Quand l’Eglise catholique française s’assoit sur la protection des données personnelles | Le Net Expert Informatique

	Quand l’Eglise catholique française s’assoit sur la protection des données personnelles

On craint, à juste titre, ce que les géants d'internet peuvent faire de nos données personnelles, on n'aurait pas imaginé que l'Eglise puisse être rangée dans la même catégorie.

Payer pour son culte

C'est pourtant ce qu'a découvert un Français vivant à Berlin au terme de multiples mésaventures. Il en fait part au travers de son blog (http://bores.fr/blog/2015/02/berlin-jour-3-pourquoi-il-est-urgent-de-vous-faire-rayer-des-listes-de-bapteme-en-france), repris dans la presse. Tout est parti du fait qu'en Allemagne, on doit payer une taxe lorsque l'on appartient à un culte, ceci afin de le financer.

La taxe s'élève à 550 € annuels. Ce Français avait pourtant déclaré être athée lorsqu'il avait rempli les documents administratifs nécessaires. Mais il a été taxé par prélèvement automatique car l'église catholique allemande s'est fait communiquer par sa paroisse d'origine en France, les documents prouvant qu'il avait été baptisé.

Certificat de baptême

Il décrit ce qu'il a ressenti : « c'est alors que j'apprends terrifié que le diocèse de la ville où je me suis fait baptiser en France a envoyé sur demande de l'église catholique de Berlin un certificat de baptême. » Conséquence, bien qu'il se sente athée convaincu, selon la loi allemande, il est redevable de l'impôt.

Conclusion, il estime que l'église catholique française passe outre la directive européenne 95/46/CE sur la protection des données personnelles. Et il s'insurge qu'elle envoie sur simple demande les données personnelles des particuliers, sans les en informer au préalable, à l'église catholique allemande afin que celle-ci récupère de l'argent.

Que fait la CNIL

La CNIL a manifestement du pain sur la planche afin de diffuser les bonnes pratiques en termes de diffusion des données au travers des frontières.

Expert Informatique et formateur spécialisé en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la formation de vos salariés afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.

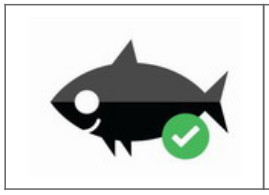
Contactez-nous

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire…

Source : http://www.larevuedudigital.com/2015/02/25/quand-leglise-catholique-francaise-sassoit-sur-la-protection-des-donnees-personnelles/

Logiciel Espion Superfish installé par Lenovo : son site Internet piraté en représailles



Logiciel Espion Superfish installé par Lenovo : son site Internet piraté en représailles

Le site Internet de Lenovo a été piraté et son trafic redirigé vers un compte Twitter critiquant l'installation par le fabricant de l'adware Superfish. Lenovo enquête sur d'autres effets possibles de cette cyberattaque.

Après le scandale du logiciel publicitaire et à risque installé par défaut sur un grand nombre de ses ordinateurs portables, Lenovo a dû s'expliquer et présenter des excuses. Mais manifestement, le fabricant doit aussi faire face à des représailles du fait de Superfish.
Mercredi 25 février, le site Internet de Lenovo était inaccessible. Cette indisponibilité fait suite à une cyberattaque. Mais avant que l'entreprise ne déconnecte son site et n'informe les visiteurs d'une maintenance en cours, celui-ci affichait un diaporama diffusant des images tirées du service Imgur. Un clic sur les images redirigeait vers un compte Twitter Lizard Squad, critique à l'égard de Lenovo pour la diffusion de l'adware Superfish.

Attaque sur le gestionnaire de domaine
Lenovo a confirmé une faille de sécurité au Wall Street Journal. « Malheureusement, Lenovo a été victime d'une cyber attaque » reconnaît le fabricant de PC. « Un effet de cette attaque a été de rediriger le trafic depuis le site Web de Lenovo. Nous étudions activement d'autres aspects de cette attaque » précise-t-il encore.
Les attaquants avaient semble-t-il pris le contrôle du site du registrar du domaine utilisé par Lenovo et pu ainsi rediriger le trafic vers un compte gratuit ouvert sur CloudFlare. Contacté par Bloomberg, le spécialiste du CDN et des services DNS déclare avoir désactivé le compte depuis.
Sur Twitter, un compte se revendiquant de Lizard Squad prétend que les hackers du groupe sont à l'origine de cette attaque réussie. Toutefois, cette revendication ne suffit pas à en faire les auteurs véritables du piratage. En janvier, ces derniers assuraient ainsi être à l'origine de la panne de Facebook. Or, cette panne résultait d'une défaillance informatique et nullement d'une attaque.

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

Source : http://www.zdnet.fr/actualites/superfish-le-site-de-lenovo-pirate-en-represailles-39815368.htm

---

Un réseau de fraudeurs cybercriminels démantelé au

Mali

Malijet La Un réseau de fraudeurs cybercriminels démantelé au Mali

Dans le cadre de la lutte contre la délinquance économique dans le domaine des télécommunications, la section de cybercriminalité de la Brigade d'investigation judiciaire (BIJ), dirigée par l'inspecteur divisionnaire, Papa Mambi Kéita, a démantelé, le 23 février 2014, un réseau de fraudeurs sur les communications mobiles d'Orange Mali en provenance de l'international. Les deux frères fraudeurs, Seydou Mahamadou Touré et Sidi Touré, ont été pris dans le bureau à l'ACI 2000 en possession de 276 puces Orange, une unité centrale et un SIMBOX.

