Sony adopte de nouvelle règles de sécurité – PS4, PS3, PS Vita News – Play3-Live

	Sony adopte de nouvelle règles de sécurité

Comme nous avons pu le voir depuis quelques jours, ni Sony, ni Microsoft ne sont à l'abri d'action malveillante de la part d'un certains groupe d'individus mal intentionné. Suite aux différents hacks dont il fut victime récemment, Sony se rend compte qu'une protection en ligne appropriée est nécessaire pour garder les clients et les parties prenantes heureuses, ils sont donc dans l'optique d'une embauche d'un nouveau directeur du management d'ingénierie en vulnérabilité pour prévenir d'autres incidents.

L'offre d'emploi stipule que le candidat retenu sera responsable de ce qui suit:
• Unifier et améliorer l'architecture de sécurité mondiale du groupe, inclure une stratégie de gestion de la vulnérabilité cohérente englobant toutes les sociétés du groupe Sony
• Servir en tant qu'expert technique référent en matière de sécurité et conseiller pour les initiatives prioritaires de sécurité
• Gérer les équipes d'ingénieurs et développeurs hautement qualifiés, conduire et orienter la pensée, le développement de carrière, le mentorat et les conseils techniques
• Superviser l'élaboration de systèmes de gestion de la vulnérabilité, des initiatives, intégration et l'assistance d'évaluation technique
• Diriger des équipes et coordonner les efforts ou initiatives concernant les tests de pénétration, le système et la gestion de la vulnérabilité de l'application, l'évaluation globale des risques techniques, et les opérations de chasse
• Développer et affiner des normes techniques de sécurité de l'information, des directives et de la formation
• Soutenir la coordination des activités de planification budgétaire de l'entreprise liées à des outils d'information et de services de sécurité, afin d'inclure le leadership des activités de planification d'entreprise de milieu de gamme
• Appuyer la gestion, la planification et l'exécution du budget de l'ingénierie de la sécurité mondiale
• Assembler et entraîner divers ensembles de l'information et des intervenants experts sécurité dans la formulation des exigences de sécurité de l'information unifiée et des normes d'architecture pour la plupart des projets et contrats du groupe
• Servir en tant qu'expert en la matière fournissant des services consultatifs intra-entreprise liés à la stratégie de l'architecture de sécurité et de mise en œuvre de la technologie
Vous l'aurez compris, Sony semble apprendre de ses erreurs et chercher une pointure dans le domaine de la sécurité afin de ne plus être victime des soucis rencontrés il y a quelques heures encore.

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

Source : http://www.play3-live.com/news/sony-adopte-de-nouvelle-reegles-de-seecuritees-70376

DDoS du PSN – Nous avons discuté avec un membre de Lizard Squad

	DDoS du PSN – Nous avons discuté avec un membre de Lizard Squad

Après trois jours de coupure, de connexion impossible et d'erreur de maintenance, le PSN semble, ce matin, plutôt accessible pour la plupart des joueurs autant sur PS4 que PS3 et PS Vita. Hier, dans la soirée, un membre de Lizard Squad a souhaité rentrer en contact avec nous, pour nous proposer quelques informations. Nous avons donc pu discuter par message écrit avec @AironeHD, qui nous en dit plus sur les causes du DDoS du PSN de Sony, et la durée souhaitée des coupures de ce même PSN.

Lizard Squad veut montrer l'incompétence de Sony

Ce qui ressort de notre interview avec l'un des contributeurs français de Lizard Squad est que le groupe de hackeur ne souhaite pas faire de mal aux joueurs. Non, la motivation est de prouver que Sony est incompétent dans sa gestion du PSN : « Nous ne sommes pas méchants nous voulons simplement « troller » ces chefs incompétents, incapables de protéger des serveurs alors qu'ils ont les moyens financiers pour le faire. » Nous apprenons également au cours de l'interview que le souhait premier de Lizard Squad n'est pas de pirater les comptes PSN et Xbox Live pour récupérer des données personnelles et bancaires, mais simplement de bloquer les serveurs online.

Lorsque nous avons demandé à AironeHD quel était le motif des attaques, celui-ci nous a répondu : « Montrer tout simplement aux chefs de Sony (avant, Microsoft également, mais plus maintenant) que leurs systèmes de sécurité sont faibles. Et que tout le monde (informaticien assez doué) peut rentrer dans leurs systèmes. Et que l'on soit connus pour nos actes. »

Le PSN sera perturbé tant que Sony ignorera Lizard Squad

Nous avons ensuite demandé à AironeHD combien de temps allait durer les coupures régulières du PSN. La réponse est claire et non équivoque : « C'est une durée indéterminée, impossible de vous dire pour l'instant. On ne compte pas lâcher. Les chefs de Sony essayent de nous ignorer. Alors nous continuons. » Enfin, nous avons tenté de savoir pourquoi le Xbox Live était moins perturbé que le PSN. Le membre de Lizard Squad déclare vaguement que les attaques échoueraient assez souvent, et qu'il était donc plus compliqué de mettre à terre le Xbox Live que le PSN. Pour les indisponibilités des serveurs EA et Activision (FIFA et Call of Duty: Advanced Warfare), les actes de Lizard Squad sont simplement du « troll » selon AironeHD.

