Cyberjihadisme : trois sites de ministères français piratés | Le Net Expert Informatique

Cyberjihadisme : trois sites de ministères français piratés

Après TV5 Monde, les sites gouvernementaux. Les portails web du ministère français de la Défense, des Affaires étrangères, de la Culture, mais aussi les sites du Sénat, de l'Organisation de l'aviation civile internationale et de la préfecture maritime de la Manche ont été piratés vendredi.

Les attaques ont été revendiquées dimanche soir, captures d'écran et données personnelles à l'appui, par un groupe intitulé «The Islamic Cyber Army» («Hackers de l'État islamique», NDLR). Ce sont ces mêmes pirates qui avaient revendiqué l'attaque de la chaîne de télévision francophone en avril dernier.
Des listes de noms d'agents publics, leurs coordonnées ou encore leurs adresses mails ont été dévoilées sur les réseaux sociaux tout le long du week-end. L'attaque, qui a commencé vendredi, a été confirmée au Figaro.fr par une source gouvernementale. Selon cette source, «à ce stade aucun serveur des trois ministères n'a été compromis et il n'y a pas eu d'exfiltration de données».

Attaque annoncée

L'opération, baptisée «France under Hacks», avait été repérée dès jeudi dernier par le Centre américain de surveillance des sites djihadistes. Le groupe avait en effet, sur Twitter, menacé «la France» d'un piratage imminent. Le Centre français d'analyse de lutte informatique défensive (Calid), chargé de la cyberdéfense auprès du ministère de la Défense, et l'Agence nationale de la sécurité des systèmes d'information (Anssi) sont toujours en train d'étudier les données volées diffusées sur le web. Il s'agirait d'une attaque bénigne et «plutôt fantaisiste». «Il est très simple de deviner les mails d'un service à partir d'un modèle-type», minimise une source ministérielle.

Source :
http://www.leparisien.fr/faits-divers/cyberjihadisme-trois-sites-de-ministeres-francais-pirates-26-10-2015-5220325.php

A la découverte de Skynet, le programme américain d’assassinats par drones | Le Net Expert Informatique

Un poste de travail à la NSA. (PAULJ.RICHARDS/AFP)

A la découverte de Skynet, le programme américain d’assassinats par drones

Skynet est un programme utilisé pour identifier des membres d'Al-Qaida puis les tuer avec des drones. « Le Monde » révèle en détails comment fonctionne le principe.

Les agents de la NSA ne manquent pas d'humour… noir. Ils ont appelé Skynet, du nom du système informatique incontrôlable de « Terminator », leur programme chargé d'analyser les métadonnées d'appels téléphoniques pour tenter de détecter des activités suspectes. Selon « Le Monde », qui a exploité les documents révélés en avril par Edward Snowden, Skynet a été déployé au Pakistan pour identifier des membres d'Al-Qaida, puis les tuer à coups de drones télécommandés. Le quotidien révèle en détails comment fonctionne ce programme.

Collecter des données sur le mode de vie des cibles

Cela commence par une collecte massive de métadonnées, principalement celles des compagnies de téléphone mobile (lieu, temps de conversation…). Au total, ce sont 80 catégories de données qui sont extraites puis analysées. « L'hypothèse fondamentale est que le mode de vie des cibles à identifier diffère fortement de celui des citoyens ordinaires », écrit « Le Monde ».

Séparer « terroristes » et « innocents » grâce à des algorithmes

Skynet s'appuie également sur la « vérité de terrain », un lot de données dans lequel les utilisateurs de téléphones mobiles ont été classés en deux catégories : « terroristes » et « innocents ». Mais comment savoir qui est terroriste et qui est innocent ? Les documents de l'agence suggèrent que Skynet utilise les données personnelles de membres connus d'Al-Qaida afin d'établir un profil type de terroriste, à lequel est comparé l'ensemble des autres profils.

Une série d'algorithmes produit ensuite un score pour chaque individu, avec un seuil prédéterminé : si le score d'un individu est supérieur au seuil, c'est un terroriste, et si son score est inférieur, il est innocent.

