BULLETIN DE VEILLE N°2

ANPT-2021-BV-02

« Un bon programmeur est quelqu'un qui regarde toujours dans les deux sens avant de traverser une rue à sens unique. »

-Doug Linder-

Fevrier 2021

Alertes de sécurité

Microsoft

Une vulnérabilité de Windows Defender restée cachée pendant 12 ans

11 Février 2021

Microsoft a enfin corrigé le bug dans son programme antivirus après que des chercheurs l'aient repéré l'automne dernier.[…]. Qu'il s'agisse du piratage Adobe Flash ou de l' exploit EternalBlue pour Windows , certaines méthodes sont tout simplement trop bonnes pour que les attaquants les abandonnent, même si elles ont dépassé leur apogée. Mais un bug critique vieux de 12 ans dans l'antivirus Windows Defender omniprésent de Microsoft a apparemment été négligé par les attaquants et les défenseurs jusqu'à récemment

La faille, découverte par les chercheurs de la société de sécurité SentinelOne, s'est manifestée dans un pilote que Windows Defender, renommé Microsoft Defender l'année dernière, utilise pour supprimer les fichiers et l'infrastructure invasifs que les logiciels malveillants peuvent créer. Lorsque le pilote supprime un fichier malveillant, il le remplace par un nouveau fichier bénin comme une sorte d'espace réservé pendant la correction. Mais les chercheurs ont découvert que le système ne vérifie pas spécifiquement ce nouveau fichier. Un attaquant pourrait, de ce fait, insérer des liens système stratégiques qui dirigent le pilote pour écraser le mauvais fichier ou même exécuter un code malveillant.

SentinelOne et Microsoft conviennent qu'il n'y a aucune preuve que la faille a été découverte et exploitée avant l'analyse des chercheurs. Maintenant que les résultats sont publics, ce n'est qu'une question de temps avant que les acteurs malveillants ne découvrent comment en profiter. Un porte-parole de Microsoft a noté que quiconque a installé le correctif du 9 février ou a activé les mises à jour automatiques est désormais protégé.

Source : *https://bit.ly/3kdh6t4*

Google

Google Chrome Zero-Day affecte Windows et les utilisateurs Mac

05 Février 2021

Google a mis en garde contre une vulnérabilité zero-day dans son moteur Web open source V8 qui est activement exploitée par des attaquants. Un correctif a été publié dans la version 88 du navigateur Chrome de Google - en particulier la version 88.0.4324.150 pour Windows, Mac et Linux. La faille (CVE-2021-21148) provient d'un débordement de mémoire tampon, a déclaré Google. "Google a connaissance de rapports selon lesquels un exploit pour CVE-2021-21148 existe dans la nature", selon la mise à jour de sécurité de Google. Bien que Google n'ait pas fourni plus de détails sur les attaquants exploitant la faille, les chercheurs de Malwarebytes ont émis une «hypothèse générale» selon laquelle l'attaque «avait été utilisée contre des chercheurs en sécurité travaillant dans différentes entreprises et organisations».

Ce rapport des chercheurs de Google a révélé que les pirates informatiques liés à la Corée du Nord ciblaient des experts en sécurité à travers une campagne d'ingénierie sociale élaborée qui établissait des relations de confiance avec eux - puis infectaient les systèmes de leur organisation avec des logiciels malveillants de porte dérobée personnalisés. Cependant, Google n'a confirmé aucune corrélation avec cette attaque. Chrome sera dans de nombreux cas mis à jour automatiquement vers sa dernière version, mais les experts en sécurité suggèrent aux utilisateurs de vérifier que cela s'est produit.

Source *: http://bit.ly/2YVxILU*

Mozilla

Une vulnérabilité critique de Firefox peut permettre l'exécution de code

9 Février 2021

Une mise à jour publiée par Mozilla pour Firefox 85 corrige une vulnérabilité de divulgation d'informations critiques qui peut être enchaînée avec d'autres failles de sécurité pour réaliser l'exécution de code arbitraire.

