Faut-il craindre une cyberguerre ?

Faut-il craindre une cyberguerre ?

Leurs PC sont leurs armes et leur guerre se mène en ligne. Après les attentats à Paris, des cyberattaques ont été menées contre des sites internet français, par des hackers affirmant agir au nom du groupe Etat islamique (EI). Dans le même temps, des « hacktivistes » se revendiquant d'Anonymous ont piraté des sites et comptes sur les réseaux sociaux des organisations islamistes et de leurs membres.

Mais c'est loin d'être terminé. Des comptes YouTube et Twitter appartenant au commandement militaire américain au Moyen-Orient (Centcom) ont également été visés, et une attaque d'envergure est annoncée pour jeudi 15 janvier. Sommes-nous à l'aube d'une cyberguerre ? Non, toujours pas, répond Gérôme Billois, expert en sécurité informatique au cabinet Solucom et administrateur du Club de la sécurité de l'information français (Clusif).

Francetv info : Peut-on parler de cyberguerre lorsque l'on évoque les attaques informatiques menées par des hackers qui se revendiquent du jihad ?
Gérôme Billois : Non, on n'y est pas du tout. Ce serait exagéré de parler de « guerre ». Aujourd'hui, nous parlons d'actes qui n'ont pas d'effets dans le monde réel. Il n'y a pas d'explosions, pas d'interruption de services essentiels comme l'énergie ou les transports. Il n'y a pas non plus de pertes humaines. On reste dans le monde virtuel.

Alors comment pourrait-on appeler cela ?
Il n'existe pas vraiment de mot pour déterminer ces actes. Après l'attaque contre la société Sony Pictures, qui a subi une destruction massive de son système d'information et le vol d'une importante quantité de données, Barack Obama parlé de cybervandalisme. Le terme semble assez juste. Ce qui se passe aujourd'hui, c'est comme si des activistes entraient dans des centaines de boutiques pour y coller leurs affiches et repartir. Les propriétaires de ces magasins n'avaient pas bien fermé la porte en partant et en revenant le lendemain matin, ils trouvent des affiches qui font la publicité de l'Etat islamique.

Pour vous, ces actions restent plutôt d'ordre symbolique ?
Extrêmement symbolique, puisqu'il s'agit d'une lutte entre deux idéologies. Avec d'un côté l'#opFrance (pour « Opération France », lancée par des cyberjihadistes), annoncée pour le 15 janvier, qui vise à tenir l'image de la France en attaquant un grand nombre de structures dans l'Hexagone, et de l'autre l'#opCharlieHebdo, qui vise à dénoncer et rendre indisponibles des sites jihadistes.

Qui se trouve derrière cette contre-attaque ? Certains revendiquent leur appartenance aux Anonymous…
On ne peut pas dire qu'il s'agit « des » Anonymous. Ce sont, en fait, des groupes très divers. Il faut d'ailleurs savoir que certains des groupes qui attaquent la France aujourd'hui ont pu participer à des opérations des Anonymous, ou s'en revendiquer. Il y a des acteurs en commun, qui œuvraient auparavant dans une même direction et se divisent aujourd'hui sur ce cas particulier. La logique de « l'hacktivisme » au sens large c'est : « Il se passe un événement, je me positionne par rapport à celui-ci et à chaque nouvel événement je redéfinis ma doctrine ».

Quelle est la force de frappe des cyberjihadistes aujourd'hui ?
Aujourd'hui, ils mènent des attaques de faible intensité. Sur une échelle de 1 à 10, ils atteignent 5, au maximum. Ces pirates utilisent des vulnérabilités connues depuis longtemps ainsi que des outils disponibles facilement sur internet. De plus, ils s'attaquent à des sites peu sécurisés et pas mis à jour. Il existe tout de même un risque à moyen terme. Ces groupes de pirates, petit à petit, vont apprendre, se développer, et augmenter ainsi leurs capacités d'attaque pour viser des services plus importants. On sait que l'EI dispose d'importants moyens financiers. Il n'aura, de toutes façons, pas de problème de matériel : avec un simple PC, vous pouvez lancer des attaques.

Qu'est-ce qui pourrait rendre ces groupes plus dangereux ?
Pour eux, il s'agit d'abord de gagner en expérience. Mais ils peuvent aussi acheter ce qu'on appelle des « vulnérabilités zero day », c'est-à-dire des connaissances sur une vulnérabilité qui n'est pas encore connue des éditeurs de sécurité. Quand vous possédez cet atout, vous pouvez attaquer un système, même s'il est mis à jour. Pour poursuivre l'analogie des boutiques vandalisées : imaginons que quelqu'un, comme un chercheur, découvre que pour la marque de serrure XYZ il existe un pass universel. Avec cette information, il peut faire deux choses : soit prévenir le fabricant de la serrure pour qu'il corrige son produit, soit vendre cette vulnérabilité à des criminels sur le marché noir.

Les pirates ont donc toujours un temps d'avance sur les systèmes de sécurité…
Oui et non. Une partie des pirates, les plus pointus, certains groupes de cybercriminels, peuvent aller jusqu'à dédier une partie de leurs moyens à faire de la recherche en attaques et trouver ces « vulnérabilités zero day ». Ces groupes-là, oui, peuvent avoir cette capacité. Il peut s'agir soit d'Etats un peu belliqueux, soit de cybercriminels pointus. Mais il n'y en a pas des milliers. Dans le cas qui nous intéresse, les pirates n'ont pas cette avance. Ils utilisent simplement des failles connues, dont certaines ont été rendues publiques depuis 2012. Or, nous sommes en 2015 et les systèmes qu'ils attaquent n'ont pas été corrigés. On parle de petites mairies, d'universités, de PME… Ces structures-là n'ont pas forcément l'expertise ni les moyens pour maintenir leurs systèmes à jour.

