Une faille de sécurité de Hacking Team a été utilisée par un important groupe de pirates | Le Net Expert Informatique

Une faille de sécurité de Hacking Team a été utilisée par un important groupe de pirates

Des groupes de pirates informatiques ont utilisé, peu après leur publication, le contenu des fichiers volés à l'entreprise Hacking Team pour se livrer à des tentatives de piratage, révèle l'entreprise de sécurité Kaspersky. Selon Kaspersky, le groupe « Darkhotel », notamment, a utilisé des vulnérabilités qui avaient été employées par Hacking Team, une entreprise spécialisée dans la vente de logiciels de surveillance.

« Darkhotel » s'est notamment signalé par le passé pour avoir utilisé des méthodes élaborées pour placer des logiciels espions – par exemple en prenant le contrôle des réseaux wifi utilisés dans de grands hôtels. Parmi ses cibles figurent des dirigeants de très grandes entreprises, dans la chimie, les cosmétiques ou la pharmacie, des militaires et des responsables d'ONG, dans plusieurs pays d'Europe, d'Asie et d'Afrique, toujours selon Kaspersky. Des cibles et un niveau de sophistication qui laissent supposer à Kaspersky qu'il s'agit d'un groupe étatique ou soutenu par un Etat.
Hacking Team, société italienne à la réputation sulfureuse, est spécialisée dans la vente de logiciels espions et de dispositifs de surveillance électronique. L'intégralité des données de l'entreprise a été publiée en ligne après un piratage, y compris le contenu des messageries de la société. Des associations et des élus européens ont demandé l'ouverture d'une enquête sur les pratiques commerciales de la société, soupçonnée d'avoir notamment vendu des logiciels au Soudan, et une réforme de la législation sur l'exportation de ces technologies.

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.lemonde.fr/pixels/article/2015/08/10/une-faille-de-securite-de-hacking-team-a-ete-utilisee-par-un-important-groupe-de-pirates_4719735_4408996.html

Démonstrations de piratages au salon de «hackers» de Las Vegas | Le Net Expert Informatique

Démonstrations de piratages au salon de «hackers» de Las Vegas

Des pirates informatiques ont fait aussi bien que la bande de George Clooney dans Ocean's eleven en arrivant samedi, lors d'un salon à Las Vegas, à ouvrir un coffre-fort et à tromper la vigilance des caméras de surveillance sans être repérés.

La réalité a fini par dépasser la fiction. Eric Van Albert et Zach Banks, deux chercheurs en informatique, ont fait dans la vraie vie ce que Hollywood a déjà accompli à moult reprises. Ils ont détourné le flux vidéo de caméras de sécurité pour injecter à la place leurs propres images et ainsi tromper la vigilance des surveillants en leur faisant croire que tout était normal. En général, au cinéma, c'est là que les cambrioleurs en profitent pour amasser leur butin et s'enfuir ni vu ni connu. Dans les faits, il ne s'agit que d'une simple démonstration, réalisée à l'occasion de la Def Conf, un célèbre salon de «hackers» à Las Vegas.
«Nous avons mis sur pied notre dispositif en restant le plus fidèle possible à ce qui se fait dans les films», a déclaré Eric Van Albert. «Nous voulions voir à quel point ce type d'attaque était plausible», a-t-il ajouté. Lui et son acolyte ont dépensé environ 500 dollars pour fabriquer l'outil qui permet de pénétrer le câble reliant les caméras aux écrans des gardiens. Le flux est ensuite passé à la moulinette d'un programme informatique qui restitue des images inoffensives.

