Forum de la Cybersécurité à Marrakech, appel à endiguer les menaces de la cybercriminalité en Afrique

Forum de la Cybersécurité à Marrakech, appel à endiguer les menaces de la cybercriminalité en Afrique

Les participants à la 6ème édition du « Marrakech Security Forum » ont appelé à faire front commun pour endiguer les menaces de la cybercriminalité en Afrique.

Face à des législations rudimentaires et un essor sans précédant des flux informatiques, les pays africains n'ont d'autre choix que de faire bloc aux niveaux institutionnel, juridique et technologique, pour contrer les menaces sécuritaires découlant de la cybercriminalité, ont-ils relevé lors d'une séance plénière sur « l'Afrique face à la cybercriminalité et au cyber-terrorisme ».
Selon le Directeur du Centre satellitaire de l'Union européenne, Pascal Legai, l'essor numérique débridé et la désuétude de l'arsenal juridique ont érigé l'Afrique en une terre de prédilection pour la cybercriminalité et son corolaire le cyber-terrorisme.
Protéiforme, le cyber-crime en Afrique mute, change en fonction des cibles et, pis encore, s'affranchit de toutes les juridictions, a-t-il fait remarquer, soulignant l'inéluctabilité « d'agir vite et de se coordonner » pour colmater les failles.
De par sa nature transfrontalière, la cybercriminalité est difficile à contrôler, d'où la nécessité, pour les Etats africains, d'harmoniser les politiques et législations nationales pour apporter une réponse normalisée aux menaces qui en découlent, a encore dit M. Legai.
De son côté, le directeur de l'Organe de coordination belge pour l'analyse de la menace (Belgique) Vandoren André a mis l'accent sur le risque que recèle le cyber-terrorisme comme étant un outil nouveau permettant aux groupes terroristes de repérer, d'incuber et d'enrôler des jeunes, « majoritairement paumés ».
La méthodologie de l'Etat islamique est une illustration on ne peut plus claire de la « propagande jihadiste » sur la toile, cette organisation ayant réussi à développer de nouveaux modus operandi, avec à l'appui une maitrise avérée de l'outil informatique et une armada de connaisseurs en la matière.
Placé sous le thème « L'Afrique face aux menaces transnationales et asymétriques », la 6ème édition du Marrakech Security Forum sert de tribune pour quelque 300 hauts responsables civils, militaires, sécuritaires, experts et représentants d'organisations internationales pour stimuler une meilleure compréhension de thématiques clés pour le devenir du continent africain.

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

Source : http://fr.starafrica.com/actualites/appel-a-endiguer-les-menaces-de-la-cybercriminalite-en-afrique.html
Par Atlasinfo

Safe Harbor et CNIL : des régulateurs allemands dénoncent le laxisme de la Federal Trade Commission (FTC)

Safe Harbor et CNIL : des régulateurs allemands dénoncent le laxisme de la Federal Trade Commission (FTC)

Des commissaires de la Cnil allemande ont lancé pour la première fois des procédure administratives contre deux transferts de données vers les Etats-Unis réalisés par des entreprises américaines sur la base de l'accord «Safe Harbor».

« La légitimité de l'accord est de plus en plus remise en question » a déclaré le commissaire Johannes Caspar (Hambourg) la semaine dernière lors d'un évènement consacré à la protection des données et organisé à Berlin. La frustration des commissaires les plus en pointe sur ce dossier vient du fait que cet accord n'a connu aucune réforme de fond suite aux révélations d'Edouard Snowden mentionnant que la NSA surveillait les données privées des citoyens allemands.
Dernier épisode en date, deux procédures administratives ont donc été initiées contre des entreprises américaines dans les landers de Berlin et de Brême.
Le programme Safe Harbor est un accord crucial pour les entreprises américaines. Google, Facebook ou encore Twitter peuvent en vertu de cet accord transférer légalement des données commerciales de l'Union européenne vers les États-Unis s'ils acceptent de respecter la loi applicable à la protection des données des citoyens des pays de l'UE. Cette loi porte essentiellement sur la collecte et le traitement des données.
C'est la FTC américaine qui doit vérifier que les exigences du Safe Harbor sont bien respectées par les entreprises américaines. Si l'accord venait à être dénoncé, cela aurait un impact important sur les activités des GAFA dans l'Union européenne.

Quel impact en cas de suspension du Safe Harbor ?
Suite au scandale d'espionnage de la NSA, de nombreuses voix européennes se sont élevées pour demander la suspension du programme Safe Harbor. Au lieu de suspendre l'accord, cependant, en novembre 2013, la Commission européenne a envoyé aux États-Unis une liste de 13 réformes qu'elle souhaite voir apporter au Safe Harbor. Le gouvernement américain n'a toujours pas pleinement répondu à la demande, même s'il avait promis de le faire pour l'été 2014. Tout cela pourrait être réglé en mai prochain, aux dernières nouvelles.
Reste que nul ne sait quel serait l'impact réel de la suspension du programme Safe Harbor. N'étant plus autorisés à transférer des données hors de l'UE, des entreprises comme Twitter, dont tous les serveurs sont aux Etats-Unis, auraient des difficultés majeures pour faire fonctionner leur activité européenne. Pour les entreprises qui ont des serveurs en Europe, cela affecterait néanmoins leur activité back-office, les données locales pouvant être transférées outre Atlantique pour subir un traitement algorithmique à des fins de profilage ou de détection des fraudes.
Mais la fin du Safe Harbor pourrait également porter préjudice à des entreprises européennes qui opèrent des données ailleurs qu'en Europe. Siemens, SAP et même BMW pour ne citer que les allemands, ont tout intérêt à expédier leurs données aux Etats-Unis quand cela est nécessaire d'un point de vue business.

