Les Provençaux protègent mal leurs données personnelles sur le Net | Le Net Expert

Les Provençaux protègent mal leurs données personnelles sur le Net | Le Net Expert

Le gestionnaire de mots de passe Dashlane a réalisé une étude anonyme auprès de 45 000 utilisateurs français afin d'évaluer le niveau de sécurité de leurs mots de passe. Si toutes les régions françaises ne sont pas exemplaires (aucune ne dépasse la note de 55 sur 100), la région Paca est classée avant-dernière.

Hackers ou cyber-escrocs, pas une semaine ne passe sans qu'un utilisateur ne voit ses identifiants et mots de passe usurpés sur la toile. Le fléau du piratage informatique est devenu une donnée constante pour les internautes. Si le cyber piratage est aujourd'hui un jeu d'enfant, notamment sur les réseaux sociaux, les utilisateurs s'obstinent pourtant à ne pas protéger suffisamment leurs données personnelles.
C'est en tout cas ce qu'a révélé Dashlane, le gestionnaire de mots de passe, qui a publié le palmarès des régions les plus soucieuses de la sécurité de leurs mots de passe. Ce classement découle d'une étude anonyme réalisée en décembre dernier auprès de 45 000 utilisateurs français. Chaque région s'est ainsi vue attribuer un score moyen de sécurité, entre 0 et 100, en fonction du niveau de sécurité des mots de passe des habitants de cette région.

La région Paca figure parmi les mauvais élèves
Si toutes les régions françaises ne sont pas exemplaires (aucune ne dépasse la note de 55), la région Paca est classée avant-dernière, avec un petit score de 49,7, à peine plus que sa voisine du Languedoc-Roussillon qui peine à atteindre le seuil de 49,4.
Pour Guillaume Desnoes, Responsable des marchés européens de Dashlane : « On observe un noyau de bons élèves, la Franche-Comté, Rhône Alpes et Auvergne, alors que le Languedoc-Roussillon et la Provence-Alpes-Côte d'Azur ferment la marche. Ce classement illustre des différences d'état d'esprit dans la manière dont les gens envisagent leur sécurité en ligne », déclare-t-il.
A l'occasion de la neuvième journée mondiale de la protection des données personnelles, le 28 janvier dernier, la Commission nationale de l'informatique et des libertés (CNIL) chargée de la protection des données en France, a rappelé quelques gestes simples pour plus de cyber sécurité : limiter la diffusion de ses données personnelles sur les réseaux sociaux, changer régulièrement ses mots de passe sur les sites internet, ou encore signaler les spams sont autant de pare-feu pour se protéger des hackers.

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

Source : http://www.laprovence.com/article/actualites/3282901/les-provencaux-protegent-mal-leurs-donnees-personnelles-sur-le-net.html
Par Michelangelus/Shutterstock.com

La sécurité Informatique n'intéresse pas assez les dirigeants

La sécurité Informatique n'intéresse pas assez les dirigeants

Une étude réalisée par Ponemon Institute montre le décalage entre les responsables sécurité des entreprises et leurs directions générales. Ces dernières se montrent peu sensibles aux risques encourus.

Bien que les responsables de la sécurité des systèmes d'information considèrent que le cybercrime et le cyberterrorisme seront des menaces majeures dans les prochaines années, ils estiment également que les cadres dirigeants de leurs entreprises ne comprennent pas complètement l'impact de ces menaces, ce qui représente un réel obstacle pour une prévention efficace.
Ainsi est présentée l'étude menée par Ponemon Institute auprès de 1006 responsables sécurité aux USA, en Europe, Moyen-Orient et Afrique. Selon les résultats, 78% des répondants affirment que les comités exécutifs n'ont pas reçu de briefing sur la stratégie en matière de cybersécurité durant les 12 derniers mois et 66% pensent que la direction ne voit pas la cybersécurité comme une priorité stratégique.
« Les responsables sécurité sont généralement d'excellents techniciens mais ils ne parlent pas le langage du business », déclarait Larry Ponemon à SC Magazine. En dépit des attaques quotidiennes, les responsables des entreprises demeurent méfiants quant aux investissements à réaliser. « Le retour sur investissement est dévastateur pour la sécurité », poursuit M. Ponemon. « La sécurité n'a pas un bénéfice net prédictif ». Toutefois, M. Ponemon constate une évolution dans la formation de ces responsables de la sécurité du SI. En effet, de plus en plus de titulaires de ces postes dans les grandes entreprises américaines disposent à la fois d'une formation technique de haut niveau et également d'une formation business de type MBA.
L'étude met également en lumière le fort turnover qui existe dans ces professions, une situation qu'il explique en partie par l'absence de plan de carrière proposé à ces personnels. « En moyenne, un responsable sécurité reste 2,1 années en poste, loin des 6 années pour les autres cadres IT. A cause de cette absence d'évolution, ils préfèrent partir pour gagner un meilleur salaire ».
De plus de nombreux dirigeants considèrent – à tort – que leurs entreprises ne peuvent être ciblées. L'un des commanditaires de l'étude précise : « beaucoup d'entreprises ne se considèrent pas comme des cibles qui intéressent les hackers ».
Les attaques zero-day, les malwares sur mobiles, le phishing le vol de données dans le cloud et les attaques contre les infrastructures réseaux sont les cinq menaces prioritaires identifiées par les entreprises. L'un des nouveaux champs va être l'Internet des objets pour lesquel seulement 1/3 des entreprises s'estiment prêtes du point de vue sécurité.

