L’histoire d’ « Internet de l’époque » avec Norman | Le Net Expert Informatique

L’histoire d’ « Internet de l’époque » avec Norman

Dans sa dernière vidéo l’« internet de l’époque », le célèbre Youtubeur Norman Thavaud s’amuse en chanson à comparer l’Internet d’aujourd’hui à celui des années 90 et début 2000.

Pour sa dernière création, Norman sort de son appartement et enrôle avec lui d’autres célèbres Youtubeurs (Hugo tout seul, Cyprien, Natoo…). L’idée : faire un clip musical qui compare les débuts du web à aujourd’hui.
Le clip, réalisé dans un style « rétro », évoque de nombreux souvenirs comme MSN, Skyblog,… mais aussi le rappeur Kamini, qui fait une apparition, connu pour son tube « Marly-Gomont », un tabac sur YouTube en 2006.

Lire la suite….

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://jactiv.ouest-france.fr/actualites/spotted/video-norman-retrace-lhistoire-internet-avec-humour-47604
Par Guirec FLECHER.

Kaspersky annonce être victime d’une Cyberattaque | Le Net Expert Informatique

	Kaspersky annonce être victime d’une Cyberattaque

L'éditeur de sécurité indique qu'une cyber-attaque a ciblé ses propres installations par le biais d'une nouvelle version du malware baptisé Duqu. Pour Eugene Kaspersky, le patron et fondateur de la société, cette offensive a pu être soutenue par un Etat.

Eugene Kaspersky prend la parole pour livrer les détails de l'attaque qui a visé les installations de l'éditeur de sécurité. Au cours d'une conférence de presse, le fondateur de la société a indiqué que les pirates ont utilisé une nouvelle variante d'un ver baptisé Duqu. Selon le patron de l'éditeur russe, le malware a été développé par une organisation très qualifiée, possiblement soutenue par un gouvernement étranger.
Eugene Kaspersky indique que ses équipes sont actuellement en train de rassembler l'ensemble des éléments pour comprendre l'attaque. Le responsable se veut toutefois rassurant. « Cette attaque n'a rien compromis pour nos clients mais également nos partenaires. Nous ne disposons pas encore de toutes les informations sur cette attaque mais je lance un avertissement clair, ne me hackez pas, c'est une mauvaise idée ».
L'éditeur s'est rendu compte de l'attaque grâce à une version Alpha de sa nouvelle solution censée lutter contre les menaces dites persistantes (ou APT pour advanced persistent threat). Pour Kaspersky le but des pirates était d'ailleurs d'espionner sa technologie permettant de traquer ce type de cyber-attaques.
Selon les spécialistes, Duqu est une variante de Stuxnet, un élément malveillant qui avait été utilisé pour attaquer des systèmes critiques dits SCADA. Stuxnet avait même permis d'organiser une cyber-attaque contre des installations informatiques présentes au sein d'une centrale nucléaire en Iran.
Toujours est-il qu'Eugene Kaspersky considère que le nouveau Duqu exploite plusieurs vulnérabilités 0-Day. Le fait d'être en mesure d'utiliser plusieurs failles jusqu'à présent inconnues est, selon le responsable, un élément important. Cela lui permet d'affirmer que les équipes derrière ce malware disposent non seulement de très solides connaissances techniques, mais également de soutiens « officiels » d'un gouvernement étranger.

Duqu, une nouvelle variante
Le malware Duqu avait déjà sévi en 2011. Mis en lumière par les équipes de Symantec, il était parvenu à se diffuser par le biais d'un fichier d'installation contenu dans un document Word (.doc) envoyé par e-mail. Une fois ouvert, ledit fichier exploitait une vulnérabilité du moteur d'analyse de font (TTF) Win32k TrueType et était ainsi capable d'infecter un poste informatique.
Microsoft avait par la suite été obligé de publier un patch de sécurité hors-cycle pour corriger les nouvelles vulnérabilités (0-Day) exploitées par le ver. A présent qu'une nouvelle variante du malware est détectée, la firme américaine pourrait à nouveau publier une mise à jour de sécurité pour l'ensemble de ses services.

