« 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

Les entreprises qui appliquent des mesures de protection des données personnelles jouissent d’une meilleure réputation, les clients leur font davantage confiance et elles se démarquent clairement sur le marché

Les entreprises qui appliquent des mesures de protection des données personnelles jouissent d’une meilleure réputation, les clients leur font davantage confiance et elles se démarquent clairement sur le marché

L'absence d'accord au niveau européen conduit les entreprises à différer toute action au profit de celles qui appliquent des règles strictes de sécurité et de confidentialité déjà en place.

Le fait que les efforts d'harmonisation des règles européennes de collecte, d'utilisation et de conservation des données s'enlisent dans des débats politiques, pourrait bien faire perdre une part substantielle de leur avantage concurrentiel à la majeure partie des entreprises de l'UE qui avouent être mal préparées aux changements à venir[i], selon Iron Mountain, le spécialiste des services de conservation et de gestion de l'information.
Dans un document consultatif*, Iron Mountain souligne l'importance pour les entreprises de mettre en œuvre de solides mesures de protection des données, indépendamment de ce que préconisent les propositions réglementaires. En effet, il est démontré que **les entreprises qui appliquent de telles mesures jouissent d'une meilleure réputation, que les clients leur font davantage confiance et qu'elles se démarquent clairement sur le marché**.

Forrester avance que « dans la lutte pour acquérir, servir et fidéliser les clients, la sécurité des données et le respect de la confidentialité sont aujourd'hui des gages qui aident à se différencier de la concurrence ».[ii]

Ce document aide les entreprises à mesurer pleinement les effets de la nouvelle réglementation et à comprendre leur importance. Bon nombre de dispositions font toujours l'objet d'intenses débats parmi les dirigeants de l'UE trois ans après la première proposition de loi : celles relatives aux données du secteur public, le droit d'accès aux données par les organismes chargés de l'application de la loi et la possibilité pour les entreprises internationales de traiter directement avec le régulateur sur leur marché d'origine (le « guichet unique »), . Le retard pris pour parvenir à un accord ne reflète pas uniquement les intérêts divergents des 28 États membres, mais aussi l'évolution rapide des technologies, des nouveaux consommateurs connectés et du Big Data.
« La proposition de loi est extrêmement puissante et elle aura des répercussions dans le monde entier », déclare Edward Hladky, Directeur Général Adjoint d'Iron Mountain France. « Certains concepts seront étudiés de près dans quelques zones géopolitiques : la cohérence des règles et leur mise en œuvre à travers les frontières, le droit à l'oubli et le besoin d'une désidentification efficace des données personnelles utilisées dans les secteurs de la santé et de la recherche. »
« Toutefois, avec autant de propositions en constante évolution, les entreprises peuvent être tentées d'attendre de voir ce que la version finale contiendra réellement. Nous pensons que ce serait une erreur. L'éthique veut que les organisations protègent les données fermement et efficacement et qu'elles les utilisent et les conservent de manière responsable et transparente. Autant cela renforce la confiance des clients, autant les violations de données les rendent méfiants. L'équation est simple : la confiance nourrit la fidélité et la fidélité nourrit les ventes. Les entreprises ont beaucoup à gagner en agissant dès maintenant, avant que la loi les oblige à le faire. »

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

Source : http://www.infodsi.com/articles/154353/attente-nouvelle-legislation-europeenne-protection-donnees-pourrait-couter-cher-competitivite-image-marque-entreprises.html
* Le livre blanc, en version anglaise, édité pour la journée européenne de la protection des donnes, « An opportunity to plan and manage the impact of legal change » est disponible sur http://www.ironmountain.co.uk/services/dpd.aspx

[i]52 % des entreprises d'après une étude menée au Royaume-Uni, en Allemagne et en France par Ipswitch Software en octobre 2014. http://www.techweekeurope.co.uk/e-regulation/european-teams-woefully-unprepared-general-data-protection-regulation-155316#ArDP0sA9ymVzYTPT.99
[ii]https://www.forrester.com/Predictions+2015+Data+Security+And+Privacy+Are+Competitive+Differentiators/fulltext/-/E-RES116328

Les travel managers doivent-ils craindre Prism ? | Le Net Expert Informatique

Les travel managers doivent-ils craindre Prism ?

Comment fonctionne Prism ? Quel en est l'intérêt pour les compagnies aériennes ? Celui des entreprises ? Qu'en est-il de la confidentialité ? Telles sont quelques unes des questions qui agitent le monde des travel managers. Éléments de réponse.