5 000 membres de Safe Harbor
Plus de 5 000 sociétés sont membre de Safe Harbor, dont en plus des sociétés citées précédemment Amazon, Hewlett-Packard, IBM ou encore Microsoft. Ces entreprises affirment se conformer à un niveau 'adéquat' au exigences de protection des données personnelles de l'Union européenne.
Mais les inspections, réalisées par la FTC (Federal Trade Commission) des Etats-Unis, sont sporadiques, et les sanctions peuvent difficilement être appliquées. « De mon point de vue, la charge de la preuve n'est pas du ressort des entreprises américaines » a dit cependant Holger Lutz, associé chez Baker & McKenzie à DataGuidance. « C'est plus du ressort de l'autorité compétente en matière de protection des données ».
Les principes du Safe Harbor sont basés sur ceux de la Directive 95/46 du 24 octobre 1995 affirme la Cnil.
Les domaines couverts concernent l'information des personnes sur la collecte de données, la possibilité accordée à la personne concernée de s'opposer à un transfert à des tiers ou à une utilisation des données pour des finalités différentes, le consentement explicite des personnes pour le recueil de données sensibles, le droit d'accès, de rectification et enfin la sécurité.
« Le Safe Harbor permet donc d'assurer une protection adéquate pour les transferts de données en provenance de l'Union européenne vers des entreprises établies aux Etats-Unis » assure la Cnil, qui précise que la liste des entreprises ayant adhéré aux principes du Safe Harbor se trouve sur le site du Département du Commerce américain.

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

Source : http://www.zdnet.fr/actualites/safe-harbor-des-regulateurs-allemands-denoncent-le-laxisme-de-la-ftc-39814338.htm
Par Guillaume Serries

Le site du gouvernement hollandais victime d’une attaque DDoS

	Le site du gouvernement hollandais victime d’une attaque DDoS

Suite à une attaque DDoS, le site du gouvernement néerlandais n'était plus accessible pendant 10 heures. L'attaque, qui a utilisé différents vecteurs, a également mis d'autres sites hors ligne.

Mardi dernier, une attaque sophistiquée par déni de service distribué (DDoS) a bloqué pendant plus de 10 heures le site du gouvernement néerlandais et d'autres sites commerciaux.
Le ministère des Affaires générales, le Centre National de la cybersécurité (NCSC), l'hébergeur Prolocation et le fournisseur de services Centric passent au crible les techniques utilisées pour mener cette attaque et tentent d'identifier ses auteurs.

« L'attaque DDoS, qui a débuté à 9 h 45 heure locale, a été difficile à contrer parce que les modalités utilisées ont changé régulièrement », a déclaré le directeur de Prolocation, Raymond Dijkxhoorn. « La stratégie était différente des attaques DDoS habituelles auxquelles nous sommes confrontés quasi quotidiennement et contre lesquelles nous arrivons plus facilement à nous défendre », a-t-il ajouté. « C'est même la première fois que nous n'arrivons pas à la contenir », a encore déclaré le directeur de Prolocation. « L'attaque visait directement les sites du gouvernement fédéral, mais elle a aussi eu pour conséquence la mise hors ligne de sites hébergés sur le même réseau », a-t-il expliqué. C'est le cas notamment du site de blogging Geenstijl.nl et de celui de l'opérateur de téléphonie Telfort, également bloqués par l'attaque. « Certains sites du même réseau ont utilisé les services de détournement anti-DDoS de fournisseurs comme Cloudflare », a aussi déclaré Raymond Dijkxhoorn. « Mais si les clients d'un même réseau ne parviennent pas tous à détourner l'attaque DDoS, il y a un de fortes chances que les autres sites soient affectés », a-t-il ajouté. Par exemple GeenStijl a utilisé Cloudflare. En général, le service arrive à maintenir le trafic jusqu'au serveur du site, même si celui-ci est visé par une attaque DDoS. « Mais le serveur de GeenStijl peut lui-même ne plus être accessible si l'attaque DDoS vise d'autres sites sur le réseau qui n'utilisent pas de service de détournement », a encore expliqué le directeur de Prolocation. Et, comme il l'a précisé, « le gouvernement néerlandais n'a pas utilisé des services de protection DDoS externes ». Selon Raymond Dijkxhoorn, l'attaque DDoS a mis en oeuvre plusieurs techniques en alternance. « Et même si Prolocation a beaucoup d'expérience en matière d'attaques DDoS, c'est la première fois que le fournisseur a du faire face à ce type de stratégie », a-t-il déclaré. À la demande du NCSC, Raymond Dijkxhoorn a refusé de donner plus de détails sur les attaques tant que l'enquête ne serait pas terminée.
Le Centre National de la cybersécurité (NCSC) et le fournisseur de services hollandais Centric ont tous deux refusé de commenter les détails de l'attaque tant que l'enquête était en cours. Mais Prolocation a évoqué l'incident avec les ingénieurs de Prolexic et d'Akamai, qui ont déjà vu des attaques DDoS basées sur des méthodes similaires ailleurs dans le monde. « Les sites hébergés sous le même bloc IP peuvent être mis hors ligne, même si un seul des sites est ciblé spécifiquement par l'attaque », a confirmé Hans Nipshagen, le directeur d'Akamai pour la Belgique, les Pays-Bas et le Luxembourg. « Si les sites du gouvernement avaient utilisé des services de filtrage DDoS externes, le réseau aurait pu tenir », a-t-il aussi ajouté. « Même s'il est difficile de savoir de l'extérieur quelles méthodes ont été utilisées contre les sites du gouvernement néerlandais, il semble que l'attaque DDoS était une attaque à grande échelle, et qu'elle a mobilisé une grosse quantité de trafic », a encore déclaré Hans Nipshagen. Selon Akamai, « certaines attaques DDoS de grande envergure utilisent de multiples vecteurs pour saturer la bande passante avec de grandes quantités de paquets à une vitesse extrêmement élevée, bloquant les sites ciblés ». Le nombre d'incidents de ce type ne cesse d'augmenter : « D'abord, les outils d'attaque sont de plus en plus faciles à utiliser. Il existe aussi une industrie criminelle florissante qui vend des services d'attaque DDoS pour le compte d'autrui », a déclaré Akamai. Après la Hollande, la France…

