Un label qualitatif pour le Cloud

Un label qualitatif pour le Cloud

Le 9 Décembre 2014, le label « Cloud Confidence » a officiellement été lancé par l'association du même nom. Cette certification est destinée à certifier la qualité d'un service Cloud en matière de sécurisation et de confidentialité des données et ne sera délivrée qu'à des offres à destination d'un des pays de l'Espace Economique Européen (EEE).

L'association « Cloud Confidence », fondée en Juillet 2014, est une association française qui regroupe 15 membres fournisseurs de services et de solutions cloud. Son but étant « de promouvoir la confiance dans les activités de Cloud entre professionnels et utilisateurs ».
Ce label « Cloud Confidence », centré sur la protection et la confidentialité des données clients, n'est pas la seule certification Cloud sur le marché français. Le réseau de clusters numérique « France IT » certifie depuis un an, les offres avec un point de vue généraliste. Plus proche du Cloud Confidence, le référentiel online publié par l'Agence Nationale de la Sécurité des Systèmes d'Information qui évalue le niveau sécuritaire des prestations Cloud.

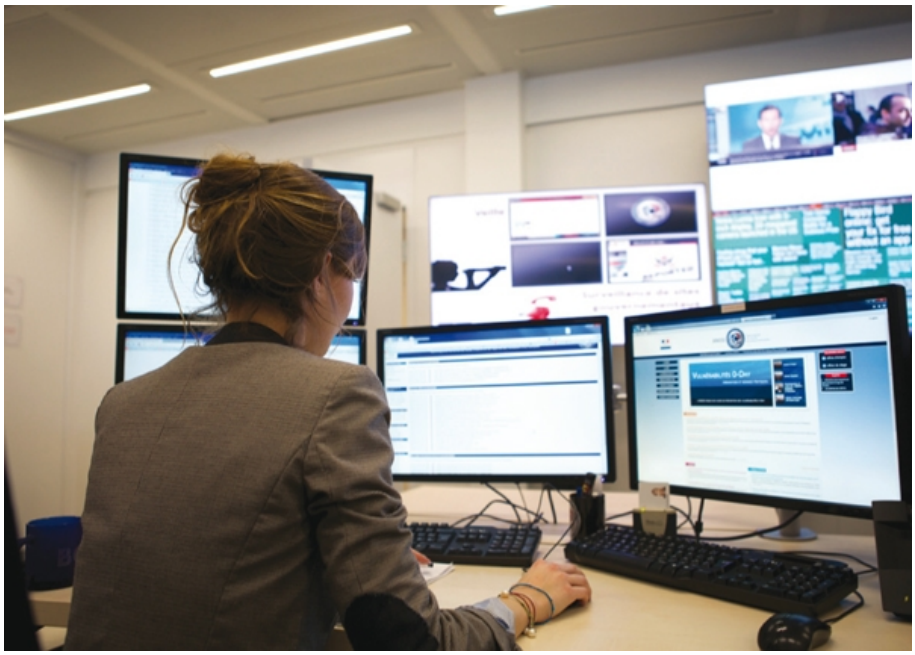
Cette multiplication de labels prouve une nouvelle fois la place de plus en plus importante prise par le Cloud sur le marché des Télécoms depuis quelques années. Il est désormais presque indispensable pour une entreprise de sécuriser au maximum ses données et ce, en passant par une solution Cloud. Les nuages ne sont donc pas forcément annonciateurs de mauvais signes…

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

Source :
http://www.categorynet.com/communiques-de-presse/internet/un-label-qualitatif-pour-le-cloud-20141211224524/

Les cyber attaques dans le

transport maritime



Les cyber attaques dans le transport maritime

La cyber-défense est classée au rang des priorités par le gouvernement. Un plan d'investissement d'un milliard d'euros sur 5 ans a été dévoilé au début de l'année pour faire face à cette nouvelle menace.

Des cyber-attaques qui inquiètent aussi le monde maritime.
« Le transport et la logistique maritimes sont le prochain terrain de jeux des pirates informatiques » : c'est le BMI, le Bureau Maritime International qui le dit..
L'organisme est spécialisé dans la lutte contre la criminalité envers le commerce maritime, notamment la piraterie et les fraudes commerciales ainsi que dans la protection des équipages. Dans un communiqué publié le 20 août 2014, le BMI a tiré la sonnette d'alarme en appelant l'ensemble de secteur à se protéger contre les cyber-attaques..
Si ces cyber-menaces inquiètent c'est parce qu'aujourd'hui dans un bateau, presque tout est informatisé. Tout est connecté à Internet entre la terre et la mer.
Aujourd'hui il est possible pour un hacker (voire un État) de détourner des informations, de prendre le contrôle d'un navire ou même de son système d'armement..
Au début c'était un jeu, c'est devenu une véritable guerre. Vous avez des menaces de ce type-là qui sont organisées comme des réseaux terroristes.

