L’attaque par impulsions électromagnétiques des réseaux ferroviaires | Le Net Expert Informatique

L’attaque par impulsions électromagnétiques des réseaux ferroviaires

De nouveaux capteurs pour faire face aux attaques EM dans le secteur ferroviaire

Virginie Deniau, coordinatrice du projet SECRET, discute des dispositifs mis au point par son équipe afin d'identifier les attaques par impulsions électromagnétiques (EM) et permettre aux opérateurs de passer à un mode sûr.
Il y a onze ans, l'attentat du métro de Madrid a prouvé que le système de sécurité ferroviaire européen n'était pas assez efficace. Mais aujourd'hui où l'équipement ferroviaire (comme dans la plupart des autres industries) est de plus en plus normalisé et connecté, entre autres, un autre type d'attaque plus insidieuse est devenue plus probable: les attaques par impulsions électromagnétiques (EM). Un projet financé par l'UE a mis au point des technologies de détection permettant au secteur de faire face à cette nouvelle menace.
Saviez-vous que bientôt il y aura autant d'appareils connectés que d'êtres humains sur Terre? Cinq milliards de ces appareils sont actuellement opérationnels et ce nombre devrait atteindre les 25 milliards d'ici 2020. Évidemment, chaque nouveau type d'appareil connecté nous rapproche de l'aube des villes intelligentes et de leurs bénéfices attendus. Mais d'un autre côté, comme le montrent les récentes actualités, les pirates informatiques et autres passionnés par la technologie animés de mauvaises intentions représentent une menace croissante pour la sécurité.
Dans le secteur ferroviaire européen par exemple, l'homogénéisation des technologies de réseau et l'utilisation accrue des communications sans fil a rendu très probable le scénario d'une attaque EM. Les brouilleurs de communication sont faciles à utiliser et aisément accessibles à tous grâce à Internet, autrement dit les communications pourraient éventuellement être brouillées, pour notamment provoquer des retards, un blocage ou une déviation des trains.
Pour permettre au secteur de faire face à cette nouvelle menace, le projet SECRET (SECurity of Railways against Electromagnetic aTtacks) a développé un ensemble de sondes de détection capables d'identifier des attaques EM lorsqu'elles surviennent, afin que les opérateurs des équipements ferroviaires puissent passer le réseau à un « mode sûr » inviolable par le type spécifique de l'attaque EM utilisé.
Virginie Deniau, coordinatrice de SECRET, discute la probabilité du scénario d'attaque par impulsions EM, des dispositifs mis au point par son équipe et de la façon dont le secteur aura bientôt besoin de s'adapter à cette nouvelle réalité.

Quelles sont les chances d'un scénario d'attaque EM?
La définition d'une attaque par impulsions EM évolue parallèlement à la multitude des applications de technologies de communication sans fil. Par le passé, les attaques EM découlaient de la production d'interférences à haute tension (Electromagnetic pulse ou micro-ondes haute tension) intentionnelles capables de perturber ou d'endommager l'équipement électronique. Aujourd'hui, ces équipements peuvent être enclenchés par une commande ou une information transmise par des liens sans fil, autrement dit, il est désormais plus facile de perturber les informations transmises et d'endommager l'équipement. Ces attaques nécessitent un signal moins puissant qui peut être généré par des appareils mobiles et autres dispositifs discrets.
Ainsi, d'un point de vue technologique, la probabilité d'une attaque augmente proportionnellement à la vulnérabilité des infrastructures. Il est cependant difficile d'établir une nette probabilité car aujourd'hui il est impossible de faire la distinction entre un défaut technique et une attaque EM. Les attaques EM par un signal de puissance relativement « faible » impliquent des perturbations mais aucun dégât permanent.

Vous avez mentionné les dispositifs mobiles. Cela signifie-t-il que n'importe qui est capable d'effectuer de telles attaques?
La connaissance de la cible est essentielle si l'on veut définir les moyens nécessaires pour effectuer une attaque EM. De nos jours, les brouilleurs de communications publiques peuvent être facilement achetés mais leur puissance et action sont restreintes.
Maintenant, si nous prenons en compte les services de communication professionnels ou de sécurité, il faut des dispositifs spécifiques pour ce genre d'attaques. Ces appareils sont habituellement limités au marché professionnel ou doivent être conçus à partir de zéro. Mais cela nécessite un certain niveau d'aptitudes et de connaissances.
Néanmoins, lorsque ces applications professionnelles sont soutenues par des services publics sans fil, elles peuvent être perturbées par des brouilleurs communs. Cela peut donc poser de nombreux problèmes, et la sécurité et l'importance des services sans fil doivent être sérieusement prises en compte.

SECRET se concentre sur la sécurité ferroviaire. Quelles pourraient-être les conséquences des attaques EM dans ce secteur?
Le principal risque direct est la perturbation du trafic ferroviaire. Il serait possible d'empêcher le départ des trains, de forcer les arrêts de train mais cela provoquerait d'importantes pertes financières et des situations ingérables. Cependant, il est difficile d'évaluer précisément les risques en cascade qui dépendent des caractéristiques de chaque réseau ferroviaire (exploitation, infrastructure, applications, etc.).

