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

Big Boss is watching you: votre patron va adorer les objets connectés

Big Boss is watching you: votre patron va adorer les objets connectés

Cela commence par des programmes vous incitant à davantage marcher que votre patron ou vos collègues de travail. Pour votre santé. Puis, certains passent aux capteurs qui mesurent avec qui vous parlez. En France, la Cnil s'inquiète du risque d'émergence de nouvelles formes de discrimination.

En 2013, l'entreprise américaine Appirio, spécialisée dans l'informatique en nuage, a décidé de promouvoir un programme de «bien-être» auprès de ses employés pour tenter de réduire les coûts de sa mutuelle santé. Elle s'est alors tournée vers la technologie très en vogue des objets connectés, équipant les employés volontaires de bracelets enregistrant des données concernant leur activité physique dans l'espoir de les encourager à une meilleure hygiène de vie.

Les résultats ont été immédiats: un an plus tard, l'entreprise affirmait avoir économisé 5% sur les frais de mutuelle, soit près de 300.000 dollars.
Appario est loin d'être un cas isolé. Yahoo a ainsi offert en 2013 à 11.000 de ses employés des bracelets Jawbone. BP et eBay ont fait de même. Houston Methodist, propriétaire d'une chaîne d'hôpitaux, est même allé plus loin en offrant 6.000 bracelets à ses employés et en leur faisant miroiter un chèque de 10.000 dollars s'ils marchaient davantage que les directeurs de l'entreprise.
Selon le patron de Fitbit, l'entreprise spécialiste des bracelets connectés fournirait déjà «les programmes de bien-être de 30 entreprises du Fortune 500», classement regroupant les plus grandes entreprises américaines.

Le volontarisme contraint
Des employés en meilleur forme et des économies sur les soins… une logique gagnant-gagnant qui convainc, peut-être parce qu'elle paraît inoffensive.
Ces bracelets viennent pourtant enrichir l'arsenal de la «soft surveillance» au travail, un concept développé dès 2005 par Gary T. Marx, chercheur au MIT. Selon lui, les mécanismes de contrôle et de «flicage» ont amorcé une mutation grâce aux nouvelles technologies numériques.

Prenant l'exemple d'un contrôle à l'aéroport, il ne s'agit plus de dire que la fouille des passagers est obligatoire, mais que ceux-ci sont «libres de refuser s'ils désirent ne pas embarquer dans l'appareil». Plutôt que d'exercer un contrôle coercitif et dur, l'autorité développe des techniques pour obtenir un «volontarisme contraint». Pourquoi contraint? Parce que «ceux qui refuseraient de se porter volontaire pourraient être regardés comme ayant quelque chose à cacher, ou comme étant de mauvais citoyens».
Grâce à des capteurs, on peut mesurer vos activités relationnelles: qui parle avec qui? Combien de temps? Sur quel ton?

Transposé au domaine de l'entreprise, les employés peuvent choisir d'adhérer ou pas aux programmes de bien-être. Mais refuser revient à prendre le risque de ne pas être considéré comme un employé en phase avec l'entreprise, ou d'être soupçonné d'avoir une faible hygiène de vie, symbole peut-être d'un manque de volonté.

Faire comme les autres pour ne pas être exclu
Certaines entreprises comme Bank of America ou Cubist Phamarceuticals vont jusqu'à placer des capteurs sur les badges de leurs employés, qui collectent en permanence des informations relationnelles: qui parle à qui, combien de temps, sur quel ton… et accessoirement le nombre de pauses cafés ou cigarettes prises dans la journée. Pas du tout effrayés par le caractère panoptique et omniprésent de leur surveillance, les employeurs la justifient par le désir de comprendre ce qui fait qu'une équipe fonctionne ou pas.
Et les employés se laissent convaincre. L'argument financier n'est pas négligé, comme le notent des chercheurs américains dans une enquête publiée par l'Institut Data & Society:
«Les employés qui refusent d'adhérer au programme, mais qui souhaitent toujours bénéficier de la mutuelle de l'entreprise, peuvent payer 600 dollars annuels de plus que les employés qui se sont soumis au programme.»
La peur de la discrimination se révèle également être un puissant moteur pour se plier à la surveillance. Un refus de me soumettre à ces dispositif peut-il nuire à mon avancement, à ma prime, ou me placer dans la première charrette d'un futur plan social? Pourra-t-on me reprocher un manque de zèle, ou une maladie non dépistée?

