Votre box pourrait bien être utilisée pour des piratages d’envergure…

	Votre box pourrait bien être utilisée pour des piratages d’envergure…

Le groupe LizardSquad, qui a notamment orchestré les attaques Ddos sur le PSN et Xbox Live à Noël, a dévoilé peu de temps après une offre payante offrant des attaques par déni de service à la demande. Un « service » qui repose essentiellement sur des routeurs privés mal sécurisés.

Le 25 décembre, le groupe LizardSquad lançait une attaque Ddos contre les services en ligne du Playstation Network et du Xbox Live. Dieu merci (ou pas) Kim Dotcom est venu à la rescousse des utilisateurs et tout est rapidement rentré dans l'ordre. Mais peu de temps après, LizardSquad lançait une offre de Ddos payante à la demande, expliquant que ses récentes attaques largement relayées dans la presse n'étaient en fait qu'une opération de communication visant à faire preuve de l'efficacité de leurs techniques.

Business is business, as usual

L'offre présentée par LizardSquad vous permet, contre espèces sonnantes et trébuchantes (mais ils acceptent aussi les bitcoins) de lancer une attaque Ddos sur la cible de votre choix. Le tout sans avoir à s'embarrasser des aspects techniques : le groupe de pirates se charge de tout, vous offrant ainsi un service clef en main pour mettre des bâtons dans les roues de vos concurrents, ennemis, amis, bref, à peu près tout ce qui est en mesure de proposer un service en ligne et qui vous dérange. Officiellement, l'outil LizardStresser est avant tout pensé pour les utilisateurs souhaitant tester la robustesse de leurs services face à une attaque Ddos.

Un exemple des prix pratiqués par LizardSquad (Crédit original de l'image : The Register)

Le journaliste Brian Krebs, spécialisé dans la cybersecurité, s'est lancé dans une petite croisade contre ce groupe de pirate. Il avait dans un précédent article entrepris de révéler l'identité de certains d'entre eux et n'hésitent pas à les qualifier de « script kiddies », un terme péjoratif qui désigne les débutants sans connaissances réelles qui récupèrent et utilisent des programmes clef en main pour s'attaquer à des sites web ou des internautes. De part et d'autre, les insultes volent, LizardSquad n'hésitant pas à affirmer que leurs serveurs sont hébergés « quelque part sur le front de Brian Krebs »

Brian Krebs s'est penché sur les méthodes utilisées par le groupe pour mener à bien leurs attaques Ddos. En effet, plusieurs options sont disponibles pour parvenir un tel résultat : certain ont recours à des botnets, Anonymous de son coté s'était fait remarquer pour l'utilisation du soft LOIC qui transformait ses utilisateurs en « botnet consentant » et d'autres méthodes reposant sur l'exploitation de failles de sécurité sont également utilisées (On pense notamment à la technique de l'amplification DNS)

Routeurs domestique : l'ennemi intérieur ?

LizardSquad dispose lui aussi de son propre réseau Botnet pour mener à bien ses attaques, explique Brian Krebs, mais celui-ci est essentiellement constitué de routeurs domestiques. L'auteur explique être parvenu, avec l'aide de chercheurs non cités, à mettre la main sur le malware utilisé par LizardSquad. Celui-ci est une version modifiée d'un trojan signalé auparavant par la firme russe Dr.Web.

Krebs remarque que ce malware a pour fonctionnalité de scanner l'ensemble du réseau afin de trouver les routeurs ayant gardé leurs paramètres d'usine. En effet, la plupart des utilisateurs négligent la sécurité de leurs routeurs wifi, et si les mots de passe configurés en usine n'ont pas été changés, accéder à l'interface n'a rien de compliqué.

Le malware n'est pas spécifique aux routeurs domestiques, explique Krebs, il est conçu avant tout pour s'attaquer aux machines utilisant Linux. Le journaliste explique que les routeurs domestiques constituent la majeure partie du botnet de LizardSquad, mais que les routeurs de certaines universités et entreprises sont probablement infectés.

Si vous craignez que votre paisible routeur domestique ne soit en réalité un agent double à la solde de LizardSquad, Krebs détaille également dans la suite de son article les techniques de base permettant de sécuriser l'accès à son routeur. La plus simple et la plus efficace reste néanmoins la plus évidente : changer ses mots de passe.

L'article de Brian Krebs :
http://krebsonsecurity.com/2015/01/lizard-stresser-runs-on-hacked-home-routers/#more-29431

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

Source :
http://www.zdnet.fr/actualites/lizardsquad-devoile-un-service-de-ddos-a-la-demande-qui-s-appuie-sur-les-routeurs-39812835.htm
Par Louis Adam

Alerte au phishing sur LinkedIn

Alerte au phishing sur LinkedIn

L'éditeur de sécurité Symantec a lancé une alerte à propos de mails de phishing ciblant les utilisateurs du réseau social LinkedIn. Ce mail frauduleux contient une pièce jointe à ne surtout pas ouvrir.

Satnam Narang, manager sécurité chez Symantec, a lancé une alerte sur la multiplication de mails de phishing visant les utilisateurs de LinkedIn. Dans un billet, ce dernier explique avoir observé un accroissement de mails prétendument envoyés par le service support du réseau social professionnel. En fait, il n'en est rien : il s'agit bien de mails frauduleux tentant de tromper les utilisateurs qui pourraient être tentés de suivre les recommandations indiquées dans ce message.