D'autres structures, susceptibles de devenir des cibles plus importantes comme les grandes banques françaises par exemple, sont-elles mieux protégées ?
Oui, les systèmes sensibles sont mieux protégés. Les grandes sociétés ont les capacités nécessaires pour investir dans la sécurité. Les banques en ligne, par exemple, réalisent quotidiennement, voire plus encore, des tests de vulnérabilité automatisés, qui mènent les mêmes actions que les pirates. Les résultats de ces tests remontent aux services de sécurité informatique qui peuvent très rapidement effectuer les mises à jour nécessaires. Ce qui n'empêche qu'un site d'une grande banque est tombé, pendant une des attaques. Mais il s'agissait d'un site satellite sur lequel il n'y avait aucune transaction financière.

Là, nous parlons de sites internet. Qu'en est-il des systèmes informatiques internes ?
Ces systèmes-là disposent d'un niveau de sécurité, a priori, plus fort. Ne peuvent y rentrer que des employés ou des collaborateurs connus. Soit parce qu'il existe une protection physique : il faut entrer dans le bâtiment de la société. Soit parce qu'il y a des mots de passe ou des cartes à puce pour accéder à distance aux données. On n'est pas pour autant à l'abri d'une attaque visant le système d'information interne. C'est ce qui est arrivé chez Sony. Le FBI l'a dit : 90% des sociétés américaines seraient tombées si elles avaient été confrontées à la même méthode de piratage. C'est énorme.

Donc la menace existe…
Oui. La vraie question est de savoir si les jihadistes passeraient à ce type d'actions. Leur logique, pour l'instant, est plutôt de faire du bruit, de multiplier les cibles, de casser des milliers de sites, pour pouvoir dire mille fois qu'ils l'ont fait. Une attaque plus poussée, qui ferait plus de mal, aurait peut-être moins de résonance médiatique.

C'est tout de même une menace prise au sérieux, sur laquelle l'Otan se penche sérieusement. Est-ce à cause des menaces de ces jihadistes ?
Pas seulement. On distingue trois grandes « familles d'attaquants » : les « hacktivistes », qui attaquent par idéologie comme les cyberjihadistes, les cybercriminels, qui volent des données pour les monnayer, et enfin les Etats, qui développent des capacités défensives et offensives. Mais on peut craindre des regroupements entre ces groupes. Dans l'exemple de Sony, l'attaque est attribuée à la Corée du Nord, mais on sait qu'elle aurait été appuyée par des groupes d' »hacktivistes ».

Comment les Etats se préparent-ils face à cette menace ?
La cyberdéfense ne se résume pas à créer des murs en attendant que des pirates tentent de les casser. Cela inclut aussi des techniques de contre-attaque, pour pouvoir neutraliser les attaquants. Tous les Etats s'y préparent. Pour ce qui est de mener des attaques, on peut estimer que tous les pays industrialisés ont déjà des moyens et les renforcent au quotidien.

Concrètement, en quoi consiste la contre-attaque face à des cyberjihadistes ?
Les moyens de contre-attaque sont quasiment les mêmes que les moyens d'attaque. On peut imaginer attaquer leurs systèmes, les rendre inopérants, capturer les données pour bien comprendre qui ils sont. On peut aussi « boucher leurs tuyaux » pour éviter que les attaques ne passent.
Mais la difficulté, dans ce domaine, est de bien savoir qui se trouve en face de nous. Dans le cas Sony, on lit que l'attaque serait partie d'un hôtel en Thaïlande. A mon avis, elle est passée par là, mais ce n'est pas son point de départ. J'ai déjà vu des attaques menées contre certains de mes clients provenir de serveurs d'écoles maternelles au Vietnam. On se doute bien que ce n'est pas un écolier vietnamien qui l'a lancée, qu'il s'agit simplement de brouiller les pistes. Dans des scénarios plus vicieux, il peut s'agir de faire croire que l'attaque vient d'un endroit en particulier, pour provoquer une contre-attaque sur cette cible. Si l'on n'attribue pas l'attaque au bon responsable, on risque d'infliger des sanctions à un leurre.

Quand vous parlez de « boucher les tuyaux », s'agit-il d'attaques par déni de service, méthode qu'utilisent justement certains hackers ?
Cette méthode-là n'est efficace que temporairement, pour freiner une attaque. Mais les Etats ont la possibilité, à distance, de faire tomber les réseaux, de les couper, plutôt que de les boucher. Je parle bien des Etats, car les entreprises privées n'ont pas le droit de contre-attaquer. La légitime défense n'existe pas dans le cyberespace. En France, le seul cadre légal aujourd'hui, c'est la loi de programmation militaire, qui donne cette capacité à l'Agence nationale de sécurité des systèmes d'information (Anssi) ou, en tout cas, aux services rattachés au Premier ministre.