« En fonction des données de la 'vérité de terrain', la NSA s'offre une marge de sécurité en choisissant un seuil garantissant que seul un certain pourcentage de 'terroristes' seront formellement classés comme tels », indique « Le Monde ». Selon les documents divulgués par Edward Snowden, l'agence a choisi 50 % : la moitié des « terroristes » sont des innocents ou des « faux négatifs » ; la moitié des « innocents » sont des terroristes, soit des « faux positifs ».

Des résultats « invalides »

En comparant les données de 100.000 individus à sept téléphones de terroristes connus, la NSA détermine un pourcentage de « faux positifs ». Là où on avait 50% de faux négatifs, l'algorithme détermine finalement 0,18% de faux positifs ou même 0,008 % pour sa version améliorée.

« En réalité, ces résultats sont scientifiquement invalides », note « Le Monde ». « Cette méthode ne permet pas la généralisation souhaitée, car les 100.000 individus sont choisis au hasard, alors que les sept terroristes proviennent d'un lot déjà connu. […] Il aurait fallu mélanger les 'terroristes' à la population générale avant de choisir un échantillon au hasard, mais cela ne serait pas pratique, à cause de leur nombre minuscule – sept au total. »

Cette erreur qui peut paraître insignifiante est en fait très importante : « 0,008 % de la population du Pakistan représente près de 15.000 'innocents' accusés à tort – tandis que, dans le même temps, 50 % des 'terroristes' ne seront pas visés, car leur score est inférieur au seuil fixé arbitrairement ».

On ignore toutefois si tous les individus classés comme « terroristes » par Skynet sont ensuite systématiquement visés par des drones.

Source :
http://tempsreel.nouvelobs.com/les-internets/20151020.OBS7967/comment-marche-skynet-le-programme-americain-d-assassinats-par-drones.html
Par A. S.

Données personnelles : mais à

quoi sert la CNIL ? – Cash Investigation ce mardi 6 octobre 2015 | Le Net Expert Informatique Replay-

	**Données personnelles : mais à quoi sert la CNIL ? diffusion du mardi 6 octobre 2015**

Achetez, vous êtes fichés. Pour mieux cibler les consommateurs, les entreprises ont trouvé la solution : récupérer leurs données personnelles, quitte à violer leur intimité. Pour cela, tous les moyens sont bons, démarchage téléphonique, questionnaires en ligne ou achat de données. Quitte parfois à flirter avec la légalité. La moindre bribe de votre intimité se paie comptant. L'ensemble des données personnelles fournies par un citoyen lambda se vend en moyenne 600 euros et certains fichiers compteraient jusqu'à 30 millions de personnes. C'est aujourd'hui un marché estimé à 300 milliards d'euros.

Des espions partout

En France, l'un des principaux acteurs de ce secteur inconnu du grand public est une filiale de La Poste, l'une des entreprises préférées des Français. « Cash Investigation » révèle que même votre facteur collecte des informations pour constituer ces bases de données qui seront vendues à n'importe quelle entreprise qui le demande.

L'enquête se poursuit à la caisse de votre supermarché. Car il y a des espions dans votre portefeuille : les cartes de fidélité. Celles qui vous permettent de bénéficier de petites ristournes. Grâce à ces cartes, les grandes enseignes recueillent des milliers d'infos sur votre consommation, et donc sur vous : l'historique de vos achats, la liste de tout ce qui remplit votre Caddie chaque semaine, sur plusieurs années. Un pic d'achat de couches pour nourrissons ? Félicitations ! Votre magasin sait qu'un heureux événement est venu élargir votre famille. Une info qui peut aussi intéresser, par exemple, les vendeurs de berlines qui vous proposent leurs nouveaux modèles avant même que vous pensiez en avoir besoin.

Tout le monde paie pour Apple…

Dans ce monde merveilleux du marketing, une entreprise impose sa loi : Apple. Les journalistes de « Cash Investigation » ont eu accès à un document ultraconfidentiel. Sous peine de rupture de contrat, la firme californienne oblige les opérateurs français à privilégier les iPhones et les produits Apple au détriment des concurrents. Même les pubs à la télé sont payées par les opérateurs. Un diktat qui leur coûte très cher : 10 millions d'euros pour SFR, par exemple. Et à la fin, ce sont tous les abonnés qui paient la facture, même ceux qui ne possèdent pas d'appareil de la marque américaine.