N.B – Cette interview avec un membre présumé de Lizard Squad en France est à but uniquement informative. Tout comme les autres membres du groupe de hackeur sur Twitter, nous ne pouvons pas prouver l'implication de AironeHD dans les attaques DDoS du PSN via des pièces justificatives. Ces déclarations ne sont donc pas des preuves, mais un bon aperçu de ce que souhaite vraiment faire Lizard Squad. Merci de votre compréhension.

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

Source : http://playerone.tv/news/v/6352/ddos-du-psn-nous-avons-discut%C3%A9-avec-un-membre-de-lizard-squad.html

---

Google enterre le 'captcha' et le remplace par une simple

case à cocher…

Google enterre le 'captcha' et le remplace par une simple case à cocher…

Le moteur assure que son nouveau dispositif d'authentification permet de contrer les robots. Il est notamment basé sur l'analyse des mouvements du curseur.

Qui ne s'est pas déjà énervé devant ces maudits captchas à entrer pour accéder à tel ou tel service en ligne ou contenu ? Rappelons qu'il s'agit d'un dispositif d'authentification basé sur des lettres (parfois illisibles) à recopier dans une case, afin de bloquer l'action de robots. Or, pour Google, cette technologie est aujourd'hui obsolète car faillible.

Le moteur a ainsi mis au point un algorithme qui contourne cette protection avec un taux de réussite de 99,8%…

Dans une note de blog, le géant affirme avoir mis au point un nouveau dispositif, « No Captcha reCaptcha », bien plus simple à utiliser par l'internaute. En effet, il suffit de cocher une case afin de prouver que l'on est bien un humain et pas un robot. Suffisant ?

C'est en effet la partie émergée de l'iceberg. La technologie de Google, basée sur l'intelligence artificielle, exploite des processus sophistiqués comme l'analyse du mouvement du curseur afin de valider que c'est bien un humain qui est à l'autre bout de la souris. Adresse IP et cookies sont également analysés.

Des géants du Web comme Snapchat et WordPress vont utiliser ce dispositif, affirme Google. Des tests menés actuellement montrent que la technologie fonctionne dans 80% des cas. Pour les 20% restants, un Captcha classique est alors demandé. Il reste donc des ajustements à réaliser…

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

Source : http://www.zdnet.fr/actualites/google-enterre-le-captcha-et-le-remplace-par-une-simple-case-a-cocher-39810785.htm

---

Le gouvernement étend les

pouvoirs de l’ANSSI

Le gouvernement étend les pouvoirs de l’ANSSI

Un décret publié au Journal Officiel est venu étendre les capacités de l’ANSSI. Le directeur et son adjoint pourront maintenant signer des actes au nom du Premier ministre lorsque ceux-ci tombent sous sa juridiction.

Choc de simplification pour l’Agence Nationale de Sécurité des Systèmes d’Information : dans un décret paru au Journal Officiel et repéré par NextInpact, l’exécutif simplifie le processus décisionnel à la tête de l’agence en permettant à son directeur et à ses adjoints de signer au nom du Premier ministre les décisions relatives aux affaires relevant de son domaine de compétence.
Plus précisément, le décret renvoie à la loi de 2009 relative à la création de l’ANSSI et qui stipule les domaines de compétences de l’agence : la qualification et certification des produits de sécurité, la vérification de signatures électroniques, la gestion des autorisations concernant les outils de chiffrement ainsi que les logiciels d’interceptions ou d’espionnage informatique soumis à plusieurs restrictions.
Le premier ministre pourra donc déléguer se pouvoir au directeur de l’ANSSI (actuellement Guillaume Poupard) et ce dernier pourra ensuite déléguer ce pouvoir à son adjoint. Un moyen pour l’ANSSI, qui a été placé au centre des initiatives du gouvernement sur la cybersécurité et la cyberdéfense, de simplifier son processus décisionnel et accroître sa réactivité.

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

Source : http://www.zdnet.fr/actualites/le-gouvernement-etend-les-pouvoirs-de-l-anssi-39804445.htm
Par Louis Adam

Le nouveau PrivatOS de Blackphone optimise la confidentialité des

utilisateurs tout en proposant un accès aux applications

	Le nouveau PrivatOS de Blackphone optimise la confidentialité des utilisateurs tout en proposant un accès aux applications

Blackphone a annoncé le lancement prochain de la plus importante mise à jour apportée jusqu'à présent à son système d'exploitation personnalisé PrivatOS. Prévue pour début 2015, cette nouvelle version de PrivatOS introduit Spaces, qui confère aux utilisateurs la possibilité unique de créer des « espaces » indépendants et distincts pour les applications, données et comptes – le tout sur un seul et même appareil.