Ouvrir un coffre-fort avec une clef USB
Les deux chercheurs pourraient s'associer avec Daniel Petro et Oscar Salazar de Bishop Fox, une entreprise de sécurité informatique qui a réussi à ouvrir un coffre-fort avec une clé USB. Le coffre n'était pas une boîte en métal épais «toute bête» mais était équipé pour compter les billets et créditer les comptes de dépositaires par internet. Les deux hommes ont indiqué qu'ils avaient choisi la prise USB parce qu'elle leur permettait d'utiliser un ordinateur plus puissant pour ouvrir le coffre. Mais Daniel Petro a souligné que, de toute façon, il fallait accéder physiquement au coffre pour pouvoir en retirer l'argent.
Pour éviter que ce scénario hollywoodien ne se répète, les deux hommes ont prévenu la compagnie qui fabrique les coffres-forts, et qui a déjà trouvé une parade à ce type d'attaque.

Source : http://www.lefigaro.fr/secteur/high-tech/2015/08/09/32001-20150809ARTFIG00158-des-hackers-s-inspirent-de-hollywood-pour-piller-des-coffres-forts.php

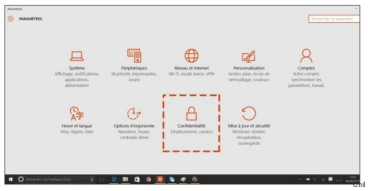
Vie privée et données personnelles sous Windows 10 : les astuces de la Cnil pour vous protéger | Le Net Expert Informatique

Vie privée et données personnelles sous Windows 10 : les astuces de la Cnil pour vous protéger

La Commission nationale de l'informatique et des libertés (Cnil) a diffusé lundi 10 août un communiqué pour aider les utilisateurs du flambant neuf Windows 10 à protéger leurs données personnelles.

Au cœur d'une polémique depuis l'adoption d'une nouvelle politique sur la collecte des données privées, le dernier système d'exploitation de Microsoft s'est vu attaqué ces derniers jours par des utilisateurs mais aussi par Marine Le Pen qui dénonçait « l'espionnage généralisé des ordinateurs des Français ».
La présidente du FN avait d'ailleurs interpellé la Cnil « pour analyser les conséquences de Windows 10 sur la vie privée des Français » et demandé des mesures « afin que Microsoft se conforme à la loi française sur la protection de la vie privée. »
Rien de tel pour l'heure mais l'organisme propose à défaut la série de réglages ci-dessous pour « limiter la communication de vos informations à l'éditeur et à ses partenaires. »

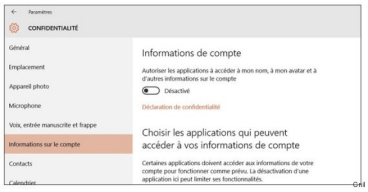
• Cliquez sur le logo Windows en bas à gauche puis sur » Paramètres « . Sélectionnez alors le menu » confidentialité » où vous pourrez modifier les principales fonctionnalités qui collectent des données :



Cnil

• Pour limiter le plus l'envoi de vos données, vous pouvez systématiquement tout désactiver.

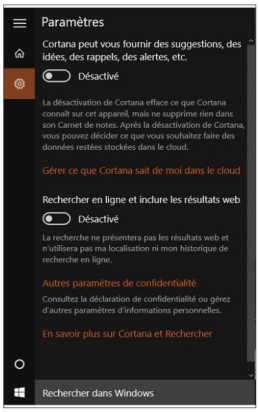
• Par défaut la géo-localisation de votre poste est activée. Il est recommandé de la désactiver depuis l'onglet » Emplacement « .



Cnil

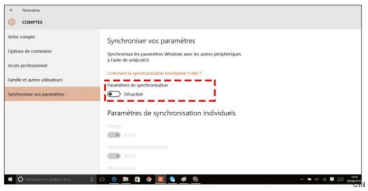
• Vous pouvez désactiver complètement la collecte de données ou empêcher certaines applications d'y accéder. Notamment pour l'Appareil photo, le Microphone, les Informations de Compte, les Contacts, lu Calendrier, la Messagerie, les communications Radio et la synchronisation avec les Autres appareils.

