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.

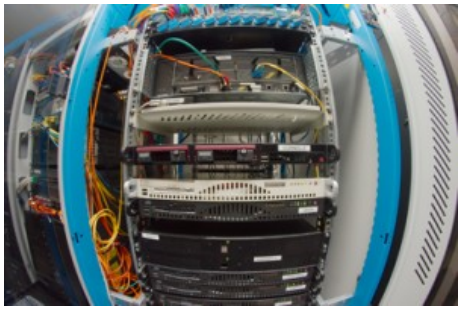
Si vous craignez que votre paisible routeur domestique ne soit en réalité un agent double à la solde de LizardSquad, Krebs détaille également dans la suite de son article les techniques de base permettant de sécuriser l'accès à son routeur. La plus simple et la plus efficace reste néanmoins la plus évidente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

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 2013, 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 », précisent 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 Boscher, 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 précaire 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'intégérance
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 intégérance 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.

Sécurisier 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 culpeuse des élus en cas de rupture des activités numériques ; la plupart n'en sont pas conscients », estime Richard Ekzewski, 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 Boscher, 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 Boscher, 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/decouvrir-la-securite-informatique-et-la-sauvegarde-des-donnees/

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

Vols, cybercriminalité, contrefaçons… Près de 50% des entreprises victimes de fraudes – 20minutes.fr

Vols, cybercriminalité, contrefaçons… Près de 50% des entreprises victimes de fraudes

Près de la moitié (49%) des entreprises de distribution et de biens de consommation au niveau mondial déclarent avoir été victimes de fraudes au cours des deux dernières années, selon une étude de PwC diffusée lundi.

«Ce chiffre ne cesse d'augmenter depuis 2009 (+12 points)», note le cabinet de conseil, qui a interrogé 5.128 dirigeants d'entreprises, dont 383 du secteur de la distribution et des biens de consommation, issus de 99 pays. La fraude la plus largement commise dans le secteur est le détournement d'actifs (76%), ce qui inclut «le vol, les décaissements frauduleux et l'appropriation illicite de matériel».

Risques liés à la cybercriminalité

La fraude aux achats arrive en deuxième position, beaucoup de répondants évoquant notamment des infractions liées à la sélection des fournisseurs (59%) ou bien aux contrats/accords de maintenance conclus avec ces derniers (39%).
Si la corruption n'est pas la fraude la plus constatée (25%), 56% des dirigeants interrogés la considèrent comme le risque le plus élevé pour une entreprise opérant à l'international.
Beaucoup de dirigeants évoquent également les risques grandissants liés à la cybercriminalité: un sur cinq déclare en avoir été déjà victime, et 27% pensent que leur entreprise y sera confrontée dans les deux années à venir.

Risque de renvoi ou de poursuites judiciaires

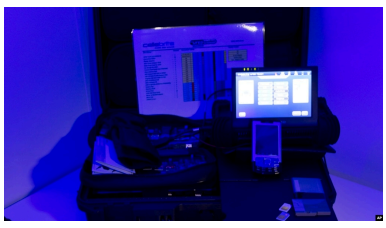
La perte de propriété intellectuelle (contrefaçon, vols de données clients…) fait également partie de leurs préoccupations pour l'avenir: seuls 7% en ont déjà fait l'expérience, mais 21% estiment qu'ils y seront confrontés d'ici deux ans.
L'étude montre que dans plus de deux tiers des cas (67%), les auteurs de ces infractions sont des collaborateurs internes aux entreprises. Ce taux est supérieur dans les secteurs de la distribution/biens de consommation, aux taux constatés sur l'ensemble des secteurs (56%).
«Les auteurs de ces faits occupent, pour la plupart, des postes de cadres intermédiaires et sont sévèrement punis lorsqu'ils sont démasqués: les entreprises pratiquent majoritairement le renvoi; elles se lancent parfois dans des poursuites civiles ou recourent aux autorités judiciaires», indique PwC.

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

Source : http://www.20minutes.fr/societe/1515087-20150112-vols-cybercriminalite-contrefacons-pres-50-entreprises-victimes-fraudes

---

Les particuliers, pierre angulaire de la lutte contre la cybercriminalité



Les particuliers, pierre angulaire de la lutte contre la cybercriminalité

En fin de compte, constate Mary Galligan des services de cybersécurité de la société Deloitte, c'est aux particuliers d'assumer leurs responsabilités.

