Le site de rencontre Madison Ashley piraté – l’analyse de Kaspersky Lab | Le Net Expert Informatique

	Le site de rencontre Madison Ashley piraté – l’analyse de Kaspersky Lab

Le site de rencontres adultères canadien Ashley Madison, qui revendique plus de 37 millions d'inscrits, a été victime d'une attaque informatique ayant pour but de voler les données personnelles d'un grand nombre d'utilisateurs. Ces données ont été brièvement mises en ligne.

Marta Janus, chercheuse en sécurité au sein de l'équipe de recherche et d'analyse (GReAT) du spécialiste en sécurité Kaspersky Lab, revient sur cette attaque :
Marta Janus « L'attaque subie par Madison Ashley nous rappelle à quel point il est important pour toutes les entreprises de mettre en place des mesures de sécurité contre les cyberattaques, afin de protéger les données personnelles de leurs utilisateurs. Un internaute qui accepte de confier certaines de ses données privées à un site web devrait être assuré que ses informations seront conservées de la façon la plus sécurisée qui soit, et les entreprises concernées devraient pouvoir s'y engager.
Il faut également rappeler que toutes les failles de sécurité qui entrainent des fuites de données privées sont un problème, quelles que soit la nature du site visé, sa moralité et même sa légalité. Dans le cas de l'attaque contre Ashley Madison, l'affaire est très sérieuse car la fuite concerne des informations comme les noms, les adresses ou encore les données bancaires. Une fois rendues publiques, ces informations pourraient par exemple être utilisées pour voler de l'argent.
Les raisons pour lesquelles une entreprise peut être victime d'une cyber attaque sont nombreuses – argent, politique ou même éthique. N'importe quelle entreprise peut être la cible d'une attaque et même si les solutions de sécurité réduisent les risques que cette attaque soit fructueuse pour les criminels, d'autres mesures existent pour une protection renforcée. Je pense notamment aux mises à jour logicielles, encore trop souvent remises au lendemain, à la réalisation régulière d'audits de sécurité ou encore au test des infrastructures. Le meilleur moyen de lutter contre ce type de cyberattaques est de se protéger avant qu'elles ne frappent en disposant d'une stratégie de sécurité complète et efficace. »

Source : https://www.globalsecuritymag.fr/Site-de-rencontre-pirate-l-analyse,20150720,54540.html
par Kaspersky Lab

Les Etats Unis devraient avoir peur des prochaines cyber-attaques ? | Le Net Expert Informatique

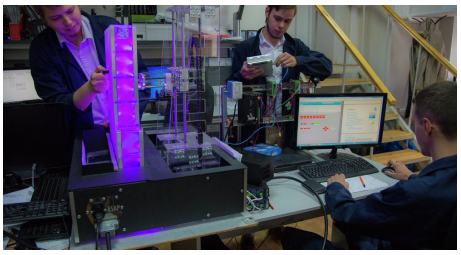
Le nouvel Economiste	Les Etats Unis devraient avoir peur des prochaines cyber-attaques ?

Mercredi dernier, la Bourse de New York et United Airlines ont suspendu leurs activités pendant plusieurs heures en raison de problèmes informatiques mystérieux, tandis que le site Internet du 'Wall Street Journal' a brièvement disparu.

Tous trois ont insisté pour dire qu'il s'agissait de problèmes techniques, et non d'attaques malveillantes. Mais l'inquiétude monte après des agressions contre de puissantes entreprises et agences américaines.
En février dernier, la compagnie d'assurance Anthem révélait que des pirates informatiques avaient volé les données de plus de 80 millions de clients. L'Office of Personnel Management, basé à Washington, révélait que des hackers avaient subtilisé des données de millions d'employés fédéraux. Commerçants ou banques, plusieurs entreprises ont aussi été attaquées.
Mercredi, au moment où la Bourse de New York était suspendue, l'université de Cambridge et le groupe d'assurances Lloyds publiaient un rapport affirmant que si une cyber-attaque s'en prenait au réseau électrique américain, les dommages pourraient s'élever à mille milliards de dollars. Quelques minutes plus tard, le directeur du FBI, James Comey, déclarait devant le Congrès qu'il avait des difficultés à venir à bout des systèmes de chiffrage des djihadistes. En mai, M. Comey expliquait que les terroristes islamiques avaient adopté l'idée d'utiliser des logiciels malveillants contre les infrastructures stratégiques. La chose est plutôt effrayante.
La question clé que les investisseurs, les politiciens et les électeurs doivent se poser est non seulement d'envisager qui pourrait être la prochaine cible, mais aussi de savoir si Washington est capable de face à ces attaques. La réponse est certainement non.
Sur le papier, les ressources ne manquent pas. En début d'année, le président Barack Obama a par exemple affecté 14 milliards de dollars à la lutte contre le cyberterrorisme. Mais le principal problème n'est plus tant un manque d'argent que de coordination : alors que la peur se propage, un nombre ahurissant d'organismes et de groupes de travail différents se sont lancés dans la lutte contre le cyberterrorisme, souvent en collaborant très peu entre eux. L'institution censée être en charge des menaces est le Département de la Sécurité nationale, mais ses compétences laissent sceptiques les responsables militaires. Le Pentagone a son propre personnel affecté aux cyberattaques, tout comme les services secrets.
"Certains pays ont trouvé des réponses : l'Australie possède un niveau impressionnant de coordination entre les secteurs public et privé sur les défenses cybernétiques. Mais avec le tribalisme exacerbé qui sévit à Washington, la triste vérité est qu'il faudra une crise majeure avant que quiconque puisse cogner sur les têtes des bureaucrates de manière efficace"
La Maison-Blanche a tenté d'obliger ces organismes à travailler ensemble. De leur côté, des organismes civils comme la Commission de réglementation nucléaire ont aussi commencé à tenir des réunions discrètes avec d'autres organismes cet automne sur ces questions. Mais la collaboration entre les secteurs reste inégale. "Le niveau de préparation des différents organismes varie énormément" admet un haut responsable de Washington au centre de cette mission. De plus, y ajouter des organismes du secteur privé entraînera une dégradation plus profonde de la situation : non seulement le Pentagone se méfie du partage de données avec d'autres institutions, mais les entreprises sont souvent terrifiées à l'idée de révéler les attaques dont elles ont fait l'objet.
Existe-t-il une solution ? Une réponse sensée pourrait être de créer une nouvelle entité qui serait l'entité centrale de lutte contre le cyberterrorisme. Il existe des précédents, la plupart des régulateurs de Washington ayant été créés pour répondre à une nouvelle menace. La Securities and Exchange Commission, par exemple, a été créée après le krach de 1929 ; la Food and Drug Administration, après des scandales concernant des médicaments dangereux. Une deuxième option serait de relancer le DHS (Department of Homeland Security) afin que celui-ci se focalise sur la lutte contre les cyberattaques. Il pourrait, par exemple, s'appeler ministère de la Sécurité Intérieure et Cybernétique.
Quoi qu'il en soit, Washington a besoin de répondre à la question qu'Henry Kissinger posait pour l'Europe : en temps de crise, "Qui dois-je appeler ?" Certains pays ont trouvé des réponses : l'Australie possède un niveau impressionnant de coordination entre les secteurs public et privé sur la défense cybernétique. Mais avec l'esprit de clan exacerbé qui sévit à Washington, la triste vérité est qu'il faudra une crise majeure avant que quiconque puisse cogner sur les têtes des bureaucrates de manière efficace. Il faut juste espérer que ce "quelque chose" ne sera pas trop dévastateur, comme une attaque réelle des transports ou des marchés.

