BULLETIN DE VEILLE N°3

ANPT-2019-BV-03

« Lorsque nous devons choisir entre l'ajout de fonctionnalités et la résolution de problèmes de sécurité, nous devons choisir la sécurité. » -Bill Gates-

Juillet 2019

Alertes de sécurité

Smartphone/Android

Agent Smith : une nouvelle espèce de logiciel malveillant mobile

10 juillet 2019

Les chercheurs de Check Point ont récemment découvert une nouvelle variante du logiciel malveillant pour mobile qui **infectait discrètement environ 25 millions d'appareils,** sans que l'utilisateur n'en soit complètement conscient. Déguisée en application liée à Google, la partie essentielle des programmes malveillants exploite diverses vulnérabilités Android connues et remplace automatiquement les applications installées sur l'appareil par des versions malveillantes sans interaction de l'utilisateur. Cette approche unique, juste-à-temps (JIT), intégrée à l'appareil, a incité les chercheurs à appeler ce logiciel malveillant «l'agent Smith» […]. «**Agent Smith**» est utilisé pour **obtenir un gain financier** grâce à l'utilisation d'annonces malveillantes. Cependant, il pourrait facilement être utilisé à des fins beaucoup plus intrusives et nuisibles, telles que **le vol de justificatifs bancaires** […].

Source *: https://research.checkpoint.com/agent-smith-a-new-species-of-mobile-malware/*

Une fausse application Samsung piège 10 millions d'utilisateurs Android

05 juillet 2019

Plus de dix millions d'utilisateurs ont été dupés en installant une fausse application Samsung nommée "Updates for Samsung" qui promet des mises à jour de firmware, mais, en réalité, redirige les utilisateurs vers un site Web rempli d'annonces et de frais de téléchargement de firmware […].

Source *: https://www.zdnet.fr/actualites/une-fausse-application-samsung-piege-10-millions-d-utilisateurs-android-39887187.htm*

La vulnérabilité Android permet de pirater votre téléphone avec des vidéos malveillantes

24 juillet 2019

Une vulnérabilité référencée CVE-2019-2107 permet aux pirates d'exécuter à distance du code arbitraire en se faufilant dans des «fichiers spécialement conçus», comme des vidéos avec une charge malveillante. Une fois que la victime a ouvert le fichier, les attaquants peuvent accéder à leur appareil […].

Bulletin *: https://source.android.com/security/bulletin/2019-07-01*

Source *: https://thenextweb.com/security/2019/07/24/google-android-vulnerability-malicious-video/*

Microsoft

Un exploit zero-day pour Windows utilisé dans une attaque extrêmement ciblée

10 juillet 2019

La recherche ESET découvre un exploit zero-day qui tire parti d'une vulnérabilité référencée en tant que CVE-2019-1132. La vulnérabilité permet une escale de privilèges locale dans Windows, en particulier une déréférence de pointeur NULL dans le composant win32k.sys. ESET a immédiatement signalé le problème aux équipes du centre de réponse aux incidents de Microsoft (MSRC), ce qui a permis à l'éditeur de corriger la vulnérabilité et de publier un correctif.

Les systèmes affectés : Windows 7 (SP1 32 et 64 bits) ; Windows Server 2008 (SP2, 32 et 64 bits ; SP1 et SP2 Itanium) ; Windows Server 2008 R2, 64 bits.

A noter que Windows XP et Windows Server 2003 sont également vulnérables, mais ces versions ne sont plus supportées par Microsoft.

Source : *https://www.welivesecurity.com/2019/07/10/windows-zero-day-cve-2019-1132-exploit/*

Détail CVE et correctif : *https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-1132*

Une vulnérabilité critique dans Microsoft File Checksum Integrity Verifier

04 juillet 2019

Une vulnérabilité classée critique a été trouvée dans Microsoft File Checksum Integrity Verifier 2.05. Affecté par ce problème est une fonction inconnue du fichier fciv.exe du composant DLL Loader. La manipulation avec une valeur d'entrée inconnue permet une attaque de classe élévation de privilèges.