Trafic de drogue, vol de données, kidnapping
Les spécialistes en cyber-défense ont identifié deux menaces principales, comme l'espionnage et le sabotage.
Un « espion » peut par exemple « voler les données techniques » pour connaître avec précisions le trajet emprunté par un bateau. Cela « permet à un concurrent de voler le marché et de pratiquer des prix plus bas », raconte Dominique Riban, de l'ANSSI (Agence nationale de sécurité des systèmes d'information).
C'est elle qui surveille les sites internet de l'État français. Elle a été créée après la publication du Livre blanc de la Défense en 2008.

Télécharger l'intégralité du Livre blanc de la Défense

« Tout est potentiellement attaquable »
L'angoisse des experts en cyber-défense c'est aussi l'attaque des géants des mers, ces containers géants qui débarquent dans les ports européens.
Le plus gros au monde doit transporter 20 000 containers pour une valeur de deux à quatre milliards de dollars. On y trouve tout un tas de systèmes de cartographie, d'informations. Tous ces systèmes là sont potentiellement attaquables.
Patrick Hebrard est titulaire de la chaire Cyber-défense des systèmes navals à l'Ecole navale. Il s'occupe aussi de cyber-défense chez DCNS. « La passerelle peut ne plus avoir la maitrise de sa propulsion et de sa gouverne », poursuit-il. « Un hacker pourrait complètement bloquer la barre d'un bateau. »
En 2011, l'Agence européenne de cyber-sécurité (ENISA) a publié un premier rapport européen sur la cyber-sécurité maritime. Elle évoquait déjà les menaces qui s'amplifiaient. Elles mettaient en garde sur les conséquences désastreuses de ces cyber-attaques.
La même année, le port d'Anvers (dans lequel des milliers de containers sont débarqués chaque semaine sur les quais) avait été piraté par un cartel de la drogue. Ils avaient réussi à récupérer la marchandise avant que les douanes n'inspectent les containers.

Un yacht (volontairement) piraté et détourné
En 2013, un groupe d'étudiants en école d'ingénieurs a fait une expérience en pleine mer : ils ont piraté un yacht de luxe pour le détourner de son trajet initial, en utilisant le système GPS..
C'était en fait un test organisé avec l'accord des propriétaires du bateau. Naviguant de Monaco à l'île de Rhodes, le yacht a été piraté en pleine mer Ionienne. Grâce à un faux boîtier simulateur GPS, ils ont envoyé des signaux de localisation avec de fausses données, des signaux plus forts que ceux transmis par les satellites. Les « faux signaux » se sont donc substitués aux vrais, en les brouillant. Le yacht a alors viré de bord, en modifiant le pilote automatique.
« Les armateurs prennent de plus en plus en compte ces menaces », explique Eric Banel, secrétaire général d'Armateurs de France. « Les politiques d'entreprises contiennent quasiment toutes un chapitre sur la cyber-criminalité. »
Quand aux constructeurs navals, comme DCNS qui construisent des bateaux pour la Marine nationale notamment, ils développent des moyens pour faire face à cette cyber-criminalité maritime, avec aussi des experts présents à terre pour surveiller les flux qui transitent entre la terre et le bateau.
L'école navale, Telecom Bretagne, DCNS et Thales se sont associés pour créer, avec le soutien de la région Bretagne, une chaire de cyber-défense des systèmes navals. Le but est de mettre en œuvre toutes les techniques pour lutter contre les menaces du cyberespace. Cette chaire universitaire mais aussi industrielle ambitionne de stimuler la cyber-innovation. Des chercheurs qui devront trouver des parades à la vulnérabilité des navires en mer, du porte-container au méthanier en passant par les navires de guerre.

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

Source : http://www.franceinter.fr/emission-le-zoom-de-la-redaction-les-cyber-attaques-dans-le-transport-maritime

Un système de traitement automatisé de données personnelles non déclaré à la Cnil ne peut servir de preuve à l’appui d’un licenciement

Un système de traitement automatisé de données personnelles non déclaré à la Cnil ne peut servir de preuve à l’appui d’un licenciement

Les informations collectées par un système de traitement automatisé de données personnelles avant sa déclaration à la Cnil constituent un moyen de preuve illicite, qui doit dès lors être rejeté des débats et par lequel l’employeur ne saurait ainsi justifier un licenciement.

Une assistante en charge de l’analyse financière a été licenciée pour cause réelle et sérieuse, l’employeur lui reprochant une utilisation excessive de la messagerie électronique à des fins personnelles.

La cour d’appel d’Amiens a jugé le licenciement justifié par une cause réelle et sérieuse.

Pour cela, elle a retenu que la déclaration tardive à la Commission nationale de l’informatique et des libertés (Cnil) de la mise en place d’un dispositif de contrôle individuel de l’importance et des flux des messageries électroniques n’avait pas pour conséquence de rendre le système illicite ni davantage illicite l’utilisation des éléments obtenus.

Elle a ainsi considéré que le nombre extrêmement élevé de messages électroniques à caractère personnel envoyés et reçus par l’intéressée durant les mois d’octobre et novembre 2009, respectivement 607 et 621, qui ne pouvait être considéré comme un usage raisonnable dans le cadre des nécessités de la vie courante et quotidienne de l’outil informatique mis à sa disposition par l’employeur pour l’accomplissement de son travail, devait être tenu comme excessif et avait eu un impact indéniablement négatif sur l’activité professionnelle déployée par la salariée durant la même période pour le compte de son employeur, celle-ci occupant une part très importante de son temps de travail à des occupations privées.