Source : http://pro.clubic.com/it-business/securite-et-donnees/actualite-769814-kaspersky.html
Par Olivier Robillart

Modalités de recours au vote électronique pour les Entreprises | Le Net Expert Informatique

Le Juge administratif rappelle qu'en matière de vote électronique pour l'élection des délégués du personnel, des règles strictes doivent être respectées.

Aux termes du premier de l'article R2314-8 du Code du travail, « l'élection des délégués du personnel peut être réalisée par vote électronique sur le lieu de travail ou à distance ».

Les obligations de sécurité et de confidentialité que doit nécessairement présenter un système de vote électronique pour garantir la sincérité du scrutin sont fixées aux articles R2314-9 à R2314-11 du Code du travail.

En outre, l'article suivant dispose que préalablement à sa mise en place ou à toute modification de sa conception, le système de vote électronique est soumis à une expertise indépendante. Ce rapport est tenu à la disposition de la Commission nationale de l'informatique et des libertés.

Au vu de ces dispositions, il apparaît donc que si l'entreprise compte organiser des élections en son sein, et utiliser pour cela un système de vote électronique, elle doit nécessairement faire réaliser une expertise indépendante lors de la conception initiale du système utilisé, mais aussi à chaque fois qu'il est procédé à une modification de la conception de ce système, et préalablement à chaque scrutin ou le recours au vote électronique est envisagé.

A l'origine de l'arrêt soumis à l'appréciation des Juges de la plus haute juridiction de l'ordre administratif, l'un des syndicats d'une société avait saisi la Commission nationale de l'informatique et des libertés (CNIL) d'une plainte relative à l'organisation des élections professionnelles, devant se tenir un peu plus tard dans l'entreprise.

La formation restreinte de la CNIL avait alors relevé plusieurs manquements à la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Parmi les manquements constatés, citons notamment le défaut d'expertise préalable indépendante de ce système, ainsi que l'absence de confidentialité des moyens d'authentification.

Un avertissement, devant notamment être publié sur le site internet de la société, avait alors été pris à l'encontre de cette dernière.

La société en cause avait alors demandé en justice l'annulation de cette délibération.

L'affaire est finalement remontée devant le Conseil d'État, qui rappelle à cette occasion que l'utilisation d'un système de vote électronique pour une élection professionnelle est subordonnée à la réalisation préalable d'une expertise indépendante lors de la conception initiale du système utilisé, mais aussi :

- à chaque fois qu'il est procédé à une modification de la conception du système ;
- et préalablement à chaque scrutin pour lequel le recours au vote électronique est envisagé.

S'agissant des sanctions prononcées par la CNIL, le Conseil d'État précise dans sa décision que la Commission ne peut pas légalement sanctionner la simple méconnaissance de l'une des recommandations qu'elle adopte. Toutefois, elle peut en tenir compte pour apprécier le respect des dispositions législatives et réglementaires que cette recommandation vise à mettre en oeuvre, et donc prononcer une sanction.

Plus d'informations ici

[block id="24761" title="Pied de page HAUT"]

A Lire aussi :

Nouveautés dans l'organisation des votes électroniques pour les élections professionnelles
3 points à retenir pour vos élections par Vote électronique
Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique
Modalités de recours au vote électronique pour les Entreprises
L'Expert Informatique obligatoire pour valider les systèmes de vote électronique
Dispositif de vote électronique : que faire ?
La CNIL sanctionne un employeur pour défaut de sécurité du vote électronique pendant une élection professionnelle
Notre sélection d'articles sur le vote électronique

Vous souhaitez organiser des élections par voie électronique ?
Cliquez ici pour une demande de chiffrage d'Expertise

Vos expertises seront réalisées par **Denis JACOPINI** :

- Expert en Informatique **assermenté et indépendant** ;
- **spécialisé dans la sécurité** (diplômé en cybercriminalité et certifié en Analyse de risques sur les Systèmes d'Information « ISO 27005 Risk Manager ») ;
- ayant suivi la **formation délivrée par la CNIL sur le vote électronique** ;
- qui n'a **aucun accord ni intérêt financier** avec les sociétés qui créent des solution de vote électronique ;
- et possède une expérience dans l'analyse de nombreux systèmes de vote de prestataires différents.

