Le piratage informatique aussi risqué pour les animaux

	Le piratage informatique aussi risqué pour les animaux

Pas évident d'y penser quand on n'est pas du milieu, mais au 21ème siècle, le braconnage se joue de plus en plus sur le terrain du numérique.

Le GPS, pour le meilleur comme pour le pire

Le balisage des animaux est une pratique qui date du début du XX^{e} siècle. **Après la pose de bagues sur les oiseaux au début du siècle, les scientifiques se sont tournés vers les transmetteurs radio dans les années 1950, avant de passer au système de suivi par satellite Argos dans les années 1970.** Aujourd'hui, c'est un autre système de suivi qu'utilisent les chercheurs : le GPS.

Cigogne équipée d'un GPS© Vasileios Karafillidis Shutterstock

Le GPS, tout le monde l'a dans son smartphone. Il nous facilite beaucoup la vie en nous aidant à nous retrouver dans une ville inconnue, en nous permettant d'appeler un taxi ou encore en nous rassurant lorsque nos enfants, rentrant seuls de l'école, utilisent leur smartphone pour partager avec nous leur localisation.

Mais au-delà de ces usages pratiques, s'en cache un plus obscur. Les balises GPS que les chercheurs placent sur les animaux ne sont pas des smartphones sophistiqués, il est donc assez facile de les pirater pour recevoir de manière indue ces données. Une faille que les braconniers exploitent à volonté, en mettant en danger la vie des animaux.

Lire aussi : la lutte contre le commerce en ligne de faune sauvage est engagée

Le cyber-braconnage, un problème qui ne sera pas résolu du jour au lendemain

Le phénomène est encore trop peu connu et réservé au milieu des chercheurs…[lire la suite]

Réagissez à cet article

Source : *Le piratage informatique, un risque pour les animaux*

Comment les « ondes de choc digitales » vont intensifier la concurrence dans tous les secteurs

	Comment les « ondes de choc digitales » vont intensifier la concurrence dans tous les secteurs

À mesure que 2020 approche, le rythme et l'impact des nouvelles technologies sur les entreprises et la société en général ne cessent de prendre de l'ampleur.
Thierry BRETON : Nous passons toujours plus de temps à interagir en ligne sur de nombreux appareils connectés. Les produits et services à destination des consommateurs ou des entreprises sont de plus en plus personnalisés, gourmands en données et sensibles au contexte. Parallèlement, **la confiance devient désintermédiée et transactionnelle** alors même que les objets interagissent directement entre eux et avec les utilisateurs en générant des flux de données de valeur.
Cependant, malgré la croissance exponentielle de nombreux développements de base dans les applications technologiques les plus innovantes, **le rythme du changement n'est pas toujours prévisible** : le progrès est hétérogène et peut même, dans certains cas, conduire à des impasses.
Parfois, **la combinaison de certaines compétences émergentes permet le développement d'innovations** telles que les véhicules entièrement autonomes, les diagnostics médicaux informatisés, les modifications génétiques ou les assistants virtuels intelligents. Dans d'autres cas, **des préoccupations autour du respect de la vie privée ou l'éthique ralentissent, voire font reculer la mise en œuvre de certaines technologies.**
Telles des ondulations à la surface d'un lac, les « ondes de choc digitales » émaneront de différentes sources et interagiront entre elles créant ainsi un environnement complexe et incertain…[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

---

Réagissez à cet article

Source : *Comment les « ondes de choc digitales » vont intensifier la concurrence dans tous les secteurs | Thierry Breton | Pulse | LinkedIn*

En 2016, les ransomwares sous Android ont augmenté de plus de 50%

	En 2016, les ransomwares sous Android ont augmenté de plus de 50%

Basé sur sa technologie LiveGrid®, ESET® publie un rapport sur les menaces Android™ : sur l'ensemble des logiciels malveillants détectés en 2016, la catégorie ransomware a augmenté de plus de 50% par rapport à 2015, le plus fort taux de menaces enregistré.

