Risques informatique : « Jusque-là, on nous prenait pour des paranos »

	Risques informatique : « Jusque-là, on nous prenait pour des paranos »

Non, même au Forum international de la cybersécurité, les experts ne hurlent pas à la cyberguerre. Leur secteur reconnu, ils restent modérés sur la menace… tout en profitant des récentes attaques.

Au FIC 2015, à Lille (Andréa Fradin/Rue89)

Se balader dans les travées du FIC, le Forum international de la cybersécurité qui se tenait à Lille ces 20 et 21 janvier, a de quoi faire flipper.
Partout, des bannières en rouge et noir ; l'une avec un gros masque d'Anonymous, l'autre reconstituant une scène de crime, rubans policiers jaunes barrant l'accès, non pas à des corps mais à des serveurs.

Des bannières aperçues sur les stands du FIC 2015 (Andréa Fradin/Rue89)

Des écrans diffusant des films où clignotent « Heartbleed », « Stuxnet » (noms des dernières vulnérabilité et attaque célèbres), dans des environnements rappelant les nanars hollywoodiens dans lesquels de petits-génies-mais-méchants-hackers lancent une opération hyper sophistiquée contre une banque, ou un organisme gouvernemental.

Au FIC 2015, à Lille (Andréa Fradin/Rue89)

En plus de l'ambiance anxiogène, s'étalent aussi tout autour de moi des termes imbitables, des anglicismes techniques qui rappellent un peu les pubs pour le shampoing, où pro-vitamine B5 et revitalisants sont remplacés par « Net HSM » et « audit de SSI ».

La France, ses fromages, sa cybersécurité…
Les noms des entreprises de sécurité informatique, et des produits qu'elles vendent, sont tout aussi carabinés : Stormshield Network Security, Arkoon, Netasq, TrustWay Proteccio, Prim'x Technologies… Sur scène, les représentants de ces sociétés défilent tout sourire, manipulant à merveille, et sans sourciller, ces intitulés barbares.
Tous viennent de recevoir un label des mains de la secrétaire d'Etat en charge du numérique Axelle Lemaire – le label « France cybersécurité » –, « l'AOC » en la matière, se réjouit un homme. Qui ajoute :
« La France était connue pour ses fromages et ses vins, elle le sera désormais pour la cybersécurité. »

Les lauréats du label France cybersécurité (Andréa Fradin/Rue89)

Des hommes, revenons-y, il n'y a d'ailleurs que ça sur scène : sur vingt lauréats, costumes sombres, coupe sage, seule une femme est montée recevoir le fameux trophée en verre dont je ne comprends pas l'utilité.

Des képis partout
Tout ce petit monde, en revanche, semble très bien comprendre. Et très bien se connaître. Dans les salles et les travées du FIC, tout aussi masculines, on se donne du « tu », on vanne sur des termes techniques tout aussi alambiqués que l'intitulé des sociétés auxquelles on appartient, on connaît le travail du voisin installé sur le siège d'à côté. Et ce, même quand son badge indique un mystérieux « ministère de la Défense ».

Des militaires, au FIC 2015, à Lille (Andréa Fradin/Rue89)

C'est d'ailleurs l'une des particularités de cet événement annuel : aux côtés des ingénieurs et informaticiens d'Airbus, Thales, Orange, Atos, et bien d'autres petites entreprises inconnues du grand public, figurent des policiers, des militaires, des gendarmes. C'est d'ailleurs eux, en grande partie, qui sont à l'origine du Forum : co-organisé par la Gendarmerie nationale, le FIC a été fondé par un général d'armée, Marc Watin-Augouard.

Des gendarmes, au FIC 2015, à Lille (Andréa Fradin/Rue89)

La cybersécurité, arme et bouclier des temps modernes, se niche quelque part à la frontière entre intérêts étatiques et objectifs de grands groupes industriels. Dans ce drôle de territoire, on parle le même langage, on opine sur les mêmes remarques.
Je ne comprends pas la moitié des références, je ne parviens pas à déchiffrer les sigles et acronymes qui pullulent ici.

« J'en veux quand même aux journalistes… »
Pas facile, vu comme ça, de saisir le petit monde de la sécurité informatique. Pourtant, il est au cœur de l'actualité.
Il y a bien sûr #OpFrance, l'opération menée ces derniers jours contre des sites internet français par des attaquants se revendiquant d'organisations islamistes. Il y a aussi eu cet incident, chez un hébergeur, qui a fait sauter bon nombre de sites d'informations en France. Et avant ça : Sony Pictures piraté, photos intimes de stars dérobées, vols de comptes et de mots de passe… Pas une semaine sans qu'une attaque informatique ne fasse les gros titres de la presse. Même chose dans les discours des hommes politiques :

« Pas un forum international sans que le mot cyber ne soit prononcé », résume le patron de l'Anssi, l'agence gouvernementale précisément en charge de la cybersécurité de la France, Guillaume Poupard.

Et l'effet se ressent directement sur le secteur.
Tous, au FIC, me confient n'avoir jamais vu une telle affluence, un tel intérêt des profanes (journaliste, grand public, politiques, petites entreprises qui débarquent sur Internet) pour leur matière.