Le nouveau PrivatOS de Blackphone optimise la confidentialité des utilisateurs tout en proposant un accès aux applications.
• La prochaine mise à jour majeure de PrivatOS inclura « Spaces » qui permet la création d'environnements indépendants et multiples sur un seul et même appareil.
• Blackphone proposera la première boutique d'applis au monde dédiée à la confidentialité.
• Le PDG de Blackphone, Toby Weir-Jones, estime que ce lancement va changer la donne pour la marque
• PrivatOS1.1 vous permet de prendre le contrôle sur votre confidentialité, sans recourir aux compromis habituels

Avec la plupart des smartphones, cloisonner l'univers professionnel et celui du divertissement est synonyme de compromis entre confidentialité et commodité : les applications et données professionnelles cohabitent au même endroit que les jeux personnels et les applications de médias sociaux, ou les utilisateurs possèdent deux appareils afin de garantir la confidentialité et le cloisonnement des deux univers. L'utilitaire Spaces est capable de cloisonner vie professionnelle et vie privée, univers réservé aux adultes et univers pour enfants, ou toute autre séparation que souhaitent mettre en œuvre les utilisateurs – sans compromis nécessaire.
Un espace « Silent Space » est proposé par défaut, qui inclut la Silent Suite d'applications destinées à la communication cryptée, la boutique d'applis de Blackphone ainsi qu'un ensemble d'applications de confidentialité pré-chargées. À partir de là, vous avez la possibilité de créer des Spaces (espaces) supplémentaires à votre convenance – quels que soient vos besoins – grâce au Centre de sécurité Blackphone ainsi qu'à PrivatOS qui assurent tous deux votre sécurité.
Le lancement en parallèle de la boutique d'applis de Blackphone – première boutique au monde exclusivement ciblée sur les applications de confidentialité – vient renforcer la position de Blackphone en tant que leader mondial de la confidentialité et de la sécurité.
Disponible en janvier 2015, la boutique d'applis de Blackphone propose un ensemble d'applications spécifiquement conçues par Blackphone qui constituent les applications les plus sécurisées du marché en termes d'optimisation de la confidentialité. Un certain nombre d'applications pré-chargées seront immédiatement disponibles dans le cadre de la mise à jour de la dernière version de PrivatOS au début de l'année 2015.

S'exprimant au sujet de ce lancement, Toby Weir-Jones, PDG de Blackphone, a déclaré :
« L'ajout de Spaces et de la boutique d'applis de Blackphone représente la mise à jour la plus importante apportée à PrivatOS depuis sa création, et devrait considérablement changer la donne pour la marque, en soulignant davantage notre engagement visant à redonner aux utilisateurs le contrôle sur la confidentialité de leurs données. Nous sommes ravis d'avoir développé Silent Space, aux côtés de Graphite Software, qui partage nos valeurs fondamentales en matière de confidentialité et de sécurité. »

S'exprimant au sujet de sa collaboration avec Blackphone, Alec Main, PDG de Graphite Software, a déclaré : « Blackphone est l'unique appareil qui place la question de la confidentialité au-dessus de tout. L'intégration de Secure Spaces de Graphite dans PrivatOS de Blackphone offre aux consommateurs la possibilité de bénéficier d'une expérience d'applications enrichie et d'un appareil professionnel convergent, tout en gardant le contrôle sur leurs informations personnelles. »

Blackphone, qui a été lancé en mars 2014, est le premier smartphone au monde spécifiquement conçu pour maximiser la confidentialité de l'utilisateur, plaçant la confidentialité des utilisateurs avant toute autre chose. Pour tous ceux désireux de prendre le contrôle sur leurs informations personnelles, Blackphone et son système d'exploitation bénéficiant d'une sécurité optimisée, PrivatOS, conçu sur Android™ KitKat, confèrent aux utilisateurs protection et contrôle sur les questions de sécurité auxquelles ils sont confrontés, sans les compromis habituels.

À propos de Blackphone/SGP Technologies SA
SGP Technologies est le fabricant de Blackphone, meilleur téléphone Android axé sur la confidentialité pour un usage personnel et au sein de l'entreprise. Créée en tant que coentreprise entre le fournisseur de communication sécurisée reconnu à l'échelle mondial, Silent Circle, et le fabricant espagnol primé de l'appareil mobile, GeeksPhone, SGP Technologies est basée à Genève, en Suisse, avec des opérations majeures à Madrid, à Washington DC, dans la Silicon Valley et dans plusieurs villes réparties à travers l'Europe, l'Asie, et l'Amérique du Nord. Pour en savoir plus sur Blackphone, rendez-vous sur https://www.blackphone.ch.

À propos de Graphite Software
Secure Spaces de Graphite pour Android permet aux utilisateurs de bénéficier des applications et des services qu'ils souhaitent, sans perdre le contrôle sur leurs données personnelles. Proposant à la fois des « Spaces » (espaces) personnels et gérés, le potentiel d'utilisation ne se trouve limité que par l'imagination du propriétaire de l'appareil, ou par un programmateur du cloud. En proposant des « Spaces » (espaces) multiples sur un seul et même appareil, Graphite Software redéfinit l'expérience mobile des utilisateurs. Pour en savoir plus sur Graphite Software, rendez-vous sur http://www.graphitesoftware.com

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

Source : http://www.pockett.net/n25303_Android_Le_nouveau_PrivatOS_de_Blackphone_optimise_la_confidentialite_des_utilisateurs_tout_en_proposant_un_acces_aux_applications

Chronique de Jawad Kerdoudi, président de l’IMRI: « La cybercriminalité, migration du crime réel vers le virtuel »

	Chronique de Jawad Kerdoudi, président de l’IMRI: « La cybercriminalité, migration du crime réel vers le virtuel »

Comme chaque semaine, l'Institut Marocain des Relations Internationales (IMRI) publie une chronique sur l'actualité. Cette semaine, son président Jawad Kerdoudi s'est intéressé à « La cybercriminalité, migration du crime réel vers le virtuel ».