Après un passage remarquable à la Brigade de recherche du 3ème arrondissement, Papa Mambi Kéita plus connu sous le sobriquet « L'Epervier du Mandé » continue à faire parler de lui à la section cybercriminalité de la Brigade d'investigation judiciaire.
Car, il vient, en collaboration avec Orange Mali, de mettre le grappin sur les deux pirates. Selon Papa Mambi Kéita, le mode opératoire des délinquants consistait à masquer les appels extérieurs effectués à l'international entrants sur le réseau Orange Mali en les contournant de leur voie normale.
Selon un responsable de la société, la fraude a causé un énorme manque à gagner à la société Orange Mali et à l'Etat malien auquel la société paye des taxes et des impôts.
Pour elle, le crime ne résulte aucunement d'une défaillance quelconque de la société qui a toujours su repérer et localiser les menaces centre son réseau. En effet, la pratique utilisée est le bypass téléphonique, connu également sous le nom de SIMBOX.
Il s'agit d'un dispositif frauduleux qui permet de contourner la voie normale des appels internationaux entrants. Selon le chef de la section cybercriminalité de la BIJ, Papa Mambi Kéita, les fraudeurs ont reconnu leur crime et disent travailler pour un camerounais basé aux Etats-Unis pour une somme de 200 000 F CFA par mois.

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

Source : http://malijet.com/les_faits_divers_au_mali/124118-cybercriminalite_au_mali_la_brigade.html
Par Youssouf Z KEITA

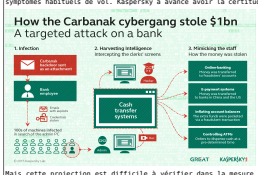
Comment les entreprises pourraient mieux se protéger des attaques informatiques de plus en plus sophistiquées ?

	Comment les entreprises pourraient mieux se protéger des attaques informatiques de plus en plus sophistiquées ?

En 2013, un distributeur automatique de billets à Kiev s'est mis à délivrer des billets tout seul à certains moments de la journée qui semblaient être fortuits sans que personne n'ait à insérer une carte ou à presser un bouton. Les caméras de surveillance ont montré que l'argent qui avait été délivré a été raflé par des clients à qui la chance semblait sourire.

Cependant, quand l'expert en cybersécurité russe Kaspersky Labs a été appelé en Ukraine pour mener une enquête, il a découvert qu'il ne s'agissait là que de la partie émergée de l'iceberg. En effet, les ordinateurs internes de la banque, utilisés par les employés qui traitent des transferts quotidiens et qui tiennent la comptabilité, avaient été infiltrés par un logiciel malveillant qui permettait aux cybercriminels baptisé du même nom que leur logiciel Carbanak (basé sur le trojan Carbep) d'enregistrer chacun de leurs mouvements. Les recherches ont montré que le logiciel malveillant qui se cachait depuis des mois a envoyé des images et des vidéos à un groupe de cybercriminels pour lui permettre de déterminer comment la banque effectuait ses routines. « L'objectif étaient d'imiter leurs activités », expliquait Sergey Golovanov qui a mené les opérations d'investigations pour le compte de Kaspersky. « De cette façon, tout aurait ressemblé à une opération quotidienne normale » a-t-il rajouté par la suite. Ils commencent par ajouter virtuellement de l'argent sur un compte bancaire en modifiant le solde disponible, puis transfèrent toute la somme ajoutée vers le compte de destination, laissant le solde d'origine intact.

Dans un rapport que Kaspersky a publié il y a quelques jours déjà, l'entreprise a avancé que la portée de cette attaque s'étendait sur plus de 100 banques et autres institutions financières dans une trentaine de pays et cette série de vols pourrait en faire le plus gros casse de banque jamais réalisé et qui a en plus été menée sans les symptômes habituels de vol. Kaspersky a avancé avoir la certitude que près de 300 millions de dollars ont été dérobés à ses clients et que la somme total du casse pourrait atteindre le triple.



Mais cette projection est difficile à vérifier dans la mesure où les vols ont été limités à 10 millions de dollars par transaction, bien que certaines banques aient étés frappé plusieurs fois. De plus, dans certains cas, les transactions étaient plus modestes, sans doute pour éviter de déclencher des alarmes. La majorité des cibles étaient situées en Russie, mais il y en avait également plusieurs au Japon, aux Etats-Unis et en Europe. A cause d'une clause de non divulgation avec les banques qui ont été touchées, Kaspersky n'a pas eu le droit d'en établir une liste qui pourrait être portée au public. Des responsables à la Maison Blanche ainsi que du FBI, d'Interpol ou d'Europol ont été débriefés dessus mais ont avancé que cela prendrait du temps pour confirmer et évaluer les pertes.

Chris Doggett, le directeur général de Kaspersky en Amérique du Nord à Boston, a avancé que le groupe de cybers criminels Carbanak représente une augmentation de la sophistication des cyberattaques sur les entreprises financières. « C'est probablement l'attaque la plus sophistiquée du monde a vu à ce jour en termes de tactiques et des méthodes que les cybercriminels ont utilisé pour rester dissimulés », a-t-il déclaré. Les cybercriminels ont pris la peine d'étudier chaque particularité des banques ciblées tandis qu'ils établissaient de faux comptes en Chine et aux Etats-Unis qui pouvaient servir de destinations de transferts. En somme, une mécanique très bien huilée.