Source : http://www.lenouveleconomiste.fr/financial-times/les-prochaines-cyber-attaques-contres-les-etats-unis-seront-terribles-27703/
Par David Pilling

Un nouveau système russe contre les cyberattaques industrielles | Le Net Expert Informatique



© PHOTO. INSTITUT D'INGÉNIERIE PHYSIQUE DE MOSCOU

Un nouveau système russe contre les cyberattaques industrielles

L'Université nationale de recherche nucléaire MePhI a conçu un système informatique baptisé Bouclier pour protéger les installations automatiques des entreprises industrielles contre les attaques cybernétiques.

Le système informatique « Bouclier » conçu par les spécialistes de l'Université nationale de recherche nucléaire MePhI pourra être utilisé pour protéger les installations automatiques des entreprises industrielles contre les attaques cybernétiques.
Il sera vendu aux pays membres du groupe des Brics, a déclaré le directeur adjoint du centre d'ingénierie de MePhI (MIFI en russe) Konstantin Mejankov dans une interview accordée à l'hebdomadaire de l'Académie des sciences de Russie Poïsk (Recherche).

La Russie présente une caméra médicale inédite
La protection des systèmes automatisés de contrôle des processus technologiques contre les cyberattaques est considérée comme l'un des principaux problèmes de l'industrie contemporaine. De telles attaques peuvent affecter la chaîne industrielle des entreprises et provoquer des accidents sur les sites, voire des catastrophes anthropiques. Les spécialistes du monde entier cherchent des moyens permettant d'améliorer la protection de l'automation industrielle.
« Les diplômés de la faculté de cybernétique et de la sécurité informatique, ainsi que le Centre de sécurité cybernétique ont participé à ce travail du MePhI. Ils ont créé ensemble le Bouclier qui protège l'automation industrielle de l'accès extérieur non autorisé et des attaques de piratage ou de subversion », explique Konstantin Mejankov.

La Russie relance sa production d'aimants haut de gamme
Il a ajouté que ce système pourrait également être installé sur les oléoducs pour contrôler l'acheminement des hydrocarbures ou encore constater l'apparition de coupures et de fuites.
Le groupe russe InfoWatch, spécialisé dans la sécurité informatique, lance aujourd'hui la vente du système Bouclier aussi bien en Russie qu'à l'étranger, notamment dans les Brics, déclare Konstantin Mejankov. « Par ailleurs, il faut savoir que ce système ne peut pas être transporté dans une boîte et être simplement branché – nos spécialistes se rendent chez chaque client pour diagnostiquer tous les systèmes de l'installation et proposer une solution personnalisée », conclut-il.

Source : http://fr.sputniknews.com/sci_tech/20150718/1017098784.html

Les entreprises attendraient-elles gentiment les attaques ? | Le Net Expert Informatique

Les entreprises attendraient-elles gentiment les attaques ?

Qu’on se le dise : n’importe qui peut se faire attaquer, qu’il s’agisse d’une petite comme d’une grande entreprise.

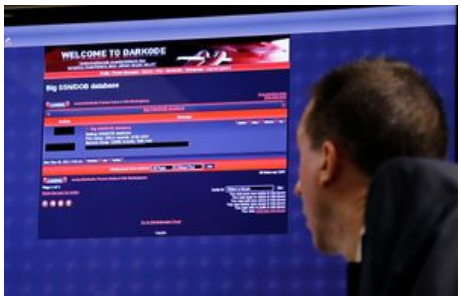
En 2013, le New York Times a subit une cyberattaque de l’armée électronique syrienne ; un groupe d’activistes soutenant Bachard El Assad. Les auteurs ont ciblé la partie la moins sécurisée du réseau, les serveurs DNS alors qu’ils sont devenus la pierre angulaire de toute applications internes ou externes.
En juin dernier, l’US Army s’est faite attaquée par les mêmes hackers. Et ce, alors même que l’Etat--Major américain avait fait de la cyberdéfense une priorité en investissant fortement. Pourtant, ces deux attaques démontrent qu’ils sont faiblement protégés et que, quelque soit leur taille, toutes les entreprises ou organismes sont des cibles potentielles. Les services informatiques n’ont donc pas su s’adapter à ces nouvelles menaces.
En France, le 1er semestre fut dense en matière de cyberattaques : TV5 Monde, Charlie Hebdo et Thales ont fait l’objet de sévères attaques de leur système informatique. On se souvient que des documents présentés comme des pièces d’identité et des CV de proches des militaires français impliqués dans les opérations contre l’EI avaient été postés sur le compte Facebook de TV5Monde par les pirates.
L’attaque avait été initialement revendiquée par des inconnus se réclamant de Daech (Etat Islamique). L’enquête s’oriente en juin vers des hackeurs russes. Le vol de données semble être le principal objectif des hackers.
Quelques semaines plus tôt, Manuel Valls annonçait que la défense française allait intégrer des community managers et hackers, plus à même de contrer les attaques. Une méthode innovante…. mais est--ce suffisant pour protéger une infrastructure réseau ?

Les entreprises françaises en mal d’inspiration ?
En général, les entreprises ne communiquent pas ou très peu sur leurs attaques. En effet, en regardant de plus près les cyberattaques subies en France, on s’aperçoit que les informaticiens n’ont pas su anticiper les nouvelles menaces. Ils ont préféré sécuriser leurs réseaux grâce à des méthodes utilisées depuis des décennies. Malheureusement, cela ne s’avère plus suffisant pour contrer les nouvelles menaces et les nouvelles techniques utilisées par les hackers.
En parallèle, cela met en exergue les problèmes d’investissement que les entreprises rencontrent et leurs manques de réactions.
Selon une étude menée par IDC [1], si la plupart des organisations sont conscientes des risques de sécurité liés aux serveurs DNS (82 % des répondants étaient conscients des menaces, qu’ils ont reconnues), l’essentiel des budgets en sécurité réseau est encore consacré à des solutions de sécurité plus traditionnelles telles que les pare--feu (68 %).
L’étude d’IDC a également révélé que même si 85 % des répondants disposent des fonctions de sécurité du DNS de base, les entreprises restent vulnérables, car ces fonctions sont généralement inefficaces en cas d’attaque.
Enfin, 73% des entreprises françaises ont subies des attaques sur leurs serveurs DNS mais elles ne sont que 7% à les considérer comme une très grande menace contre 27% aux Etats-- Unis, alors que les dégâts subies lors de ces attaques ont été très importants (vol de données, interruption de service, …).
Sans prise de conscience des responsables informatiques français, les cyberattaques ne cesseront de s’intensifier. Avec la multiplication des appareils connectés à internet, dans tous les domaines d’activités (hôpitaux, grandes administrations ou petites entreprises, dans la banque, l’énergie, la défense,), les données continueront d’avoir de la valeur aux yeux des pirates informatiques si les RSI ne changent pas leurs méthodes de protection.