Denis JACOPINI ainsi **respecte l'ensemble des conditions recommandées** dans la Délibération de la CNIL n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.

Son expérience dans l'expertise de systèmes de votes électroniques, son indépendance et sa qualification en sécurité Informatique (ISO 27005 et cybercriminalité) vous apporte l'assurance d'une qualité dans ses rapport d'expertises, d'une rigueur dans ses audits et d'une impartialité et neutralité dans ses positions vis à vis des solutions de votes électroniques.

Correspondant Informatique et Libertés jusqu'en mai 2018 et depuis Délégué à La Protection des Données, nous pouvons également vous accompagner dans vos démarches de mise en conformité avec le RGPD (Règlement Général sur la Protection des Données).

Contactez-nous

E-réputation et faux commentaires : les « faussaires du Web » | Le Net Expert Informatique

E-réputation et faux commentaires : les « faussaires du Web »

Un aspect de l'e-réputation (cyber-réputation, web-réputation, réputation numérique comme on voudra) de nouveau porté à l'attention du public : les faux commentaires, qui incluent notamment les faux avis de consommateurs.

Les « faussaires du Web »
Un article du Monde, en date du 31 mai sur le site du quotidien, intitulé « Faux commentaires : dans la nébuleuse des faussaires du Web », sous la plume de Morgane Tual, examine longuement ce phénomène des « commentaires truqués qui pullulent sur la toile ».
Parmi les producteurs des faux commentaires ou avis, l'article évoque les agences d'e-réputation. Il est vrai que certaines agences offrent leurs services pour publier des commentaires supposés émaner de consommateurs contents (dans le but de promouvoir un peu artificiellement une marque ou une entreprise) ou mécontents (dans le but de couler la réputation d'un concurrent ou d'un ennemi).
Si l'article évoque la condamnation d'une entreprise devant la justice française pour ce genre de pratique, il met peu en lumière le cadre légal de telles pratiques. Nous nous arrêtons sur cet aspect, en quelque sorte en complément de cet intéressant article.

Des pratiques hors-la-loi à plusieurs égards
La première pratique consiste donc à chanter les louanges d'un commerçant ou d'un prestataire. Il importe de savoir que cette pratique est strictement encadrée dans des limites légales qui sont souvent franchies allègrement par des prestataires peu soucieux de respecter le droit ou par une ignorance coupable dès lors qu'ils se posent en professionnels.

Les « pratiques commerciales trompeuses »
Il faut en effet savoir que le code de la consommation qualifie de « pratiques commerciales trompeuses » le fait de « se présenter faussement comme un consommateur » (article L.121-1, 21° du code de la consommation). Et toute pratique commerciale trompeuse constitue un délit, pénalement sanctionné par un maximum de 2 ans de prison et/ou de 300 000 € d'amende (article L.121-6 du même code).
Il s'ensuit que lorsqu'un prestataire publie un commentaire laissant penser que son auteur est un consommateur – satisfait ou mécontent, d'ailleurs – il se met hors-la-loi et encourt les peines prévues au code de la consommation. La question sera de rapporter la preuve de qui est derrière le pseudonyme qui publie l'avis. Mais il est des moyens techniques qui permettent de le faire.

La concurrence déloyale
Le seconde pratique consiste à poster des avis de prétendus consommateurs mécontents des services d'un commerçant ou prestataire. Non seulement cette pratique tombe sous le coup des pratiques commerciales trompeuses, mais comme elle nuit à un commerçant ou un prestataire, elle peut constituer selon les cas un acte de concurrence déloyale, ou un dénigrement de produits ou de services.

Un acte de concurrence déloyale
Dès l'instant que l'auteur ou le commanditaire des avis négatifs est en situation de concurrence avec l'entreprise attaquée, ces avis sont considérés comme des actes de concurrence déloyale.
Comme dans tous les pays de liberté économique, la concurrence est libre en France. Ce qui l'est moins, c'est d'user de procédés déloyaux qui s'apparentent dans ce cas à de l'abus de droit (abuser de la liberté de concurrence). La jurisprudence a ainsi forgé depuis de longues années cette notion de concurrence déloyale, bâtie sur la base des articles 1382 et suivants du code civil (responsabilité dite civile : réparation du dommage causé à un tiers par l'auteur des faits l'ayant occasionné, donc octroi de dommages-intérêts visant à indemniser le préjudice subi par la victime).