D'autres attaques qui ont également fait parler les médias comme celle qui a vu 76 millions de comptes clients de l'institution financière JPMorgan Chase être piratés ont poussé les banques à s'interroger sur la raison pour laquelle des pirates les considèrent comme des proies relativement facile. Pour pouvoir faire face aux menaces ou future menaces, certaines institutions ont estimé qu'elles devaient très vite colmater des failles non seulement dans la sécurité de leur système mais également dans celui des entreprises partenaires ou conseillères. Et si la réponse était toute autre ?

La raison principale pour laquelle les cybercriminels voient de grandes entreprises ainsi que leurs partenaires principaux comme des proies relativement faciles est une déconnexion alarmante entre les membres du conseil de l'administration de l'entreprise et leurs services informatiques. Le rapport « exposer les fissures de la cybersécurité : une perspective mondiale » publié par l'Institut Ponemon l'année dernière a mis en évidence le fait que les professionnels de la sécurité se trouvent « inefficaces, isolés et dans l'obscurité » lorsqu'ils font face aux cybermenaces. Après avoir interrogés 4 880 professionnels expérimentés de la sécurité informatique provenant de 15 pays, le rapport a découvert :

- un déficit dans l'efficacité des solutions en matière de sécurité;
- un décalage entre les dirigeants de l'entreprise et la valeur perçue de la perte des données ;
- une visibilité limitée dans les activités cybercriminelles.

De plus, le panel a avancé que près de la moitié des cadres dirigeants siégeant au conseil d'administration ont une faible compréhension de la question de sécurité. Mais le problème semble encore plus profond. Il faut réaliser que les départements informatiques ont également leur part de responsabilité dans cette déconnexion qui a pris de l'ampleur entre eux et le C.A.

Cette situation est imputable en partie à ce legs du temps où les dirigeants d'une société naviguaient pour la plupart en zone totalement inconnue en ce qui concerne l'informatique. Mais elle est également le résultat d'une impasse émotionnelle qui existe désormais entre les chefs de services informatique qui défendent ce qu'ils considèrent comme leurs fiefs personnels sans réaliser que la cybersécurité a des impacts à tous les niveaux des opérations de l'entreprise. Le cantonnement de la cybersécurité fait de cette manière peut cultiver la complaisance au sein des entreprises, berçant les dirigeants dans une douce illusion selon laquelle leurs cyberdéfenses sont impénétrables.

Une image plus réaliste serait pour le PDG de comprendre que son entreprise peut être piratée (si ce n'est pas déjà le cas). A moins qu'une entreprise n'effectue régulièrement des tests de pénétration sur ses défenses numériques, il est probable qu'une partie de ses données soit compromise à son insu.

Les départements informatiques peuvent penser à tort que la cybersécurité n'est qu'un problème qui relève de l'informatique, mais elle concerne en réalité d'autres domaines, y compris les ressources humaines. Plusieurs violations de données, par exemple, ne sont pas issues d'un piratage externe mais plutôt interne, parfois il s'agit de l'œuvre d'un employé mécontent ou malhonnête ou même d'un ancien employé. Des estimations avancent que près d'un ex-employé sur trois en Angleterre a encore accès à des données détenues par leur ancien employeur.

Aussi, la première mesure à prendre serait déjà de déterminer quelles données peuvent être compromises et par qui. Pour ce faire, les chefs d'entreprise pourraient appuyer des enquêtes menées en interne par les équipes informatique puisqu'elles ont la capacité de voir à leurs « angles morts ».

Parfois, un intrus peut avoir pénétré le système d'information d'une entreprise pendant des mois, voire des années, avant qu'elle n'en prenne conscience. Dans un tel cas de figure, les dégâts peuvent être difficiles à quantifier. Par exemple, s'il s'agit d'un concurrent, il peut avoir acquis des stratégies commerciales en examinant ses documents confidentiels quasiment en temps réel. S'il s'agit d'un cyber-pirate, il peut utiliser les informations obtenues pour détourner des fonds de l'entreprise. Quoiqu'il en soit, il existe des logiciels de prochaine génération qui permettent de retracer l'historique complète de chaque document, afin que l'entreprise puisse avoir connaissance de l'utilisation des données voire même de l'utilisateur.

Si aucune donnée sensible n'a été violée, il n'y a pas de raison de penser qu'elles ne le seront pas à l'avenir. Ce qui signifie qu'il faut développer une stratégie de gestion de crise afin de limiter les dommages qui pourraient être causés par une violation significative des données. Sans une stratégie efficace, il est possible de vous retrouver en train de payer des primes d'assurance voire perdre la confiance de vos partenaires et de vos clients.

Expert Informatique et formateur spécialisé en sécurité Informatique, en cybercriminalité et en protection des données personnelles, Denis JACOPINI est en mesure de prendre en charge, en tant qu'intervenant de confiance, externe à l'entreprise, la sensibilisation de vos salariés au risque informatique et à la cybercriminalité afin de les informer des risques, des conséquences et des bonnes pratiques de l'informatique au quotidien.
Contactez-nous

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

Source : http://www.developpez.com/actu/81729/Comment-les-entreprises-pourraient-elles-mieux-se-proteger-des-attaques-informatiques-de-plus-en-plus-sophistiquees/

Gemalto a bien été attaqué, mais ses réseaux sécurisés seraient restés étanches

Gemalto a bien été attaqué, mais ses réseaux sécurisés seraient restés étanches

Oui des attaques ont bien été détectées, mais Gemalto précise que ses réseaux sécurisés n'ont pas été pénétrés. Le vol massif de clés de SIM ? Impossible en 2010 du fait du chiffrement des échanges avec les opérateurs. Et d'autres facteurs permettent de pondérer les conséquences de ces attaques.