[1] Enquête IDC sur la sécurité des serveurs DNS, avril 2014

Source : https://www.globalsecuritymag.fr/Les-entreprises-attendraient-elles,20150715,54386.html
par Hervé Dhelin, Directeur Marketing d’EfficientIP

Le forum de pirates Darkode est tombé après une opération menée par le FBI | Le Net Expert Informatique

	Le forum de pirates Darkode est tombé après une opération menée par le FBI

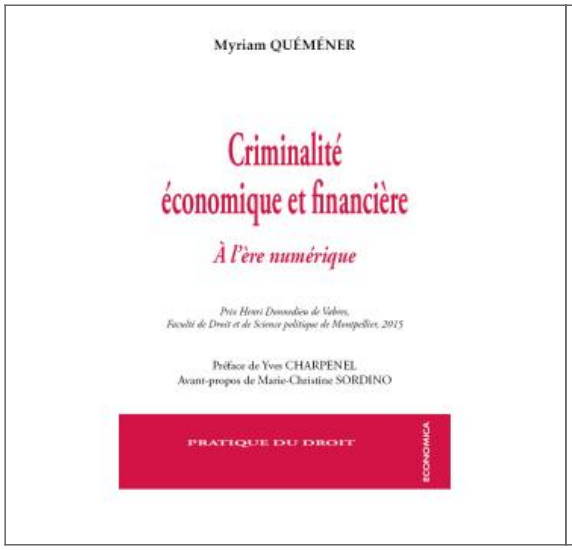
Sous la supervision du FBI , le forum Darkode, qui constituait un point de rendez-vous majeur des pirates pour mener des cyber-attaques, est tombé.

C'est la fin du forum dédié au piratage par lequel il était possible d'acheter, de vendre, de monnayer et de partager des informations ou des outils favorisant des cyber-attaques.
Il a fallu que le FBI s'infiltre dans ce monde underground pour en connaître les coulisses d'administration.
Un accès était uniquement possible par cooptation sous le contrôle des gestionnaires de Darkode : on recensait plusieurs centaines de membres (entre 250 et 300 selon LeMonde.fr).
Mais tout postulant devait démontrer au préalable ses « talents » c'est-à-dire ses capacités à alimenter les ressources malware diffusées via Darkode.
Selon les autorités américaines, des mandats d'arrêt concernant une douzaine de personnes présumées en charge de l'administration de Darkode ont été émis dans trois districts, mais en tout, on évoque 70 membres de Darkode interpellés ou recherchés dans le monde.
Une vingtaine de pays ont été associés à la coupure de ce forum qui entre dans une opération plus large contre la cyber-criminalité baptisée « Shrouded Horizon » : outre les Etats-Unis, on trouve des pays comme l'Australie, le Royaume-Uni, le Brésil, le Canada, la Colombie, la Croatie, le Nigéria, l'Allemagne ou Israël.
« Sur les 800 forums dédié à la criminalité sur Internet, Darkode représentait l'une des plus graves menaces à l'intégrité des données informatiques aux Etats-Unis et dans le monde », déclare David Hickton, procureur fédéral pour le district Ouest de Pennsylvanie, cité dans le communiqué du ministère de la Justice.

A travers le centre anti-cyberciminalité EC3, l'Europe était dans la boucle.
Europol a précisé de son côté que l'opération menée sous la supervision du FBI a abouti à 28 arrestations, 37 perquisitions et un nombre important de saisies de matériel informatique susceptibles d'abriter des preuves et des données pour pousser l'enquête encore plus loin.

Source : http://www.itespresso.fr/darkode-fbi-fait-tomber-forum-ombre-102787.html
Par Philippe Guerrier

La criminalité économique et financière à l’ère numérique | Le Net Expert Informatique



La criminalité économique et financière à l’ère numérique

Les banques, les compagnies d'assurances, les sites gouvernementaux, les compagnies pétrolières et, maintenant, l'industrie aéronautique avec la cyberattaque de la compagnie polonaise LOT : le cybercrime cible des secteurs de plus en plus sensibles, sources de dégâts humains majeurs. Au-delà des pertes financières, c'est le cœur du système politique, économique et juridique qui est aujourd'hui menacé par ce fléau.

Que fait l'État, la justice, pour enrayer ces comportements ? Fabriquer des lois en série est-elle « la » solution face à l'existence de cyberparadis, d'une cyberéconomie souterraine de plus en plus puissante, et à la volatilité des preuves ? Le Point.fr a interrogé Myriam Quemener, magistrate, auteur d'un ouvrage de référence sur le sujet : La criminalité économique et financière à l'ère numérique*.

Le Point.fr : « Certaines formes de cybercriminalité sont le fait de réseaux mafieux structurés issus de pays n'ayant pas de législation dédiée à ce phénomène », écrivez-vous. Le décalage entre les législations étatiques est-il surmontable et à quelle échéance ? Que font les autorités françaises en attendant une prise en charge globale et harmonisée de cette délinquance ?
Myriam Quemener : Les pays européens ont harmonisé leurs législations et la coopération internationale se renforce en permanence. La Convention de Budapest, seul traité relatif à la lutte contre la cybercriminalité, a déjà été signée par 46 pays, et d'autres États sont actuellement en négociation pour y adhérer. Pour ce qui concerne la France, notre pays dispose d'un arsenal ancien, en particulier la loi de 1988 dite « loi Godfrain » qui permet de réprimer les piratages informatiques et les cybermenaces. Cet arsenal s'est progressivement enrichi et perfectionné pour permettre le recours à des procédures adaptées à l'univers numérique. De nouvelles structures sont nées, comme l'Anssi, qui met en œuvre la stratégie gouvernementale en matière de cybersécurité, mais aussi une nouvelle sous-direction de lutte contre la cybercriminalité et un pôle numérique au parquet de Paris qui a vocation à s'étoffer. On a aussi créé le procureur de la République financier à compétence nationale exclusive en matière de délits boursiers et pour les affaires économiques et financières complexes qui sont aussi souvent à dimension internationale.

Quels sont les nouveaux moyens d'investigation des enquêteurs pour déjouer les attaques ?
Sur le plan procédural, le législateur a transposé le régime des interceptions téléphoniques à Internet. Il a aussi innové en prévoyant l'infiltration numérique, qui est une enquête sous pseudonyme. Elle permet à l'enquêteur d'utiliser un nom d'emprunt pour entrer plus facilement en contact avec le cyberdélinquant. Depuis la loi du 13 novembre 2014, l'enquête sous pseudonyme jusqu'alors utilisée en matière de pédopornographie et de contrefaçon s'applique à l'ensemble des procédures de criminalité organisée.

Les données personnelles sont considérées comme « l'or noir du XXIe siècle ». La semaine dernière, une importante base de données américaine abritant les coordonnées, données de santé et autres informations personnelles d'environ 20 millions de fonctionnaires a été piratée. Quel usage les cyberdélinquants font-ils des données récupérées, et à quoi peut-on s'attendre dans les années qui viennent ?
Ils récupèrent ces données et les revendent sur les marchés noirs du Web (Darknet) qui sont des réseaux parallèles aux réseaux ouverts du type Google. Cela permet par exemple de faire des achats sous de fausses identités ou d'obtenir des virements en se faisant passer pour une entreprise connue. Les données personnelles servent aussi à créer de faux profils, et tout cela se répercute sur l'e-réputation des entreprises. L'usurpation d'adresses IP (spoofing) qui permet de commettre des fraudes à la téléphonie mobile se développe aussi de manière considérable.