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

Source : http://www.lemondeinformatique.fr/actualites/lire-le-site-du-gouvernement-hollandais-victime-d-une-attaque-ddos-60227.html

---

Télés connectées : un espion dans le salon ?

Télés connectées : un espion dans le salon ?

Les téléviseurs Samsung sont l'équivalent du télécran du roman 1984 : un objet de surveillance qui enregistre tout ce qui est dit dans une pièce et épie les faits et gestes des utilisateurs. C'est la comparaison que faisait, dimanche, Parker Higgins, militant de l'organisation de défense des libertés américaines EFF.

Depuis, un vent de panique s'est emparé de possesseurs de téléviseurs connectés de la marque sud-coréenne et d'une partie de la presse. La raison : une phrase figurant dans les conditions d'utilisation édictées par Samsung, qui précise que **les services de commande à la voix existant sur ses téléviseurs peuvent être amenés à transmettre des conversations privées à un « service tiers »** :

« Nous vous signalons que, si les mots que vous prononcez contiennent des informations privées ou confidentielles, ces informations feront partie des données transmises à un tiers lorsque vous utiliserez le service de reconnaissance vocale. »

Glaçante, la phrase n'est pourtant pas une nouveauté : elle figure depuis longtemps dans les conditions d'utilisation des téléviseurs Samsung. Et on la retrouve également, presque mot pour mot, dans les conditions d'utilisation d'un téléviseur de la marque concurrente LG. Que signifie réellement ce jargon juridique ?

Actif ou passif ?

Pour le comprendre, il faut savoir comment fonctionnent les technologies de reconnaissance vocale. Qu'il s'agisse d'un téléphone Android ou iOS, d'une télévision, d'un ordinateur de bord dans une voiture, les objets dotés de cette fonctionnalité fonctionnent selon deux modes, actif ou passif. Dans le mode actif, il faut appuyer sur une touche pour indiquer à l'objet qu'il doit « écouter » ; dans le mode passif, l'objet « écoute » par défaut ce qui se passe autour de lui et déclenche une action s'il reconnaît une commande préenregistrée.

La reconnaissance vocale est une technologie complexe, qui nécessite une importante puissance de calcul pour bien fonctionner et reconnaître correctement les mots prononcés. Dans la plupart des cas, les objets qui ont besoin de pouvoir reconnaître plus que quelques mots-clés utilisent la puissance de calcul de machines très rapides connectées à Internet, et non uniquement la puce du téléphone ou de la télévision.

Les mots captés par l'objet sont donc transmis à distance à un serveur qui les analyse et renvoie sa conclusion à l'appareil. Pour fonctionner, ces services ont donc besoin de « transmettre des données à un tiers » — en l'occurrence, pour les téléviseurs Samsung, le leader mondial de la reconnaissance vocale, Nuance. Les données sonores transmises peuvent effectivement contenir des informations très personnelles, puisque la reconnaissance vocale « traite » l'ensemble de ce qui lui est transmis. La présence de ces termes dans les conditions d'utilisations est donc « normale » et s'apparente à un avertissement.

Accusé d'écouter les conversations de ses clients, Samsung a affirmé au Guardian qu'il n'enregistrait pas les sons captés par ses téléviseurs, et que les données sonores étaient uniquement « fournies à un service tiers durant une recherche de commande vocale ». Sollicitée par Le Monde, Nuance confirme qu'elle est bien destinataire de ces données vocales. *« Nous n'utilisons ces données qu'à des fins d'amélioration de notre technologie. […] Lorsque nous travaillons avec des entreprises tierces, un contrat garantit la confidentialité des données. […] Nous ne vendons pas ces données à des fins de marketing ou de publicité »*, écrit Gretchen Herault, le responsable de la vie privée de la société.

« Tempête dans un verre d'eau »

Autant d'informations qu'il est parfois difficile d'appréhender dans les conditions d'utilisation de ces télévisions connectée. Clauses floues, langage juridique abscons, textes interminables et difficilement accessibles… Ces textes sont la plupart du temps incompréhensibles pour quelqu'un qui n'a pas des connaissances en droit ni la patience de les lire.