• Cortana, l'assistante embarquée dans Windows 10, a besoin d'accéder à plusieurs types d'informations pour fonctionnet. Vous pouvez désactiver Cortana soit en cliquant sur l'icone de Cortana (le cercle) soit directement depuis la barre des taches, soit depuis le menu démarrer. En cliquant sur le livre puis sur » Paramètres » de Cortana.



Cnil

• Si vous disposez d'un compte connecté qui synchronise vos paramètres entre les différents terminaux équipés de Windows 10, vous pouvez désactiver cette synchronisation (et la collecte des données associées), en allant dans la fenêtre de » Paramètres » et en cliquant sur » Comptes « .



Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.huffingtonpost.fr/2015/08/10/vie-privee-donnees-personnelles-windows-10-astuces-cnil_n_7965788.html

Boeing planche sur des drones capables de déployer des logiciels espions | Le Net Expert Informatique

Boeing planche sur des drones capables de déployer des logiciels espions

Le spécialiste de l'aéronautique Boeing travaille sur la production de drones capables d'infecter les ordinateurs et smartphones aux alentours.

En début de mois, nous apprenions que la société milanaise Hacking Team, qui propose des outils d'interception des communications entre internautes aux gouvernements ou aux pouvoirs publics, avait elle-même été hackée. Quelque 400 gigaoctets de données confidentielles ont été récupérés révélant la nature des relations entre Hacking Team et ses partenaires. Ces documents sont mis à disposition sur le site Wikileaks.
Parmi les informations révélées, la filiale Insitu de Boeing, spécialisée dans la production de drones, avait signé un partenariat avec Hacking Team afin de procéder à des hacks à distance. L'appareil serait ainsi en mesure de cibler un smartphone ou un ordinateur portable en particulier puis de l'infiltrer via un réseau Wi-Fi.
Selon le magazine The Intercept, qui rapporte l'information, le drone en question est prévu pour pouvoir accéder aux fichiers à distance, récupérer le journal des appels, l'historique des messageries instantanées ou encore les emails.
Au sein des emails aspirés sur les serveurs de Hacking team, nous trouvons notamment une feuille de route datant du mois de juin. Celle-ci fait mention d'un petit appareil pouvant être transporté par un drone et capable de récupérer les données transitant via les réseaux.
Le document explique que l'attaque devra prendre en charge Windows 10 ainsi que le navigateur Microsoft Edge et Skype Web. Sur OS X, Hacking Team a finalisé un dispositif scannant les sauvegardes locales d'iTunes et planchait sur la capture des certificats d'iCloud et des images de l'application Photos.
Retrouvez tous les détails de ce projet en italien sur cette page.

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.clubic.com/antivirus-securite-informatique/virus-hacker-piratage/spyware-logiciel-espion/actualite-774222-boeing-planche-drones-capables-deployer-spyware.html

Un drone mis au point contre les incendies de forêt | La foire du drone | Le Net Expert Informatique

	Un drone mis au point contre les incendies de forêt

Le drone est moins cher, plus souple d'utilisation qu'un hélicoptère et, souvent, moins dangereux. Ces arguments font déja mouche dans l'audiovisuel, la supervision agricole, la surveillance des ouvrages d'art mais aussi sur le terrain du maintien de l'ordre puisque la gendarmerie va se doter, dans ce but, d'une flotte d'une vingtaine de petits appareils sans pilote, selon Le Parisien.

Les drones pourraient, demain, également changer la donne dans le domaine de la sécurité civile, plus particulièrement en matière de prévention et de lutte contre les incendies de forêt.

Conçu par la société catalane Singular Aircraft, installée à Barcelone et à Malte, le Flyox 1 est un gros hydravion sans pilote. Apparemment, il s'agit du plus imposant drone civil qui existe à l'heure actuelle. Cet engin volant mesure 11,50 mètres de longueur pour 14 mètres d'envergure et pèse 1 750 kilos. Il peut emporter un chargement de deux tonnes, décoller (sur 313 mètres) ou atterrir (209 mètres lui suffisent) sur une piste classique, l'eau ou des marécages. Il peut rester 6 heures et 45 minutes en vol. Flyox 1 – dommage qu'il ait hérité d'un nom qui fleure bon le produit antimoustiques – a réalisé un premier test grandeur nature mi-mai en Islande où il a effectué un vol de 457 kilomètres sans perturber le trafic aérien autour de l'aéroport de Reykjavik.