« En raison d'activités irrégulières, votre compte LinkedIn a fait l'objet d'une mise à jour de sécurité obligatoire. Parfois, LinkedIn rejette les identifiants dans les cas où nous pensons que le compte pourrait avoir été compromis. Pour ce faire, nous avons développé une nouvelle façon de garder votre compte sûr et attaché à ce mail un formulaire pour achever ce processus. Merci de le télécharger et de suivre les instructions sur votre écran » peut-on lire dans le mail de phishing.

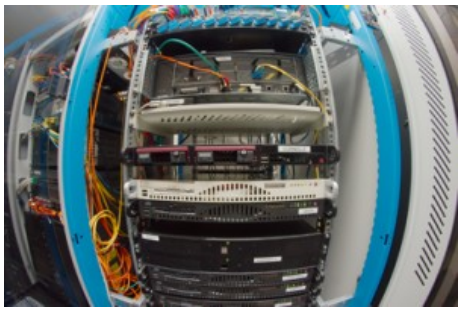
Celui-ci est écrit de façon tout à fait correcte et peut donc piéger d'autant plus facilement l'utilisateur.
En cliquant sur le formulaire, une copie du véritable site, dont la source a été modifiée, s'affiche invitant l'utilisateur à se connecter avec ses identifiants. *« La méthode utilisée permet de contourner les listes noires du navigateur qui souvent détectent les sites web suspicieux pour prévenir les utilisateurs qu'ils sont victimes de phishing […] Les utilisateurs devraient envisager d'activer l'authentification à double facteur qui est la véritable mise à jour de sécurité […] »*, a prévenu Satnam Narang

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

Source : http://www.lemondeinformatique.fr/actualites/lire-alerte-au-phishing-sur-linkedin-59912.html?utm_source=mail&utm_medium=email&utm_campaign=Newsletter
Par Dominique Filippone

Assurer la sécurité

informatique et la sauvegarde des données

	**Assurer la sécurité informatique et la sauvegarde des données**

Cyber-attaques, vols ou incendies… Garantir la protection des données numériques, notamment à caractère personnel, devrait être une priorité pour les collectivités.

Insultes à l'encontre de la France mais aussi des États-Unis et d'Israël : le 24 janvier 2023, au lieu d'accéder au site internet de la ville de Fruges (62), c'est ce type de message que les internautes découvrent. Plus tôt dans le mois, c'est le site de l'office de tourisme du Sancerrois qui était victime d'un piratage entraînant la suppression de l'agenda des animations et un surcroît de travail pour les agents.
« Partout en France les collectivités, insuffisamment protégées, sont visées par des cyber-attaques. Or elles les décrédibilisent et peuvent avoir des conséquences très graves », constate le commandant Rémy Février, ancien chargé de mission intelligence économique à la région de gendarmerie Nord-Pas-de-Calais(1). Selon lui, la commune est l'échelon territorial le plus fragile, détenant beaucoup de données sensibles avec de faibles moyens de protection.

Courriels contaminés
Les sites internet sont souvent une voie royale pour les hackers. « Si l'arborescence n'a pas été verrouillée, il est facile de remonter à l'ensemble du système d'information et d'accéder aux fichiers et aux mots de passe », met en garde Rémy Février. Les pirates peuvent aussi prendre le contrôle d'ordinateurs via des virus « troyens » contractés par des courriels ou des sites web contaminés.
« La récupération illicite d'informations est un enjeu majeur de nature à induire des répercussions civiles et pénales pour les élus locaux. Les vols de données à caractère personnel peuvent par exemple conduire à des vols d'identité », prévient le « cyber-gendarme » qui déplore le manque de statistiques fiables sur ces sujets.

Plan de continuité
Avec le développement de l'e-démocratie, de l'e-administration ou de la dématérialisation des appels d'offres, le « cyber-risque » est multiplié. « Qu'est ce qui empêchera demain une entreprise d'aller voir frauduleusement l'offre de ses concurrents ? » s'interroge Rémy Février.
En dehors de la malveillance, la simple sécurisation des données numériques est problématique. Incendie, inondation, explosions, vols… « Je recueille beaucoup de témoignages d'élus ayant perdu tout ou partie de leurs données », constate Maurice de Bosscher, responsable technique au centre de gestion du Nord.
« Pour une remise en route rapide en cas de sinistre, il est impératif de posséder des sauvegardes hors site. La collectivité doit prévoir un plan de continuité d'activité englobant ses systèmes d'information. C'est encore trop peu souvent le cas », insiste Rémy Février.

Trois conseils

Développer une culture de la sécurité
« Le bon sens prévient 80 % des problèmes : ne laissons pas le mot de passe visible, vidons de leurs données les ordinateurs avant de s'en débarrasser », dit Rémy Février, chargé de mission intelligence économique. Il s'agit de créer une culture de la sécurité des systèmes d'information à tous les niveaux et de former le personnel, avec des élus moteurs.
Dans chaque collectivité, un correspondant responsable de la sécurisation du réseau à intérêt de se rapprocher des services de l'État pour bénéficier d'informations récentes et de formations spécifiques. Il peut aussi trouver appui auprès de l'Agence nationale de la sécurité des systèmes d'information (Anssi).
« On ne peut faire l'économie d'une charte définissant le bon usage des systèmes d'information, ce qu'il est possible ou non de faire, et cependant 90% des communes n'en possèdent toujours pas, assure en outre Hervé Fortin, responsable sécurité des systèmes d'information du conseil général (CG) de l'Aisne qui conseille d'intégrer dans le plan de sécurisation les recommandations du référentiel général de sécurité (RGS) et de la Cnil.

