données d'internautes peu vigilants. Les chiffres de l'APWG montrent que sur 80% de sites malveillants dans le monde on retrouve cinq suffixes Internet frauduleusement exploités, dont celui de la Belgique. Plusieurs raisons expliquent l'attrait de ces suffixes par les pirates. A commencer par le fait qu'une URL se terminant par «.be» reste très bon marché comparée à d'autres codes territoriaux. Autre argument, la démarche pour s'enregistrer est entièrement automatisée. Les noms de domaine deviennent actifs

à peine quelques secondes après leur enregistrement. Last but not least : en Belgique, il se passe au moins vingt heures avant que les pirates ne soient interpellés, ce qui laisse une journée entière à d'éventuels pirates pour poser leurs pièges.

'Phishing' au Royaume de Sa Gracieuse Majesté : une victime toutes les 7 secondes !

L'étude que vient de publier CPP, une société spécialisée dans la protection par cartes, est des plus édifiantes. Nos voisins britanniques auraient reçu quelque 3,7 milliards de tentatives de 'phishing' l'an dernier. 26% des internautes anglais auraient été victimes de hackers. L'étude estime le nombre annuel de victimes à 4 millions, soit une victime toutes les 7 secondes. Chacune aurait perdu en moyenne 285£, l'essentiel des attaques de 'phishing' visant les institutions financières et les banques. On y trouverait aussi du scam Nigerian et des attaques contre les loteries. CPP évalue le montant annuel des pertes à 1,3 Md£. Le pays est une cible privilégiée des «phishers» américains, russes et chinois, ces derniers ayant, au fil des années, affiné la qualité de leurs emails.
http://www.cpp.co.uk

GESTION DES VULNERABILITES

Les données des PME restent encore mal protégées

Une étude mondiale commanditée par Symantec sur la protection des données dans les PME montre que malgré une certaine prise de conscience des risques d'attaques et de pertes de données, les besoins d'éducation, d'information et de bonnes pratiques restent importants. Les PME interrogées, dans le monde, au niveau EMEA et en France considèrent la perte de données et les cyber-attaques comme les principaux risques auxquels elles sont confrontées, devant la criminalité ordinaire, les catastrophes naturelles et le terrorisme. 77% des PME de la zone EMEA et 74% des PME françaises interrogées ont reconnu d'ailleurs avoir subi une attaque Internet. Lorsqu'elles réussissent, ces attaques représentent un coût moyen non-négligeable : 242.000 €. Si 70% des entreprises interrogées considèrent les cyber-attaques comme importantes ou très importantes, des progrès sont encore à réaliser du côté de la protection des données elles-mêmes. 93% des PME françaises interrogées ont cependant préparé un plan de reprise d'activité, un chiffre en forte progression par rapport aux études précédentes réalisées par Symantec sur ce sujet. Cependant, 33 % d'entre elles considèrent leur plan comme plutôt bon ou excellent, montrant ainsi un besoin en éducation et en accompagnement.
En France et en Europe, la perte de données stratégiques constitue une menace constante pour les PME. Si 71 % d'entre elles se déclarent plutôt ou extrêmement préoccupées par le risque de perte d'informations électroniques et 33 % ont déjà été victimes de la perte de données confidentielles ou propriétaires, 71% des PME de la zone EMEA déclarent avoir perdu un terminal (ordinateur ou téléphone portable) et elles ne sont que 28% à protéger leurs smartphones avec un mot de passe. Parmi les priorités des PME, l'amélioration des compétences informatiques est citée par 68 % des entreprises comme leur préoccupation principale, suivie par l'amélioration du système de sécurité des ordinateurs qui est une priorité pour 67% des PME interrogées. La sauvegarde, la restauration et l'archivage des données est également cruciale puisque 62% des sociétés estiment que c'est l'une des principales activités à perfectionner.
«*Les PME sont confrontées à une augmentation des risques pour leurs informations confidentielles, notamment les numéros de leurs comptes bancaires, de leurs cartes de crédit, ainsi que les fichiers contenant des informations sur leurs clients et leur personnel. Qu'il s'agisse d'une attaque par un logiciel malveillant, d'une panne de serveur ou d'un appareil mobile volé, une perte de données peut être très préjudiciable, voire fatale, pour une PME*, explique Stéphane Gaillard, directeur des ventes de Symantec. *Il y a un an, une enquête de Symantec a constaté qu'1/3 des PME ne disposait même pas de la protection antivirus*

la plus basique. Il est intéressant de voir que les PME françaises reconnaissent les risques auxquels elles sont confrontées et qu'elles prennent des mesures pour mieux protéger leurs données.»
http://www.symantec.com

VIE PRIVEE

La CNIL toujours réservée sur le projet de loi Loopsi 2

Lors du traditionnel bilan de la Cnil (voir notre précédent numéro), son président Alex Türk a estimé que, malgré les efforts du gouvernement pour rendre le texte de loi plus respectueux de la vie privée et des libertés des français, la commission attendait des modifications substantielles concernant les fichiers de police, la captation de données sur les accès publics à Internet et la vidéosurveillance. Après un premier avis partiel rendu en 2009, c'est à la demande du rapporteur de la loi au Sénat que la Cnil a formulé ses remarques sur les principales dispositions de la future loi dans le cadre d'un avis complet dans lequel la commission réitère des demandes non prises en compte jusque-là. Elle juge en effet nécessaire que les fiches des fichiers polémiques Judex et Stic ayant fait l'objet d'une mise à jour ne soient plus consultables, que l'utilisation d'outils de captation dans les points publics d'accès à Internet soit encadrée avec traçabilité des captations et de leur utilisation et enfin que la sous-traitance de la vidéosurveillance soit soumise aux mêmes contrôles, même en cas de traitements offshore. ■
http://www.cnil.fr

A nos lecteurs
Des informations supplémentaires sur l'actualité des offreurs de solutions de sécurité informatique sont accessibles en ligne. Pour y accéder, connectez-vous sur le site **www.publi-news.fr** puis consultez le fil quotidien d'informations, **PUBLINET**, rubrique **Sécurité**.