Toulouse attaqué par le virus «Rançongiciel» | Le Net Expert Informatique

Toulouse attaqué par le virus «Rançongiciel»

Ce mardi 10 mars, le système informatique de la ville de Toulouse a été attaqué par le virus «Rançongiciel», a confirmé hier une source municipale à La Dépêche du Midi3.

Vendredi 6 mars, les services informatiques municipaux avaient été mis en garde sur une éventuelle attaque par une autre collectivité de l'agglomération, qui avait elle-même été la cible de ce virus. «Rançongiciel» se propage par l'ouverture de pièces jointes dans les courriels, le téléchargement de fichiers infectés, la navigation sur internet. Il s'installe silencieusement dans l'ordinateur contaminé dont il crypte certains types de documents qui deviennent alors illisibles. Les pirates adressent alors un message dans lequel ils demandent une rançon en échange de la clé de déchiffrement des données. Généralement, cette clé n'est jamais fournie, même en cas de paiement.

Ce mardi 10 mars, un «Rançongiciel» a été détecté dans le système informatique de la ville de Toulouse qui avait été placé sous surveillance. Des mesures de précaution, comme l'interruption du travail en réseau, ont été prises immédiatement pour éviter sa propagation. De source interne, aucun fichier n'a été endommagé. Le réseau a été rétabli ce jeudi à 15 heures.

Expert Informatique assermenté 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.ladepeche.fr/article/2015/03/13/2065766-le-reseau-de-la-ville-attaque-par-le-virus-rancongiciel.html

---

Alerte ! Des escrocs se font passer pour des techniciens en informatique | Le Net Expert Informatique

Alerte ! Des escrocs se font passer pour des techniciens en informatique

Mercredi, une habitante de Saint-Pal-de-Mons a subi une tentative d'escroquerie par des cybercriminels. Elle a reçu un appel téléphonique d'une personne parlant anglais se présentant comme employée d'une célèbre entreprise d'informatique. Selon les dires de son interlocuteur, son ordinateur serait infecté d'un virus. L'appel a été transmis à un second présumé technicien qui, toujours en anglais, a proposé à la San-palouse de prendre la main sur la machine.

La femme a alors eu la puce à l'oreille lorsqu'on a lui a demandé ses coordonnées bancaires. Elle a raccroché et s'est rendue dans une entreprise spécialisée. Des fichiers de son ordinateur ont été endommagés.
Elle a ensuité déposée plainte auprès des gendarmes de la communauté de brigades de Saint-Didier-en-Velay.
Selon nos informations, les premiers éléments tendraient vers une escroquerie depuis l'étranger, l'indicatif « 00221 » au moment de l'appel étant celui du Sénégal.

Expert Informatique assermenté 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.leprogres.fr/faits-divers/2015/03/13/cybercriminalite-ils-se-font-passer-pour-des-techniciens-en-informatique

---

Limelight lance un service de détection de limitation de l'impact des attaques DDoS – Global Security Mag Online | Le Net Expert Informatique

Un service de détection de limitation de l'impact des attaques DDoS

Les menaces à la cyber sécurité connaissent une évolution croissante en termes de complexité, de rythme et d'échelle. Selon un enquête récente mondiale, menée en collaboration avec TechValidate, les clients sont le plus préoccupés par l'impact des cyberattaques de type DDoS sur la diffusion de contenu numérique [TVID : 957-39D-E29]. En outre, la majorité des clients interrogés croient que leur fournisseur de CDN est le mieux placés pour les aider à détecter et à limiter l'impact des attaques DDoS [TVID : 0B3-2FC-2FD].

Limelight Networks, Inc. annonce la disponibilité de sa solution DDoS Attack Interceptor, basée sur la plateforme Limelight OrchestrateTM (« Orchestrate »). Composante centrale du service Limelight Orchestrate Security, DDoS Attack Interceptor offre plusieurs lignes de défense pour la protection des clients : notification proactive en cas d'attaque, nettoyage du trafic et protection contre les coûts imprévus en raison des pics de trafic.