Dans son avis concernant la vulnérabilité - le bug n'a pas d'identifiant CVE - Mozilla l'a décrit comme un «débordement de tampon dans les calculs de hauteur de profondeur pour les textures compressées». Le problème, signalé par les chercheurs Abraruddin Khan et Omair via l'initiative Zero Day Initiative (ZDI) de Trend Micro, n'affecte apparemment que Firefox fonctionnant sous Windows - les autres systèmes d'exploitation ne sont pas affectés.

Le chercheur de vulnérabilités ZDI Hossein Lotfi a déclaré à SecurityWeek que la vulnérabilité est un bug de divulgation d'informations qui existe dans l'implémentation de la méthode API compresséeTexImage3D dans WebGL2.

L'exploitation oblige l'attaquant à convaincre l'utilisateur ciblé de visiter une page Web malveillante ou d'ouvrir un fichier malveillant. La Cybersecurity and Infrastructure Security Agency (CISA) des États-Unis a conseillé aux utilisateurs et aux administrateurs d'examiner l'avis de Mozilla et de prendre les mesures nécessaires. Un correctif est inclus dans Firefox 85.0.1 et Firefox ESR 78.7.1.

Source : *https://bit.ly/3qMfDML*

Adobe

Adobe : La version chinoise de Flash infectée par un adware

24 Février 2021

Des chercheurs en sécurité affirment que l'application chinoise de Flash se comporte comme un logiciel publicitaire et ouvre les fenêtres du navigateur pour afficher des publicités. Bien que l'application Flash Player ait officiellement atteint sa fin de vie le 31 décembre dernier, Adobe a permis à une entreprise chinoise locale de continuer à distribuer Flash en Chine, où l'application reste encore à la base d'une grande partie de l'écosystème informatique local et continue à être largement utilisée dans les secteurs public et privé.

Lors d'une analyse ultérieure, les chercheurs ont découvert que l'application installait effectivement une version valide de Flash, mais qu'elle téléchargeait et exécutait également des charges utiles supplémentaires. Plus précisément, l'application télécharge et exécute nt.dll, un fichier qui se charge dans le processus FlashHelperService.exe et ouvre une nouvelle fenêtre de navigateur à intervalles réguliers, montrant divers sites à forte densité de publicités et de pop-up. Ce comportement spammeur n'est évidemment pas passé inaperçu. Tant les utilisateurs réguliers que les autres entreprises de sécurité l'ont également remarqué. Cisco Talos a classé ce processus comme la menace la plus largement détectée pour les semaines se terminant le 14 et le 21 janvier, et le fichier s'est également classé dans son Top 10 pour les semaines se terminant le 7 janvier, le 11 février et le 18 février.

Cette menace particulière n'a pas d'impact sur les utilisateurs occidentaux, puisque la version de Flash qu'ils téléchargent sur flash.cn ne fonctionne pas sur les systèmes situés en dehors de la Chine. Mais, à la lumière du rapport de Minerva, ils ne devraient même pas essayer de la tester, car cela pourrait conduire à l'installation de logiciels publicitaires et compromettre la sécurité de leurs systèmes/réseaux.

Source : *https://bit.ly/3aON6k4*

Android : apparition de 5 vulnérabilités critiques

24 Février 2021

Google a corrigé cinq vulnérabilités critiques dans son système d'exploitation Android dans le cadre de son bulletin de sécurité de Février. Deux des failles étaient des vulnérabilités d'exécution de code à distance trouvées dans le framework et le système multimédia d'Android.

Trois autres failles critiques de Qualcomm ont été signalées par Google et corrigées par Qualcomm – dans le cadre d'une divulgation distincte du bulletin de sécurité. L'une de ces failles (CVE-2020-11163) a un score CVSS (Common Vulnerability Scoring System) de 9,8 sur 10.