La récente attaque aux Etats-Unis des systèmes informatiques de Sony Pictures relance le problème de la cybercriminalité. Celle-ci est définie comme l'ensemble des infractions pénales spécifiques liées aux technologies de l'information et de la communication. Ces infractions concernent plusieurs secteurs tels que le « carding » qui porte sur le piratage des cartes bancaires, le « skimming » criminalité qui s'attaque aux automates, le « phising » qui est une pêche des informations bancaires et commerciales, et enfin les escroqueries sur internet de toutes sortes qui englobent la xénophobie, la pedopornographie, l'incitation à l'usage des stupéfiants, le proxenétisme, le terrorisme, et le piratage téléphonique au préjudice des opérateurs.
Ce phénomène prend de plus en plus d'ampleur avec le développement d'internet qui est certes un moyen formidable de communication, mais également un instrument puissant de pouvoir et de guerre. Selon le Computer Crime Research Center, seuls 12% des cybercrimes étaient connus par la police et la justice en 2004. Plusieurs scandales ont défrayé la chronique, dont celui de la NSA en 2013 provoqué par Edward Snowden. Le coût global des cyberattaques a été estimé à 300 milliards d'euros pour les entreprises en 2013. Les Etats-Unis perdent entre 17,5 à 87,5 milliards d'euros par an, et 556 millions de personnes dans le monde ont été victimes de cybercriminalité. Cette situation risque d'empirer du fait du développement extraordinaire des investissements dans le secteur technologique numérique tels que ADSL, L4G, WIFI, Cloud. Le phénomène risque de s'amplifier également par la dématérialisation des processus, le développement du e-commerce et du e-learning, la croissance des paiements en ligne, l'augmentation des utilisateurs du Web qui a enregistré un taux de croissance de 46% entre 2012 et 2013. Le haut lieu mondial de la cybercriminalité pour la création de logiciels malveillants est la Chine, suivie par la Russie, les Etats-Unis, le Brésil et le Royaume-Uni. Pour les machines détournées la première place appartient aux Etats-Unis, suivie par la Chine, la Corée du Sud, l'Allemagne et la France. Enfin par les crimes relatifs aux arnaques sur internet, la palme revient à l'Afrique en particulier la Côte d'Ivoire et le Nigeria.

MINIMISER LES CONSÉQUENCES DE L'ATTAQUE
Pour se protéger contre la cybercriminalité, il est clair que le risque zéro n'existe pas. Il faut faire en sorte que si elle arrive, les conséquences de l'attaque soient minimes. Il faut pour cela renforcer les moyens matériels et humains, procéder à une modification de la législation, développer une culture de l'informatique, et associer le secteur privé à la lutte contre ce fléau. Il faut également privilégier l'approche préventive, c'est-à-dire qu'il faut augmenter les difficultés des attaques en diminuant les profits potentiels. Cela signifié le renforcement de la robustesse des infrastructures informatiques et de télécommunications. Il faut enfin s'appuyer sur des structures de veille et d'alerte telles que le CERT/CC américain. La coopération internationale est indispensable, car les pays qui ne sont pas dotés de lois contre la cybercriminalité sont des paradis numériques, où les cybercriminels peuvent lancer des attaques informatiques ou héberger des sites illicites en toute impunité. Elle a déjà commencé par la Convention de Budapest du 23 Novembre 2001 sur la cybercriminalité qui a le mérite de régler les problèmes de compétence et d'entraide entre Etats, et de les obliger à conserver certaines données pour permettre le traçabilité de l'information. Elle énumère plusieurs infractions (accès illégal, interception illégale, atteinte à l'intégrité des données et des systèmes) pour lesquelles chaque pays doit avoir un volonté politique et une coopération efficace de leurs services de justice et de police. Cette coopération internationale pose le problème de la gouvernance d'internet sur le plan mondial. Certains s'interrogent sur la pertinence d'une réglementation, d'autres demandent qu'elle soit déclarée comme un bien commun, et placée sous le contrôle de l'ONU ou d'un organisme intergouvernemental autonome.

QU'EN EST-IL DE CETTE QUESTION DE LA CYBERCRIMINALITÉ POUR LE MAROC ?
D'après Microsoft, le Maroc est 3,5 fois plus vulnérable aux logiciels malveillants que la moyenne mondiale. Le Maroc présente des failles touchant l'administration et les infrastructures qui constituent des menaces pour la sécurité nationale publique et économique. Preuve en est le piratage à partir du mois d'Octobre 2014 de documents confidentiels marocains relatifs à la diplomatie, au Sahara, et aux services de l'appareil de l'Etat. Le cybercriminel se fait appeler Chris Coleman, sévit sur un compte Twitter et n'a pas caché son objectif de nuire au Maroc. Une lecture officielle de ce cybercrime a été présentée le 11 Décembre 2014 devant la Chambre des Conseillers accusant les services spécialisés algériens d'avoir monté et accompagné cette opération. Dès lors, il faut que la cybercriminalité soit un chantier prioritaire pour le gouvernement, et passe du stade défensif à celui offensif. D'où la nécessité de créer une structure civile placée à un haut niveau, et qui aura par vocation la centralisation des informations et la coordination entre les services civils et militaires. Elle doit disposer également d'un centre de documentation chargé recueillir les statistiques spécifiques en vue de les analyser. Elle devra jouer un rôle opérationnel, signaler les contenus illicites sur internet, et apporter une assistance technique au profit du secteur public et privé. Elle sera également chargée de la formation et de la sensibilisation, et assurera les relations avec les Agences internationales chargées de lutter contre la cybercriminalité.