Expert Informatique et formateur spécialisé en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel, Denis JACOPINI est 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.mag-securs.com/news/articletype/articleview/articleid/34569/la-securite-it-n-interesse-pas-assez-les-dirigeants.aspx

---

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

Université Lyon 3 : 88.000 contacts ont été dérobés par les pirates informatiques

Université Lyon 3 : 88.000 contacts ont été dérobés par les pirates informatiques

Les services de l'université Lyon 3 avait d'abord parlé d'une fuite d'environ 5000 contacts pour la plupart étudiants, cependant depuis une plus récente information du site lepoint.fr, l'université aurait reconnu avoir fait fuité par erreur, 88 000 contacts. Un cas plus grave que le premier dont on vous avez fait écho au début du mois de février. Pour rappel, les fichiers dérobés contenaient les noms, prénoms, date de naissance, informations sur le cursus suivis, adresses personnelles postale et électronique, numéros d'étudiants fixe et mobile, mais aussi des conversations échangées par e-mail entre les étudiants et le personnel de l'université ou encore les coordonnées d'entreprises partenaires de l'université.

Des mesures contre les cyberattaques prises en décembre
Contactée par lepoint, l'université « a regretté un cafouillage de communication », avant qu'Yves Condemine, le directeur des systèmes d'informations (DSI), explique que « la base de données piratées concerne 88 000 contacts ». Bien qu'aujourd'hui « les problèmes sont réglés », il affirme néanmoins que « des mesures avaient été prises dès décembre », après des alertes envoyées par un des étudiants de l'université. Le directeur des services d'informations reste cependant « encore prudent » dans la surveillance du réseau même si « rien ne permet aujourd'hui de penser que (l')infrastructure soit compromise », affirme t-il.

L'agence de cyberdéfense n'analysera pas le réseau de l'université
Cependant, l'université n'a pas souhaité l'intervention de l'agence de cyberdéfense. Malgré l'urgence de la situation et la charge de travail nécessaire pour analyser la totalité du réseau, l'université a souhaité s'occuper seule de cette tâche. L'incident à néanmoins était signalé à son ministère de tutelle qui a contacté l'Anssi, l'agence nationale de cyberdéfense, sans pour autant la saisir. « Nous sommes restés en contact avec l'Anssi, via le ministère de l'Enseignement supérieur », affirme Yves Condemine à lepoint. Pas très rassurant si l'agence de cyberdéfense ne peut ni analyser, ni trouver d'éventuelles portes dérobées dans le réseau, ni même remonter jusqu'aux pirates pour comprendre leurs intentions en piratant la base de données d'une université.

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

Source : http://www.digischool.fr/a-la-une/universite-lyon-3-contacts-derobes-pirates-informatiques-26701.php

---

92% des salariés français sont incapables de détecter du phishing

92% des salariés français sont incapables de détecter du phishing

Le facteur humain est toujours le point faible en matière de cybersécurité. Il s'avère que 92% des salariés français sont incapables de détecter les tentatives de phishing les plus courantes. Intel Security estime que le coût global de la cybercriminalité dans le monde peut être estimé à quelque 445 milliards de dollars. Il est par ailleurs estimé que deux tiers des courriels envoyés dans le monde sont des spams destinés à extorquer de l'information ou de l'argent.

Une étude conjointe menée par McAfee Labs, filiale d'Intel Security, et le centre de cybercriminalité européen d'Europol (EC3) révèle toute l'importance du facteur psychologique dans la réussite des attaques informatiques. « **Le facteur humain est toujours le point faible en matière de cybersécurité** », a expliqué Raj Samani, le directeur technique d'Intel Security.