Pouvez-vous nous en dire davantage sur les outils que vous avez développés?
La vision de SECRET est que si on est capable de détecter une attaque EM avec certitude, nous pouvons alors tenter de passer à un mode de sécurité ferroviaire parfaitement adapté à la situation et permettant aux opérateurs de regagner le contrôle. Le défi consiste donc à développer des solutions de détection rapide et fiable. C'est dans cet esprit que de nombreuses solutions ont été étudiées dans le cadre de SECRET. Certaines pourraient être mises en œuvre au sein des terminaux de communication et d'autres nécessiteraient des dispositifs dédiés mais offrent l'avantage de suivre divers canaux de communication.
À des fins de résistance, nos capteurs ont été couplés à un terminal d'acquisition et de décision chargé d'analyser les résultats de ces capteurs de détection et de commander une plateforme de télécommunications reconfigurable. D'après les résultats sortants des capteurs, le terminal de décision dirige les messages à transmettre vers le canal de communication le plus résistant à l'attaque EM. Manifestement, cette approche nécessite le déploiement de nombreux réseaux de communication.

Quand prévoyez-vous la commercialisation de la technologie de SECRET?
En raison de la mobilité et du large spectre d'environnements ferroviaires électromagnétiques, la fiabilité et l'absence totale de défauts des solutions de détection est difficile à démontrer à bord d'un train. Néanmoins, lorsque le train est immobile, les technologies de SECRET peuvent être vraiment efficaces. Nous pouvons donc envisager une commercialisation relativement rapide à l'aide de ces technologies afin de protéger les gares et autres infrastructures cruciales.
Parallèlement, les technologies de SECRET peuvent contribuer à l'évolution des normes de télécommunications employées dans les infrastructures critiques. Au lieu d'améliorer la performance en termes de vitesse de données, les normes peuvent évoluer pour fournir des informations en temps réel quant à la qualité des services ou de la présence des signaux brouilleurs (intentionnels ou non-intentionnels). Elles pourraient ensuite fournir un diagnostic pertinent et activer le processus d'intervention adéquat.

Les voies ferrées européennes font déjà l'objet d'une pression économique et sécuritaire importante. Pensez-vous que le secteur peut soutenir les coûts supplémentaires qu'impliquerait la mise en œuvre de solutions de SECRET?

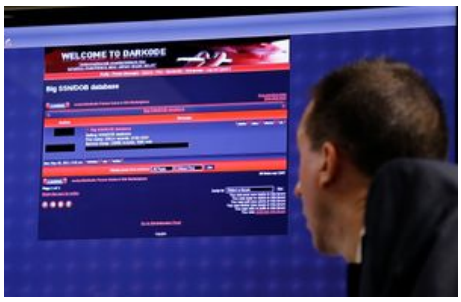
Je pense qu'avec cette menace croissante, il sera nécessaire de garantir la résilience du réseau ferroviaire contre de telles attaques. Habituellement, les systèmes de communication sans fil ne représentent qu'un faible pourcentage du budget d'un projet ferroviaire. Or, ces systèmes sont essentiels dans les plans opérationnels et de sécurité. Les attaques à impulsions EM peuvent avoir des conséquences considérables en termes de coût, et avec un déploiement trop simple, elles peuvent également faire l'objet d'actions malveillantes. Ainsi, une solution contre les attaques EM devrait être envisageant en trouvant un équilibre entre les risques, les impacts et les investissements.

Quels sont vos projets maintenant que le projet touche à sa fin?
Nous aimerions tester notre analyse d'attaques EM avec d'autres types d'attaques telles que les attaques physiques ou les cyber-attaques. En effet, les attaques de brouillage peuvent facilement entraîner d'autres actions malveillantes afin d'empêcher les transmissions vidéo ou d'alarme. Par conséquent, les analyses de risques doivent prendre en compte le risque d'une combinaison d'attaques physiques et de brouillage. Nous pensons également que l'architecture de détection pour les attaques EM proposées dans SECRET devrait être associée à d'autres outils de surveillance de l'infrastructure afin d'obtenir une meilleure vue de ce qui se passe sur le réseau en temps réel.

Pour plus d'informations voir: projet SECRET

Source : http://www.techno-science.net/?onglet=news&news=14158

Le forum de pirates Darkode est tombé après une opération menée par le FBI | Le Net Expert Informatique



Le forum de pirates Darkode est tombé après une opération menée par le FBI

Sous la supervision du FBI , le forum Darkode, qui constituait un point de rendez-vous majeur des pirates pour mener des cyber-attaques, est tombé.

C'est la fin du forum dédié au piratage par lequel il était possible d'acheter, de vendre, de monnayer et de partager des informations ou des outils favorisant des cyber-attaques.
Il a fallu que le FBI s'infiltre dans ce monde underground pour en connaître les coulisses d'administration.
Un accès était uniquement possible par cooptation sous le contrôle des gestionnaires de Darkode : on recensait plusieurs centaines de membres (entre 250 et 300 selon LeMonde.fr).
Mais tout postulant devait démontrer au préalable ses « talents » c'est-à-dire ses capacités à alimenter les ressources malware diffusées via Darkode.
Selon les autorités américaines, des mandats d'arrêt concernant une douzaine de personnes présumées en charge de l'administration de Darkode ont été émis dans trois districts, mais en tout, on évoque 70 membres de Darkode interpellés ou recherchés dans le monde.
Une vingtaine de pays ont été associés à la coupure de ce forum qui entre dans une opération plus large contre la cyber-criminalité baptisée « Shrouded Horizon » : outre les Etats-Unis, on trouve des pays comme l'Australie, le Royaume-Uni, le Brésil, le Canada, la Colombie, la Croatie, le Nigéria, l'Allemagne ou Israël.
« Sur les 800 forums dédié à la criminalité sur Internet, Darkode représentait l'une des plus graves menaces à l'intégrité des données informatiques aux Etats-Unis et dans le monde », déclare David Hickton, procureur fédéral pour le district Ouest de Pennsylvanie, cité dans le communiqué du ministère de la Justice.