Un peu moins d'une semaine après la publication par The Intercept de documents décrivant des attaques contre des fournisseurs de cartes SIM, Gemalto, un des acteurs ciblés, a présenté les conclusions de ses investigations.
Et cette analyse semble effectivement confirmer le scénario d'une opération conjointe de deux agences de renseignement étrangères, la NSA et le GCHQ.

Des attaques « graves et sophistiquées », mais sur des réseaux périphériques
« Nous avons analysé la méthode décrite dans les documents et les tentatives d'intrusion sophistiquées que nous avions détectées sur notre réseau en 2010 et 2011 rendent l'information qui est décrite probable » déclare Olivier Piou, le directeur général de Gemalto.
Pour étayer cette conclusion, l'entreprise s'appuie sur la détection de « deux attaques particulièrement sophistiquées qui pourraient effectivement être liées à cette opération ». Le directeur de la sécurité de Gemalto, Patrick Lacruche, décrit ces deux attaques précises en 2010.
La première a été identifiée en juin de cette année. « Nous avons identifié une activité suspecte sur un de nos sites français. Un tiers a essayé de se connecter à un de nos réseaux que nous appelons Office, c'est-à-dire le réseau de communication des employés entre eux et avec le monde extérieur. »
Toujours en 2010, un second incident est détecté par l'équipe de sécurité : « Il s'agissait de faux emails envoyés à un de nos clients opérateurs mobiles en usurpant des adresses email authentiques de Gemalto. Ces faux emails contenaient un fichier attaché qui permettait le téléchargement d'un code malveillant. » Le client sera alerté et l'attaque signalée aux autorités.
Suivront sur la « même période » plusieurs « tentatives d'accès aux ordinateurs » de salariés de l'entreprise, ciblés en raison vraisemblablement de leurs « contacts réguliers » avec les clients de Gemalto.

Des vols de clés ? Possibles dans des « cas exceptionnels »
Si les attaques, qualifiées de « graves et sophistiquées », semblent avérées, le fournisseur de cartes SIM exclut en revanche qu'elles aient pu aboutir à la compromission de ses produits de sécurité ou à l'interception massive de clés de chiffrement.
Patrick Lacruche l'assure, ces attaques n'ont affecté « que des parties externes des réseaux Gemalto ». Or les « clés de cryptage et plus généralement les données clients ne sont pas stockées sur ces réseaux ».
Car, poursuit-il, « nous n'avons rien détecté d'autre, que ce soit dans les parties internes du réseau de notre activité SIM » ou « dans les parties du réseau sécurisé d'autres produits comme les cartes bancaires ». Ces « réseaux sont isolés entre eux et ne sont pas connectés au monde extérieur » indique encore le responsable sécurité.
L'entreprise reconnaît cependant que des interceptions de clés ont pu, dans des « cas exceptionnels », éventuellement être réalisées. Pour le justifier, Gemalto fait savoir qu'il avait « dès avant 2010 », mis en place un système d'échange sécurisé avec ses clients. Ce chiffrement empêcherait donc que les clés, en cas d'interception, puissent être exploitées ensuite pour des écoutes.

Au pire, seuls les réseaux 2G seraient affectés par des écoutes
Serge Barbe, le vice-président de Gemalto en charge des produits et services, a apporté d'autres informations permettant selon lui de relativiser les conséquences de ces attaques et les risques d'espionnage pour les clients des opérateurs.

Ainsi, si des clés de chiffrement de SIM avaient effectivement été dérobées, celles-ci ne permettraient de procéder à des écoutes que sur des communications 2G. Or, la faiblesse de cette technologie, « pensée dans les années 80 », était déjà connue.

« Donc si les clés de cryptage de cartes SIM 2G étaient interceptées par des agences de renseignement, il leur était techniquement possible d'espionner les communications » reconnaît Serge Barbe, qui précise toutefois que ces cartes étaient pour la plupart des cartes prépayées, c'est-à-dire dont le cycle de vie était réduit.

Mais qu'en est-il alors des SIM des générations suivantes ? Le vol auprès du fournisseur ou de l'opérateur des clés permet-il des opérations d'espionnage des communications ? Non selon Gemalto pour qui la faiblesse des carte 2G a été « éliminée » par la suite.

La sécurité a « encore été largement renforcée, je dirais même repensée, avec l'arrivée des cartes SIM de troisième et quatrième générations » revendique Serge Barbe. « L'interception et le décryptage en cours d'échange entre le fournisseur et l'opérateur ne permettrait pas aux pirates de se connecter aux réseaux 3G ou 4G et donc par conséquent d'espionner les communications ».

« Les cartes 3G et 4G ne pouvaient pas être affectées par l'attaque qui est décrite » dans les documents attribués aux GCHQ. Malgré tout, « ces produits plus récents ne sont toutefois pas utilisés universellement dans le monde » tient à préciser le représentant de Gemalto.