Singular Aircraft

« Chaque année, environ une centaine de pompiers meurent (…). Flyox 1 souhaite mettre fin à ces statistiques en surveillant les forêts, en détectant de façon précoce les incendies et en les éteignant », affirme l'entreprise. Singular Aircraft assure que son gros hydravion peut larguer un peu plus de deux mille litres d'eau ou de produit retardant. Ses caractéristiques d'aéronef dépourvu de pilote lui permettent de multiplier les passages (ravitaillements compris, il peut fonctionner plus de cinquante heures d'affilée) et les vols nocturnes ne lui posent aucun problème. Cet appareil peut aussi, assurent ses inventeurs, surveiller les frontières et porter assistance ou encore transporter du fret vers des zones inhospitalières et les parachuter.

Eléments du tableau de commande du Flyox (Singular Aircraft)

Apparemment opérationnel au plan technique, le plus dur commence pour Flyox 1. Même si son promoteur fait valoir que son coût d'utilisation est très largement avantageux – mais ne fournit pas vraiment de données chiffrées –, ce drone-hydravion à très large rayon d'action risque fort de représenter un coût d'acquisition très élevé pour les collectivités. Il devra donc faire la démonstration de son efficacité, ce qui passe sans doute par la capacité de ne pas cantonner chaque appareil à un seul type d'usage. Sur ce terrain des gros drones civils, la concurrence ne manque pas. A commencer par celle des grands groupes déjà présents sur le secteur du drone militaire.

Source : http://drones.blog.lemonde.fr/2015/07/19/un-drone-mis-au-point-contre-les-incendies-de-foret/

Augmentation de la taille moyenne d’attaques DDoS | iTPro.fr | Le Net Expert Informatique

Augmentation de la taille moyenne d’attaques DDoS

Arbor Networks, spécialiste de la protection contre les attaques DDoS, publie ses statistiques relatives aux attaques DDoS pour ce second trimestre.

Tant en bits par seconde qu'en paquets par seconde, il semblerait que les attaques de type DDoS soient de plus en plus imposantes. L'attaque la plus forte de ce second trimestre de type « UDP Flood » a atteint 196 bits/s. Le problème réside surtout dans le fait que cette amplitude n'est plus aussi rare qu'auparavant.Au deuxième trimestre, 21 % d'entre elles ont dépassé 1 Gbit/s, la progression la plus forte enregistrée étant celle dans la fourchette des 2 à 10 Gbit/s. Le mois de juin a aussi été marqué par l'augmentation des attaques entre 50 et 100 Gbit/s principalement de type « SYN Flood » ciblant le Canada et les Etats-Unis.
Darren Anstee, directeur des technologies de sécurité pour Arbor Networks explique que« si les attaques d'une ampleur extrême monopolisent les gros titres, c'est la progression de la taille moyenne des attaques DDoS qui inquiète les entreprises à travers le monde. Les entreprises doivent définir clairement leur risque en matière de DDoS. Face à des attaques moyennes capables de saturer l'accès Internet de bon nombre d'entreprises, il est essentiel de saisir les risques et les coûts d'une attaque et de mettre en place les plans, services et solutions appropriés. »
Du côté des attaques par amplification et réflexion, il semblerait que celles exploitant SSDP soient en baisse puisque 84 000 ont été détectées au second trimestre contre 126 000 au deuxième. Cependant, la taille moyenne des attaques d'amplification par réflexion DNS, NTP, SSDP et Chargen a augmenté au deuxième trimestre 2015 et 50 % de ce type d'attaques ciblaient le port UDP 80 (HTTP/U) pour une durée de 20 minutes (contre 19 pour le premier). A noter que ce type d'attaque permet d'amplifier la volumétrie du trafic par un nombre de réponses envoyé plus important tout en masquant les sources. Cette technique exploite notamment le manque de mesures mises en place par les opérateurs pour filtrer le trafic et la mauvaise configuration d'équipement fournissant des services UDP.