La faille est liée à la puce de réseau local sans fil (WLAN) utilisée pour les communications Wi-Fi.

En tout, Google a corrigé 22 vulnérabilités dans le système d'exploitation Android, dont 15 comprenaient des vulnérabilités d'élévation de privilège. 22 autres failles de sécurité ont été corrigées par Qualcomm et ont eu un impact sur une gamme de fonctions de l'appareil telles que le Wi-Fi, la caméra et les écrans de l'appareil.

La plus grave des failles critiques dans le système d'exploitation Android est une vulnérabilité de sécurité dans le composant Media Framework qui permet l'exécution de code à distance, permettant à un attaquant distant utilisant un fichier spécialement conçu d'exécuter du code arbitraire dans le contexte d'un processus privilégié, selon Google. La faille est identifiée comme CVE-2021-0325 et a reçu une note «critique» sur Android 8.1 et 9, mais une note «élevée» sur Android 10, 11 et 12, a déclaré la société.

«L'évaluation de la gravité est basée sur l'effet que l'exploitation de la vulnérabilité aurait éventuellement sur un appareil affecté, en supposant que les atténuations de plate-forme et de service sont désactivées à des fins de développement ou si elles sont contournées avec succès», selon le bulletin de sécurité.

Le correctif lui-même sera livré en deux parties, la première corrigeant 20 vulnérabilités dans le système d'exploitation Android et la seconde qui corrige 23 failles trouvées dans le noyau Android et divers composants de Qualcomm, selon Google.

Source : https://bit.ly/37LhASi

Actualité

IA et API : les réponses A + pour garder les données sécurisées et privées

05 février 2021

De nombreux responsables de la sécurité considèrent les réglementations et les processus internes conçus pour gérer et sécuriser les données comme des formalités administratives qui entravent l'innovation. Rien ne pouvait être plus loin de la vérité.

La protection des données précieuses n'a jamais été une proposition simple. Cependant, à mesure que les frontières des données se sont estompées et que l'apprentissage automatique (ML) et d'autres formes d'intelligence artificielle (IA) ont pris racine, la capacité à gérer et à protéger les données est devenue exponentiellement plus compliquée pour les équipes de sécurité. Un désir croissant de calculer dans le cloud et à la périphérie a de profondes ramifications. D'une part, les organisations doivent s'adapter à des réglementations de plus en plus strictes sur les données, telles que le règlement général sur la protection des données (RGPD) de l'UE, le California Consumer Privacy Act (CCPA) et le Health Insurance Portability and Accountability Act (HIPAA). Et d'autre part, il est également nécessaire de libérer toute la valeur des données au sein des chaînes d'approvisionnement et des partenariats commerciaux, sans révéler de secrets commerciaux et d'informations personnelles identifiables (PII).

Les organisations doivent se concentrer sur «les multiples risques liés à la sécurité et à la confidentialité des données, car les données circulent entre les appareils, les systèmes et les cloud», a déclaré Rehan Jalil, PDG de la société de cybersécurité Securiti. Cela comprend les risques internes, les risques externes et l'accès de tiers aux données sensibles.

Jalil prévient que le problème particulièrement épineux est que les organisations saisissent souvent une étude d'impact sur la vie privée (PIA) qui n'est rien de plus qu'un «instantané dans le temps». Cette méthode d'identification et de gestion des risques de confidentialité peut bien fonctionner dans les modèles de développement en cascade traditionnels, mais « les processus de développement de logiciels modernes et agiles impliquent des mises à jour fréquentes du code, ce qui peut rendre ces PIA obsolètes au moment où elles sont écrites », dit-il. En conséquence, une approche plus automatisée et basée sur l'API pour intégrer la confidentialité dans le processus de développement est nécessaire, ajoute Jalil.