La vie privée, comme au bureau: surveillée
La «soft surveillance» pose surtout des problèmes de vie privée. Illustration: en mars 2014, une employée de la firme pharmaceutique CVS a déposé plainte contre son employeur après que celui-ci avait exigé sous peine d'amende, dans le cadre de son programme de bien-être, qu'elle communique son poids et son niveau d'activité sexuelle.
La géolocalisation concentre particulièrement les critiques. La mise sous surveillance des véhicules d'entreprise ne réjouit pas nécessairement des employés qui bénéficiaient jusqu'alors d'une certaine marge d'autonomie avec leur outil de travail et qui s'inquiètent de savoir que leur patron peut en apprendre tant sur eux.
Une inquiétude qui a amené fin 2013 une bonne partie des techniciens français de l'entreprise Xerox à faire grève. Un boîtier devait être installé dans les véhicules de dépannage pour récupérer des données sur le parcours et la conduite des employés. Une initiative interprétée par les techniciens comme une nouvelle manière de les «pister continuellement», et peut-être, plus tard, d'indexer leurs primes individuelles sur ce flicage.

Les Etats-Unis conquis, la France un peu moins
Abandonner des pans de notre vie privée contre des avantages tarifaires?
Le marché américain a ouvert grands les bras à la «soft surveillance». La moitié des entreprises comptant plus de 50 employés ont des programmes de bien-être, et la popularité des objets connectés devrait rapidement rendre ceux-ci particulièrement invasifs. La législation encadre très peu ces pratiques, autorisant par exemple un employeur à poursuivre en justice un employé pour «vol de temps».
La France sera plus difficile à conquérir. La loi et la Cnil encadrent très strictement les prélèvements biométriques comme la mise sous surveillance des employés, que ce soit via des dispositifs relatifs à la géolocalisation, les caméras, l'activité en ligne ou les mails.
«Ce n'est pas tant la surveillance elle-même qui est encadrée, que l'exploitation de ces outils de surveillance», résume Anthony Bem, juriste spécialisé dans les nouvelles technologies. «Pour pouvoir employer un élément comme preuve, il faut que le salarié ait été informé de l'existence du dispositif de surveillance.» C'est le principe dit de la «loyauté de la preuve».
Un employeur doit aussi justifier l'installation d'un dispositif de surveillance par un intérêt légitime pour l'entreprise, c'est-à-dire qu'elle soit conforme à la nature du travail à accomplir et proportionnée quant au but recherché. Tout un arsenal législatif vient ensuite encadrer avec plus de finesse le déploiement de ces dispositifs, avec par exemple l'interdiction stricte d'installer une caméra filmant directement un poste de travail.

Une législation trop «soft»?
La législation est donc plutôt protectrice en ce qui concerne les cas de surveillance «classique» (plus de 800 plaintes par an). Mais sous l'influence des nouvelles technologies, les lignes se brouillent et la protection devient plus complexe.
Que ce soit dans l'utilisation de la voiture de service ou les heures supplémentaires à la maison avec l'ordinateur du travail, où s'arrête la vie professionnelle et où commence la vie privée? Que peut-on apprendre d'un employé en étudiant ses activités, et dans quel mesure cela peut-il influer sur sa carrière? La Cnil s'en inquiétait dans un document publié en juin 2014 et appelait le législateur à construire un «cadre éthique et juridique à la hauteur de ces enjeux».