La vulnérabilité a été publiée en 04/07/2019 par John Page (hyp3rlinx). La notice d'information est disponible en téléchargement sur hyp3rlinx.altervista.org L'attaque nécessite une approche locale. Une exploitation réussie requiert une seule session d'authentification. Des détails techniques et un exploit a été publié disponible en téléchargement sur le site hyp3rlinx. Il est déclaré comme proof-of-concept. Cette vulnérabilité a été classée comme 0-day non publique pendant au moins 31 jours.

Source *: https://vuldb.com/fr/?id.138390*

Vecteur d'attaque Excel de Microsoft Office

02 juillet 2019

Les chercheurs en sécurité ont découvert une nouvelle faille dans le programme Excel de Microsoft Office. Les attaquants peuvent exploiter une fonctionnalité trouvée dans Excel, appelée Power Query, pour lancer une attaque à distance par Dynamic Data Exchange (DDE) sur une feuille de calcul Excel. Cela pourrait permettre à un attaquant de charger des logiciels malveillants, de profiler un périphérique et d'exécuter des commandes arbitraires sur la machine d'un utilisateur.

Logiciel affecté : Microsoft Office 2016 et versions antérieures. Pour plus d'informations et de détails sur le vecteur d'attaque, visitez le site : https://www.mimecast.com/blog/2019/06/exploit-using-microsoft-excel-power-query-for-remote-dde-execution-discovered/

Source *: https://www.csa.gov.sg/singcert/news/advisories-alerts/microsoft-office-excel-attack-vector*

Le webmail Microsoft Office 365 révèle les adresses IP lors de l'envoi d'e-mails

26 juillet 2019

Le Webmail Microsoft Office 365 expose les adresses IP privées aux destinataires lors de l'envoi d'e-mails. En effet, lors de l'envoi d'e-mails à l'aide du Webmail Office 365, votre adresse IP locale sera injectée dans le message en tant qu'en-tête de courrier supplémentaire.

La solution est de se connecter au Webmail d'office 365 à l'aide d'un VPN ou de Tor. Ainsi, l'adresse IP des services sera injectée dans le courrier électronique plutôt que l'adresse locale des utilisateurs.

Source *: https://cyware.com/news/microsoft-office-365-webmail-exposes-ip-addresses-while-sending-emails-cede7beb*

Les attaquants créent un faux site Office 365 pour pousser le cheval de Troie TrickBot

19 juillet 2019

Une nouvelle campagne d'attaque de logiciels malveillants utilisant un faux site Web Office 365 a été découverte récemment. La campagne est utilisée pour fournir un cheval de Troie voleur de mots de passe TrickBot, déguisé en mises à jour de navigateur Chrome et Firefox.

Selon Bleeping Computer , le faux site Web Office 365 est très similaire à n'importe quel site de Microsoft. En fait, tous ses liens pointent vers des pages hébergées sur des domaines Microsoft.

Les utilisateurs visitant ce faux site Web s'afficheront avec une alerte concernant la mise à jour de leur navigateur avec la dernière version. Le format de l'alerte est légèrement différent pour les utilisateurs de Chrome et de Firefox […].

Source *: https://cyware.com/news/attackers-create-fake-office-365-site-to-push-trickbot-trojan-a5c9bd18*

Le cyber command US alerte à propos des pirates informatiques qui exploitent une faille d'Outlook

02 juillet 2019

Le Cyber Command US a publié le 02/07/2019 une alerte via Twitter au sujet d'acteurs malveillants abusant d'une vulnérabilité Outlook pour installer un logiciel malveillant sur des réseaux gouvernementaux.

Le bug Outlook, découvert et détaillé par les chercheurs en sécurité de SensePost, permet à un acteur malveillant d'échapper à la sandbox Outlook et d'exécuter du code malveillant sur le système d'exploitation sous-jacent.