La cybercriminalité est partout, ont constaté les participants. Même le Pentagone en fait les frais puisque lundi, les comptes Twiter et YouTube du Commandement Central (CENTCOM) ont été piratés. Comment mieux se protéger ? Souvent, fait valoir l'expert Austin Berglas, qui travaille pour le FBI, un employé tout à fait innocent prend une décision fatale.
« Peu importe combien d'argent une organisation consacre à la cyber-sécurité ; c'est encore et toujours un employé, ou le dernier utilisateur de l'ordinateur, qui clique sur un lien malveillant » explique Austin Berglas.
Malheureusement, il n'en faut pas beaucoup pour sombrer dans la cybercriminalité : un serveur, qu'on peut louer, un code malicieux, qu'on distribue par e-mail – et voilà, le cybercriminel prend le contrôle de votre ordinateur.
En fin de compte, constate Mary Galligan des services de cybersécurité de Deloitte, c'est aux particuliers d'assumer leurs responsabilités.
« Nous devons commencer à réfléchir à ce que faisons-nous pour protéger nos informations. Nous nous attendons à ce que les milieux d'affaire fassent le nécessaire pour nous, mais nous ne sommes pas disposés à prendre les mesures de sécurité les plus simples », constate Mme Galligan. Pour commencer, il faut que les usagers comprennent que rien n'est secret sur le web, et qu'ils prennent des mesures en conséquence.

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

Source : http://www.lavoixdelamerique.com/content/les-particuliers-pierre-angulaire-de-la-lutte-contre-la-cybercriminalite/2596924.html

---

L'après Charlie Hebdo, le chiffrement déjà un problème ?

L'après Charlie Hebdo, le chiffrement déjà un problème ?

C'était prévisible. Et le fait que le premier ministre David Cameron soit actuellement en campagne pour les législatives au Royaume-Uni n'y est sans doute pas étranger. De retour de la marche organisée en France en hommage aux victimes des attentats, ce dernier a proposé de faire évoluer les lois sécuritaires au nom de la lutte contre le terrorisme.

Et l'occasion fait le larron. Le premier ministre en profite en effet pour s'attaquer au chiffrement des communications. Ce n'est pas nouveau puisque les autorités du pays, notamment les agences de renseignement, se montraient particulièrement virulentes à l'égard des entreprises du Web très actives sur le chiffrement suite aux révélations de Snowden sur les pratiques d'espionnage des Etats.

Pas de communications inviolables

Ce n'est plus la coopération volontaire de ces acteurs de l'Internet qui semble désormais préoccuper David Cameron qui appelle à renforcer les lois autour du chiffrement afin de pouvoir ainsi accéder aux communications chiffrées.

« La question reste posée : allons-nous autoriser des moyens de communication pour lesquels des interceptions sont impossibles ? Et ma réponse à cela, c'est : non, nous ne devons pas. Le premier devoir de tout gouvernement est de protéger notre pays et nos concitoyens » a déclaré le premier ministre.

Le chef du gouvernement britannique ne précise toutefois pas comment il prévoit de rendre les communications chiffrées accessibles. Aux Etats-Unis, le FBI avait encouragé les éditeurs à inclure des portes dérobées dans les téléphones afin de permettre les interceptions par les autorités.

Assurément, ces attentats seront l'occasion pour le directeur du GCHQ, Robert Hannigan, d'encourager de nouveau les acteurs du web à la mise en place d'un « new deal » avec les gouvernements, ou coopération plus étroite avec le renseignement, afin de protéger les citoyens. Car après tout, déclarait-il quelques mois plus tôt, « la vie privée n'a jamais été un droit absolu ».

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

Source : http://www.zdnet.fr/actualites/l-apres-charlie-hebdo-le-chiffrement-deja-un-probleme-39812783.htm

---

Les entreprises françaises sont de plus en plus victimes de hackers et d'espions

industriels

	Les entreprises françaises sont de plus en plus victimes de hackers et d'espions industriels

Devant un environnement économique de plus en plus concurrentiel et incertain, les formations spécialisées en sécurité des entreprises tardent à se développer en France.