« Au total, nous avons constaté **une augmentation de près de 20% des logiciels malveillants** (tous confondus) **sous Android en un an.** Sur cette plateforme, les ransomwares sont ceux qui se sont le plus développés. Selon le FBI (1), cette menace aurait rapporté jusqu'à 1 milliard de dollars aux cybercriminels l'année dernière. Avec une forte augmentation au cours du premier semestre 2016, nous pensons que cette menace ne disparaîtra pas de sitôt », déclare Juraj MALCHO, Chief Technology Officer chez ESET et qui abordera ce sujet lors du Mobile World Congress 2017.

Au cours des 12 derniers mois, **les cybercriminels ont reproduit des techniques identiques à celles utilisées pour la conception de malwares infectant des ordinateurs**, afin de concevoir leurs propres logiciels malveillants sur Android : écran de verrouillage, cyrpto-ransomwares… Ainsi, ils ont réussi à développer des méthodes sophistiquées permettant de cibler uniquement les utilisateurs des différentes versions de cette plateforme.
En plus d'utiliser des techniques d'intimidation comme le « Police ransomware (2) », les cybercriminels chiffrent et cachent la charge utile malveillante sous l'application compromise, afin de rendre sa présence indétectable.
D'après les observations d'ESET, les ransomwares sous Android se concentraient sur l'Europe de l'EST puis sur les Etats-Unis en 2015, avant de migrer vers le continent asiatique en 2016. « Ces résultats montrent la vitesse de propagation de cette menace, active à l'échelle mondiale », ajoute Juraj MALCHO.

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

---

=

Réagissez à cet article

Source : *Boîte de réception (252) – denis.jacopini@gmail.com – Gmail*

De nouveaux malwares super furtifs se cachent dans la mémoire des serveurs

	De nouveaux malwares super furtifs se cachent dans la mémoire des serveurs

Kaspersky met en évidence une souche malveillante qui se cache dans la mémoire des systèmes et exploite des applications de confiance pour dérober des données. 10 organisations au moins en ont été victimes en France.

Une nouvelle espèce de logiciels malveillants, mise en évidence par Kaspersky Lab, ressemble bien à un cauchemar pour administrateurs système et responsables informatiques. Il s'agit d'une forme de malware utilisant des logiciels légitimes (comme l'outil de tests de pénétration Meterpreter) pour infecter un système, avant de détourner des services Windows couramment utilisés pour assurer son implémentation et son fonctionnement. Une fois le malware en cours d'exécution à l'intérieur de Windows, il efface toute trace de son existence et réside dans la mémoire du serveur. Le temps d'exfiltrer des informations qu'il convoite avant de s'effacer de lui-même.
Parce que ces nouveaux malwares, que Kaspersky a baptisés MEM: Trojan.win32.cometer et MEM: Trojan.win32.metasploit, résident en mémoire, ils ne peuvent pas être détectés par des antivirus standards, qui analysent le disque dur d'un ordinateur. En outre, le malware se cache en réalité à l'intérieur d'autres applications, ce qui le rend pratiquement invisible également des outils utilisant des techniques de listes blanches, comme c'est le cas de nombreux pare-feu.

Le redémarrage efface toute trace

Selon un billet de Kaspersky sur le blog Securelist, le processus fonctionne en plaçant temporairement un utilitaire d'installation sur le disque dur de l'ordinateur. C'est ce petit outil qui loge le logiciel malveillant directement en mémoire en utilisant un fichier MSI standard de Windows avant d'effacer l'utilitaire. Une fois que le malware commence à collecter les données ciblées, il emploie une adresse de port inhabituelle (:4444) comme voie d'exfiltration.
L'ensemble de ces caractéristiques rendent ces malwares très furtifs. Car ils n'existent que dans la mémoire d'un ordinateur, ce qui signifie qu'un logiciel anti-malware n'a une chance d'identifier l'infection que lors d'une analyse de ladite mémoire, et uniquement pendant que le malware est toujours actif. Le redémarrage de l'ordinateur effacera toute trace, rendant inutile toute analyse 'forensic'.