Source *: https://www.zdnet.fr/actualites/le-cyber-command-us-alerte-a-propos-des-pirates-informatiques-qui-exploitent-une-faille-d-outlook-39887041.htm#xtor=123456*

Sodinokibi ransomware utilise maintenant un ancien Windows zero-day

04 juillet 2019

Un ransomware nommée Sodinokibi (également Sodin ou REvil) utilise une ancienne vulnérabilité «zero-day» de Windows pour s'élever en accès administrateur aux hôtes infectés.

La vulnérabilité, une faille d'élévation de privilèges connue sous le nom de CVE-2018-8453, avait été corrigée dans les mises à jour de sécurité Microsoft du mois d'octobre 2018 après son utilisation par un groupe de piratage parrainé par l'État connu sous le nom de FruityArmor depuis août 2018 […]. La découverte la plus intéressante a été celle d'une "clé squelette" dans le code Sodinokibi, qui sert de porte dérobée au processus de cryptage, permettant au créateur de Sodinokibi de décrypter n'importe quel fichier, quelles que soient les clés de cryptage publiques et privées d'origine utilisées pour le verrouillage, les données d'une victime […].

Source *:https://www.zdnet.com/article/sodinokibi-ransomware-is-now-using-a-former-windows-zero-day/*

Détails : *https://securelist.com/cve-2018-8453-used-in-targeted-attacks/88151*

VPN

Les VPN de Palo Alto, Fortinet et Pulse vulnérables

24 juillet 2019

Les chercheurs en sécurité Cheng-Da Tsai et Tingyi Chang sont parvenus à exploiter des vulnérabilités dans les solutions de réseaux privés virtuels (VPN) de plusieurs fabricants dont Palo Alto, Fortinet et Pulse. Des serveurs Uber et Twitter ont pu être hackés et des patchs de sécurité ont été poussés. […] Les chercheurs en sécurité, membres des réseaux Devcore et Chroot vont dévoiler les détails de leurs derniers travaux lors de la prochaine Black Hat 2019 à Las Vegas.

Des correctifs ont vite été publiés sur les sites officiels des fournisseurs.

Source *: https://techcrunch.com/2019/07/23/corporate-vpn-flaws-risk/*

D-link

Vulnérabilité dans Adobe Flash Player (AFP)

06 juillet 2019

Une vulnérabilité a été trouvé dans D-Link Central WiFi Manager CWM(100) (Wireless LAN Software) et classée problématique. Affectée est une fonction inconnue du fichier PayAction.class.php. La manipulation du paramètre **passcode** dans le cadre de Parameter mène à une vulnérabilité de classe cross site scripting.

La vulnérabilité a été publiée le 06/07/2019 et référencée CVE-2019-13374. Il est possible de lancer l'attaque à distance. Les détails techniques sont connus, mais aucun exploit n'est disponible.

Il est recommandé de mettre à jour à la version v1.03R0100_BETA6 qui patch cette vulnérabilité.

Source *: https://vuldb.com/fr/?id.137456*

Cisco

Des vulnérabilités de criticité élevée dans des produits Cisco

08-18 Juillet 2019

Cisco a publié des mises à jour de sécurité pour corriger les vulnérabilités détectées dans plusieurs produits Cisco. Plusieurs vulnérabilités de gravité élevée ont été identifiées et nécessitent une attention immédiate.

L'exploitation réussit de ces vulnérabilités pourrait permettre à un attaquant de prendre le contrôle du système affecté et d'exécuter des codes malveillants, y compris un déni de service DoS, la corruption de la mémoire, l'exécution de commandes arbitraires sur le système d'exploitation sous -jacente en tant que ***root,*** contournement des validations de sécurité et connexion d'un serveur non autorisé au VLAN de l'infrastructure pour lancer une attaque de pré-chargement de DLL.