Dans un arrêt du 8 octobre 2014, la Cour de cassation censure la décision des juges du fond
Ceux-ci ne se sont en effet fondés que sur des éléments de preuve obtenus à l’aide d’un système de traitement automatisé d’informations personnelles avant qu’il ne soit déclaré à la Cnil, qui constituent pourtant un moyen de preuve illicite et doit dès lors être rejeté des débats.
Par Clément HARIRA

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

S o u r c e : http://droit-public.lemondedudroit.fr/droit-a-entreprises/droit-social/198246-un-systeme-de-traitement-automatise-de-donnees-personnelles-non-declare-a-la-cnil-ne-peut-servir-de-preuve-a-lappui-dun-licenciement.html

La CNIL et l'Inria vont révéler les indiscrétions d'Android

La CNIL et l'Inria vont révéler les indiscrétions d'Android

CNIL va diffuser lundi une étude intéressante montée avec l'Inria. Elle visera à informer les utilisateurs de la masse de données personnelles passant dans les mains de leur smartphone et des applications installées. Une première campagne visait l'iPhone en avril 2013. Cette fois Android sera sur le grill.

Android, passoire ou blockhaus à données personnelles ?
Après une auscultation qui aura duré 3 ans, la CNIL va publier lundi une étude menée à bien avec l'Institut national de recherche en informatique et en automatique (Inria).
L'objet ? Révéler au grand jour les données qui sont enregistrées, stockées et diffusées par les smartphones. Alors que « plus de 30 millions de Français utilisent quotidiennement smartphones et tablettes (…) les utilisateurs savent très peu de choses sur ce qui se passe à l'intérieur de ces « boites noires » » affirment les deux entités dans un communiqué commun.

L'iPhone déjà épinglé en avril 2013
Ce projet de sensibilisation baptisé Mobilitics avait déjà fait l'objet d'une première vague de résultats en avril 2013, mais les attentions s'étaient alors concentrées sur les iPhone. Lors de cette campagne précédente, la CNIL et l'Inria avaient flairé 189 applications pour récolter 9 Go de données sur une période de trois mois. L'opération dénonçait par exemple le fait que trop d'applications et jeux aient pu obtenir l'identifiant unique de l'appareil (46 %) sa géolocalisation (33 % environ) ou avoir accès au carnet d'adresses (8 %) sans toujours pleinement justifier ces indiscrétions ou du moins informer l'utilisateur. Apple avait alors réagi en modifiant certains paramètres, notamment concernant l'accès à l'UDID

« De nombreux acteurs tiers sont destinataires de données, par l'intermédiaire d'outils d'analyse, de développement ou de monétisation présents dans les applications. Les analyses permettent d'identifier plusieurs acteurs recevant des informations récupérées par l'intermédiaire de cookies spécifiques aux applications. Les acteurs classiques du traçage en ligne sont déjà très présents au sein de certaines applications, mais les chiffres montrent également l'émergence d'acteurs nouveaux dédiés au mobile » remarquait alors la CNIL. Du coup, celle-ci réclamait des magasins d'application de nouveaux modes d'information « des utilisateurs et de recueil du consentement. »

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

Source : http://www.nextinpact.com/news/91332-la-cnil-et-l-inria-vont-reveler-indiscretions-d-android.htm

Panorama 2015 des menaces informatiques

	**Panorama 2015 des menaces informatiques**

McAfee, filiale d'Intel Security, publie son nouveau rapport annuel, intitulé '2015 Threats Prediction', qui met l'accent sur les principales menaces prévues pour l'année 2015. McAfee présente conjointement son rapport 'November 2014 Threat Report' relatif à l'analyse des menaces informatiques du dernier trimestre 2014.

Les prévisions 2015 de McAfee en matière de menaces :
1. Une fréquence accrue du cyber-espionnage. La fréquence des attaques de cyber-espionnage continuera d'augmenter. Les pirates actifs de longue date mettront en place des techniques de collecte des informations toujours plus furtives, tandis que les nouveaux venus chercheront des solutions pour subtiliser de l'argent et perturber les activités de leurs adversaires.
Les cyber-espions actifs de longue date travailleront à parfaire des méthodes toujours plus efficaces pour demeurer cachés sur les systèmes et les réseaux de leurs victimes. Les cybercriminels continueront à agir davantage comme des cyber-espions, en mettant l'accent sur les systèmes de surveillance et la collecte de renseignements sensibles relatifs aux individus, à la propriété intellectuelle et à l'intelligence opérationnelle. McAfee Labs prévoit que la cyberguerre sera davantage utilisée par les plus petits États et les groupes terroristes.