Manuel Valls va annoncer une série de mesures, dont certaines concernent internet. Où placer le curseur, entre la neutralité de net, le verrouillage pour empêcher les cyberjihadistes de nuire et la protection de la vie privée ?
C'est une question idéologique fondamentale, mais on n'y trouvera pas de réponse parfaite. Ce qui est certain, c'est qu'il y a une menace, qui, il faut le préciser, représente une très faible portion des usages d'internet. L'énorme majorité des usages sont très bénéfiques, pour l'économie, la culture, notre quotidien. Le plus important, selon moi, c'est le contrôle des moyens qu'on se donne. Il faut, certes, pouvoir être très réactif, car les attaques peuvent être menées très vite, mais il faut se contrôler pour éviter de tomber dans la surveillance généralisée. Ce contrôle peut être exercé par la justice ou des autorités indépendantes.

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

Source : http://www.francetvinfo.fr/monde/terrorisme-djihadistes/faut-il-craindre-une-cyberguerre_796909.html

---

Cyberdéfense: la guerre de demain a déjà commencé

Cyberdéfense: la guerre de demain a déjà commencé

Paris – A l'heure des cyberattaques en série, notamment après les dernières caricatures du prophète Mahomet, le Calid, « gendarme » des systèmes informatiques de l'armée française, est sur le pied de guerre, derrière la façade discrète d'un immeuble parisien.

Installé devant un rideau d'écrans, un cybersoldat en treillis scrute attentivement les informations qui défilent. Soudain une mention « SUSPICIOUS » (suspect) se détache en rouge sur l'un des ordinateurs.
« J'ai relevé une alerte sur un site, un utilisateur qui essaie d'aller sur un serveur cloud », lâche le sous-officier qui, avec une trentaine d'autres militaires, surveille 24 heures sur 24 les réseaux du ministère de la Défense, à l'affût du moindre intrus mal ou très mal intentionné.
« Ce qu'on cherche à détecter, c'est un pic de réseau anormal, un trafic important de messagerie. On dispose pour cela de +capteurs+ sur les entrées vers nos réseaux, les postes de travail », explique le cybersoldat, qui préfère garder l'anonymat.
Et les ennemis invisibles ne manquent pas. Le 6 janvier, le site du ministère a été piraté par le groupe Anonymous. Ces derniers jours, l'armée a été la cible d'une dizaine de cyberattaques visant notamment des régiments. Le 12 janvier encore, des pirates se réclamant de l'organisation Etat islamique (EI) prenaient brièvement le contrôle des comptes Twitter et Youtube du commandement militaire américain au Moyen-Orient (Centcom).
« Les gens de Daech (acronyme de l'EI en arabe) ont de l'argent, recrutent des informaticiens. Ils manquent peut-être de réseaux de renseignement sur les cibles mais sont capables assez rapidement de bloquer des sites », relève le vice-amiral Arnaud Coustillière, responsable Cyberdéfense à l'état-major des armées.
« C'est de la gesticulation. Mais dans la guerre de l'image, ce peut être très intéressant », ajoute ce spécialiste. Les jihadistes n'ont pas en revanche les moyens, selon lui, de mener des attaques d'envergure.
Le Calid (Centre d'analyse de lutte informatique défensive) surveille aussi les cyberattaques qui peuvent paralyser des systèmes d'armes ou détourner de l'information sur les moyens et les cibles des forces. Il envoie pour cela des équipes au coeur des théâtres d'opération.
Car plus que les attaques de sites internet, voilà bien le véritable cauchemar des états-majors: que des missiles soient stoppés net dans leur course, des drones, piratés, des frégates, détournées à distance au beau milieu d'une intervention militaire.

– 'Dans la peau de l'attaquant' –
En Afrique, l'opération antijihadiste française Barkhane a ainsi été la cible d'une tentative d'attaque cyber, confie-t-on au ministère de la Défense. « Cela peut se faire à partir d'un ordinateur et d'un téléphone ».
Depuis longtemps déjà, James Bond fait des émules. Lors du raid israélien contre de présumées installations nucléaires syriennes en 2007, une attaque numérique a ainsi trompé les défenses adverses en renvoyant une image radar tronquée.
Dans l'affaire Stuxnet, un ver informatique, espionnant et reprogrammant des automates industriels, s'est attaqué aux centrifugeuses iraniennes soupçonnées de faire de l'enrichissement d'uranium à des fins militaires.
Les systèmes sont d'autant plus vulnérables qu'ils sont de plus en plus interconnectés. Sur un navire, navigation, propulsion, combat et communications sont intégrés. Faute de sécurisation, il sera bientôt possible de bloquer le bateau en pleine mer ou de l'empêcher de combattre.
Derrière le Calid, des dizaines de chercheurs de la Direction générale de l'armement (DGA) s'emploient à anticiper cette cyberguerre de demain.
« On se met dans la peau de l'attaquant et on voit quelles attaques on peut mener sur nos propres systèmes d'armes pour voir quelles menaces sont crédibles », raconte Frédéric Valette, chef du pôle sécurité des systèmes d'information à la DGA.
Face à une menace de plus en plus pressante, la France s'est dotée d'un budget cyberdéfense d'un milliard d'euros sur la durée de la loi de programmation militaire (2014-2019). Le Calid doit doubler de taille dans les cinq ans à venir et 400 spécialistes être recrutés.
La France reste loin derrière les Etats-Unis, la Chine et Israël, à un niveau comparable avec la Grande-Bretagne ou la Russie, selon le ministère de la Défense.
« L'idée c'est d'arriver à un niveau de sécurité suffisant. Il n'y a pas de sécurité absolue. Il faut savoir anticiper, mettre en place des niveaux de protection adaptés et être capables de réagir en cas d'attaque », résume M. Valette.