Sur scène, un expert lance :
« Il faut parler le langage normal des entreprises […]. Etre ergonomique, simple d'utilisation ! »

Entre deux ateliers, deux autres chambrent la presse :
« J'en veux quand même aux journalistes, et à leur traitement de cette actualité…
– Il faut leur expliquer en moins de deux syllabes ! »

Les effets de la petite phrase de Cazeneuve
Cet impératif, le ministre de l'Intérieur Bernard Cazeneuve l'a lui-même sommé en ouverture du Forum, par une petite phrase par la suite énormément commentée :
« La lutte contre les cybermenaces ne peut plus être réservée au cénacle élitiste de quelques experts. »

Le stand Hexatrust, au FIC 2015, à Lille (Andréa Fradin/Rue89)

Pour le secteur, c'est à la fois une aubaine et une malédiction. Une aubaine, car l'ouverture de ces thèmes au grand public leur assure une visibilité dont ils n'ont jamais bénéficié. Une reconnaissance aussi. Dans les allées, nombreux sont ceux qui m'ont confié :

« Jusque-là, on nous prenait pour des paranos. »

Les cyberattaques, souvent invisibles, sont une menace floue, impalpable. Les échos que la presse et le monde politique donnent aux incidences directes et concrètes de ce risque le rendent forcément plus immédiat.

Et facilite aussi le business : gros bonnets du CAC 40 et PME de la région sont venus faire le tour des exposants du FIC.

Des clients : « Ça ne m'arrivera jamais ! »
Bien sûr, les réticences existent toujours :
« Les clients nous disent : "Ça ne m'arrivera jamais !" »
« Ils ne voient pas en quoi ils sont concernés jusqu'à ce que ça touche un concurrent direct. »
Et les contrats, contrairement à ce que souhaitait Axelle Lemaire (« J'espère que les contrats se signent ! ») ne se font pas en un tournemain. Certains représentent un investissement de dizaines, de centaines de milliers d'euros, voire de millions pour un « package complet » sécurisant tous les postes d'une grosse boîte :
« Il faut entre 12 et 24 mois pour signer un contrat. »
Mais oui, l'intérêt est là.

Le stand du ministère de l'Intérieur, au FIC 2015, à Lille (Andréa Fradin/Rue89)

Mais l'ouverture est pour certains synonyme de trahison. D'abandon de la connaissance éclairée au profit d'intérêts commerciaux, ou de récupération politique, forcément trop simplistes.

« Bienvenue au Fric ! Euh, au FIC ! »
Un participant note le fossé existant entre les prises de parole en plénière, investie par les politiques, et les ateliers, où l'on parle concret : comment fait-on une enquête lors d'une attaque utilisant malgré elle des milliers de machines infectées par un logiciel malveillant ? Comment la coopération entre les agences chargée de la cyberdéfense s'établit en Europe et dans le monde ?

Un autre, pourtant lui-même exposant, se rappelle :
« Avant ce n'était pas comme ça. Au début, il n'y avait que des képis. Aucun sponsor, aucune marque. C'était plus confidentiel mais moins marketing. Le salon n'a jamais été aussi grand que cette année. »

Au FIC 2015, à Lille (Andréa Fradin/Rue89)

Au matin du 20 janvier, juste avant les préliminaires officiels menés par Bernard Cazeneuve, Pierre de Saintignon (vice-président du conseil régional du Nord-Pas-de-Calais) provoquait l'hilarité de la salle en lançant :
« Merci pour votre présence à cette septième édition du Fric ! Euh, du FIC ! »

Lapsus révélateur de l'un des paradoxes qui traverse le secteur : tous reconnaissent bien sûr qu'il faut faire du business. Mais en aparté, chacun concède aussi que parfois, ça va trop loin :
« Certains en font des tonnes pour vendre leurs produits ! »
« Il faut démystifier, il y a de l'expertise, mais comme partout ! Ça ne sert à rien d'utiliser des mots compliqués, la cybersécurité, c'est simple ! »

Le petit dernier du business de la peur
D'eux-mêmes aussi, ils reconnaissent le business de la peur, souvent reproché au secteur. Cette méthode commerciale, que les initiés désignent aussi par l'acronyme FUD, pour « Fear, Uncertainty and Doubt » (« peur, incertitude et doute »), est classique dans les professions qui vendent des solutions censées protéger de tel ou tel danger.

Elle consiste à grossir le danger en question, à le rendre plus imminent, plus inévitable et plus dommageable qu'il ne l'est vraiment. On le retrouve partout : dans le business des alarmes, des assurances, et désormais de la cybersécurité.

