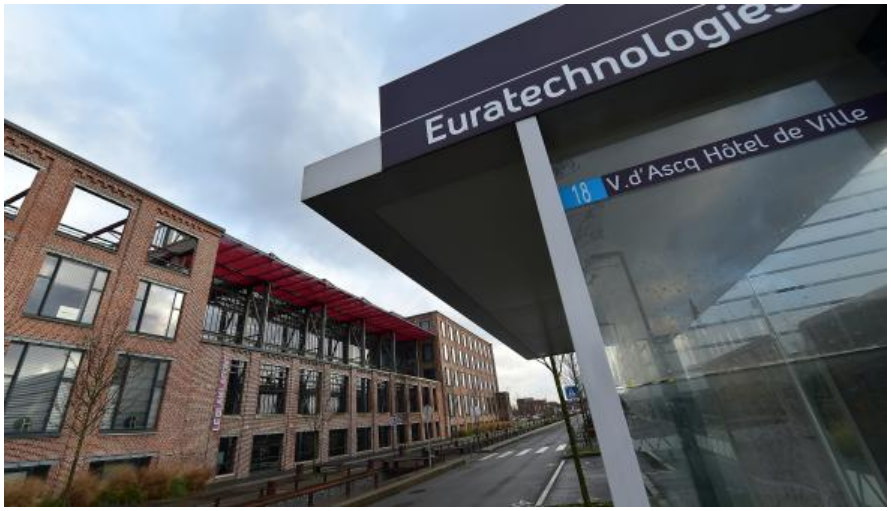
« On peut abattre une entreprise avec une attaque informatique » | Le Net Expert Informatique

	« On peut abattre une entreprise avec une attaque informatique »

La sécurité informatique est aujourd'hui un enjeu majeur pour nos sociétés. Lors du dernier Forum international de la cybersécurité à Lille, le Clubster cybersécurité et confiance numérique a été lancé en Nord-Pas-de-Calais. La filière s'organise, tout comme nos entreprises.

Toutes les secondes, 49 % des internautes dans le monde sont victimes d'actes malveillants. En une semaine, une entreprise peut subir jusqu'à 1400 attaques informatiques de plus ou moins grande importance. Chaque année, la cybercriminalité coûte 2,5milliards d'euros à la France. Huit des dix objets connectés les plus populaires (ordinateur, smartphone, etc.) peuvent présenter un risque pour la vie privée. Plus de 90 % des 64000 cyberinfractions recensées en 2013 par l'Observatoire national de la délinquance et des réponses pénales (ONDRP) sont des escroqueries et des attaques financières.
On l'aura compris, protéger ses données et ses échanges informatiques est un enjeu majeur tant pour les entreprises que pour n'importe quel citoyen.
Lors du dernier Forum international de la Cybersécurité qui s'est tenu à Lille, la Région a lancé le Cluster Cybersécurité et confiance numérique, premier du genre en France. Une centaine d'entreprises, écoles et universités, laboratoires et institutions représentant 6500 salariés, décident de travailler ensemble pour faire décoller une vraie filière, générant déjà un chiffre d'affaires de près de 535millions d'euros.

Grands noms
« Nous avons là un secteur prometteur avec des croissances de marché énorme », constate Raouti Chehih, directeur d'Euratechnologies qui héberge le cluster. Au printemps, un incubateur va être lancé pour accueillir les jeunes pousses les plus prometteuses en matière de cybersécurité.
« Notre région a déjà une forte expérience avec ses grands noms de la distribution, de la finance, de la santé, qui génèrent de forts besoins en matière de sécurité informatique. » Les innovations émergent (lire ci-contre). Le lillois Dhimyotis est le leader français dans le domaine de la certification et de la signature électronique. Le seul éditeur français d'antivirus, AxBx, est à Villeneuve-d'Ascq. À nous de nous imposer parmi les meilleurs.