Pour le dernier volet de cette enquête, direction l'Indonésie. Dans les quartiers pauvres de Jakarta, de nombreux enfants souffrent de malnutrition. En cause, le lait en poudre que l'on donne aux nourrissons. Il augmente les risques de maladie par rapport à l'allaitement au sein. Les sages-femmes poussent les jeunes mères à nourrir leur bébé avec du lait maternisé, en particulier celui vendu par une filiale du géant français Danone. Une pratique proscrite par l'Organisation mondiale de la santé, et désormais interdite par la loi indonésienne. « Cash Investigation » révèle comment, en échange de séances de formation, de fournitures professionnelles gratuites ou de cadeaux, les sages-femmes se transforment en ambassadrices de la marque. Le marketing n'a décidément pas de limite.

Consultez la vidéo

Même si remplir un formulaire de déclaration à la CNIL est gratuit et enfantin, il vous engage cependant, par la signature que vous apposez, à respecter scrupuleusement la loi Informatique et Libertés. Cette démarche doit d'abord commencer par un Audit de l'ensemble de vos systèmes de traitements de données. Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : http://www.francetvinfo.fr/internet/cash-investigation-donnees-personnelles-mais-a-quoi-sert-la-cnil_1109973.html

40 % des lycéens de l'agglomération de Mont-de-Marsan victimes de cyber-attaques | Le Net Expert Informatique

40 % des lycéens de l'agglomération de Mont-de-Marsan victimes de cyber-attaques

Le résultat est issu d'une étude menée l'an passé par l'Education nationale dans les établissements secondaires de l'agglomération montoise.

Depuis lundi 12 octobre et jusqu'au jeudi 22, le Bureau information jeunesse (BIJ) de Mont-de-Marsan, en lien avec l'Education nationale, pilote une série d'animations collectives inédites autour d'Internet, de ses atouts, mais surtout de ses risques, notamment pour les plus jeunes. Cette opération baptisée @Sans Danger a été imaginée suite aux résultats préoccupants d'un sondage mené l'an passé dans les établissements secondaires de l'agglomération montoise.

D'après cette enquête, plus de 40 % des jeunes interrogés disent en effet avoir été victimes au moins une fois d'une « cyber attaque », et 12 % confient avoir déjà déploré une usurpation d'identité.

Pour aller plus loin, le service scolaire du lycée montois Frédéric-Estève a travaillé avec le BIJ et l'Agence landaise pour l'informatique (Alpi) sur un échantillon de 30 autres élèves. Si 85 % avouent être très actifs sur les réseaux sociaux, 66 % confessent avoir déjà été gênés par des commentaires ou photos mis en ligne.

Autre réalité intéressante, trois quarts des sondés ont « conscience qu'il faut se protéger », notamment en ce qui concerne les données personnelles. Or, aussi actifs soient-ils sur le Web, bien peu d'entre eux savent réellement comment s'y prendre.

Tout le programme de cette « semaine d'éducation cyber citoyenne » est en ligne sur le site de la mairie.

Source :
http://www.sudouest.fr/2015/10/13/mont-de-marsan-40-des-lyceens-de-l-agglomeration-victimes-de-cyber-attaques-2153291-3452.php
par Vincent Dewitte

Les disques durs chiffrés de Western Digital critiqués pour leurs failles de sécurité | Le Net Expert Informatique

Les disques durs chiffrés de Western Digital c

Dans un papier publié le mois dernier, trois chercheurs en cybersécurité se sont penchés sur le chiffrement offert par plusieurs disques durs externes de la marque Western Digital. Les modèles testés sont vulnérables à des attaques permettant de contourner le chiffrement proposé.