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

Source : http://www.lexpress.fr/actualites/1/societe/cyberdefense-la-guerre-de-demain-a-deja-commence_1642214.html

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

Que risquez-vous si 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.

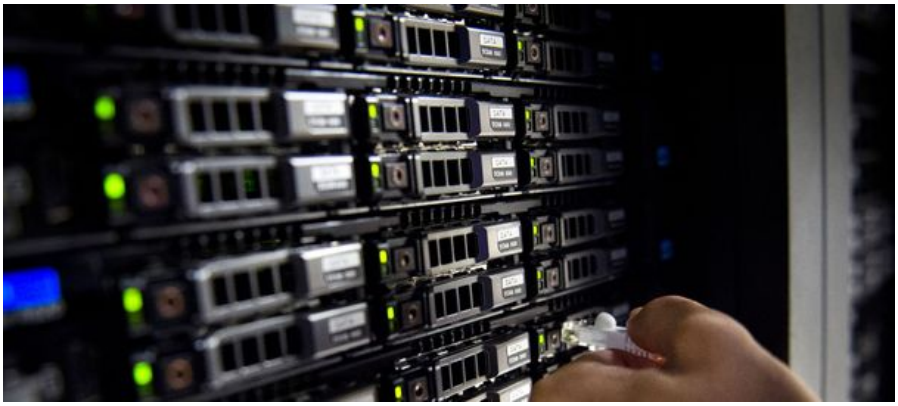
Enfin, selon l'article 226-17 du Code pénal, le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en oeuvre les mesures prescrites à l'article 34 est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

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

Trois contrats pour assurer son informatique

	Trois contrats pour assurer son informatique

En France, en 2013 les violations de données informatiques ont coûté 6,1 milliards d'euros aux victimes dans le monde professionnel.

Qu'elle soit de production ou de gestion, l'informatique est présente dans chaque entreprise. Il est nécessaire de couvrir non seulement le matériel, mais également les données qu'elle contient. En France, en 2013 les violations de données informatiques ont coûté 6,1 milliards d'euros aux victimes dans le monde professionnel : trois fois plus qu'en 2010 (2,2 milliards d'euros). En 2014, le coût par donnée piratée se chiffrerait à 351 euros contre 98 euros en 2010, selon les estimations de la société de sécurité informatique Symantec.
Aux traditionnels risques de dommages du matériel informatique et de responsabilité civile, s'ajoute depuis peu, la cybercriminalité. Le point sur les trois catégories de contrat que peut souscrire l'entreprise.
A noter : les contrats multirisques de matériels de bureaux peuvent couvrir les dommages informatiques. En revanche, la responsabilité civile comme la criminalité informatique font l'objet de contrats spécifiques, à souscrire séparément.

1. Dommages informatiques
Existant sur le marché français depuis une quinzaine d'années, l'assurance de dommages couvre le matériel informatique en cas d'incendie et de vol. L'assureur garantit essentiellement les frais de reconstitution des données et les coûts supplémentaires d'exploitation, en versant un capital à l'entreprise ayant subi un dommage. Traditionnellement, cette garantie faisait l'objet d'un contrat d'assurance « Tous Risques Informatiques ». Mais la tendance consiste à l'inclure dans le contrat « Multirisques Bureaux ».

2. Responsabilité civile
A ce stade, il faut distinguer la responsabilité civile d'exploitation, de la responsabilité professionnelle.
La responsabilité civile d'exploitation joue par exemple lorsqu'une entreprise transmet un virus informatique à un client.
La responsabilité civile professionnelle pour les mises en cause de l'entreprise au titre de ses prestations : conseils ou services. « Couvrant les dommages immatériels causés au cours d'une mission, la responsabilité civile professionnelle intéresse surtout les sociétés d'informatique », précise Benoît Salembier, à la tête du cabinet de courtage Add Value Assurances.

3. Criminalité informatique
Les compagnies d'assurance anglo-saxonnes ont une longueur d'avance sur leurs homologues européens. Les quelques acteurs en pointe sur les nouvelles technologies – Ace Europe, Hiscox, Beazley, Chartis, CNA – proposent un contrat ou garantie réduisant les risques de piratage et d'intrusion dans les systèmes d'information d'une entreprise.
Le contrat « Cybercriminalité » proposé par le courtier Add Value permet à l'entreprise de couvrir sa responsabilité et les dommages subis suite à une attaque informatique. « Les frais de restauration des données perdues constituent un vrai sujet. Les pertes de revenus ou d'exploitation consécutives à cette attaque sont également à prendre en compte. Quand on est une marque importante, il arrive que les hackers demandent une rançon à l'entreprise attaquée pour lui restituer les données », détaille Benoit Salembier.
Deux critères jouent sur le risque de criminalité. D'une part la taille de la base de données d'une entreprise : plus elle est grande, plus elle est exposée aux risques de piratage. D'autre part, la nature des données. Plus elles sont sensibles, plus elles sont exposées à la cybercriminalité. Ainsi par exemple les cabinets d'avocats, les experts comptables et même les journalistes seraient particulièrement visés.