Pour le patron de Gemalto, Olivier Piou, une conclusion s'impose dans cette affaire d'espionnage : « l'encryptage systématique des échanges et l'utilisation de cartes de dernière génération, couplés à des algorithmes personnalisés pour chaque opérateur, sont la meilleure réponse à ce genre d'attaque. » Bref, une bonne opportunité finalement pour l'entreprise de faire la promotion de ses produits et pratiques de sécurité.

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

Source : http://www.zdnet.fr/actualites/gemalto-a-bien-ete-attaque-mais-ses-reseaux-securises-seraient-restes-etanches-39815336.htm
Par Christophe Auffray

Sécurité : OS X et iOS auraient été les systèmes les plus vulnérables en 2014

Sécurité : OS X et iOS auraient été les systèmes les plus vulnérables en 2014

Le spécialiste des solutions de sécurité GFI a publié un nouveau rapport mesurant le degré de vulnérabilité des systèmes d'exploitation en 2014. L'OS de Microsoft ne ferait plus partie du top 3.

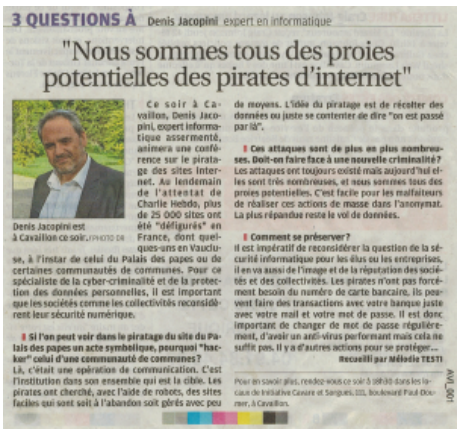
Au sein de la base de vulnérabilités nationale hébergée par le gouvernement américain, 7038 vulnérabilités auraient été rapportées au total en 2014, à raison de 19 par jour en moyenne, selon GFI. Celles-ci concernent aussi bien les systèmes d'exploitation que les applications. A titre de comparaison, en 2013, 4794 failles avaient été ajoutées.
L'année dernière 24% de ces vulnérabilités ont été jugées sérieuses, soit 1887 contre 1492 l'année précédente. Selon GFI, les applications seraient responsables pour 83% de ces failles de sécurité contre 13% pour les systèmes d'exploitation eux-mêmes et 4% pour le matériel.
C'est OS X qui se trouve en pôle position des systèmes vulnérables avec 147 mentions saisies au sein de la base de données dont 64 jugées importantes. En seconde place, nous retrouvons iOS avec 127 failles devant le kernel de Linux. « Bien que les systèmes de Microsoft ont toujours un nombre considérable de vulnérabilités, il est intéressant de noter qu'ils ne sont plus dans le top 3 », affirme GFI. Reste que combinés, Windows Server 2008 et 2013 ainsi que Windows Vista, 7, 8, 8.1 et RT détiennent au total 4010 failles rapportées dont 168 importantes.
Les navigateurs trônent en tête des logiciels les moins sécurisés avec, en première place du palmarès, Internet Explorer suivi de Chrome et Firefox. Le plugin Flash Player et la plateforme Java sont respectivement en quatrième et cinquième place devant le client mail Thunderbird.

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

S o u r c e
http://pro.clubic.com/it-business/securite-et-donnees/actualite-755309-securite-os-ios-auraient-systemes-vulnerables-2014.html?&xvc_mode=f&xvc_campaign=NL_ClubicPro_New_24/02/2015&partner=-&xvc_position=873687217&xvc_misc=-&crmID=639453874_873687217&estat_url=http%3A%2F%2Fpro.clubic.com%2Fit-business%2Fsecurite-et-donnees%2Factualite-755309-securite-os-ios-auraient-systemes-vulnerables-2014.html

---

Nous sommes tous des proies potentielles des pirates d'Internet



3 QUESTIONS À Denis Jacopini expert en informatique

"Nous sommes tous des proies potentielles des pirates d'internet"

Ce soir à Cavaillon, Denis Jacopini, expert informatique assermenté, animera une conférence sur le piratage des sites internet. Au lendemain de l'attentat de Charlie Hebdo, plus de 25 000 sites ont été "défigurés" en France, dont quelques-uns en Vaucluse, à l'instar de celui du Palais des papes ou de certaines communautés de communes. Pour ce spécialiste de la cyber-criminalité et de la protection des données personnelles, il est important que les sociétés comme les collectivités reconsidèrent leur sécurité numérique.

Denis Jacopini est à Cavaillon ce soir. PHOTO DR

Si l'on peut voir dans le piratage du site du Palais des papes un acte symbolique, pourquoi "hacker" celui d'une communauté de communes ?
Là, c'était une opération de communication. C'est l'institution dans son ensemble qui est la cible. Les pirates ont cherché, avec l'aide de robots, des sites faciles qui sont soit à l'abandon soit gérés avec peu de moyens. L'idée du piratage est de récolter des données ou juste se contenter de dire "on est passé par là".

Ces attaques sont de plus en plus nombreuses. Doit-on faire face à une nouvelle criminalité ?
Les attaques ont toujours existé mais aujourd'hui elles sont très nombreuses, et nous sommes tous des proies potentielles. C'est facile pour les malfaiteurs de réaliser ces actions de masse dans l'anonymat. La plus répandue reste le vol de données.