A travers le centre anti-cyberciminalité EC3, l'Europe était dans la boucle.
Europol a précisé de son côté que l'opération menée sous la supervision du FBI a abouti à 28 arrestations, 37 perquisitions et un nombre important de saisies de matériel informatique susceptibles d'abriter des preuves et des données pour pousser l'enquête encore plus loin.

Source : http://www.itespresso.fr/darkode-fbi-fait-tomber-forum-ombre-102787.html
Par Philippe Guerrier

Etude d’impacts sur la vie privée : découvrez la méthode | Le Net Expert Informatique

17

La CNIL publie sa méthode pour mener des PIA (Privacy Impact Assessment) pour aider les responsables de traitements dans leur démarche de mise en conformité et les fournisseurs dans la prise en compte de la vie privée dès la conception de leurs produits.

De l'application de bonnes pratiques de sécurité à une véritable mise en conformité
La Loi informatique et libertés (article 34), impose aux responsables de traitement de « prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données ».
Chaque responsable doit donc identifier les risques engendrés par son traitement avant de déterminer les moyens adéquats pour les réduire.
Pour aider les TPE et PME dans cette étude, la CNIL a publié en 2010 un premier guide sécurité. Celui-ci présente sous forme de fiches thématiques les précautions élémentaires à mettre en place pour améliorer la sécurité d'un traitement des données personnelles.
En juin 2012, la CNIL publiait un autre guide de gestion des risques sur la vie privée pour les traitements complexes ou aux risques élevés. Il aidait les responsables de traitements à avoir une vision objective des risques engendrés par leurs traitements, de manière à choisir les mesures de sécurité nécessaires et suffisantes.

Une méthode plus rapide, plus facile à appliquer et plus outillée
Ce guide a été révisé afin d'être plus en phase avec le projet de règlement européen sur la protection des données et les réflexions du G29 sur l'approche par les risques. Il tient aussi compte des retours d'expérience et des améliorations proposées par différents acteurs.
La CNIL propose ainsi une méthode encore plus efficace, qui se compose de deux guides : la démarche méthodologique et l'outillage (modèles et exemples). Ils sont complétés par le guide des bonnes pratiques pour traiter les risques, déjà publié sur le site web de la CNIL.

Un PIA (Privacy Impact Assessment) ou étude d'impacts sur la vie privée (EIVP) repose sur deux piliers :
1.les principes et droits fondamentaux, « non négociables », qui sont fixés par la loi et doivent être respectés. Ils ne peuvent faire l'objet d'aucune modulation, quelles que soient la nature, la gravité et la vraisemblance des risques encourus ;
2.la gestion des risques sur la vie privée des personnes concernées, qui permet de déterminer les mesures techniques et d'organisation appropriées pour protéger les données personnelles.

Pour mettre en oeuvre ces deux piliers, la démarche comprend 4 étapes :
1.étude du contexte : délimiter et décrire les traitements considérés, leur contexte et leurs enjeux ;
2.étude des mesures : identifier les mesures existantes ou prévues (d'une part pour respecter les exigences légales, d'autre part pour traiter les risques sur la vie privée) ;
3.étude des risques : apprécier les risques liés à la sécurité des données et qui pourraient avoir des impacts sur la vie privée des personnes concernées, afin de vérifier qu'ils sont traités de manière proportionnée ;
4.validation : décider de valider la manière dont il est prévu de respecter les exigences légales et de traiter les risques, ou bien refaire une itération des étapes précédentes.

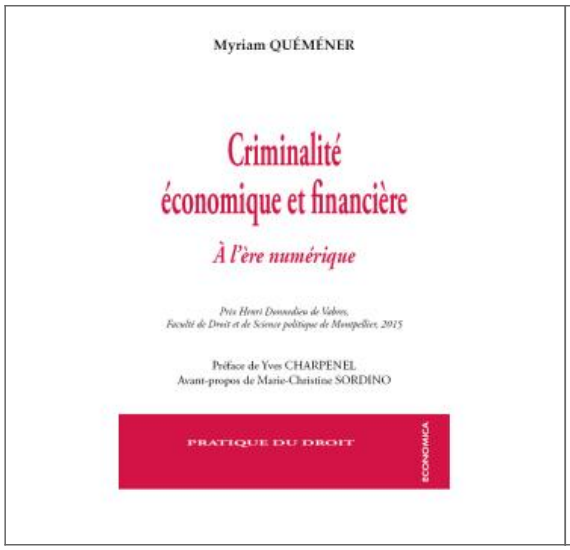
L'application de cette méthode par les entreprises devrait ainsi leur permettre d'assurer une prise en compte optimale de la protection des données personnelles dans le cadre de leurs activités.

PIA, LA MÉTHODE
PIA, L'OUTILLAGE

Source : http://www.newspress.fr/Communique_FR_289793_1332.aspx

---

La criminalité économique et financière à l'ère numérique | Le Net Expert Informatique



La criminalité économique et financière à l'ère numérique

Les banques, les compagnies d'assurances, les sites gouvernementaux, les compagnies pétrolières et, maintenant, l'industrie aéronautique avec la cyberattaque de la compagnie polonaise LOT : le cybercrime cible des secteurs de plus en plus sensibles, sources de dégâts humains majeurs. Au-delà des pertes financières, c'est le cœur du système politique, économique et juridique qui est aujourd'hui menacé par ce fléau.