Un acte de dénigrement de produits ou de services
Il se peut que l'auteur ou le commanditaire des faux avis ne soit pas en situation de concurrence avec l'entreprise à laquelle il veut nuire. Dans ce cas, la jurisprudence, sur les mêmes bases juridiques larges, a forgé le concept de dénigrement de produits et de services, qui donc peut déboucher sur le même type de condamnation à des dommages-intérêts substantiels.

Bonnes pratiques et déontologie professionnelles
Il est tout de même des prestataires qui ont une déontologie professionnelle et qui par conséquent se refusent catégoriquement à agir en dehors du cadre légal.
C'est bien sûr le cas des Infostratèges qui excluent systématiquement ce genre de pratique, malgré les demandes de certains clients peu scrupuleux… qui ne deviennent ou ne restent pas longtemps nos clients dans ce cas.

Voir l'intéressant article de Morgane Tual sur le site du Monde :
www.lemonde.fr/pixels/article/2015/05/31/faux-commentaires-dans-la-nebuleuse-des-faussaires-du-web_4638853_4408996.html

---

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.les-infostrateges.com/actu/15062009/e-reputation-et-faux-commentaires-les-faussaires-du-web
Par Didier FROCHOT

Les attaques informatiques s'achètent sur le blackmarket | Le Net Expert Informatique

Les attaques informatiques s'achètent sur le blackmarket

De 75 dollars le million d'adresses e-mail à plusieurs milliers de dollars pour une faille zero day exploitable… G Data a plongé dans le « blackmarket » pour en ressortir les principaux tarifs du marché de la cybercriminalité.

G Data s'est penché sur le marché de la cybercriminalité pour en étudier fonctionnement et offres de contenus. Baptisé « blackmarket », cet environnement construit autour de sites spécialisés, de forums privés, de structures d'anonymisation (proxy, VPN anonymes, réseau Tor…), de messageries protégées, de serveurs bulletproof (peu regardants sur la nature des fichiers stockés), de moteurs de recherche spécialisés et autres places de marchés de produits illicites, permet d'accéder à des montagnes de données personnelles, des kits de piratages en tout genre et de services d'attaques à la demande.
Au bout de son plongeon dans le blackmarket, les experts du SecurityLabs de l'éditeur allemand spécialisé en solutions de sécurité en a ressorti quelques informations éclairantes sur la vitalité du marché de la cybercriminalité. Un marché dont les tarifs évoluent entre une poignée de dollars et plusieurs centaines. La vente de données personnelles illégalement collectées se situe dans la zone basse des tarifs et, surtout, se commercialisent en volumes. Ainsi les accès aux comptes e-mails (adresse, nom d'utilisateur et mot de passe) se négocient 5 dollars le lot de 10 000. Les seules adresses e-mails, celles que se font notamment dérober les opérateurs et qui seront essentiellement exploitées pour des campagnes de phishing, ne se revendent pas plus de 10 dollars par poignées de 100 000, autour de 75 dollars le million. Les profils numériques qualifiés sont, eux, d'autant plus rentables qu'ils se revendent à l'unité : autour de 50 dollars pour une carte bancaire valide de type Gold ou Premier, un compte bancaire ou Paypal; 70 dollars l'identité complète dite Fullz (nom, prénom, adresse postale, données de cartes bancaires, comptes email, comptes bancaires).