Au FIC 2015, à Lille (Andréa Fradin/Rue89)
Dans les boîtes de sécurité informatique, personne ne nie le problème, ou n'esquive la question quand je l'aborde. Certains reconnaissent même en faire un peu, ironisant sur le service marketing qui fait parfois un peu de buzz sur une attaque. Beaucoup affirment, quand je souligne dans un sourire que les discours alarmistes profitent à la bonne santé du secteur, que ce n'est pas si simple. Tel cet exposant :
« C'est positif dans une certaine mesure : s'il y a une peur, alors il peut y avoir une prise de conscience.
Mais il y a aussi le risque que les gens aient trop peur, et disent : "Finalement, vos produits ne servent à rien, puisque les attaques passent de toute manière." »

Malaise autour du mot « cyberguerre »
L'exemple de la prétendue cyberguerre est à ce titre saisissant : là encore, très peu de participants au FIC utilisent ou légitiment ce terme, que l'on retrouve pourtant de plus en plus souvent dans les médias. Au contraire, la grande majorité se montre très prudente avec ce concept. Et l'ambiance générale ne laisse pas franchement penser à un état de siège.

Au stand des principaux intéressés, les représentants de la Défense sont assez mal à l'aise dès que j'aborde le sujet. Et me dirigent vers la parole officielle, celle du contre-amiral Arnaud Coustillière, officier général de la cyberdéfense, cette « quatrième armée pour un quatrième espace », depuis 2011. Ce dernier ne parle pas de cyberguerre, et se refuse à tout catastrophisme.

Un autre ajoute : « De la peur, procède la paralysie. »

Le stand du ministère de la Défense, au FIC 2015, à Lille (Andréa Fradin/Rue89)

De même, tous s'accordent à minimiser les attaques de ces derniers jours, qualifiées de « simples graffitis » par le directeur de l'Anssi. Les experts en rigolent, assurent que ces attaques sont consubstantielles au Web. De même, ou presque, que les solutions pour s'en protéger. Certains vont jusqu'à dire :

« A la limite, si des sites tombent sous ces attaques, tant pis pour eux. Ils l'ont bien cherché, ils ne se sont pas protégés. »

Extrait d'une vidéo diffusée au FIC 2015, à Lille (Andréa Fradin/Rue89)

Pourtant, ce sont bien ces attaques qui font la une des journaux, de même que ce sont bien elles qui se retrouvent citées en exemple dans le discours politique. Le décalage entre les confidences de ceux qui vivent de la cybersécurité et l'image qui en ressort dans le grand public me déstabilise.

« Human after all »
Ce n'est d'ailleurs pas le seul grand écart : bien loin de l'image des attaques hyper complexes élaborées dans des cervelles de cybercriminels machiavéliques, bien loin des termes techniques qu'ils choisissent eux-mêmes pour désigner leurs produits et leurs sociétés, les experts en cybersécurité s'attachent à m'expliquer que leur domaine n'a finalement rien de compliqué.

Au FIC 2015, à Lille (Andréa Fradin/Rue89)
Qu'au-delà des solutions techniques, du modus operandi des cyberattaques, la cybersécurité se rapporte avant tout à l'humain, au bon sens, et à la gestion des risques :

« La gestion des risques, on en fait tous les jours. Quand on traverse la route, on fait de la gestion de risques : on regarde à droite, à gauche, on détermine s'il est dangereux de traverser à ce moment-là. Pareil avec les incendies. C'est la même chose ici. »

Et que les intrusions informatiques, même les plus spectaculaires, relèvent le plus souvent d'imprudence humaine : le fait de brancher une clé USB trouvée par hasard dans son entreprise, le fait de ne pas protéger d'un mot de passe les caméras de son réseau de surveillance (souvenez-vous de notre enquête à ce sujet…).

De l'eau qui file entre nos doigts
Finalement, je m'attendais à des cris d'orfraie sur la menace permanente et la guerre imminente, mais passés les visées marketing et politiques, j'ai avant tout eu droit à des discours modérés. Je m'attendais à être noyée sous la technique, mais passés les slogans publicitaires, j'ai eu du bon sens.

Entre impératifs commerciaux, récupération politique et réputation à tenir, le monde de la cybersécurité ne fait finalement que jongler avec ses paradoxes. Et en même temps, comment pourrait-il se débarrasser de ces forces contradictoires ? Etat, industriels, experts : les corps qui composent l'univers cybersécuritaire existent parce qu'ils prétendent pouvoir apporter une solution à un problème pourtant fondamentalement insolvable.

Dans les cyberattaques, Etats et individu isolé jouent désormais à armes égales. Avec Anonymous et d'autres, la notion d'organisation nébuleuse n'a jamais eu autant de sens. Et quand une enquête s'ouvre enfin pour déterminer l'origine d'une action malveillante, il est quasiment impossible de remonter à la source : une preuve a beau avoir été obtenue (une adresse IP, par exemple), cette dernière peut en fait s'avérer être une fausse piste. Et toute l'énergie mobilisée pour l'identifier (contacter le pays d'origine, attendre un accord de coopération qui ne vient parfois jamais…) doit être regénérée pour se déporter sur un autre pays, où l'on pourra peut-être encore faire chou blanc.

La cybersécurité revient donc un peu à essayer d'attraper de l'eau entre ses doigts. A appréhender un espace de pur mouvement, sans frontières, avec des termes, des codes, des normes forcément déjà obsolètes et inadéquates. C'est un ouvrage sans cesse détricoté, c'est Sisyphe en réseau. Et bien sûr, les acteurs qui s'évertuent à trouver des réponses ne peuvent se présenter sous ce jour.