Quels sont les prochains défis de la criminalité astucieuse sur Internet ?
En cette période où le terrorisme frappe de façon dramatique, il est important de s'attaquer avec vigueur au financement du terrorisme, et cette lutte passe par une politique publique pragmatique et déterminée contre des phénomènes comme le cyberblanchiment ou les escroqueries aux faux ordres de virement.
Il faut par ailleurs être attentif et vigilant face à des outils numériques comme le crowdfunding (financement participatif) ou les crédits à la consommation. Les sommes obtenues au travers de ces formes de prêt peuvent en effet servir à financer des activités illicites. Il en est de même du « trading haute fréquence » qui permet d'envoyer des ordres d'achat à une vitesse de l'ordre de la nanoseconde, grâce à des algorithmes superpuissants, permettant des manipulations de cours. Le courtage à haute fréquence a aussi ses dérives : un courtier londonien a récemment été arrêté pour une manipulation sur le marché des contrats à terme électroniques aux États-Unis, qui avait contribué au mini-krach de mai 2010 à Wall Street.
Il faut aussi suivre avec attention le développement de ces fameuses « monnaies virtuelles » qui contournent le système bancaire et permettent d'échapper à tout contrôle étatique en raison de l'absence de traçabilité. Les objets connectés, qui favorisent l'usurpation de profils complets, et le cloud computing qui contient des données sensibles à valeur commerciale sont aussi des cibles potentielles de cyberattaques. D'autant que de nombreuses failles de sécurité existent et peuvent être exploitées par les cybercriminels.

Qu'est-ce qui dissuade vraiment les délinquants, qu'ils soient isolés ou membres d'organisations criminelles ?
La mise en place d'une stratégie globale au niveau des services de l'État est de nature à dissuader les cyberdélinquants, de même que les condamnations et démantèlements de réseaux de cybercriminels qui ne cessent d'augmenter grâce aux moyens d'investigation et à l'expertise de plus en plus pointue des enquêteurs dédiés.

Pensez-vous que l'Internet a démultiplié les risques, ou les a-t-il seulement déplacés ?
L'absence de confrontation physique auteur-victime, propre à Internet, facilite le passage à l'acte. Le système des rencontres virtuelles attire des personnes mal intentionnées qui peuvent plus facilement extorquer de l'argent, notamment via des sites de vente entre particuliers. Aujourd'hui, la cybercriminalité s'industrialise et s'organise sous forme de structures hiérarchisées allant de la main-d'œuvre de base qui récupère des données jusqu'aux têtes de réseau qui donnent les ordres.

Ces phénomènes sont-ils, comme le changement climatique, irréversibles ?
Je ne le pense pas, car, actuellement, il y a une mobilisation importante, du secteur tant public que privé, pour lutter contre ces phénomènes. Il est indispensable de multiplier les actions de formation pluridisciplinaire des acteurs publics et privés qui concourent à la lutte contre ces attaques. Cependant, il ne faut pas perdre de vue que ce type de délinquance lance un défi au temps judiciaire, c'est même une course contre la montre !

L'ouvrage en vente ici

Source : http://www.lepoint.fr/chroniqueurs-du-point/laurence-neuer/cybercrime-un-defi-lance-au-temps-judiciaire-13-07-2015-1943938_56.php

---

| Le Net Expert Informatique

Les Chiffres et Statistiques du numérique : Usages, risques, cybercriminalité (Dernière infos rajoutées le 17/07/2015)

Dernière infos rajoutées le 17/07/2015

Dans le but de vous permettre de mieux juger l'importance du Risque Informatique et de la Cybercriminalité en France et ailleurs, nous avons souhaité mettre à disposition le résultat de nos collectes successives de statistiques relativement impressionnantes.

Ces chiffres ne m'appartiennent pas et pour chacun d'eux, est indiqué la date d'ajout dans ce document et la source d'information associée. Cependant, **si vous souhaitez reprendre tout ou partie du résultats de mes recherches, je vous demanderais soit de citer « Denis JACOPINI » ou « Le Net Expert » comme source de votre information**.

Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Imaginez un instant que vous soyez consommateur. Vous découvrez soudain que vos données (coordonnées personnelles, bancaires ou encore médicales) se trouvent diffusées sur le net, sans votre accord, à cause de la négligence d'un professionnel.
Imaginez maintenant que ce professionnel c'est vous, et ce, malgré la mise en application imminente du projet de règlement Européen sur la Protection des données personnelles, le risque d'anéantir votre réputation et de vous sanctionner lourdement. Certes, le mal est fait mais pire, les Cybercriminels sauront en profiter !

Lorsque, lors de conférences, je m'adresse à des entreprises pour leur parler de sécurité informatique et de risque de piratage, les chefs d'entreprises, pourtant vêtus d'une responsabilité souvent pénale, me rétorquent du « On n'est pas concerné, on n'est pas la Nasa », du « On n'a pas de secret qui pourrait intéresser des pirates, on ne risque rien » ou bien du « de toute façon, le peu de contrôles que la CNIL fait n'aboutissent qu'à des amendes symboliques ».

De leur répondre : « Bien sur que si, vous avez des informations secrètes, et même ultra secrètes : LES DONNEES A CARACTERE PERSONNEL DE VOS CLIENTS ». Et vous avez même ente vos main quelque chose d'encore plus précieux que ça : VOTRE REPUTATION »

Trop peu respectée, la loi informatique et libertés fixe impose à tout responsable de traitement de données

personnelles de mettre en place des mesures de sécurité appropriées à la protection des données à caractère personnel.

Sans cela, données non protégées = données piratées et diffusées dans la nature = risque pénal mais surtout réputation salie.

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. Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

INTERNET DANS LE MONDE EN 2014

42% de la population mondiale soit 3,025 milliards de personnes utilisent le réseau internet. (D27-S35)

Sur l'ensemble du continent africain, le taux de pénétration d'Internet est estimé à 16% en 2014 soit 167 millions d'internautes, contre 110 millions en 2010. (D27-S35)

Le nombre des utilisateurs d'Internet en Afrique devrait être multiplié par 3.5 d'ici 2015 pour que le nombre d'internautes atteigne près de 600 millions. (D27-S35)

Nombre d’internautes : 3,001,769,770 (35% de la population mondiale). (D9-S16)

Le cap des 3,2 milliards d’internautes devrait être dépassé dans le monde en 2014

Taux de pénétration d’Internet dans le Monde :
81% en Amérique du Nord (86% au Canada, 80% aux USA) (D9-S16)
78% en Europe de l’Ouest (83% en France) (D9-S16) 18% en Afrique (D9-S16)
12% en Asie du Sud (D9-S16)
822 240 nouveaux sites Internet sont mis en ligne chaque jour (D9-S16)

Chaque minute sur Internet : (D9-S16)
2 millions de requêtes Google sont effectuées
347 nouvelles publications WordPress sont publiées
571 nouveaux sites web sont créés
2000 nouvelles photos sont ajoutés sur Tumblr
204 millions d’emails sont envoyés

Denis JACOPINI est à l’origine de cette collecte d’information. Merci de le citer si vous utilisez le résultat de ce travail.

Denis JACOPINI est Expert Informatique assermenté et formateur spécialisé en mise en conformité avec la CNIL, en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel.

Posez vos questions

TÉLÉCHARGEMENT ILLÉGAL ET LOI HADOPI

10% des abonnés avertis une fois récidivent. (D23-S31)

Sur les 8,9% de titulaires d'un abonnement à Internet ayant reçu un premier avertissement (entre octobre 2010 et juin 2014, soit plus de 3,2 millions d'emails envoyés), ils ne sont plus que 10,4% d'entre eux à avoir été avertis une deuxième fois – puis 0,4% à s'être retrouvés en phase 3. (D23-S31)

70% diminuent leur consommation illicite après l'avertissement 1. (D23-S31)

88% diminuent leur consommation illicite après l'avertissement 2. (D23-S31)

Après un avertissement, seulement 23% à déclarer se tourner vers une offre légale. (D23-S31)

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. Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

LA SÉCURITÉ ET LES CERTIFICATS SSL

Jusqu’à 91% des internautes n’iront pas plus loin en cas d’avertissement au risque de malware ou de phising. (D17 – S25)

Plus des 2/3 (77%) des sites Internet propagateurs de malwares sont des sites légitimes infectés. (D17 – S25)

Un site Internet sur 8 comporte des vulnérabilités critiques. (D17 – S25)

Denis JACOPINI est à l’origine de cette collecte d’information. Merci de le citer si vous utilisez le résultat de ce travail.