PowerShell détourné

Kurt Baumgartner, chercheur au sein des Kaspersky Lab, explique que ses équipes de recherche ont d'abord trouvé ce logiciel malveillant dans une banque en Russie. L'équipe a pu accéder au serveur, dans ce cas un contrôleur de domaine, avant que le système ne redémarre, ce qui leur a permis d'isoler la souche infectieuse. L'équipe de Kaspersky a alors constaté que les attaquants utilisaient un script PowerShell pour installer un service malveillant dans la base de registre de l'ordinateur.
Selon le chercheur, si ce malware furtif échappera aux antivirus qui cherchent des signatures sur le disque dur d'un ordinateur, il peut toujours être découvert via des logiciels de protection qui traqueront ses activités suspectes : création de tunnels de communication chiffrée pour exfiltrer les données, démarrage de services ou lancement de l'activité PowerShell. Kurt Baumgartner assure que ses équipes suivent l'évolution du malware – qui devrait muter pour échapper aux défenses qui vont être mises en œuvre suite à la publication de Kaspersky – et qu'il convient notamment de surveiller la diffusion de données à partir de lieux différents sur le réseau utilisant le tunnel de communication caractéristique de la souche.

La France, second pays ciblé

Et de conseiller aux équipes de sécurité de scruter les journaux système et de surveiller le trafic sortant du réseau. Tout en précisant qu'il vaut mieux stocker ces données hors ligne de sorte que le logiciel malveillant ne puisse pas trouver et effacer ces preuves. Autre astuce pour contrarier les assaillants : désactiver PowerShell. Une solution radicale mais parfois difficile à mettre en œuvre, de nombreux administrateurs ayant recours à cet utilitaire…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : Anatomie du malware super furtif, caché dans la mémoire des serveurs

---

Le fonctionnement d’Internet ne tient qu’à (presque) un fil

L'imaginaire populaire associe souvent Internet aux satellites, mais 99,8 % du trafic intercontinental passe par les 366 câbles sous-marins répartis sur la planète. « Grâce à la fibre optique, les capacités de ces câbles sont des millions de fois supérieures à ce que nous savons faire avec les satellites ».
Rien n'est plus facile que de couper Internet : il suffit de sectionner des câbles. Ils sont simplement enterrés, voire posés sur le fond des océans.

La câbles sous marins ont pris une importance prépondérante pour l'acheminement des connexions internet. Se sont des ressources de plus en plus essentielles et toutes perturbations provoqueraient de très importantes conséquences.
Selon le New York Times les Russes joueraient actuellement avec les nerfs des autorités américaines en laissant des navires très proches de ces câbles sous-marins et n'hésitant pas à frôler ces derniers… Or, il faut savoir que non seulement ces câbles sont très difficile à protégés du fait de leur longueur de plusieurs milliers de kilomètres mais aussi bizarre que cela puisse paraitre, aucune loi maritime n'interdit de s'en approcher, la navigation était libre dans les eaux internationales.
D'après le même journal, la coupure d'un de ces câbles rendrait les liaisons intercontinentales quasiment impossibles dans les fait tant les ressources sont très utilisées avec des possibilité de re-routage très limité dans les faits.
Ultra-rapides puisqu'ils évitent la perte de temps induite par la durée nécessaire pour effectuer une transmission par satellite mais pourtant vulnérables, ces câbles se retrouvent parfois à 1 ou 3 mètres sous le fond à proximité des côtés et au large, touchent le fond des océans. Pas suffisant hélas aujourd'hui pour se mettre à l'abri des menaces humaines et naturelles : Requins, tremblements de terre, bateaux et pêcheurs véreux coupant parfois des kilomètres de câbles pour les revendre comme en 2007 au Vietnam.
En 2015, c'est une ancre qui fût à l'origine d'une section de câble privant presque toute l'Algérie d'Internet pendant deux semaines. Tout comme en Égypte en 2008 (perte immédiate de 70% de sa capacité de connexion à internet).

Actuellement, 99,8% du trafic internet intercontinental transite via 366 câbles sous-marins soit plus d'un million de kilomètres de câbles à fibre optique parsemant le fond des océans. Une fois en surface, ils sont rattachés à des stations d 'atterrissement. Ces dernières sont d'ailleurs elles aussi assujetties aux menaces. « En cas de conflit militaire, si plusieurs câbles sont sabotés,nous risquons rapidement une saturation de notre accès à Internet» s'inquiète Jean-Luc Vuillemin.
Heureusement, des systèmes de secours existent comme le principe de redondance. 01net l'a vulgarisé parfaitement dans ses lignes il y a quelques années : « Les câbles transatlantiques rejoignent eux la Bretagne et la Normandie. Pour garantir les transmissions sous-marines dans les deux sens, plusieurs sécurités sont prévues. Le câble lui-même comporte deux paires de fibres optiques au lieu d'une. Le doublage suffit pour résoudre les problèmes électroniques, comme la panne d'un multiplexeur ou d'un routeur, la plus courante. Chaque opérateur crée ensuite des redondances du réseau en posant plusieurs câbles distants sur chaque liaison desservie. Celle entre la France et les Etats-Unis se répartit entre sept câbles, directs ou transitant par le Royaume-Uni. »
Enfin, certains ont trouvé une alternative au sabotage physique des câbles, les services de renseignements de certains pays avec leurs mouchards placées eux-aussi au fond de l'eau.