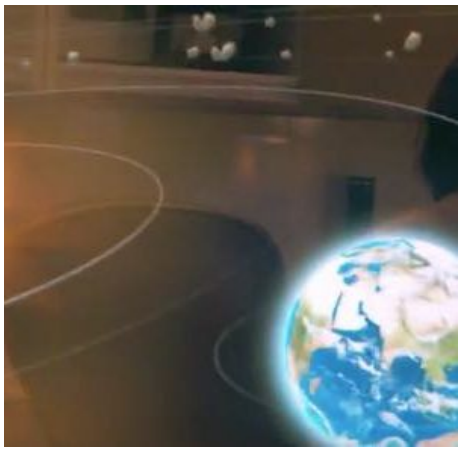
Le chiffrement proposé par les disques durs Western Digital des gammes Passport et My Book souffre de nombreux défauts selon trois chercheurs en cybersécurité. Dans un papier publié il y a un mois, les trois experts se sont penchés sur les conditions d'implémentation du chiffrement dans les différents produits de ces deux gammes de disques durs externes, qui proposent un outil de chiffrement des données stockées sur le disque dur afin d'en protéger l'accès.
Ainsi, la plupart des disques de la gamme proposent un chiffrement s'appuyant sur un mot de passe connu par l'utilisateur. Ce mot de passe est haché grâce à la fonction de hachage SHA256 afin de générer une seconde clef, baptisée DEK (Data Encryption Key), stockée sur le disque et permettant de chiffrer ou déchiffrer les données lors de leur utilisation par l'utilisateur.

Nombreuses erreurs

Mais cette implémentation, étudiée par les chercheurs, souffre de nombreuses vulnérabilités qui rendent possible pour un attaquant expérimenté d'accéder aux données chiffrées sur le disque dur. Ainsi, dans un des modèles analysés, le mot de passe enregistré par l'utilisateur était stocké en clair sur le firmware de l'appareil.
Les chercheurs relèvent également des erreurs dans la génération des chiffres aléatoires utilisés pour le chiffrement des données, qui se basent sur l'horloge interne de l'ordinateur, ou encore la possibilité d'extraire le hash présent sur certains modèles, ce qui ouvre la possibilité d'une attaque par bruteforce. Ces vulnérabilités nécessitent néanmoins que l'attaquant ait physiquement accès au disque dur en question pour pouvoir être exploitées.
Les chercheurs expliquent avoir informé Western Digital des différentes failles trouvées sur les disques durs de la gamme, mais n'avoir aucune information quant à un éventuel correctif prévu par le constructeur.

Source :
http://www.zdnet.fr/actualites/les-disques-durs-chiffres-de-western-digital-critiques-pour-leurs-failles-de-securite-39826890.htm

Démo de Réalité augmentée : Magic Leap fait son show | Le Net Expert Informatique

	Démo de Réalité augmentée : Magic Leap fait son show

Sur le terrain de la réalité augmentée, il y a Microsoft avec ses prometteuses HoloLens… Mais il y a aussi Google qui a massivement investi dans Magic Leap, une start-up spécialisée dans ce domaine.

La firme se propose d'améliorer les interactions des utilisateurs avec les objets virtuels, notamment au niveau des sensations, en travaillant sur la réalité augmentée. L'objectif ? Gommer les frontières sensitives entre perception du réel et du virtuel pour faciliter les interactions entre les deux univers.

Pour ce faire, la société a développé une technologie qui permet de projeter une sculpture de lumière en 3D sur la rétine de l'utilisateur. La solution repose à la fois sur un logiciel et un produit « wearable » complémentaire développé aussi en interne.

Il y a un an presque jour pour jour, la start-up annonçait donc un nouveau tour de table de 542 millions de dollars réunissant Google et Qualcomm. Sundar Pichai et Don Harrison, vices président de Google et Paul E Jacobs, président de Qualcomm, ont rejoint le conseil de direction de Magic Leap. Legendary Entertainment a également mis la main au portefeuille. Web, processeurs, cinéma ; l'activité des investisseurs donne également un cadre au développement futur de Magic Leap.

Aujourd'hui, Magic Leap présente les fruits de sa R&D.