Les administrateurs sont invités à installer immédiatement les dernières mises à jour de sécurité disponibles.

Plus de détails sur les alertes et les patchs de sécurité se trouvent dans la source.

Source *https://tools.cisco.com/security/center/publicationListing.x?product=Cisco&sort=-day_sir#~Vulnerabilities*

Vmware

VMWARE ESXI 6.5 HOSTD DÉNIE DE SERVICE

11 juillet 2019

Une vulnérabilité a été trouvé dans VMware ESXi 6.5 (Virtualization Software) et classée problématique. Affectée par cette vulnérabilité est une fonction inconnue du composant hostd. Une manipulation de valeur d'une variable d'entrée mène à une vulnérabilité de classe déni de service.

Les détails de cette vulnérabilité référencée CVE-2019-5528 sont inconnus et un exploit n'est pas disponible pour le public. La notice d'information est disponible en téléchargement sur vmware.com.

Correctif *: https://www.vmware.com/security/advisories/VMSA-2019-0011.html*

Source *: https://vuldb.com/fr/?id.137789*

LinkdIn

Une énorme lacune sur LinkedIn met la sécurité des utilisateurs en péril

26 juillet 2019

Rijnders découvert une faille grave intégrée à une fonctionnalité très élémentaire de LinkedIn permet aux utilisateurs de publier une offre d'emploi officielle sur la page d'entreprise LinkedIn de presque toute entreprise. Ces listes non officielles apparaissent sur la page "Emplois" de l'entreprise et ressemblent à toute autre offre d'emploi publiée légitimement par l'organisation […].

Paul Rockwell, un porte-parole de l'entreprise a déclaré, Ce problème était dû à un bogue dans notre expérience des emplois en ligne qui permettait aux membres de modifier l'entreprise après qu'un poste avait déjà été publié. Le problème est maintenant résolu.

Source *: https://mashable.com/article/linkedin-jobs-security-flaw/*

LibreOffice

Le simple fait d'ouvrir un document dans LibreOffice peut pirater votre ordinateur (non corrigé)

26 juillet 2019

LibreOffice contient une vulnérabilité grave non corrigée d 'exécution de code qui pourrait introduire des malwares dans votre système dès que vous ouvrez un fichier document malicieux.

LibreOffice est l'une des alternatives les plus populaires et open source à la suite Microsoft Office et est disponible pour les systèmes Windows, Linux et macOS.

Plus tôt ce mois-ci, LibreOffice a publié la dernière version 6.2.5 de son logiciel, qui corrige deux vulnérabilités graves (CVE-2019-9848 et CVE-2019-9849), mais le correctif de cette dernière a été contourné, affirme le chercheur en sécurité Alex Inführ.

La solution est de réinstaller le logiciel sans macros ou au moins sans composant LibreLogo, en attendant la publication du correctif.

Source *: https://thehackernews.com/2019/07/libreoffice-vulnerability.html*

Détails CVE *: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9849*

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9848

Juniper

Juniper Networks corrige des dizaines de vulnérabilités

11 juillet 2019

Juniper Networks a publié 11 alertes de sécurité, deux critiques, cinq critiques élevée et quatre moyennes, portant sur un grand nombre de vulnérabilités sur plusieurs lignes de produits.

Certains problèmes pouvant survenir si les vulnérabilités associées sont exploitées incluent un de déni de service, un débordement de pile, entraînant l'immobilisation du processus du démon de protocole de routage local, ainsi que le redémarrage du processeur.