Facebook et Microsoft main dans la main
En mai 2016, Facebook et Microsoft ont annoncé la construction en duo d'un câble sous-marin à fibres optiques, qui traversera l'océan Atlantique pour relier Virginia Beach aux USA jusqu'à Bilbao en Espagne.

Le général Keith B. Alexander, chef du Cyber Command veut un deuxième Internet aux Etats-Unis
Pour certains, la cyberguerre est un sujet de scénario de films de science fiction ; pour d'autres, c'est la réalité de la guerre contemporaine.
Dans un entretien avec plusieurs journalistes, dont rend compte cette semaine le New York Times, le général Alexander propose la création d'un réseau Internet distinct de celui qui existe aujourd'hui, afin de sécuriser le réseau électrique américain, considéré comme le maillon faible de la sécurité des Etats-Unis.
Cette proposition d'une ampleur considérable, financièrement et techniquement, est lancée publiquement par le général en anticipation d'une remise à plat de tous les enjeux stratégiques liés à Internet par la Maison Blanche d'ici à janvier. Elle fait partie d'un exercice classique aux Etats-Unis de lobby public en faveur d'arbitrages budgétaires par chaque branche de l'appareil militaire, mais pas seulement.

Des « bombes logiques » dans le réseau électrique
Le réseau électrique américain actuel utilise les réseaux Internet et se révèle donc particulièrement vulnérable. C'est la thèse développée au début de l'année par Richard A. Clarke, un ancien responsable de la Sécurité de l'administration Clinton, dans un livre coécrit avec Robert K. Knake, intitulé « Cyber War : The Next Threat to National Security and What to do About It » (« Cyber guerre : la prochaine menace à la sécurité nationale et ce qu'il faut faire »).
Clarke affirme que les services américains ont découvert dans le réseau électrique américain des « bombes logiques » chinoises. Une « bombe logique », c'est comme un virus informatique, dormant, qui peut se déclencher à distance et des années plus tard si nécessaire. Ces « bombes » auraient pu être introduites par une faille dans le réseau internet utilisé par les producteurs et distributeurs d'électricité.

Dans son livre, Richard A. Clarke utilise cette découverte pour plaider en faveur d'un réseau internet séparé pour les installations vitales des Etats-Unis (comme le montre le schéma ci-dessus).
En effet, selon lui, la vulnérabilité du Net américain peut potentiellement mettre les Etats-Unis à genoux en peu de temps en cas de cyber-attaque, privant le pays d'électricité, de transports, de services d'urgence, et affaiblissant même sa capacité de défense.
L'ancien conseiller de Bill Clinton se livre même à un exercice de simulation de cyberguerre avec la Chine, avec des étudiants, basé sur un scénario étrangement similaire à un sujet de tension entre Washington et Pékin il y a quelques mois, peu après la sortie du livre.
Il imagine ainsi une crise entre la Chine et le Vietnam sur la souveraineté d'îles riches en hydrocarbures dans la mer de Chine, et un engagement de Washington au côté du Vietnam. Ça ne vous rappelle rien ? C'est ce qui s'est produit l'été dernier, sur le plan diplomatique uniquement…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : « Qui a le savoir, a le pouvoir »: Les câbles sous-marins, le maillon faible de la cyberguerre

---

Une puce RFID sous la peau. Des salariés volontaires l'ont essayé…

Une puce RFID sous la peau. Des salariés volontaires l'ont essayé…

Une entreprise belge a implanté une puce RFID sous la peau de huit de ses salariés volontaires. Rencontre.