Plusieurs milliers de dollars la faille zero day exploitable
Les cybercriminels financièrement plus ambitieux orienteront leurs activités vers la vente de produits et services. L'installation d'un Bot, bien utile pour prendre le contrôle d'un réseau de PC infectés, se négocie autour de 50 dollars les 1000 machines à la soldes des cyberattaquants. Lesquels pourront également exploiter ces Bots pour organiser des attaques par déni de service distribué (DDoS). Un service proposé entre 10 et 200 dollars l'heure d'attaque. Le tarif pour une campagne de spam, non traçable (via un service de diffusion hébergé sur un serveur bulletproof) tombe en revanche autour de 5 dollars les 20 000 envois.
La création et l'hébergement (sur un serveur piraté) d'une page web infectieuse dans le cadre d'une campagne d'hameçonnage (phishing) se facture entre 10 et 30 dollars. Mais on trouve également des outils d'attaques plus onéreux (car censés être plus efficaces). Par exemple, le kit d'exploitation Nuclear, qui exploite les bannières publicitaires Google Ads pour dérouter l'utilisateur vers un site infectieux, est disponible autour de 1500 dollars. La palme revient aux outils capables d'exploiter les failles zero day de Windows à raison de plusieurs milliers, voire plusieurs dizaines de milliers de dollars, selon G Data.

Source : http://www.silicon.fr/besoin-dune-attaque-ddos-comptez-entre-10-200-dollars-de-lheure-118545.html
Par Christophe Lagane

Les hébergeurs Français inquiets du projet de loi renseignement | Le Net Expert Informatique

Le projet de loi sur le renseignement, adopté par le Sénat mardi 9 juin, pourrait mettre en péril la compétitivité des hébergeurs français, alors que le marché est en pleine croissance.

Le Sénat à voté mardi 9 juin, le projet de loi sur le renseignement, présenté par le gouvernement au nom de la lutte contre le terrorisme. 251 sénateurs, en majorité à droite mais aussi à gauche, ont voté pour, 68 contre, et les autres se sont abstenus. Cette loi controversée permettrait à l'État d'« imposer aux opérateurs la mise en œuvre sur leurs réseaux d'un dispositif destiné à détecter une menace terroriste sur la base de traitements automatisés » (Art. L. 851-4).
Ces « boites noires », comme les appellent les opposants, filtreront les données qui circulent à l'aide d'un algorithme validé par une commission composée de parlementaires, de juristes et d'experts. Les services de renseignement collecteront alors des métadonnées donnant la possibilité de traquer toutes les activités de n'importe quel internaute.

L'objectif affiché par le gouvernement est de pouvoir détecter plus efficacement toute menace terroriste. Les services de renseignement pourront par exemple détecter les connexions à un site internet terroriste, ou capter les communications vers des pays jugés sensibles.
Personne ne conteste le besoin d'une surveillance accrue des réseaux. Mais cette loi ne fait cependant pas l'unanimité. Les premiers à se sentir lésés sont les hébergeurs français. Après avoir attiré, pendant tout ce temps, des clients en leur expliquant qu'en France leurs données resteraient confidentielles et ne risquaient pas d'être interceptées, voilà que l'État s'octroie un libre accès à leurs réseaux et à tout ce qui y circule.
Certains menacent maintenant, dans un communiqué destiné au Premier ministre, de délocaliser leurs infrastructures dans des pays moins intrusifs, en amenant avec eux emplois et vecteurs de croissance économique, dénonçant les risques que cette loi peut apporter à leur industrie.