Bruce Schneier, pape de la cybersécurité américain et guest star du FIC 2015, déclarait lors de sa conférence :
« La résilience est la clé de la sécurité informatique. […] Comment on se débrouille ? Comment on s'adapte ? Comment on survit ? »
C'est drôle : la résilience, cette capacité d'adaptation aux altérations, est précisément ce qui définit Internet.

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

Source : http://rue89.nouvelobs.com/2015/01/23/forum-cybersecurite-jusque-prenait-paranos-257257
Par Andréa Fradin

Le danger de la société du Big Data

Le danger de la société du Big Data

Pour comprendre le monde de demain, il faut garder en tête une seule date : l'année 2002 ! C'est durant l'année 2002 que nos sociétés ont produit pour la première fois plus de données que l'humanité depuis sa création.

C'est fou mais aujourd'hui et demain davantage encore, tous les objets qui nous entourent communiqueront entre eux et donneront une foule d'informations numériques sur nous. Il y aura des puces insérées dans nos matelas qui mesureront nos cycles de sommeil, nos frigos qui nous alerteront sur les produits périmés ou les courses à faire, sans oublier nos puces bancaires qui sont déjà dans nos smartphones et qui mesureront le moindre achat ou paiement, que ce soit pour s'alimenter ou payer un parking. Bref, toutes ces données numériques, ces datas comme disent les professionnels, rendront notre vie transparente et nous serons nus comme des vers pour ceux ou celles qui détiendront ces informations, ces fameuses datas.

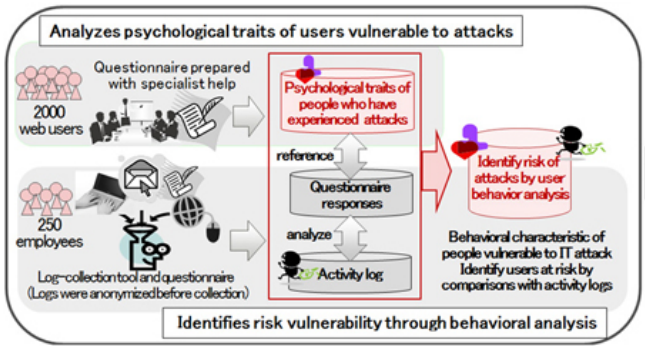
Tous les objets qui nous entourent communiqueront entre eux et donneront une foule d'informations numériques sur nous.

Aujourd'hui, personne n'en a cure, car bien souvent, on se dit que les informations qui sont données (ou seront données demain) sont inoffensives, voire même nous aident à vivre mieux. C'est vrai, par exemple, quand c'est une brosse à dents qui nous avertit que notre hygiène buccale laisse à désirer, c'est vrai aussi lorsqu'une puce, glissée sous notre peau, nous donnera de précieuses indications sur notre état de santé.
Tout cela et bien d'autres choses encore sont vraies mais pour autant, ce business du Big Data est également porteur de dangers… Et là, visiblement à part quelques intellectuels, personne ne semble s'en soucier. Qui peut dire si demain, notre mutuelle, notre banquier ou notre assureur ne regardera pas toutes ces données sur notre santé pour traquer les mauvaises habitudes des fumeurs, des buveurs, de ceux et celles qui mangent trop gras, ou trop salé ou qui ne sont pas abonnés à une salle de sport ou que sais-je encore.
Il ne faut pas se leurrer, la tentation sera trop grande pour ces assureurs ou ces banquiers de nous appliquer un tarif individualisé, un tarif en fonction de notre profil de risque exact. Si c'est le cas, c'est un changement de société radical qui s'annonce ! Cela serait la fin de la mutualisation des risques comme l'indique le journal Les Echos. En clair, les moins chanceux seront laissés au bord du chemin, sans couverture d'assurance ou alors à un tarif impayable.
Le danger de cette société du Big Data, c'est que si demain tout le monde se sent épié, plus personne n'osera prendre des risques… Cela sera une société immobile, que nous fabriquerons sans le savoir. C'est la raison pour laquelle, je le dis souvent, nous ne sommes pas seulement en crise, nous sommes dans une société en pleine mutation. Et nous percevons pour le moment qu'une petite partie de ces changements… C'est interpellant mais aussi très passionnant à comprendre.

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

Source : http://trends.levif.be/economie/politique-economique/le-danger-de-la-societe-du-big-data/article-opinion-362781.html
Par Amid Faljaoui

Une solution pour identifier des utilisateurs vulnérables aux cyber-attaques ?



Une solution pour identifier des utilisateurs vulnérables aux cyber-attaques ?

La société Fujitsu a annoncé avoir développé une technologie permettant d'identifier les utilisateurs vulnérables aux cyber-attaques, ayant des comportements potentiellement « à risque » donc vulnérables aux cyber-attaques. La solution est basée sur l'analyse des activités des utilisateurs sur leur ordinateur.