On peut ainsi découvrir dans une vidéo d'une minute (voir en bas de page) un aperçu des technologies développées depuis 2010 où les interactions entre environnement réel et objets virtuels, s'adaptant aux angles de vision et aux perspectives sont clairement démontrées.

Mais la phase de commercialisation est encore lointaine, le travail autour des applications est loin d'être achevé. Microsoft de son côté a annoncé être capable de livrer ses premières HoloLens aux développeurs l'année prochaine pour 3000 dollars.

Source :

http://www.zdnet.fr/actualites/realite-augmentee-magic-leap-fait-la-demo-de-sa-techno-39826910.htm

Facebook : vous serez prévenu en cas de piratage par un Etat. Vraiment ? | Le Net Expert Informatique

Dans un post de blog, le RSSI de Facebook, Alex Stamos, indique que le réseau social préviendra les utilisateurs qu'il soupçonne d'être victimes d'une cyberattaque perpétrée par un groupe étatique. Une politique que Google avait déjà mise en place sur ses services.

Facebook souhaite renforcer la sécurité des données personnelles des utilisateurs et annonce, dans un post de blog signé par son RSSI, son intention de signaler les tentatives de piratage menées par des groupes liés aux gouvernements contre les utilisateurs de ses services. Une notification spécifique sera ainsi affichée sur les comptes répondant aux critères retenus par Facebook, invitant les utilisateurs à activer l'authentification double facteur proposé par le site.

Facebook propose déjà des alertes dans les cas où il soupçonne une authentification frauduleuse : ainsi, quand l'utilisateur se connecte depuis une adresse IP différente, celle-ci est notifiée sur le compte. L'authentification à double facteur empêche entièrement de se connecter depuis une IP inconnue de Facebook si l'utilisateur n'est pas en mesure d'entrer un code que le service envoie sur son téléphone.

Un air de déjà vu?

Beau geste de la part de Facebook, mais le réseau social reste particulièrement avare en terme de précisions. Ainsi, Facebook ne communique pas sur les critères qu'il retient pour déterminer l'implication d'un gouvernement dans le piratage d'un compte : la tache n'a pourtant rien d'aisé tant on sait que l'attribution des cyberattaques est une science qui n'a rien d'exact. Alex Stamos explique ainsi que ces critères sont tenus secrets pour « protéger l'intégrité de nos méthodes » mais que ces notifications ne seront utilisées que dans les cas « où les preuves viennent fortement appuyer nos suppositions. »

On peut également s'interroger sur la mise en place d'un système à deux vitesses : il paraît évident que Facebook notifiera un utilisateur américain victime d'un piratage d'origine chinoise ou russe, mais en fera-t-il autant pour un citoyen russe victime d'un piratage orchestré par la NSA ? Difficile à dire, Facebook reste peu disert sur la question.

La mise en place de cette mesure par Facebook est en tout point similaire à ce qu'avait déployé Google en 2012 : chez le géant du moteur de recherche, on se garde également de mentionner les critères retenus pour qualifier l'attaque et on pousse l'utilisateur à mettre en place un mécanisme d'authentification à deux facteurs.

Source :
http://www.zdnet.fr/actualites/facebook-vous-serez-prevenu-en-cas-de-piratage-par-un-etat-vraiment-39826746.htm

---

En France, les cyber-attaques

sur les entreprises explosent | Le Net Expert Informatique

	En France, les cyber-attaques sur les entreprises explosent

Les entreprises françaises ont subi en moyenne 21 incidents de cybersécurité par jour en 2015. C'est 51% de plus qu'il y a un an selon une étude mondiale du cabinet PwC.

