Alerte de cyberattaques dans les avions | Le Net Expert Informatique

Alerte de cyberattaques dans les avions

L'Agence européenne de sécurité aérienne (AESA) estime que l'aviation est vulnérable et qu'il faut mettre en place des structures dédiées pour lutter contre cette nouvelle menace.

En mai dernier, lorsque le hacker Chris Roberts avait fait les gros titres avec son histoire de piratage d'un avion en plein vol, les compagnies aériennes ont rétorqué en cœur qu'une telle action serait totalement impossible. Elle estimaient que M. Roberts n'était qu'un vantard mythomane. Mais les instances de régulation commencent à voir les choses d'un œil différent, à commencer par celles de l'Union européenne.

Interrogé par l'association des journalistes de la presse aéronautique et spatiale (AJPAE), le directeur exécutif de l'Agence européenne de sécurité aérienne (AESA) Patrick Ky a souligné la vulnérabilité de l'aviation à un éventuel acte de piratage. « C'est un risque auquel il faut qu'on se prépare, l'aviation est vulnérable. Dire que l'aviation n'est pas sujette au cyber-risque, c'est se voiler la face », a-t-il déclaré. Selon le patron de l'agence, il faut mettre en place des « réseaux spécifiques » de spécialistes en cyberattaques pour « informer de la menace et des moyens de s'en prévenir ».

L'AESA fait appel à un hacker

M. Ky a affirmé avoir pu lui-même constater les capacités d'un hacker à pénétrer le réseau de communication d'une compagnie aérienne. « J'ai fait appel à un hacker qui a la particularité d'avoir également une licence de pilote commercial, a-t-il expliqué auprès des Echos. En moins de 5 minutes, il est parvenu à rentrer dans le réseau Acars ». Acars (Aircraft Communication Addressing and Reporting System) est un système de communication et de surveillance par radio basé sur l'échange de messages entre un avion et une station au sol. Il intervient dans la gestion du trafic aérien et permet de s'assurer du bon fonctionnement des équipements de l'aéronef. Mais le hacker ne s'est pas arrêté là. « Il ne lui a fallu que deux ou trois jours pour pénétrer dans le système de contrôle d'un avion au sol. Pour des raisons de sécurité, je ne vous dirai pas comment il a fait », ajoute Patrick Ky.

En décembre dernier, cinq grandes organisations internationales de l'aviation (OACI, ACI, CANSO, IATA et ICCAIA) avaient adopté une feuille de route commune pour harmoniser leurs mesures respectives en matière de cybermenaces, et souligné que « la sécurité et la sûreté du système aéronautique mondial » étaient « potentiellement vulnérables aux attaques de pirates informatiques et autres cybercriminels ».

Denis JACOPINI est Expert Informatique, formateur et chargé de cours à l'Université.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

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

Source :
http://hightech.bfmtv.com/internet/l-europe-sonne-l-alerte-sur-le-risque-de-cyberattaques-dans-les-avions-920964.html
Par Gilbert Kallenborn

Il s’implante une puce NFC dans la main pour pirater des smartphones Android | Le Net Expert Informatique

Glissée sous la peau, la puce NFC devient invisible après que la plaie a cicatrisé. DRPhoto:	**Il s’implante une puce NFC dans la main pour pirater des smartphones Android**

Les pirates ne reculent devant rien pour hacker des téléphones mobiles. Dernière expérience en date : s’implanter une puce NFC dans la main. Rien que ça.

Seth Wahle est un ingénieur pour une société spécialisée dans les technologies sans fil, APA Wireless. A ses heures perdues, ce hacker teste la sécurité de ce type de dispositif. Et ne fait pas dans la demi-mesure : il est parvenu à s’implanter une puce NFC sous la peau de la main, à la jonction entre le pouce et l’index de sa main gauche. De la sorte, il est capable de hacker des smartphones Android rien qu’en les effleurant avec sa paume.

Comment a-t-il fait ?

Le magazine américain Forbes explique qu’il a trouvé une puce NFC que l’on peut implanter sans danger sous la peau d’un être humain. Dotée de seulement 888 bytes de mémoire, elle est encapsulée dans un petit récipient en verre vendu sur un site chinois et qui est usuellement utilisé pour implanter des puces RFID dans le bétail pour le marquer. Pour la somme de 40 dollars (35 dollars), il a ensuite trouvé une personne qui a accepté de lui injecter la puce sous la peau à l’aide d’une seringue spéciale. Ne restait plus ensuite qu’à attendre que la plaie créée cicatrise.

Un simple contact téléphone-main et un programme s’installe discrètement

Avec ce dispositif, Seth Wahle affirme qu’il est désormais capable de hacker n’importe quel smartphone Android doté de la technologie NFC (communication proche par simple contact). Il lui suffit de mettre le téléphone brièvement en contact avec la paume de sa main pour que celui-ci ne se rende sur une page web piratée qui va déclencher le téléchargement d’un petit programme. Et ce, sans alerter les systèmes de sécurité du smartphone.