UNE SIMPLE ATTAQUE PEUT RUINER VOTRE BUSINESS
Il y a eu l'affaire Snowden, du nom de l'informaticien qui a révélé le programme de surveillance informatique de masse des services secrets américains. Il y a eu le blocage complet du site américain de Sony. Il y a eu le pillage de 40millions de données clients du géant de la distribution américaine Target…
« Dans une société totalement connectée, on voit une explosion des menaces sur les réseaux informatiques. On a de l'escroquerie, des attaques entre États, de l'espionnage industriel, du terrorisme. C'est sur tous ces fronts qu'il faut travailler. » Pierre Calais est le directeur général adjoint de Stormshield à Villeneuve-d'Ascq. La société, fruit du rapprochement entre la société nordiste Netasq et la société lyonnaise Arkoon, et filiale d'Airbus Defence and Space, est surtout le numéro un européen en matière de sécurité informatique (220salariés dont 80 à Villeneuve-d'Ascq).
« La maîtrise de la technologie est aussi une question de confiance et de souveraineté. Nous sommes aujourd'hui encore trop dépendants des technologies américaines et désormais chinoises. Il est fondamental de maîtriser la sécurité des systèmes d'information pour garder son indépendance. C'est aussi cela l'enjeu du cluster cybersécurité qui se développe dans notre région. »
Stormshield développe, pour les plus grands noms de l'industrie et de la défense, tout un panel de systèmes de protection et de sécurité des réseaux. « Un simple anti-virus ou pare-feu ne suffit plus. Il faut aussi protéger des menaces inconnues. Pour cela il faut détecter très vite les comportements anormaux sur les réseaux, les données, les postes de travail comme les réseaux, pour pouvoir les bloquer. »
Et l'enjeu ne concerne pas que les grandes entreprises. « Les PME et TPE croient souvent qu'elles ne manipulent pas de données importantes. Mais toutes les entreprises possèdent des fichiers clients et des données qui peuvent intéresser des pirates. Aujourd'hui, on peut mettre le business d'une entreprise par terre seulement avec une attaque informatique. Et les plus petites entreprises sont les plus vulnérables, car les moins protégées, par ignorance, ou par souci d'économie. »
C'est souvent après un cambriolage que l'on pense à mettre une alarme. Mais il est trop tard…
Lire la suite….

Expert Informatique et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, 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.lavoixdunord.fr/economie/cybersecurite-on-peut-abattre-une-entreprise-avec-ia0b0n2692787

Quasiment 100% des responsables IT français inquiets de la sécurité des objets connectés | Le Net Expert Informatique

Quasiment 100% des responsables IT français inquiets de la sécurité des objets connectés

Une enquête menée par le cabinet Vanson Bourne montre que les responsables informatiques français sont nombreux à s'impliquer dans des projets liés aux objets connectés. Cela ne les empêche pas de se montrer particulièrement vigilants sur les risques qui en découlent en matière de sécurité.

Alors que l'on pensait que les responsables informatiques français étaient plutôt frileux en matière d'objets connectés, les résultats d'une enquête menée par le cabinet Vanson Bourne pour le compte de Trend Micro montrent que cela n'est vraiment pas le cas. Parmi les 800 responsables informatiques dans le monde interrogés en novembre 2014, 86% des répondants français (100 au total) vont ainsi jusqu'à encourager l'utilisation des objets connectés dans leur organisation. Des organisations qui sont d'ailleurs de plus en plus nombreuses à s'engager (ou prévoir de le faire) dans des programmes impliquant des objets connectés. Ces programmes ont principalement pour vocation à augmenter le bien-être au travail (54%) ou encore à améliorer la productivité des collaborateurs (51%).
En revanche, la mise en oeuvre de projets informatiques faisant appel à objets connectés ne se fait pas au détriment de la sécurité des données. **Ainsi, la quasi-totalité (99%)** des responsables informatiques interrogés considèrent que l'utilisation des objets connectés présente des risques pour l'entreprise. « L'accès aux réseaux sociaux et aux boîtes mails personnelles, l'application la plus courante des objets connectés, est considéré par deux-tiers des répondants comme la plus risquée pour la sécurité des données de l'entreprise », indique Trend Micro. « En outre, près d'un quart des responsables informatiques interrogés admettent que leur entreprise a déjà été victime d'une faille de sécurité provenant d'un équipement mobile personnel, avec des conséquences alarmantes ».

Des politiques Byod élargies aux objets connectés
Par ailleurs, 77% des responsables informatiques interrogés indiquent être favorables à l'encadrement de l'utilisation des objets connectés sur le lieu de travail (77%), une grande majorité (92%) estimant d'ailleurs que les politiques mises en place pour encadrer le Byod vont être amenées à évoluer pour tenir compte de ces équipements.

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

Source : http://www.lemondeinformatique.fr/actualites/lire-99-des-responsables-it-francais-inquiets-de-la-securite-des-objets-connectes-60414.html
Par Dominique Filippone

Après les élèves, au tour des parents d'être au fait de la cybercriminalité | Le Net Expert Informatique

Après les élèves, au tour des parents d'être au fait de la cybercriminalité

Le Service de police de L'Assomption/Saint-Sulpice tenait sa traditionnelle conférence sur la cybersécurité dans le cadre du programme « Pour moi, un bon gang c'est…» le jeudi 26 février dernier à la Maison de la culture de L'Assomption.