Connaître son parc et sécuriser l'intégrance
Un schéma directeur informatique recensant matériel et câblages permet une remise en route rapide. « Sans cela, un simple dysfonctionnement peut prendre des proportions fâcheuses », explique Rémy Février. Choisir de faire suivre son matériel en intégrance implique d'obtenir un maximum de garanties sur la sécurité offerte par le prestataire, avec clauses de confidentialité et vérification de la qualité du service.
« Il est utile de s'appuyer sur les services des renseignements généraux pour bénéficier de leurs connaissances », conseille Johane Protin, responsable sécurité des systèmes d'information du conseil général des Hauts-de-Seine.

Sécuriser les postes nomades
« Les outils nomades multiplient les risques de vols et de pertes de données. Il est préférable d'équiper les collaborateurs de terminaux fournis par la collectivité et de les former au risque », conseille Hervé Fortin.
Des outils facilitent la sécurité : chiffrement des données ou une clef USB de type ID. Outre d'un mot de passe, elle contient les applications nécessaires et crée sur le disque dur de l'ordinateur d'accueil une zone mémoire temporaire sécurisée sur laquelle il ne reste aucune trace une fois la clef ôtée.

Systèmes d'information : la responsabilité pénale des élus
Avoir insuffisamment protégé ses systèmes d'information peut entraîner la mise en examen des élus responsables.
Les élus peuvent par exemple être mis en cause si des sites illégaux sont consultés alors qu'aucune mesure de restriction d'accès à internet n'a été mise en place. « La réglementation dans ce domaine est jurisprudentielle et il ressort clairement de cette jurisprudence qu'un élu, au même titre qu'un chef d'entreprise, peut être mis en examen pour ne pas s'être suffisamment protégé », met en garde Rémy Février, chargé de mission intelligence économique, qui estime que la majorité des élus ne connaissent pas les responsabilités qui leur incombent.
« Même si l'élu délègue un responsable sécurité des systèmes d'informations, la responsabilité de protéger les données, notamment celles à caractères personnelles, reste au final de son ressort », insiste-t-il.
Au-delà de ces aspects juridiques, les élus ont la responsabilité de protéger la nouvelle valeur publique qu'est la « cyber-confiance ».
« Il existe une responsabilité collégiale des élus en cas de rupture des activités numériques ; la plupart n'en sont pas conscients », estime Richard Ekiewski, le conseiller communautaire délégué à la prévention des risques de Lille métropole.

Centre de gestion du Nord : un coup de pouce pour les petites collectivités
Ordinateur infecté par des virus troyens, PC volés ou endommagés par une inondation. Nous constatons tous les jours que les communes ne sont pas assez protégées », explique Maurice de Bosscher, responsable technique de Creatic.
Le centre de ressources du centre de gestion (CDG) du Nord, créé en 2000, épaule les collectivités en matière de nouvelles technologies de l'information et de la communication. « Nous avons créé une plate-forme d'échange pour faciliter la dématérialisation. Pour qu'elle fonctionne de façon sécurisée, il faut auparavant résoudre les problèmes de sécurité de base », constate Maurice de Bosscher, ajoutant que dans le département, plus de 500 collectivités n'ont pas de responsable informatique.

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

Source : http://www.courrierdesmaires.fr/61602/dossier-la-securite-informatique-et-la-sauvegarde-des-donnees/

Le fichage des passagers heurte les libertés individuelles

	Le fichage des passagers heurte les libertés individuelles – Politis

Ce procédé de récupération de données personnelles par le biais des compagnies aériennes était, jusqu'à présent, rejeté par le Parlement européen, pour incompatibilité avec la Charte européenne des droits fondamentaux.

Dimanche 11 janvier, réunion de crise à Paris. Bernard Cazeneuve a réuni ses homologues européens pour évoquer les attentats qui ont frappé la capitale quelques jours auparavant. Le but : prendre des mesures pour renforcer la lutte contre le terrorisme. Très vite, le Passenger Name Record (PNR) se retrouve sur les lèvres des politiques et s'affirme comme étant une des réponses à apporter pour renforcer la lutte anti-terroriste.

L'idée est reprise officiellement mardi à la tribune de l'Assemblée nationale par Manuel Valls. Le Premier ministre, s'engage à la mettre en place en France rapidement et y « appelle, de manière solennelle, (…) le Parlement européen à prendre enfin, toute la mesure de ces enjeux et à adopter ce dispositif, comme nous le demandons depuis deux ans ». Ainsi, la France réclame que le Parlement européen « débloque » le PNR afin qu'il puisse entrer en vigueur sur tout le territoire européen.
Qu'est-ce que le PNR ? Il s'agit en fait des données personnelles concernant un passager d'une compagnie aérienne. Ces données regroupent, d'après le texte officiel, les dates du voyage, l'itinéraire, les informations figurant sur le billet, les coordonnées du passager, le nom de l'agent de voyage auprès duquel le vol a été réservé, le moyen de paiement utilisé, le numéro du siège et des données relatives aux bagages.

La récupération de ces données constitue un manquement certain à la protection de la vie privée et des données personnelles. La conservation des données, leurs potentielles transmission à d'autres organes que les départements de sécurité et enfin, l'incompatibilité globale du PNR avec la Charte européenne des droits fondamentaux ont amenés le Parlement européen à rejeter la plupart des textes de type PNR.