En réaction, le Consumentenbond, l'équivalent néerlandais de l'UFC-Que choisir, a lancé l'an dernier une étude exhaustive sur les problèmes de vie privée posés par les téléviseurs connectés. L'organisation de protection des consommateurs a dressé un tableau comparatif des conditions d'utilisation de ces appareils, et le résultat est sans appel : celles de Sony ne font « que » six pages, tandis que celles de Samsung atteignent… cinquante-sept pages.

« La polémique autour de Samsung est de l'ordre de la tempête dans un verre d'eau », explique-t-on au siège de l'organisation, interrogée par Le Monde sur le sujet :

« Ces téléviseurs n'écoutent pas en permanence tout ce qui se passe dans la pièce — le problème le plus important, c'est que leurs conditions d'utilisation ne sont absolument pas transparentes et sont beaucoup trop longues. »

Dans le détail, le Consumentenbond note que la quasi-totalité des constructeurs ont inclus des clauses extrêmement larges et peu claires, voire illégales en droit européen. LG et Samsung ne précisent par exemple pas clairement quelles données sont collectées et dans quel but ; Sony l'explique clairement, mais ne dit pas qui collecte et conserve les données ; Panasonic est non seulement trop flou, mais exige aussi un paiement pour l'accès à ses données personnelles. Philips est le constructeur qui s'en tire le moins mal, selon l'étude : ses conditions d'utilisation sont certes longues, mais plutôt complètes et claires. L'entreprise reste cependant peu claire sur les types de tiers pouvant avoir accès aux données.

Les analyses effectuées par le Consumentbond sur des modèles des cinq constructeurs montrent que ces derniers collectent de très nombreuses informations — chaînes regardées, nom du film en cours de diffusion, recherches effectuées… Prises isolément, ces informations peuvent sembler peu dangereuses pour la vie privée. Mais l'**agrégation de ces « métadonnées » sur l'activité d'un téléspectateur permet, en définitive, d'en savoir beaucoup sur lui, ses goûts, ses habitudes** — parfois plus que si la télévision « écoutait » réellement toutes les conversations autour d'elle.

De vastes quantités de données personnelles collectées

Pour le démontrer, un informaticien britannique, Jason Huntley, a décidé en 2013 de brancher un outil d'analyse de trafic sur la télévision LG qu'il vient d'acheter. Il découvre alors que l'appareil transmet au fabriquant une gigantesque quantité d'informations — comme les films qu'il regarde ou ses changements de chaîne. Plus ennuyeux encore, le téléviseur enregistre le nom de tous les fichiers présents sur les clés USB qui sont branchées dessus et envoie ces données aux serveurs de LG.

A l'époque, M. Huntley publie un post de blog où il détaille ses découvertes ainsi que la réponse du constructeur, lequel estime que ces captations ne posent pas de problème puisque M. Huntley a accepté les conditions d'utilisation de sa télévision. Après une série d'articles très critiques à l'encontre de LG, le constructeur bloque la collecte de données — prévue notamment pour l'affichage de publicités ciblées.

« Mais l'année dernière, LG a forcé ses utilisateurs à accepter de nouvelles conditions d'utilisation », explique au Monde Jason Huntley, avec des clauses très floues.

« Les nouvelles conditions semblent les autoriser à collecter toutes les informations qu'ils recueillaient auparavant, y compris des informations sur des fichiers personnels hébergés sur des objets connectés au téléviseur. Cependant, lors de tests que j'ai effectués depuis, je n'ai pas trouvé de preuve qu'ils enregistrent effectivement ces informations. Je les soupçonne d'avoir prévu tous les cas de figure si à l'avenir ils décidaient d'activer de nouvelles collectes. »

Dans ses analyses, Jason Huntley n'a pas détecté de transmission suspecte ou non chiffrée de données vocales, mais il note que les constructeurs sont libres de changer de technologie de reconnaissance vocale ou de décider de transmettre ces données à d'autres partenaires, **« ce qui augmenterait les chances que les données soient utilisées à mauvais escient ou volées »**.

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

Source : http://www.lemonde.fr/pixels/article/2015/02/11/teles-connectees-un-espion-dans-le-salon_4573664_4408996.html
Damien Leloup Journaliste au Monde

Le groupe Capgemini lance une nouvelle ligne de services mondiale dédiée à la cybersécurité

Le groupe Capgemini lance une nouvelle ligne de services mondiale dédiée à la cybersécurité

Capgemini lance sa nouvelle ligne de services mondiale dédiée à la cybersécurité. Celle-ci repose sur l'expertise de 2 500 professionnels de la cybersécurité, notamment des consultants, des auditeurs, des architectes, des spécialistes de la Recherche & Développement et des hackers éthiques , ainsi qu'un réseau mondial de 5 Centres Opérationnels de Sécurité (SOC, Security Operations Centers) et un large écosystème de partenaires technologiques. Capgemini prévoit une croissance élevée à deux chiffres de sa nouvelle ligne de services au cours des douze prochains mois. Elle doit permettre aux entreprises de mettre en œuvre un programme de transformation digitale en toute sécurité et de tirer parti des technologies du « SMACT » (Social, Mobile, Analytics, Cloud and Internet of Things) en toute confiance.