« Les entreprises de tous les secteurs industriels, toutes les tailles et toutes les régions du monde sont en danger en raison du facteur social », résume Raj Samani. Il explique qu'« il est important de comprendre que les cybercriminels s'avèrent souvent être de bons psychologues et que le facteur humain est souvent utilisé comme un point d'entrée pour les cyberattaques » en précisant que les hackers savent parfaitement user de la séduction, du respect de l'autorité, du conformisme social et du besoin de retourner une faveur, sans oublier la loyauté ou la peur de rater une opportunité.

Cette étude révèle par exemple qu'en France, 92% des salariés sont incapables de détecter les tentatives de phishing les plus courantes et les plus fréquemment utilisées.

Ce résultat est d'autant plus inquiétant pour les entreprises françaises que le rapport révèle que 18% des utilisateurs visés par un courriel d'hameçonnage deviennent finalement des victimes après avoir cliqué sur un lien frauduleux.

C'est ainsi que Raj Samani conclut en déclarant qu'«il est crucial pour les entreprises d'éduquer leurs employés sur la cybersécurité en plus des mesures prises sur les niveaux opérationnels et techniques».

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.linformatique.org/cybercriminalite-92-des-salaries-francais-sont-incapables-de-detecter-du-phishing/
Par Emilie Dubois

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.

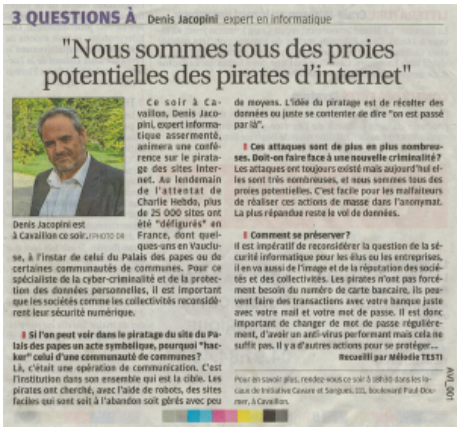
Au sein de la base de vulnérabilités nationale hébergée par le gouvernement américain, 7038 vulnérabilités auraient été rapportées au total en 2014, à raison de 19 par jour en moyenne, selon GFI. Celles-ci concernent aussi bien les systèmes d'exploitation que les applications. A titre de comparaison, 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 4018 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?&svc_mode=MG&svc_campaign=NL_ClubicPro_New_24/02/2015&partner=-&svc_position=873687217&svc_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. LP/HOTO 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?
LA, 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 l'initiative Cavaire et Sanguis, 103, boulevard Paul Doumer, à Cavaillon.