Que fait l'État, la justice, pour enrayer ces comportements ? Fabriquer des lois en série est-elle « la » solution face à l'existence de cyberparadis, d'une cyberéconomie souterraine de plus en plus puissante, et à la volatilité des preuves ? Le Point.fr a interrogé Myriam Quemener, magistrate, auteur d'un ouvrage de référence sur le sujet : La criminalité économique et financière à l'ère numérique*.

Le Point.fr : « Certaines formes de cybercriminalité sont le fait de réseaux mafieux structurés issus de pays n'ayant pas de législation dédiée à ce phénomène », écrivez-vous. Le décalage entre les législations étatiques est-il surmontable et à quelle échéance ? Que font les autorités françaises en attendant une prise en charge globale et harmonisée de cette délinquance ?
Myriam Quemener : Les pays européens ont harmonisé leurs législations et la coopération internationale se renforce en permanence. La Convention de Budapest, seul traité relatif à la lutte contre la cybercriminalité, a déjà été signée par 46 pays, et d'autres États sont actuellement en négociation pour y adhérer. Pour ce qui concerne la France, notre pays dispose d'un arsenal ancien, en particulier la loi de 1988 dite « loi Godfrain » qui permet de réprimer les piratages informatiques et les cybermenaces. Cet arsenal s'est progressivement enrichi et perfectionné pour permettre le recours à des procédures adaptées à l'univers numérique. De nouvelles structures sont nées, comme l'Anssi, qui met en œuvre la stratégie gouvernementale en matière de cybersécurité, mais aussi une nouvelle sous-direction de lutte contre la cybercriminalité et un pôle numérique au parquet de Paris qui a vocation à s'étoffer. On a aussi créé le procureur de la République financier à compétence nationale exclusive en matière de délits boursiers et pour les affaires économiques et financières complexes qui sont aussi souvent à dimension internationale.

Quels sont les nouveaux moyens d'investigation des enquêteurs pour déjouer les attaques ?
Sur le plan procédural, le législateur a transposé le régime des interceptions téléphoniques à Internet. Il a aussi innové en prévoyant l'infiltration numérique, qui est une enquête sous pseudonyme. Elle permet à l'enquêteur d'utiliser un nom d'emprunt pour entrer plus facilement en contact avec le cyberdélinquant. Depuis la loi du 13 novembre 2014, l'enquête sous pseudonyme jusqu'alors utilisée en matière de pédopornographie et de contrefaçon s'applique à l'ensemble des procédures de criminalité organisée.

Les données personnelles sont considérées comme « l'or noir du XXIe siècle ». La semaine dernière, une importante base de données américaine abritant les coordonnées, données de santé et autres informations personnelles d'environ 20 millions de fonctionnaires a été piratée. Quel usage les cyberdélinquants font-ils des données récupérées, et à quoi peut-on s'attendre dans les années qui viennent ?
Ils récupèrent ces données et les revendent sur les marchés noirs du Web (Darknet) qui sont des réseaux parallèles aux réseaux ouverts du type Google. Cela permet par exemple de faire des achats sous de fausses identités ou d'obtenir des virements en se faisant passer pour une entreprise connue. Les données personnelles servent aussi à créer de faux profils, et tout cela se répercute sur l'e-réputation des entreprises. L'usurpation d'adresses IP (spoofing) qui permet de commettre des fraudes à la téléphonie mobile se développe aussi de manière considérable.

Quels sont les prochains défis de la criminalité astucieuse sur Internet ?
En cette période où le terrorisme frappe de façon dramatique, il est important de s'attaquer avec vigueur au financement du terrorisme, et cette lutte passe par une politique publique pragmatique et déterminée contre des phénomènes comme le cyberblanchiment ou les escroqueries aux faux ordres de virement.
Il faut par ailleurs être attentif et vigilant face à des outils numériques comme le crowdfunding (financement participatif) ou les crédits à la consommation. Les sommes obtenues au travers de ces formes de prêt peuvent en effet servir à financer des activités illicites. Il en est de même du « trading haute fréquence » qui permet d'envoyer des ordres d'achat à une vitesse de l'ordre de la nanoseconde, grâce à des algorithmes superpuissants, permettant des manipulations de cours. Le courtage à haute fréquence a aussi ses dérives : un courtier londonien a récemment été arrêté pour une manipulation sur le marché des contrats à terme électroniques aux États-Unis, qui avait contribué au mini-krach de mai 2010 à Wall Street.
Il faut aussi suivre avec attention le développement de ces fameuses « monnaies virtuelles » qui contournent le système bancaire et permettent d'échapper à tout contrôle étatique en raison de l'absence de traçabilité. Les objets connectés, qui favorisent l'usurpation de profils complets, et le cloud computing qui contient des données sensibles à valeur commerciale sont aussi des cibles potentielles de cyberattaques. D'autant que de nombreuses failles de sécurité existent et peuvent être exploitées par les cybercriminels.

Qu'est-ce qui dissuade vraiment les délinquants, qu'ils soient isolés ou membres d'organisations criminelles ?
La mise en place d'une stratégie globale au niveau des services de l'État est de nature à dissuader les cyberdélinquants, de même que les condamnations et démantèlements de réseaux de cybercriminels qui ne cessent d'augmenter grâce aux moyens d'investigation et à l'expertise de plus en plus pointue des enquêteurs dédiés.