2. Attaques fréquentes, profitables et sévères envers l'Internet des objets. A moins d'intégrer le contrôle de la sécurité dès la conception des produits, le fort déploiement de l'IdO devrait dépasser les priorités de sécurité et de confidentialité. La valeur croissante des données pouvant être recueillies, traitées et partagées par ces dispositifs devrait attirer leurs premières attaques en 2015.
La prolifération croissante des appareils connectés dans des environnements tels que la santé pourrait également fournir aux logiciels malveillants un accès à des données personnelles plus sensibles que les données relatives aux cartes de crédit. En effet, selon le rapport de McAfee Labs intitulé « Cybercrime Exposed : Cybercrime-as-a-Service », chacune de ces données représenterait un gain d'environ 10 $ pour un cybercriminel, soit 10 à 20 fois la valeur d'un numéro de carte de crédit américaine volé.

3. Les débats autour de la vie privée s'intensifient. La confidentialité des données sera toujours menacée, dans la mesure où les pouvoirs publics et les entreprises peinent à déterminer ce qui constitue un accès équitable et autorisé à des « informations personnelles » mal définies.

En 2015, les discussions vont se poursuivre pour définir ce que sont les « informations personnelles » et dans quelle mesure elles peuvent être accessibles et partagées par des acteurs étatiques ou privés. Nous allons voir une évolution de la portée et du contenu des règles de la protection des données ainsi que des lois de réglementation de l'utilisation de l'ensemble de données préalablement anonymes. L'Union Européenne, les pays d'Amérique latine, ainsi que l'Australie, le Japon, la Corée du Sud, le Canada et bien d'autres pays adopteront des lois et des règlements de protection des données plus strictes.

4. Les ransomwares évoluent dans le Cloud. Les logiciels de demande de rançon (ransomware) connaîtront une évolution dans leurs méthodes de propagation, de chiffrement et de cibles visées. McAfee Labs prévoit également que de plus en plus de terminaux mobiles essuieront des attaques.

Une nouvelle variante de ransomware capable de contourner les logiciels de sécurité devrait aussi faire son apparition. Elle ciblera spécifiquement les terminaux dotés de solutions de stockage dans le Cloud. Une fois l'ordinateur infecté, le ransomware tentera d'exploiter les informations de connexion de l'utilisateur pour ensuite infecter ses données sauvegardées dans le Cloud. La technique de ciblage du ransomware touchera également les terminaux qui s'abonnent à des solutions de stockage dans le Cloud. Après avoir infecté ces terminaux, les logiciels de ransomware tenteront d'exploiter les informations de connexion au Cloud. McAfee Labs s'attend à une hausse continue des ransomwares mobile, utilisant la monnaie virtuelle comme moyen de paiement de la rançon.

5. De nouvelles surfaces d'attaque mobiles. Les attaques mobiles continueront d'augmenter rapidement dans la mesure où les nouvelles technologies mobiles élargissent la surface d'attaque.
L'émergence de kits de génération de logiciels malveillants sur PC et la distribution de code source malveillant pour mobile permettront aux cybercriminels de désormais cibler ces appareils. Les app stores frauduleux continueront d'être une source importante de malwares sur mobile. Le trafic engendré par ces boutiques d'applications sera notamment conduit par le 'malvertising', qui s'est rapidement développé sur les plateformes mobiles.

6. Les attaques dirigées contre les points de vente augmentent et évoluent avec les paiements en ligne. Les attaques dirigées contre les points de vente demeureront lucratives et l'adoption croissante par le grand public des systèmes de paiement numérique sur appareils mobiles offrira aux cybercriminels de nouvelles surfaces d'attaque à exploiter.

Malgré les efforts des commerçants de déployer des cartes à puce et à code PIN, McAfee Labs prévoit pour 2015 une hausse significative des failles de sécurité liés aux points de vente. Cette prédiction est notamment basée sur le nombre de dispositifs de points de vente devant être upgradés en Amérique du Nord. La technologie de paiement sans contact (NFC) devrait devenir un nouveau terrain propice à de nouveaux types d'attaques, à moins que les utilisateurs ne soient formés au contrôle des fonctions NFC sur leurs appareils mobiles.

7. Logiciels malveillants au-delà de Windows. Les attaques de logiciels malveillants ciblant des systèmes d'exploitation autres que Windows exploseront en 2015, stimulées par la vulnérabilité Shellshock.

McAfee Labs prévoit que les conséquences de la vulnérabilité Shellshock seront ressenties au cours des années à venir par les environnements Unix, Linux et OS X, notamment exécutés par des routeurs, des téléviseurs, des systèmes de contrôle industriels, des systèmes de vol et des infrastructures critiques. En 2015, McAfee Labs s'attend à une hausse significative des logiciels malveillants non-Windows dans la mesure où les hackers chercheront à exploiter cette vulnérabilité.

8. Exploitation croissante des failles logicielles. Le nombre de failles décelées dans des logiciels populaires continuant d'augmenter, les vulnérabilités enregistreront une forte hausse.

McAfee Labs prévoit que l'utilisation de nouvelles techniques d'exploitation telles que la falsification de pile (stack pivoting), la programmation orientée retour (ROP, Return Oriented Programming) et la programmation orientée saut (JOP, Jump-Oriented Programming), combinées à une meilleure connaissance des logiciels 64 bits, favorisera l'augmentation du nombre de vulnérabilités détectées, suivi en cela par le nombre de logiciels malveillants exploitant ces nouvelles fonctionnalités.