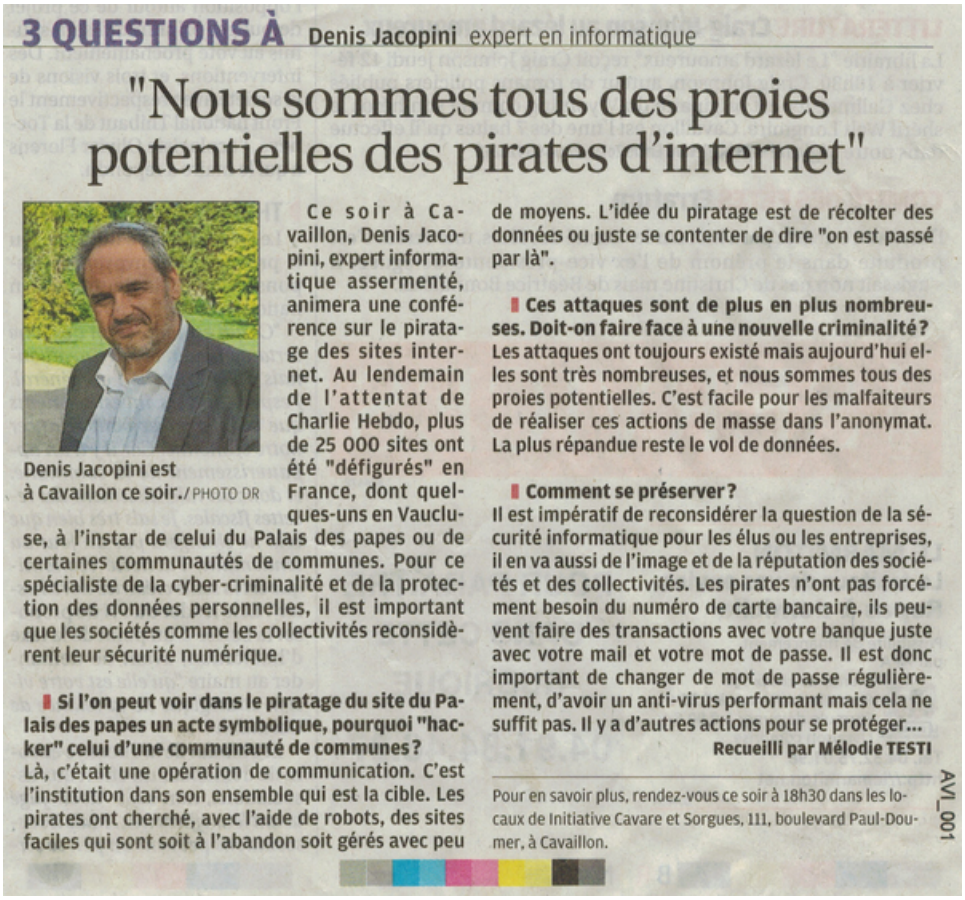
AVL_001

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

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

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 (lire notre édition du 16 janvier). 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.

Qu'est-ce qu'une cyber-attaque ?

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

Il semble impossible, quelle que soit la structure attaquée, de s'en prémunir.

A-t-on une idée du nombre de victimes que font ces attaques ?

Mais cette lutte coûte cher pour de petites structures comme une mairie !

GROS PLAN

La e-reputation

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

Départs régionaux et voyages accompagnés

HAVAS VOYAGES

Midi Libre

SALON DE L'AGRICULTURE À PARIS

330€*

3 jours / 2 nuits

Du 27 FÉVRIER au 01 MARS 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

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…

Source : http://www.itespresso.fr/internet-explorer-microsoft-donne-un-coup-de-fouet-au-https-88802.html#ZlJQDlMwDry82Trz.99

TrueCrypt n'est pas mort,

l’audit bouge encore

TrueCrypt n’est pas mort, l’audit bouge encore

Les développeurs chargés d’auditer la sécurité de TrueCrypt ont donné quelques nouvelles de leur avancement. Le développement du logiciel de chiffrement avait été interrompu brusquement durant l’été 2014, soulevant de nombreuses inquiétudes quant à la fiabilité du programme.

L’affaire TrueCrypt fait partie des mystères de la cybersécurité: en mai, le site web distribuant le logiciel annonçait la fin du développement, ajoutant que TrueCrypt n’était « plus sûr » et que les utilisateurs qui décidaient de s’appuyer dessus s’exposaient « à des failles de sécurité non comblées.»
Une nouvelle version du logiciel était distribuée par la même occasion, fortement déconseillée par la plupart des experts en cybersécurité. Un coup dur : TrueCrypt était l’un des projets considérés comme les plus solide en matière de protection des données et, aux dernières nouvelles, donnait encore du fil à retordre aux analystes de la NSA selon des documents datés de 2012.

Doutes et remises en question
Un audit de TrueCrypt avait néanmoins été initié en 2013, en s’appuyant sur un crowdfunding réalisé auprès de la communauté afin de financer un examen en profondeur du code source du logiciel. Si celui-ci avait été lancé bien avant l’arrêt brutal du développement, ses résultats sont aujourd’hui très attendus par les utilisateurs de TrueCrypt. Mais depuis juin 2014, aucune nouvelle n’avait émané du projet, suscitant les interrogations de la communauté.
Sentant monter l’inquiétude, Matthew Green, le chercheur à l’origine du projet d’audit a posté une mise à jour faisant le point sur l’avancement des travaux du groupe. Et c’est bien la moindre des choses : le financement de cet audit a été réalisé sur une opération de crowdfunding, qui avait rassemblé 70.000 dollars au mois de décembre 2013. Compte tenu de la somme récoltée auprès de donateurs et de l’actualité inquiétante du développement de Truecrypt, l’initiative menée par Matthew Green et Kenn White est surveillée de très près.
L’annonce de l’arrêt du développement a d’ailleurs suscité de nombreuses interrogations au sein du groupe chargé de l’audit du code : « L’annonce de l’abandon du projet par l’équipe de Truecrypt nous a poussé à reconsidérer notre approche. Etait-ce vraiment la bonne manière d’utiliser nos ressources ? Ne devrions-nous pas nous pencher au contraire sur les forks de Truecrypt qui émergeaient alors ? »
Matthew Green explique que le projet d’audit a donc connu une longue période de remise en question, mais que le projet est aujourd’hui à nouveau sur les rails, au travers d’un partenariat avec la société NCC Group North America, qui reprend en charge la poursuite de l’audit. Celui-ci entre dans sa seconde phase, après la publication d’une première partie qui avait noté quelques vulnérabilités mais aucune backdoor sérieuse au sein du code de la dernière version de TrueCrypt jugée fiable, la version 7.1a du logiciel.

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

Source : http://www.zdnet.fr/actualites/chiffrement-truecrypt-n-est-pas-mort-l-audit-bouge-encore-39815118.htm
Par Louis Adam