Après avoir fait le tour des classes de toutes les écoles primaires et secondaires sur le territoire de L'Assomption et de Saint-Sulpice, c'était autour des parents de s'informer sur les tendances et les dangers du web et des médias sociaux.

Présent à cette conférence, le directeur de l'école primaire Gareau à L'Assomption, René Dupuis, est venu parler des répercussions entourant le phénomène des médias sociaux qui provoque bien des maux de têtes au personnel enseignant, et ce, à un très jeune âge.

« Même si j'évolue dans une école primaire, je tenais ce soir à mentionner à quel point on vit vraiment des problèmes avec Facebook et Internet. Des menaces sont lancées entre les internautes le soir, souvent entre les élèves d'une même classe, et le lendemain ça rebondit à l'école. Les élèves se lancent des regards noirs et veulent régler des comptes, a-t-il expliqué. Et il ne faut pas penser que ça se passe juste dans les classes de cinquième et de sixième année. Déjà en troisième année, ça commence. »

C'est l'agent Sylvain Lessard et la cyberenquêteuse Marie-Ève Richard qui sont venus animer la présentation aux parents.

« Les parents ont besoin de savoir quoi faire avec ça, de savoir que l'intimidation, ce n'est pas vrai que ça se passe uniquement au secondaire, expliquait Sylvain Lessard, policier au Service de police de L'Assomption/Saint-Sulpice depuis 2004. De savoir aussi que tout le monde, maintenant, se retrouve sur la même planète: les bons comme les mauvais.

Laisser des traces

Dans sa présentation, Sylvain Lessard tient à ce que parents et élèves retiennent que tout ce qui est fait sur Internet laisse des traces qui peuvent durer toute une vie. Des photos compromettantes ou des déclarations fracassantes sur Facebook peuvent notamment avoir des répercussions sur une future carrière.

« 93 % des recruteurs déclarent visiter le profil social des candidats avant de décider d'en recruter un, 55 % ont reconsidéré leur avis après avoir consulté leur profil social », déclare l'agent Lessard.

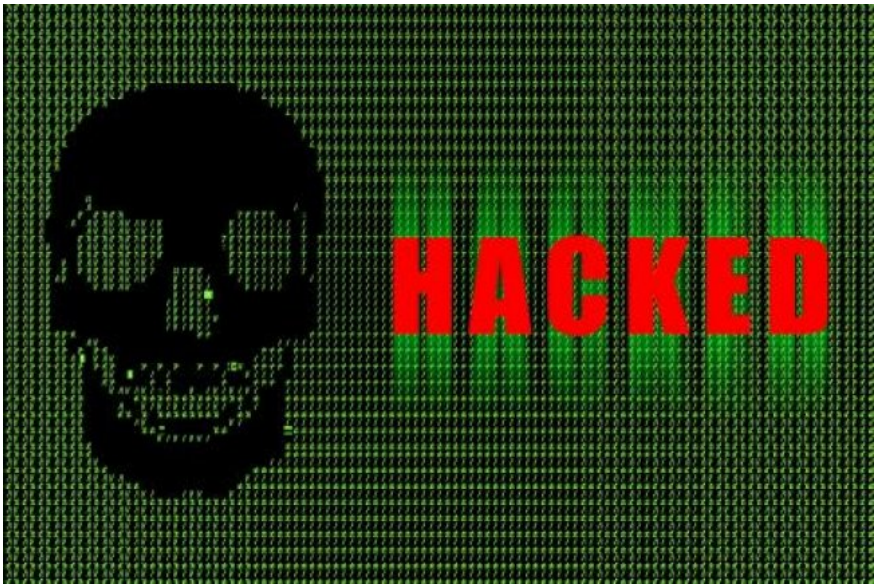
Selon Marie-Ève Richard, les arnaques aux sentiments, très populaires sur les médias sociaux dans Lanaudière, font en sorte que les victimes sont ciblées de façon très pointilleuse. Les faux profils sont monnaie courante dans ce genre d'arnaque et les filles, autant que les garçons, sont susceptibles d'être ciblés.

Pour prévenir les problématiques liées à l'utilisation d'internet; avoir un mot de passe fort, difficile à déchiffrer, accompagner les jeunes dans leurs pratiques, protéger ses renseignements personnels, être conscient que le cyberespace est public et éviter de se venger sur Internet si on est en colère sont autant de conseils judicieux donnés aux parents.