9. De nouvelles tactiques d'évasion pour le sandboxing. Le contournement du sandbox deviendra un problème de sécurité informatique majeur.

Des vulnérabilités ont été identifiées dans les technologies d'analyse en environnement restreint (sandboxing) mises en œuvre avec les applications critiques et populaires. McAfee Labs prévoit une croissance du nombre de techniques visant à l'exploitation de ces vulnérabilités ainsi que le contournement des applications de sandboxing. Aujourd'hui, un nombre significatif de familles de logiciels malveillants parviennent à identifier les systèmes de détection de type sandbox et à les contourner. A ce jour, aucun logiciel malveillant en circulation n'est parvenu à exploiter des vulnérabilités de l'hyperviseur pour échapper à un système de sandbox indépendant. Il pourrait en être autrement en 2015.

Pour lire le rapport 'McAfee Labs – Threat Report' dans son intégralité, cliquez ici : http://mcaf.ee/ojbsz

Retour sur 2014
Durant le troisième trimestre 2014, McAfee Labs a détecté plus de 307 nouvelles menaces par minute, soit plus de 5 chaque seconde, avec une croissance des logiciels malveillants sur mobile en hausse de 16 % sur le trimestre, soit une croissance annuelle de 76 %. Les chercheurs de McAfee Labs ont également identifié de nouvelles tentatives visant à tirer profit des protocoles de sécurité Internet, notamment les vulnérabilités de protocoles SSL tels que Heartbleed et BERserk, ainsi que l'abus répété des signatures numériques pour masquer les malwares comme étant légitimes.

Pour 2015, McAfee Labs alerte sur les techniques de cyber-espionnage des pirates informatiques et prévoit que les hackers actifs de longue date mettront en place des techniques de collecte de données confidentielles toujours plus furtives au travers d'attaques ciblées étendues. Les chercheurs du Labs prévoient ainsi de mettre davantage d'efforts sur les vulnérabilités liées à l'identification d'applications, de systèmes d'exploitation et au réseau, ainsi que sur les limites technologiques du sandboxing, dans la mesure où les hackers tentent de se soustraire à l'application de détection par hyperviseur.

« L'année 2014 restera dans les mémoires comme l'année où la confiance en matière de sécurité informatique a été ébranlée », déclare David Grout, directeur Europe du Sud de McAfee, filiale d'Intel Security. « Les nombreux vols et pertes de données ont altéré la confiance de l'industrie envers le modèle d'Internet ainsi que celle des consommateurs dans la capacité des entreprises à protéger leurs données. La confiance des entreprises, ainsi que celle des organisations, ont également étaient impactées et les a poussé à s'interroger sur leur capacité à détecter et à détourner les attaques dont elles ont été la cible », poursuit David Grout. « En 2015, l'industrie d'Internet devra se renforcer pour restaurer cette confiance, mettre en place de nouvelles normes pour s'adapter au nouveau paysage des menaces et adopter de nouvelles stratégies de sécurité qui requièrent de moins en moins de temps dans la détection des menaces. Ainsi, nous devons tendre à un modèle de sécurité intégrée dès la conception de chaque appareil. »

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

Source : http://www.globalsecuritymag.fr/McAfee-Labs-dresse-le-panorama,20141210,49364.html

---

Sony Pictures va piéger les films piratés pour mettre un terme aux fuites

Sony Pictures va piéger les films piratés pour mettre un terme aux fuites

Victime d’un piratage à l’envergure peu commune, Sony Pictures semble être plus que déterminé à mettre un terme à la diffusion de ses fichiers sur le Net. En effet, la filiale du groupe japonais orchestrerait elle-même plusieurs opérations de piratage afin d’empêcher le partage de documents sensibles…

L’information est révélée par le site Re/Code, qui évoque des sources « en connaissance directe du dossier ». Selon celles-ci, Sony Pictures s’appuierait sur les datacenters asiatiques d’Amazon utilisés pour fournir les services cloud du marchand afin de mener une attaque par déni de service sur les sites proposant de télécharger des données issues du récent piratage dont la compagnie a été victime. Et ce ne serait pas tout : le Japonais s’attèlerait également à décourager les curieux en diffusant des copies piégées des fichiers volés.
Rappelons que Sony Pictures a toutes les raisons de chercher à mettre un terme à ces fuites. Outre des films encore inédits, la centaine de To de données volées contenait aussi de nombreux documents personnels d’employés et d’acteurs, des rapports financiers, ou encore des accords confidentiels. Si la diffusion de ces informations a d’ores et déjà occasionné quelques grincements de dents, le Japonais se doit de limiter les dégâts, d’autant que tout ce butin numérique n’est pas encore disponible sur le Web. La méthode, toutefois, peut laisser perplexe.
Cependant, ce n’est pas la première fois qu’un poids lourd des médias combat le feu par le feu. En 2007, plusieurs firmes, dont Sony Pictures mais aussi Universal, EMI, Paramount ou encore Ubisoft avaient été pointées du doigt pour avoir eu recours aux services de MediaDefender, dont les tactiques anti-piratage étaient fort décriées. En effet, ce spécialiste de la défense des intérêts des producteurs de médias pratiquait déjà la diffusion de faux fichiers afin de rendre le piratage franchement laborieux – sans compter qu’il s’était particulièrement illustré par un litige avec The Pirate Bay, qui l’accusait, non sans preuve, d’avoir orchestré une attaque en bonne et due forme contre ses serveurs.