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

Source : http://www.aufait.ma/2014/12/23/chronique-de-jawad-kerdoudi-president-de-limri-la-cybercriminalite-migration-du-crime-reel-vers-le-virtuel_635947
par Jawad Kerdoudi, président de l'IMRI

La cybersécurité a-t-elle une obligation de résultat ?

La cybersécurité a-t-elle une obligation de résultat ?

Obligation de résultat ou obligation de moyens : qu'est-ce que cela implique en matière de cybersécurité ? Olivier Iteanu, avocat à la Cour (www.iteanu.com), nous livre son analyse et revient sur la sanction infligée à Orange par la Cnil.

Chacun conviendra qu'il est absurde de considérer que la sécurité en général, et plus particulièrement celle attachée aux systèmes d'information, soit soumise à une obligation de résultat. Aucune technologie, aucun système de défense n'est capable de garantir une fiabilité à 100 % contre toute attaque. L'éditeur d'une solution ou le prestataire qui prétendrait le contraire serait tout simplement un menteur. L'esprit humain est ainsi fait, et c'est tant mieux, qu'un jour ou l'autre, l'attaquant, venu de l'extérieur ou plus encore, de l'interne, trouve le moyen de contourner les meilleures protections techniques et organisationnelles mises en place.
Le pendant de l'obligation de résultat ou son contraire, est l'obligation de moyens. Dans le cas de l'obligation de moyens, si l'attaque a causé des dommages à des tiers, ceux-ci ne peuvent se retourner contre le maître du système attaqué pour obtenir réparation que si une négligence ou une faute prouvées peut être retenue contre lui. Dans le cas de l'obligation de résultat, le tiers n'aura qu'à démontrer l'existence de l'attaque et son dommage, pour engager la responsabilité du maître du système, sans même avoir à démontrer que ce dernier a commis une faute. Evidemment, on comprend ici que les conséquences de l'un ou de l'autre régime juridique sont radicalement différentes.
On est en droit de se demander si le système plein de bon sens de l'obligation de moyens en matière de cybersécurité, n'est pas remis en cause par une décision récente de la Commission Nationale de l'Informatique et des Libertés du 7 août 2014, qui a sanctionné Orange pour manquement à l'obligation de sécurité prévue à la Loi informatique et libertés.
http://www.cnil.fr/fileadmin/documents/approfondir/deliberations/Formation_contentieuse/D2014-298_avertissement_ORANGE.pdf

Que dit la loi ?
Pour mémoire, la Loi du 6 janvier 1978 en son article 34 prévoit que « Le responsable du traitement est tenu de prendre toutes précautions utiles (…) pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. » Le défaut de prendre « toutes précautions utiles » est sanctionné des peines maximales de 5 ans de prison et de 300 000 € d'amende par l'article 226-17 du Code pénal. Et comme la matière informatique et libertés prévoit une double peine aux contrevenants à la Loi, la Cnil peut également prendre une sanction dite administrative à l'encontre du responsable du traitement défaillant. Les sanctions de la Cnil peuvent être pécuniaires, jusqu'à 300 000 € en cas de récidive et portent surtout atteinte à l'image du condamné, car ces sanctions sont publiques, donnent lieu à publication, et sont régulièrement reprises par la presse et les médias.

Orange attaqué… et condamné
Une décision récente de la Commission Nationale de l'Informatique et des Libertés du 7 août 2014 a sanctionné Orange pour manquement à l'obligation de sécurité prévue à la Loi informatique et libertés. Dans l'affaire jugée, Orange était alertée en mars 2014 par un client et découvrait que le serveur d'un prestataire de l'opérateur « chargé de réaliser certaines campagnes de marketing direct » par courriel avait été piraté. Plus de 1,3 millions de clients d'Orange étaient impactés par cette attaque. L'enquête révélait qu'Orange avait confié à un premier prestataire la mission de réaliser des campagnes de emailing auprès de ces clients. Ce prestataire avait lui-même sous-traité la prestation à un prestataire secondaire. C'est ce dernier qui était piraté.