Correctif :https://kb.juniper.net/InfoCenter/index?page=content&channel=SECURITY_ADVISORIES

Source : https://www.scmagazine.com/home/security-news/vulnerabilities/juniper-networks-patches-dozens-of-vulnerabilities/

Actualité

Une nouvelle attaque permet aux applications Android de capturer des données de haut-parleur sans aucune autorisation

17 juillet 2019

Une équipe de chercheurs en cyber sécurité a réussi à mettre en évidence une nouvelle attaque qui pourrait permettre à des applications malveillantes d'écouter la voix sortant des haut-parleurs de votre smartphone sans exiger la permission de l'appareil […]. Le capteur accéléromètre de Smart phone est utilisé pour capturer des données de haut-parleur. Surnommée Spearphone, cette attaque nouvellement démontrée tire parti d'un capteur de mouvement basé sur du matériel, appelé accéléromètre, intégré à la plupart des appareils Android et accessible sans restriction par n'importe quelle application installée sur un appareil, même sans autorisation.

Source *: https://thehackernews.com/2019/07/android-side-channel-attacks.html*

Plus de 1000 applications Android collectent des données même après avoir refusé des autorisations.

Des chercheurs ont découvert que plus de 1000 applications Android contournaient les paramètres d'autorisation de confidentialité […].

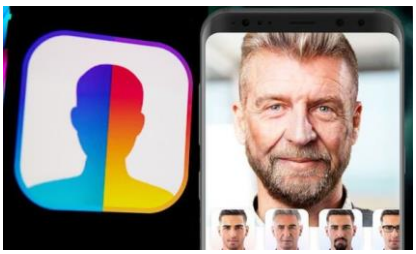
L'étude a examiné plus de 88000 applications du magasin Google Play, afin de déterminer comment les données étaient transférées depuis les applications lorsque les autorisations leur étaient refusées. Les 1325 applications qui violaient les autorisations sur Android utilisaient des solutions de contournement masquées dans leur code, qui prendraient des données personnelles provenant de sources telles que des connexions Wi-Fi et des métadonnées stockées dans des photos.

Les chercheurs ont découvert que Shutterfly, une application de retouche photo, recueillait les coordonnées GPS des photos et les transmettait à ses propres serveurs, même lorsque les utilisateurs refusaient d'autoriser l'application à accéder aux données de localisation […].

Source *: https://www.cnet.com/news/more-than-1000-android-apps-harvest-your-data-even-after-you-deny-permissions/*

Alerte FaceApp - Les quatre choses à savoir avant d'utiliser cette application populaire

23 juillet 2019



FACEAPP est devenu viral la semaine dernière grâce à son filtre qui permet aux utilisateurs de paraître plus âgés ou plus jeunes - bien que l'application s'est révélée incroyablement populaire, elle a également suscité de nombreuses inquiétudes quant à la protection de la vie privée. Contrairement à la plupart des autres applications de ce type, FaceApp n'effectue pas son traitement sur un appareil particulier. Au lieu de cela, l'application, développée par une équipe en Russie, envoie des photos à ses serveurs pour effectuer le processus de modification.

S'adressant à TechCrunch, les créateurs de l'application, Wireless Lab, ont déclaré qu'il "pourrait" stocker les photos des utilisateurs dans ses clouds, et ce, pour "la performance et le trafic".

La chercheuse en sécurité Jane Manchun Wong a également analysé l'application et a déclaré que peu d'information sont envoyées au serveurs de l'application. Cependant, une option permettant aux utilisateurs de supprimer leurs photos des serveurs doit être ajoutée.

FaceApp a déclaré accepter les demandes de suppression des données des utilisateurs qui doit se faire à partir de l'application elle-même.

A considérer avant l'utilisation de toute application mobile :

- Les autorisations demandées
- La sécurité dans le cloud « commence avec l'utilisateur », partager ses informations à ses conséquences
- Comprendre la politique de confidentialité d'une application
- Faites vos recherches avant de télécharger une application.

Source *:https://www.express.co.uk/life-style/science-technology/1155772/FaceApp-old-filters-security-warning-Android-iPhone*

Sérieusement ? Cisco a mis les certificats et les clés Huawei X.509 dans ses propres commutateurs

4 juillet 2019

Cisco a révélé de nombreuses vulnérabilités dans son équipement réseau, notamment un bogue embarrassant qui plaçait le boogeyman technologique de l'Ouest dans le kit de la firme américaine. Cisco demande aux clients d'appliquer des mises à jour pour 18 vulnérabilités de gravité moyenne et élevée dans ses produits, ainsi qu'un bogue curieux qu'il qualifie «informationnel » et qui affecte les commutateurs Small Business 250, 350, 350X et 550X.