Cybercriminalité : deux exemples de sinistres garantis
Avec le concours d'Add Value Assurances, voici deux cas de criminalité informatique réels avec les garanties que vous pouvez demander à votre assureur.
Exemple n°1. Piratage d'un site internet
Une société X crée un site e-commerce afin de vendre ses produits au grand public. Son succès attise la convoitise de ses concurrents. Des hackers réussissent à pirater son site et à le mettre hors service, ce qui signifie l'arrêt quasi complet de l'activité. En effet cette société commercialise ses produits à 75% sur internet.
L'assureur peut prendre en charge les frais engagés par les consultants mandatés pour identifier la faille de sécurité, et remettre le site web en état, à hauteur du plafond de garantie défini dans le contrat. De même, il indemnise l'entreprise de la perte de chiffre d'affaires sur la période d'arrêt du site internet, à hauteur du plafond de garantie défini dans le contrat.

Exemple n°2. Extorsion de données clients
Des hackers ont détourné une base de données clients d'une agence de voyage comprenant notamment leurs coordonnées bancaires. Ils demandent une rançon de quelques centaines de milliers d'euros euros à la direction pour la récupérer. Après deux semaines de négociation et le paiement de la rançon, l'entreprise piratée récupère sa base de données.
La base de données était assurée. L'assureur mandate ses consultants spécialisés pour accompagner l'assuré et mener à bien les négociations. Il indemnise l'entreprise assurée pour le paiement des honoraires des consultants et de la rançon, dans la limite des plafonds définis dans le contrat.
A noter. Avant de souscrire un contrat informatique, mieux vaut s'adresser à un expert qui déterminera votre exposition aux risques. En fonction de cela, votre intermédiaire d'assurance – courtier ou agent – évaluera le capital à assurer. Bien sûr, il faut être vigilant aux exclusions, c'est-à-dire les cas où l'assurance ne joue pas. Exemple : les dommages dus à une erreur de programmation sont généralement exclus. Et bien examiner les plafonds de garantie et les franchises

En savoir plus sur
http://lentreprise.lexpress.fr/gestion-fiscalite/responsabilites-assurances/trois-contrats-pour-assurer-son-informatique_1641399.html

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

Source :
http://lentreprise.lexpress.fr/gestion-fiscalite/responsabilites-assurances/trois-contrats-pour-assurer-son-informatique_1641399.html
Par Martine Denoune

Thierry Mandon veut entamer la transformation numérique de l’Etat

Thierry Mandon veut entamer la transformation numérique de l’Etat

Le secrétaire d'État à la Réforme de l'État et à la Simplification, annonce un vaste plan pour accélérer la transformation digitale de l'Etat. Elle passe par plus d'open data, la mise en place de plusieurs projets numériques ou encore la création de « correspondants digitaux » dans les administrations.

2015 sera probablement l'année de grands changements en terme de « numérisation » de l'Etat. Déjà l'année dernière, le gouvernement avait annoncé plusieurs projets concernant le numérique. Nous pensons par exemple à la réorganisation des infrastructures, à la création d'un service interministériel créé par la DISIC ou encore au programme « Dites-le nous une seule fois ». Rappelons également qu'en décembre dernier, Axelle Lemaire avait quant à elle confirmé le lancement « début 2015 » de l'Agence Française du Numérique. Plus globalement, le rapport Lemoine rendu en novembre 2014 donnait lui aussi de nombreuses pistes de réflexion « pour adapter l'économie française à la transformation numérique ».
Les pistes sont donc nombreuses mais le secrétaire d'État à la Réforme de l'État et à la Simplification Thierry Mandon a donné plus de détails sur les chantiers à venir cette année. Le premier « paquet » concerne l'open data avec 4 mesures concrètes :
• L'ouverture des données en « open data » deviendra la « règle générale »
• L'utilisation sera gratuite
• L'utilisation de ces données sera également « conforme aux règles européennes pour certaines redevances »
• De nouveau pouvoirs seront données à l'administrateur général des données pour notamment régler les éventuels « conflits entre administrations »

Transformation numérique et correspondants digitaux
Thierry Mandon veut surtout accélérer la transformation numérique de l'Etat ; un thème qui concerne également les entreprises privés. « Il y a une nécessité de révolutionner le management du changement dans l'Etat », explique-t-il. Car selon lui, la « culture digitale est insuffisamment partagée et comprise dans les administrations » et cela doit entraîner un « programme massif de diffusion de la culture digitale » dans l'Etat.


Thierry Mandon, lors du débat d'orientation pour la stratégie numérique de la France

S'il faut attendre la concrétisation de tous ces projets, il faut d'abord saluer la prise de conscience du secrétaire d'État, qui est déjà en soi une première étape importante à franchir. D'ailleurs, il se livre à une analyse intéressante : « La révolution numérique implique de grands changements pour les grandes entreprises et les grandes administrations. Elles sont encore organisées de manière hiérarchique, autoritaire, quand le numérique impose une vraie démocratisation et des mises en place de politiques publiques, déhiérarchisées. Les grandes organisations ont et auront à piloter cette transformation qui sera longue ».
Pour diffuser cette « culture digitale », Thierry Mandon annonce également la création d'un nouveau statut, celui des « correspondants digitaux ». Ils auront la responsabilité de définir « la mise en œuvre des politiques numériques et de faire l'interface avec les usagers ».