Le lien de désinscription, qui se trouvait au bas du courriel de prospection, menait par une modification de l'URL aux 700 fichiers de prospects et de clients d'Orange, permettant à l'indélicat à les aspirer. Le 25 avril 2014, Orange notifiait la faille de sécurité à la Cnil comme elle y est contrainte depuis le Paquet Télécom d'août 2011 et un Règlement 611/2013 de la Commission européenne du 24 juin 2013. Le 5 mai 2014, la presse s'emparait de l'affaire. Une semaine plus tard, la Cnil diligentait sur deux jours un contrôle dans les locaux d'Orange qui révélait les circonstances dans lesquelles les 700 fichiers de clients et prospects avaient été aspirés. Orange déposait une plainte pénale. Mais Orange était également convoquée devant la formation contentieuse dite restreinte de la Cnil, qui lui infligeait un avertissement public le 9 août 2014 pour manquement à l'obligation de sécurité.

Orange se trouvait donc à la fois victime et responsable. Ce qui nous interpelle dans cette décision, ce sont les motifs retenus par la Cnil pour sanctionner Orange. Le premier grief est que selon l'autorité française, Orange « n'a pas fait réaliser d'audit de sécurité sur la version de l'application technique spécifiquement développée par son prestataire secondaire. » Face à la généralité de l'obligation imposée par la Cnil, on cherche désespérément la base légale à ce grief. Mais à supposer celui-ci fondé, on peut penser que le prestataire secondaire a, quant à lui et en sa qualité de professionnel, procédé à cet audit. Tenir Orange, le client dans cette relation, responsable au motif qu'elle n'a pas procédé à cet audit devrait glacer le sang de tous les clients utilisateurs. Le second motif nous paraît, quant à lui, lunaire. La Cnil reproche à Orange d'avoir « communiqué de manière non sécurisé les mises à jour de ses clients » à ses prestataires. L'enquête avait certes révélé qu'Orange avait transmis les 700 fichiers de ses clients et prospects par simple courriel, mais la même enquête a établi que ce n'est pas durant cette communication que les fichiers ont été captés. Cette communication ne serait donc pas en cause. Enfin, la Cnil reproche à Orange « qu'aucune clause de sécurité et de confidentialité des données n'était imposée à son prestataire secondaire »,c'est-à-dire au sous-traitant du sous-traitant d'Orange, c'est-à-dire la société avec laquelle elle n'a pas de contrat … C'est compte tenu de ces « défaillances » que la Cnil entre en voie de condamnation à l'encontre d'Orange.

Cette décision nous amène à deux commentaires sous formes de conclusions.
D'une part, il y a un auteur à cette infraction, « quelque part dans le monde » qui a accédé illicitement aux serveurs et a procédé à l'aspiration des fichiers. Les adresses IP relevées par les serveurs du prestataire attaqué ont désigné des pays lointains. Dans ce genre d'affaires, l'enquête judiciaire est souvent en panne. L'enquête bute en effet sur des difficultés de coopérations policières et judiciaires en termes de délais, de paperasserie et de coûts quasi insurmontables, sans compter que certains pays ne coopèrent tout simplement pas. Dans ce contexte, le seul condamné de l'histoire a toutes les chances d'être la victime, Orange. Il y a tout de même ici quelque chose de choquant sur le fond. En outre, c'est Orange qui a notifié elle-même la faille à la Cnil par application de la Loi certes. Si chaque notification donne lieu à condamnation de son auteur, ceux-ci risquent désormais de réfléchir à deux fois avant de se lancer dans ce qui apparaît comme « la gueule du loup ».

D'autre part, les griefs retenus à l'encontre d'Orange nous paraissent d'une interprétation des plus sévères des précautions utiles de l'article 34 de la Loi de 1978 et surtout très généraux, laissant dans le désarroi et l'insécurité juridique tous utilisateurs des systèmes d'information et de leurs services. Enfin, faire tenir Orange responsable des agissements du sous-traitant de son sous-traitant paraît déraisonnable.

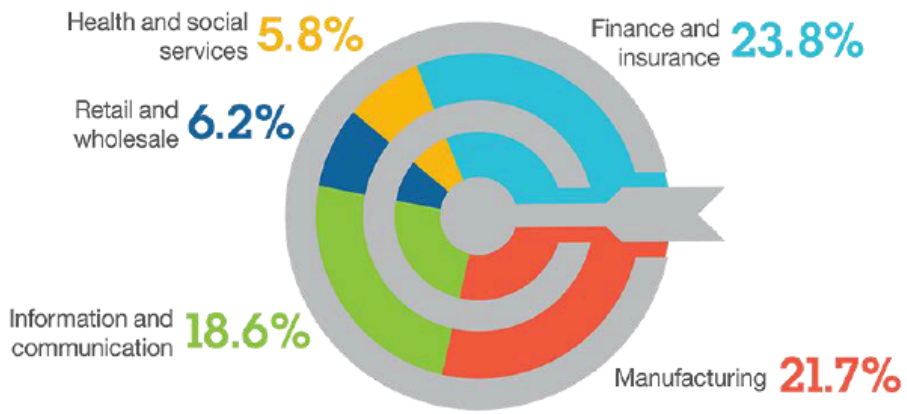
En conclusion, on a le sentiment ici que le cri des victimes et des médias a couvert tout raisonnement juridique. Il fallait un responsable. L'auteur de l'infraction introuvable, c'est sur la victime qu'on se rabat. C'est un mode de fonctionnement regrettable sur le plan des principes et qui ne devrait pas se généraliser.

A défaut, oui, la cybersécurité deviendrait synonyme d'obligation de résultat.