La menace représentée par les cyberattaques sur les entreprises se précise alors que le gouvernement va présenter avec l'Anssi (Agence nationale de la sécurité des systèmes d'information), une charte pour la sécurité des emails signée par cinq fournisseurs de services de messagerie, une étude mondiale révèle l'ampleur du problème.
Selon l'étude The Global State of Information Security Survey 2016 réalisée par le cabinet d'audit et de conseil PwC, en France, le nombre de cyber-attaques recensées a progressé à hauteur de 51% au cours des 12 derniers mois.
Cette explosion est supérieure à la hausse constatée au niveau mondial, le nombre de cyber-attaques visant les entreprises ayant progressé de 38% en 2015.
Cette étude, qui recense la façon dont plus de 10.000 dirigeants dans 127 pays gèrent la cybersécurité dans leurs organisations relève également que ces derniers ont augmenté leur budget pour lutter contre la cyber-criminalité
Au niveau mondial, ces budgets ont augmenté de 24%, renversant la tendance baissière de l'année dernière.

PwC – Le budget moyen de cybersécurité des entreprises françaises interrogées s'est établi à 4,8 millions d'euros par entreprise en 2015, soit un budget en hausse de 29% par rapport à l'année dernière

Le budget moyen de cybersécurité des entreprises françaises interrogées s'est établi à 4,8 millions d'euros par entreprise en 2015, soit une hausse de 29%, plus élevée que celle constatée au niveau mondial.
Ce chiffre est à comparer avec le niveau estimé des pertes financières liées à des incidents de cybersécurité, soit en moyenne à 3,7 millions d'euros par entreprise en France, soit une augmentation de 28% par rapport à 2014.

Le piratage de la chaîne TV5 Monde aurait ainsi coûté plus d'une dizaine de millions d'euros.
En France comme dans le monde, la source des menaces reste majoritairement interne aux entreprises. Cependant les sources de cyber-attaques qui ont progressé le plus en 2015 sont, elles, externes aux entreprises.
Le fait saillant tient au fait que la responsabilité des fournisseurs et des prestataires de service actuels est de plus en plus invoquée dans la progression de ces incidents informatiques.

« Ce qui ne peut être protégé, peut être assuré »
Cette responsabilité est en hausse d'environ 32% pour les fournisseurs et de 30% pour les prestataires de services. Cela est dû au fait que les entreprises travaillent de plus en plus en collaboration avec des partenaires commerciaux et industriels externes, ce qui accroît les « portes d'entrée » pour le piratage informatique.
Selon Philippe Trouchaud, associé chez PwC, « Les chiffres indiquent qu'une entreprise française sur 5 pense que ses concurrents sont potentiellement à l'origine de certaines attaques subies en 2015. En effet, ces derniers sont particulièrement attirés par les données de type propriété intellectuelle, les business plans, les données de R&D, etc ».
« Ce qui ne peut pas être protégé peut être assuré », note PwC, qui estime que le marché mondial de la cyberassurance (pour atténuer les effets financiers d'une cyberattaque) va tripler d'ici 2015, à 7,5 milliards de dollars.

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source :
http://bfmbusiness.bfmtv.com/entreprise/en-france-les-cyber-attaques-sur-les-entreprises-explosent-922703.html
Par F.Bergé

Le premier procès contre un data center s’ouvre aujourd’hui | Le Net Expert Informatique

Le procès qui s'est ouvert jeudi 1er octobre devant le tribunal administratif de Montreuil (Seine-Saint-Denis) est une première : il pose la question de la croissance effrénée des centres de données numériques, dit « data centers », en agglomération et notamment en région parisienne. Le collectif Association Urbaxion'93 s'attaque en effet à Interxion, l'un des géants de cette activité en pleine expansion. « Nous demandons l'annulation de l'autorisation d'exploiter du data center de la rue Rateau, à La Courneuve, en raison d'une irrégularité de l'enquête publique et d'insuffisances dans l'étude d'impact », explique Roxane Sageloli, avocate du Cabinet Huglo-Lepage et Associés, spécialisé dans le droit de l'environnement et de l'urbanisme.

Inauguré le 29 novembre 2012, le vaste bâtiment de 9.000 m2 aux allures d'entrepôt crée des nuisances permanentes aux riverains installés, pour les plus proches, à une dizaine de mètres seulement de la longue façade grise et sans fenêtre. « Il fait du bruit en permanence et a été implanté sans concertation suffisante avec la population, presqu'à notre insu en fait », dénonce Matilda Mijajlovic, l'une des habitantes de la rue Rateau à l'initiative de la création du collectif.