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

Source : http://www.hebdorivenord.com/Actualites/2015-03-03/article-4063973/Apres-les-eleves,-autour-des-parents-detre-au-fait-de-la-cybercriminalite/1
Par Marie-Claude Chiasson

Votre entreprise à peut-être une base de données à la merci des pirates informatiques



Votre entreprise à peut-être une base de données à la merci des pirates informatiques…

Des étudiants du « Center for IT-Security, Privacy and Accountability » de Sarrebruck (CISPA – Sarre) ont récemment révélé des failles de sécurité portant sur 40.000 bases de données. Ces données, portant sur des entreprises basées en France et en Allemagne, listent des noms, adresses et courriels de millions de clients.

La cause en est une base de données open source mal configurée, utilisée par de nombreux sites de vente en ligne. Si les opérateurs adoptent les paramètres par défaut de ces bases, les données sont alors disponibles en ligne sans protection. Plus grave encore, ces données peuvent être modifiées. Or le fournisseur de la base de données, MongoDB Inc., est l'un des acteurs majeurs du secteur au niveau mondial. Les étudiants à l'origine de cette découverte ont ensuite interrogé un moteur de recherche public pour identifier les entreprises utilisant ces bases de données non protégées.
Selon le CISPA, les étudiants ont notamment détecté une base de données qui pourrait appartenir à un opérateur français de télécommunication, contenant les adresses et numéros de téléphones de huit millions de clients, en France et en Allemagne. Ils ont également identifié la base de données d'un site de commerce en ligne, comprenant des informations de paiement. Ces données facilitent, pour des personnes mal intentionnées, l'usurpation d'identité en ligne. A ce titre, le CISPA a contacté différentes autorités chargées de la protection des données (les « Computer Emergency Response Teams – CERTs », la Commission nationale de l'informatique et des libertés – CNIL, et le Bureau allemand pour la sécurité de l'information – BSI. Le fournisseur a également été informé des problèmes générés par une mauvaise configuration des bases de données par les entreprises clientes.
Le CISPA, rattaché à l'Université de la Sarre, a été fondé en 2011 par le Ministère fédéral de l'enseignement et de la recherche (BMBF) en tant que centre de compétence pour la cybersécurité. En plus de l'Université de la Sarre, l'Institut Max Planck pour l'informatique (MPII), l'Institut Max Planck pour les systèmes logiciels (MPI-SWS), ainsi que le Centre allemand de recherche sur l'intelligence artificielle (DFKI) travaillent conjointement au sein du CISPA. Avec environ 200 chercheurs, le centre est l'un des plus grands centres de recherche sur la cybersécurité en Europe.

Expert Informatique et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, 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.science-allemagne.fr/fr/actualites/technologies-de-linformation-et-de-la-communication-tic/bases-de-donnees-pres-de-40-000-failles-decouvertes-par-des-etudiants-sarrois/

La formation du personnel, seule vraie solution contre les attaques informatiques

La formation du personnel, seule vraie solution contre les attaques informatiques

Publié quelques jours après la révélation d'une cyberattaque qui a touché plus de 100 banques à travers le monde et causé aux alentours de 900 millions d'euros de dégâts, le nouveau rapport d'Intel Security démontre toute l'importance d'une prise de conscience collective et souligne la nécessité d'éduquer les collaborateurs aux méthodes de persuasion utilisées par les hackers.

Dans ce fameux cyber-casse dont l'existence a été révélée la semaine dernière, ce sont des attaques de phishing ciblées qui ont permis de créer des brèches au sein des réseaux bancaires, démontrant ainsi la faiblesse intrinsèque du « pare-feu humain ». Ce que confirme l'étude Threat Report d'Intel Security qui indique que 92 % des employés français ne sont pas en mesure d'identifier un courriel de phishing sur sept. »Aujourd'hui, les cybercriminels n'ont pas nécessairement besoin de savoir-faire technique pour atteindre leurs objectifs, explique Paul Gillen, directeur des opérations du Centre Européen de lutte contre la cybercriminalité.
Certains logiciels malveillants peuvent infecter les ordinateurs en y accédant directement par emails. Ces attaques ciblées manipulent les victimes et les incitent à ouvrir des pièces jointes, prétendument légitimes, ou à cliquer sur un lien qui semble provenir d'une source sûre ».
Sur l'année 2014, McAfee Labs a constaté une augmentation spectaculaire du nombre d'URL malveillantes soit plus de 30 millions de liens suspects. Une hausse qui peut être attribuée à la fois à une forte croissance du nombre de liens de phishing, ainsi qu'à une utilisation plus commune des URL courts qui cachent, souvent, des sites Web malveillants. Le rapport des 500 chercheurs du McAfee Labs pointe par ailleurs du doigt le fait que deux tiers des emails mondiaux sont des spams qui visent à soutirer des informations et de l'argent à leurs destinataires.
Il est donc important que les consommateurs et les collaborateurs d'entreprises soient informés des techniques d'escroquerie couramment utilisées dans le monde numérique.
« Pour conserver une longueur d'avance sur les cybercriminels et réduire le risque d'être l'une des victimes de la cybercriminalité, les entreprises doivent non seulement optimiser leurs processus et compter sur la technologie mais aussi former leurs personnels pour pallier à la brèche dans ce qu'on nomme 'l'OS humain' » conclut Raj Samani, Directeur Technique EMEA d'Intel Security.