Accepteriez-vous de vous faire pucer pour le boulot ?
C'est ce qu'ont consenti huit des douze salariés d'une agence digitale belge, comme avant eux une entreprise suédoise : mi-décembre, au milieu de leur petit open space blanc et rouge, un pierceur néerlandais leur a logé sous la peau, entre la base du pouce et l'index, une puce RFID (radio frequency identification).
L'une de celles que l'on implante habituellement sous le poil des animaux de compagnie ou des brebis.
Sa silhouette sombre, longue comme un grain de riz, apparaît à travers la chair quand l'un des salariés pucés serre le poing pour nous la montrer.
Comme il l'a fait devant d'autres journalistes avant nous, Tim Pauwels se plie allègrement à la démonstration : sur le trottoir de Malines, ville grise entre Bruxelles et Anvers où l'entreprise est située, il colle avec délicatesse sa main sous l'interphone. Bip!
Miracle tant attendu : la porte s'ouvre. Nous entrons.

« Adoptons la technologie »

L'idée de se faire implanter une puce pour ouvrir la porte de leur boîte leur est venue un vendredi. A l'instar des si cool entreprises de la Silicon Valley, les salariés de Newfusion ont chaque semaine « deux heures de libre » dédiées à la cogitation de projets.
Parce que certains oubliaient régulièrement leur clé, ils ont lancé un vendredi le projet de les remplacer par un système électronique de badges. « Plus facile, plus digital », précise dans un anglais fluide Vincent Nys, 27 ans, qui a lancé NewFusion il y a quatre ans.
« On a passé deux jours dessus, on l'a mis en place mais quelques jours plus tard, ils oubliaient leur carte. Alors on a réfléchi : « quelle est la prochaine étape ? » Nous voulions faire quelque chose d'innovant et ouvrir une discussion. »

Une puce RFID et l'un des kits commandés par Newfusion (Emilie Brouze)
En parfaite adéquation avec son époque, Vincent Nys adore l'innovation (il répète le mot à l'envi). Les milliers de personnes dans le monde qui possèdent une puce électronique se divisent à son sens en deux catégories. Ceux qui le font pour se différencier – « être unique, spécial » – et les consommateurs précoces, « comme nous ». Ceux qui n'ont pas peur de se dire :

« Adoptons la technologie et allons plus loin. »
Son associé complète :
« Ceux qui avancent sont ceux qui ouvrent les portes aux autres… Il faut innover pour pouvoir faire des progrès. »
Innovons donc en ouvrant des portes.

« Est-ce qu'on le sent ? »

Avant de commander les puces à une entreprise américaine qui les commercialise en kits stérilisés, il y a tout de même eu discussion au sein de Newfusion. « On a eu un débat, mais pas celui qu'il y a dans les médias », rétorque Vincent Nys :
« Est-ce que c'est sûr ? Est-ce qu'il y a des implications médicales ? Est-ce qu'on pourra passer un scanner ? Est-ce qu'on le sent ? Est-ce que ça à un impact sur notre vie ? »
Seulement quatre salariés ont refusé de se faire pucer. « Je ne perds pas mon badge, je n'ai pas vu l'intérêt d'une puce », répond Sam Van Campenhout, développeur.
« Je crois que je n'aimerais pas avoir quelque chose sous ma peau. C'est bizarre », ajoute Sil Colson, jeune designer multimédia.

Sil Colson fait partie des salariés ayant refusé de s'implanter une puce RFID (Emilie Brouze)

Ce qui pourrait la faire changer d'avis ? Que la puce contienne son passeport et qu'il suffise de présenter sa main au moment des contrôles, sans risquer d'oublier ou d'égarer le document en vacances. Ou que la puce contienne les infos essentielles de son carnet médical, immédiatement accessible en cas d'urgence. Pour ouvrir la porte d'entrée, Sil préfère conserver son badge.
Un autre développeur raconte que lui a tout de suite été enthousiaste à l'idée (sa copine un peu moins) : « J'adore la technologie. »
En quelques heures, il a bidouillé un programme que le patron lui demande de nous montrer. Alors Dries Van Craen presse sa main droite contre un boîtier relié à son ordinateur. Bip! (La sonorité est la même qu'à la caisse d'un supermarché.)
S'affiche sur l'écran, sur un fond automnal, un message de bienvenue personnalisé. Sur la colonne de droite sont empilés ses morceaux de musique préférés, au-dessus des temps de transport pour rentrer chez lui, actualisés en temps réel.
Le patron s'enthousiasme :
« Voilà ce que tu peux faire sans argent et en une demi-journée. Avec des années et une vision, on pourra faire plein de choses. »
Le jeune patron technophile a installé chez lui un système lui permettant d'ouvrir la porte de son domicile d'un geste de la main.
Prochaine étape : bricoler un moyen de régler son éclairage intérieur grâce à la même puce (un jeu de lumières pour ses soirées en solitaire, un autre quand il est avec sa compagne).