Vue de la rue Rateau et de son data center sur GoogleEarth.

Si le bâtiment est bruyant, c'est parce qu'il faut refroidir les centaines de serveurs informatiques qu'il abrite et qui fonctionnent 24 heures sur 24 et 365 jours par an. Mais le plus grave est ailleurs : 580.000 litres de fuel sont stockées dans des citernes servant à alimenter les huit générateurs nécessaires au fonctionnement de l'installation. « Ces générateurs produisent 76 MW d'électricité, ce qui équivaut à la consommation d'une ville de 50.000 habitants », détaille Khadija Aït Oumasste, autre membre du collectif, qui habite également rue Rateau. Le bâtiment abrite en outre 8 salles de batteries au plomb reliées entre elles.

Les data centers pourraient consommer autant d'énergie qu'un million d'habitants

Pour le Conseil d'architecture, d'urbanisme et de l'environnement de Seine-Saint-Denis (CAUE 93), un organisme qui conseille les collectivités locales, le data center de la rue Rateau représente un danger pour le quartier, non pas par son activité propre, mais par la quantité de fioul qui y est stockée et par la présence de batteries de sauvegarde implantées sur le site et à proximité des habitations. « Cette activité n'est pas compatible par sa "nature" avec le caractère résidentiel du quartier et il est de nature à porter atteinte à la sécurité publique », écrit le directeur du CAUE 93 dans un courrier adressé au collectif.

Cette prise en compte de la sécurité des riverains est au cœur de la contestation. Le procès intenté à Interxion est d'autant plus important qu'il s'agirait du premier procès de ce genre. « Nous exploitons des failles du dossier, notamment le fait que les risques d'incendie et d'explosion n'ont pas été suffisamment pris en considération. Mais on ne peut pas implanter d'installations aussi importantes que ce type de data centers aussi près d'habitations », s'insurge Roxane Sageloli.

Outre les nuisances et le risque, le choix des technologies et leur impact écologique sont également au cœur du problème. Les data centers du Grand Paris pourraient en effet consommer en 2030, si rien n'est fait pour les freiner, autant qu'une ville d'un million d'habitants, selon Daniel Thepin, auteur d'un rapport pour l'Institut d'aménagement d'Ile-de-France, cité dans un article de la Tribune.fr.


Khadija Aït Oumasste et Matilda Mijajlovic, habitantes de la rue Rateau
et membres du collectif Association Urbaxion'93.

La communauté d'agglomération Plaine Commune, qui regroupe notamment, au nord de Paris, La Courneuve, Aubervilliers et Saint-Denis, est ainsi devenue, selon Daniel Thepin, le paradis des data centers, avec la plus forte concentration en Europe sur un territoire.

Pour sa part, Interxion a prévu de doubler la capacité du centre de stockage de la rue Rateau en construisant un bâtiment similaire. Et il projette de construire un autre data center de 44.000 m2 en plein centre de la Courneuve. « Notre action semble avoir retardé la phase 2 de l'installation de la rue Rateau, mais quid de ce data center géant ? » interroge Matilda Mijajlovic. Elle affirme qu'aucun des 400 emplois annoncés dans le journal de Plaine Commune pour la création de la phase 1 n'a vu le jour.

Source : http://www.reporterre.net/Le-premier-proces-contre-un-data-center-s-ouvre-aujourd-hui

Daech se forme au piratage : « Le risque, c’est un cyber-11-Septembre » | Le Net Expert Informatique

	**Daech se forme au piratage : « Le risque, c’est un cyber-11-Septembre »**

Le groupe islamiste aurait tenté de pirater les firmes énergétiques américaines, avec dans l'idée de produire des black-out. Il n'a pour l'instant pas réussi.

La chaîne de télévision raconte que Daech a tenté (en vain) de pirater des firmes énergétiques américaines lors d'une grande conférence organisée la semaine dernière. Toutefois, le groupe islamiste utilise des outils de piratage dépassés, incapables de pénétrer dans les systèmes pour les couper ou les faire exploser.