Comment se préserver ?
Il est impératif de reconsidérer la question de la sécurité informatique pour les élus ou les entreprises, il en va aussi de l'image et de la réputation des sociétés et des collectivités. Les pirates n'ont pas forcément besoin du numéro de carte bancaire, ils peuvent faire des transactions avec votre banque juste avec votre mail et votre mot de passe. Il est donc important de changer de mot de passe régulièrement, d'avoir un anti-virus performant mais cela ne suffit pas. Il y a d'autres actions pour se protéger…

Recueilli par Mélodie TESTI

Pour en savoir plus, rendez-vous ce soir à 18h30 dans les locaux de Initiative Ceinture et Sangles, 111, boulevard Paul Doumer, à Cavaillon.

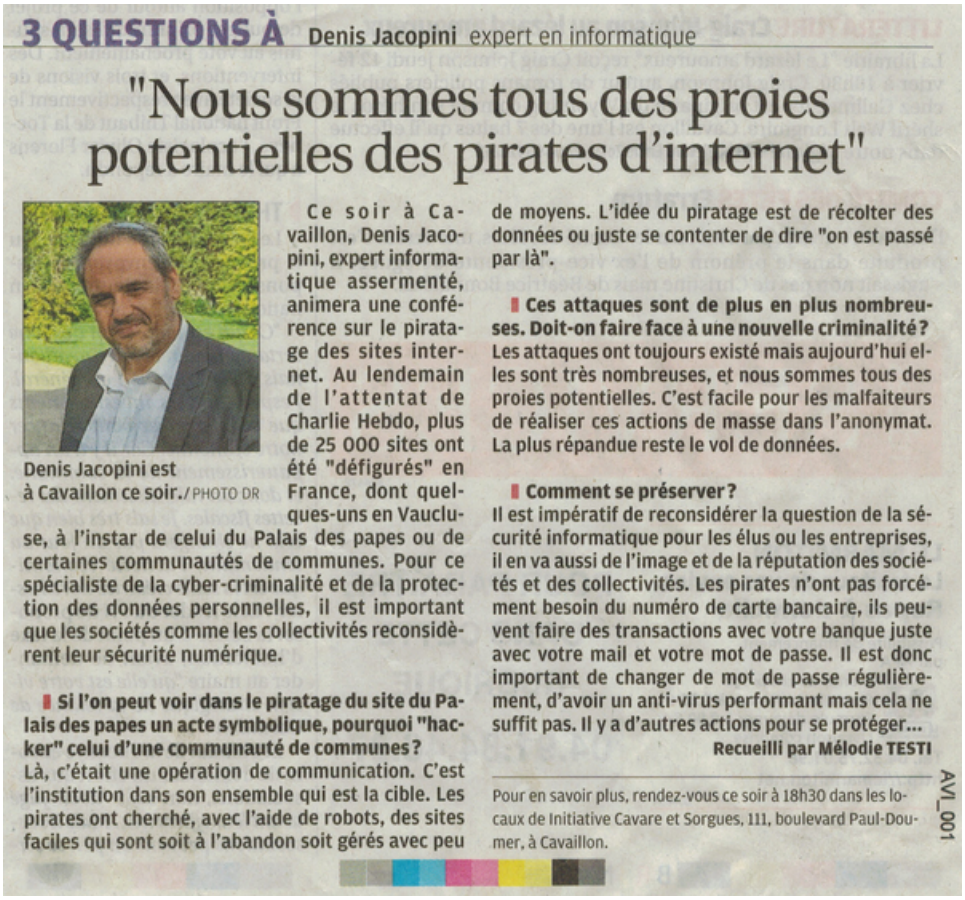
AVO_001

Nous sommes tous des proies potentielles des pirates d'Internet

A la suite des attentats de Paris à Charlie Hebdo le 7 janvier 2015, plus de 25000 sites Internet ont été « défigurés » en France. Dans le but de continuer à sensibiliser les chefs d'entreprises et Elus qui ne connaissent ou ne maîtrisent pas encore bien le sujet, le 10 février 2015, Denis JACOPINI a animé une conférence à Cavaillon.

Victime d'actes illicites, les cibles de la cybercriminalité se sentent démunies face à ce risque incoercible. Après un état des lieux, la conférence à dévoilé les principales raisons pour lesquelles la cybercriminalité sévit aussi facilement.

Enfin, des solutions de bon sens ont été présentées, concernant à la fois la mise en place de mesures de sécurité, mais aussi le respect de la loi informatique et libertés chargée d'encadrer l'usage et la protection des données personnelles, des données à caractère personnel.



3 QUESTIONS À Denis Jacopini expert en informatique

"Nous sommes tous des proies potentielles des pirates d'internet"

Denis Jacopini est à Cavaillon ce soir./PHOTO DR

Ce soir à Cavaillon, Denis Jacopini, expert informatique assermenté, animera une conférence sur le piratage des sites internet. Au lendemain de l'attentat de Charlie Hebdo, plus de 25 000 sites ont été "défigurés" en France, dont quelques-uns en Vaucluse, à l'instar de celui du Palais des papes ou de certaines communautés de communes. Pour ce spécialiste de la cyber-criminalité et de la protection des données personnelles, il est important que les sociétés comme les collectivités reconsidèrent leur sécurité numérique.

Si l'on peut voir dans le piratage du site du Palais des papes un acte symbolique, pourquoi "hacker" celui d'une communauté de communes ?