En phase avec le président du Syntec Numérique


Interrogé récemment par nos soins, le président du Syntec Numérique Guy Mamou-Mani saluait « l'excellente orientation prise par Thierry Mandon ». Toutefois, il est aussi amer et critique sur l'usage qui est fait des outils numériques. « L'application de paiement des impôts en ligne est superbe, mais utilisée par 1/3 des foyers fiscaux français. Tout comme MonServicePublic est un outil génial mais sous utilisé. Pourquoi ? », s'interrogeait-il, rappelant que la France est « un pays extraordinaire » en la matière. En 2015, il attend le déploiement de tous ces projets et surtout « un Etat plus léger, moins cher et plus efficace ».

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

Source : http://www.linformaticien.com/actualites/id/35431/thierry-mandon-veut-entamer-la-transformation-numerique-de-l-etat.aspx
par Emilien Ercolani

Après les attentats de Paris – Mesures contre le piratage informatique

Après les attentats de Paris – Mesures contre le piratage informatique

Un groupe se réclamant de l'Etat islamique (EI) a piraté, lundi, le compte Twitter du commandement de l'armée américaine au Moyen-Orient et en Asie centrale (US Central Command, CentCom).
Le #ministère français de la Défense a annoncé avoir renforcé ses systèmes de protection contre les attaques informatiques.

Le ministère français de la Défense a annoncé avoir renforcé ses systèmes de protection contre le piratage informatique quelques jours après les attentats jihadistes de Paris et à la suite d'une dizaine d'attaques dont ses sites internet ont été la cible. Deux de ces attaques « concernaient deux régiments de l'armée de Terre, dont une école », a ainsi déclaré à la presse le vice-amiral Arnaud Coustillière, responsable du pôle cyber-défense à l'état-major des Armées.
Au lendemain de la manifestation monstre, dimanche à Paris, en hommage aux 17 personnes tuées dans les attentats de la semaine dernière, « il a été décidé de monter le niveau de vigilance sur internet » et, « depuis mardi, je dispose d'une cellule de crise pour surveiller » les pirates informatiques, a ajouté le vice-amiral Coustillière. « Nous considérons que c'est une crise comme une autre, nous prenons des mesures de précaution et de vigilance (…) mais on ne peut pas parler de cyber-guerre », a-t-il ajouté, rappelant que le ministère de la Défense a environ 350 sites internet.

LE MINISTÈRE DE LA DÉFENSE VISÉ LE 6 JANVIER
« Les attaques contre le site de la Dicod (service de communication du ministère) continuent, il y a régulièrement des gens qui viennent tester le site de la Dicod », a précisé l'officier. « Pour moi, ces attaques sont la réponse à la manifestation de dimanche dernier, par des gens qui n'adhèrent pas à un certain nombre de valeurs », a-t-il dit.
Le site internet du ministère de la Défense avait déjà été cible le 6 janvier d'une attaque informatique revendiquée par le groupe Anonymous qui affirmait vouloir « venger » le militant écologiste Rémi Fraisse tué en octobre pendant la répression d'une manifestation.
Ces données sont à rapporter au fait que, selon les sources ouvertes et disponibles, mais qui n'émanent pas du ministère de la Défense, il y a eu depuis le 10 janvier de l'ordre de 20.000 attaques en France, par des « groupes plus ou moins structurés ou des hackers islamistes bien connus », contre les sites internet les plus variés, d'écoles, d'institutions, de pizzerias, etc., a ajouté le responsable. Ces attaques se font soit par saturation des sites, soit par pénétration ou « défacement », une opération qui consiste à remplacer la page d'accueil par une autre.

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

Source : http://www.parismatch.com/Vivre/High-Tech/Mesures-contre-le-piratage-informatique-691194

Côte d’Ivoire : Deux caissières d’une agence Western Union épinglée

Côte d’Ivoire : Deux caissières d’une agence Western Union épinglée

L’équipe de la PLCC a épinglé récemment Dames Wamien Ahou Chantal et Oulobo Ahou Véronique, toutes deux caissières d’une maison de transfert d’argent de la place.
L’interpellation fait suite à l’exploitation d’une information anonyme selon laquelle ces dames se sont rendues complices d’un cybercriminel au fait de recevoir de ce dernier par SMS, des codes de transaction. Et ce, en vue de retirer des fonds. La contrepartie de ce concours frauduleux serait qu’elles prendraient 10% et expédieraient le reliquat au cybercriminel via orange money.

Après interrogatoire, les nommées WAMIEN AHOU CHANTAL ET OULOBO AHOU AHOU VERONIQUE ont reconnu sans ambage avoir rencontré un certain nommé GYPY ainsi que les faits qui leur sont reprochés.
De l’acte délictueux, elles ont avoué avoir retiré quatre (04) mandats Western-Union d’un montant total de 1 225 207 FCFA. De cette somme, elles ont également fait l’aveu d’avoir pris 106 000 FCFA et expédié le reste au cybercriminel par orange money.

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

Source : http://www.connectionivoirienne.net/106570/cote-divoire-cybercriminalite-deux-caissieres-dune-agence-western-union-epinglee

L’hôpital cible d’une attaque informatique

L’hôpital cible d’une attaque informatique – 16/01/2015

Châteauroux. Des pirates informatiques s'en sont pris, mercredi soir, au réseau informatique du centre hospitalier. A priori, sans conséquences graves.