Car le débat n'est pas nouveau. A Strasbourg, plusieurs projets de PNR ont déjà été présentés depuis une dizaine d'année. En 2004, c'était avec les États-Unis qu'il était question de créer une base de données sur les passagers.
Le texte avait était rejeté par la Cour de justice de l'Union européenne, non parce qu'il constituait une violation de la législation européenne, mais pour vice de forme. Un projet de loi similaire est à nouveau présenté au Parlement en 2011. A ce moment, et contrairement à 2004, un avis positif du Parlement est impératif pour que ce texte soit voté. A la surprise générale, il est adopté. C'est la commission des libertés civiques qui rejette finalement la directive PNR en 2013. L'année suivante, en novembre 2014, le Parlement demande que le PNR avec le Canada soit examiné par la Cour de justice européenne.
Les PNR étaient donc rejetés…jusqu'à la semaine dernière, où devant les drames qui touchèrent la capitale française, les autorités réactivent le projet. Pourtant, d'après le G29, un groupe de travail représentants les autorités indépendantes de protection des données nationales, les USA, un pays qui pratique le PNR, « n'ont jamais prouvé de façon concluante que la quantité considérable de données passagers collectée est véritablement nécessaire à la lutte contre le terrorisme et la grande criminalité ». En effet, selon Claudine Guerrier, enseignante-chercheuse en droit à l'institut des Mines Télécom, le PNR n'aurait réussi à faire intercepter que deux terroristes en dix ans.
Alors si le PNR est d'une efficacité relative, et si, comme le dit le contrôleur européen des données, Peter Hustinx, le PNR est contraire aux droits fondamentaux de l'UE, pourquoi les politiques insistent-ils aussi lourdement pour que le Parlement européen l'adopte ?
« Il faut qu'ils disent à l'opinion public qu'ils sont efficace », explique la députée européenne Front de gauche Marie-Christine Vergiat. « La question n'est pas d'être pour ou contre le terrorisme, la question est de ne pas se servir de ce prétexte pour mettre en place une surveillance généralisée. Ne pas agir au mépris des libertés publiques. »
Claudine Guerrier partage l'analyse : « C'est une mesure de facilité. Elle ne pose pas de problèmes de mise en place sur le plan juridique. Elle est quasiment prête, il n'y a qu'à prendre pour base les textes des précédents PNR qui n'ont pas aboutis. »
Mais si le Parlement européen tient bon depuis une dizaine d'années, cette fois, Marie-Christine Vergiat craint que « sous la pression de l'actualité et des Etats membres, certains eurodéputés ne changent d'avis à l'Assemblée ». Le PNR sera à l'ordre du jour du Conseil européen consacré en février à la lutte contre le terrorisme. Quoi qu'il arrive, Manuel Valls a de son côté annoncé que « la plate-forme de contrôle française sera opérationnelle dès septembre 2015 ».
Par Marie Roy

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

Source : http://www.politis.fr/PNR-Le-fichage-des-passagers,29704.html

---

Protection des données : le Cese préconise un

renforcement de l’éducation au numérique

Protection des données : le Cese préconise un renforcement de l’éducation au numérique

Dans un avis adopté à l’unanimité le 13 janvier intitulé « Données numériques : un enjeu d’éducation et de citoyenneté », le Conseil économique social et environnemental (Cese) appelle le gouvernement à déclarer l’éducation au numérique pour tous grande cause nationale 2016.

Une prise de position qui arrive en pleine actualité sur fond de terrorisme, mais aussi dans le contexte de l’affaire Prisme qui met en accusation les agences américaines du renseignement sur la surveillance des citoyens, des entreprises et des Etats. Elle relance le débat sur la question des données et des équilibres à établir entre leur bonne exploitation par tous dans une optique d’intérêt général et la protection des libertés individuelles.
Les opportunités du numérique sont considérables. La multiplication des données statistiques, des échanges collaboratifs dans le monde, a fait sensiblement progresser la recherche sur le traitement de certaines maladies. Les villes sont désormais mieux à même de gérer l’espace public, l’énergie ou la mobilité des citoyens. L’éducation bénéficie d’un immense apport de connaissances. « Mais dans le même temps, les sujets relatifs à la protection de la vie privée et le risque que ces données révèlent une partie de nous-mêmes et de notre vie privée montrent aussi qu’il y a danger », tempère Eric Peres, le rapporteur de la section de l’éducation, de la culture et de la communication du Cese qui présentait le projet d’avis en assemblée plénière.

En mettant l’accent sur ce sujet, le Cese « ne veut pas stigmatiser, mais plutôt contribuer à mieux gérer le déluge de données numériques à la fois pour en faire des opportunités d’intérêt général et aussi protéger les citoyens ».

Dans cette perspective, l’avis met l’accent sur quelques préconisations prioritaires.
L’école reste un lieu sensible à la fois « pour faire de l’information numérique un véritable outil de savoir et permettre dès le plus jeune âge d’apprendre à maîtriser l’usage des outils et aussi celui des données personnelles numériques ». Le Cese reprend pour l’essentiel des propositions déjà formulées dans d’autres instances, notamment la généralisation du brevet informatique (B2i) ou encore, dans l’enseignement supérieur, l’augmentation du volume d’heures d’informatiques dans les classes préparatoires scientifiques et le développement de formations spécialisées autour de la donnée (data scientist, data broker).