Cette technologie permettrait de créer des mesures de sécurité plus adaptées, comme l'affichage de messages individualisés d'alertes aux utilisateurs qui cliquent souvent sur les liens ou e-mails suspicieux, ou augmenter le niveau de menace lié aux e-mails envoyés entre départements d'une même entreprise par des utilisateurs propices à être infectés par des virus.
Jusqu'ici, un des problèmes des logiciels de sécurité est de ne pas pouvoir contrôler l'erreur humaine, comme la propension d'un utilisateur à cliquer sur les liens malveillants dans des e-mails, ou sur des sites infectés. Cette technologie permettrait d'y remédier.
Afin de développer cette solution, Fujitsu a utilisé un questionnaire en ligne, réalisé avec des experts en psychologie sociale, afin d'identifier les traits psychologiques des personnes vulnérables à trois types d'attaques : les infections par un virus, les arnaques et les fuites d'information. La société s'est également intéressée aux activités des utilisateurs pour les e-mails, l'accès internet ainsi qu'aux actions de la souris et du clavier.
Cette technologie a été présentée en détail lors du 32ème Symposium sur la Cryptographie et Sécurité de l'Information qui se tient depuis le 20 Janvier dans la ville de Kita-Kyushu.
http://www.bulletins-electroniques.com/actualites/77686.htm
http://ajw.asahi.com/article/business/AJ201501190057
http://www.fujitsu.com/global/about/resources/news/press-releases/2015/0119-01.html

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

Source :
http://www.infohightech.com/une-solution-pour-identifier-des-utilisateurs-vulnerables-aux-cyber-attaques/

Charlie Hebdo : Microsoft a fourni en 45mn des données au FBI

	Charlie Hebdo : Microsoft a fourni en 45mn des données au FBI

S**ur demande du FBI, Microsoft a livré en un temps record des informations liées à des comptes de messagerie de suspects impliqués dans l'attentat de Charlie Hebdo. Une attitude qui remet sur le devant de la scène l'éternel débat entre protection des données personnelles et enjeux de sécurité.**

45 minutes. Tel a été le temps de réaction éclair de Microsoft pour transmettre au FBI des données liées à l'attentat qui a frappé Charlie Hebdo le 7 janvier dernier. Le journal économique Bloomberg explique ainsi que la firme de Redmond a répondu de façon hyper réactive à une requête du FBI réalisée dans le cadre de cette terrible affaire.

Brad Smith, avocat général de Microsoft, aimerait bien que sa société n'ait pas à jouer sur les deux tableaux en matière de vie privée et de sécurité. (crédit : D.R.)

« Il y a juste deux semaines, en pleine chasse aux suspects impliqués dans l'attaque de Charlie Hebdo, le gouvernement français a demandé à obtenir le contenu de mails de deux comptes clients détenus par Microsoft », a indiqué dans un discours à Bruxelles Brad Smith, l'avocat général de l'éditeur dont Bloomberg s'est fait écho. La firme de Redmond s'est ainsi montrée particulièrement coopérative en répondant à la demande du FBI de faire remonter le contenu des e-mails en question en tout juste 45 minutes.
Une réactivité dont n'a justement pas toujours fait preuve le même Microsoft pour fournir des informations, également liées à des mails et comptes de messagerie, à la justice américaine dans le cadre d'autres affaires comme celle, récente, relative à un trafic de drogue. La firme de Redmond ayant alors à l'époque tenu un discours qui tranche avec la réactivité dont elle a fait preuve pour répondre à la requête du FBI dans l'affaire Charlie Hebdo : « En vertu du 4e amendement de la constitution américaine, les utilisateurs ont le droit de garder leurs communications par courriel privées. Nous avons besoin que notre gouvernement respecte les protections constitutionnelles de vie privée et respecte les règles en matière de vie privée établies par la loi ».

Microsoft en aucun cas prêt à se substituer au législateur
Mais depuis les attentats qui ont marqué la France et leurs répercussions partout dans le monde, des voix politiques se sont élevées pour fendre l'armure de la vie privée au nom des enjeux de sécurité. Notamment celle du Premier Ministre de la Grande-Bretagne, David Cameron, qui a prôné pour un renforcement des pouvoirs des services de sécurité pour s'assurer que les terroristes n'utilisent pas Internet pour communiquer secrètement entre eux.
« Si les membres du gouvernement veulent déplacer le curseur entre sécurité et vie privée, la façon appropriée de le faire est de modifier la loi plutôt que de demander aux acteurs privés comme nous de le déplacer nous-mêmes », a déclaré Brad Smith. Une saillie qui ne va à coup sûr pas manquer de raviver l'éternel débat – et les polémiques – entre ardents défenseurs de la vie privée et militants d'une sécurité sans faille. Car si tout le monde est d'accord pour détecter et empêcher les terroristes d'agir, l'étendue et la puissance des moyens à mettre en oeuvre pour y parvenir est loin de faire l'unanimité.

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

Source : http://www.lemondeinformatique.fr/actualites/lire-charlie-hebdo-microsoft-a-fourni-en-45mn-des-donnees-au-fbi-59995.html
par Dominique Filippone

Protection des données personnelles : L'AFCDP

endosse la déclaration du groupe article 29

Protection des données personnelles : L'AFCDP endosse la déclaration du groupe article 29

Le 8 décembre 2014, à l'Unesco et en présence du Premier ministre, la Présidente de la CNIL a dévoilé la « Déclaration commune des autorités européennes de protection des données réunies au sein du groupe de l'article 29(1) ».