Les entreprises françaises sont de plus en plus victimes de hackers et d'espions industriels. Le nombre d'entreprises concerné par ces piratages s'élève à 360. 300 millions d'euros c'est ce qu'ont coûté ces attaques par les gangs internationaux sur les trois dernières années. Face à ces menaces, la Direction Centrale de la Police Judiciaire (DCPJ) et le Medef vont sceller un accord pour résorber le phénomène, mercredi 14 janvier 2015. L'Office central pour la répression de la grande délinquance financière (OCRGDF) a quant à lui officialisé un accord signé avec l'Ecole des ingénieurs de numérique pour lutter contre « le fléau des escroqueries aux faux virements ».
L'Epita (l'école des ingénieurs du numérique) est aujourd'hui, un des rares établissements français à proposer un enseignement qui se focalise sur la sécurité des entreprises. « Aujourd'hui, il manque une vraie filière qui aille du niveau bac +1 à bac +5 » d'après Olivier Hassid interrogé par Le Figaro, dirigeant du Club des Directeurs de Sécurité et de Sureté des Entreprises (CDSE). D'après ses dires, la pluralité des matières permet de créer une filière avec des acquis enseignés en licence. La France montre un réel retard concernant les formations sur la sécurité des entreprises.

Les grandes écoles intéressées par ce domaine de sécurité
Deux raisons à ce retard, d'une part le manque de prise en compte des enjeux qui est dû à l'insuffisance de la recherche, et d'autre part le manque de besoin exprimé par les entreprises. « Les problématiques de sécurité ont réellement vu le jour dans années 2006/2007. C'est à ce moment là qu'un certain nombre de grands groupe ont créé des directions en sûreté et sécurité », explique Olivier Hassid.
« Les balbutiements de la formation en sécurité datent des années 90 avec la création de l'IHESI, aujourd'hui devenu l'Institut national des hautes études de la sécurité et de la justice (INHESJ) » raconte le dirigeant du Club. L'INHESJ est la véritable première formation française en matière de sécurité. En plus des formations de l'INHESJ, on retrouve aujourd'hui en France un Master en Gestion globale des risques et des crises à l'université Paris 1, une licence en sécurité à l'université Paris Descartes et, depuis quelques temps, un certificat du management de la sécurité et de la sûreté informatique, avec l'école Epita qui valide la qualité de la formation.
Mais selon Oliver Hassid, le développement des formations spécialisées en sécurité des entreprises doit être impératif pour peut-être un jour arriver à un cursus complet. Il indique que « Les instituts d'études politiques s'intéressent à ces problématiques, tout comme les écoles de commerces. Il y a une vraie tendance avec l'effet Snowden et les inquiétudes concernant le cyberespace. »

Vers un rapprochement de la sécurité et l'intelligence économique
Au vu du développement de l'enjeu sécuritaire, la notion d'intelligence économique s'est développée en France. Le concept a émergé dans la seconde partie des années 90, immédiatement, contrairement à la sécurité des entreprises, des formations ont été créées. Christian Harbulot crée en 1997 l'école de guerre économique (EGE), et d'autres également à cette période comme l'Ecole Européenne d'Intelligence Economique (EEIE). Aujourd'hui ce genre de formations est aussi retrouvé dans les grandes écoles de commerce et d'ingénieurs mais aussi à l'université.
Selon Christian Harbulot, le directeur de l'EGE, et Olivier Hassid, on se dirige vers le rapprochement de ces deux pôles stratégiques des entreprises car leur rapport à l'information est similaire. Ainsi, les futures formations devraient joindre les deux domaines à l'avenir.
Il y a bon nombre d'enjeux et les fraudes sont de plus en plus sophistiquées. La criminalité via les réseaux est en expansion, les risques géopolitiques et la sécurité des entreprises à l'international peuvent augmenter dans un contexte encore plus instable.

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

Source : http://www.digischool.fr/enseignement/securite-entreprise-vraie-filiere-peine-mettre-place-france-25849.php
Par Manare BARCHI

Cyber-guerre islamiste : fortes attaques contre des sites bretons le 9 janvier 2015

	**Cyber-guerre islamiste : fortes attaques contre des sites bretons cette nuit**

La cyber-guerre aurait-elle débuté en Bretagne?

Au milieu de la nuit du jeudi 8 au vendredi 9 janvier, des sites institutionnels de communes françaises ont été attaqués par des pirates informatiques islamistes . « The Islamic State Stay Inchallah, Free Palestine, Death to France, Death to Charlie Hebdo », un message islamiste pro-Daesh, pour la Palestine libre et se réjouissant de la mort de la France et de Charlie Hebdo a été mis en ligne est toujours diffusé à 6h30 ce matin sur certains des sites hackés. Pour les sites des communes de la région parisienne, l'attaque est signée « L'APoca-DZ ».