L'évolution rapide de la cybercriminalité a placé la sécurité au cœur des préoccupations des dirigeants. En effet, **entre 2013 et 2014, le nombre des cyberattaques a augmenté de 120%** dans le monde et **le coût estimé de la cybercriminalité pour les entreprises s'élève en moyenne à 7,6 millions de dollars par an**, soit une augmentation de 10%. En outre, les hackers ont considérablement accru leurs connaissances des systèmes ciblés. De ce fait, les conséquences de leurs attaques sont de plus en plus importantes. Pour les entreprises du secteur de l'industrie, ces conséquences ne sont pas seulement financières ou réputationnelles mais peuvent également être matérielles ou humaines.
La nouvelle ligne de services mondiale dédiée à la cybersécurité de Capgemini répond aux problématiques de sécurité des systèmes IT, des systèmes industriels (OT), ainsi que des objets connectés (IoT- Internet Of Things). Selon la récente étude menée par Capgemini Consulting auprès de fournisseurs de technologies d'objets connectés, **les entreprises doivent être mieux préparées à faire face aux menaces qui pèsent sur la sécurité et sur la confidentialité des données** : seules 33% d'entre elles pensent que leurs objets connectés sont « très résistants » aux futures menaces de cybersécurité et 70% considèrent que « les questions de sécurité influencent les décisions d'achat des clients relatives aux objets connectés » .
La nouvelle ligne de services développera des services packagés et industrialisés qui peuvent être répliqués dans tous les pays. Ces offres de services packagés répondent aux besoins de sécurité de l'IT de nouvelle génération tels que la sécurité des infrastructures Hadoop, la sécurité des SDDC (Software-Defined Data Centers), ainsi que la sécurité des Clouds hybrides privés et publics. De nouvelles offres seront également lancées, telles que des tests de sécurité des applications « as-a-service » et des solutions de gestion des identités et des accès « as-a-service », pour permettre aux entreprises de tirer parti de l'approche Cloud et faciliter le déploiement de solutions de sécurité.
Selon Forrester Research , « L'importance de la protection de la vie privée, la recrudescence des cyberattaques et l'éclatement du périmètre de l'entreprise digitale ont obligé les professionnels de la sécurité et de la gestion des risques à renforcer la protection des données elles-mêmes. Dans la bataille pour recruter, servir et fidéliser ses clients, la protection de la vie privée et la sécurité des données sont devenues des avantages concurrentiels, et de ce fait une priorité business et technologique. »

La ligne de services mondiale dédiée à la cybersécurité de Capgemini permettra aux entreprises d'adopter une approche globale et pragmatique de leur stratégie de sécurité. Elle consolide l'expertise de Capgemini en tant qu'intégrateur de systèmes et fournisseur de services. Elle repose également sur sa connaissance approfondie de la cybersécurité, acquise dans le cadre des nombreuses missions réalisées auprès de ses clients au cours des dix dernières années dont celles menées pour le ministère du Travail et des Retraites (DWP) au Royaume-Uni, l'Agence spatiale française (CNES), Alstom Transport et Foyer (le plus important groupe d'assurance au Luxembourg).

Capgemini a conçu une gamme de services de cybersécurité assurant la protection des utilisateurs (identité numérique et contrôle d'accès), des applications, des terminaux (les terminaux de bureau, smartphones, tablettes, capteurs et autres objets connectés), des infrastructures (stockage, réseaux, serveurs, virtualisation et orchestration) et des données.

Les services proposés sont les suivants :

• Le conseil en sécurité et l'audit de sécurité
o Cela inclut l'évaluation des systèmes de sécurité, la définition de feuilles de route, les conseils opérationnels de sécurité et les audits de sécurité, tels que les tests d'intrusion et les investigations numériques.
o En janvier 2015, lors du Forum international de la cybersécurité (FIC), le prix « Label France Cybersecurity » a été décerné à Sogeti France, filiale du groupe Capgemini, par Axelle Lemaire, Secrétaire d'Etat chargée du numérique pour ses services d'audit de sécurité.
o Capgemini a aussi récemment conduit plusieurs missions de conseil comme pour Alstom Transport, incluant une analyse de risques, l'identification des cibles de sécurité et des recommandations d'architecture afin d'assurer la cybersécurité des trains et du système de signalisation.

• La conception et le développement de solutions pour protéger les systèmes informatiques, les systèmes industriels et les systèmes intelligents (objets connectés) :
o Grâce à l'acquisition d'Euriware, société française de services informatiques, Capgemini propose des services pour sécuriser les systèmes SCADA (systèmes de contrôle et d'acquisition de données). En outre, Sogeti High Tech offre des services qui permettent d'intégrer la sécurité dans le processus de développement des objets connectés.
o En outre, en partenariat avec Pivotal, Capgemini a récemment lancé une offre de Détection de Comportements Anormaux (Anomalous Behavior Detection) pour permettre aux entreprises d'identifier et de répondre aux menaces informatiques internes et externes les plus sophistiquées.