« Disrupter » le marché

Quand on lui fait remarquer l'utilité à ce stade toute relative de ces puces sous-cutanées, Vincent Nys assume. Parce qu'il ne s'agit pas que de se débarrasser des badges d'entrée : c'est une piste de développement pour Newfusion.
« Dans nos têtes, on ne s'est même pas demandé ce qu'on pouvait faire avec [les puces RFID]. On s'est dit « Allons-y, faisons-le ». On ne s'est pas trop préoccupé de questions éthiques, morales et des possibles applications.
On pense qu'il faut être les premiers à le faire. On commence par « disrupter » le marché, puis on créé des applications. «
Sur la RTBF, qui a diffusé l'un des premiers reportages sur l'opération de puçage, Alexis Deswaef, président de la ligue des Droits de l'Homme en Belgique, soulevait une question éthique : « Dans le futur, braderons-nous un peu plus nos droits à la vie privée pour plus de sécurité ou de confort ? »
En dépit des critiques, Vincent Nys, comme son associé, sont ravis des retombées médiatiques, eux qui espéraient intéresser seulement quelques blogs techs avec leur communiqué de presse : on parle d'eux dans le monde entier. Quelle bonne pub ! Des banques, une société de transports publics ou encore une municipalité ont d'ores et déjà pris contact avec eux.

« Big Brother »

A côté de ces potentiels nouveaux clients, Newfusion a aussi reçu une cinquantaine de messages désagréables. « Des gens qui faisaient référence aux années Hitler – parce qu'on marquait les gens -, des personnes qui nous traitaient d'antéchrist ou nous parlent de Big Brother… » Beaucoup d'après lui n'ont pas bien compris la technologie.
Vincent Nys fait défiler certains commentaires Facebook sur son téléphone : « Ce n'est pas éthique », « 0% liberté », « il est temps que je lise de nouveau « 1984 » »… Il remarque :
« Ils sont tous fixés sur ce livre. »

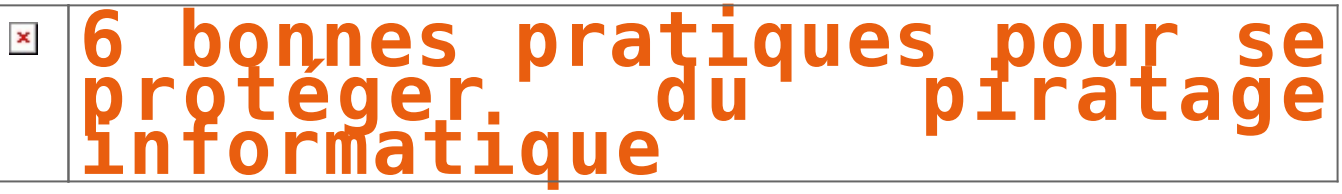
Vincent Nys, fondateur et directeur de Newfusion, le 9 février 2017 à Malines (Emilie Brouze)
Au début, le patron répondait poliment et pédagogiquement à ceux qui ne sont manifestement pas mûrs pour "aller plus loin" : non, non, non, il ne s'agit pas de traquer les gens. La puce RFID qu'il a lui aussi sous la peau fonctionne sans batterie et ne peut pas transmettre à un tiers la localisation du porteur.
Elle contient un numéro unique ainsi qu'un espace mémoire lui permettant par exemple d'enregistrer sa carte de visite pour la donner à un client en posant sa main sur son smartphone.
Alors oui, le patron peut savoir exactement quand un des employés pucés entre ou sort du bâtiment, « comme avec les badges ou la caméra fixée à l'extérieur », semble-t-il relativiser. « Mais ce n'est pas le but et ce n'est pas notre culture. Les employés ont des horaires de travail souples. »…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : Travailleurs belges pucés : « On ne s’est pas trop préoccupé de questions éthiques » – L’Obs

---

6 bonnes pratiques pour se protéger du piratage informatique



Par manque de temps ou de ressources, les PME négligent le risque de piratage informatique. Quelques règles de bon sens suffisent pourtant à écarter en partie les menaces.

