Alerte : Nouvelle vulnérabilité dans les navigateurs Microsoft

Alerte : Nouvelle vulnérabilité dans les navigateurs Microsoft

Une vulnérabilité a été découverte dans les navigateurs Microsoft. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance.

1 – Risque(s)

• exécution de code arbitraire à distance

2 – Systèmes affectés

• Internet Explorer 11 pour Windows 7
• Internet Explorer 11 pour Windows 8.1
• Internet Explorer 11 pour Windows 10
• Internet Explorer 11 pour Windows Server 2012 et 2016
• Microsoft Edge pour Windows 10

3 – Résumé

Une vulnérabilité a été découverte dans les navigateurs Microsoft. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance.

4 – Contournement provisoire

Une vulnérabilité présente dans les navigateurs Internet Explorer et Edge permet à un attaquant d'exécuter du code arbitraire depuis une page internet malveillante.
Cette vulnérabilité exploite une faille de type confusion de type et peut être déclenchée en définissant des valeurs particulières pour les propriétés d'un objet tableau dans une page Web spécialement conçue.
On notera que cette vulnérabilité est atténuée par l'utilisation de la mesure de sécurité de Windows Control Flow Guard (CFG) au sein de l'application. Un attaquant souhaitant exploiter la vulnérabilité devra ainsi mettre en oeuvre un contournement de la contre-mesure CFG.
Aucun correctif n'est prévu par Microsoft avant la publication mensuelle des correctifs de sécurité du mois de mars. Dans l'attente de la disponibilité d'un correctif de sécurité, le CERT-FR recommande de privilégier l'utilisation de navigateurs autres qu'Internet Explorer ou Edge pour la navigation sur Internet.

5 – Documentation

• Rapport de Bogue de Project Zero du 23 février 2017
https://bugs.chromium.org/p/project-zero/issues/detail?id=1011
• Référence CVE CVE-2017-0037
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0037
.

Source : *Vulnérabilité dans les navigateurs Microsoft*

Nouvelles tensions autour du Privacy Shield entre l’Europe et les USA

Nouvelles tensions autour du Privacy Shield entre l’Europe et les USA

Une coalition d'associations demande à la Commission européenne de suspendre le nouvel accord sur les données personnelles, intitulé Privacy Shield, si les États-Unis ne réforment pas leur politique en matière de renseignement.

Le rejet envers le Privacy Shield ne faiblit pas. Dans une lettre ouverte datée de mars, une coalition d'associations européennes et internationales, dont La Quadrature du Net, demandent aux États-Unis et à l'Union européenne de suspendre l'exécution de ce mécanisme juridique. L'accord transatlantique « *ne donne pas assez de garanties à la protection des données personnelles des Européens* » jugent-elles.
Le **Privacy Shield** est l'accord qui encadre les transferts des données personnelles vers les États-Unis. Il remplace l'ancien Safe Harbor que la Cour de justice de l'Union européenne a invalidé fin 2015 parce que les protections apportées par le droit européen n'étaient pas assurées aux USA.
La raison ? Les lois américaines sur le renseignement actuellement en vigueur outre-Atlantique. « *Au moment de l'adoption de cet accord, plusieurs groupes ont souligné que la loi américaine était inadaptée pour protéger les données des européens et ne satisfaisait pas le critère d'« équivalence substantielle » imposé par la Cour de justice de l'Union européenne* », écrivent les signataires.
Ils rappellent qu'ils « *ont à plusieurs reprises pointé du doigt les défauts présents dans les mécanismes américains de recours et de supervision des violations de la vie privée, les insuffisances dans les limitations de la collecte, l'accès et l'utilisation des données personnelles, et les incertitudes des garanties écrites* ». Pour toutes ces raisons, et sans action du côté américain, la suspension est l'unique solution.
« *Sans réelle réforme de la surveillance, nous pensons qu'il est de votre responsabilité, à défaut d'une meilleure option, de suspendre le Privacy Shield. Nous vous exhortons à clarifier ce positionnement pour vos homologues américains* » ajoutent les associations. Sinon, « *nous considèrerons cela comme un message fort envoyé à l'Union européenne déclarant que nos droits sont sans importance* ».