Pensez-vous que l'Internet a démultiplié les risques, ou les a-t-il seulement déplacés ?
L'absence de confrontation physique auteur-victime, propre à Internet, facilite le passage à l'acte. Le système des rencontres virtuelles attire des personnes mal intentionnées qui peuvent plus facilement extorquer de l'argent, notamment via des sites de vente entre particuliers. Aujourd'hui, la cybercriminalité s'industrialise et s'organise sous forme de structures hiérarchisées allant de la main-d'œuvre de base qui récupère des données jusqu'aux têtes de réseau qui donnent les ordres.

Ces phénomènes sont-ils, comme le changement climatique, irréversibles ?
Je ne le pense pas, car, actuellement, il y a une mobilisation importante, du secteur tant public que privé, pour lutter contre ces phénomènes. Il est indispensable de multiplier les actions de formation pluridisciplinaire des acteurs publics et privés qui concourent à la lutte contre ces attaques. Cependant, il ne faut pas perdre de vue que ce type de délinquance lance un défi au temps judiciaire, c'est même une course contre la montre !

L'ouvrage en vente ici

Source : http://www.lepoint.fr/chroniqueurs-du-point/laurence-neuer/cybercrime-un-defi-lance-au-temps-judiciaire-13-07-2015-1943938_56.php

---

| Le Net Expert Informatique

Bercy devra gérer non pas une, mais deux lois numériques | Le Net Expert Informatique

	**Bercy devra gérer non pas une, mais deux lois numériques**

La loi numérique, tout le monde en parle. Même le chef de l'Etat a abordé le sujet lors de l'interview du 14 juillet. Désormais, il semble probable qu'au lieu d'un texte il y en ait deux. Un signé Macron pour la croissance, l'autre signé Axelle Lemaire pour les libertés.

La question revient à chaque fois qu'un journaliste rencontre un responsable gouvernemental proche du dossier. « Où en sommes-nous de la loi numérique dont on parle depuis 2013 ? » La réponse est toujours la même, ou presque : « Nous y travaillons, nous vous tiendrons informé quand nous aurons avancé ». Rien n'est vraiment officiel mais en fait, il n'y aura pas une loi, mais deux. L'une sur la transformation numérique de l'économie, l'autre sur les libertés individuelles.

Lors de la traditionnelle interview du 14 juillet, le chef de l'Etat y a fait une allusion. « Je vais préparer une loi sur le numérique, tout ce qui est activités nouvelles, tout ce qui peut provoquer de l'emploi ». Le message s'adresse clairement à Emmanuel Macron, ministre de l'économie, de l'Industrie et du Numérique.
Dès le lendemain, lors d'un point presse, le ministre est revenu sur le sujet. Sans entrer dans les détails, il a simplement précisé que les premières propositions seront faites au plus tard début 2016. Et pour calmer les impatients, il a prévenu qu'il prendra le temps nécessaire pour l'élaborer. Et en effet l'exercice promet d'être délicat.
Emmanuel Macron est parfaitement conscient du levier que représente le numérique en matière de création d'emploi. Mais il doit composer entre une nouvelle économie qui bouscule les règles des entreprises traditionnelles. Tandis que ces dernières se trouvent, elles, confrontées à une concurrence qu'elles estiment déloyale, voire illégale selon les cas.

Une loi Macron 2 pour la transformation numérique
Dans son message, François Hollande a été plutôt clair: « il faut qu'il n'y ait rien dans nos règles, dans nos formalités qui puisse entraver ». La guerre entre Uber et les taxis est l'un des exemples les plus frappants de la crainte que génère le potentiel des nouvelles technologies. Ce sera donc à Emmanuel Macron de gérer ce dossier dans une loi qui a déjà un nom: Macron 2.
Autres sujets d'importance, les données personnelles et les libertés individuelles face aux géants du Net. Ces sujets devraient faire parti d'un second texte qui sera cette fois sous la responsabilité d'Axelle Lemaire. Le cœur de ce projet devrait donner plus de poids à la Cnil dont le pouvoir, notamment celui de sanctionner, doit être renforcé. En janvier 2015, sa présidente, Isabelle Falque-Pierrotin faisait déjà des propositions sur le contenu du texte.
Mais la présidente de la Cnil est également présidente des Cnil européennes, connues sous le nom de « Groupe de l'article 29 » et dans ce cadre, elle rappelle que le texte devra être compatible avec le projet de règlement européen. « La législation sur les données personnelles ayant une portée économique croissante, les modifications éventuelles ne doivent pas créer de distorsion entre pays de l'Union. » Le cadre est posé. Reste désormais à savoir quand Axelle Lemaire présentera cette loi. Avant ou après celle d'Emmanuel Macron?

Source : http://bfmbusiness.bfmtv.com/entreprise/bercy-devra-gerer-non-pas-une-mais-deux-lois-numeriques-902051.html
Par Pascal Samama

Cyclisme et vol de données – la cyber-criminalité appliquée au sport | Le Net Expert Informatique

Le Tour de France 2015 va-t-il connaître son premier cyber scandale ? C'est en tout cas ce que l'on peut supposer après la divulgation de certaines données de performances du cycliste Crhis Froome qui ont été dérobées, estime Tanguy de Coatpont, directeur général France & Afrique du nord de Kaspersky Lab qui partage son analyse.