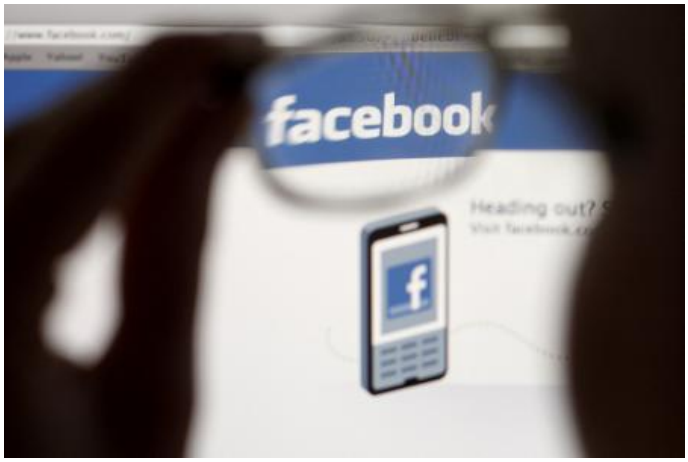
Nous organisons régulièrement des actions de sensibilisation ou de formation au risque informatique, à l'hygiène informatique à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Vous souhaitez participer à une de nos formations ?
Besoin d'informations complémentaires ?
Contactez-nous

Expert Informatique et formateur spécialisé en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel, Nous sommes 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.infodsi.com/articles/154213/formation-personnel-seul-vrai-rempart-attaques-informatiques.html

Inquiétant: les employés de Facebook n’ont pas besoin de votre mot de passe pour accéder à votre profil | Le Net Expert Informatique

	Inquiétant : les employés de Facebook n’ont pas besoin de votre mot de passe pour accéder à votre profil

Voilà une révélation qui ne va pas rassurer alors que la protection des données personnelles sur Internet est une véritable préoccupation des internautes : selon un artiste finlandais, les employés de Facebook ont accès à tous les profils du réseau social… sans mot de passe.

Le musicien finlandais Paavo Siljamäki était en visite, le 24 février dernier, dans le quartier général de Facebook, à Los Angeles. Il a alors eu droit à une démonstration de l'utilisation du réseau social par des employés du site web. Et ceux-ci ont montré qu'ils pouvaient aller bien plus loin qu'une simple visite de profil.

« Un ingénieur de Facebook s'est connecté directement comme s'il était sous mon nom sur Facebook, et pouvait donc voir tout mon contenu privé sans demander de mot de passe », explique le musicien… sur Facebook. « C'est pourquoi je me demande combien d'employés de Facebook ont la possibilité d'avoir accès à tous les comptes ? Quelles sont les règles sur qui et quand peut-on avoir accès à nos données privées et comment pourrait-on le savoir que quelqu'un y a eu accès ? (Mon compte ne m'a pas indiqué que quelqu'un avait accédé à mon profil) ».
Ces questions, n'importe quel utilisateur de Facebook pourrait se les poser. En cette période trouble durant laquelle de nombreux internautes s'interrogent sur la protection de leurs données personnelles par les grandes compagnies comme Facebook, Google, Apple, Amazon, etc.
Facebook a partiellement répondu aux questions de Paavo Siljamäki sur VentureBeat. Un porte-parole explique ainsi que seuls des employés désignés ont accès « aux informations nécessaires pour faire leur travail », à savoir résoudre des bugs ou répondre aux demandes d'aide. Des équipes de sécurité indépendantes gèrent ensuite les cas considérés comme suspects par des groupes de travail mis en place au sein des équipes de Facebook, et contrôlés, du moins pour l'Europe, par le bureau de la commission irlandaise de protection des données.
VentureBeat confirme donc que Facebook peut avoir accès à tous les profils sans mot de passe, mais seulement si cela est demandé pour les raisons ci-dessus et si vous l'autorisez.