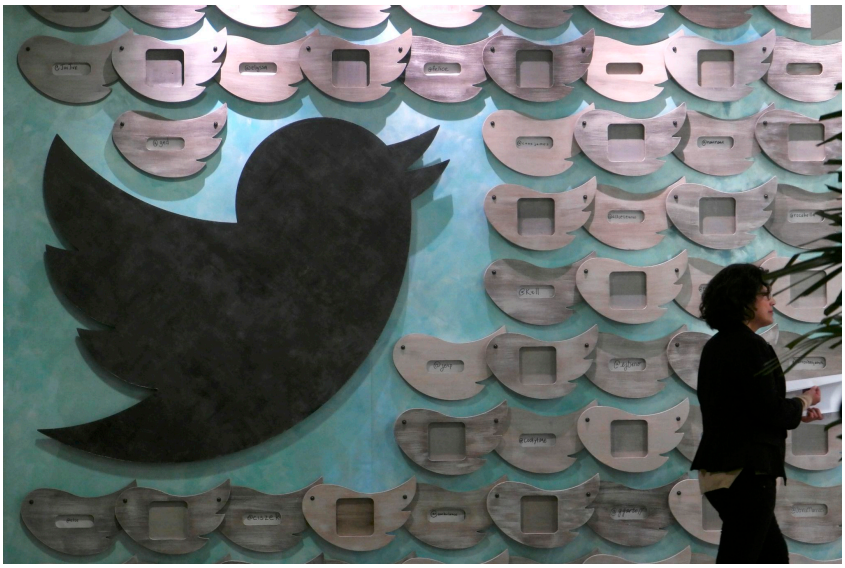
INQUIÉTUDE EN EUROPE

Les associations civiles ne sont pas les seules à s'alarmer des faiblesses du Privacy Shield. L'été dernier, le groupe de l'article 29 (G29), qui rassemble au niveau européen toutes les autorités de protection des données et de la vie privée, comme la Commission nationale de l'informatique et des libertés en France, a ainsi fait part de son inquiétude, après avoir critiqué le Privacy Shield dans un avis du 13 avril 2016…[lire la suite]

Réagissez à cet article

Source : *Privacy Shield : levée de boucliers contre l'accord sur les données personnelles entre l'Europe et les USA – Politique – Numerama*

La lutte du cyberharcèlement sur Twitter grâce à l'intelligence artificielle



La lutte du cyberharcèlement sur Twitter grâce à l'intelligence artificielle

---

Le réseau social va s'aider d'outils d'apprentissage automatique pour repérer plus vite les messages allant à l'encontre de ses règles d'utilisation

Un concert d'excuses et quelques mesures concrètes. Après plusieurs années de silence et d'hésitation, Twitter promet que 2017 sera l'année de la lutte contre le harcèlement. Le réseau social présente trois nouveaux outils pour limiter l'influence des discours de haine et des attaques ciblés contre ses utilisateurs. Ils seront déployés à partir de mardi. D'autres fonctionnalités devraient être présentées dans le courant de l'année. «Nous avons entendu vos critiques. Nous n'avons pas progressé assez l'année dernière», avait déclaré Ed Ho, vice-président de Twitter, fin janvier. «Nous continuerons à être attentifs à vos retours, d'apprendre des critiques et de sortir des nouvelles fonctionnalités jusqu'à ce que tous nos utilisateurs ressentent ces changements.» Twitter va se reposer sur une nouvelle arme pour l'aider dans sa modération: l'intelligence artificielle.

Repérer plus rapidement les agressions

Le nouveau plan de Twitter comporte trois mesures phares. La première doit lutter contre la création abusive de nouveaux comptes par des utilisateurs déjà bannis du réseau social. Il est difficile de repérer ces internautes. Il changent généralement d'adresse mail, de numéro de téléphone et d'adresses IP pour s'inscrire à nouveau. Twitter va s'appuyer sur un programme d'apprentissage automatique afin de repérer les resquilleurs. Tout compte banni définitivement du réseau social sera analysé afin de repérer des signaux permettant d'identifier une personne, comme une manière de parler, des sujets ou des victimes de prédilection, des hashtags préférés, etc. Si un nouveau compte Twitter correspond à cette analyse, il pourra être rapidement supprimé.

Twitter crée également une nouvelle option pour masquer les images choquantes dans les recherches de tweets. Sont concernées les photos pornographiques ou violentes. Elles seront repérées automatiquement. Par exemple, une personne tapant «Bataclan» dans la barre de recherche de Twitter devrait en théorie ne pas voir de photos de la tuerie. Cet outil devrait aussi être utile pour les personnes faisant l'objet d'une campagne de dénigrement, afin de ne pas voir son pseudo associé à des images pornographiques ou violentes. L'option sera enclenchée par défaut, mais pourra être désactivée dans les réglages Twitter.

Dernier outil lancé par le réseau social: les réponses à un tweet seront bientôt classées par ordre d'intérêt. Les messages automatiquement détectés comme «peu intéressants» par Twitter seront relégués en bas. Parmi les critères examinés par le réseau social: si le compte est nouveau et ne suit aucune autre personne, s'il a déjà été signalé pour abus ou qu'il emploie des insultes.

Accélérer le signalement

L'intelligence artificielle ne va pas remplacer les modérateurs de Twitter. Elle interviendra pour accélérer le signalement de contenus. Comme les autres réseaux sociaux, Twitter applique une modération *a posteriori*: les utilisateurs doivent lui signaler les contenus problématiques pour qu'ils soient contrôlés et éventuellement supprimés s'ils enfreignent les règles d'utilisation. Le réseau social collabore aussi avec les autorités qui peuvent lui signaler des contenus illégaux. En France, plus de 466 tweets ont fait l'objet d'une demande de retrait par la police ou le gouvernement entre janvier et juin 2016…[lire la suite]

Réagissez à cet article

Source : *Twitter s’appuie sur l’intelligence artificielle pour lutter contre le harcèlement*

Yahoo subit un énième hack embarrassant, la patronne du groupe se justifie sur Tumblr

Yahoo subit un énième hack embarrassant, la patronne du groupe se justifie sur Tumblr

---

Yahoo donne les détails des hacks qui ont touché plus d'un milliard de comptes, et en révèle un nouveau. Et la patronne se serait fait sucrer ses primes.