Pour ajouter à la complexité, il faut s'assurer que l'IA et les données sont utilisées de manière éthique, souligne Marques. Deux catégories clés comprennent l'IA sécurisée, dit-il: l'IA responsable et l'IA confidentielle. L'IA responsable se concentre sur la réglementation, la confidentialité, la confiance et l'éthique liées à la prise de décision à l'aide de modèles d'IA et de ML. L'IA confidentielle implique la manière dont les entreprises partagent des données avec d'autres pour résoudre un problème commercial courant.

Source : *http://bit.ly/2N4wECI*

Les attaques de ransomwares touchent les principaux utilitaires

05 Février 2021

Eletrobras, la plus grande compagnie d'électricité d'Amérique latine, fait face à une suspension temporaire de certaines opérations. Deux entreprises de services publics au Brésil ont subi des attaques de ransomwares distinctes, les forçant à interrompre temporairement certaines opérations et services. Dans un cas, des données sensibles ont été volées et publiées en ligne, y compris des connexions d'accès au réseau et des plans d'ingénierie.

Centrais Eletricas Brasileiras (Eletrobras) et Companhia Paranaense de Energia (Copel) ont tous deux signalé des attaques. Cette dernière semble être l'œuvre de Darkside, qui a fuité les données volées lors de l'attaque en ligne, selon un rapport publié. Darkside est un groupe de ransomwares techniquement innovant qui a tenté de se présenter comme un Robin des Bois altruiste et numérique en faisant des dons de bienfaisance avec le Bitcoin volé aux victimes.

Le groupe a déclaré avoir volé plus de 1000 gigaoctets de données Copel lors de l'attaque, y compris des informations sensibles permettant d'accéder à une infrastructure clé, des informations personnellement identifiables (PII) de la direction et des clients, et des plans d'ingénierie détaillés du réseau de l'entreprise. , selon le rapport, qui comprenait un instantané d'une annonce pour les données d'un forum de hackers.

Eletrobras est le plus grand service public d'Amérique latine et propriétaire d'Eletronuclear, qui construit et exploite des centrales nucléaires. Copel est le plus grand fournisseur de services publics de l'État brésilien de Parana. On ne sait pas pour l'instant qui est derrière l'attaque d'Eletrobras, ce que la société a reconnu dans un communiqué de presse publié. L'attaque a touché le réseau administratif de sa filiale Eletronuclear, qui gère deux centrales nucléaires, Angra1 et Angra 2. Quant à l'attaque contre Eletronuclear, la société a dû suspendre certains de ses systèmes pour protéger l'intégrité des données, a déclaré la société.

Source : *http://bit.ly/39Xp6e9*

Suite à l'attaque d'Oldsmar, le FBI met en garde contre l'utilisation de TeamViewer et de Windows 7

10 Février 2021

Une alerte du FBI avertit les entreprises de l'utilisation de systèmes Windows 7 obsolètes, de mots de passe de compte médiocres et du logiciel de partage de bureau TeamViewer.

Au lendemain de l'incident d'Oldsmar, où un attaquant non identifié a eu accès au réseau d'une station de traitement d'eau et a modifié les dosages chimiques à des niveaux dangereux, le FBI a envoyé une alerte, attirant l'attention sur trois problèmes de sécurité qui ont été constatés sur le réseau de l'usine après le fameux piratage.

L'alerte, appelée notification du secteur privé, ou code PIN du FBI , met en garde contre l'utilisation de systèmes Windows 7 obsolètes, de mauvais mots de passe et du logiciel de partage de bureau TeamViewer, exhortant les entreprises privées et les organisations fédérales et gouvernementales à examiner les réseaux internes et à accéder en conséquence aux politiques.

Le code PIN du FBI désigne spécifiquement TeamViewer comme un logiciel de partage de bureau à surveiller après que l'application ait été confirmée comme point d'entrée de l'attaquant dans le réseau de la station de traitement d'eau d'Oldsmar.