Expert Informatique et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, 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.sudinfo.be/1225989/article/2015-03-02/inquietant-les-employes-de-facebook-n-ont-pas-besoin-de-votre-mot-de-passe-pour

---

Les 5 techniques que les cybercriminels utilisent pour pénétrer les réseaux | Le Net Expert Informatique

Les 5 techniques que les cybercriminels utilisent pour pénétrer les réseaux

Il existe au moins 5 techniques de nature « discrète et graduelle » que les cybercriminels utilisent désormais pour pénétrer les réseaux et accomplir leur mission, et que les professionnels de la sécurité doivent comprendre et repérer afin de défendre plus efficacement leur entreprise :

1. Les kits d'exploits : les concepteurs de kits d'exploits connus comme Blackhole ont été repérés par les autorités et stoppés dans leurs actions. Les hackers ont ainsi réalisés que les attaques de grande ampleur ne sont pas toujours les plus efficaces – que ce soit de par la taille des infrastructures ou des moyens malveillants mis en œuvre. Ainsi les hackers préfèrent disposer du 4ème ou 5ème kit d'exploits le plus connu et utilisé, pour ne pas trop attirer l'attention.

2. Le spam « Snowshoe » : avec cette technique, le hacker diffuse beaucoup de messages sur une grande surface d'attaque pour échapper aux outils de détection traditionnels. Le spammeur Snowshoe envoie un email non sollicité en utilisant un grand nombre d'adresses IP mais à un faible volume de messages par adresse IP, avec pour objectif de contourner les technologies de réputation anti-spam basées sur l'adresse IP. Il change rapidement le corps du texte, les liens, les adresses IP utilisées pour la diffusion et ne répète jamais la même combinaison.

3. Le spear phishing sophistiqué : les hackers continuent d'affiner leurs messages, bien souvent en utilisant des techniques d'ingénierie sociale, de sorte que même les internautes expérimentés ont du mal à repérer les faux messages. Les récentes attaques de spear phishing semblent provenir de fournisseurs ou d'opérateurs connus, desquels les utilisateurs reçoivent régulièrement des messages – par exemple, les prestataires de services, les sites de vente en ligne et les fournisseurs de contenus musicaux et de loisirs. Ces emails peuvent contenir un nom de confiance, un logo connu et inviter le destinataire à réaliser une action familière, comme donner son avis à propos d'une commande récente, ou donner un numéro pour le suivi de sa livraison. Cette mécanique bien huilée et discrète donne aux utilisateurs un faux sentiment de sécurité, les incitant à cliquer sur des liens malveillants contenus dans l'e-mail.

4. Le partage d'exploits entre deux fichiers différents : les malwares Flash peuvent désormais interagir avec JavaScript pour cacher des activités malveillantes en partageant un exploit entre deux fichiers et formats différents : un fichier Flash, un fichier JavaScript. Cela dissimule l'activité malveillante et rend l'identification, le blocage ainsi que l'analyse de l'exploit beaucoup plus difficile. Cette approche permet également aux hackers d'être plus efficaces dans leurs attaques. Par exemple, si la première étape d'une attaque est entièrement en JavaScript, la seconde étape, le transfert du code malicieux, ne se produirait qu'après l'exécution avec succès du code JavaScript. De cette façon, seuls les utilisateurs qui peuvent exécuter le fichier malveillant reçoivent celui-ci.

5. Le malvertising : les créateurs de malwares ont mis au point un nouveau business modèle perfectionné qui utilise les modules publicitaires des navigateurs Web pour diffuser des logiciels malveillants et des applications indésirables. Les utilisateurs achètent, téléchargent et installent des outils tels que Adobe ou des logiciels vidéo depuis des sources qu'ils estiment légitimes. En réalité, ces applications sont livrées avec un logiciel malveillant. Cette nouvelle approche de diffusion de malwares est un succès pour les hackers car de nombreux utilisateurs font naturellement confiance aux publicités ou les considèrent comme bénignes. Les hackers gagnent de l'argent à partir d'un grand nombre utilisateurs, par petites touches, en infectant de manière persistante leur navigateur et en se cachant sur leur machine.