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

Source : http://www.solutions-logiciels.com/actualites.php?titre=La-cybersecurite-a-t-elle-une-obligation-de-resultat-&actu=15232
par Juliette Paoli

Cyber sécurité : Le Maroc doit bien s'armer



Cybersécurité : Le Maroc doit bien s'armer

Le coût de la cybercriminalité dans le monde s'est chiffré en 2013 à 350 milliards de dollars*. Au-delà de l'enjeu économique colossal, la multiplication des cyber-attaques et de quelques cyber-guerres pose la question du «contrôle» de ce nouvel espace de souveraineté, créé par l'Homme.

Le Maroc classé 49e pays mondial à risque en matière de sécurité Internet et 3e au niveau africain dans le dernier rapport de Symantec (Symantec Corporation – Internet Security Threat Report 2013). Le risque d'une attaque virtuelle est bien réel, et les PME sont les premières cibles des cyberattaquants.
Au Maroc, le niveau des organisations marocaines par rapport à la norme ISO 27002 est encore trop faible. En effet, rares sont les entreprises marocaines ayant mis en place à ce jour une Politique de Sécurité des Systèmes d'Information (PSSI).
Pourtant la protection face aux cyber-menaces et leur évolution constante (globalisation, …) apparaît comme une initiative majeure : les attaques informatiques contre les infrastructures nationales représentent des menaces réelles. La prévention et la réaction aux attaques informatiques sont une priorité absolue des dispositifs de cyber-sécurité, en particulier les structures organisationnelles.

Aujourd'hui, les entreprises repensent leurs tactiques de cybersécurité
Selon l'étude IBM CISO (Chief Information Security Officer) parue en décembre 2014 qui visait à découvrir et à comprendre comment les entreprises se protègent actuellement contre les cyber-attaques. Elle révèle que 70% des responsables de la sécurité pensent avoir des technologies traditionnelles matures, qui mettent l'accent sur la prévention des intrusions réseau, la détection avancée des logiciels malveillants et l'analyse de la vulnérabilité du réseau.
Cependant, près de 50% reconnaissent que le déploiement de nouvelles technologies de sécurité est prioritaire pour leur entreprise. Ils ont identifié trois principaux domaines nécessitant un changement drastique : la prévention des fuites de données, la sécurité du Cloud et la sécurité des appareils et des mobiles.

Toujours selon l'étude IBM CISO :
La sécurité du Cloud reste en tête de l'ordre du jour : bien que la préoccupation liée à la sécurité du Cloud reste forte, près de 90% des personnes interrogées ont adopté le Cloud ou sont actuellement en train de mettre en place des initiatives en la matière. Dans ce groupe, 75% des responsables s'attendent à voir leur budget dédié à la sécurité du Cloud augmenter, voire de manière significative dans les 3 à 5 ans à venir.
La sécurité intelligente basée sur l'analyse des données est prioritaire : plus de 70% des responsables de la sécurité déclarent que les renseignements de sécurité en temps réel sont de plus en plus importants pour leur entreprise. Malgré cette constatation, l'étude révèle que des domaines tels que la classification et la découverte des données ainsi que l'analyse des renseignements de sécurité sont relativement peu matures (54%) et ont fortement besoin d'être améliorés ou transformés.
Les besoins dans la sécurité mobile restent importants : malgré une main-d'oeuvre de plus en plus mobile, seulement 45% des responsables de la sécurité déclarent qu'ils ont une approche efficace de la gestion des terminaux mobiles. En fait, selon l'étude, lorsque l'on adresse le sujet de la maturité, la sécurité des mobiles et des appareils arrive en fin de liste (51%).

Au Maroc, les structures organisationnelles s'organisent
La nouvelle stratégie "Maroc Numeric 2020" que le ministère de l'Industrie, du commerce, de l'investissement et de l'économie numérique, est en train de préparer, devra continuer à positionner le Maroc comme un hub technologique régional, en réalisant des progrès en termes de "transformation sociale" et d'accompagnement de l'entreprise et des différents chantiers de l'E-gouvernement. Surtout ce dernier, s'inscrit dans la poursuite des progrès réalisés depuis des années en matière des technologies de l'information, de sécurité en continuant à positionner le Maroc comme hub régional et à fournir des services aussi bien au citoyen qu'à l'entreprise, particulièrement la Petite et Moyenne.

Les PME, cible privilégiée et pourtant…
Paradoxalement alors que le Maroc est 3,5 fois plus vulnérable aux logiciels malveillants que la moyenne mondiale**, les PMEs, 1er tissu économique marocain, la cyber-criminalité, les défaillances techniques ou informatiques sont peu préoccupantes et donc peu prises en compte.

IBM a bien compris les enjeux de la sécurité des données en entreprise : « ces nouvelles offres sont conçues pour protéger les données et applications vitales de l'entreprise grâce à des techniques analytiques avancées, développées au sein même de l'entreprise, dans les clouds publics et privés, et dans les terminaux mobiles. » Actuellement, 75% des failles de sécurité nécessitent plusieurs jours, semaines voire mois pour être détectées, ce qui peut causer d'importants dommages.