La crucifixion de **Yahoo** continue, et si ce n'est pas déjà fait, on ne peut que vous recommander à ce stade de supprimer votre éventuel compte Yahoo. Dans un communiqué, l'entreprise est revenue par le menu sur toutes les attaques qui ont gravement entaché la réputation de l'entreprise depuis 2014. On y apprend en prime que dernièrement, des hackers ont obtenu du code propriétaire de Yahoo et ont pu fabriquer de faux cookies.
Cela leur aurait permis d'accéder à 32 millions de comptes entre 2015 et décembre 2016. Sur cette masse, seuls 26 utilisateurs auraient été prévenus. L'entreprise explique également collaborer avec les autorités depuis que son enquête a révélé la possible implication de **hackers** soutenus par un état dans ces piratages. En tout, plus d'un milliard de comptes Yahoo ont été compromis depuis 2014…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Yahoo subit un énième hack embarrassant, la patronne du groupe se justifie sur Tumblr*

1,2 million de francs détournés d’une entreprise Bernoise

1,2 million de francs détournés d’une entreprise Bernoise

CYBERCRIMINALITÉ – Une société bernoise a été victime de piratage informatique. En tout, 1,2 million de francs ont été détournés. Le patron ne décolère pas, s'étonnant du manque de réactivité des banques.

Des cyber-criminels sont parvenus à détourner 1,2 million de francs des comptes de la société bernoise Küng Holding. Mis à part 160'000 francs, l'argent a pu être récupéré, mais le patron de l'entreprise Christoph Küng ne décolère pas.

Ce dernier s'étonne d'une part que trois banques aient déclenché sans demande d'éclaircissements des paiements vers d'obscures adresses. Dans un cas, 785'000 francs ont notamment été versés à un individu au Kirghizistan. D'autre part, M. Küng estime que le logiciel de paiement utilisé comporte de sérieux problèmes de sécurité.

Ces failles ont rendu possibles les ordres de paiement du pirate informatique, a confié jeudi Christoph Küng à l'ats. Il confirmait des informations publiées par le site internet Inside Paradeplatz, le Bund et la Berner Zeitung.

Cheval de Troie

Les cyber-criminels ont agi en utilisant le cheval de Troie Gozi, qui s'introduit dans les ordinateurs par le biais d'une pièce-jointe dans un courriel. Ces ordres de paiement ont seulement éveillé les soupçons de PostFinance, qui a considéré une demande de virement de 49'000 francs comme « inhabituelle ».

Les trois banques ont en revanche autorisé ces paiements sans difficulté. Ce n'est que par la suite que Christoph Küng a pu péniblement stopper une grande partie de ces virements et récupérer l'argent.

La société informatique suisse qui a développé le logiciel se défend des accusations, estimant que Küng Holding n'a pas installé une mise à jour importante. Christoph Küng nie toutefois cette affirmation…[lire la suite]

NDLR : Denis JACOPINI souhaiterai bien être Expert judiciaire désigné sur cette affaire. Analyser le moyen utilisé par le pirate informatique pour modifier le comportement du logiciel de comptabilité devrait être très instructif !

La responsabilité de l'éditeur va t-elle être recherchée en raison de l'existence d'une faille de sécurité sans son logiciel et en raison de sa possible négligence pour ne pas avoir mis en place des mesures de sécurité adapté au coté sensible de la fonction de virement automatique ?

La responsabilité du dirigeant qui n'a pas appliqué la mise à jour recommandée est elle engagée ?

Peut-être bien que l'expertise permettra d'aboutir à une toute autre cause .

Si nous le pouvons, nous suivrons cette affaire.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Piratage informatique dans une entreprise bernoise: 1,2 million de francs détournés*

Les dangers des jouets connectés | Denis JACOPINI

Les dangers des jouets connectés | Denis JACOPINI

La gamme Cloudpets de Spiral Toys a été piratée. Plus de 800000 comptes ont été piratés avec les informations qui y sont liées et plus de 2,2 millions de messages vocaux se retrouvent également sur la toile. Les peluches connectées de la marque permettait en effet aux parents et aux enfants de s'échanger des messages par le biais d'une application téléphonique, à travers l'ours en peluche.

Denis JACOPINI a été Interviewé par la revue Atlantico à ce sujet :