Denis JACOPINI est Expert Informatique assermenté et formateur spécialisé en mise en conformité avec la CNIL, en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel.

Posez vos questions

LES FRANCAIS ET LE PAIEMENT SANS CONTACT NFC

15 % utilisent la fonction NFC de leur CB (D24-S32)

19 % ignorent si leur carte dispose de cette option (D24-S32)

34% estiment cette technologie utile (D24-S32)

22% des Français sont à l'aise avec le paiement sans contact (D24-S32)

44 % ont connaissance de la fonction paiement sans contact de leur carte bancaire (D24-S32)

29 % ne s'en servent pas sachant qu'ils ont cette option (D24-S32)

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.
Besoin d’informations complémentaires ?

Contactez-nous

Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

LA SÉCURITÉ ET LE BYOD

95% des entreprises se disent menacées par des problèmes de sécurité liés au BYOD. (D17-S24)

82% pensent même que le nombre d’incidents dans ce domaine va croître en 2015 par rapport à 2014. (D17-S24)

47% des entreprises ont éprouvé des intrusions suite à des brèches présentes dans des appareils mobiles. (D17-S24)

64% pensent qu’Android est toujours considéré comme le système d’exploitation le plus risqué des OS mobiles. (D17-S24)

Denis JACOPINI est à l’origine de cette collecte d’information. Merci de le citer si vous utilisez le résultat de ce travail.

Denis JACOPINI est Expert Informatique assermenté et formateur

spécialisé en mise en conformité avec la CNIL, en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel.

Posez vos questions

LA SÉCURITÉ EN ENTREPRISE

Une étude internationale a interrogé 450 décideurs informatiques et révèle que de nombreuses sociétés se heurtent aux exigences de gouvernance et de sécurité des échanges de données. (D22-S30).

23% des entreprises ont récemment échoué à un audit de sécurité, tandis que

17 % doutent de leur capacité à réussir un audit de conformité des échanges de données.

Le coût total moyen d'une atteinte à l'intégrité des données s'élève à 2,4 millions d'euros.

La stratégie d'intégration n'est pas alignée avec les structures et les politiques de gouvernance, de confidentialité et de sécurité des données pour 71% des entreprises.

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. Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

LA CYBERCRIMINALITE ET LES MOBILES

Entre janvier et juin 2014, le nombre d'infections touchant les terminaux mobiles a progressé de 17% (20% seulement sur tout 2013. (D15-S22)

0,65% des smartphones en circulation sont infectés d'un malware. Les smartphones équipés d'Android comptent 60% des équipements mobiles infectés contre 40% pour les PC portables équipés de Windows.

De leur côté, les iPhone, les BlackBerry, les téléphones sous Symbian et sous Windows Phone totaliseraient moins de 1%.

Le cheval de Troie *Android.Trojan.Coogos.A!tr* représenterait 35,69% des attaques ciblant Android.

Denis JACOPINI est à l'origine de cette collecte d'information. Merci de le citer si vous utilisez le résultat de ce travail.

Denis JACOPINI est Expert Informatique assermenté et formateur spécialisé en mise en conformité avec la CNIL, en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel.

Posez vos questions

LE CLOUD EN ENTREPRISE

Enquête Eurostat : Utilisation des TIC dans les entreprises en 2014 (D19-S21)

19% des entreprises utilisait des services de cloud computing en 2014

45% secteur de l'information & de la communication

27% activités spécialisées, scientifiques et techniques

14% et 20% dans tous les autres secteurs économiques

Pour les 81% des entreprises n'utilisant pas le cloud, une connaissance insuffisante de ces services informatiques constituait le principal facteur bloquant.

En 2014, les proportions les plus élevées d'entreprises

utilisant le cloud ont été observées en Finlande (51%), en Italie (40%), en Suède (39%) ainsi qu'au Danemark (38%). À l'opposé, les services de cloud computing étaient utilisés par moins de 10% des entreprises en Roumanie (5%), en Lettonie et en Pologne (6% chacun), en Bulgarie, en Grèce et en Hongrie (8% chacun).
Dans seize États membres, le cloud était principalement utilisé pour les services de courrier électronique, notamment en Italie (86%), en Croatie (85%) et en Slovaquie (84%). Les services de cloud computing étaient principalement utilisés pour le stockage de fichiers dans onze autres États membres, les proportions les plus élevées ayant été observées en Irlande (74%), au Royaume-Uni (71%), au Danemark ainsi qu'à Chypre (70% chacun), tandis que l'hébergement de la base de données de l'entreprise était l'usage du cloud le plus courant aux Pays-Bas (64%).

Enquête Unitrend auprès d'entreprises (D19-S21) :

78% ont connu des coupures des applications critiques.

63% estiment que les pertes ainsi engendrées vont de quelques centaines de dollars à plus de 5 millions.

28% des entreprises touchées par un incident estiment que leurs entreprises ont été privées de fonctions clés de leurs datacenters pendant des périodes pouvant aller jusqu'à plusieurs semaines.

73% des entreprises déclarent ne pas prêtes pour la restauration après sinistre.

60% estiment qu'elles n'ont pas complètement documenté leur plan de reprise d'activité.

23% n'ont jamais testé ces plans de reprise d'activité.

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. Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

CE QUE PENSENT LES ENTREPRISES DE LEUR SECURITÉ

Sept entreprises sur dix seraient convaincues de disposer d'un pare-feu de nouvelle génération (*Next Generation Firewall*, ou NGFW) alors que… non, elles ne seraient en fait que 30 % à en posséder. (D16-S23)

54 % des DSI français pensent que leur pare-feu dispose de capacités de détection avancées efficaces, intégrant notamment des fonctions de sandboxing spécifiques aux fameux NGFW. (D16-S23)

31 % des décideurs IT estiment que leur entreprise utilise trop de solutions de sécurité pour gérer les menaces. (S16-S23)

Denis JACOPINI est à l'origine de cette collecte d'information. Merci de le citer si vous utilisez le résultat de ce travail.

Denis JACOPINI est Expert Informatique assermenté et formateur spécialisé en mise en conformité avec la CNIL, en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel.

Posez vos questions

LE DROIT À L'OUBLI

Les plaintes liées au droit à l'oubli, en hausse de quatre points par rapport à 2012, ont représenté 34 % du nombre total de plaintes en 2013. (D13-S20)

Denis JACOPINI est à l'origine de cette collecte d'information. Merci de le citer si vous utilisez le résultat de ce travail.

Denis JACOPINI est Expert Informatique assermenté et formateur spécialisé en mise en conformité avec la CNIL, en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel.