Là, c'était une opération de communication. C'est l'institution dans son ensemble qui est la cible. Les pirates ont cherché, avec l'aide de robots, des sites faciles qui sont soit à l'abandon soit gérés avec peu de moyens. L'idée du piratage est de récolter des données ou juste se contenter de dire "on est passé par là".

Ces attaques sont de plus en plus nombreuses. Doit-on faire face à une nouvelle criminalité ?

Les attaques ont toujours existé mais aujourd'hui elles sont très nombreuses, et nous sommes tous des proies potentielles. C'est facile pour les malfaiteurs de réaliser ces actions de masse dans l'anonymat. La plus répandue reste le vol de données.

Comment se préserver ?

Il est impératif de reconsidérer la question de la sécurité informatique pour les élus ou les entreprises, il en va aussi de l'image et de la réputation des sociétés et des collectivités. Les pirates n'ont pas forcément besoin du numéro de carte bancaire, ils peuvent faire des transactions avec votre banque juste avec votre mail et votre mot de passe. Il est donc important de changer de mot de passe régulièrement, d'avoir un anti-virus performant mais cela ne suffit pas. Il y a d'autres actions pour se protéger...

Recueilli par Mélodie TESTI

Pour en savoir plus, rendez-vous ce soir à 18h30 dans les locaux de Initiative Cavare et Sorgues, 111, boulevard Paul-Doumer, à Cavaillon.

AVI_001

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

Source : http://www.horizon2020.gouv.fr/pid29774/securite.html

Cyber-attaques : Denis Jacopini, expert, alerte – Article dans Midi Libre Gard…

13

	Cyber-attaques : Denis Jacopini, expert, alerte – Article dans Midi Libre Gard…

Avec Denis Jacopini, expert informatique près la cour d'appel de Nîmes et consultant auprès des entreprises, après une série de piratages de site internet en France et dans le Gard.Après les attentats du 7 janvier, de nombreux sites internet d'institutions locales ou religieuses en France ont été piratés par des groupes de hackers se présentant comme des islamistes, dont celui du palais des Papes à Avignon, victime d'un «défaçage» (remplacement de la page d'accueil du site) par un groupe dénommé Fallaga team . Ces phénomènes de piratage ne sont pas nouveaux et s'accentuent. Ils sont imputables à différents types de malfaiteurs et se matérialisent de manière très différente. Décryptage des cyber-attaques avec Denis Jacopini, expert judiciaire près la cour d'appel de Nîmes et des juridictions du Gard, du Vaucluse, de l'Ardèche et de la Drôme. Denis Jacopini : « Les chefs d'entreprise ne sont pas assez sensibilisés. » DR Qu'est-ce qu'une cyber-attaque ? C'est une attaque informatique utilisant les réseaux de télécommunication et cela existe depuis qu'Internet s'est répandu dans le…


Bagnols

Midi Libre midilibre.fr MERCREDI 11 FÉVRIER 2015 | 3

Cyber-attaques : « Les sociétés ne se protègent pas »

Entretien | Avec Denis Jacopini, expert informatique près la cour d'appel de Nîmes et consultant auprès des entreprises, après une série de piratages de site internet en France et dans le Gard.

Contexte

« On peut stopper le phénomène si on change les mentalités »

GROS PLAN

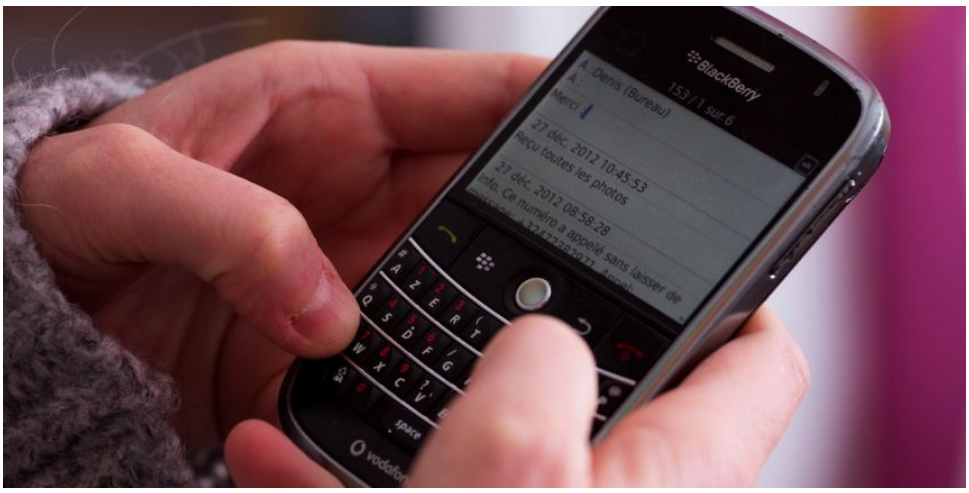
La e-reputation

Gard : 20 faits de piratage de sites en 2014 et cinq en 2015

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

Source : http://www.midilibre.fr/2015/02/11/cyber-attaques-les-societes-ne-se-protegent-pas,1123222.php

Attention, votre employeur a désormais le droit de fouiller dans les SMS de votre téléphone pro !



Il faudra désormais prendre garde à ce que vous écrivez depuis votre téléphone portable professionnel… Photo : Sipa

Attention, votre employeur a désormais le droit de fouiller dans les SMS de votre téléphone pro !