Atlantico : Une société d'ours en peluche connectés a été récemment piratée, les messages laissés par les parents à leurs enfants sont désormais hackable. Ce n'est pas la première fois que ce type de piratage arrive, pour protéger nos enfants, devrions-nous les éloigner de ce type de jouets connectés ?
Denis JACOPINI : En effet, au-delà du risque relatif à la protection des données personnelles des enfants et de leurs parents, la revue Que choisir avait déjà alerté les consommateurs en fin 2016 sur des risques inhérents au connexions non sécurisée de plusieurs jouets connectés.
Qui a tenu compte du résultat de cette étude pour revoir la liste des jouets qui seraient présents dans la hotte légendaire ?
La relation entre les enfants et les jouets va bien au-delà de la technologie et des risques qu'elle peut représente.
Les jouets bénéficie également de phénomènes de mode et l'engouement, sauf erreur, se fout bien de la qualité des produits et encore moins de leur sécurité.
Manque de connaissance, inconscience, crédulité ou trop de confiance de la part des parents ? Il est vrai qu'on peut facilement croire que si des jouets se trouvent sur nos rayons, c'est qu'ils ont forcément dû passer avec succès toute une batterie de tests rassurant pour le consommateur.
Pour la part des jouets à usage familial testés, même si les normes EN71 et EN62115 ont été récemment révisées pour répondre aux exigences de la nouvelle directive 2009/48/CE, les validations se reposeront sur des niveaux satisfaisants en terme de propriétés physiques et mécaniques, d'inflammabilité, de propriétés chimiques, électriques ou bien relatives à l'hygiène et à la radioactivité.
Vous l'aurez remarqué, aucun test n'est prévu pour répondre à des mesures ne serait-ce que préventive en terme de protection des données personnelles et encore moins en matière se sécurité numérique.
Alors finalement, pour répondre à votre question : « devrions-nous éloigner les enfants de ce type de jouets connectés ? »
A mon avis, en l'absence de normes protectrices existantes, la prudence devrait être de mise. Certes, il est impossible de se protéger de tout. Cependant, il serait à minima essentiel que les parents soient informés des risques existants et des conséquences possibles que pourraient provoquer des piratages par des personnes mal intentionnées pour prendre des mesures qu'ils jugent utiles.

Atlantico : Comment pouvons-nous restreindre la possibilité de piratage de données pour ce type d'objet ?
D.J. : La situation confortable serait que le consommateur soit vigilant pour ce qui concerne les mesures de sécurité couvertes par l'appareil et celles qui ne le sont pas. Malheureusement, ces gardes-fous ne sont qu'à l'état d'étude.
Sauf à vous retrouver dans un environnement ou le voisin le plus proche se trouve à plusieurs dizaines de mètres, être prudent dans l'usage de ces objets pourrait par exemple consister à :
– Si le jouet le permet, changer le mot de passe par défaut et mettre en place un mot de passe complexe pour accéder à sa configuration ;
– Si le jouet le permet, activer les connexions sécurisées par cryptage ;
– Si le jouet le permet, désactiver les connexions à partir d'une certaine heure ;
– N'utiliser les jouets connectés que dans des environnements protégés, en raison de la portée limitée des communications Bluetooth (par des distances suffisantes entre le jouet et des pirates éventuels) ;
– Pour les jouets utilisant le Wifi,
– Mettre en place des protections physiques contre les rayonnements électromagnétiques dans certaines directions ;
– Cacher les caméras si elles ne sont pas utilisées ;
– En fin d'utilisation du jouet, ne pas se satisfaire d'éteindre l'appareil qui ne sera peut-être seulement en veille, mais retirer les piles ou placer le jouet dans un espace protégé (fabriquez une cage de Faraday) ;
Enfin, compte tenu que le bon fonctionnement du jouet est lié à l'acceptation des conditions contractuelles d'utilisation des donnés personnelles ne respectent pas les règles européennes relative à la protection de ces données et de la vie privée car les fabricants sont généralement situés hors Europe, ne pas accepter ces conditions reviendrait à être privé de l'usage des fonctions du jouet.

Atlantico : Concrètement, les objets connectés sont une porte ouverte à notre intimité, quels sont les dangers liés à ce type d'objets ?
A défaut d'information de la part des fabricants et d'alerte de la part des médias, il serait, à mon avis, adapté que le consommateur reconsidère les objets numériques et particulièrement les objets connectés comme étant des équipements dont les fonctions et conséquences induites risquent de se retourner contre son utilisateur.
L'année dernière, l'association de consommateurs UFC-Que choisir a mis en garde les consommateurs sur le stockage des données. Elle a d'ailleurs saisi sur le sujet la Commission nationale de l'informatique et des libertés et la Direction générale de la concurrence, de la consommation et de la répression des fraudes.
En effet, tout ce que disent les enfants à la poupée testée est enregistré et mystérieusement stocké sur des serveurs à l'étranger et géré par la société Nuance Communications. L'Association européenne de défense des consommateurs a déclaré : « Tout ce que l'enfant raconte à sa poupée est transmis à l'entreprise, basée aux États-Unis, Nuance Communications, spécialisée dans la technologie de reconnaissance vocale ».
Quelles sont les conséquences d'un tel usage de nos données ?
L'objectif évident est le matraquage publicitaire des enfants, car certains jouets ont une certaine tendance à faire souvent allusion à l'univers de Disney ou à Nickelodeon par exemple.
Enfin, des tests ont montré qu'un tiers situé à 20 mètres du jouet peut s'y connecter par Bluetooth et entendre ce que dit votre enfant à sa poupée ou à son robot, sans même que vous en soyez averti. La connexion peut même se faire à travers une fenêtre ou un mur en béton et le nom Bluetooth par défaut du jouet connecté, permet très simplement de les identifier.
Plus grave encore… Un tiers peut prendre le contrôle des jouets, et, en plus d'entendre votre enfant, communiquer avec lui à travers la voix du jouet.
Que ça soit en en terme d'écoute et d'espionnage à distance de l'environnement de l'enfant et de celui des parents, ou en terme de prise de contrôle à distance de l'appareil risquant de terroriser ou pire, traumatiser l'enfant, la prudence doit d'abord rester de mise.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement..
(Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