Mais revenons-en à l’affaire qui nous occupe. Pour l’heure, les spécialistes qui se penchent sur le cas de Sony Pictures sont unanimes : il s’agit d’une attaque sophistiquée, qui aurait sans l’ombre d’un doute fonctionné contre une vaste majorité de systèmes. Son origine, toutefois, demeure à confirmer. Bien que les regards se soient d’emblée tournés vers la Corée du Nord, et bien que les pirates aient explicitement demandé l’annulation du film The Interview, qui met en scène l’assassinat de Kim Jong-un par deux journalistes plutôt limités, le régime nie avoir avoir entrepris une quelconque action à l’encontre de Sony Pictures au-delà de ses sommations de renoncer au long-métrage. Une autre piste, de plus, a fait son apparition : une des salves de leaks (fuites) a été orchestrée depuis le très chic hôtel St. Regis, à Bangkok. De quoi s’interroger sur la véritable identité des curieusement vindicatifs Guardians of Peace.

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

Source : http://www.lesnumeriques.com/sony-pictures-mene-attaque-ddos-pour-mettre-terme-fuites-n37601.html
Par Johann Breton

Un « coffre-fort » en ligne pour le stockage des données

Un « coffre-fort » en ligne pour le stockage des données

L'Institut Hasso Plattner (HPI) de Potsdam (Brandebourg) et l'Imprimerie fédérale (Bundesdruckerei) ont convenu d'un partenariat de recherche. Dans le cadre d'un premier projet pilote, un « coffre-fort en ligne » sera développé et mis à la disposition du grand public, de l'administration et des entreprises. Ce système doit permettre à l'utilisateur de stocker et gérer ses données en toute sécurité.

Le HPI, centre de recherche sur les TIC créé et financé par le co-fondateur de l'entreprise SAP, apporte sa technologie « Cloud-RAID » [1]. Les techniques RAID, généralement appliquées aux disques durs, consistent à répartir les données sur plusieurs supports physiques distincts pour améliorer les performances, la sécurité ou la tolérance aux pannes du système. Cette architecture a été adaptée au cloud.

L'Imprimerie fédérale contribue au projet, quant à elle, avec sa plateforme « Trusted Service ». Celle-ci garantit l'identification fiable des utilisateurs du « coffre-fort en ligne » par un document d'identité. La solution, où les données ne doivent être visibles que par l'utilisateur concerné, doit être flexible et facile à utiliser. Plusieurs fournisseurs de cloud sont intégrés au projet, ce qui implique qu'aucun prestataire ne sera, seul, en possession de l'ensemble des données.

Le projet pilote court jusqu'en mars 2015. Afin d'intensifier les recherches en matière de la gestion de l'identité numérique, les deux partenaires prévoient la mise en place d'un laboratoire sur la sécurité au HPI.

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

Source : http://www.bulletins-electroniques.com/actualites/77364.htm

Cyber-sécurité : 10 tendances pour 2015

	**Cyber-sécurité : 10 tendances pour 2015**

L'année 2014 a été particulièrement chargée pour les professionnels de la sécurité informatique. A quoi s'attendre pour 2015 ? Le point avec Thierry Karsenti, directeur technique Europe de Check Point.

Pour l'année 2014, « nous nous attendions à une augmentation des tentatives d'ingénierie sociale, et l'avons bien constatée. Elles ont conduit à d'importantes fuites de données dans plusieurs enseignes bien connues. Les campagnes de logiciels malveillants ciblées se sont également intensifiées. Les attaques de « RAM scraping » et les attaques de rançonneurs ont fait les gros titres. Le nombre de problèmes de sécurité mobile a également continué d'augmenter, indique Thierry Karsenti. Le hic, ce sont les vulnérabilités massives qui ont été découvertes dans des composants informatiques établis, tels que Heartbleed et BadUSB, qui ont touché des dizaines de millions de sites web et d'appareils dans le monde entier. Personne n'y avait été préparé. 2015 verra-t-il les mêmes cyber-risques ?

1. **Les logiciels malveillants « zéro seconde »**

Plus d'un tiers des entreprises auraient téléchargé au moins un fichier infecté par des logiciels malveillants inconnus au cours de l'année dernière. Les auteurs de logiciels malveillants utilisent de plus en plus des outils spécialisés de masquage, afin que leurs attaques puissent contourner les mécanismes de détection des produits antimalwares et infiltrer les réseaux. Efficaces, les bots continueront d'être une technique d'attaque privilégiée, indique Thierry Karsenti.

2. **La mobilité**

Comme vecteurs d'attaque, les appareils mobiles offrent un accès direct à des actifs plus variés et plus précieux que tout autre moyen d'attaque individuel. « C'est également le maillon faible de la chaîne de sécurité, qui donne aux agresseurs un accès à des informations personnellement identifiables, des mots de passe, la messagerie professionnelle et personnelle, des documents professionnels, et l'accès aux réseaux et aux applications d'entreprise », précise le directeur technique.