Perdre ses données suite à une attaque informatique peut avoir de lourdes conséquences pour une start-up ou une PME. L'entreprise peut même ne jamais s'en relever. Piratage de site Internet, clé USB piégée, vol de mot de passe, programme espion caché dans des pièces jointes… Les cyber menaces sont de plus en plus fréquentes. Quelles sont les règles simples pour s'en protéger ? Le point avec Stéphane Dahan, président de Securiview, entreprise spécialisée dans le management de la sécurité informatique.

#1 : Identifier les données les plus sensibles

« *Faites preuve d'une saine paranoïa*, affirme Stéphane Dahan. *C'est-à-dire sachez définir précisément quelles sont les informations à protéger dans l'entreprise* ». Inutile donc de mettre des barrières partout sans discernement. Quelle que soit leur forme (mail, papier, fichier), posez vous donc la question : quelles sont les données les plus sensibles et quelle est la probabilité qu'on me les vole ? « *Ensuite, il faut les localiser. Messagerie, Dropbox, téléphone, autant de pistes de fuite possible pour des informations qui ont de la valeur.* »

#2 : Mettre à jour les systèmes et sauvegarder

« *Ne pas oubliez de mettre à jour régulièrement ses antivirus et ses systèmes d'information. On voit trop souvent des entreprises négliger cet aspect* », soutient Stéphane Dahan. N'oubliez pas non plus de **sauvegarder périodiquement vos dossiers stratégiques**. « *Idéalement, ils doivent être stockés à plusieurs endroits. Si un serveur brûle, que vous soyez capable de les retrouver ailleurs* ».

#3 : Assurer la confidentialité des données clés

A l'intérieur de l'entreprise, assurez-vous que seuls les salariés ayant besoin des informations sensibles puissent y accéder. Par exemple, que les mots de passe ou clés de chiffrement ne soient **attribués qu'aux personnes qui ont besoin de les connaître**.

#4 : Définir et faire appliquer la politique de mot de passe

Attention dans le choix des mots de passe ! C'est trop souvent le talon d'Achille des systèmes d'information. « *Eviter de choisir les plus bateau comme abc123 ou 12345, une mauvaise habitude plus courante qu'on ne le dit* », insiste Stéphane Dahan. Idéalement, fixez des règles de choix et de dimensionnement des mots de passe et **renouveler ces derniers régulièrement**.

#5 : Protéger les terminaux mobiles

Les postes mobiles sont des points d'accès potentiels pour des pirates informatiques. Selon l'ANSSI (Agence nationale de la sécurité des systèmes d'information), ils doivent bénéficier au moins des mêmes mesures de sécurité que les postes fixes. Même si cela représente une contrainte supplémentaire, les conditions d'utilisation des terminaux nomades imposent même le renforcement de certaines fonctions de sécurité.

#6 : Sensibiliser l'équipe au risque de piratage

Périodiquement, rappelez à votre équipe quelques règles élémentaires : ne pas divulguer des mots de passe à un tiers, ne pas contourner les dispositifs de sécurité internes, éviter d'ouvrir la pièce jointe d'un message venant d'une adresse inconnue, etc. La sensibilisation doit également porter sur **l'utilisation des réseaux sociaux**. « *Les comptes Facebook ou Linkedin des collaborateurs sont des mines d'informations pour les pirates*, explique Stéphane Dahan. *Ils s'en servent pour adresser des messages très personnalisés qui vont leur permettre d'entrer dans le système d'information de l'entreprise.* »…[lire la suite]

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

Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en 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 : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l’article mis en page : 6 bonnes pratiques pour se protéger du piratage informatique, Marketing et Vente – Les Echos Business

---

Comment faire face au risque de Cyberattaques sur les infrastructures énergétiques ?