Malgré les petits fours, malgré le poisson et la volaille à la julienne de légumes suivie d'un assortiment de desserts programmé pour coïncider avec le service d'un dernier verre de champagne, le dîner aérien organisé le 10 février dernier dans un chic hôtel parisien par l'AFTM – l'Association française des travel managers, dont c'est un des rendez-vous les plus prisés – en a laissé plus d'un sur sa faim… Pour cause : le thème de cette soirée – débat était « Qu'est-ce que Prism ? ». Une question qui n'avait jamais encore été mise sur la table en France, alors même qu'un nombre croissant d'entreprises se la posent en interne. « De nombreuses interrogations sont restées en suspend », confirme le délégué général de l'association, Thibault Barat.

« Beaucoup d'incompréhension »

Sur son site internet, Prism – passé il y a trois ans sous le contrôle du groupe américain Sabre – se définit comme le leader de la data sur les voyages corporate, qu'il collecte et consolide pour les compagnies aériennes. « Il y a beaucoup d'incompréhension sur le sujet », souligne néanmoins Thibault Barat, qui rappelle que Prism a commencé à revenir avec insistance aux oreilles des travel managers français alors que l'affaire Snowden était sur le devant de la scène. Une association sulfureuse qu'une autre coïncidence ne fait rien pour atténuer : Prism est aussi le nom donné à un programme de surveillance électronique américain relevant des activités de la NSA… « Nous ne faisons que gérer de la data », a martelé Herman Mensink, vice-président de Prism pour la zone Europe, Moyen Orient et Afrique. Une vocation d'apparence plutôt bénigne qui comporte toutefois d'importantes zones de gris.

« Que va-t-on faire de nos données ? »

« Que va-t-on faire de nos données ? », s'est inquiété un travel manager qui participait à ce dîner débat – et qui a tenu à conserver l'anonymat. A en croire les nombreuses questions qui ont fusé, une fois la présentation de Herman Mensink terminée, la protection de données, parfois hautement stratégiques, s'impose comme le souci majeur des entreprises françaises face à la montée en puissance de Prism. Inquiétude balayée d'un revers de manche par son vice-président EMEA: « La vocation du groupe est de gérer des données ». Comprendre : tout autre aspect du programme relève de la négociation entre les entreprises et les compagnies aériennes.

Une auto-justification qui a surtout pour conséquence de mettre en exergue l'un des points du dispositif Prism jugés problématiques : « Aucun contrat n'unit Prism aux entreprises. Ces dernières ne sont en interaction qu'avec les compagnies aériennes, qui, lorsqu'elles contractualisent avec Prism, leur demandent de communiquer leurs données à Prism, tiers avec qui elles n'ont aucun lien légal ». Moyennant quoi les entreprises ont accès à une tarification avantageuse.

La formule n'est pas sans rappeler l'accord déjà en place entre les travel managers corporate français et Air France. Sauf que là, souligne notre travel manager anonyme, « Rentre dans le process un intervenant extérieur qu'on ne maîtrise absolument pas. Quelle garantie avons-nous vis-à-vis de ses agissements ? Et, en cas de litige, qui tranchera ? » (les donnée collectées en mode cloud par Prism sont stockées, pour une durée d'un an minimum, sur des serveurs situés aux États-Unis).

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

Source : http://www.decision-achats.fr/Thematique/marches-1036/travel-meetings-10135/Breves/travel-travers-Prism-251605.htm

Les sites terroristes et pédopornographiques supprimables de Google | Le Net Expert Informatique

Les sites terroristes et pédopornographiques supprimables de Google

Le décret relatif au déréférencement des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites pédopornographiques a été publié au Journal Officiel aujourd'hui.

Ce déréférencement sur les moteurs de recherches (Google, Bing…) complète le blocage de ce type de sites voté en novembre et mis en œuvre depuis le début du mois de février. De nombreuses voix s'élèvent contre ces dispositifs administratifs (sans intervention du juge) jugés contre-productifs.
Décret n° 2015-253 du 4 mars 2015 relatif au déréférencement des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique

---

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.liberation.fr/direct/element/840/

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/

Des salariés de Twitter sont la cible de menaces de mort de la part de terroristes de

l’état islamique | Le Net Expert Informatique

Des salariés de Twitter sont la cible de menaces de mort de la part de terroristes de l’état islamique