Les bogues de ces commutateurs ne sont pas assez sérieux pour obtenir son propre identifiant CVE, mais ils fournissent une leçon sur les risques bien connus d' utilisation de composants open source dans des produits sans exécuter les contrôles de sécurité appropriés.

Les certificats faisaient partie d'un package de test d'un composant open-source appelé OpenDaylight. Celui-ci contenait des scripts de test et des données, y compris les certificats délivrés par Huawei.

Les développeurs de Cisco les ont utilisés pour des tests et ils ont tout simplement oublié de supprimer les certificats avant de les envoyer aux périphériques, […].

Cisco a supprimé ces certificats et les clés associées du logiciel FindIT Network Probe et du micrologiciel des commutateurs Small Business 250, 350, 350X et 550X, à partir des versions répertoriées sur son bulletin de sécurité.

Source *: https://www.zdnet.com/article/seriously-cisco-put-huawei-x-509-certificates-and-keys-into-its-own-switches/*

Avis : *https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-sb-switches-findit*

La toute première souche de logiciels malveillants repérée exploitant le nouveau protocole DoH (DNS over HTTPS)

03 juillet 2019

Des chercheurs en sécurité de Netlab, une unité de recherche de menaces réseau du géant chinois de la cybersécurité Qihoo 360, ont découvert la toute première souche de programmes malveillants exploitant le protocole DNS over HTTPS (DoH).

Le malware, nommé Godlua, a été détaillé dans un rapport publié le 01/07/2019 par les chercheurs de la société […].

Les chercheurs de Netlab ont déclaré que le malware fonctionnait comme un bot DDoS et qu'ils l'avaient déjà utilisé dans des attaques, notamment contre liuxiaobei.com, la page d'accueil d'un site de fans de Liu Xiaobei […].

Source *:https://www.zdnet.com/article/first-ever-malware-strain-spotted-abusing-new-doh-dns-over-https-protocol/*

Un attaquant DDoS passera deux ans en prison

03 juillet 2019

L'un des hommes derrière une série d'attaques de 2013 sur des jeux comme League of Legends et DOTA 2 a été condamné à 27 mois de prison et doit verser 95000$ en restitution à une autre de ses victimes.

Thompson gérait le compte Twitter « DerpTrolling », et son cas concernait en fait Daybreak Games, anciennement Sony Online Entertainment, à qui il devait payer 95000$ après avoir déterminé le montant des revenus perdus de l'entreprise entre décembre 2013 et janvier 2014 lors de ses attaques.

Il s'en est sorti assez légèrement. La peine maximale à laquelle il aurait pu être condamné est une amende de 250 000 $ et dix ans de prison.

Source *: https://kotaku.com/ddos-attacker-will-spend-two-years-in-prison-1836091110*

Une entreprise de cybersécurité supprime le code relatif à la vulnérabilité «BlueKeep» de Windows extrêmement dangereuse

26 juillet 2019

Des chercheurs de l'entreprise américaine Immunity ont développé un exploit pour le redoutable bug Windows, connu sous le nom de BlueKeep.

BlueKeep a permis à de nombreux chercheurs en sécurité de rester éveillés la nuit craignant la publication d'un exploit ou le développement d'un ver dont les dégâts rivaliseront avec ceux de WannaCry ou NotPetya- deux virus qui se propagent de manière presque incontrôlable dans le monde entier, bloquant des milliers d'ordinateurs -. BlueKeep est potentiellement si grave que Microsoft n'a pas été le seul à pousser très fort pour que les utilisateurs appliquent des correctifs. La NSA, le DHS (Department of Homeland Security), le centre national de cybersécurité du Royaume-Uni et bien d'autres […].