Posez vos questions

CYBERCRIMINALITÉ

5 entreprises sur 6 employant plus de 2 500 personnes ont été la cible de cyberattaques en 2014 (D28-S36)

Entre 2013 et 2014, le nombre des cyberattaques a augmenté de 120% dans le monde et le coût estimé de la cybercriminalité pour les entreprises s'élève en moyenne à 7,6 millions de dollars par an, soit une augmentation de 10% (D26-S34)

61 % des victimes d'une attaque DDoS ont temporairement perdu l'accès à des informations critiques (D25-S33)

38 % ont été dans l'incapacité de poursuivre leur activité principale(D25-S33)
33 % font état de pertes d'opportunités et de contrats (D25-S33)
Dans 29 % des cas, le succès d'une attaque DDoS a eu un impact négatif sur la cote de crédit de l'entreprise (D25-S33)
Dans 26 % des cas, a entraîné une augmentation de ses primes d'assurance (D25-S33)
A la suite d'une attaque DDOS, 49 % ont payé pour faire modifier leur infrastructure informatique, 46 % ont eu recours à leurs avocats et 41 % ont fait appel à des gestionnaires de risque (D25-S33)

72 % des victimes ont divulgué des informations relatives à une attaque DDoS contre leurs ressources. En particulier, 43 % des responsables interrogés ont informé leurs clients d'un incident, 36 % l'ont signalé aux autorités et 26 % en ont parlé aux médias. 38 % des entreprises ont subi une atteinte à leur réputation à la suite d'une attaque DDoS et près d'une sur trois a dû demander l'aide de conseillers en image (D25-S33)

48 % des attaques cibleraient directement des applications web des e-commerçants. (D20-S28)

40 % des attaques par injection SQL et 64 % des campagnes de trafic http malveillant concernent les sites de commerce en ligne. (D20-S28)

Selon l'enquête d'Imperva, les sites de commerce en ligne sont attaqués deux fois plus souvent que des sites plus classiques. Les attaques durent aussi plus longtemps : près de deux fois plus longtemps qu'en 2013. (D20-S28)

68% des internautes envisagent un achat sur internet d'ici la fin de l'année. (D20-S28)

La valeur économique pillée par la cybercriminalité en 2013 représente 190 milliards d'euros. (D18-S26)
Pour illustrer un coût :
« Sony s'est fait voler 1,5 million de données de cartes bleues. Le dommage direct : 150 millions. Mais Sony réclame à son assureur 1,3 milliard de dollars pour compenser l'arrêt complet de leur serveur pollué de e-commerce, c'est-à-dire de leurs ventes, la modification de leur système d'information et la campagne de communication qui a suivi. »

Après avoir analysé les données de plus de 100.000 incidents de sécurité sur 10 ans, Verizon a indiqué que 92 % des attaques peuvent être réparties en 9 types de menaces (les attaques de malwares, la perte ou le vol d'appareils, les attaques DDoS, les arnaques à la carte bancaire, les attaques

d’applications web, le cyber-espionnage, les intrusions, le vol interne et les erreurs humaines), ce qui signifie que les entreprises font toujours face aux mêmes risques et aux mêmes attaques, depuis tout ce temps, et à plusieurs reprises. (D12-S19)

Les fraudes en ligne par carte bancaire ont représenté 64,6% du total des fraudes en 2013, soit un rapport de un à vingt par rapport aux magasins physiques. (D11-S18)

Les e-commerçants ne sont que 43 % à utiliser ces méthodes de protection renforcés (par SMS ou par biométrie) 10 millions de français, 33% des Internautes majeurs victimes de cybercrime (Symantec/Norton 2013). (D1-S1)

47% des logiciels étaient piratés en 2005 contre 37% en 2011. (D6-S11)

Les condamnations d’entreprises ayant piraté des logiciels se sont élevées à 1,3 millions d’euros en 2013, en hausse de 30% par rapport à 2012, représentant 12% du montant des condamnations européennes. (D6-S11)

En juin 2014, 3,2 millions de premiers avertissements ont été expédiés depuis sa création et 333.723 deuxièmes avertissements (lettre recommandée) et 71 dossiers transmis à la justice. (D10-S17)

75 % des messages partent de machines classiques (ordinateurs de bureau ou portables, smartphones, tablettes), le reste provient d’appareils connectés. (D3-S6)

Dans 33% des cas, l’introduction d’un malware est réalisée au travers d’une application mobile. (D2-S5)

58% des entreprises pointent l’inefficacité des antivirus du marché pour lutter contre les malwares. (D2-S5)

56% des PC sont infectés via des emails de type « phishing ». (D2-S5)

40% des infections par Malware sont dues aux sites pornographiques. (D2-S5)

Plus de 30% de nos ordinateurs personnels stockent des fichiers illicites à notre insu. (D2-S4).

61% des sites malveillants sont en fait des sites institutionnels. (D1-S1) (D1-S3)

1 site Internet sur 500 est infecté par de malwares (D1-S3)

Google bloque 10000 sites Internet par jour (D1-S3)

400 Millions de personnes sont concernées par des cyberattaques chaque année (D1-S3)

93 % des grandes entreprises ont été victimes d'une cyberattaque en 2012 (D1-S2)

Attaques cybercriminelles +42% en 2012. (D1-S1)

Attaques en ligne +30% en 2012. (D1-S1)

Maliciels sur mobiles +58% en 2012. (D1-S1)

31% des cibles sont des PME en 2012 contre 18% en 2011. (D1-S1)

Denis JACOPINI est à l'origine de cette collecte d'information. Merci de le citer si vous utilisez le résultat de ce travail.

Denis JACOPINI est Expert Informatique assermenté et formateur spécialisé en mise en conformité avec la CNIL, en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel.

Posez vos questions

MESSAGERIE ÉLECTRONIQUE

144 milliards d’emails sont échangés chaque jour. (D9-S16)

68,8% d’entre eux sont des spams. (D9-S16)

Denis JACOPINI est à l’origine de cette collecte d’information. Merci de le citer si vous utilisez le résultat de ce travail.

Denis JACOPINI est Expert Informatique assermenté et formateur spécialisé en mise en conformité avec la CNIL, en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel.

Posez vos questions

LES VOLS

3 français sur 10 disent avoir déjà perdu ou s’être fait voler leur téléphone. (D7-S14)

630 000 vols de téléphones portables en 2011. (D5-S9)

160 000 vols de téléphones portables en 2010. (D5-S8)

Denis JACOPINI est à l'origine de cette collecte d'information. Merci de le citer si vous utilisez le résultat de ce travail.

Denis JACOPINI est Expert Informatique assermenté et formateur spécialisé en mise en conformité avec la CNIL, en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel.

Posez vos questions

RÉSEAUX SOCIAUX

18 % des sociétés de plus de 10 salariés ont un compte dans un réseau social. (D6-S13)

Moins de 13% des sociétés dans le domaine de la construction, du transport ou de l'industrie ont un compte dans un réseau social. (D6-S13)

38 % des sociétés dans le domaine de l'hébergement et de la restauration ont un compte dans un réseau social. (D6-S13)

60 % des sociétés dans le domaine de la communication, de

l’information ou de la réparation d’ordinateurs ont un compte dans un réseau social. (D6-S13)

80% d’entres utilisent les réseaux sociaux pour développer leur image ou commercialiser leurs produits. (D6-S13)

43 % des sociétés de plus de 250 salariés ont un compte. (D6-S13)

5% utilisent les blogs et les sites Internet de partage de contenu multimédia. (D6-S13)

4% utilisent des outils de partage de connaissance. (D6-S13)

Twitter a 900 millions de comptes crées dans le monde mais seulement 241 millions sont actifs. (D5-S11)

Facebook : 1,23 milliard d’utilisateurs actifs dans le monde. (D5-S11)

LinkedIn : 150 millions d’utilisateurs actifs dans le monde. (D5-S11)

Google+ : 300 millions d’utilisateurs actifs dans le monde. (D5-S11)

Tumblr : 166 millions d’utilisateurs actifs dans le monde. (D5-S11)

Viadeo : 55 millions de membres dans le monde dont 8 millions en France et 4,4 millions de visiteurs uniques. (D5-S11)

Instagram : 200 millions d’utilisateurs actifs dans le monde. (D5-S11)

Pinterest : 20 millions d’utilisateurs actifs dans le monde. (D5-S11)

Denis JACOPINI est à l'origine de cette collecte d'information. Merci de le citer si vous utilisez le résultat de ce travail.