« Depuis plusieurs années, le sport connaît un engouement croissant auprès des publicitaires et des entreprises qui y investissent massivement, attirant par conséquent des cybercriminels poussés par l'appât du gain ou une volonté de nuire. Il n'est également pas difficile d'imaginer les conséquences psychologiques que peut avoir un vol de données sur un athlète dont le succès repose en partie sur sa concentration.
Les rumeurs concernant le possible piratage des données sportives de Chris Froome viennent nous rappeler que de nombreux aspects de la vie moderne, y compris le sport de haut niveau, sont de plus en plus connectés. Il y a quelques années, l'idée que les données d'un coureur du Tour de France soient dérobées aurait semblée anecdotique mais avec l'avancée des technologies et l'émergence des solutions d'analyse des performances qui sont aujourd'hui critiques à l'entraînement de nombreux sportifs, ce n'est plus surprenant. Ces sportifs doivent également faire face à une autre réalité : alors qu'ils sont maintenant élevés au rang de célébrités, les informations concernant leurs performances intéressent tout autant que celles qui concernent leur vie privée.
En sachant cela, tout individu ou entreprise doit prendre les mesures qui s'imposent pour protéger ses données informatiques. Même lors d'événements sportifs, où les données doivent être transmises et analysées quasiment en temps réel, il est impératif de prendre en compte les questions de sécurité informatique pour protéger les informations sensibles que sont les performances des athlètes mais également protéger les systèmes sur lesquels elles transitent.
Le partenariat entre Kaspersky Lab et l'écurie de Formule 1 de Ferrari nous a permis de mieux comprendre les défis auxquels ils sont confrontés pour sécuriser les données transmises lors des courses. Pour Ferrari, une solution de sécurité efficace est vitale afin de protéger les données qui sont une source d'information essentielle à l'équipe. Elles transitent très rapidement pour éviter d'être compromises et la solution de sécurité ne doit pas augmenter le temps de latence. Il n'est pas difficile d'imaginer que les contraintes de complexité et de performance sont similaires dans d'autres sports comme le cyclisme professionnel. »

Source : http://www.itrmanager.com/articles/157190/cyclisme-vol-donnees-cyber-criminalite-appliquee-sport.html

La mise en place de la riposte contre la cybercriminalité | Le Net Expert Informatique

La mise en place de la riposte contre la cybercriminalité

Le 08 juillet 2015, c'est-à-dire le mercredi dernier, l'Observateur permanent du Canada au Conseil de l'Europe, Alan Bowman, a déposé l'instrument de ratification de la Convention de Budapest sur la cybercriminalité, faisant ainsi de ce pays le 47ème Etat partie à ce mécanisme international de lutte contre la cybercriminalité.

Au dernier décompte, 07 autres États ont signé la Convention et 12 ont été invités à y adhérer, ce qui porte à 66 le nombre des États Parties ou qui se sont officiellement engagés à devenir Parties au traité.
« La Convention sur la cybercriminalité, aussi connue comme la Convention de Budapest sur la cybercriminalité ou Convention de Budapest, est le premier traité international qui tente d'aborder les crimes informatiques et les crimes dans Internet en harmonisant certaines lois nationales, en améliorant les techniques d'enquêtes et en augmentant la coopération entre les nations. Il a été rédigé par le Conseil de l'Europe avec la participation active d'observateurs délégués du Canada, du Japon et de la Chine.

Qu'est ce que la cybercriminalité ?
À la fin d'août 2011, plusieurs pays européens avaient signé le traité ». Selon une revue de la littérature disponible sur la question, la cybercriminalité reste encore un concept difficile à appréhender. En France, un rapport du groupe de travail interministériel sur la lutte contre la cybercriminalité datant de février 2014 appréhende la question dans toute sa complexité. Au regard de cette complexité, le rapport note que la Commission européenne a du s'en expliquer dans une communication au Parlement européen en date du 22 mai 2007 en ces termes : "Faute d'une définition communément admise de la criminalité dans le cyberespace, les termes 'cybercriminalité', 'criminalité informatique' ou 'criminalité liée à la haute technologie' sont souvent utilisés indifféremment".
La question préoccupe aussi l'OCDE selon laquelle « la cybercriminalité renvoie à tout comportement illégal contraire à l'éthique ou non autorisé qui concerne le traitement automatique de données et/ou de transmissions de données ».

Que dit l'ONU ?
Pour l'organisation mondiale, tombe sous le coup de la cybercriminalité « tout comportement illégal faisant intervenir des opérations électroniques qui visent la sécurité des systèmes informatiques et des données qu'ils traitent ». Pour autant qu'elle offre des outils juridiques susceptibles d'aider les pays à enquêter sur la criminalité informatique et de poursuivre en justice les auteurs de ce crime, la Convention de Budapest est un instrument qui mérite une large vulgarisation surtout en ces temps de guerre asymétrique à l'échelle planétaire.
C'est une simple question de bon sens quand on sait que seule la coopération entre Etats est susceptible de porter un coup d'arrêt à cette nouvelle forme de criminalité aux conséquences imprévisibles. Mais un survol rapide de la liste des Etats parties ou qui s'apprêtent à y adhérer permet de réaliser, là aussi, que l'Afrique est encore à la traine. Alors qu'on arrête de geindre si les autres réfléchissent à notre place et nous imposent leurs quatre volontés.