3. **Les systèmes de paiement mobile**

Le lancement d'Apple Pay avec l'iPhone 6 est susceptible de relancer l'adoption des systèmes de paiement mobiles par les consommateurs, ainsi que d'autres systèmes de paiement concurrents : "Tous ces systèmes n'ont pas été testés pour résister à de réelles menaces, ce qui pourrait signifier d'importantes chances de succès pour les agresseurs qui trouveront des vulnérabilités à exploiter ».

4. **Les failles dans l'open source**

Qu'il s'agisse de Heartbleed (voir l'interview de Patrick Duboys, fondateur d'Alice and Bob http://www.solutions-logiciels.com/actualites.php?actu=14573) ou de Shellshock (voir l'interview vidéo de Vincent Hinderer, expert en cyber-sécurité au Cert du groupe Lexsi http://www.solutions-logiciels.com/actualites.php?actu=15039), les vulnérabilités critiques des plates-formes open source communément utilisées (Windows, Linux, iOS) sont très prisées par les agresseurs car elles offrent d'énormes possibilités. Logiquement, ces derniers vont donc continuer de rechercher des failles pour essayer de les exploiter.

5. **Les attaques sur les infrastructures critiques**

Les systèmes Scada qui commandent les processus industriels devenant de plus en plus connectés, cela va étendre les vecteurs d'attaque qui ont déjà été exploités par des agents logiciels malveillants connus tels que Stuxnet. Près de 70% des entreprises d'infrastructures critiques interrogées par le Ponemon Institute ont subi des attaques au cours de l'année passée.

6. **Les objets connectés**

L'Internet des objets fournit aux criminels un réseau mieux connecté et plus efficace pour lancer des attaques. Les entreprises doivent se préparer à leur impact.

7. **Les réseaux définis par logiciel (SDN)**

La sécurité n'est pas intégrée au concept SDN, « et doit l'être », affirme Thierry Karsenti qui enchérit : « *Avec son adoption croissante dans les centres de données, nous nous attendons à voir des attaques ciblées qui tentent d'exploiter les contrôleurs centraux SDN pour prendre le contrôle des réseaux et contourner les protections réseau* ».

8. **L'unification des couches de sécurité**

Pour lui, les architectures de sécurité monocouche et les solutions isolées provenant de différents fournisseurs n'offrent plus une protection efficace pour les entreprises. Il affirme que de plus en plus de fournisseurs proposeront des protections unifiées issues de développements, de partenariats et d'acquisitions.

9. **Les protections en mode SaaS**

Thierry Karsenti prévoit « une utilisation croissante des solutions de sécurité sous forme de services pour fournir visibilité, contrôle, prévention des menaces et protection des données ». Cette augmentation se fera parallèlement à l'utilisation croissante des services de sécurité externalisés dans le Cloud public.

10. **L'évolution des analyses grâce au Big Data**

Le Big Data va apporter d'énormes possibilités à l'analyse des menaces pour identifier de nouveaux schémas d'attaque, selon l'éditeur. Les fournisseurs intégreront de plus en plus ces capacités analytiques à leurs solutions, et les entreprises devront également investir dans leurs propres systèmes d'analyse pour prendre les bonnes décisions en fonction du contexte et des menaces pesant sur leur activité. Le partage collaboratif de renseignements sur les menaces continuera de se développer, pour proposer des protections à jour qui répondent aux besoins spécifiques des utilisateurs finaux. Le directeur technique de Check Point ajoute que ces possibilités alimenteront à leur tour des solutions de sécurité unifiées capables de fournir automatiquement une protection contre les nouvelles menaces émergentes pour renforcer la sécurité des entreprises.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…
Source : http://www.solutions-logiciels.com/actualites.php?actu=15189&titre=Cyber-securite-10-tendances-pour-2015 Par Juliette Paoli

Sony victime de hackers organisés et obstinés

Sony victime de hackers organisés et obstinés

Outre une société de sécurité mandatée par Sony, le FBI enquête lui aussi sur l'attaque informatique qui a visé récemment une filiale du groupe japonais, Sony Pictures. Et de premiers éléments ont été présentés par les enquêteurs au Sénat américain.

Ainsi comme les experts en sécurité de Mandiant, le FBI estime que l'attaque était inhabituelle et complexe à prévenir. Seules quelques entreprises auraient eu la capacité de bloquer la réalisation d'une telle attaque, estime l'agence fédérale.

Une attaque efficace sur 90% des entreprises

« Le malware qui a été utilisé aurait passé 90% des protections Internet qui sont déployées à l'heure actuelle dans le secteur privé et aurait probablement constitué un défi y compris pour un gouvernement fédéral » a déclaré le directeur adjoint de la division cybersécurité du FBI, Joe Demarest.

A l'occasion de cette audition devant un comité du Sénat, ce dernier a également précisé, selon The Hill, que l'attaqué était organisée et que son niveau de sophistication était extrêmement élevé. Quant à l'identité des auteurs, le FBI estime ne pas pouvoir la déterminer à ce stade, faute de preuves suffisantes.