Source : http://www.itpro.fr/n/augmentation-taille-moyenne-dattaques-ddos-21404/

Une Jeep quitte la route suite à son piratage par deux hackers | Le Net Expert Informatique

Une Jeep quitte la route suite à son piratage par deux hackers

Charlie Miller et Chris Valasek, deux experts en sécurité ont piraté une automobile à distance et pris le contrôle de plusieurs de ses fonctions, dont les freins, grâce à une faille du système Uconnect du fabricant Fiat Chrysler.

Le logiciel et l'électronique sont de plus en plus présents dans les véhicules. Mais, les constructeurs doivent sans doute encore renforcer leur expertise dans le domaine du logiciel et aussi de la sécurité informatique.
Ce n'est pas la première fois que des experts en sécurité démontrent des vulnérabilités dans les moyens de transports. Les deux chercheurs Charlie Miller et Chris Valasek en ont fait une nouvelle démonstration avec un journaliste de Wired, Andy Greenberg.

Un patch à déployer manuellement, sur chaque voiture
Les deux hackers ont profité d'une faille du système de bord Uconnect, déployé dans nombre de voitures connectées du constructeur Fiat Chrysler et permettant de communiquer avec le véhicule depuis un smartphone.
Le fabricant n'avait certainement pas pensé aux actions réalisées par Miller et Valasek. Ces derniers ont donc pu se connecter à distance à la voiture, grâce à son adresse IP, et en prendre le contrôle : freiner ou couper les freins, déclencher les essuie-glaces pour gêner le conducteur, éteindre le moteur…
D'après Wired, qui a publié un article sur la prise de contrôle de la voiture, la faille de Uconnect affecte plusieurs modèles de véhicules de 2013 et 2014 du constructeur, parmi lesquels les Jeep, Dodge Ram et Dodge Viper.
Fiat Chrysler, le fabricant, était informé et a diffusé un correctif de sécurité la semaine dernière, un petit mois avant la présentation des deux chercheurs en sécurité prévue à la Black Hat. Problème : le patch doit être installé manuellement, ce qui impose aux propriétaires des véhicules concernés de se rendre chez leur garagiste agréé.

VIDÉO – Pour une expérience, deux chercheurs américains sont parvenus à pirater une Jeep à distance, tandis qu'elle roulait sur une autoroute. Chysler a produit un correctif.

C'est une vidéo très angoissante que vient de publier Wired. On y voit un des journalistes du magazine spécialisé, Andy Greenberg, rouler à plus de 100 kilomètres par heure sur une autoroute du Missouri, dans une Jeep Cherokee récente. Sans qu'il n'actionne aucun bouton, les ventilateurs s'activent au niveau maximum. Il poursuit sa conduite, tandis que sa radio se met en route et diffuse du hip-hop à un niveau sonore dont il n'est pas coutumier. Une minute plus tard, son réservoir de liquide lave-vitres se vide et ses essuie-glaces battent la mesure. Il ne voit plus grand-chose. Mais un problème plus important arrive. La transmission de son véhicule est coupée, la Jeep ralentit. Pendant une longue minute, durant laquelle il craint de se faire emboutir par un semi-remorque, Andy Greenberg ne peut rien faire.

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.zdnet.fr/actualites/deux-hackers-piratent-une-jeep-et-lui-font-quitter-la-route-39822718.htm

Hacking Team a travaillé sur un drone capable d'infecter des ordinateurs à distance | Le Net Expert Informatique

Hacking Team a travaillé sur un drone capable d'infecter des ordinateurs à distance

De nouvelles informations émergent des centaines de milliers d'e-mails piratés au fabricant de logiciels espions Hacking Team. Des échanges ont montré que l'entreprise italienne a été contactée par Insitu, un fabricant de drones appartenant à Boeing, pour travailler sur un système qui permettrait aux engins de pirater des réseaux Wi-Fi à distance, a relevé le site The Intercept.