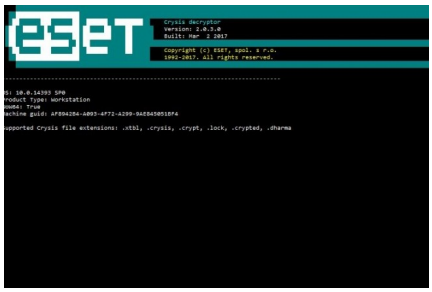
Réagissez à cet article

Source : *Jouet connecté : après un piratage, les données de 800000 familles fuitent sur le web*

Le Ransomware Dharma enfin décrypté

	Le Ransomware Dharma enfin décrypté

Les clés de déchiffrement du ransomware Dharma ainsi que toutes ses variantes ont été mises en ligne par un utilisateur. Kaspersky et Eset ont mis à jour leurs outils de lutte contre les ransomwares pour permettre à toute personne ou entreprise de déchiffrer gratuitement leurs fichiers chiffrés.



Les fournisseurs de sécurité dont Kaspersky et Eset ont mis à jour leurs outils pour permettre de déchiffrer les fichiers piégés par le ransomware Dharma. (crédit : D.R.)

C'est une belle victoire qui vient d'être remportée contre le diabolique ransomware Dharma. Les personnes ayant des fichiers chiffrés par ce programme peuvent en effet souffler car ils peuvent désormais avoir accès à des clés de déchiffrement pour pouvoir les retrouver. Apparu pour la première fois en novembre, Dharma est basé sur l'ancien programme de ransomware Crysis. Il est facile de le reconnaitre par l'ajout aux fichiers chiffrés de l'extension .[email_address].dharma. , l'adresse mail correspondant à celle utilisée par le pirate pour tenter d'extorquer sa victime.
Mercredi, un utilisateur sous le pseudonyme de gektar a publié un lien vers un post Pastbin sur le forum du support technique de BleepingComputer.com. Un post indiquant contenir les clés de déchiffrement du ransomware Dharma et de toutes ses variantes. Etrangement, la même chose s'est produite en novembre avec les clés de son prédécesseur, Crysis ce qui a permis à des chercheurs de créer des outils de déchiffrement. Aucune autre motivation que celle de mettre à disposition ces clés n'a été enregistrée concernant gektar. La bonne nouvelle est que ce leak a permis aux chercheurs de Kaspersky et d'Eset de vérifier son travail. Bingo : les deux sociétés ont mis à jour leurs outils de déchiffrement respectifs à savoir RakniDecryptor et CrysisDecryptor.

Une guerre des gangs dans les ransomwares

Cette situation devrait résonner à l'oreille des personnes touchées par des ransomwares qui ne devraient pas oublier de conserver une copie de leurs fichiers chiffrés à leur insu. Les chercheurs trouvent en effet parfois des failles dans les implémentations du chiffrement des ransomwares leur permettant de casser le chiffrement des clés. Dans d'autres cas, les autorités judiciaires et de police saisissent les serveurs de commande et de contrôle utilisés par les gangs de ransomware et publient ces clés.
Dans d'autres cas comme ici, les clés arrivent à la surface par d'autres moyens inexpliqués. Peut être parce que le développeur du ransomware a décidé de fermer boutique et décide de lâcher les clés, ou alors a-t-on à faire à une rivalité entre deux gangs de hackers qui se mettent des bâtons dans les roues pour court-circuiter l'activité des uns et des autres. Dans tous les cas, il est également recommandé de jeter un oeil sur le site NoMoreRansom.org, régulièrement mis à jour et proposant aussi bien des outils que des conseils pour lutter contre ces fichus ransomwares.

Article rédigé par Lucian Constantin / IDG News Service

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DIRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Un ransomware piège les Mac*

Les drones volent au secours des agriculteurs

Les drones volent au secours des agriculteurs

Et si l'avenir de l'agriculture se jouait… dans les airs ? Depuis quelques années, les exploitants agricoles ont effet la possibilité d'analyser leurs parcelles à l'aide d'un

drone.…[Lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement..
(Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur sur cette page.

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

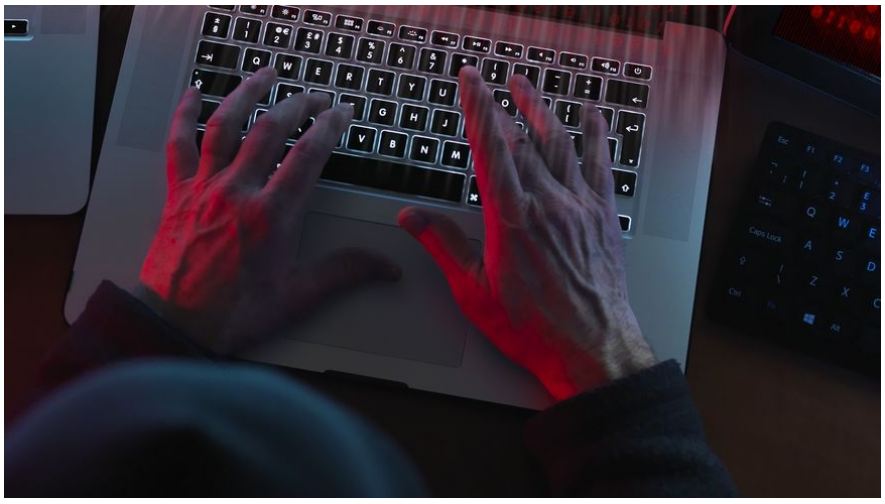
- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert
INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Comptes bidons, « fake news », vol de données : ces manipulations informatiques qui pourraient perturber la Présidentielle