D'autres sites ont été visés.
Ainsi une série de sites bretons est désormais hors service. Les sites de différents commerçants mais aussi des sites institutionnels tel celui de la mairie de Port-Louis ont été hackés. Les attaques ont été revendiquées par au moins deux groupuscules.
Le site du camping de Fouesnant et celui de la mairie de Port-Louis ont été attaqués par un groupuscule du nom de FALLAGA TEAM et à cette heure, le message est toujours en ligne.
Liste d'une partie des sites hackés, dont peu ont été remis en service à 6h30 ce matin :
http://www.alrsaildesign.com
http://www.art-culinaire-conseil.com
http://www.art-table-discount.com
http://www.artdelatable-alencon.com
http://www.aspnet_client
http://www.authonimmobilier.com
http://www.avaugourhotel.com
http://www.balladins-blois.com
http://www.bopp.fr
http://www.brasserie-bleue.com
http://www.camping-ecureuils.com
http://www.camping-fouesnant.com
http://www.camping-la-padrelle.com
http://www.camping-lesdunes-29.com
http://www.camping-soirdete.com
http://www.campingcourseulles.com
http://www.campinglesetangs.com
http://www.cataglenn.com
http://www.cave-du-moros.com
http://www.celtik-jump.fr
http://www.chantier-lobrichon.fr
http://www.christian-brossault.fr
http://www.clara-sanitaryware.com
http://www.comecat.com
http://www.concept-nettoyage.com
http://www.d-dayhouse.com
http://www.domaine-du-bocage.fr
http://www.dunemerveille.com
http://www.eprim-nord.com
http://www.espace-audition.com
http://www.europa-quiberon.com
http://www.francimo-bretagne.com
http://www.francsgarcons.com
http://www.grandhotelsolesmes.com
http://www.grandhoteltours.com
http://www.guemene.fr
Accueil
http://www.habitat-loisirs.com
http://www.handiflow.com
http://www.haras-maurea.com
http://www.hotel-aloe.com
http://www.hotel-bretagne-quiberon.com
http://www.hotel-cancale.fr
http://www.hotel-croixdusud.com
http://www.hotel-de-bretagne35.fr
http://www.hotel-de-lisle.com
http://www.hotel-finistere.com
Accueil
http://www.hotel-france-europe.com
http://www.hotel-larochelle-charmilles.fr
http://www.hotel-lebussy.fr
http://www.hotel-les-douves.com
http://www.hotel-mulsanne.fr
Accueil
http://www.hotelargentan.com
http://www.hoteldelahague.com
http://www.hotelducormier.fr
http://www.hoteldуparc-bordeaux
http://www.hotelleboutondor.com
http://www.hotelloscolo.com
http://www.i-c-c.fr
Accueil
http://www.la-haute-foret.com
http://www.lamaisonraphael.com
http://www.larosee.fr
http://www.le-divellec.com
http://www.le-teuff.com
http://www.leboissoleil.com
http://www.ledivenah.com
http://www.lemanoirdusphinx.com
http://www.lepasseurdulenn.com
http://www.lericordeau.com
http://www.lescarsbleus.com
http://www.lesenfantsgatthes.com
http://www.librimmo3.com
Accueil
http://www.locations-belle-ile-vacances.com
http://www.loftinnvannes.com
http://www.lorient-laser-industrie.com
http://www.manoir-bodrevan.com
http://www.maury-transports.com
http://www.moteurs-ammi.com
http://www.moueloservices.fr
http://www.moulin-neuf.net
http://www.olistis-vannes.ecomouest.info
http://www.oree-du-bois.com
Accueil
http://www.parcergreo.com
http://www.pays-muzillac.fr
http://www.pensuinea-mariana.com
http://www.perceval-medica.com
http://www.pharedekerbel.com
http://www.photos-bretagne.com
http://www.prat-ar-coum.com
http://www.prestifeu.com
http://www.prieuredesgourmands.com
http://www.relaisdes3pommes.com
http://www.residence-helios.com
http://www.residence-ondine.com
http://www.rhuys-vacances.com
http://www.rouleco.com
http://www.tableau-unique.com
http://www.tecnoland.fr
http://www.terasses-du-lac.com
http://www.thermobaby.com
http://www.uncottageennormandie.com
http://www.videka-diana.com
Accueil
http://www.vit2be-diana.com
http://www.voyagesmarzin.com
Accueil
http://silhouettebienetre.com
http://revedeluxe.com
http://www.salon-esprit-bien-etre.fr
http://www.asimplesoft.com
http://www.blackbeard.fr
http://www.bauzer-industrie.fr
http://www.peexel.fr
http://claudi-nettoyage.fr
http://claudipro.fr
http://www.leblogdepeexel.fr
ACCUEIL
http://www.ecoloetancheite.fr/
Lire la suite…