Une gestion proactive de la sécurité par IBM
Les solutions proposées par IBM devraient permettre d'apporter une vue d'ensemble de l'état de la sécurité informatique, pour savoir qui utilise le cloud et de quelle façon. Les nouveaux outils peuvent être déployés dans le cloud ou sur site, pour s'adapter aux environnements informatiques des entreprises. Par ailleurs, les éventuelles menaces peuvent être identifiées en temps réel, grâce aux données d'analyse mises à disposition par IBM, appuyées sur 20 milliards d'événements quotidiens repérés dans plus de 130 pays***

Les offres de sécurité IBM apportent la sécurité intelligente pour aider les organisations à protéger les personnes, les données, les applications et les infrastructures. Les solutions IBM couvrent la gestion des identités et des accès, le SIEM (Security Information and Event Management), la sécurité des données, la sécurité des applications, la gestion du risque, la gestion des terminaux, la nouvelle génération de protection contre les intrusions, la lutte contre la fraude financière avec le rachat de Trusteer et d'autres sujets. IBM dispose d'une des plus importantes organisations de recherche et développement et de mise en oeuvre dans le domaine de la sécurité.

La cybercriminalité reste la deuxième forme la plus répandue de criminalité économique selon PwC;
La cyber-criminalité coûterait **327 milliards d'euros** par an. Selon un rapport publié par le « Center for Strategic and International Studies »;
 65% des utilisateurs d'internet ont été victimes d'une cyberattaque (virus, fraude à la carte de crédit en ligne, vol d'identité)- Soit 1.5 millions de personnes par jour (Mashable); Aux Etats-Unis, 40 millions de personnes ont été victimes de vols de données personnelles.

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

Source : http://lobservateurdumaroc.info/2014/12/23/cyber-securite-le-maroc-doit-bien-sarmer/
* (Le coût des failles informatiques selon l'étude menée pour le compte de Microsoft en 2013, par l'observatoire IDC (International Data Corporation)
** Source Microsoft
*** Source http://ibm.com/fr/security

STAPLES précise les conditions de la faille informatique dans 115 de ses magasins en août et septembre

STAPLES précise les conditions de la faille informatique dans 115 de ses magasins en août et septembre

Staples a apporté vendredi soir de nouveaux éléments dans le cadre de l'enquête sur la faille de sécurité qui a exposé un mois durant, de mi-août à mi-septembre derniers, des données de paiement de ses clients. L'enseigne américaine de matériel et fournitures de bureau a ainsi indiqué qu'un programme informatique malveillant avait été introduit dans le système de 115 de ses 1 400 points de vente aux Etats-Unis, touchant 1,16 million de transactions par carte bancaire.

Cette cyber-attaque a permis aux pirates de récupérer des noms de clients, mais leur numéro de carte, la date de péremption de celle-ci et leur code de vérification, dans 113 boutiques du 10 août au 16 septembre. Les deux autres magasins touchés ont été exposés aux mêmes indiscrétions du 20 août au 16 septembre.

Au travers de conférences ou de formations, Denis JACOPINI sensibilise des directeurs, des cadres et des salariés aux risques induits par les nouveaux usages de l'informatique en entreprise et dans les collectivités, ainsi que leurs responsabilités pénales.
Contactez-nous

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

Source :
http://www.zonebourse.com/STAPLES-INC-4904/actualite/STAPLES–precise-les-conditions-de-la-faille-informatique-dans-115-de-ses-magasins-en-aout-et-septe-19577610/

Des plans de réacteurs nucléaires ont été piratés

Des plans de réacteurs nucléaires ont été piratés

Des documents internes de Korea Hydro & Nuclear Power Co. (KHNP), notamment des plans de réacteurs nucléaires sud-coréens, ont été dérobés et publiés de nouveau vers 1h30 ce dimanche sur Internet, pour la quatrième fois depuis le 15 décembre.

Un internaute, qui serait à l'origine de ces vols de données, a publié sur le réseau social Twitter des documents internes concernant le Réacteur 2 de la centrale de Kori, le Réacteur 1 de la centrale de Wolsong et le manuel informatique utilisé dans les centrales nucléaires du pays.
Le soi-disant «président du groupe antinucléaire à Hawaï» a demandé d'arrêter le fonctionnement des premier et troisième réacteurs à Kori et le deuxième à Wolsong à partir du jour de Noël, en menaçant d'effectuer une deuxième série de «destructions» si les réacteurs ne sont pas arrêtés.
KHNP a indiqué hier que la publication de ces documents qui ne contiennent pas d'informations confidentielles n'affectera pas la sécurité des centrales nucléaires dans un communiqué de presse. La société a néanmoins dit qu'elle effectuerait un exercice de simulation général contre l'éventualité d'une cyberattaque en vue de renforcer ses contre-mesures.
Le ministère du Commerce, de l'Industrie et de l'Energie Yoon Sang-jick a présidé lui aussi une réunion extraordinaire pour vérifier la cybersécurité hier matin suite à la fuite des documents internes en convoquant des chefs d'entreprises publiques spécialisées dans la production d'électricité et d'énergies, dont Korea Electric Power Corp. (KEPCO).

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

Source : http://french.yonhapnews.co.kr/national/2014/12/21/0300000000AFR20141221000200884.HTML