Immunity, entreprise américaine de consulting en sécurité, a annoncé le 23/07/2019 avoir développé un exploit pour BlueKeep et l'a inclus dans sa boîte à outils de tests de pénétration Canvas, disponible uniquement pour les abonnés payants. Les clients de Canvas peuvent désormais exploiter ce bug en utilisant le code propre à Immunity.

Source *:https://www.vice.com/en_us/article/njvvvb/cybersecurity-firm-drops-code-for-the-incredibly-dangerous-windows-bluekeep-vulnerability*

12 défis auxquels les entreprises sont confrontées lors de l'utilisation d'un logiciel open source

26 juillet 2019

L'utilisation de logiciels libres a augmenté au cours de la dernière décennie. Ils se sont considérablement améliorés, offrant des fonctions comparables à celles de titres créés par des professionnels, ainsi que des coûts initiaux peu élevés et des fonctionnalités créatives.

Mais si les systèmes open source présentent des avantages, il convient de surveiller un certain nombre de points de blocage. Des questions ont été posées à une groupe d'experts de YEC. Leurs meilleures réponses sont ci-dessous :

1. ***Sécurité*** : Les plates-formes open source peuvent augmenter le risque de violation de la sécurité.
2. ***Complexité déroutante*** : Cela peut devenir si complexe lors de l'ajout de fonctionnalité.
3. ***Mises à jour :*** ce type de logiciel n'a pas de fournisseur qui publie des mises à jour. Au lieu de cela, les développeurs doivent les rechercher. Pour s'en assurer, des programmes de gouvernance doivent être mis en place désignant l'équipe informatique devant gérer les correctifs et les mises à jour afin de garantir leur sécurité et leur fonctionnalité.
4. ***Communauté et licences*** : Il est crucial de s'assurer que le logiciel est maintenu à jour et qu'il dispose d'une large communauté pour poursuivre son soutien. il est extrêmement important de s'assurer que les licences concordent avec le modèle de l'entreprise et son cas d'utilisation.
5. ***Formation*** : L'open source ne contient généralement pas autant de manuels de formation et de ressources que les logiciels payants et emballés.
6. ***Manque de support client :*** L'un des problèmes rencontrés lors de l'utilisation de logiciels open source est le manque de support client.
7. ***Sources mystérieuses*** : déterminer la source qui modifient le code utilisé devient quasiment impossible. Cela pose un problème sérieux de sécurité car avec l'utilisation de certains logiciels open-source, le travail est exposé, souvent sans le savoir, à des pirates et des exploits.
8. ***Compatibilité*** : l'incompatibilité des logiciels open source avec ceux propriétaire (à source fermé) est souvent source de diminution la qualité des services
9. ***Courbe d'apprentissage*** : Pour les propriétaires d'entreprise qui ne sont pas particulièrement férus de technologie, les logiciels open source ouvert tels que WordPress peuvent parfois nécessiter une courbe d'apprentissage abrupte.
10. ***Ne pas prioriser une politique*** : La première chose à faire est de définir une stratégie pour votre entreprise ou votre organisation concernant votre utilisation open source.
11. ***Vision d'ensemble :*** Les logiciels open source sont parfaits pour les affaires et il existe une tonne de logiciels de valeur dans tous les secteurs. Toutefois, en raison de la nature complexe de ces logiciels, il peut être difficile de prendre du recul et d'avoir une vue d'ensemble lors de l'exploitation du logiciel.
12. ***Prise en charge du coût*** : L'un des avantages des logiciels open source est leur coût. Cependant, de nombreuses entreprises ne calculent pas l'engagement de temps nécessaire à l'exécution et à la maintenance. La gestion des problèmes liés aux logiciels

open source prend souvent du temps. Pour éviter cela, le coût net de la prise en charge de ces solutions avec des alternatives commerciales doivent être comparés

Source *: https://thenextweb.com/podium/2019/07/26/12-challenges-businesses-face-when-using-open-source-software/*

Pourquoi les risques de cybersécurité dans le cloud computing augmentent-ils ?