Vers des délocalisations massives ?
Outre le scepticisme autour de la capacité de l'État à traiter et analyser une quantité massive de données, le débat sur le caractère liberticide de cette loi et les risques d'abus, de dérives et de fuites qui pourrait avoir lieu, les craintes qu'ont les hébergeurs concernent en grande partie la réaction qu'auront leurs clients face à ces mesures.
En effet, ils jugent que « les entreprises et les particuliers choisissent un hébergeur sur des critères de confiance et de transparence qu'il ne sera plus possible de respecter ». Un grand travail a été fait pour rassurer le grand public, ainsi que les entreprises, sur la confidentialité des données hébergées dans des datacenters français, car il s'agit bien ici d'un avantage compétitif primordial qu'ont les hébergeurs locaux face aux grands acteurs américains du cloud, qui est menacé aujourd'hui.
Dans leur communiqué, ces six hébergeurs français affirment que 30 à 40 % de leurs clients sont étrangers et ont choisi la France pour l'importance accordée à la protection des données. Ils rappellent aussi qu' « il leur faudra entre 10 minutes et quelques jours pour quitter leur hébergeur français » et migrer dans un pays où les garanties de confidentialité pour les clients seront plus importantes.
Les hébergeurs français seraient donc face au même phénomène qu'ont connu leurs homologues américains lors de la mise en place aux États-Unis du Patriot Act. Face à la comparaison inévitable faite entre ces deux lois, Matignon se défend en rappelant que le gouvernement ne met pas en place un dispositif de surveillance massif des données sur Internet ou des conversations privées comme c'est le cas aux États-Unis, et assure vouloir éviter tout abus ou dérive en créant une commission de contrôle indépendante, appelée CNTCR, qui devra toujours donner son avis préalable à la mise en œuvre de la technique de renseignement et pourra exercer un contrôle a posteriori.
Nous parlons bien d'un marché avec une croissance à deux chiffres (+20 % en 2014) qui risque de prendre du plomb dans l'aile. En plus des hébergeurs français qui risquent de retirer certains investissements de France, j'imagine facilement de grands acteurs européens ou mondiaux choisir de s'implanter ailleurs qu'en France par souci de confidentialité des données.
On pourrait penser à terme que les petits hébergeurs seraient bloqués dans une situation où leurs clients voudraient migrer, mais en réalité ils pourront toujours louer des mètres carrés à l'étranger en fonction des demandes.
En résumé, les pure players pourront plus ou moins s'adapter face à un éventuel exode de leurs clients. Le grand perdant de cette histoire semble être donc pour moi être l'économie numérique française.

Le temps de l'optimisation légal
Autour de toutes ces discussions, je vois bien la confidentialité d'accès aux données représenter une nouvelle opportunité commerciale pour les hébergeurs qui proposeront à leurs clients de géolocaliser leurs données en fonction de la législation locale. Ils vont devoir proposer la solution qui garantit au mieux la confidentialité d'accès aux données pour gagner quelques affaires.
Les acteurs européens par exemple, donnent depuis toujours la possibilité à leurs clients français et européens de choisir dans quels pays héberger leurs données avec des datacenters répartis dans toute l'Europe afin d'optimiser au mieux leurs besoins en confidentialité, sécurité et respect des règles et lois locales.
En somme, cette loi pénalise les acteurs franco-français en réduisant leurs marges de manœuvre du fait des contraintes imposées par l'État et met en péril leur compétitivité en tant qu'acteur national en les mettant au même niveau que les autres acteurs internationaux.
Il serait peut-être plus judicieux aujourd'hui d'établir un partenariat gagnant-gagnant entre l'État français et les hébergeurs locaux qui se disent tous prêts à collaborer pour assurer la sécurité sur le territoire, en mettant en place une infrastructure règlementaire moins disproportionnée et plus ciblée sur les objectifs de l'État en évitant de la même manière de mettre en péril leur avantage sur le sol français.

Source : http://www.lesechos.fr/idees-debats/cercle/cercle-133763-loi-sur-le-renseignement-quel-avenir-pour-les-hebergeurs-1126557.php
Par France Weill / Director IT & Cloud Services Channels Europe – COLT

Interdictions de stade : le PSG à nouveau épinglé par la CNIL | Le Net Expert Informatique

Interdictions de stade : le PSG à nouveau épinglé par la CNIL

Le Paris-Saint-Germain (PSG) est à nouveau épinglé dans le traitement de certains de ses supporteurs. La Commission nationale de l'informatique et des libertés (CNIL) a publié, mercredi 10 juin, un communiqué officiel pour signifier une nouvelle mise en demeure à l'encontre du club de football de la capitale. Il s'agit de la deuxième procédure de ce type en deux ans.

La Commission, chargée de sanctionner les manquements à la loi informatique et libertés, reproche aux dirigeants du club francilien de ne pas s'être « borné à gérer la liste des interdits de stade à l'intérieur du cadre légal, mais d'avoir décidé d'exclure les personnes faisant l'objet de ces mesures, après l'expiration de celles-ci, pendant une durée au moins équivalente ».