En accord avec cette préférence des clients, DDoS Attack Interceptor est directement intégrée dans le réseau CDN mondial de Limelight. Contrairement aux offres concurrentes, qui fonctionnent au niveau du routeur, la solution de Limelight place la détection directement dans le PoP du réseau CDN, offrant la seule détection en fonction de la situation accompagnée de technologies d'atténuation dans le Cloud. Le système de détection perfectionné de Limelight surveille en permanence le réseau pour détecter tout trafic malveillant. Allant au-delà des simples techniques de vérification des signatures, le moteur de détection utilise des techniques brevetées sur les comportements qui comparent la base de référence à partir du volume et des schémas et qui différencie de manière intelligente un bon trafic d'un trafic douteux.
Lorsqu'une attaque est détectée, le système détermine le centre de nettoyage distribué optimal dans le monde et y dirige le trafic, qui y sera alors filtré avant d'être retransmis à l'origine. Le service est entièrement fourni dans le Cloud via la plateforme Limelight Orchestrate, ce qui offre des performances élevées et une haute disponibilité, surtout en temps de sérénité, tout en offrant simultanément une détection continue. Les clients n'ont pas besoin d'acheter un matériel quelconque et aucune dépense d'investissement n'est nécessaire pour bénéficier de la totalité des fonctionnalités de cette offre.
Avec une capacité Egress de plus de 11 Tbit/s, la plateforme Orchestrate de Limelight gère plus de sept milliards de demandes utilisateurs par heure, garantissant la capacité de DDoS Attack Interceptor à gérer les plus grandes cyberattaques connues aujourd'hui. La solution offre un délai d'atténuation à la pointe de l'industrie, basculant rapidement en mode atténuation et offrant une base de référence coordonnée, une détection active et une atténuation rapide qui assurent le démarrage rapide du nettoyage, avec une très courte durée d'accélération, même pour les attaques plus difficiles à détecter.
Aujourd'hui, Limelight a également annoncé la disponibilité de Orchestrate 3.0, une plateforme complète conçue spécialement pour la diffusion de contenu numérique avec une qualité d'expérience (QoE) exceptionnelle. La plateforme Orchestrate 3.0 comprend le plus grand nombre d'améliorations jamais apportées par la société, que ce soit au niveau de l'infrastructure, de la suite logicielle ou de l'offre de services. Elle améliore ainsi pratiquement tous les aspects de l'expérience client et élargit l'offre de la société en incluant de nouveaux services axés sur la sécurité.

Réseau privé mondial Limelight
Le réseau mondial Limelight est l'un des réseaux privés de diffusion de contenu numérique les plus vastes au monde. Avec plus de 80 PoPs et 11 Tbps de capacité Egress, ce réseau a permis la diffusion sur Internet de quelques-uns des évènements les plus importants au monde. Le réseau Limelight assure la diffusion du contenu numérique tout en offrant une expérience d'une qualité irréprochable, quels que soient les pics de trafic et indépendamment des caprices de l'Internet public. Les autres améliorations que la version V3.0 apporte au réseau Limelight comprennent des mises à niveau des disques à circuits intégrés, une capacité supplémentaire de traitement, une bande passante plus large et une connectivité accrue, et de nouveaux points de présence dans le monde.

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

Source : http://www.globalsecuritymag.fr/Limelight-lance-un-service-de,20150312,51490.html

---

Trend Micro dresse le bilan de l'année écoulée dans son rapport annuel de sécurité | Le Net Expert Informatique

Trend Micro dresse le bilan de l'année écoulée dans son rapport annuel de sécurité

Les cyber-attaques réussies contre Sony, avec environ 100 Téraoctets de données piratées et des dommages estimés à près de 100 millions de dollars, sont venues couronner une année mémorable en termes de cyber-sécurité. Le rapport de sécurité annuel de Trend Micro, intitulé « The High Cost of Complacency » (Le coût élevé de la négligence), revient sur ce piratage ainsi que sur les événements de sécurité majeurs qui ont de nouveau illustré l'obstination des cybercriminels et la sophistication de leurs attaques en 2014.