• Surveillance de la sécurité 24h/24 et 7j/7 :
o Aujourd'hui, Capgemini exploite cinq Centres Opérationnels de Sécurité (SOC, Security Operation Centers) mutualisés, qui sont les yeux et les oreilles permettant de détecter et de réagir aux cyberattaques. Ils sont situés en France, au Royaume-Uni, au Luxembourg et en Inde – où il y en a deux. Ces centres bénéficient de l'aide d'équipes de Recherche & Développement spécialisées en identification de vulnérabilités et en investigations numériques. Capgemini construit actuellement un sixième SOC en Belgique. Il conçoit et met également en place des SOC ad hoc pour ses clients.

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

Source : http://www.globalsecuritymag.fr/Le-groupe-Capgemini-lance-une,20150212,50774.html
Par Marc Jacob

En 2015, vous serez la première cible visée par la cybercriminalité

13

En 2015, vous serez 13la première cible visée par la cybercriminalité

ESET®, pionnier globale en protection proactive depuis plus de deux décennies, vient de publier un rapport très complet sur les principales tendances pour 2015 en cybercriminalité. Ce rapport est gratuit et peut être télécharger sur in the white paper section on WeLiveSecurity.com.

Alors que l'an dernier tout se concentrait autour de la protection de la vie privée sur Internet et le malware sur Android, de nouveaux secteurs de risques en sécurité informatique émergent en 2015. Le rapport gratuit Trends for 2015, est axé sur les cinq principaux domaines sur lesquelles les entreprises doivent se concentrer pour combattre les attaques. Il explique pourquoi les entreprises doivent être sur leurs gardes, commente l'évolution des menaces et leur donne des conseils pour protéger au mieux leurs actifs.
"Alors que les organisations améliorent continuellement leurs connexions digitales, de nouvelles pistes s'ouvrent aux cybercrime, " explique Marc Mutelet, CEO de MGK Technologies, distributeur exclusif des produits ESET sur la Belgique et le Luxembourg. L'astuce est de faire en sorte que vos défenses soient plus impénétrables que celles des entreprises qui vous entourent. En comprenant mieux le paysage des menaces vous êtes bien mieux préparé pour contrer les choses indésirables qui se cachent autour de vous. "

Le rapport est axé sur les principaux risques :
1. L'évolution of des APTs
2. Malware au point de vente
3. Fuite de l'information
4. Vulnérabilités
5. Internet des objets …. ou Internet des menaces?

"Nous pouvons tous imaginer combien il est frustrant pour les entreprises de devoir continuellement protéger leurs actifs contre les pirates et les criminels, c'est pour cela que nous avons voulu leur fournir de l'aide avec ce rapport, " commente Marc Mutelet. "Nous avons demandé à nos experts en sécurité de nous fournir une analyse détaillée de ce qu'ils pensent être des menaces émergeantes. Ce rapport est destiné à fournir des informations supplémentaires aux organisations, à les aider à revoir leurs technologies et processus de sécurité et à mettre en place les ressources nécessaires aux endroits stratégiques. "

Le rapport détaillé peut être téléchargé sur :
http://www.welivesecurity.com/wp-content/uploads/2015/02/trends-2015-targeting-corporate-world.pdf.

Vous êtes un chef d'entreprise, un élu, vous souhaitez sensibiliser votre personnel au risque informatique et le sensibiliser aux bonnes pratiques, n'hésitez pas à nous contacter.

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

Source :
http://www.informaticien.be/articles_item-17148-En_2015__les_entreprises_sont_la_premiere_cible_visee_par_la_cybercriminali.html

---

Bases de données : près de 40.000 failles découvertes par des étudiants sarrois

Bases de données : près de 40.000 failles découvertes par des étudiants sarrois

Des étudiants du « Center for IT-Security, Privacy and Accountability » de Sarrebruck (CISPA – Sarre) ont récemment révélé des failles de sécurité portant sur 40.000 bases de données. Ces données, portant sur des entreprises basées en France et en Allemagne, listent des noms, adresses et courriels de millions de clients.

La cause en est une base de données open source mal configurée, utilisée par de nombreux sites de vente en ligne. Si les opérateurs adoptent les paramètres par défaut de ces bases, les données sont alors disponibles en ligne sans protection. Plus grave encore, ces données peuvent être modifiées. Or le fournisseur de la base de données, MongoDB Inc., est l'un des acteurs majeurs du secteur au niveau mondial. Les étudiants à l'origine de cette découverte ont ensuite interrogé un moteur de recherche public pour identifier les entreprises utilisant ces bases de données non protégées.
Selon le CISPA, les étudiants ont notamment détecté une base de données qui pourrait appartenir à un opérateur français de télécommunication, contenant les adresses et numéros de téléphones de huit millions de clients, en France et en Allemagne. Ils ont également identifié la base de données d'un site de commerce en ligne, comprenant des informations de paiement. Ces données facilitent, pour des personnes mal intentionnées, l'usurpation d'identité en ligne. A ce titre, le CISPA a contacté différentes autorités chargées de la protection des données (les « Computer Emergency Response Teams – CERTs », la Commission nationale de l'informatique et des libertés – CNIL, et le Bureau allemand pour la sécurité de l'information – BSI. Le fournisseur a également été informé des problèmes générés par une mauvaise configuration des bases de données par les entreprises clientes.
Le CISPA, rattaché à l'Université de la Sarre, a été fondé en 2011 par le Ministère fédéral de l'enseignement et de la recherche (BMBF) en tant que centre de compétence pour la cybersécurité. En plus de l'Université de la Sarre, l'Institut Max Planck pour l'informatique (MPII), l'Institut Max Planck pour les systèmes logiciels (MPI-SWS), ainsi que le Centre allemand de recherche sur l'intelligence artificielle (DFKI) travaillent conjointement au sein du CISPA. Avec environ 200 chercheurs, le centre est l'un des plus grands centres de recherche sur la cybersécurité en Europe.