"Au-delà de ses utilisations légitimes, TeamViewer permet aux cyberacteurs d'exercer un contrôle à distance sur les systèmes informatiques et de déposer des fichiers sur les ordinateurs des victimes, ce qui le rend fonctionnellement similaire aux chevaux de Troie d'accès à distance (RAT)", a déclaré le FBI.

L'alerte du FBI n'indique pas spécifiquement aux organisations de désinstaller TeamViewer ou tout autre type de logiciel de partage de bureau, mais avertit que TeamViewer et d'autres logiciels similaires peuvent être utilisés de manière abusive si des attaquants accèdent aux informations d'identification du compte des employés ou si les comptes d'accès à distance (tels que ceux utilisés pour Accès Windows RDP) sont sécurisés avec des mots de passe faibles.

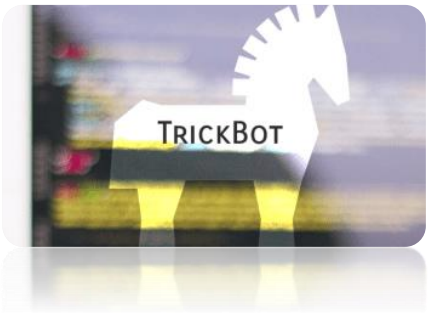
En outre, l'alerte du FBI met également en garde contre la poursuite de l'utilisation de Windows 7, un système d'exploitation qui est arrivé en fin de vie l'année dernière, le 14 janvier 2020, un problème dont le FBI a également mis en garde les entreprises américaines l'année dernière .

Cette partie de l'avertissement a été incluse parce que la station d'épuration d'Oldsmar utilisait toujours les systèmes Windows 7 sur son réseau, selon un rapport du gouvernement du Massachusetts .

Source : *https://zd.net/3uuznXy*

Une nouvelle campagne de phishing fournit un cheval de Troie Windows

15 Février 2021



Les chercheurs de Fortintet identifient des attaques de phishing distribuant une nouvelle variante du cheval de Troie Bazar, un malware qui crée une porte dérobée complète sur les PC Windows infectés

Une nouvelle campagne de phishing tente d'attirer les victimes vers le téléchargement de la dernière version d'un cheval de Troie malveillant – et elle a des liens avec l'une des opérations cybercriminelles les plus prolifiques actives dans le monde aujourd'hui.

Le cheval de Troie Bazar est apparu l'année dernière, et un déploiement réussi du logiciel malveillant peut fournir aux cybercriminels une porte dérobée vers les systèmes Windows compromis, leur permettant de contrôler le dispositif et d'obtenir un accès supplémentaire au réseau afin de collecter des informations sensibles ou de livrer des logiciels malveillants, y compris des ransomwares.

La porte dérobée a été utilisée dans des attaques visant des secteurs comme la santé, la technologie, la fabrication et la logistique en Amérique du Nord et en Europe. Des chercheurs l'ont associée aux développeurs de Trickbot, l'une des formes les plus courantes de logiciels malveillants pour les pirates informatiques cherchant à pénétrer les réseaux.

Les chercheurs en cybersécurité de Fortinet ont identifié une nouvelle variante du cheval de Troie Bazar, équipée de techniques d'analyse pour rendre les logiciels malveillants plus difficiles à détecter par les logiciels antivirus. Il s'agit notamment de cacher les API malveillantes dans le code et de ne les appeler qu'en cas de besoin, d'obfusquer le code de manière supplémentaire et même de chiffrer certaines chaînes du code pour le rendre plus difficile à analyser.

Les nouvelles techniques ont été ajoutées à Bazar vers la fin janvier et coïncidé avec une campagne de phishing destinée à distribuer la version mise à jour du logiciel malveillant.