» Ce Web dont les djihadistes se servent est aussi un allié »

L'attaque s'est produite mercredi soir. « Nous avons constaté un ralentissement des ordinateurs », raconte Xavier Bailly, directeur adjoint de l'hôpital de Châteauroux. Selon lui, le virus aurait infecté les ordinateurs du centre hospitalier « connectés à Internet ». D'après nos informations, il s'agirait de Trojan Kryptik, cheval de Troie qui aurait la capacité de dérober des données stockées.

« Nos équipes informatiques ont fait le nécessaire auprès des endroits sensibles de l'établissement pour sécuriser certains postes de travail. » Selon lui, le fonctionnement normal des différents services n'aurait pas été impacté. Pourtant, d'après nos informations, le Samu est resté, mercredi, injoignable pendant une quinzaine de minutes.

Cyberdjihadistes contre Anonymous

Hier, le site Internet du centre hospitalier, www.ch-chateauroux.fr, était « temporairement indisponible ». « Les autorités nous ont indiqué qu'une action de malveillance d'envergure aurait peut-être lieu aujourd'hui (lire hier), révèle Xavier Bailly. C'est pourquoi nous avons coupé Internet. »

Hier, l'état-major de l'armée française a annoncé que plus de 19.000 sites Internet français avaient été la cible, ces derniers jours, de cyber attaques similaires. D'après une source proche de l'enquête, celle dont a été victime l'hôpital de Châteauroux a été pilotée depuis l'étranger, sans qu'on puisse encore en définir la provenance exacte.

Cette attaque informatique d'ampleur nationale serait une réponse aux Anonymous, groupe d'hackers activistes qui traquent, depuis l'attentat à Charlie Hebdo, les « cyberjihadistes » sur Internet et les réseaux sociaux. D'après le site Internet Zataz.com, spécialisé dans l'actualité informatique, certaines opérations ont été baptisées : Opération anti France, Opération anti Charlie, Opération Je ne suis pas Charlie, etc.

Ce n'est pas la première fois que l'hôpital de Châteauroux est la cible de pirates informatiques. « Nous avons déploré d'autres actes, il y a huit ou neuf mois », reconnaît Xavier Bailly. La vie des services n'en avait pas été bouleversée.

réactions

» Pas d'autres sites ciblés « , selon la préfecture de l'Indre

Préfecture de l'Indre : « A notre connaissance, il n'y a pas eu d'autres sites ciblés mais il n'est pas exclu qu'il y en ait eu. Il n'y a pas de conséquences importantes pour l'instant. Nous recommandons de mettre régulièrement à jour les systèmes antivirus. »

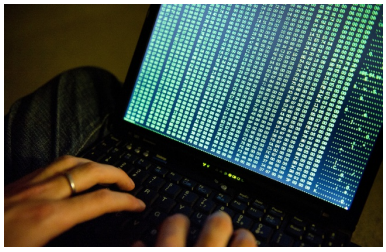
> Philippe Guibon, directeur de la clinique Saint-François : « Nous avons eu un problème serveur, mercredi, mais c'était en interne, cela n'a rien à voir avec une cyber attaque. En revanche, nous avons appris que, dans d'autres régions, des établissements avaient été alertés, dès lundi, d'un risque potentiel d'une attaque, le 15 janvier, pour les sites Internet français. Nous sommes étonnés et un peu inquiets de ne pas avoir été mis au courant. »

> Alexis Rousseau-Jouhennet, chargé de communication de la ville de Châteauroux : « Nous avons, tous les jours, des tentatives d'intrusion. Lundi, l'adresse mail d'un agent communal a été piratée mais cela n'a rien à voir avec les réseaux islamistes. Nous avons une veille informatique permanente. Nous sommes vigilants. »

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

Source : http://www.lanouvellerepublique.fr/Indre/Actualite/Faits-divers-justice/n/Contenus/Articles/2015/01/16/L-hopital-cible-d-une-attaque-informatique-2187330

Sites d'info bloqués: La thèse de la cyberattaque écartée



Sites d'info bloqués: La thèse de la cyberattaque écartée

Ce n’est sans doute pas la grosse attaque promise par les hackers islamistes qui s’en prennent depuis une semaine au Web français, mais le timing interroge. De nombreux sites d’information, dont 20minutes.fr, ont été bloqués une heure et demie ce vendredi matin en raison d’un incident technique chez leur hébergeur Oxalide d’une ampleur a priori inédite.

France Inter, Le Parisien, Slate… et Sushi Shop

Les sites de 20 Minutes, L’Express, Mediapart, France Info, France Inter, Le Parisien, Slate, ZDNet ou encore Marianne, tous hébergés par Oxalide, sont devenus inaccessibles vers 10h. Des sites d’e-commerce, comme Sushi Shop, ont eux aussi été perturbés. Vers 11h30 certains sont redevenus accessibles. «Le niveau actuel d’information ne permet ni d’affirmer que la responsabilité d’Oxalide soit engagée, ni qu’il s’agisse d’un acte malveillant lié à l’actualité», affirmait l’hébergeur un peu avant 13h. Un peu plus tard, il tweetait: «Les premiers éléments en notre possession nous permettent d’écarter l’hypothèse d’une attaque externe de type DDoS.»