Co-régulation des données personnelles dans les villes
L’entreprise et l’administration ont aussi rôle à jouer, mais cette fois, dans la « gestion éthique des données ». En assurant des pratiques « loyales, licites, transparentes et encadrées », elles amélioreraient leur image vis à vis du public et pourraient en tirer quelque avantage. Le rôle du correspondant informatique serait sensiblement renforcé. Par ailleurs, les membres du conseil recommandent un encadrement plus strict de la gestion des données transmises par les objets connectés « en faisant de la protection un réglage par défaut ». Ils militent également « pour un droit des citoyens au silence des puces » et souhaitent la généralisation du consentement préalable de l’usager (Opt-in) pour l’exploitation des données personnelles.
Pour tout cela, une régulation normative est nécessaire. Aussi le conseil réaffirme-t-il son soutien à la sortie du projet de règlement européen sur la protection des données. Au niveau national, il préconise un renforcement de la Cnil, notamment à travers son pouvoir de sanction financière. Et il encourage aussi des voies plus originales « permettant de rendre aux individus le contrôle de l’utilisation de leurs propres données ».
A cette fin il propose la création de plateformes publiques assurant la gestion de données sensibles telles que les données de santé. Au niveau local, il suggère même la mise en place de solutions de co-régulation à travers des régies locales jouant le rôle de tiers de confiance. Elles seraient chargées de conserver et de gérer les données personnelles, utiles par exemple à l’amélioration des services d’une ville. Les citoyens accepteraient de mettre en commun leurs données dans le cadre de projets d’intérêt général, sur la base d’une gouvernance solidaire et coopérative.

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

Source : http://www.localtis.info/cs/ContentServer?pagename=Localtis/LOCActu/ArticleActualite&jid=1250268282051&cid=1250268279645
Par Philippe Parmantier / EVS

FIC 2015 : Les cybergendarmes garants de la confiance numérique

	FIC 2015 : Les cybergendarmes garants de la confiance numériqueInformatique

5 jours avant l'ouverture du Forum International de la Cybersécurité, nous avons pu rencontrer les forces de gendarmerie à la pointe de la lutte contre la cybercriminalité.

Juste avant la septième édition du FIC (les 20 et 21 janvier 2015 au Grand Palais de Lille), nous avons pu rencontrer le jeudi 8 janvier les organisateurs du salon et les équipes de cybergendarmes de Paris (Section de recherche de Paris et ses spécialistes N-Tech) et de Rosny Sous Bois (C3N).
L'occasion de faire un premier point sur les principaux enjeux de cette manifestation dédiée à la cybersécurité et les menaces les plus inquiétantes pour les entreprises comme les citoyens. Comme nous l'a expliqué le général (2s) Marc Watin-Augouard, fondateur du FIC, « cette 7e édition du FIC, lancé en 2007, attend plus de 4 000 personnes françaises et étrangères. 3 000 inscrits aujourd'hui, dont 800 utilisateurs dans les entreprises (RSSI, risques manager, directeurs juridiques…), 800 offreurs, 800 institutionnels, 300 personnes du monde académique, et 400 étrangers (britanniques, allemands…). […]
Si la dimension business du salon s'affirme, trois lignes de force sont attendues sur le salon :
• l'innovation dans les technologies de sécurité et de confiance numérique,
• les données
• la place de l'humain dans la cybersécurité ».
Comme tous les ans plusieurs ateliers seront bien sûr organisés avec notamment une démonstration technique de Thales sur une simulation de cyberattaques, et des challenges techniques avec l'Epita et Sogeti.

Le colonel Mathieu Frustié, commandant la section de recherches (SR) de Paris avec 2 de ses experts en cybercriminalité, le capitaine Gwénaël Rouillec et le major Etienne Neff.
Et comme tous les ans les politiques seront de la partie avec Bernard Cazeneuve (le ministre de l'Intérieur), Thomas de Mezière (le ministre allemand de l'Intérieur), Jean-Yves Le Drian (le ministre de la Défense) et Axelle Lemaire (secrétaire d'Etat chargé du Numérique). Rappelons enfin que le FIC est organisé par la Gendarmerie Nationale, Euratechnologies et le CEIS avec le soutien financé de la Région Nord-Pas de Calais.
Au C3N, la Gendarmerie est bien entrée dans le 21 siècle. Cette journée porte ouverte à la cybergendarmerie a également été l'occasion de parler de l'affaire Charlie Hebdo, et notamment des outils employés pour analyser les forums Internet et les réseaux sociaux. L'équipe du colonel Eric Freyssinet, responsable du C3N, utilise l'outil OsincLab développé avec Thales pour détecter et suivre des communautés et des utilisateurs afin de dresser une véritable cartographie de leurs relations (amis sur les réseaux sociaux, gens parlant de la même chose…). Suite à l'attentat contre Charlie Hebdo, de nombreux tweets manifestaient par exemple leur satisfaction #bienfaitpourcharlie. Le travail de la brigade consiste avant tout à comprendre ce qui se passe et traquer toutes les expressions d'incitation à la haine raciale. Les auteurs pouvant éventuellement être poursuivis si la Justice se saisit de l'affaire. Une équipe place Beauvau, le SRTI, effectue également une surveillance des groupuscules et identitaires sur Internet, tout comme la DGSI (Direction générale de la sécurité intérieure) qui possède des équipes spécifiques pour suivre les activistes sur les réseaux publics ou souterrains.

Le colonel Eric Freyssinet, responsable du C3N de Rosny sous Bois qui déménagera à Pontoise en juin prochain.

Nous reviendrons la semaine prochaine sur le travail de ces supergendarmes numériques qui réalisent un travail éprouvant pour anticiper les menaces, sensibiliser les entreprises et les collectivités et très souvent assurer la répression dans les affaires d'extorsion, de vols et de pédophilie. 1800 gendarmes N-Tech, c'est à dire formés aux techniques d'investigation numériques, couvrent le territoire français et collaborent avec les services de police judiciaire et de gendarmerie. A Rosny sous Bois par exemple, deux drones saisis dans le cadre d'une retentissante affaire de survols sont actuellement analysés par le laboratoire technique afin de déterminer leurs plans de vol. Nous ne pouvons pas en dire plus…


Les drones saisis dans une affaire de survol sont étudiés par les experts du C3N.