Les thèmes utilisés par les e-mails de phishing destinés à susciter l'intérêt des victimes potentielles des entreprises comprennent de faux rapports de plainte de clients, de faux relevés de facturation et la fausse offre d'un bonus financier. Quel que soit le thème du courriel, les attaques de phishing du cheval de Troie Bazar tentent d'encourager une victime potentielle à cliquer sur un lien qui prétend rediriger vers un PDF contenant des informations supplémentaires sur l'objet du message.

Afin d'éviter d'être victime d'attaques de phishing distribuant Bazar ou tout autre type de logiciel malveillant, les chercheurs

recommandent aux organisations de fournir des conseils à leurs employés sur la manière d'identifier et de se protéger contre les attaques et les escroqueries.

Les organisations doivent également s'assurer qu'elles ont mis en place une stratégie d'application des patchs, qui empêche les logiciels malveillants de pouvoir exploiter des vulnérabilités connues comme moyen d'accéder aux réseaux.

Source : *https://bit.ly/3dJjvKS*

Un nouveau piratage permet aux attaquants de contourner le code PIN MasterCard en les utilisant comme carte Visa

19 Février 2021

Des chercheurs en cybersécurité ont révélé une nouvelle attaque qui pourrait permettre à des criminels de tromper un terminal de point de vente pour qu'il effectue des transactions avec la carte sans contact Mastercard d'une victime tout en pensant qu'il s'agit d'une carte Visa.

La recherche, publiée par un groupe d'universitaires de l'ETH Zurich, s'appuie sur une étude détaillée en septembre dernier qui s'est penchée sur une attaque de contournement de code PIN, permettant aux acteurs malveillants d'utiliser la carte de crédit Visa EMV volée ou perdue d'une victime pour effectuer des achats de grande valeur sans connaître le code PIN de la carte, et même tromper le terminal en acceptant des transactions par carte hors ligne non authentiques.

"Il ne s'agit pas simplement d'un mélange de marques de cartes, mais cela a des conséquences critiques", ont déclaré les chercheurs David Basin, Ralf Sasse et Jorge Toro. "Par exemple, les criminels peuvent l'utiliser en combinaison avec l'attaque précédente contre Visa pour contourner également le code PIN des cartes Mastercard. Les cartes de cette marque étaient auparavant présumées protégées par code PIN."

Suite à une divulgation responsable, les chercheurs de l' ETH Zurich ont déclaré que Mastercard avait mis en œuvre des mécanismes de défense au niveau du réseau pour contrecarrer de telles attaques. Les résultats seront présentés au 30e Symposium sur la sécurité USENIX en août plus tard cette année.

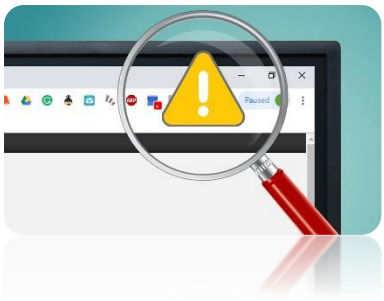
Tout comme l'attaque précédente impliquant des cartes Visa, les dernières recherches exploitent également des vulnérabilités «critiques» dans le protocole sans contact EMV largement utilisé, mais cette fois la cible est une carte Mastercard.

À un niveau élevé, cela est réalisé à l'aide d'une application Android qui implémente une attaque de type man-in-the-middle (MitM) au sommet d'une architecture d'attaque de relais, permettant ainsi à l'application non seulement d'initier des messages entre les deux extrémités - le terminal et le carte - mais aussi d'intercepter et de manipuler les communications NFC (ou Wi-Fi) pour introduire de manière malveillante une discordance entre la marque de la carte et le réseau de paiement.

Source : *https://bit.ly/3aMxnC7*

Les extensions de navigateur gagnent en traction en tant que vecteur d'attaque

12 Février 2021



Google a supprimé l'extension The Great Suspender du Chrome Web Store et publié une notification indiquant que l'extension contient des logiciels malveillants.