« Dans les années à venir, les individus pourraient être priés d'apporter les preuves d'un comportement sain »
Texte de la Cnil

C'est le monde de l'assurance qui agit aujourd'hui en cheval de Troie de cette «soft surveillance» made in America. Les assureurs promettent des réductions de coûts de mutuelle pour les entreprises et des effectifs en meilleure forme, des réductions tarifaires pour les assurés. Axa a ainsi lancé un jeu-concours durant l'été 2014 en France où chaque heureux assuré gagnait un bracelet et le droit de le porter pour obtenir de petites remises s'il remplissait son quota quotidien de marche.
Dans son cahier sur les objets connectés, la Cnil reconnaît le risque de l'émergence de nouvelles formes de discrimination et prend la situation très au sérieux:
«Le scénario dans lequel une assurance santé ou une mutuelle conditionnerait l'obtention d'un tarif avantageux à l'accomplissement d'un certain nombre d'activités physiques, chiffres à l'appui, se dessine. Dans les années à venir, les individus pourraient être priés d'apporter les preuves d'un comportement sain, sur le modèle du "usage-based insurance".»
Et cela ne se limite pas à la santé. Allianz et Direct Assurance, filiale d'Axa, se sont lancées dans le «pay as you drive»: les assurés acceptent un système embarqué dans leur véhicule qui analyse leur conduite en permanence monnayant quelques réductions. Et à en croire le PDG d'Axa, on vous suivra bientôt jusque dans votre canapé grâce à l'essor d'entreprises comme l'Américain Nest qui propose des thermostats connectés. On n'a pas fini d'être surveillé.

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

Source : http://www.slate.fr/story/94731/objets-connectes-surveillance-travail
Par Philippe Vion-Dury

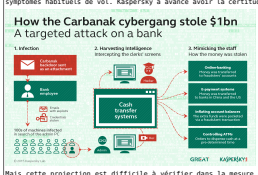
Comment les entreprises pourraient mieux se protéger des attaques informatiques de plus en plus sophistiquées ?

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

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

---

Non, la politique de confidentialité de Facebook n'est pas un progrès

Non, la politique de confidentialité de Facebook n'est pas un progrès

Avec ses nouvelles règles, entrées en vigueur en janvier 2015, Facebook promettait transparence et contrôle pour les utilisateurs. D'après un rapport commandé par la Cnil belge, ce contrôle s'avère en vérité très restreint.

« Vous avez le contrôle ». C'est le message qu'a tenu à faire passer Facebook auprès de ses utilisateurs en introduisant une nouvelle version de sa politique de confidentialité et de ses conditions d'utilisation.
Mais ce contrôle s'avère en vérité à géométrie variable, et même parfois tout bonnement inexistant, en particulier lorsqu'il s'agit pour l'utilisateur de limiter la collecte de ses données à des fins publicitaires. D'après le rapport rendu à l'autorité belge de protection des données personnelles par des chercheurs universitaires, il ne fait pas de doute que Facebook viole le droit européen.

D'anciennes « pratiques rendues plus explicites » et étendues
Cette situation préexistait toutefois à l'entrée en vigueur en janvier 2015 des nouvelles conditions d'utilisation du réseau social. « Pour être clair : les changements introduits en 2015 n'étaient pas tous drastiques. La plupart des 'nouveaux' termes et règles de Facebook sont simplement d'anciennes pratiques rendues plus explicites » souligne le rapport en préambule.
Pas pire qu'avant alors ? Pas si vite. Les juristes estiment en effet que la firme a aussi profité de ce changement pour étendre ses traitements de données. En substance, Facebook combine une grande variété de sources et de types de données, et de plus en plus y compris hors de ses seuls services.
Et si Facebook se montre plus gourmand en données, il a en revanche fait (ou presque) du sur-place sur l'information des utilisateurs et les moyens dont ils disposent pour contrôler ou s'opposer à ces traitements.
« Les usages des données sont encore seulement communiqués de manière générale et abstraite. La majeure partie de la politique d'utilisation des données consiste en des hypothèses et des termes vagues plutôt qu'en des déclarations claires quant à l'utilisation réelle des données » analyse le rapport.
« En outre, les choix qu'offre Facebook à ses utilisateurs sont limités. Pour nombre des utilisations de données, le choix pour les utilisateurs relève simplement du 'à prendre ou à laisser'. S'ils n'acceptent pas, ils ne peuvent plus utiliser Facebook […] » est-il encore précisé.