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

Source : http://www.bulletins-electroniques.com/actualites/77892.htm

Inquiétudes : Chez Samsung, c’est la télé qui vous regarde

	Inquiétudes : Chez Samsung, c’est la télé qui vous regarde

Attention à ce que vous dites lorsque vous êtes confortablement assis devant votre téléviseur, puisque cela pourrait se retourner contre vous. Si Big Brother vous regardait, la SmartTV de Samsung, elle, vous écoute.

Grâce à sa commande par reconnaissance de la parole, la SmartTV, ce nouveau téléviseur connecté à internet de Samsung peut effectivement enregistrer ce que vous dites et le transmettre à une tierce partie, rapporte The Daily Beast.
Seule une petite mise en garde, noyée quelque part dans la version anglaise de la politique de confidentialité de la SmartTV, informe d'ailleurs les consommateurs quant à cette fonctionnalité permettant au téléviseur d'enregistrer vos conversations.
« **Veuillez prendre note que si vos paroles contiennent des informations personnelles ou sensibles, ces paroles peuvent faire partie des données enregistrées et transmises à une tierce partie.** » La version française de la politique de confidentialité n'en fait d'ailleurs pas mention, souligne Fabien Deglise, dans Le Devoir.
Ainsi, l'appareil de Samsung ne collecte pas seulement les mots que lui dictent les téléspectateurs, mais aussi des bribes des conversations que tiennent les personnes qui sont assises devant l'écran.
Si vous êtes trop paresseux pour utiliser votre télécommande, vous feriez peut-être mieux de vous limiter dans vos sujets de conversation. Comme le remarque The Daily Beast, entre deux épisodes de votre série préférée, ne discutez surtout pas d'évasion fiscale ou de consommation de drogue, parce que cela pourrait se retourner contre vous.
En s'immisçant de la sorte dans les conversations des téléspectateurs, **Samsung pourrait compromettre la vie privée de ses consommateurs**, affirme d'ailleurs le Daily Beast. Les consommateurs devraient pouvoir savoir à qui – et sous quelle forme – leurs informations sont transmises. Si les données transmises ne sont pas codées, les téléviseurs pourraient effectivement se transformer en de véritables postes d'écoute.
En réponse aux inquiétudes soulevées par certains consommateurs, Samsung a dit prendre la vie privée de ses consommateurs très au sérieux. Le géant de l'électronique sud-coréen se veut également rassurant et affirme avoir recours à des techniques d'encodage des données afin d'assurer la confidentialité des informations émises par ses consommateurs.
Samsung insiste aussi sur le fait que la fonctionnalité de commande par reconnaissance de la parole peut être désactivée en tout temps. De plus, la commande vocale ne fonctionne pas si la télévision n'est pas connectée à internet.
Par ailleurs, comme le rappelle Business Insider, le système Siri, qui transmet aussi de l'information à une tierce partie, a déjà fait l'objet de telles inquiétudes.

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

Source : http://www.egaliteetreconciliation.fr/Chez-Samsung-c-est-la-tele-qui-vous-regarde-31023.html

Paiement sans contact : votre carte bancaire risque-t-elle de se faire pirater

Paiement sans contact : votre carte bancaire risque-t-elle de se faire pirater ?

Près de la moitié des cartes bancaires sont désormais équipées de la technologie de paiement sans contact. Un développement à marche forcée qui alimente les craintes de fraude chez les consommateurs.

Une envolée… en toute discrétion. En un an, le nombre de cartes de paiement sans contact en circulation en France a bondi de 50%, pout atteindre 30,3 millions en octobre 2014, selon les derniers chiffres de l'Observatoire du NFC et du sans contact. Elles représentent désormais 47,4% de l'ensemble des cartes bancaires, contre 31% douze mois plus tôt.
Pour savoir si votre carte est dotée de cette technologie, c'est très simple : elle comporte alors un petit logo représentant des ondes se propageant. Si vous ne le saviez pas, rien d'étonnant : les banques ont en effet assez peu communiqué sur le sujet, équipant le plus souvent leurs clients lors d'un renouvellement de carte sans forcément les en informer.

La généralisation de ce nouvel outil de paiement est-elle pour autant synonyme de risque pour consommateurs ? Plusieurs experts en sécurité informatique ont déjà pointé du doigt les potentielles failles de ce système. « Les informations contenues sur cette carte ne sont pas cryptées et peuvent être récupérées très facilement grâce à un smartphone », prévient Thomas Livet, de la société Sifaris.
Nous l'avons testé, le procédé est en effet d'une simplicité enfantine : il suffit de télécharger l'une des multiples applications dédiées disponibles sur la plate-forme d'Android avec un smartphone compatible avec la technologie « NFC », puis de diriger ce téléphone vers une carte bancaire pour obtenir en quelques secondes les 16 numéros inscrits au recto, la date d'expiration et le nom de la banque (voir la capture plus bas). Inquiétant.
Reste que certaines données essentielles ne peuvent pas être aspirées : en particulier le cryptogramme, c'est-à-dire les 3 chiffres inscrits au dos de la carte faisant office de code de sécurité lors d'un paiement en ligne, ainsi que le nom de l'utilisateur. Ce qui complique de fait la tâche des escrocs, puisque la plupart des grands sites de e-commerce français et étrangers demandent ces informations pour valider un paiement. « Evidemment on pourrait concevoir un logiciel pour générer les 999 combinaisons possibles de cryptogramme, mais cela paraît bien compliqué pour ce genre de petites escroqueries », relativise Maxime Chipoy, de l'association de défense des consommateurs, UFC Que Choisir.