Un rapport daté du 1er juillet montre d'ailleurs qu'Hacking Team travaillait sur un système d'injection réseau utilisable par drone, c'est-à-dire « un équipement conçu pour insérer du code malicieux dans les communications d'un réseau Wi-Fi », explique le site spécialisé Ars Technica.

« Nous ne pouvons vendre nos produits qu'à des entités gouvernementales »

Selon un premier e-mail envoyé en avril, Insitu s'est montré intéressé par une présentation de Hacking Team à l'IDEX 2015, un salon de la défense qui s'est tenu aux Emirats arabes unis en février. « Nous aimerions potentiellement intégrer votre système de piratage de Wi-Fi à un système aérien et nous souhaiterions prendre contact avec un de vos ingénieurs qui pourrait nous expliquer, plus en détail, les capacités de l'outil, notamment la taille, le poids et les spécifications de votre système Galileo [un logiciel espion] », écrit alors Giuseppe Venneri, ingénieur mécanique en formation chez Insitu.

« Gardez à l'esprit que nous ne pouvons vendre nos produits qu'à des entités gouvernementales », répond un responsable de Hacking Team, sans fermer la porte à une collaboration. Selon un e-mail interne, le même responsable de Hacking Team indique qu'Insitu travaille avec des agences gouvernementales et demande quels produits seraient les plus adaptés à la demande du fabricant.

Aucun accord trouvé

La correspondance entre Insitu et Hacking Team s'est arrêtée en mai et a été fortement retardée par des discussions d'ordre légal, chaque entreprise souhaitant utiliser son propre accord de non-divulgation avant de démarrer les discussions commerciales. Les courriels les plus récents suggèrent que les négociations n'ont jamais commencé.

Le vendeur de logiciels espions italien Hacking Team est sous pression depuis un piratage qui a conduit à la publication de plus de 400 gigabits de données confidentielles début juillet. Certains documents indiquent notamment que l'entreprise pourrait avoir vendu des solutions de surveillance à des pays sous embargo comme le Soudan et la Russie.

Source : http://www.lemonde.fr/pixels/article/2015/07/20/hacking-team-a-travaille-sur-un-drone-capable-d-infecter-des-ordinateurs-a-distance_4691260_4408996.html
Par Florian Reynaud

Norauto inaugure la « révision connectée » grâce au boîtier Xee | Le Net Expert Informatique

Norauto inaugure la « révision connectée » grâce au boîtier Xee

Les clients Norauto pourront, bientôt, se laisser installer un boîtier connecté dans leur auto. Le but : leur fournir des informations, des services, et les alerter de la prochaine révision.

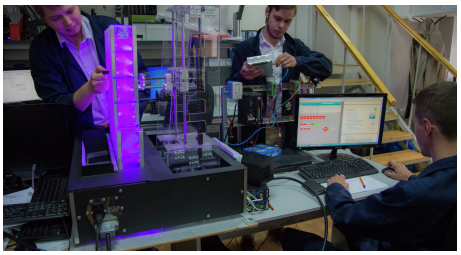
En associant son application mobile, lancée en 2013, au boîtier connecté Xee, Norauto se dit désormais prêt à proposer un service d'un nouveau genre : la « révision connectée ». Alors que l'appli se limitait jusqu'alors au suivi des entretiens auto, elle sera bientôt capable de signaler aux automobilistes lorsqu'il est temps d'aller à la révision. Pour cela, l'enseigne équipera les voitures d'un petit appareil sur la prise diagnostic (OBD).
Fabriqué par la société lilloise Eliocity depuis l'automne 2014, Xee – concurrent des solutions Automatic ou Drust – a plusieurs fonctionnalités : localiser l'auto grâce à sa puce GPS, envoyer un SOS en cas de problème, déclencher une alerte s'il y a une effraction, aider à améliorer la conduite en observant le comportement du conducteur, et en lui prodiguant des conseils sur l'application (changements de rapports…), et d'autres.
Grâce à la connaissance du kilométrage en temps réel, l'application préviendra des révisions à venir, comme c'est déjà le cas dans certains véhicules haut de gamme. L'avantage pour le client est qu'aucune modification du véhicule n'est nécessaire pour le rendre compatible. La « révision connectée » sera dans un premier temps testée auprès d'un panel d'utilisateurs, afin de la peaufiner. Elle sera aussi limitée aux possesseurs d'iPhone.