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

Source : http://www.lemondeinformatique.fr/actualites/lire-fic-2015-les-cybergendarmes-garants-de-la-confiance-numerique-59858.html
Par Serge Leblal

La Cnil lance un nouveau label sur la gestion des données

La Cnil lance un nouveau label sur la gestion des données

Face à la prolifération des données qu'une entreprise a à gérer et à la complexité réglementaire qui l'accompagne, la Cnil lance un nouveau label visant à prouver la conformité de sa gouvernance.

Garantir à ses clients que l'on est conforme aux bonnes pratiques de la Cnil en matière de gestion des données personnelles, c'est l'objet de ce nouveau label « Gouvernance Informatique et Libertés » dévoilé par la Commission. Après les labels « formation », « procédure d'audit » et « coffre-fort numérique », la Cnil veut maintenant donner au Correspondant Informatique et Libertés (Cil) un autre moyen d'améliorer la gestion.
Pour rappel, le Cil est depuis 2005 la personne intermédiaire entre une entreprise et la Cnil. Du coup, ce nouveau référentiel s'adressera forcément aux organisations possédant un tel référent (plus de 10 000 à ce jour). La création de ce nouveau label est partie du constat du régulateur que les entreprises et organismes publics avaient de plus en plus besoin « d'identifier clairement les procédures à mettre en place pour une bonne gestion des données personnelles ». Pour y prétendre, 25 exigences (.rtf) ont été définies par la Cnil.
Celles-ci sont organisées en trois thématiques : l'organisation interne liée à la protection des données, la méthode de vérification de la conformité des traitements à la loi Informatique et Libertés et la gestion des réclamations et incidents. Pour le régulateur, ce label témoignera « de la volonté de l'organisme d'innover et de traiter les données personnelles de manière responsable » et constituera donc un atour pour ses clients.

Tous les organismes, publics ou privés ayant désigné un correspondant informatique et libertés peuvent prétendre à ce label.
Téléchargez le dossier de candidature
Une fois complété, envoyez le dossier
soit par le biais du formulaire de dépôt en ligne
soit par courrier postal (CNIL, 8 rue Vivienne, CS30223, 75083 paris Cedex 02)

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

Source : http://pro.clubic.com/legislation-loi-internet/donnees-personnelles/actualite-749887-cnil-gestion-donnees-personnelles-entreprise.html

La traque de la gendarmerie sur Internet

	La traque de la gendarmerie sur Internet

Au lendemain de l'attaque de Charlie Hebdo, la presse informatique spécialisée était invitée par la gendarmerie pour mieux faire connaître ses outils et ses équipes dédiées à la lutte anticriminelle dans le Cyber espace.

Programmée de longue date, la visite des services de gendarmerie, et la rencontre avec les équipes en charge de la traque informatique, le 8 janvier, préparait le grand rendez-vous annuel de la cyber criminalité des 20 et 21 janvier, le FIC, qui s'ouvrira en effet à Lille.
La gendarmerie française en est l'un des promoteurs avec Euratechnologies et la compagnie européenne d'intelligence stratégique (CEIS), l'organisation ayant le soutien économique de la Région Nord-Pas de Calais.
Le Général Marc Watin-Augouard, l'un des créateurs du FIC (Forum International de la Cybercriminalité) se réjouissait d'ailleurs de la venue de spécialistes étrangers de nombreuses polices et de plusieurs membres des différentes cellules de recherches du cyber espace parmi les 4000 visiteurs attendus. Pour sa 7eme édition, ce sont 40 ateliers durant les deux journées du FIC qui permettront de mesurer les dernières évolutions de la lutte contre la criminalité informatique. Outre Bernard Cazeneuve, notre ministre de l'Intérieur, celui de l'Allemagne Thomas de Mezière et Jean-Yves Le Drian, notre ministre de la Défense, devraient détailler les ambitions d'un « Shengen du numérique ». Axelle Lemaire, la secrétaire d'Etat chargée du Numérique devrait relancer une fois de plus la filière française sécurité qui progresse doucement. Le premier Ministre, Manuel Walls, non confirmé, pourrait venir appuyer ses ministres dans cette période de crise.
Le Lieutenant-colonel Freyssinet, chef de la division cybercriminalité de la gendarmerie, précisait ce jeudi-là, les différentes opérations menées pour réduire les risques liés aux attentats: « Dés hier après midi, nous nous sommes mis en mode de surveillance pour identifier les réactions favorables aux attentats et créer une base réduite d'individus à priori dangereux. C'est exactement ce que l'on fait dans la rue pour identifier les gens qui auraient un comportement inquiétant. On fait une nette différence entre une simple réaction épidermique et des appels à la violence.
L'équipe se sert d'un outil d'analyse statistique OsincLab développé avec Thales pour détecter et identifier des groupes de personnes parlant du même sujet. Interrogé sur les possibilités d'empêcher l'accès à des sites en langue française incitant au terrorisme, le Lieutenant-colonel Freyssinet nous a précisé : «Les sites dangereux sont protégés par des sites écrans et des sites relais. Ils sont abrités dans des pays qui n'ont pas les mêmes législations que nous. On ne peut se rendre sur certains sites à l'étranger, il faut des commissions rogatoires. On le pratique parfois dans le cadre de la recherche pédopornographique mais cela reste exceptionnel. La Convention de Budapest sur la cybercriminalité a permis d'avancer mais il n'existe pas encore pas de Schengen numérique ».