Pas de sanctions pour l'instant

La CNIL pointe notamment l'interdiction de stades de certains supporteurs parisiens, ainsi que la conservation de données personnelles au-delà du délai de l'interdiction. Or, seuls le préfet ou le juge peuvent prendre, ou étendre, des mesures d'interdiction de stade.

Dans son communiqué, la CNIL rappelle que cette mise en demeure n'est pas synonyme de sanction. « Aucune suite ne sera donnée à cette procédure si la société [le PSG] se conforme à la loi dans le délai imparti d'un mois », peut-on lire. Dans le cas contraire, l'organisme de défense des libertés individuelles et publiques pourrait nommer un rapporteur qui sera chargé de proposer une sanction à l'égard du champion de France en titre.

En janvier 2014, la CNIL avait autorisé le club dirigé par Nasser Al-Khelaïfi à créer un fichier afin de lister les supporteurs exclus du stade par les autorités selon des motifs bien précis comme « l'existence d'un impayé, le non-respect des règles de billetterie, l'activité commerciale dans l'enceinte sportive en violation des conditions générales de ventes, etc. », précise le communiqué.

.

Source : http://www.lemonde.fr/ligue-1/article/2015/06/10/interdictions-de-stade-le-psg-a-nouveau-epingle-par-la-cnil_4651214_1616940.html
Par Kozi Pastakia

Conférence Octopus 2015 sur la cybercriminalité : Le

Conseil de l’Europe se penche sur l’accès de la justice aux données | Le Net Expert Informatique

Conférence Octopus 2015 sur la cybercriminalité : Le Conseil de l’Europe se penche sur l’accès de la justice aux données

Comment assurer l'accès aux données, enquêter efficacement sur les infractions commises par le biais d'Internet et engager des poursuites à l'encontre de leurs auteurs lorsque les éléments de preuve se trouvent dans le « cloud » ? Du 17 au 19 juin, le Conseil de l'Europe réunira des experts du monde entier, des responsables gouvernementaux, des fonctionnaires de police et des professionnels d'internet en vue de renforcer la coopération internationale pour lutter contre la cybercriminalité.

Cette conférence portera également sur les défis liés à la protection des enfants contre leur sollicitation en ligne à des fins sexuelles (« grooming ») et sur la radicalisation sur internet.
Les 300 participants examineront, dans le cadre d'une série d'ateliers partiellement ouverts à la presse, les questions suivantes :

– Le renforcement des capacités en matière de cybercriminalité: bonnes pratiques et futurs programmes (*)
– Les preuves électroniques : accès de la justice pénale aux données
– Les victimes de la cybercriminalité: qui s'en soucie ? (*)
– La législation en matière de cybercriminalité et la mise en œuvre de la Convention de Budapest
– La coopération internationale: améliorer le fonctionnement des points de contact accessibles 24 heures sur 24 et sept jours sur sept
– Les modes opératoires normalisés pour le traitement des preuves électroniques
– Les politiques, activités et initiatives adoptées en matière de cybercriminalité par les organisations internationales et les organisations du secteur privé
– La radicalisation sur internet : le point de vue de la justice pénale
– La protection des enfants contre la violence sexuelle en ligne
Les discussions s'appuieront notamment sur un rapport publié récemment et qui se penche sur les difficultés des autorités pénales à obtenir des preuves électroniques.
La conférence sera ouverte notamment par le Secrétaire Général du Conseil de l'Europe, Thorbjørn Jagland, la Représentante Spéciale du Secrétaire Général des Nations Unies sur la violence à l'encontre des enfants, Marta Santos Pais, et le Préfet chargé de la lutte contre les cybermenaces (France), Jean-Yves Latournerie.