Les professionnels de la sécurité et les cybercriminels sont dans une course permanente pour tenter de déjouer l'autre. Les hackers sont de plus en plus professionnels, non seulement dans leurs approches pour lancer des attaques, mais aussi pour échapper aux outils de détection, par des moyens que nous n'avions pas vus jusqu'à présent. Mais en continuant à innover et à apprendre sur la base de ce qu'ils observent, les professionnels de la sécurité peuvent identifier et contrer ces nouvelles techniques d'attaques.

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

Source : http://www.informatiquenews.fr/quelles-reponses-aux-nouvelles-cyberattaques-christophe-jolly-cisco-31360
Par Christophe Jolly, Directeur Sécurité de Cisco France

Découvrez l’accord qui autorise la surveillance des données informatique

	Découvrez l’accord qui autorise la surveillance des données informatique

Le Patriot Act est une loi antiterroriste qui a été adoptée par les Etats-Unis après le 11 septembre 2001. Promulguée dans l'urgence comme une loi d'exception, elle a été prolongée à deux reprises et est toujours en vigueur à l'heure actuelle. Le Patriot Act autorise l'administration américaine à accéder à tout moment et sans autorisation judiciaire aux données informatiques des entreprises ou des particuliers qui ont un lien, quel qu'il soit, avec les États-Unis. En pratique, cela peut poser de graves problèmes pour une entreprise ayant stocké ses données confidentielles ou celles de son client chez un hébergeur américain, même s'il s'agit d'une filiale localisée dans un pays différent.
Qu'en est-il alors des entreprises françaises ? Quelles solutions existent pour assurer la confidentialité des informations privées des entreprises ?

Le risque de fuite de l'information
Dans un environnement hyperconcurrentiel, les risques de divulgation d'informations confidentielles pèsent sur toutes les entreprises puisque chacune a une part de marché à défendre ou une image à préserver. Néanmoins, toutes ne sont pas forcément impactées par l'étendue du Patriot Act, cela va dépendre de leur système d'information (organisation, gérance, etc.). Aujourd'hui, le développement de logiciels et la gestion des systèmes d'informations sont souvent sous-traités partiellement ou totalement à des fournisseurs pour notamment réduire les coûts de gestion ou bien bénéficier du savoir-faire et l'expertise de spécialistes. Cependant, cette externalisation (en mode Saas ou autre) peut ouvrir la porte au Patriot Act en faisant le choix, délibérément ou par manque d'informations, d'un prestataire de services de nationalité américaine pour l'hébergement des données.
En outre, l'Agence Nationale de la Sécurité Américaine (NSA) bénéficie de l'accès direct aux informations stockées sur les serveurs américains, et même aux données des fournisseurs de services informatiques américains (et donc de leurs clients) dont les serveurs sont situés en dehors des Etats-Unis ! Rappelons qu'en mai 2014, Microsoft (société de droit américain relevant donc du Patriot Act) a été sommé de céder aux autorités américaines les informations privées d'un client, bien que celles-ci fussent hébergées en Irlande.

Qui des données issues d'Office 365?
Si l'on prend maintenant l'exemple des solutions Microsoft 365 (Outlook en accès web), les informations sont enregistrées et traitées par un serveur américain qui relève du Patriot Act. Les entreprises, en utilisant ces services, peuvent donc être espionnées et leurs informations sensibles exploitées. De plus, les autorités américaines qui n'ont aucune obligation d'informer les propriétaires des données consultées ni des modalités de conservation ! Ainsi, du moment où elles passent par un serveur américain, les données des entreprises ne sont plus considérées comme sécurisées et courent donc un risque non négligeable de confidentialité (au niveau de l'intelligence économique notamment). C'est un risque que l'on peut comparer au piratage informatique sauf que dans le cas Patriot Act, il s'agit d'une intrusion légale.