« L'essentiel d'une stratégie de cyber-sécurité repose sur l'identification de ce qui est le plus important, le déploiement de technologies adéquates et la sensibilisation des utilisateurs », explique Raimund Genes, CTO de Trend Micro. « C'est le rôle de tout un chacun, pas seulement des informaticiens, que de préserver les données sensibles de l'entreprise. »
Les informations rassemblées au sein de ce rapport confirment notamment la prédiction formulée par Trend Micro fin 2013, selon laquelle un piratage majeur de données se produirait en moyenne une fois par mois. Pour les entreprises, le besoin de déployer des dispositifs de protection des réseaux et de détection des intrusions se fait d'autant plus sentir.
« A l'image du piratage de Sony, l'envergure et la portée des attaques perpétrées l'année dernière se sont avérées dramatiques », commente Tom Kellermann, Chief Cybersecurity Officer de Trend Micro. « Malheureusement, il ne s'agit sans doute que d'un aperçu de ce que l'avenir nous réserve. »

Parmi les principaux éléments traités dans ce rapport de sécurité 2014 :
Il ne faut négliger aucune menace, aussi minime soit-elle. Les pirates utilisent des méthodes simples pour déjouer la sécurité des entreprises et causer d'importants dégâts.
Les RAM scrapers, ces malware installés sur les terminaux de points de vente, sont presque devenus monnaie courante en 2014. Plusieurs cibles notables ont perdu des millions de données clients au profit des malfaiteurs tout au long de l'année.
De nouvelles attaques ont démontré qu'aucune application n'était invulnérable face à des pirates qui se diversifient.
La banque en ligne et mobile a connu ses plus importants défis de sécurité en 2014, notamment une sérieuse remise en question de l'authentification à deux facteurs comme garant de la sécurité des opérations sensibles.
Les ransomware ont gagné en puissance et en sophistication. Ils se sont étendus à de nouvelles régions du monde et à de nouvelles cibles. Ils vont désormais jusqu'à chiffrer les fichiers sur les systèmes infectés pour s'assurer du paiement de la rançon.

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

Source : http://www.globalsecuritymag.fr/Trend-Micro-dresse-le-bilan-de-l,20150309,51375.html

1 milliard d’adresses mails volées, 2 pirates inculpés | Le Net Expert Informatique

1 milliard d’adresses mails volées, 2 pirates inculpés

Les deux pirates vietnamiens qui ont piraté 8 fournisseurs de services de messagerie américains et volé 1 milliard d’adresses et des informations confidentielles entre 2009 et 2012 ont été inculpés. Un troisième homme qui a permis de tirer 2 millions de dollars de cette affaire est aussi dans le collimateur de la justice.

Il s’agissait bien du casse du siècle. Deux pirates, de nationalité vietnamienne, ont été inculpés, le premier -plaidant coupable – pour le piratage de 8 fournisseurs de services de messagerie et le second pour le vol d’informations confidentielles. D’après le département de la Justice américaine (DOJ), il s’agit de la plus importante brèche de données dans l’histoire des États-Unis. Les attaques se sont déroulées entre février 2009 et juin 2012.
Après avoir volé ce trésor de guerre d’adresses mails, les pirates ont envoyé des spams à des dizaines de millions d’utilisateurs, et parvenus à générer 2 millions de dollars de profits, toujours selon le DOJ.
Quoc Nguyen, 28 ans, a piraté les serveurs de fournisseurs de messagerie et volé des données marketing contenant plus d’un milliard d’adresses mails et, avec son compère Giang Hoang (25 ans), utilisé ces données pour envoyer des spams. Ce dernier a été arrêté en 2012 avant d’être extradé aux États-Unis l’année dernière. Le verdict pour son procès est prévu le 21 avril. Quant à Quoc Nguyen, il est toujours en fuite. En parallèle, un grand jury fédéral a par ailleurs inculpé ce week-end un ressortissant canadien, Da Silva, co-propriétaire de 21 Celsius, une société qui fait tourner le site e-commerce Marketbay.com. Ce dernier s’est rendu complice de Nguyen en lui permettant de générer les 2 millions de dollars de revenus à partir des vols de données réalisées, entre mai 2009 et octobre 2011.