L'AFCDP (Association Française des Correspondants à la protection des Données à caractère Personnel) se reconnait pleinement dans les quinze points de cette déclaration, qu'elle vient d'endosser.
Les projets européens de règlement et de directive relatifs à la protection des données doivent assurer un haut niveau de protection des données aux personnes, conforme aux valeurs et droits fondamentaux de l'Europe.
« Dans la continuité de ce que fait le CIL aujourd'hui, le futur Délégué à la protection des données doit être un acteur clé de la protection des données personnelles dans la proposition de règlement » déclare Paul-Olivier Gibert, Président de l'AFCDP, « Cet expert contribuera à rendre plus effective la protection des données personnelles, à réduire les contraintes administratives inutiles, et à créer la confiance ».
Les projets européens de règlement et de directive relatifs à la protection des données doivent être adoptés en 2015. Outre contribuer à l'unification du marché numérique européen, ces textes doivent assurer un haut niveau de protection des données aux personnes, conforme aux valeurs et droits fondamentaux de l'Europe.
« Les propositions que nous avons formulées auprès de Bruxelles2, via la Confédération européenne des organisations de protection des données (CEDPO), vont dans ce sens » ajoute Paul-Olivier Gibert.
Pour la Présidente de la CNIL, Madame Isabelle Falque Pierrotin, cette déclaration permet de réaffirmer les valeurs communes de l'Europe : « Notre vie quotidienne est numérique et les données personnelles constituent la particule élémentaire de ce monde numérique. Des quantités gigantesques de données sont stockées, traitées et partagées sans que les individus disposent d'une réelle maîtrise de leurs données. Du fait de son histoire et de sa culture, l'Europe doit faire entendre sa voix à un moment charnière. C'est l'objet de la déclaration politique adoptée par les 28 autorités de protection européennes qui réaffirment les valeurs communes de l'Europe et proposent des actions concrètes pour assurer un équilibre entre protection des données personnelles, innovation et impératifs de sécurité. En activant l'ensemble de ces leviers, l'Europe pourra proposer un cadre éthique durable et offrir un environnement de confiance aux citoyens et de compétitivité aux acteurs économiques. »

L'AFCDP a été créée dès 2004, dans le contexte de la modification de la Loi Informatique & Libertés qui a officialisé un nouveau métier, celui de « Correspondant à la protection des données à caractère personnel » (ou CIL, pour Correspondant Informatique & Libertés).
L'AFCDP est l'association représentative des CIL, mais elle rassemble largement. Au-delà des professionnels de la protection des données et des Correspondants désignés auprès de la CNIL, elle regroupe toutes les personnes intéressées par la protection des données à caractère personnel. La richesse de l'association réside – entre autres – dans la diversité des profils des adhérents : Correspondants Informatique & Libertés, délégués à la protection des données, juristes et avocats, spécialistes des ressources humaines, informaticiens, professionnels du marketing et du e-commerce, RSSI et experts en sécurité, qualiticiens, archivistes et Record Manager, déontologues, consultants, universitaires et étudiants.

Quelques membres de l'AFCDP :
3 Suisses, Accor, Adecco, AG2R La Mondiale, American Hospital of Paris, AXA, BP France, Carrefour, Cecurity.com, Caisse nationale des allocations familiales, Communauté Urbaine de Marseille Provence, Conseil Général de Seine-Maritime, CCIP, CPAM des Bouches du Rhône, Crédit Immobilier de France, Ecole Polytechnique, Fédération Nationale des Tiers de Confiance, Orange, IBM France, INRA, Groupe Casino, Legrand, Malakoff Mederic, Michelin, La Poste, Port autonome de Dunkerque, RATP, Région Haute Normandie, Région Lorraine, Sénat, SNCF, Ville de Paris, Ville de Saint-Etienne, Total…
1 Texte en français disponible sur http://europeandatagovernance-forum.com/pro/fiche/quest.jsp
2 Appel à mesures d'incitation afin de promouvoir la désignation de délégués à la protection des données, disponible en français sur http://www.novosite.nl/editor/assets/cedpo/CEDPO_Warsaw_Declaration_final%20in%20French.pdf

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

Source : http://www.dsih.fr/article/1327/protection-des-donnees-personnelles-l-afcdp-endosse-la-declaration-du-groupe-article-29.html

---

Les services DDoS à la

demande des pirates de Sony, Lizard Squad, piratés

	Les services DDoS à la demande des pirates de Sony, Lizard Squad, piratés

L’adage veut que les cordonniers soient toujours les plus mal chaussés. Le piratage de LizardStresser, le service de DDoS à la demande de Lizard Squad, tend à confirmer cette règle : le fichier contenant les identifiants et mots de passe des membres n’était même pas chiffré.