Denis JACOPINI est Expert Informatique assermenté et formateur spécialisé en mise en conformité avec la CNIL, en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel.

Posez vos questions

ÉQUIPEMENTS DES FRANCAIS

Un foyer sur cinq (21,523%) en France dispose d'une tablette tactile. (D5-S11)

Ils n'étaient que 14,1% au 4e trimestre 2012. (D5-S11)

L'accès à l'Internet mobile double chaque année. (D9-S16)

70% des internautes sont des utilisateurs quotidiens. (D9-S16)

8 nouveaux utilisateurs chaque seconde. (D9-S16)

Denis JACOPINI est à l'origine de cette collecte d'information. Merci de le citer si vous utilisez le résultat

de ce travail.

Denis JACOPINI est Expert Informatique assermenté et formateur spécialisé en mise en conformité avec la CNIL, en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel.

Posez vos questions

LES BLOGS et BLOGUEURS

En France, seulement 4% des blogueurs sont des professionnels. (D4-S7)

65% des blogueurs gagnent 0€ / mois (passion). (D4-S7)

18% des blogueurs gagnent moins de 100€/ mois. (D4-S7)

10% des blogueurs gagnent entre 100€ et 1000€/ mois. (D4-S7)

7% des blogueurs gagnent plus de 1000€/ mois. (D4-S7)

Denis JACOPINI est à l'origine de cette collecte d'information. Merci de le citer si vous utilisez le résultat de ce travail.

Denis JACOPINI est Expert Informatique assermenté et formateur spécialisé en mise en conformité avec la CNIL, en sécurité

Informatique, en cybercriminalité et en protection des données à caractère personnel.

Posez vos questions

GOOGLE ET LA PRESSE

Rappelez-vous, en février 2013, Google acceptait de verser 60 millions d'euros à la presse française sur 3 ans. (D8-S15)

Pour l'année 2013, 16 millions d'euros ont été versés. Voici comment ont été dépensés les millions pour les 12 principaux bénéficiaires (23 au total) :
Le Nouvel Observateur a reçu 2 millions d'euro pour créer une édition numérique quotidienne.
L'Express, 1,97 millions pour analyser les données utilisateurs.
Le Figaro, 1,8 millions pour renforcer son site de vidéos.
Le Monde, 1,8 millions pour une future édition du matin sur mobiles.
Ouest-France, 1,4 millions pour deux éditions en ligne par jour.
La Voix du Nord, 840.000 euros pour créer 1524 portails.
La Croix, 835.000 euros pour analyser son audience.
Slate, 758.000 euros pour analyser les conversations numériques

Denis JACOPINI est à l'origine de cette collecte d'information. Merci de le citer si vous utilisez le résultat de ce travail.

Denis JACOPINI est Expert Informatique assermenté et formateur spécialisé en mise en conformité avec la CNIL, en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel.

Posez vos questions

Date de la Mises à jour de ce document : (1) 14/03/2014 – (2) 27/03/2014 – (3) 07/04/2014 – (4) 20/04/2014 – (5) 23/04/2014 – (6) 25/04/2014 – (7) 08/05/2014 – (8) 17/05/2014 – (9) 23/06/2014 – (10) 12/07/2014 – (11) 17/07/2014 – (12) 22/07/2014 – (13) 02/09/2014 – (14) 03/09/2014 – (15) 10/09/2014 – (16) 28/10/2014 – (17) 30/10/2014 – (18) 31/10/2014 – (19) 03/11/2014 – (20) 29/11/2014 – (21) 11/12/20214 – (22) 12/12/2014 – (23) 28/12/2014 – (24) 25/01/2015 – (25) 29/01/2015 – (26) 13/02/2015 – (27) 25/05/2015 – (28) 17/07/2015

Sources :
(1)
http://www.symantec.com/fr/fr/about/news/release/article.jsp?prid=20130416_01 (2)
http://www.lemondeinformatique.fr/actualites/lire-%20cybersecurite-en-europe-les-geants-de-l-internet-%20dispenses-de-declarer-les-incidents-56868.html
(3)

https://www.symantec-wss.com/fr/cybercrime4/int/thanks#.Uyr10rK9KSP
(4) Jean-Paul PINTE le 21/03/2014 cours de Cybercriminalité UM1
(5) http://www.testsdintrusion.com/40-infections-malware-dues-aux-sites-pornographiques/
(6) http://www.tomshardware.fr/articles/internet-objet-frigo-spam,1-46695.html
(7) La Quotidienne du 14 04 2014 (France 5) source NWE
(8) http://www.sfr.fr/securite/protection-virus/protection-donnees
(9) http://www.economiematin.fr/les-experts/item/9596-kill-switch-protection-vol-telephone-legislation
(10) http://www.alexitauzin.com/2013/04/combien-dutilisateurs-de-facebook.html
(11) http://www.economiematin.fr/ecoquick/item/7764-etude-equipements-francais-smartphones-tablettes
(12) http://www.zdnet.fr/actualites/logiciels-pirates-13-million-d-euros-de-couts-pour-les-entreprises-francaises-poursuivies-39800283.htm
(13) http://www.zdnet.fr/actualites/les-entreprises-francaises-desertent-les-reseaux-sociaux-selon-l-insee-39800331.htm
(14) http://www.monreseau-it.fr/dossiers/les-antivirus-pour-smartphones-sontils-necessaires-6.htm
(15) http://ecrans.liberation.fr/ecrans/2014/05/15/le-fonds-google-a-verse-16-millions-d-euros-aux-medias-francais-en-2013_1018165
(16) http://www.blogdumoderateur.com/chiffres-internet/
(17) http://www.zdnet.fr/actualites/hadopi-la-machine-a-avertissements-bat-des-records-39803735.htm
(18) http://www.01net.com/editorial/623890/cartes-bancaires-20-fois-plus-de-fraudes-sur-internet-qu-en-magasin/#?xtor=EPR-1-[NL-01net-Actus]-20140716

(19) http://www.huffingtonpost.fr/cyrille-badeau/lutte-cybercriminalite-perdue_b_5595494.html?utm_hp_ref=france
(20) http://www.lepoint.fr/chroniqueurs-du-point/laurence-neuer/google-aux-commandes-du-droit-a-l-oubli-02-06-2014-1830043_56.php
(21) http://www.zdnet.fr/actualites/reprise-d-activite-73-des-entreprises-ne-sont-pas-pretes-apres-un-sinistre-dans-le-cloud-39805553.htm
(22) http://pro.clubic.com/it-business/securite-et-donnees/actualite-725971-etude-15-smartphones-infectes-malware.html
(23) http://www.lemagit.fr/actualites/2240233481/Securite-des-entreprises-francaises-moins-matures-quelles-ne-le-pensent?asrc=EM_MDN_35775718
(24) http://www.zdnet.fr/actualites/byod-des-couts-lies-a-la-securite-parfois-eleves-39808695.htm
(25) https://www.symantec-wss.com/campaigns/15354/fr/assets/infographic/index.html#.VFINvCKG8t4
(26) http://www.paristechreview.com/2014/10/27/espionnage-industriel/
(27) http://www.internetlivestats.com/internet-users/
(28) http://www.commentcamarche.net/news/5865731-les-e-commercants-cibles-par-les-attaques-des-cybercriminels
(29) http://epp.eurostat.ec.europa.eu/cache/ITY_PUBLIC/4-09122014-AP/FR/4-09122014-AP-FR.PDF
(30) http://www.info.expoprotection.com/site/FR/L_actu_des_risques_malveillance__feu/Zoom_article,I1602,Zoom-ce92e8de85306f8f94bb572e6ec6d325.htm
(31) http://www.zdnet.fr/actualites/telechargement-un-avertissement-d-hadopi-ca-calme-39803911.htm
(32) http://pro.clubic.com/e-commerce/paiement-en-ligne/actualite-751153-nfc.html
(33) http://www.globalsecuritymag.fr/Kaspersky-Lab-et-B2B-International,20150128,50328.html
(34) http://www.globalsecuritymag.fr/Le-groupe-Capgemini-lance-une,20150212,50774.html
(35) http://www.info-afrique.com/5336-en-afrique-communication-digitale/