Un thème repris par le ministre de l'intérieur, dimanche, ce qui veut dire qu'il devrait y avoir à terme une homogénéisation des procédures. Bien que la recherche des tueurs des membres de Charlie Hebdo le mercredi 7 janvier, ait été confiée à la préfecture de police, la gendarmerie via le GIGN et le BRI étaient en première ligne. Tous ses services étaient, depuis la mise en place du plan Vigipirate, en alerte maximale. Le paroxysme a été atteint, le dimanche 11 janvier, avec la surveillance des différentes manifestations de soutien aux victimes du terrorisme.

Gérer les différentes crises du moment sans perdre de vue l'essentiel
Mais cette crise exceptionnelle n'a pas remis en cause les activités régulières et le travail de fond des services du centre de lutte contre les criminalités numériques surnommé le C3N. La surveillance, la lutte contre la vente de produits illicites (drogues, médicaments frauduleux, produits de contrefaçons) et l'espionnage industriel qui minent l'économie française constituant leur travail quotidien. Ce sont les sujets qui seront traités au FIC la semaine prochaine.
the-world-of-cybercrime-is-becoming-increasingly-dominated-by_16001213_800941061_0_0_14082810_300 La défense des sites d'entreprise et la lutte contre les attaques à leurs présidents, qui ont connu une croissance exceptionnelle, sont le principal souci actuel. Identifiées par un travail d'ingénierie sociale incroyable les cibles des voleurs montrent que leur savoir faire ne fait que s'accroître. Les 1800 gendarmes N-Tech, dont plus de 250 à Paris, c'est à dire formés aux techniques d'investigation numériques, sont encore en nombre insuffisant pour couvrir tout le territoire français. Le N-tech est un enquêteur spécialisé dans le domaine des nouvelles technologies et de la cybercriminalité. Ils collaborent avec les services de police judiciaire et de gendarmerie. Le BRI comprend par exemple 253 spécialistes Ntech, 1540 correspondants et 37 Antech, des spécialistes ultra pointus

Des équipements récents
Parmi les nombreux équipements présentés lors de la visite des locaux de la gendarmerie, les UFED (Universal Forensics Extraction Device) sont des outils d'intervention rapides. Ces extracteurs de données (photo)UFED2 sont destinés à « faire parler » les téléphones mobiles, découverts sur des sites de crimes ou sur des personnes soupçonnées de malversations. Ils permettent de lire tous les éléments contenus dans de stockage : les contacts, l'historique des appels, les données de réseaux sociaux, les vidéos, les textes, les photos, etc. Des dizaines d'interfaces pour différents types (Android, Windows phone, IOS, et bien d'autres) et des centaines d'autres interfaces sont utilisées pour des connections modèles d'appareils mobiles.
Le même type d'appareil existe pour extraire les données des PC ou tablettes sans jamais modifier les contenus, un impératif pour le bon fonctionnement de la justice.
Pour les appareils endommagés, l'INL, le département informatique et électronique est capable d'extraire les données de n'importe quel support de stockage. Qu'il s'agisse de puces de circuits abimés au cours d'incendies ou d'immersions prolongées. Les analyses permettent, par exemple, de connaître grâce aux informations issues des GPS, la trajectoire des personnes et des véhicules mis en cause.

Au centre national d'analyse des images de pédopornographie
Le service d'analyse qui fonctionne en continu 24/24 avec trois officiers suit les activités sur le net de plusieurs centaines de personnes et tente, dés que c'est possible d'identifier les victimes et contrevenants. Interrogé sur place l'un des trois officiers qui tenait a rester anonyme nous confiait : « L'essentiel des images et des vidéos qui sont saisies proviennent de pays étrangers. Mais il reste une petite production en France. C'est en particulier favorisé par la multiplication de caméras et des smartphones. Au-delà des personnes, on cherche souvent à localiser les lieux et les dates de prises de vues, ce qui permet d'identifier par exemple les lieux privilégiés du tourisme sexuel. C'est possible grâce à de nombreux outils d'analyses utilisés par l'ensemble des services liés à Interpol qui maintient un fichier des personnes inculpées. On est parfois face à des situations difficiles où par exemple dans une vidéo un père est en train de prendre son bain avec ses enfants qui jouent et ce document est utilisé dans le cadre d'une procédure de divorce pour prouver que le père a des attitudes incestueuses. »
Confrontés à des images parfois intolérables, ces gendarmes sont accompagnés psychologiquement. « On peut changer de services si l'on n'en peut plus. Pour moi, cela fait plus de 5 ans et l'on se soutient. C'est important d'être au sein d'une équipe qui vous écoute.»
Une réflexion qui montre que le travail des forces comme celles des médecins urgentistes d'ailleurs est difficile. L'accumulation des tragédies quotidiennes éprouve, même s'ils s'en défendent, les nerfs des personnes qui vont au secours des autres.

Internet qui est au coeur de la crise actuelle favorise-t-il les crimes en tous genres ?
Que dire des télévisions qui à longueur d'années progamment des films policiers et des reportages sur de crimes violents. La TV, Internet, les jeux vidéos ultra réalistes en banalisant « l'ultra violence « sont devenus une véritable école du crime. Les jeunes désoeuvrés, souvent à la recherche d'une identité valorisante, peuvent facilement endosser les costumes de « rebelles vengeurs ».
Les évènements récents mettent en lumière la prise de conscience collective et les nouvelles mesures qui seront prises pour limiter les impacts de la « jungle » du net devraient simplifier au moins le travail des enquêteurs. Mais si l'on peut réduire les effets du mal, l'analyse des causes des différentes ruptures de notre société doit rester le sujet principal du travail des politiques.