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.lemondeinformatique.fr/actualites/lire-1-milliard-d-adresses-mails-volees-2-pirates-inculpes-60472.html?utm_source=mail&utm_medium=email&utm_campaign=Newsletter

Tendances et prévisions en

cybercriminalité pour 2015 | Le Net Expert Informatique

Tendances et prévisions en cybercriminalité pour 2015

Augmentation des attaques ciblées En 2015, les attaques ciblées deviennent encore plus sophistiquées. Souvent appelées APT (Advanced Persistant Threats), elles sont différentes des cyberattaques traditionnelles. Conçues pour attaquer des victimes spécifiques et pour être silencieuses, les attaques ciblées peuvent être cachées et non détectées dans des réseaux insuffisamment sécurisés.
"Le vecteur des attaques ciblées profite généralement des attaques d'ingénierie sociale", explique Pablo Ramos, chef du laboratoire de recherche ESET en Amérique Latine. "C'est alors que la manipulation psychologique est utilisée pour pousser les victimes potentielles à commettre certaines actions ou à divulguer des informations confidentielles. Les attaques peuvent également prendre l'apparence d'exploits jour-zéro, où elles profitent de vulnérabilités nouvellement découvertes dans un système d'exploitation ou une application particulière."
Au cours de 2014, le blog WeLiveSecurity d'ESET a publié un certain nombre d'analyses approfondies concernant les attaques ciblées, telles que BlackEnergy campaign et Operation Windigo .

Les systèmes de paiement en ligne attirent plus de malware
Alors que toujours plus de personnes adoptent les systèmes de paiement en ligne pour des biens et des services, ces systèmes deviennent encore plus attrayants pour les concepteurs de malware intéressés par les gains financiers.
2014 a vu la plus grande attaque connue à ce jour en matière de paiement digital, quand un pirate a récolté plus de 600.000 dollars US en Bitcoins et Dogecoins en utilisant un réseau de machines infectées.
ESET a signalé les attaques effectuées en mai contre Dogevault site , où les utilisateurs du très populaire portefeuille électronique ont signalé des retraits non autorisés de leurs comptes avant que le site ne soit obligé d'être déconnecté suite à la destruction des données du site par les attaquants. On estime que 56.000 dollars US ont été volés aux utilisateurs du portefeuille en ligne.
Nous avons aussi vu des attaques de force brute telles que Win32/BrutPOS , qui ont essayé d'accéder aux comptes protégés par un mot de passe en les bombardant de mots de passe populaires afin d'avoir un accès à distance – un rappel général en faveur de l'utilisation de mots de passe forts et uniques.

L'internet des choses – nouveaux jouets pour pirates
Alors que de nouveaux appareils se connectent à internet et stockent plus de données, ils deviennent un vecteur d'attaque attrayant pour les cybercriminels. Au cours de 2014, nous avons trouvé plus de preuves de la hausse de cette tendance. Lors de la conférence Defcon, on a vu les attaques sur les voitures en utilisant le dispositif ECU, ou sur la voiture Tesla qui a été piratée afin d'en ouvrir les portes alors qu'elle roulait.
Des attaques et des concepts ont aussi été montrés dans le secteur de la télévision sur différents systèmes, systèmes biométriques sur smartphones, routeurs – pour ne pas mentionner Google glasses.
C'est un domaine émergent pour la cybercriminalité et il restera un secteur de concentration pour l'industrie de la sécurité. Alors que cela pourrait prendre des années avant de devenir une menace grave, il faut agir dès à présent afin de mieux prévenir ce type d'attaques.
Plus d'information
Le rapport complet est disponible sur WeLiveSecurity.com.

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

Source : https://mail.google.com/mail/u/0/?hl=fr&shva=1#inbox/14be54fe5faeb40f?compose=14be53ae312f08d7

Nouveau coup de filet dans le milieu de la cybercriminalité au Mali | Le Net Expert Informatique

Nouveau coup de filet dans le milieu de la cybercriminalité au Mali

Trois nouvelles interpellations ont eu lieu, ce jeudi, au Mali dans une affaire de lutte contre la cybercriminalité. Une bande dirigée depuis les Etats-Unis trafique les lignes de téléphonie mobile, et empoche une partie importante des sommes qui reviennent normalement aux opérateurs. Rien que pour le Mali, selon la section cybercriminalité de la police nationale, le manque à gagner serait évalué à plusieurs centaines de millions de francs CFA.