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

Source : http://7seizh.info/2015/01/09/cyber-guerre-islamiste-fortes-attaques-contre-des-sites-bretons-cette-nuit/
Par 7seizh.info

l’Allemagne victime d’attaques DDoS

l’Allemagne victime d’attaques DDoS

Les sites du gouvernement allemand, ainsi que la page de la chancelière Angela Merkel, ont été piratés mercredi 7 janvier. L’attaque a été revendiquée par un groupe pro-russe qui demande à Berlin de cesser son soutien au gouvernement ukrainien. Le premier ministre ukrainien est actuellement en visite en Allemagne.

Un groupe de hackers pro-russes, connu sous le nom de CyberBercut, a revendiqué la cyberattaque de plusieurs sites du gouvernement allemand, dont la page d’Angela Merkel et le site du ministère des Affaires étrangères. Le groupe appelle l’Allemagne à cesser son soutien financier à Kiev. Selon les services de renseignements allemands, les sites du gouvernement font face à en moyenne 3 000 tentatives de piratage par jour, certaines venant de l’étranger. Le premier ministre ukrainien, Arseni Iatseniouk, actuellement en visite à Berlin, a attribué l’attaque aux services secrets de Moscou.
Selon Steffen Seibert, le porte-parole du gouvernement, les data-centers sont victimes d’une attaque sévère, perpétrée par des systèmes extérieurs, comme le relate Reuters. Le but des pirates est de saturer les serveurs pour les mettre hors service (attaque DDoS, attaque par déni de service).

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

Source : http://www.industrie-techno.com/cybersecurite-l-allemagne-victime-d-attaques-ddos.35488

Le ministère de la Défense attaqué par des ‘Anonymous’

Le ministère de la Défense attaqué par des ‘Anonymous’

Le site Web du ministère de la Défense était inaccessible en raison d’une attaque en déni de service revendiquée par un groupe baptisé Anonymous OpGPII. Ils déclarent vouloir venger la mort du militant Rémi Fraisse.

Le site Internet du ministère de la Défense a fait l’objet hier 6 janvier d’une attaque informatique en déni de service, le rendant ainsi inaccessible aux internautes une bonne partie de la journée. « Le Centre d’analyse en lutte informatique défensive (Calid) est sur le coup » indiquait hier un porte-parole du ministère à 20Minutes.

Le DDoS a depuis été revendiqué sur Twitter par les membres d’un groupe se revendiquant d’Anonymous et baptisé « Anonymous OpGPII ». Ces derniers justifient cette attaque informatique par la mort du militant écologiste et opposant au barrage de Sivens, Rémi Fraisse, tué par une grenade des gendarmes le 25 octobre dernier. D’ailleurs pourquoi la Défense et non l’Intérieur dont dépend désormais la gendarmerie ?

« Aujourd’hui, nous commençons une opération pour le venger » déclarent des Anonymous dans un message mis en ligne sur le site Pastebin et repéré par le Figaro. « Pendant trop longtemps, Anonymous est resté à l’écart, nous n’avons pas pris de mesures. Mais maintenant, nous allons le faire » promettent-ils encore.

Un autre membre des Anonymous assurait cependant hier à 20 Minutes que le mouvement (jamais véritablement coordonné) n’était en rien responsable de l’attaque contre le ministère de la Défense. « Cela dit, cela fait des années qu’on leur a fait remarquer que leur site est truffé de failles » soulignait-il aussi.

De quoi permettre de futures attaques ? Une plainte pourrait en tout cas être déposée par le ministère, qui précise par ailleurs que deux adresses IP, liées au déni de service, ont été identifiées et signalées aux autorités.

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

Source : http://www.zdnet.fr/actualites/le-ministere-de-la-defense-attaque-par-des-anonymous-39812391.htm