Choix limités et faux sentiment de contrôle
En vérité, les seules options de contrôle dont les internautes disposent sur le service portent sur l'accès à leurs contenus par les autres utilisateurs. Les auteurs de l'étude relèvent d'ailleurs que les règles par défaut de partage restent problématiques.
Et ainsi cette granularité dans le contrôle de la confidentialité s'estompe dès qu'il s'agit pour Facebook et des partenaires de collecter et exploiter des données. Les utilisateurs ne peuvent alors exercer « un contrôle significatif » sur l'exploitation de leurs données personnelles. Cette situation se traduit chez l'utilisateur par « un faux sentiment de contrôle » tranche le rapport.
D'ailleurs, la définition de l'opt-out appliquée par Facebook à la publicité sociale et comportementale ne respecte pas la législation en matière de recueil effectif du consentement. Dans certains cas, comme le partage des données de localisation, les juristes précisent que les utilisateurs n'ont tout simplement aucun droit d'opposition.
Si cette analyse juridique a été commanditée par la Cnil belge, ce n'est pas un hasard. Celle-ci participe en effet, aux côté des autorités allemande et néerlandaise, à un groupe de travail de l'Article 29 sur la conformité de la politique de confidentialité de Facebook avec le droit européen.
A noter que des représentants de Facebook ont rencontré le ministre belge en charge de la confidentialité afin de discuter des conclusions de ce rapport. La firme assure d'ailleurs respecter les lois du pays en matière de protection des données. Une ligne de défense qui était celle de Google en 2012 après l'entrée en vigueur d'une nouvelle politique de confidentialité.

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

Source : http://www.zdnet.fr/actualites/non-la-politique-de-confidentialite-de-facebook-n-est-pas-un-progres-39815200.htm
Par Christophe Auffray
c

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

Près d'un tiers des Européens donnent de fausses informations pour protéger

leurs données personnelles

Près d'un tiers des Européens donnent de fausses informations pour protéger leurs données personnelles

Une majorité d'européens (57%) s'avoue inquiet quant à la sécurité de leurs informations personnelles, selon le rapport 2015 sur la protection des données privées publié par l'éditeur de solutions antivirus Symantec.

81% des adultes interrogés estiment que leurs données ont de la valeur (équivalentes à moins de 1.000 euros pour 57% d'entre eux), ce qui explique que 66% déclarent qu'ils aimeraient pouvoir mieux les protéger, mais ne savent pas nécessairement comment faire. À l'inverse, ils sont 14% à ne voir aucun inconvénient à ce que les entreprises partagent leurs données avec des tiers.
Ce sont les données bancaires dans lesquelles les sondés ont le plus confiance en la sécurité en ligne (66%), devant celles médicales (60%), loin devant toutes celles relatives aux achats en ligne (15%). En conséquence, ils évitent dans la mesure du possible de poster des informations trop personnelles afin de se protéger (57%) et n'hésitent même plus à communiquer de fausses données pour parer à toute éventualité (31%).
À noter que, dans tous les cas, les données concernant le panel français ne diffèrent guère des résultats globaux européens, puisqu'ils sont par exemple 56% à s'inquiéter pour la sécurité de leurs données personnelles partagées sur Internet. Ils sont en revanche plus nombreux que la moyenne (66%, contre 57% au niveau européen) à refuser de poster systématiquement certaines informations trop personnelles en ligne.
Cette étude a été conduite en ligne par Edelman Berland pour Symantec en décembre 2014, auprès de 7.041 répondants répartis dans sept pays européens (Allemagne, Danemark, Espagne, France, Italie, Pays-Bas et Royaume-Uni) selon la méthode des quotas.