Source : http://malijet.com/la_societe_malienne_aujourdhui/132840-chronique-du-web-la-riposte-contre-la-cybercriminalite-se-met-en.html

Alerte partagez ! Deux nouvelles failles zero-day dans le plugin Flash d'Adobe | Programmez! | Le Net Expert Informatique

Alerte partagez ! Deux nouvelles failles zero-day dans le plugin Flash d'Adobe

Il y en a des choses intéressantes dans les 400 Go de données récemment dérobées à la société The Hacking Team et publiées sur Pastebin

The Hacking Team est une société qui vit du cyber espionnage, mais qui en l'occurrence contribue pour le moment et à l'insu de son plein gré à la sécurité informatique. En effet le code source de son logiciel espion phare, DaVinci, fait partie des 400 Go volés. Et ce code source est riche d'enseignements.
Ainsi, il est apparu en fin de semaine dernière que DaVinci exploitait une faille zero-day dans le plugin Flash d'Adobe. Faille qu'Adobe a d'ailleurs rapidement corrigée.
Mais ce n'est pas tout. Après cette faille CVE-2015-5119, deux autres failles zero-day ont été identifiées grâce à The Hacking Team CVE-2015-5122 et CVE-2015-512 respectivement. Des failles dans le plugin Flash, encore et toujours… FireEye et Trend Micro détaillent quelques informations techniques à propos de ces failles, sur les pages citées.
Dans les deux cas, les failles consistent en des corruptions mémoire, dont l'exploit rend possible l'exécution d'un code arbitraire sur la machine attaquée. Il s'agit donc de failles hautement critiques, qui pour l'instant ne sont pas corrigées. En attendant les correctifs, les experts en sécurité recommandent très vivement la désactivation du plugin Flash, en raison de la gravité de ces failles.
Lire la suite….

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

Source : http://www.programmez.com/actualites/hacking-hacking-team-deux-nouvelles-failles-zero-day-dans-le-plugin-flash-dadobe-23012

Wi-Fi en avion, où en sommes nous ? | Le Net Expert Informatique

	Wi-Fi en avion, où en sommes nous ?

À l'approche des vacances, nombreux sont ceux qui vont emprunter l'avion pour rejoindre une destination plus ou moins proche. Mais à l'heure où nous aimons être connectés en permanence, il n'est pas facile d'obtenir du Wi-Fi en avion, même si les offres se démocratisent…

Partir chercher le soleil ou le dépaysement à l'autre bout du monde n'est pas donné à tout le monde. Pour ceux qui ont la chance de s'envoler vers d'autres contrées, le voyage est souvent long et ennuyeux, surtout qu'il n'est pas toujours possible de rester connecté « avec le monde d'en bas », là où sont vos amis, vos collègues et tout ce qui fait votre quotidien. Pendant longtemps, les compagnies aériennes étaient formelles : il n'est pas possible d'utiliser Internet en vol, trop compliqué, trop coûteux, trop dangereux ! Bref, il fallait se contenter d'attendre en espérant que rien n'arrive sur la planète réseaux durant les heures de vol. Mais face à une demande toujours plus forte, pour ne pas dire constante, de nombreuses compagnies ont mis en place des offres dédiées à Internet qui permettent, moyennant un supplément plus ou moins important, de voyager connecté.

Y a-t-il un réseau dans l'avion ?

Avant de prendre notre envol, faisons une courte escale pour expliquer la technologie mise en œuvre dans les avions pour y « installer Internet ». Pour l'heure, deux types de connexion sont disponibles, chacune pouvant se suffire à elle-même ou pouvant être combinée avec l'autre. La première consiste à utiliser les antennes relais pour mobiles, que l'on trouve à intervalles réguliers sur la terre ferme. Chaque avion qui passe dans la zone de couverture peut bénéficier du réseau, un équipement particulier intégré à l'avion se chargeant de jouer les entremetteurs. Pour parfaire cette couverture, certaines compagnies ont largement investi dans le déploiement d'antennes terrestres orientées vers le ciel, et donc spécifiquement dédiées aux avions. Quoi qu'il en soit, la limite du système est qu'il ne couvre que les liaisons continentales. En clair, au-dessus de l'eau ne comptez pas dessus.
Heureusement, les satellites sont capables de prendre le relais. Dans ce cas, la position géographique de l'avion n'a aucune influence puisque ce sont les satellites de télécommunication qui se chargent d'apporter un réseau local dans l'avion. C'est la solution exploitée par l'américain Row44 pour connecter les avions, tandis que son compatriote Gogo (anciennement Aircell), qui équipe depuis plusieurs années des centaines d'appareils des compagnies Delta, American Airlines ou Airtran, exploite, lui, le réseau terrestre (limité aux vols internes donc).

Connexion difficile

Face aux progrès de la technologie embarquée, nous sommes en droit de nous demander pourquoi cela semble difficile de fournir un accès dans un avion, dès lors que la technologie extérieure – qui permet à l'avion de se connecter – est active et exploitable. Il y a d'abord une question d'ordre économique. Pour équiper un avion d'un système Wi-Fi, il y a un coût non négligeable qui peut aller de 100 000 dollars pour un réseau terrestre à plus de 500 000 dollars pour les satellites. S'ajoute le temps d'installation qui nécessite une immobilisation de l'appareil qui ne vole pas et donc, ne rapporte rien. Ainsi les spécialistes estiment que la rentabilité d'un tel équipement implique un taux d'utilisation de 20 % au minimum, or, pour l'heure, il se situe généralement (pour les avions équipés) autour des 5 % !
Si nous poussons l'étude un peu plus loin, nous découvrons que les difficultés d'engagement des compagnies dans cette voie sont la conséquence d'une faible utilisation du service lorsqu'il est proposé. Pour prendre le cas des États-Unis, où environ 86 % de la flotte est équipée (toutes compagnies confondues), seuls 8 % des usagers profitent du réseau à bord ! Les raisons de ce désintérêt sont multiples : mauvaise qualité de la connexion, des tarifs jugés trop élevés, et pour certains un besoin de se « couper du reste du monde » le temps du voyage, afin d'en profiter pour se divertir autrement ou se reposer.