Le chef du réseau est basé aux Etats-Unis et l'on ne connaît que son prénom : Monsieur Constant. Il a la double nationalité, camerounaise et américaine. C'est un as de l'informatique et Internet n'a pas de secret pour lui.
Constant repère dans des pays d'Afrique de l'Ouest de jeunes travailleurs dans des cybercafés. Ils reçoivent de ce nouveau partenaire basé aux Etats-Unis des appareils sophistiqués. Des outils qui servent à masquer, via Internet, les appels internationaux.
Par exemple, de Bamako un client appelle en dehors du pays, à Paris, via un numéro appartenant à une société malienne de téléphonie mobile. Mais dans le cœur du compteur détraqué, l'appel est considéré comme une communication locale. Or le client qui téléphone va, lui, payer une communication internationale.
Selon la section de lutte contre la cybercriminalité de la police malienne qui travaille avec très peu de moyens, un opérateur privé local aurait déjà perdu, par ce procédé, quelques centaines de millions de francs CFA. Au moins huit personnes ont déjà été arrêtées ou interpellées au Mali. Et dans deux autres pays voisins, des complices sont actuellement recherchés.

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

Source : http://www.rfi.fr/afrique/20150306-mali-reseau-cybercriminels-passe-etre-demantele/

Les femmes principales victimes d'harcèlement sur le net | Le Net Expert Informatique

Les femmes principales victimes d'harcèlement sur le net

En 2014, quatre affaires liées à la cybercriminalité ont été enregistrées par les services de police. Elles ont trait, toutes, à la publication de photos compromettantes, à caractère sexuel, de jeunes filles sur des réseaux sociaux.

«Même si le phénomène demeure marginal par rapport à d'autres contrées, il n'en constitue pas moins une menace sérieuse pour la société où le taux de pénétration du haut débit dans les foyers est en constante augmentation», indique l'officier Belabes.
Les victimes, âgées entre 19 et 26 ans, ont fait l'objet d'un véritable chantage de la part de maitre-chanteurs qui n'ont pas hésité à poster leurs photos sur Facebook notamment, note-t-il en précisant que ces affaires sont en cours d'instruction. «La cybercriminalité se limite pour le moment à la diffusion de scènes obscènes sur Internet et à l'atteinte à la vie privée des citoyens.
Les affaires sur lesquelles enquête la police font suite à des plaintes déposées par les victimes ou leurs parents», ajoute-t-il. C'est à la section de lutte contre la criminalité liée aux NTIC, composée d'informaticiens et rattachée au service de police judicaire (PJ), qu'échoit la mission de traquer les délinquants informatiques. «Créée il y a moins de deux années au niveau de la sûreté de la wilaya, cette section dispose de moyens technologiques appropriés pour lutter efficacement, en coordination avec les services centraux de la DGSN, contre cette nouvelle forme de criminalité insidieuse, invisible et transnationale», assurent les responsables de la PJ. «Les moyens mis en œuvre par la DGSN pour lutter contre les crimes et délits liés aux nouvelles technologies de l'information et de la communication sont dirigés prioritairement à la formation spécialisée des enquêteurs et techniciens», affirment-ils, en soulignant qu'il est encore difficile, actuellement, de contrôler à 100% les réseaux Internet pour la simple raison que beaucoup de sites et de réseaux sont hébergés à l'étranger.
Pour les limiers de la PJ, cela ne les empêche pas de solutionner des affaires dont le caractère «sensible» nécessite une certaine expertise et des enquêtes informatiques longues et minutieuses. C'est le cas de la dénommé N.N., 17 ans, harcelée par deux individus qui ont publié sur Facebook des photos d'elle prises à son insu.
La jeune adolescente ayant subi des semaines durant un harcèlement continu, a fini par déposer plainte auprès de la brigade de protection des mineurs, selon l'officier Belabes.
Les investigations menées par la section de lutte contre la cybercriminalité ont permis, suite à la perquisition des domiciles des dénommés M.C. (20 ans) et de son complice L.H. (21 ans), la découverte des photos stockées dans les disques durs de leur P.C. Les deux mis en cause déférés, ce lundi devant le parquet, ont été mis en examen.

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.elwatan.com/regions/ouest/belabes/cybercriminalite-les-femmes-principales-victimes-d-harcelement-sur-le-net-05-03-2015-288988_138.php
Par Abdelkrim Mammeri

« 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 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/