Comptes bidons, « fake news », vol de données : ces manipulations informatiques qui pourraient perturber la Présidentielle

Elles ont beaucoup fait parler d'elles durant la campagne présidentielle américaine : certaines pratiques malveillantes sur Internet pourraient aussi peser sur l'élection en France. Voici en quoi elles consistent.
Interview par Marina Cabiten (France Bleu)

Des pirates informatiques qui œuvrent contre Hillary Clinton, et donc en faveur de Donald Trump, le tout commandité par le Kremlin : il ne s'agit pas d'un scénario de film mais d'une accusation très sérieuse formulée par les autorités américaines lors de la campagne présidentielle. Internet est un outil puissant pour les manipulations informatiques, à différents degrés. Et la France est, selon plusieurs acteurs de la cybercriminalité, très mal préparée à ces usages détournés. Voici comment des personnes mal intentionnées pourraient perturber la campagne.

Inonder les réseaux sociaux de faux utilisateurs : l'astroturfing

Tout un chacun peut utiliser son compte Facebook ou Twitter pour s'exprimer, et éventuellement partager ses opinions politiques. Mais cette utilisation des réseaux sociaux peut être bidonnée. Ce phénomène est appelé astroturfing, du nom d'une marque de pelouse synthétique pour les stades : Astroturf. Autrement dit, il s'agit de faire prendre aux internautes du faux gazon pour de l'herbe naturelle… Comment ? **En inondant les réseaux sociaux de faux comptes automatisés, les "bots"**, qui diffusent des messages rédigés par les initiateurs de cette technique de "marketing politique" qui ne dit pas son nom, et garantit l'anonymat.
N'importe quel internaute peut créer et animer des faux comptes. Avec un peu plus de moyens financiers, il peut payer pour qu'un réseau social comme Facebook donne plus de visibilité à une page ou à un post via un algorithme qui fera apparaître le message sur davantage de "murs" d'utilisateurs, qui n'ont rien demandé. Sur Twitter, il peut acheter des "followers" (personnes qui suivent le compte) pour donner une fausse légitimité à ses comptes artificiels. Le degré ultime est de se payer un logiciel qui fait ça tout seul, voire d'employer quelqu'un pour l'exploiter. Cela existe, au sein d'entreprises privées mais parfois aussi de partis politiques. **C'est une forme de propagande de plus en plus répandue.** Le gouvernement français a annoncé récemment son intention de surveiller les réseaux sociaux pour éventuellement repérer des "mouvements" suspects de ce type.

Quand des sites partisans se font passer pour des organes de presse : les « fake news »

L'expression "Fake news", qui se traduit littéralement par « fausses informations », est très en vogue depuis la présidentielle américaine et vient de la diffusion sur Internet de prétendus articles de presse, qui ne sont en réalité pas rédigés par des journalistes. Des articles contenant des informations non vérifiées, parfois erronées, voire carrément mensongères dans le but bien précis de manipuler l'opinion.
La mécanique est la même que pour l'astroturfing, tout faire pour que ces "fake news" soient largement vues sur Facebook et les autres réseaux sociaux ou forums. Selon les calculs du site Buzzfeed, les articles relayant de fausses informations **(comme le faux soutien du pape François à Donald Trump, ou la révélation imaginaire de ventes d'armes par Hillary Clinton à l'organisation Etat islamique)** ont suscité 8,7 millions d'interactions sur Facebook durant la campagne américaine, contre 7,3 millions pour les articles de la presse traditionnelle.
En France récemment, plusieurs médias ont fait part de leur volonté de lutter contre ce phénomène, allant même pour certains jusqu'à nouer un partenariat avec Facebook et Google. ***"Le problème c'est que la rumeur court toujours beaucoup plus vite que la rectification ou la suppression du contenu"***, objecte Denis Jacopini, diplômé en cybercriminalité et sécurité de l'information, ***"laissant s'installer dans l'esprit de l'électeur ces fausses affirmations."***

De vrais contenus, mais dérobés et diffusés sans autorisation : le vol de données

La menace la plus sophistiquée reste le vol d'informations numériques. C'est l'exemple des pirates informatiques (hackers) qui ont récupéré près de 20.000 courriels de responsables du parti d'Hillary Clinton. Ils sont entrés dans les serveurs du parti démocrate dès l'été 2015, accumulant ces données parfois embarrassantes sans que personne ne s'en aperçoive, pour les publier au moment opportun pour déstabiliser le camp démocrate. Une cyberattaque venue de Russie pour aider Donald Trump à gagner l'élection, affirme la CIA dans un rapport révélé par la presse américaine. ***"Aucun parti politique français n'est actuellement protégé contre une telle malveillance"***, assure Denis Jacopini.
Selon le Canard Enchaîné (numéro du 8 février 2017), **les services secrets français s'inquiètent de cyberattaques russes** durant la Présidentielle, qui auraient pour but d'aider la campagne de Marine Le Pen. De son côté, le secrétaire général du mouvement « En Marche ! » Richard Ferrand a affirmé publiquement que les pirates russes visent particulièrement Emmanuel Macron et ont déjà attaqué à plusieurs reprises son site web.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Comptes bidons, « fake news », vol de données : ces manipulations informatiques qui pourraient perturber la Présidentielle*

Cybersécurité dans le monde : à quoi peut-on s'attendre ?