Petit retour en arrière. Nous sommes fin décembre, à quelques heures de Noël, et le groupe de pirates connu sous le nom de Lizard Squad se rappelle au bon souvenir de tout le monde en mettant le PlayStation Network et le Xbox Live hors ligne. Les conséquences s’étendent sur plusieurs jours et le collectif peut se réjouir : il a livré une démonstration très visible de la force de frappe de son réseau basé sur des routeurs piratés. Son service LizardStresser, qui propose de lancer des attaques DDoS à la demande, enregistre alors de nombreuses inscriptions.
Mais cette période faste n’a été que de courte durée. En effet, outre plusieurs arrestations, notamment outre-Manche, un autre pirate ou groupe de pirates s’en est pris au site hébergeant le service LizardStresser. Le service en lui-même est a priori intact, mais sa base de données incluant notamment les pseudonymes et mots de passe des membres est maintenant dans la nature. Or, de manière assez curieuse, Lizard Squad n’a pas jugé nécessaire de se protéger contre le piratage : ses fichiers sont stockés en clair.

Ceux-ci ayant rapidement été publiés, tout le monde a pu voir que les affaires marchaient plutôt bien. Au moment du piratage, LizardStresser comptait la bagatelle de 14 241 membres. Beaucoup, toutefois, n’étaient que des curieux. Comme le pointe KrebsonSecurity, ils n’étaient « que » quelques centaines à avoir alimenté leur compte dans le but de financer une attaque. En tout, Lizard Squad aurait perçu un peu plus de 11 000 $, versés en bitcoins.
Bien sûr, le collectif de pirates n’a que modérément apprécié de voir de ses précieuses données étalées sur la toile. Une copie des documents, en particulier, était disponible sur Mega. Le groupe ne s’est donc pas démonté et a formulé une requête au titre de la loi DMCA, qui protège le droit d’auteur en imposant aux hébergeurs de retirer les contenus publiés illégalement. Comble de l’absurde, celle-ci a été acceptée. De nombreuses copies, néanmoins, demeurent disponibles sur d’autres sites.

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

Source : http://www.lesnumeriques.com/lizard-squad-service-ddos-a-demande-pirate-n38817.html

L’UE doit-elle obliger les géants de l’Internet à céder leurs clés de chiffrement ?

Council of the European Union
General Secretariat

Brussels, 17 January 2015
(OR. en)

DS 1035/15

LIMITE

MEETING DOCUMENT

From: EU Counter-Terrorism Coordinator
To: Delegations
Subject: EU CTC input for the preparation of the informal meeting of Justice and Home Affairs Ministers in Riga on 29 January 2015

This is a first paper for discussion in COSI on 20 January 2015. It does not yet include the Commission's proposals which will be discussed in the College on 21 January, nor the contributions from the Member States. The document which will be submitted to the informal meeting of JHA ministers in Riga on 29/30 January will be shorter, include the outcome of the COSI discussions as well as contributions from the Member States and the Commission.

Europe is facing an unprecedented, diverse and serious terrorist threat. The horrific attacks that took

L’UE doit-elle obliger les géants de l’Internet à céder leurs clés de chiffrement ?

La montée en puissance du terrorisme en Europe relance le débat sur le chiffrement des communications et la création de backdoors réservés aux forces de l’ordre européenne. Le coordinateur antiterrorisme de l’UE, Gilles de Kerchove, demande sans détour un accès aux clefs de chiffrement des géants de l’Internet.

Les géants de l’Internet vont-ils bientôt être obligés de partager leurs clés de chiffrement avec la police et les agences de renseignement européennes pour les aider à lutter contre le terrorisme ? C’est en tout cas une recommandation ferme de Gilles de Kerchove, le coordinateur antiterrorisme de l’Union Européenne. C’est une suggestion étonnante quand on se souvient que les entreprises comme Google ou Facebook ont commencé à chiffrer leurs communications pour lutter contre la curiosité des agences de renseignement chinoises mais aussi américaines, anglaises, allemandes, hollandaises et françaises comme l’ont indiqué les documents révélés par Edward Snowden.

L’association de protection des droits civils Statewatch
a divulgué un document rédigé par le coordinateur
antiterroriste Gilles de Kerchove.

Gilles de Kerchove suggère que la Commission européenne « devrait revoir ses règles pour obliger les entreprises de l’Internet et des télécommunications opérant dans l’UE à fournir … aux autorités nationales compétentes un accès à leurs communications [c’est à dire leurs clefs de chiffrement] », selon un document divulgué par l’association de protection des droits civils Statewatch. Dans ce document, M. de Kerchove expose ses vues sur les mesures anti-terrorisme à prendre dans l’UE en vue d’une réunion des ministres de la Justice et de l’Intérieur de l’UE à Riga, la semaine prochaine.

Des keyloggers pour suivre les échanges

Cette proposition est controversée parce que, comme le note le coordinateur, la généralisation du chiffrement pour les échanges sur Internet rend très difficile, voire impossible, les interceptions légales par les autorités nationales compétentes. Nous avons discuté de ces questions avec les cybergendarmes de Paris (Section de recherche de Paris et ses spécialistes N-Tech) et de Rosny Sous Bois (C3N). Sans coopération des fournisseurs de services (Whatsapp, Skype ou encore iMessage), il est très difficile de lire les messages échangés. La solution la plus facile – pour les forces de l’ordre – est aujourd’hui l’installation d’un cheval de Troie ou keylogger (un enregistreur de frappes) sur les terminaux des suspects, smartphones, tablettes ou PC. Une opération toujours délicate puisqu’elle doit être effectuée à l’insu des utilisateurs.
« Whatsapp ou Viber commencent à être très utilisés par les criminels avec des mobiles jetables », nous avait confié le major Etienne Neff de la section de Paris. « Les criminels sont aujourd’hui plus sophistiqués et utilisent également des solutions payantes ». Les forces de l’ordre peuvent toujours accéder aux métadonnées fournies par les opérateurs mais il faut séparer le flux et le reconditionner pour le traiter.