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

Source : http://www.leparisien.fr/high-tech/pres-d-un-tiers-des-europeens-donnent-de-fausses-informations-pour-proteger-leurs-donnees-personnelles-24-02-2015-4555475.php

---

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 se ferait plus partie du top 3.

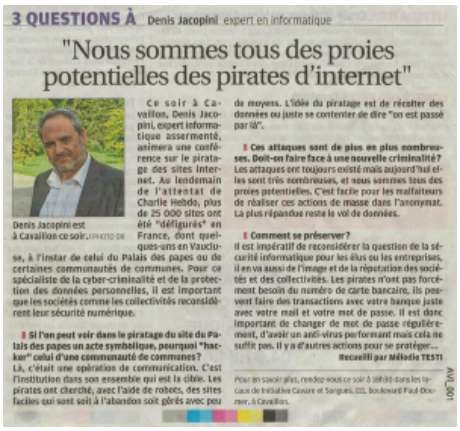
Au sein de la base de vulnérabilités nationale hébergée par le gouvernement américain, 7038 vulnérabilités auraient été rapportées au total en 2014, à raison de 19 par jour en moyenne, selon GFI. Celles-ci concernent aussi bien les systèmes d'exploitation que les applications. A titre de comparaison, 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=M&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 l'Initiative Cavaure et Sanguès, 111, Boulevard Paul Doumer, à Cavaillon.

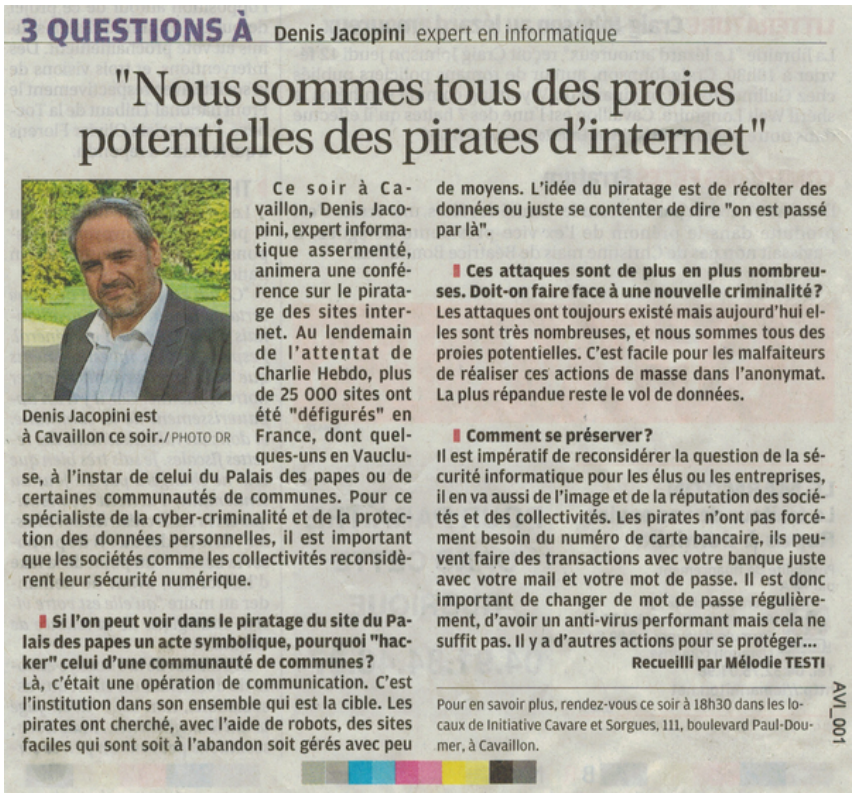
AVL_001

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