La Cour de cassation a récemment rendu un arrêt qui donne aux SMS échangés sur les téléphones portables mis à disposition par les employeurs une présomption de « caractère professionnel ». Si vous voulez être certain que vos textos privés ne puissent être utilisés contre vous, il faudra désormais inscrire les mots « personnel » ou « perso » dans vos messages…

C'est une décision passée totalement inaperçue, mais qui concerne des centaines de milliers de salariés : tous ceux qui se sont vus mettre à disposition un téléphone portable par leur employeur. La Cour de cassation, dans un arrêt rendu le 10 février, que metronews s'est procuré, a validé le principe selon lequel les SMS envoyés ou reçus par cet appareil « sont présumés avoir un caractère professionnel ». Conséquence : « l'employeur est en droit de les consulter en dehors de la présence de l'intéressé, sauf s'ils sont identifiés comme étant personnels ».

Un processus pas « déloyal »

La plus haute juridiction de l'ordre judiciaire était invitée à statuer sur le litige opposant deux sociétés de courtage, GFI Securities Limited et Newedge. Cette dernière, reprochant à son concurrent d'avoir été déloyal en débauchant « un grand nombre » de ses salariés, avait utilisé comme preuve pour l'attaquer des SMS échangés entre ses anciens employés, qui évoquaient leur départ concerté de l'entreprise. En l'occurrence, Newedge négociant des produits financiers, tous les messages envoyés et reçus par ses salariés étaient automatiquement enregistrés sur un serveur informatique, conformément à la législation en vigueur.

Cette filiale de la Société Générale n'a donc eu qu'à effectuer une recherche à base de mots-clé pour retrouver et faire constater par huissier les SMS en question. Qui, pour la cour de Cassation comme pour la Cour d'appel de Paris dans un arrêt rendu il y a deux ans, constituent bien des preuves recevables : leur utilisation ne peut être considérée comme un « processus déloyal » ni « être assimilée à l'enregistrement d'une communication téléphonique privée effectuée à l'insu de l'auteur des propos ».

Pour les emails, c'était déjà le cas

Si dans cette affaire, les SMS avaient la particularité d'être stockés sur un serveur, la décision « est destinée à faire jurisprudence » pour tous les salariés à qui l'employeur a mis un téléphone portable à disposition, assure à metronews maître Jean-Philippe Duhamel, avocat au Conseil d'Etat et à la Cour de cassation. Avec cette décision souligne-t-il, la justice a manifesté « un souci de cohérence et de simplicité ». La Cour de cassation avait en effet déjà pris des arrêts similaires en ce qui concerne les fichiers détenus sur un ordinateur de travail ou les emails envoyés par un salarié depuis sa boîte pro. Depuis mai 2013 ainsi, l'employeur est dans son droit s'il ouvre en dehors de la présence de son employé un courrier électronique qui n'a pas été identifié comme personnel.

Comment éviter que vos textos privés ne puissent être utilisés contre vous ? La seule solution, explique Jean-Philippe Duhamel, est d'y intégrer « une mention les identifiant comme personnels, par exemple en les faisant commencer par les mots 'personnel' ou 'perso' ». Un peu contraignant pour des messages courts qui, contrairement aux emails, ne comportent le plus souvent pas de champ « objet ». Il existe toutefois une autre solution, plus radicale : réserver vos communications privées à votre téléphone personnel.

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

Source : http://www.metronews.fr/info/attention-votre-employeur-a-desormais-le-droit-de-fouiller-dans-les-sms-de-votre-telephone-pro/mobs!1pxxcsNP7VEA/
Par Gilles DANIEL

Microsoft donne un coup de fouet au HTTPS dans Internet Explorer

Microsoft donne un coup de fouet au HTTPS dans Internet Explorer

Microsoft renforce la sécurité et la consultation des sites Internet au sein de son navigateur Web Internet Explorer en déployant le système HSTS.

Le support du HTTP Strict Transport Security (HSTS) fait son entrée dans la version d'Internet Explorer proposée au sein de la mouture de test de Windows 10.
Ce système renforce la sécurité des communications entre l'internaute et les serveurs Web. Il permet de s'assurer que la connexion est sécurisée. Si le certificat de chiffrement n'est pas correct, la connexion au site ne sera pas possible.
De plus, le mélange de contenus sécurisés et en clair au sein d'une même page Web n'est pas permis par le HSTS.
Une liste de sites Web devant utiliser le HTTPS par défaut est fournie avec Internet Explorer.
Elle s'appuie sur celle créée pour le projet Chromium. Des mécanismes spécifiques permettent également de s'assurer que l'internaute ne basculera pas en HTTP lorsqu'il a débuté sa visite sur un site en HTTPS, explique Silicon.fr.
L'objectif est de s'assurer que la séance de surf sur un site Web s'effectue de bout en bout de façon sécurisée, en HTTPS, c'est-à-dire de manière chiffrée.
Les mauvaises langues remarqueront que Microsoft a pris son temps. Le HSTS est en effet pris en compte depuis les versions 4 de Firefox, Chrome et Chromium, soit depuis plusieurs années déjà.
Les serveurs Web open source les plus populaires (Apache, Nginx, etc.) sont aujourd'hui compatibles avec ce protocole de sécurité. L'offre IIS de Microsoft peut également être configurée pour prendre en compte le HSTS.

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

S o u r c e : http://www.itespresso.fr/internet-explorer-microsoft-donne-un-coup-de-fouet-au-https-88802.html#ZlJQDlMwDry82Trz.99