Turbulences à 30 000 pieds

Proposer Internet dans un avion n'est pas une idée nouvelle, et c'est ce qui explique que nous ayons aujourd'hui un peu de recul pour constater comment les passagers se comportent lorsque cette option est disponible. Entre 2004 et 2006, la compagnie Lufthansa proposait à ses passagers une connexion haut-débit FlyNet sur certains vols, avant d'y renoncer faute de rentabilité. Nouvelle tentative en décembre 2010, lorsque FlyNet embarque de nouveau à bord de la Lufthansa, avec une nouvelle offre Internet payante. Aujourd'hui, c'est Panasonic qui se charge d'amener le Wi-Fi à bord de la compagnie allemande, avec une offre qui va de 10,95 euros pour une heure jusqu'à 19,95 euros pour 24 heures.

Lufthansa Copyright Creative Commons

L'exemple de Panasonic est assez intéressant au niveau de ce qu'il est nécessaire d'améliorer puisque l'entreprise exploite la bande Ku, idéale au regard du nombre de satellites en activité, mais qui montre rapidement ses limites en termes de débit et de transfert des données. C'est ce qui pousse des sociétés comme Inmarsat et Honeywell à se tourner plutôt vers la bande Ka (connexion de 10 Mo/s), plus rapide et moins onéreuse que l'actuelle bande Ku. « En combinant les capacités de communication par satellite d'Honeywell avec une connectivité mondiale Immarsat XPress, les voyageurs pourront tout faire, des médias sociaux en temps réel, aux vidéo-conférences en passant par des présentations multimédia en vol, pratiquement n'importe où dans le monde, avec une expérience similaire à celle de la maison ou du bureau », assurent Honeywell et Inmarsat dont le réseau Global Xpress est en fonction depuis l'année dernière.

Et pourtant, malgré les embûches et les coûts, les compagnies aériennes ne lâchent pas l'affaire, car si les passagers sont encore peu nombreux à passer à l'acte, ils affirment massivement, dans toutes les études réalisées sur cette question, qu'une fois la partie technique au point et la question des coûts mieux encadrée, l'accès au Wi-Fi en vol est une véritable attente. Comme souvent en matière de technologie, les compagnies doivent donc essuyer les premiers plâtres, accepter de perdre au début (parfois beaucoup) pour mieux rebondir par la suite. Avec 3 milliards de passagers par an, possédant souvent plusieurs appareils connectables (téléphone, tablette, portable), c'est un immense marché qui s'ouvre, à même de justifier les investissements d'avenir qui sont consentis.

Demain le monde

Nous le voyons, la technologie se développe à grands pas et il n'est plus forcément obligatoire de mettre ses appareils mobiles en « mode avion » avant d'embarquer. Mais cette avancée ne doit pas masquer la réalité du bras de fer qui se joue en coulisses. Les compagnies aériennes historiques sont victimes, depuis plusieurs années maintenant, de petits cousins low-cost qui cassent les prix et permettent, sensiblement, de dynamiser le marché. L'accès à Internet, qui impose un investissement très important, pourrait donc devenir un argument commercial de poids, surtout si (comme le promettent les compagnies), les prix ne sont pas exorbitants.

Partant de là, la course entre les géants de l'aviation est bien réelle pour s'assurer du service le plus efficace, pertinent et à même de répondre aux attentes des passagers de toutes les classes, à commencer par ceux de la classe affaire. Depuis 2013, le groupe franco-néerlandais Air France-KLM fait des annonces régulières allant dans le sens d'une connexion prochaine à bord, mais à ce jour le projet semble stagner. À l'automne 2015, de nouveaux tests seront menés sur certains vols, court et moyen-courriers, par le biais d'une connexion payante fournie par Orange. S'ils sont concluants, le service pourrait être étendu à plusieurs appareils.

Et pour vos prochaines vacances ?

Tout cela nous ramène à notre postulat de départ : quid des prochaines vacances ? Aujourd'hui, de nombreuses compagnies proposent des accès au Wi-Fi payants. Il n'y a que quatre compagnies – Norwegian, Qantas, SAS et Turkish Airlines – qui assurent un service « gratuit », sur certains vols, pour une durée parfois limitée (offre de lancement) ou pour certains passagers (classe affaire).

Pour les autres compagnies, il faut compter en moyenne 11 euros de l'heure ou une vingtaine d'euros pour toute la durée du voyage ou 24 heures. Ce site répertorie toutes les offres disponibles en fonction des compagnies, en précisant les modèles d'avions concernés et le fournisseur. À ce jour, on dénombre 25 compagnies aériennes qui fournissent du Wi-Fi sur certains vols.

Enfin, il est important de rappeler que l'aspect technique n'est pas totalement maîtrisé, et que l'expérience en ligne, depuis un avion, reste aléatoire et soumise à des paramètres extérieurs qui peuvent altérer le bon fonctionnement. Mais les possibilités sont bien présentes, et vous pouvez vous tourner vers la compagnie sur laquelle vous comptez voyager afin de savoir ce qu'elle fournit en matière de connexion. Petit à petit, nous nous rapprochons d'un septième ciel connecté, mais le transfert pourrait prendre encore quelques mois avant une arrivée à bon port !

Source : http://www.clubic.com/mag/transports/article-771520-1-avion-wi-fi-point-offres.html?estat_svc=s%3D223023201608%26crmID%3D639453874_1059724550