L'intention est forte, heureusement les capacités sont faibles », commente à CNN John Riggi, responsable de la division cyber au FBI. « Mais, nous restons préoccuper s'ils achètent plus de capacités. »

En effet, il existe un important marché noir pour les outils de piratage. Un logiciel malveillant se vend ainsi entre 12 et 3.500 dollars, selon la firme de sécurité Symantec. Avec le bon arsenal et en apprenant à exploiter les failles de sécurité, l'Etat islamique pourrait s'introduire dans les systèmes des fournisseurs d'énergie américains.

Vers un « cyber-armageddon » ?

Le réseau électrique américain présente la particularité d'être essentiellement mécanique, alimenté par 7.000 centrales, 700.00 kilomètres de lignes à haute tension et 3,5 millions de lignes de raccord… Le tout sert 150 millions de foyers, via 3.300 sociétés différentes. Cette infrastructure, vétuste et obsolète, a déjà montré des failles, à savoir la multiplication des black-out ces dernières années dans les grandes villes, y compris New York. Ainsi, en 2013, à Cookeville (Tennessee), le simple passage d'un raton-laveur dans une installation électrique a produit une boule de feu, privant 6.000 Américains d'électricité pendant 24 heures…

Les Etats-Unis disent depuis longtemps redouter des cyber-attaques sur son réseau électrique (et sur l'ensemble de ses infrastructures, toutes faibles), craignant un « cyber-armageddon » ou un « cyber Pearl Harbor » qui mettrait à bas l'ensemble du pays. L'intérêt de Daech pour le système donne déjà des sueurs froides aux autorités américaines. Une cyber-attaque qui réussirait à s'introduire dans le système pourrait ainsi couper le courant dans de larges régions du pays, voire pourrait faire exploser les machines pour un black-out durable.

Un somme un « cyber-sabotage » qui porterait la marque de l'organisation islamiste. Dès 2013, l'ancien directeur de l'Anssi, Patrick Pailloux (aujourd'hui à la DGSE), prévenait « l'Obs » :

Ma plus grande crainte concerne le cybersabotage, c'est-à-dire l'introduction dans un système pour le saboter, soit une utilisation quasi militaire de l'informatique. A la manière de ce qu'on a vu en Iran avec le virus Stuxnet. »

En 2010, Stuxnet, un programme malveillant, sans doute coproduit par les services américains et israéliens, a été introduit dans les systèmes informatiques contrôlant les centrifugeuses iraniennes qui enrichissent l'uranium nécessaire à la fabrication de l'arme atomique.

« Le risque d'un cyber-11-Septembre »

« Le risque de demain, c'est un cyber-11-Septembre », a lancé en début d'année le député socialiste Eduardo Rihan Cypel, co-auteur du dernier Livre blanc sur la défense et la sécurité nationale.

La possibilité que des terroristes s'emparent des outils informatiques pour lancer « une cyberattaque massive » ne relève plus du fantasme. « Il faut se préparer à tous les scénarios possibles, jusqu'à des attaques massives financées par des groupes terroristes », estime le lieutenant-colonel Eric Freyssinet, chef de la division de lutte contre la cybercriminalité. Avant d'ajouter :

Malheureusement, les groupes terroristes ont de l'argent. Il n'y a qu'un pas pour qu'ils se munissent de cyber-armes, surtout qu'il n'y a pas besoin de beaucoup de moyens humains pour les utiliser, quelques dizaines de personnes suffisent pour lancer une attaque massive. »

Inquiétant. Pour autant, les officiels américains se veulent rassurant sur une éventuelle cyber-attaque contre le réseau électrique. Selon les autorités, citées par CNN, il faudrait des capacités techniques importantes pour comprendre le fonctionnement de l'infrastructure acheminant l'énergie, et encore plus pour la saboter. Surtout que l'ensemble est désormais surveillé par le FBI, mais aussi la CIA et la NSA.

Source :
http://tempsreel.nouvelobs.com/tech/20151019.OBS7872/daech-se-forme-au-piratage-le-risque-c-est-un-cyber-11-septembre.html
Par Boris Manenti