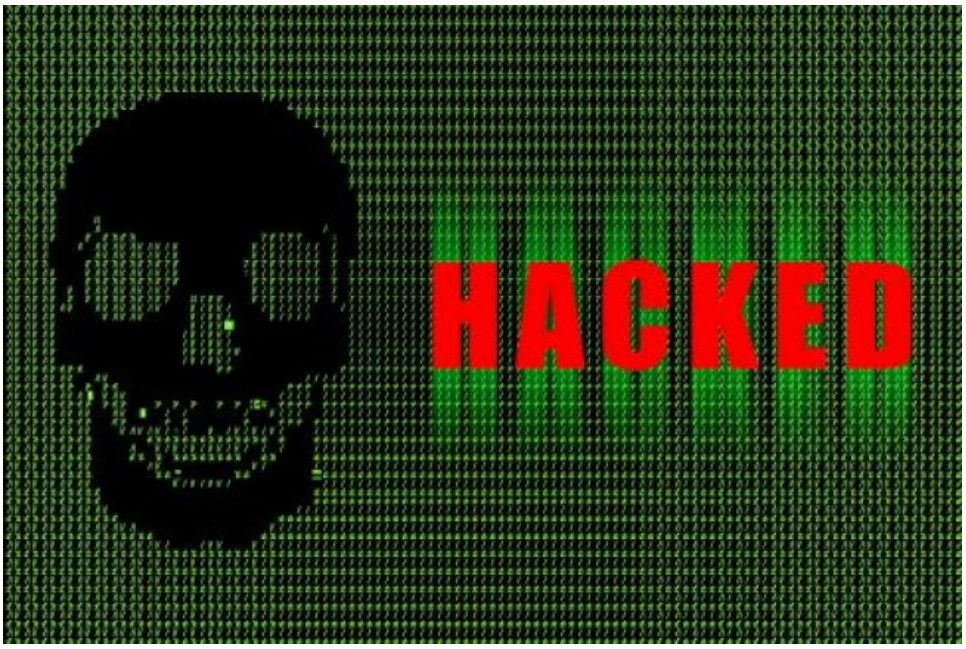
Assurer la confidentialité des données privées
Dans ce contexte, trois étapes apparaissent essentielles pour permettre aux entreprises de ne pas être sujette à cette éventuelle fuite de l'information, et pour s'assurer le contrôle sur l'accès aux données :
• **Faire le tri**
Dans un premier temps, il appartient aux entreprises de catégoriser leurs données, afin de cibler et de trier les informations sensibles, celles-ci pouvant revêtir de nombreux aspects : secret des affaires, communication financière et stratégique, brevets, éléments de recherche et développement, débats des conseils d'administration, mais aussi tout ce qui relève des échanges électroniques du quotidien.
• **Sensibiliser les collaborateurs**
Pour prévenir le risque d'être confronté au Patriot Act, on note aussi l'importance de la communication au sein même de l'entreprise pour informer et responsabiliser les collaborateurs à la sécurité des données. Cette sensibilisation peut éviter une soumission par négligence au Patriot Act, comme c'est le cas lors des échanges par email via des services de messagerie grand-public (webmails) qui sont très populaires, mais souvent américains. Ainsi, former ses employés aux enjeux de la confidentialité des données et aux conséquences que peuvent avoir certains de leurs actes virtuels, c'est protéger le capital informationnel de l'entreprise tout en instaurant de bonnes pratiques en matière de sécurité informatique.
• Être vigilant
Une fois les données catégorisées et les collaborateurs sensibilisés, l'entreprise doit être très attentive aux conditions de stockage de l'information dite sensible.
Le meilleur moyen de se protéger du Patriot Act américain consiste à être vigilant quant à l'origine de l'hébergeur et du serveur. Une vérification de toute la chaîne de fournisseurs – et pas uniquement du serveur – s'impose donc pour s'assurer que les données ne sont pas concernées par cette loi américaine.
Ainsi il faut que l'entreprise privilégie les opérateurs européens dont les serveurs sont situés sur le territoire européen. Dans le cas d'une entreprise française, il est bien évidemment préférable de choisir des prestataires à caractère souverain dont les serveurs sont localisés en France.
En effet, pour protéger l'information sensible de l'entreprise, la France et les acteurs européens créent des certificats (par exemple le Label Cloud Confidence ou le Label Cyber Sécurité France) dans l'idée de labéliser les services qui respectent le principe de conservation de l'information dans le cadre juridique européen.
Enfin, d'autres mesures classiques existent pour protéger ses informations privées : chiffrement des données, engagement de confidentialité, audits systématiques pour tester régulièrement la sécurité des logiciels utilisés, etc. Tous ces moyens de protection témoignent d'une véritable prise de conscience de la part des entreprises de la valeur critique de leurs données et de la nécessité de les protéger.
Par Nadim Baklouti, Directeur R&D Leading Boards (solution de dématérialisation des Conseils d'Administration), et Gaetan Fron, Directeur DiliTrust (service de datarooms électroniques).

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.informatiquenews.fr/le-patriot-act-et-la-securite-des-donnees-des-entreprises-francaises-nadim-baklouti-et-gaetan-fron-euqity-31046

| Le Net Expert Informatique

	Votre entreprise a peut-être elle aussi une base de données à la merci des pirates…