(36) http://www.lesechos.fr/idees-debats/cercle/cercle-135717-comment-les-entreprises-doivent-elles-se-premunir-des-nouvelles-cyberattaques-1137238.php

Utilisation des repères : Un repère (D2-S3) indiquera qu'il fait référence à la (D)ate de mise à jour n°2 et à la (S)ource n°3 soit dans notre document, une mise à jour de notre document le 27/03/2014 et la référence https://www.symantec-wss.com/fr/cybercrime4/int/thanks#.Uyr10rK9KSP

Cet article vous à plu ? Laissez-nous un commentaire (notre source d'encouragements et de progrès)

Cyclisme et vol de données – la cyber-criminalité appliquée au sport | Le Net Expert Informatique

Le Tour de France 2015 va-t-il connaître son premier cyber scandale ? C'est en tout cas ce que l'on peut supposer après la divulgation de certaines données de performances du cycliste Crhis Froome qui ont été dérobées, estime Tanguy de Coatpont, directeur général France & Afrique du nord de Kaspersky Lab qui partage son analyse.

« Depuis plusieurs années, le sport connaît un engouement croissant auprès des publicitaires et des entreprises qui y investissent massivement, attirant par conséquent des cybercriminels poussés par l'appât du gain ou une volonté de nuire. Il n'est également pas difficile d'imaginer les conséquences psychologiques que peut avoir un vol de données sur un athlète dont le succès repose en partie sur sa concentration.
Les rumeurs concernant le possible piratage des données sportives de Chris Froome viennent nous rappeler que de nombreux aspects de la vie moderne, y compris le sport de haut niveau, sont de plus en plus connectés. Il y a quelques années, l'idée que les données d'un coureur du Tour de France soient dérobées aurait semblée anecdotique mais avec l'avancée des technologies et l'émergence des solutions d'analyse des performances qui sont aujourd'hui critiques à l'entraînement de nombreux sportifs, ce n'est plus surprenant. Ces sportifs doivent également faire face à une autre réalité : alors qu'ils sont maintenant élevés au rang de célébrités, les informations concernant leurs performances intéressent tout autant que celles qui concernent leur vie privée.
En sachant cela, tout individu ou entreprise doit prendre les mesures qui s'imposent pour protéger ses données informatiques. Même lors d'événements sportifs, où les données doivent être transmises et analysées quasiment en temps réel, il est impératif de prendre en compte les questions de sécurité informatique pour protéger les informations sensibles que sont les performances des athlètes mais également protéger les systèmes sur lesquels elles transitent.
Le partenariat entre Kaspersky Lab et l'écurie de Formule 1 de Ferrari nous a permis de mieux comprendre les défis auxquels ils sont confrontés pour sécuriser les données transmises lors des courses. Pour Ferrari, une solution de sécurité efficace est vitale afin de protéger les données qui sont une source d'information essentielle à l'équipe. Elles transitent très rapidement pour éviter d'être compromises et la solution de sécurité ne doit pas augmenter le temps de latence. Il n'est pas difficile d'imaginer que les contraintes de complexité et de performance sont similaires dans d'autres sports comme le cyclisme professionnel. »

Source : http://www.itrmanager.com/articles/157190/cyclisme-vol-donnees-cyber-criminalite-appliquee-sport.html

La mise en place de la riposte contre la cybercriminalité | Le Net Expert Informatique

La mise en place de la riposte contre la cybercriminalité

Le 08 juillet 2015, c'est-à-dire le mercredi dernier, l'Observateur permanent du Canada au Conseil de l'Europe, Alan Bowman, a déposé l'instrument de ratification de la Convention de Budapest sur la cybercriminalité, faisant ainsi de ce pays le 47ème Etat partie à ce mécanisme international de lutte contre la cybercriminalité.

Au dernier décompte, 07 autres États ont signé la Convention et 12 ont été invités à y adhérer, ce qui porte à 66 le nombre des États Parties ou qui se sont officiellement engagés à devenir Parties au traité.
« La Convention sur la cybercriminalité, aussi connue comme la Convention de Budapest sur la cybercriminalité ou Convention de Budapest, est le premier traité international qui tente d'aborder les crimes informatiques et les crimes dans Internet en harmonisant certaines lois nationales, en améliorant les techniques d'enquêtes et en augmentant la coopération entre les nations. Il a été rédigé par le Conseil de l'Europe avec la participation active d'observateurs délégués du Canada, du Japon et de la Chine.

Qu'est ce que la cybercriminalité ?
À la fin d'août 2011, plusieurs pays européens avaient signé le traité ». Selon une revue de la littérature disponible sur la question, la cybercriminalité reste encore un concept difficile à appréhender. En France, un rapport du groupe de travail interministériel sur la lutte contre la cybercriminalité datant de février 2014 appréhende la question dans toute sa complexité. Au regard de cette complexité, le rapport note que la Commission européenne a du s'en expliquer dans une communication au Parlement européen en date du 22 mai 2007 en ces termes : "Faute d'une définition communément admise de la criminalité dans le cyberespace, les termes 'cybercriminalité', 'criminalité informatique' ou 'criminalité liée à la haute technologie' sont souvent utilisés indifféremment".
La question préoccupe aussi l'OCDE selon laquelle « la cybercriminalité renvoie à tout comportement illégal contraire à l'éthique ou non autorisé qui concerne le traitement automatique de données et/ou de transmissions de données ».

Que dit l'ONU ?
Pour l'organisation mondiale, tombe sous le coup de la cybercriminalité « tout comportement illégal faisant intervenir des opérations électroniques qui visent la sécurité des systèmes informatiques et des données qu'ils traitent ». Pour autant qu'elle offre des outils juridiques susceptibles d'aider les pays à enquêter sur la criminalité informatique et de poursuivre en justice les auteurs de ce crime, la Convention de Budapest est un instrument qui mérite une large vulgarisation surtout en ces temps de guerre asymétrique à l'échelle planétaire.
C'est une simple question de bon sens quand on sait que seule la coopération entre Etats est susceptible de porter un coup d'arrêt à cette nouvelle forme de criminalité aux conséquences imprévisibles. Mais un survol rapide de la liste des Etats parties ou qui s'apprêtent à y adhérer permet de réaliser, là aussi, que l'Afrique est encore à la traine. Alors qu'on arrête de geindre si les autres réfléchissent à notre place et nous imposent leurs quatre volontés.

Source : http://malijet.com/la_societe_malienne_aujourdhui/132840-chronique-du-web-la-riposte-contre-la-cybercriminalite-se-met-en.html