Les entreprises également sous surveillance

L’appel à plus de surveillance des échanges sur Internet est revenu sur le devant de la scène en Europe suite aux assassinats perpétués dans les bureaux du magazine satirique Charlie Hebdo et à l’épicerie HyperCacher à Paris. Après les deux attentats, les ministres de la Justice et de l’Intérieur de l’UE avaient publié une déclaration commune dans laquelle ils soulignaient qu’il est essentiel « d’entretenir une étroite collaboration avec les FAI pour endiguer la propagande terroriste en ligne ».
Si la Commission a refusé de commenter les plans anti-chiffrement de M. de Kerchove, le document fuité contient des détails supplémentaires comme le contrôle du « chiffrement décentralisé » des entreprises. Cela pourrait être une référence au chiffrement de bout-en-bout utilisé par certaines entreprises sensibles pour verrouiller leurs communications.

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

Source : http://www.lemondeinformatique.fr/actualites/lire-l-ue-doit-elle-obliger-les-geants-de-l-internet-a-ceder-leurs-cles-de-chiffrement-59993.html
Par Serge Leblal

France Télévisions et ses sites régionaux victimes d’une attaque informatique

France Télévisions et ses sites régionaux victimes d’une attaque informatique

Les sites régionaux et ultramarins de France Télévisions ont été victimes d’une cyber-attaque hier matin.
Vous êtes nombreux à vous en être aperçus : le site internet de France 3 Pays de La Loire ne fonctionnait pas normalement ce mercredi 21 janvier. Les serveurs informatiques qui hébergent les sites régionaux et ultramarins de France Télévisions en région parisienne ont en effet été victimes d’une cyberattaque durant la nuit de mardi à mercredi.

Après interventions des services techniques, les sites régionaux et ultramarins de France Télévisions ont retrouvé leur aspect normal en tout début de matinée. Il était en revanche impossible d’y publier des informations jusqu’à la fin du processus de mise à jour des protocoles de sécurité. Le problème est désormais résolu.

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

Source : http://france3-regions.francetvinfo.fr/pays-de-la-loire/2015/01/21/france-televisions-et-ses-sites-regionaux-victimes-dune-attaque-informatique-637201.html

Forum international de la Cybercriminalité: Bernard

Cazeneuve débloque 108 millions d’euros pour aider les enquêteursNicolas Messayaz / Sipa Olivier Aballain

Forum international de la Cybercriminalité: Bernard Cazeneuve débloque 108 millions d’euros pour aider les enquêteurs

Denis JACOPINI, expert judiciaire en informatique diplômé en Cybercriminalité, était présent ce mardi au 7eme Forum International de lutte contre la Cybercriminalité.

Le repérage et la traque des réseaux jihadistes sur internet sont au programme de Bernard Cazeneuve ce mardi: le ministre de l’Intérieur a ouvert à Lille le 7e Forum international de lutte contre la Cybercriminalité (FIC).
Le rendez-vous tombe à pic, puisque Manuel Valls lui-même a rappelé le 19 janvier sur i-Télé que «ce n’est pas dans les mosquées que ces recrutements [de djihadistes] s’organisent, c’est le plus souvent sur internet».
Après une rencontre avec le ministre de l’Intérieur allemand, Bernard Cazeneuve a prononcé un discours vers 10h au cours duquel il a annoncé le déblocage de 108 millions d’euros sur 3 ans pour développer les moyens des services de l’État pour l’enquête en matière de criminalité sur internet

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

Source : http://www.20minutes.fr/lille/1521015-20150120-direct-bernard-cazeneuve-forum-international-cybercriminalite
Par Olivier Abalain

Le Forum International de la Cybersécurité FIC 2015 en vidéo

Le Forum International de la Cybersécurité FIC 2015 en vidéo

« Nous sommes tous les vecteurs de cyberattaques » pour le fondateur du Forum de la cybercriminalité »

Le ministre de l'Intérieur Bernard Cazeneuve a inauguré mardi matin le Forum international de cybersécurité à Lille. Le général Marc Watin-Augouard, fondateur du Forum FIC et directeur du CREOGN, a expliqué que « nous sommes tous les vecteurs de cyberattaques, soit directes, soit par rebonds. »

Source vidéo : « Nous sommes tous les vecteurs de cyberattaques » pour le fondateur du Forum de la cybercriminalité

La cybersécurité au Grand Palais

Orange, cybersécurité et cyberdéfense

Le plateau TV pendant le Forum International de la Cybersécurité 2015 – FIC 2015
Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://videos.tf1.fr/infos/2015/nous-sommes-tous-les-vecteurs-de-cyberattaques-pour-le-fondateur-8549855.html