Cybersécurité dans le monde : à quoi peut-on s'attendre ?

L'année 2016 a démontré que les mesures de sécurité traditionnelles ne suffisaient plus et que de nouvelles stratégies devaient être mises en place. 2017 va donc s'inscrire dans la continuité de ce qui a déjà été amorcé l'année passée, à savoir : toujours plus de sécurité pour toujours une protection maximisée. Les experts de NTT Security ont fait ressortir les tendances et les prévisions pour cette année qui débute.

Selon Garry Sidaway, Vice-Président Senior de la Stratégie de Sécurité

1. L'identité restera au cœur des enjeux

Au risque de nous répéter, les mots de passe fournissent aujourd'hui des garanties insuffisantes. À l'ère du digital et de la mobilité, commodité et sécurité ne font pas bon ménage. Certes, les mots de passe sont bien pratiques, mais ils sont de moins en moins perçus comme une preuve d'identité irréfutable. Devant l'utilisation croissante des smartphones et les exigences de simplicité des consommateurs et des professionnels, les solutions d'identité resteront donc au cœur des préoccupations en 2017. C'est ainsi que le mot de passe traditionnel cèdera du terrain face à la poussée du « multi-facteurs », une méthode combinant plusieurs facteurs d'authentification (localisation, possession d'un objet, d'une information, etc.). Cette association entre physique et digital, avec en toile de fond l'émergence de méthodes d'authentification avancées, favorisera le développement de nouvelles solutions de gestion des identités.

2. Le mobile sera omniprésent

Au royaume du digital, le mobile est roi. Un roi qui bouscule l'ordre établi dans de nombreux domaines, des méthodes de paiement jusqu'aux interactions sociales. Véritables hubs digitaux, nos smartphones constituent désormais non seulement une fenêtre de contrôle et d'interaction avec le monde mais aussi une interface d'identification et d'authentification. Dans un tel contexte, 2017 verra le curseur de la menace se déplacer des ordinateurs portables vers les appareils mobiles. Si, traditionnellement, les acteurs de la sécurité se sont concentrés sur les systèmes back-end et les conteneurs, ils devront revoir leur approche pour placer le mobile au cœur de leur dispositif.

3. Les entreprises surveilleront la menace interne

Le problème des menaces internes ne date pas d'hier. Côté défense, les progrès réalisés dans les domaines de l'analytique et de la détection des anomalies devraient se poursuivre en 2017. Dans un milieu de l'entreprise de plus en plus dynamique, définir les critères d'un comportement utilisateur « normal » restera un défi de taille. Toutefois, avec le développement de nouvelles techniques de machine learning, nous verrons l'analyse comportementale s'opérer directement au niveau des terminaux.

4. Fin de la détection basée sur les signatures

Antivirus nouvelle génération, solutions de sécurité des terminaux, solutions de détection et de réponse aux incidents… Peu importe leur nom, les solutions de protection des terminaux se projetteront bien au-delà de la détection basée sur des signatures statiques, à commencer par les outils d'analyses avancées que l'on retrouvera systématiquement sur ces solutions. Leur force résidera notamment dans leur capacité à exploiter la puissance du cloud pour partager l'information sur les menaces connues. La diversité et le volume sans précédent des malwares engendreront l'émergence d'une nouvelle approche. Destinée à enrayer le syndrome dit du « patient zéro », cette démarche reposera à la fois sur une collaboration internationale et l'utilisation d'une cyberveille prédictive et proactive pour libérer toute la force du collectif.

5. Le tout-en-un fera de plus en plus d'adeptes

Alors que le marché de la cybersécurité se consolide, les entreprises se tournent vers des solutions de sécurité couvrant l'intégralité des environnements TIC. Traditionnellement, la force des prestataires de sécurité managée (MSS) s'est située dans leur capacité à intégrer un maillage d'outils complexes et pointus. Aujourd'hui, la situation a changé. Tout l'enjeu consiste à intégrer le facteur sécurité à tous les échelons du cycle opérationnel de l'entreprise. Les clients chercheront donc un partenaire capable d'agir sur tous les fronts : applications métiers, infrastructure réseau, services cloud et de data center autour d'une console de gestion centralisée. En 2017, les solutions multifournisseurs apparaîtront comme datées. Les acteurs de la sécurité devront ainsi coordonner un service complet de bout en bout pour répondre aux enjeux de l'espace de travail digital.

Selon Stuart Reed, Directeur Senior Product Marketing

6. Les consommateurs exigeront plus de transparence

Une étude récente de NTT Security a mis en lumière les attentes croissantes des cyberconsommateurs en matière de transparence, tant sur le plan des pratiques que de la gestion des incidents. Ces conclusions traduisent notamment une sensibilisation accrue des consommateurs sur les questions de sécurité suite aux scandales de violations à répétition. La tendance est appelée à se poursuivre en 2017 et au-delà. Notons enfin que les entreprises dotées de politiques de sécurité et de plans d'intervention efficaces diminueront leur exposition au risque, tout en profitant d'un puissant levier de compétitivité.