Comment faire face au risque de Cyberattaques sur les infrastructures énergétiques ?

Cette étude analyse les risques de cyberattaques sur des infrastructures énergétiques européennes, ainsi que leurs potentielles conséquences, notamment sur les réseaux électriques. Elle offre également une approche comparative des mesures prises par différents pays d'Europe afin de protéger leur industrie et collaborer à l'échelle de l'Union européenne.

La digitalisation de l'industrie énergétique permet de révolutionner les processus de production, de stockage, de transport et de consommation d'énergie. Nos infrastructures énergétiques, conçues il y a plusieurs décennies et prévues pour demeurer fonctionnelles pour de nombreuses années encore, côtoient désormais des équipements numériques avec lesquels elles interagissent au quotidien. Ces évolutions, qui sont aujourd'hui un gage de disponibilité, d'efficacité et de réactivité sur toute la chaîne de valeur énergétique, ouvrent pourtant la voie à un type de menace qui jusqu'en 2010 avait relativement épargné cette industrie : les cyberattaques.

Le nombre et la technicité des attaques ont augmenté après les dégâts causés par le virus Stuxnet au sein du complexe d'enrichissement nucléaire iranien de Natanz, bien que cette attaque demeure la plus sophistiquée observée à ce jour. Et s'il y a une réelle prise de conscience des enjeux dans le secteur énergétique, les risques persistent. Les politiques de transition énergétique et les efforts d'intégration des énergies renouvelables ne feront que renforcer cette tendance tant que la cybersécurité ne fait pas partie de la réflexion sur l'avenir du système énergétique.

La réglementation tente de s'adapter, notamment en France où les autorités collaborent étroitement avec les entreprises de l'énergie pour faire émerger un cadre réglementaire contraignant, et protéger les Opérateurs d'Importance Vitale (OIV). Cette démarche inspire également d'autres pays d'Europe, mais des mesures communes à toute l'Union européenne sont à prendre rapidement afin de garantir la sécurité de nos réseaux énergétiques, fortement interconnectés.

LIRE L'ETUDE (PDF)

Original de l'article mis en page : Cyberattaques et systèmes énergétiques: faire face au risque | IFRI – Institut français des relations internationales

---

Réagissez à cet article

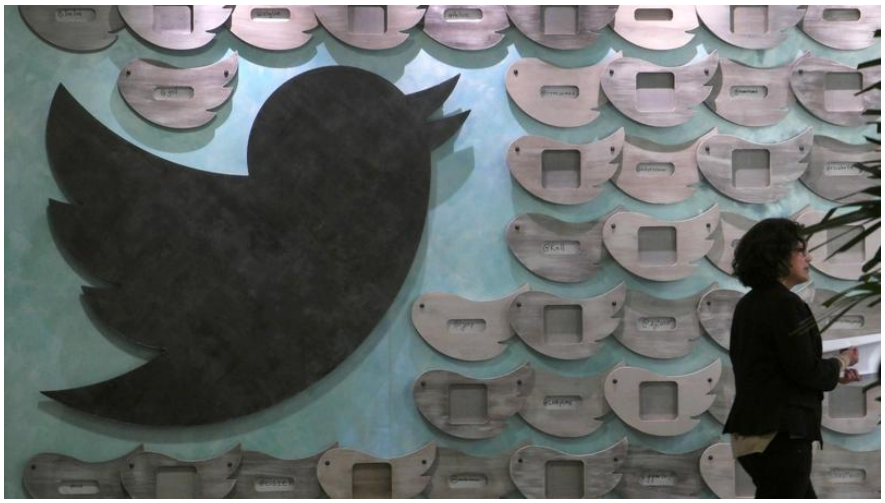
La liste des zones interdites à la photographie aérienne est publique

Non, il n’est pas interdit de voler en France ni de prendre des photos aériennes. En revanche, la réglementation encadre strictement l’usage d’un drone et un nouvel arrêté publié le 27 janvier 2017 fixe la liste des zones interdites à la prise de vue aérienne.…[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.

Réagissez à cet article

Twitter s'appuie sur l'intelligence artificielle pour lutter contre le harcèlement



Twitter s'appuie sur l'intelligence artificielle pour lutter contre le harcèlement

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.…[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.

Réagissez à cet article