Même s’il semble dès lors écarté, le scénario d’une cyberattaque était considéré comme plausible en fin de matinée par les experts en sécurité informatique. «Toutes les caractéristiques techniques d’une attaque par déni de service (DDoS, lorsqu’un site est noyé sous les requêtes de connexion)» étaient réunies, selon Thierry Karsenti, directeur technique Europe de l’entreprise de sécurité informatique Checkpoint. «Il s’agit probablement d’une attaque DDoS», estimait auprès de 20 Minutes Olivier Hassid, directeur général du Club des directeurs de sécurité des entreprises. «Vu les cibles, on peut penser à une attaque virtuelle venant d’islamistes», renchérissait Eric Filiol, expert à l’École supérieure d’informatique, électronique, automatique.

Mercenaires en ligne

Pour Gérôme Billois, expert du cabinet Solucom, «si une attaque par déni de service menée dans le but de nuire à la liberté d’expression était confirmée, on ne serait plus sur du menu fretin.» Car jusqu’ici, les très nombreuses cibles touchées par les hackers tendance islamistes souffraient de failles faciles à identifier souvent causées par un simple défaut de mise à jour logicielle. S’en prendre à l’hébergeur de nombreux sites de presse dénoterait une montée en puissance, peut-être rendue possible grâce à l’achat des services de cybercriminels dotés de véritables moyens.

Car comme le rappellent Gérôme Billois et Eric Filiol, la cybercriminalité est un business en pleine expansion et les hackers s’achètent comme des mercenaires. «Il existe une grille tarifaire», explique Gérôme Billois. «Pour 200 dollars, des sites hébergés en Europe centrale proposent de louer à l’heure 1.000 machines infestées permettant de lancer une attaque DDoS», illustre Eric Filiol. Qu’elle ait lieu aujourd’hui ou plus tard, une attaque contre la presse française serait peut-être moins la preuve d’une montée en puissance des «cyberdjihadistes» que de leur volonté de mettre la main au portefeuille.

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

Source : http://www.20minutes.fr/high-tech/1518695-20150116-sites-info-bloques-incident-technique-attaque-informatique
Par Nicolas Bégasse et Romain Lescurieux

Attentats : les attaques contre les sites Web français

s’intensifient

Attentats : les attaques contre les sites Web français s’intensifient

Si les attaques sont pour le moment limités à du ‘défaçage’, les experts en sécurité craignent que les hacktivistes islamistes changent de braquet ce jeudi. Mais pour le moment, les attaques sont nombreuses mais limitées.

L’escalade des attaques a bien eu lieu. Premiers à réagir, les Anonymous qui ont promis de venger les victimes de Charlie Hebdo avec l’opération #OpCharlieHebdo. Cette offensive des hactivistes a évidemment provoqué une réaction de hackers de l’autre bord, soutenant les islamistes radicaux.
Et ces derniers ont massivement attaqué de nombreux sites Web français de tout ordre (églises, municipalités, universités, hôpitaux…). « Plus d’un millier de sites ont été touchés au total, plus ou moins fortement. Ces sites sont majoritairement de petite taille », explique à l’AFP François Paget, expert chez McAfee. D’autres sources avancent un chiffre de 19.000 sites touchés.

Plus de 1000 sites français cybervandalisés
La plupart du temps, il s’agit de campagnes de «defacement», soit une modification de la page d’accueil des sites visés avec la publication de messages à caractère idéologique. «Il n’y a de Dieu qu’Allah», «Death to France» (Mort à la France) ou encore «Death to Charlie»… Il ne s’agit donc pas d’une cyberguerre (comme certains voudraient le faire croire) mais plutôt de cybervadalisme.
Ces attaques ne sont d’ailleurs pas bien compliquées à mener : « des CMS, des applications Drupal, Joomla, WordPress tout simplement non mis à jour. Des mots de passe un peu trop légers… », commente le spécialiste Zataz.
Mais ces attaques pourraient prendre une nouvelle dimension ce jeudi. « Les revendications initiales parlaient d’un point d’orgue le 15 janvier », indique Gérôme Billois, expert du Cercle européen de la sécurité informatique et consultant pour le cabinet Solucom.
« Ce ne sont bien sûr que des suppositions, mais on pourrait par exemple assister jeudi à l’attaque de sites plus visibles, à des attaques plus groupées, ou à un changement de technique », estime le spécialiste.
A titre préventif, l’Agence nationale de la Sécurité des Systèmes d’information (ANSSI) a envoyé un petit manuel pédagogique dans les ministères, afin de faire le point sur les mesures de sécurité à prendre en urgence tandis que le volet numérique du plan vigipirate aborde les questions de sécurité informatique pour les opérateurs d’importance vitale.
AnonGhost a ainsi revendiqué ce jeudi la publication de coordonnées personnelles d’une dizaine d’employés des ministères des Finances et de l’Intérieur et affirment posséder une base de plus de 10.000 noms. Le collectif MECA (Middle-East Cyber Army revendiquait de son côté trois attaques contre le syndicat Sud Michelin, et l’institut de mathématiques de Toulouse….
Bref, on est encore très loin de la cyberguerre mais « C’est la première fois qu’un pays est confronté à une vague aussi importante de cybercontestation », observe ainsi le vice-amiral Arnaud Coustillière, officier-général de la cyberdéfense.

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

Source : http://www.zdnet.fr/actualites/attentats-les-attaques-contre-les-sites-web-francais-s-intensifient-39812939.htm