Des liens avec la Corée du Nord ont été évoqués depuis le début de l'affaire, mais non confirmés. Les autorités du pays ont depuis démenti être à l'origine de cette cyberattaque, après avoir entretenu le flou au départ.

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

Source : http://www.zdnet.fr/actualites/sony-victime-de-hackers-organises-et-obstines-39811145.htm

Un autre programme secret de la NSA cible les réseaux GSM mondiaux

	Un autre programme secret de la NSA cible les réseaux GSM mondiaux

Des documents livrés par Edward Snowden évoquent un programme d'espionnage secret de la NSA. Appelé Auroragold, il cible les membres du GSMA pour recueillir des informations confidentielles sur les failles et les systèmes de cryptage, exploitées ensuite pour s'infiltrer dans les réseaux mobiles.

Selon des informations contenues dans des documents livrés par l'ex-consultant Edward Snowden, la NSA a lancé une campagne secrète pour intercepter les communications internes d'opérateurs et d'acteurs du secteur de la téléphonie mobile dans le but d'infiltrer leurs réseaux partout dans le monde. Dans un article publié samedi par le site The Intercept, qui a également mis en ligne les documents concernés, l'Agence nationale de sécurité américaine a mené, dans le cadre d'un programme appelé Auroragold, des opérations encore jamais rendues publiques.
Deux unités – Wireless Portfolio Management Office et Target Technology Trends Center – mises sur pied par la NSA, ont été chargées de surveiller de près les membres de la GSM Association, espionnant plus de 1200 adresses emails. L'objectif était d'intercepter dans les entreprises visées des messages internes et de recueillir des informations sur les failles de sécurité des réseaux et le cryptage des communications.
Les derniers documents indiquent qu'en mai 2012, sur les 985 réseaux de téléphonie mobile mondiaux, la NSA avait récolté des informations techniques sur 70 % d'entre eux. Mis à part les pays de quelques opérateurs ciblés – Libye, Chine et Iran – le document fourni par l'ancien consultant de l'agence américaine, toujours réfugié en Russie, ne contient aucun nom d'entreprises. Ces opérations d'espionnage ont permis à la NSA de récupérer des documents IR.21 utilisés par les membres de la GSMA pour signaler des failles de sécurité dans leurs réseaux. Les IR21 contiennent également des détails sur les solutions de cryptage utilisées par les opérateurs mobiles. D'après les documents d'Edward Snowden, la NSA, qui n'a pas répondu à une demande de commentaire, s'est servie de ces informations pour contourner le cryptage des communications.

Espionnage tous azimuts
Depuis juin 2013, de nombreux rapports et articles basés sur les documents fournis par Edward Snowden montrent l'étendu des opérations d'espionnage menées par la NSA sur Internet et les réseaux télécoms à travers le monde. Ils ont aussi permis de savoir que la NSA avait piraté les courriels de dirigeants de pays alliés des États-Unis et de découvrir qu'elle avait infiltré les réseaux et les systèmes d'entreprises étrangères, comme c'est le cas du constructeur chinois Huawei. L'an dernier, divers articles parus dans ProPublica, The Guardian et The New York Times, ont révélé que, pendant plusieurs années, la NSA s'était employée à affaiblir les normes de sécurité pour faciliter les opérations d'espionnage à grande échelle du gouvernement américain. Par exemple, des articles publiés en septembre 2013 par le Guardian et le NYT indiquent, sur la base des documents de Snowden, que la NSA a créé sa propre version du standard Dual_EC_DRBG (Dual Elliptic Curve Deterministic Random Bit Generator), un générateur de nombres aléatoires utilisé en cryptographie. Cette norme, approuvée pour un usage mondial en 2006, contiendrait une porte dérobée permettant à la NSA de s'introduire dans les systèmes de communications. Dès 2007, certains spécialistes et l'éditeur lui-même, RSA Security, recommandaient de désactiver par défaut le Dual_EC_DRBG. Des documents divulgués par Edward Snowden l'an dernier ont également apporté la preuve que la NSA pouvait espionner le trafic GSM chiffré avec l'algorithme A5/1.

Fin novembre, Symantec et Kaspersky Labs ont révélé l'existence d'un malware baptisé Regin, probablement développé par les États-Unis. Actif depuis au moins six ans, Regin cible les réseaux cellulaires GSM pour espionner les gouvernements, les infrastructures des opérateurs de téléphonie mobile, des instituts de recherche, des entreprises et des particuliers. En plus de ces opérations secrètes, la NSA espionne collectivement les conversations téléphoniques des citoyens américains. Le mois dernier, le directeur de la NSA, Michael Rogers a déclaré que l'agence ne prévoyait pas de réviser son programme de collecte : un projet de loi déposé devant le Sénat pour encadrer cette collecte n'a pas abouti.
Glenn Greenwald et Laura Poitras, les deux éditeurs et fondateurs du site The Intercept, ont déjà aidé Edward Snowden à diffuser ses documents par le biais de différents médias.

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

Source : http://www.lemondeinformatique.fr/actualites/lire-un-autre-programme-secret-de-la-nsa-cible-les-reseaux-gsm-mondiaux-59530.html
Par Jean Elyan / IDG News Service