7. L'innovation en moteur de consolidation

Du point de vue de l'offre comme des fournisseurs de cybersécurité, 2016 a été placée sous le signe de la consolidation. Au rang des plus grosses opérations, on citera l'acquisition de BlueCoat par Symantec, la série de rachats par Cisco et, plus proche de nous, la création de NTT Security autour de trois piliers : analytique de pointe, cyberveille avancée et conseils d'experts en sécurité. Derrière ce phénomène de consolidation, on retrouve une constante : l'innovation. Concrètement, les grandes entreprises ont racheté des spécialistes pour accéder à leurs compétences et les englober dans une offre plus aboutie. Ces grands acteurs profitent enfin d'économies d'échelle considérables – et de l'expertise et de l'efficacité qui en découlent – pour mener des programmes d'incubation qui viendront à leur tour stimuler l'innovation. Cette tendance de fond souligne bien l'importance de l'innovation pour évoluer au rythme des besoins de sécurité des clients.

8. L'identité des objets

Avec l'essor de l'IoT, la frontière entre physique et digital s'estompe peu à peu pour créer des expériences clients plus pratiques, rapides et efficaces. Seulement voilà, les cybercriminels ont eux aussi investi la sphère de l'IoT à l'affût de la moindre vulnérabilité. On a ainsi recensé des cyberattaques se servant d'objets connectés (caméras de vidéosurveillance, imprimantes…) pour lancer des attaques DDoS qui sont parvenues à paralyser des sites comme Twitter et Spotify. L'année 2017 verra sans doute une recrudescence des attaques perpétrées à l'encontre des objets connectés. D'où le besoin impérieux d'intégrer ces appareils à une politique de sécurité plus complète, notamment pour mieux contrôler l'identité et la légitimité de leurs utilisateurs.

9. L'analytique changera la donn

L'un des grands défis de la cybersécurité pourrait se résumer par cette question : comment produire une information cohérente à partir d'une avalanche de données issues de dispositifs multiples ? Si l'analyse de données a pour fonction première de « donner du sens », l'évolution des menaces doit nous inciter à revoir nos méthodes d'interprétation et de contextualisation de l'information. Dans cette optique, les outils avancés d'analyse du risque vous permettront de prendre les bonnes décisions. Au-delà des événements présents, ces outils ont pour fonction de décortiquer les données historiques pour faire ressortir des tendances, mais aussi d'utiliser l'intelligence artificielle pour identifier les schémas comportementaux annonciateurs d'une attaque. Fondées sur des technologies avancées de machine learning, des outils d'analyse automatiques et des experts en astreinte permanente, les solutions d'analytique de pointe promettent de changer la donne dans le secteur des MSS.

Selon Kai Grunwitz, Vice-Président Senior Europe Centrale

10. La cybersécurité va s'imposer comme un facteur clé de succès

Pour être reconnue comme tel par tous les acteurs concernés, la cybersécurité doit s'intégrer en amont à l'ensemble des processus métiers de l'entreprise. Dans un monde connecté où le digital gagne chaque jour en importance, les entreprises veulent pouvoir compter sur une sécurité parfaitement incorporée à leurs stratégies métiers et IT. Outre son rôle indispensable de gardienne des données sensibles, du capital intellectuel et des environnements de production, la cybersécurité sera également partie intégrante de l'innovation et de la transformation de l'entreprise.

La sécurité ne sera plus seulement le problème des DSI, mais s'invitera au cœur des processus métiers et constituera l'un des ressorts de la chaîne de valeur. Enfin, la gestion du cycle de sécurité constituera un différenciateur clé autant qu'une priorité essentielle dans le cadre d'une stratégie de sécurité orientée métiers. Elle procurera aux entreprises un avantage concurrentiel et un réel levier de valeur ajoutée.

Selon Chris Knowles, Directeur solutions

11. Le RGPD sera partout !

Si vous pensiez que le Règlement général sur la protection des données (RGPD) a été l'un des grands thèmes de 2016, attendez de voir ce que 2017 vous réserve. Alors que les fournisseurs proclameront les avantages de leurs technologies et que les équipes juridiques plancheront sur la définition d'une sécurité réellement irréprochable, les clients, eux, se lanceront dans les préparatifs.

12. Au royaume des aveugles, les borgnes sont rois… mais plus pour très longtemps !

Pour beaucoup d'entreprises, la sécurité se résume à la protection d'un périmètre au moyen de périphériques inline censés analyser l'intégralité du trafic et intervenir sur la base d'éléments visibles. Toutefois, la mobilité croissante des collaborateurs, associée à l'explosion du nombre d'applications cloud en entreprise, créent des « angles morts ». À commencer par le transit d'informations via des tunnels cryptés, le stockage et le traitement de données à l'extérieur de data centers sécurisés, ou encore les communications entre machines virtuelles qui échappent totalement à la surveillance des dispositifs de sécurité existants. En 2017, les entreprises se pencheront sur ce phénomène afin d'éliminer les angles morts et de reprendre le contrôle de leur sécurité.

Réagissez à cet article

Source : *Cybersécurité dans le monde : à quoi peut-on s’attendre ?*