Même si la possibilité de se faire escroquer par ce biais n'est pas nulle, le risque de fraude paraît donc limité. Aucune arnaque liée au système de paiement sans contact n'est d'ailleurs pour le moment remontée aux oreilles de l'UFC. Même son de cloche chez CLCV : « Nous avons eu des plaintes relatives au paiement sans contact, mais uniquement concernant le manque de communication des banques sur le sujet, et non en raison d'escroqueries », explique Olivier Gayraud, de l'association.
Certes, la technologie sans contact facilite aussi la tâche des fraudeurs qui arrivent à subtiliser une de ces cartes : ils peuvent en effet l'utiliser sans avoir à taper le code pin, dans n'importe quel magasin équipé de la technologie sans contact. Mais le montant de chaque transaction est limité à 20 euros, et vous devez retaper le code pin une fois dépassé un certain plafond, défini généralement entre 80 et 100 euros selon les banques.
Si vous craignez tout de même de vous faire hacker votre carte, vous avez le droit de demander à votre banque la désactivation de la fonctionnalité de paiement sans contact, voire une nouvelle carte bancaire non équipée de cette technologie. Même si les établissements sont parfois réticents à le faire, n'hésitez pas à insister : « Si votre conseiller s'y oppose, exigez un refus par écrit. Cela devrait suffire à débloquer la situation », conseille Olivier Gayraud. Certaines banques peuvent aussi fournir gratuitement des étuis de protection, faisant office de « cage de Faraday », permettant d'isoler complètement la carte bancaire des ondes extérieures. Il est aussi possible d'acheter ces étuis dans le commerce pour quelques euros, voire des portefeuilles « anti-NFC » moyennant entre 10 et 30 euros.

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

Source : http://www.capital.fr/finances-perso/actualites/paiement-sans-contact-votre-carte-bancaire-risque-t-elle-de-se-faire-pirater-1010288
Par Thomas Le Bars

Objets de santé connectés : l’Ordre des médecins appelle à une régulation

	Objets de santé connectés : l’Ordre des médecins appelle à une régulation

Bracelets capteurs d'activité physique, pèse-personnes connectés ou tensiomètres reliés à un smartphone: le développement « exponentiel » des objets de santé connectés rend nécessaire une « régulation » de ce secteur, a estimé mardi l'Ordre des médecins.

Le Conseil national de l'ordre des médecins (CNOM) a diffusé un « livre blanc » sur la santé connectée, à l'occasion d'un colloque à Paris sur « les enjeux de la santé connectée ».
« Le CNOM se prononce pour une régulation qui impose d'informer l'usager afin qu'il conserve sa liberté dans ce monde connecté et qui assure la fiabilité des technologies et la protection des données personnelles », selon ce livre blanc.
Les objets de santé connectés sont des objets munis de capteurs pour mesurer des paramètres du corps comme le poids, la fréquence cardiaque ou la pression artérielle et qui sont capables de transmettre ces données à une application mobile sur téléphone portable ou à un service web spécifique pour y être stockées et analysées.
Certains de ces objets connectés comme des tensiomètres (pour prendre la tension) ou des glucomètres (pour prendre la glycémie) sont conseillés par des médecins à leurs patients pour leur permettre de suivre plus efficacement des paramètres essentiels à leur santé.
Avec ce livre blanc, l'Ordre des médecins « exprime la nécessité d'une régulation » mais pas nécessairement celle « d'épaissir les volumes du Dalloz sur le droit de la santé », a indiqué le Dr Jacques Lucas, vice-président du CNOM lors du colloque.
L'Ordre fait des propositions pour « définir un cadre du bon usage » de ces outils, alors que les patients sont précisément « en attente de conseils de la part de leurs médecins » sur ces nouveaux objets.
Autre proposition de l'Ordre, l'instauration d'une régulation « adaptée, graduée et européenne » pour ces outils avec comme « minimum » l'obligation d'une « déclaration de conformité à un certain nombre de standards ».
Une telle déclaration devrait porter au moins sur la confidentialité des données recueillies, sur la sécurité informatique et sur la sûreté sanitaire de l'outil en question, selon l'Ordre.
La sécurité et la confidentialité des données sont un point clé dans le domaine de la santé connectée puisque ces outils sont capables de dialoguer avec un téléphone portable ou un site internet dédié.
En France, il est interdit de collecter des données personnelles comme celles liées à la santé, sans l'accord de la personne concernée. La vente de données de santé nominatives est également prohibée.
L'Ordre « appelle à un usage responsable et pragmatique de la santé connectée » et « souhaite que les questions éthiques soulevées par ces technologies donnent lieu à des débats publics ».

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

Source : http://www.notretemps.com/internet/objets-de-sante-connectes-l-ordre-des,i78194