25 juillet 2019

La société de sécurité informatique Skybox Security a publié la mise à jour semestrielle de son rapport sur les tendances en matière de vulnérabilité et de menaces. Parmi les principales conclusions du rapport du premier trimestre 2019 est la croissance rapide des vulnérabilités liées au centenaires cloud.

En résumé, les conteneurs cloud sont des machines virtuelles (VM) légères et peu onéreuses, qui peuvent être utilisées pour remplacer les VM traditionnelles dans de nombreux déploiements de cloud computing en raison de leur rapidité et de leur simplicité. Cependant, cette facilité de déploiement peut entraîner des failles de sécurité avec les anciennes images de conteneur, notamment les vulnérabilités connues, rapidement répliquées et déployées dans une infrastructure cloud publique, privée ou hybride. Selon la startup basée à Silicon Valley, les vulnérabilités dans les logiciels de conteneur ont augmenté de 46% au premier semestre de 2019 par rapport à la même période de 2018 et de 240% par rapport aux chiffres de deux ans auparavant […].

Le rapport susmentionné est en pièce jointe à ce bulletin.

Source *:https://www.forbes.com/sites/jeanbaptiste/2019/07/25/why-cloud-computing-cyber-security-risks-are-on-the-rise-report/#b25419562109*

Evènements

Evènements du mois

#LOI1807DZ, mise en œuvre

11/18 juillet 2019, ALGER

https://www.linkedin.com/company/unidees-alg-rie/?originalSubdomain=fr

La loi 18-07 relative à la protection des personnes physiques dans le traitement des données à caractère personnel ou #LOI1807DZ est entrée en vigueur le 10 Juin 2018. Elle implique certains changements majeurs pour l'entreprise sur le traitement et l'utilisation des données des particuliers.

Durant le mois de Juillet 2019, UNIDEES a proposé à travers des Workshops UNIDAY de mieux comprendre cette réglementation au niveau organisationnel et technique. Pour le 1er chapitre organisé le 11 Juillet 2019, le thème était sur comment classifier les données à caractère personnel et lutter efficacement contre leur fuite de votre entreprise avec les solutions Symantec "Information Centric Tagging" & "Data Loss Prevention". Le 2nd chapitre organisé le 18 Juillet 2019, les workshops ont discuté sur comment mieux sécuriser l'accès à des sites non classés et risqués tout en évitant de bloquer excessivement l'accès Web en isolant les URL ou les sites non classés avec des profils de risque potentiellement dangereux. La combinaison de l'isolation Web avec la passerelle Web Symantec, alimentée par l'intelligence Web au niveau des risques de Symantec Global Intelligence Network, fournit une couche d'isolation qui protège les utilisateurs contre les menaces provenant de sites Web ou d'URL non classés avec des profils potentiellement dangereux

LeHack19

6 et 7 juillet 2019, Paris

https://lehack.org/fr

Initiée en 2003 par l'équipe HZV (HackerZvoice), et inspirée par la célèbre DEF CON de Las Vegas, leHack est l'une des plus anciennes conférence de hacking underground francophone.

Autour de conférences, d'ateliers et de challenges, leHack vise à rassembler les professionnels de la sécurité informatique et les hackers de tous niveaux de qualification. Cette manifestation leur permet de découvrir les dernières avancées techniques et d'évaluer leurs compétences dans le domaine.

Les conférences (y compris celles des éditions précédentes) peuvent être visualisées sur la chaine YouTube Asso HZV.

Reference	ANPT-2019-BV-03
Titre	Bulletin de veille N°3
Date de version	30 juillet 2019
Pièce jointe	Rapport SKYBOX SECURITY
Contact	ssi@anpt.dz