L'ambition de Norauto, grâce à Xee, est de personnaliser sa relation client
À terme, l'application sera étendue à tous les automobilistes possédant un véhicule produit après 2000 – le plus susceptible d'embarquer une prise OBD – ainsi qu'à l'écosystème Android. Dans la mesure où Eliocity propose une plateforme ouverte aux développeurs, il est probable que de nouveaux services viennent enrichir l'application. Car la révision connectée n'est qu'une première étape. Plus tard, Norauto voudrait remonter davantage d'information de chaque véhicule, afin de personnaliser sa relation. Et attirer dans ses centres.

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://pro.clubic.com/actualite-e-business/actualite-774146-norauto-inaugure-revision-connectee-boitier-xee.html
Par Thomas Pontiroli

Un nouveau système russe contre les cyberattaques industrielles | Le Net Expert Informatique



© PHOTO. INSTITUT D'INGÉNIERIE PHYSIQUE DE MOSCOU

Un nouveau système russe contre les cyberattaques industrielles

L'Université nationale de recherche nucléaire MePhI a conçu un système informatique baptisé Bouclier pour protéger les installations automatiques des entreprises industrielles contre les attaques cybernétiques.

Le système informatique « Bouclier » conçu par les spécialistes de l'Université nationale de recherche nucléaire MePhI pourra être utilisé pour protéger les installations automatiques des entreprises industrielles contre les attaques cybernétiques.
Il sera vendu aux pays membres du groupe des Brics, a déclaré le directeur adjoint du centre d'ingénierie de MePhI (MIFI en russe) Konstantin Mejankov dans une interview accordée à l'hebdomadaire de l'Académie des sciences de Russie Poïsk (Recherche).

La Russie présente une caméra médicale inédite
La protection des systèmes automatisés de contrôle des processus technologiques contre les cyberattaques est considérée comme l'un des principaux problèmes de l'industrie contemporaine. De telles attaques peuvent affecter la chaîne industrielle des entreprises et provoquer des accidents sur les sites, voire des catastrophes anthropiques. Les spécialistes du monde entier cherchent des moyens permettant d'améliorer la protection de l'automation industrielle.
« Les diplômés de la faculté de cybernétique et de la sécurité informatique, ainsi que le Centre de sécurité cybernétique ont participé à ce travail du MePhI. Ils ont créé ensemble le Bouclier qui protège l'automation industrielle de l'accès extérieur non autorisé et des attaques de piratage ou de subversion », explique Konstantin Mejankov.

La Russie relance sa production d'aimants haut de gamme
Il a ajouté que ce système pourrait également être installé sur les oléoducs pour contrôler l'acheminement des hydrocarbures ou encore constater l'apparition de coupures et de fuites.
Le groupe russe InfoWatch, spécialisé dans la sécurité informatique, lance aujourd'hui la vente du système Bouclier aussi bien en Russie qu'à l'étranger, notamment dans les Brics, déclare Konstantin Mejankov. « Par ailleurs, il faut savoir que ce système ne peut pas être transporté dans une boîte et être simplement branché – nos spécialistes se rendent chez chaque client pour diagnostiquer tous les systèmes de l'installation et proposer une solution personnalisée », conclut-il.

Source : http://fr.sputniknews.com/sci_tech/20150718/1017098784.html