Contexte
La Convention sur la cybercriminalité (« Convention de Budapest ») est le seul traité international juridiquement contraignant dans ce domaine. Elle a eu des répercussions dans le monde entier, où elle a conduit au renforcement et à une plus grande harmonisation de la législation relative à la cybercriminalité.
Depuis 2001, 66 pays ont signé, ratifié ou ont été invités à adhérer à la Convention. Plus de 120 pays coopèrent avec le Conseil de l'Europe au renforcement de leur législation et de leur capacité de lutte contre la cybercriminalité.
Programme – Fiche d'information – Encore plus d'information
Lien vers la retransmission (17 juin de 9h à 12h30 dans l'hémicycle et discussions en salle 1) #octopus2015

Trois tendances de sécurité

informatique à retenir pour 2015 | Le Net Expert Informatique

Trois tendances de sécurité informatique à retenir pour 2015

De nombreuses études placent la sécurité au cœur des TI pour 2015. Retrouvez ci-dessous trois tendances à retenir pour cette année :

Les attaques seront inévitables!
La question n'est plus de se demander si on sera attaqué et quand, mais plutôt de se préparer aux impacts d'une attaque, car cette attaque arrivera de toute façon.
Il faut donc avant tout s'assurer de minimiser les impacts d'une attaque potentielle et être proactif. Pour faire face à ces nombreuses tentatives d'attaques, les organisations doivent mettre en place un SOC (pour Security Operations Manager en anglais) ou du moins constituer des ressources qui vont gérer les opérations de sécurité quotidiennement et en temps réel.
Ces ressources vont être aidées dans leur travail par des outils innovateurs, mais doivent s'appuyer sur une expertise poussée pour analyser la masse d'activités. Par exemple, il ne suffit pas d'avoir un SIEM, mais il faut savoir le gérer.

Impartir sa sécurité
Puisque les attaques sont de plus en plus sophistiquées, l'expertise demandée par les ressources opérationnelles est de plus en plus poussée.
De plus, le temps à consacrer aux activités quotidiennes augmente de manière significative. Il est donc plus logique de faire appel à un fournisseur externe pour assurer ces activités afin que les ressources de l'organisation puissent se consacrer à la portion stratégique de la sécurité.
L'année 2015 verra de plus en plus d'impartition des opérations de sécurité sur la base du mode sécurité à la demande (SaaS).

Priorité à la sécurité applicative
Les réseaux sont de plus en plus protégés, car le cœur de l'infrastructure des organisations est sécurisé grâce aux nombreuses années d'évolution à ce sujet.
Par définition, les attaques ciblent toujours les points faibles d'une organisation et dans bien des cas, les applications Web sont les plus vulnérables : code non sécuritaire, failles non corrigées, mises à jour non appliquées… De nombreuses raisons peuvent s'ajouter à la liste.
Or, les applications Web représentent l'image de l'organisation et constituent bien souvent un accès privilégié aux données sensibles. La protection ciblée des applications Web sera mise de l'avant en 2015.

Source : http://www.directioninformatique.com/blogue/securite-informatique-trois-tendances-2015/36154
Par Matthieu Demoor

Démantèlement d’un réseau de cybercriminalité bancaire-Europol | Le Net Expert Informatique

Démantèlement d’un réseau de cybercriminalité bancaire-Europol

Europol a annoncé mercredi l'arrestation de 49 personnes soupçonnées d'appartenir à un groupe de cybercriminels actifs dans plusieurs pays d'Europe qui auraient dérobé plusieurs millions d'euros sur des comptes bancaires européens. Les présumés coupables agissaient en Belgique, Espagne, Italie, Pologne et Royaume-Uni ainsi qu'en Géorgie, précise dans un communiqué l'agence de police européenne basée à La Haye.

Des perquisitions ont eu lieu dans 58 lieux différents. Des ordinateurs, des téléphones et divers documents ont été saisis.

Les arrestations ont eu lieu mardi.
« Les enquêtes menées en parallèle ont révélé une fraude d'ampleur internationale d'un montant total de six millions d'euros accumulés sur une très courte période », lit-on dans le communiqué.
Les suspects, principalement originaires du Nigeria, du Cameroun et d'Espagne, transféraient leurs « profits illicites » hors de l'Union européenne via un réseau sophistiqué de transactions visant au blanchiment de l'argent, précise le communiqué d'Europol.

Lire la suite….

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.boursorama.com/actualites/demantelement-d-un-reseau-de-cybercriminalite-bancaire-europol-ce20264eef326a073c96c7b8763fdd9a
Par Anthony Deutsch; Danielle Rouquié pour le service français