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

Source : http://www.informatiquenews.fr/cybercriminalite-traque-gendarmerie-internet-28190

Obama cherche à renforcer la protection des données personnelles

Obama cherche à renforcer la protection des données personnelles

Face au nombre record de piratages sur le sol américain en 2014 et aux milliers de données personnelles lâchées dans la nature, Barack Obama a présenté un panel de lois destinées à renforcer la cyber-sécurité des entreprises et à réguler leur comportement.

2014 se traduit par un nombre record de cyber attaques ayant ciblé plusieurs grandes entreprises, dont Target, Home Depot, Staples et bien sûr Sony. Ajoutons à cela que près de la moitié des adultes américains se serait fait hacker en 2014. A tel point que CNN est allé jusqu'à développer un outil, "What hackers know about you ?" (Que savent les hackers sur vous ?). Celui-ci renseigne l'utilisateur sur ses données potentiellement menacées selon les entreprises dont il est client. Rien de rassurant, donc.

Citant un récent sondage selon lequel 91% des américains ont aujourd'hui le sentiment d'avoir perdu le contrôle sur leurs données personnelles, le président Barack Obama a proposé la mise en place d'un Personal Data Notification & Protection Act.

Premier objectif : harmoniser la législation au niveau fédéral et fixer aux entreprises un délai maximum de 30 jours pour avertir leurs clients en cas de piratage de leurs données privées. A l'heure actuelle, 47 lois étatiques différentes légifèrent sur la question. En fonction de l'Etat dans lequel il vit, un citoyen peut donc être averti ou non en cas de problème.
Le second projet de loi est spécifiquement consacré aux étudiants. Inspiré d'une loi californienne promulguée l'an dernier, le Student Digital Privacy Act interdirait aux entreprises de vendre les données d'étudiants dans un but non-éducatif. A l'heure où tablettes et ordinateurs portables se généralisent dans les salles de classe, de plus en plus de données sont collectées, et parfois vendues à des publicitaires ou des institutions financières. Cette loi vise à éviter que les données des étudiants ne soient utilisées de manière déloyale par leurs futurs employeurs ou banquiers. Une charte circule déjà parmi les entreprises à cet effet, et 75 sociétés l'auraient déjà signée (dont Apple et Microsoft). Les entreprises assurant un service éducatif qui ne signeraient pas cet engagement pourraient être dépossédées de leur mission.
Enfin, le chef de l'Etat a également proposé la mise en place d'une déclaration des droits à la vie privée du consommateur, le Consumer Privacy Bill of Rights, qui donnerait à celui-ci la possibilité de décider quelles données personnelles sont collectées et comment elles sont utilisées. La cyber-sécurité des entreprises détenant des données personnelles serait également renforcée. « Plus nous protégerons les données des consommateurs, plus il sera difficile pour les hackers de frapper nos entreprises et d'affaiblir notre économie. » a affirmé Barack Obama. Aux entreprises également de renforcer leurs systèmes. Sony par exemple, dont la console de jeux Playstation Network a été piratée pendant Noël, promet des investissements importants dans des serveurs et des techniciens capables de les gérer en cas d'attaques.

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

Source : http://www.atelier.net/trends/articles/obama-cherche-renforcer-protection-donnees-personnelles_433077

Que risquez-vous vous égarez une clé USB, un disque dur, ou si on vous vole les données de votre entreprise ?

Que risquez-vous vous égarez une clé USB, un disque dur, ou si on vous vole les données de votre entreprise ?

Si votre système informatique se fait pirater (comme l'ont été les sites Internet de SONY, Orange, Google, Bercy, le ministère des Finances…), les auteurs de l'attaque ne sont pas les seuls à être inquiétés d'une telle fuite. Les responsables du traitement peuvent en effet avoir à fournir quelques explications à la CNIL. Même sanction, si vous perdez votre clé USB, disque dur externe ou pire, votre ordinateur portable. Et pour cause, si vous manipulez des données qui permettent d'identifier une personne, communément appelées des données personnelles), vous êtes tenus à une série d'obligations de sécurité afin d'éviter la violation de données à caractère personnel (destruction, perte, altération, divulgation, accès non autorisé).

L'article 34 bis de la loi Informatique et Libertés les oblige par exemple à avertir sans délai la CNIL et à tenir à jour un registre des incidents. En principe, les particuliers, victimes collatérales de cette faille, doivent également être informés sans délai, sauf si la CNIL « a constaté que des mesures de protection appropriées ont été mises en œuvre par le fournisseur afin de rendre les données incompréhensibles à toute personne non autorisée à y avoir accès et ont été appliquées aux données concernées par ladite violation ». En clair, pas d'alerte direct des clients si les rustines ont été correctement appliquées.
Plus globalement, l'article 34 de la loi Informatique et Libertés impose au responsable d'un traitement de prendre toutes précautions utiles pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. Évidemment, cette protection diffère selon la nature des données et des risques présentés par le traitement.
Enfin, selon l'article 226-17 du Code pénal, le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en oeuvre les mesures prescrites à l'article 34 est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.
Etonnant non ?

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

Source : http://www.nextinpact.com/news/91600-un-partenaire-tf1-pirate-quelles-consequences-juridiques.htm
Extrait de Marc Rees adapté par Denis JACOPINI