En effet, il a été découvert qu'une fonctionnalité secrète a été ajoutée par un nouveau responsable, qui pourrait être utilisée abusivement pour exécuter à distance du code arbitraire. Cependant, ce n'est pas la seule instance d'une extension de navigateur utilisée comme vecteur d'attaque.

Il existe différentes manières d'exploiter les navigateurs infectés.

Les acteurs de la menace peuvent récupérer les informations des utilisateurs. Contrôlez le navigateur de la victime depuis un emplacement différent sans vous soucier des défenses locales.

De plus, ces extensions peuvent être utilisées pour mettre en place un canal d'exfiltration vers le navigateur du hacker.

Des extensions de navigateur malveillantes sont de plus en plus utilisées pour infecter des millions d'utilisateurs à travers le monde. Le fait le plus choquant est que ces extensions sont juste devant nous et que nous ne sommes pas conscients de leurs capacités. Bien que Google supprime de telles extensions quotidiennement, les acteurs de la menace proposent des moyens uniques de faire passer du code dans les postes de travail.

Source : https://bit.ly/3usolSq

Evènements

Evènements du mois

ISMG SUMMETS
02-24 Février 2021, En ligne
https://bit.ly/3dFux3x

Durant le mois de Février, 3 SOMMETS ont été organisés dans le cadre des événements d'ISMG, soit :

- Sommet virtuel sur la cyber sécurité : Zero Trust 02-03 février 2021
- Sommet virtuel sur la cyber sécurité : gestion des identités et des accès 16-17 février 2021
- Sommet virtuel sur la cyber sécurité : Asie du Sud-Est 23-24 février 2021

Le sommet virtuel Zero Trust a permis d'obtenir des informations d'experts de la part de praticiens, de chercheurs et de fournisseurs sur les mythes et les réalités concernant la confiance zéro, les directives et normes émergentes et la manière dont la confiance zéro est déployée avec succès.

Dans le second sommet virtuel, des experts du domaine ont été présents pour permettre aux participants d'apprendre à franchir la ligne entre commodité, accessibilité et sécurité.

Et enfin, le dernier sommet a présenté un aperçu des leaders d'opinion en cyber sécurité sur les mythes et les réalités du déploiement de nouveaux cadres, de l'application des leçons apprises et a permis aux participants de réfléchir de manière stratégique, au-delà de l'hypothèse qu'une équipe plus nombreuse est le meilleur moyen de répondre à un risque accru.

CISO Exchange
24 février 2021, En ligne
https://bit.ly/3aPTbN3

Le CISO Exchange a présenté divers échanges conçus pour créer une expérience exclusive pour le responsable de la sécurité de l'information et les responsables de la sécurité de l'information, où ont été offertes de véritables interactions entre pairs. Dans cette collaboration de haut niveau, les cadres ont connecté, identifié et comparé les solutions aux défis commerciaux critiques auxquels ils sont confrontés.

Evènements du mois prochain

Dark Reading Webinar
09 Mars 2021, En ligne
http://bit.ly/2O6k9Hm

Les cyber-attaquants ont touché des cibles et des bases de données sensibles ont été violées : que faire maintenant ? Que devez-vous dire aux clients, employés et autres parties prenantes ; et quand ? Avez-vous un plan pour contenir les dommages, éliminer la menace, éviter la destruction des preuves et maintenir l'entreprise opérationnelle en même temps ? Savez-vous comment respecter les exigences de conformité, répondre aux questions des clients et payer tous les coûts imprévus d'une violation de données ? Soyez prêt avec quelques réponses. Dans ce webinaire, vous pourrez découvrir les processus et procédures, outils et techniques qui devraient être inclus dans votre playbook de réponse aux violations de données, afin que votre « mauvaise journée » infosec n'ait pas besoin d'être pire.

Reference	ANPT-2021-BV-02
Titre	Bulletin de veille N°2
Date de version	28 Février 2021
Contact	ssi@anpt.dz