Une fois celui-ci installé et actif, il est capable de récupérer n’importe quelles données du mobile et même de prendre des photos. Son système n’est pas encore optimal (il perd assez vite la connexion avec le téléphone piraté, notamment quand ce dernier est verrouillé ou redémarré) mais génère déjà de nombreuses questions et craintes pour le futur. Seth Wahle, qui a montré sa performance aux journalistes de Forbes, s’apprête à la présenter plus en détail lors d’une importante conférence de hackers qui se tiendra à Miami du 15 au 17 mai prochain. Nul doute que son intervention sera très suivie…

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l’Université.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source :
http://www.metronews.fr/high-tech/pour-pirater-des-smartphones-android-il-s-implante-une-puce-nfc-dans-la-main/modD!v2YdgmEKKTEuE/

Les PME pourraient être victimes de la remise en cause du Safe Harbor | Le Net Expert Informatique

Les PME pourraient être victimes de la remise en cause du Safe Harbor

Les réactions ont été nombreuses, suite à la décision de la Cour européenne de Justice de remettre en cause l'accord de Safe Harbor entre les Etats-Unis et l'Europe. La France, par exemple, s'en est félicitée. Mais les conséquences restent incertaines. La remise en cause du Safe Harbor, en soi, ne constitue pas une révolution. Cet accord ne faisait que faciliter les transferts de données entre Europe et Etats-Unis : les sociétés américaines pouvaient collecter et exploiter ces données en échange d'une certification annuelle obtenue auprès des autorités américaines. Près de 5.000 entreprises fonctionnaient sous ce régime.

Mais ce n'est pas le seul moyen d'acheminer des données des deux côtés de l'Atlantique. Les entreprises américaines et européennes peuvent signer, entre elles, des clauses contractuelles standards. Elles peuvent aussi obtenir le consentement des utilisateurs, mais ce cas ne fonctionne que pour les entreprises s'adressant aux particuliers, pas aux professionnels. Enfin, elles peuvent demander une autorisation à la Cnil.

D'autres plaintes ?

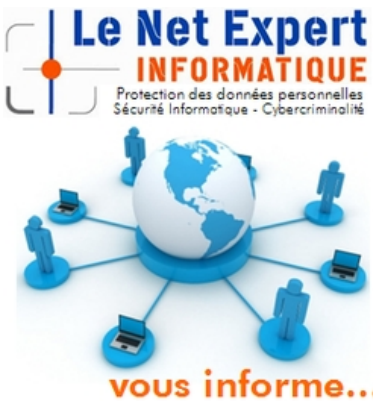
Ces autres possibilités dressent en tout cas, en négatif, le portrait des probables « victimes » de ce nouveau flou : les petites et moyennes entreprises, européennes ou américaines, qui n'ont pas de service juridique fourni en interne pour pouvoir signer des clauses contractuelles ou s'occuper de la question rapidement. « Nous sommes inquiets. Pas forcément pour nous, car tous nos échanges sont régis par des contrats, mais pour les petites entreprises, qui n'ont pas de service juridique ou d'avocats pour s'occuper de ces sujets », confirmait il y a quelques jours Stephen Deadman, directeur adjoint de la vie privée chez Facebook, de passage à Paris.

Le cabinet d'avocats Bryan Cave, de son côté, a déjà reçu plusieurs dizaines de clients inquiets ces jours-ci. « C'est d'autant plus inquiétant que les entreprises françaises ont moins l'habitude, par rapport aux entreprises anglo-saxonnes notamment, de travailler avec des conseillers juridiques, affirme l'avocat Joseph Smallhoover, de Bryan Cave, qui conseille plusieurs sociétés américaines et européennes. Et ce sont ces mêmes PME qui sont le plus créatrices d'emplois. » Et ce n'est sans doute pas fini. « En affirmant que les Etats-Unis n'ont pas un niveau de protection suffisant, la Cour européenne de Justice ouvre aussi la voie à des attaques contre les clauses contractuelles », poursuit Joseph Smallhoover. C'est pour cette raison que les responsables politiques appellent, eux, depuis plusieurs jours, à fournir un nouveau cadre aux transferts de données. La ministre de la Justice Christiane Taubira a estimé vendredi qu'il fallait « aller vite parce qu'on ne peut pas prendre le risque ni d'un vide juridique, ni d'un manque de protection, ni d'un manque de garanties par rapport à la circulation des informations. » Les négociations entre Europe et Etats-Unis pourraient bien s'accélérer.

Denis JACOPINI est Expert Informatique, formateur et chargé de cours à l'Université.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source :
http://www.lesechos.fr/tech-medias/hightech/021393249999-les-pme-pourraient-etre-victimes-de-la-remise-en-cause-du-safe-harbor-1164083.php
Par Nicolas RAULINE

Les 10 ans des Correspondants Informatique et Libertés CIL | Le Net Expert Informatique



Les 10 ans des Correspondants Informatique et Libertés CIL

Le 13 octobre 2015, la CNIL a rassemblé les correspondants Informatique et Libertés (CIL) à l'occasion des dix ans de la fonction. 16300 organismes ont déjà désigné un CIL dont le rôle de pilote de la conformité sera consacré dans le futur règlement européen avec un renforcement de ses missions et moyens.

La convention organisée pour les 10 ans des CIL

A la veille d'un tournant majeur de la réglementation en matière de données personnelles, la CNIL et les CIL ont dressé le bilan des 10 années d'existence de la fonction de CIL. A l'occasion d'un événement organisé le mardi 13 octobre par la CNIL, ils ont échangé sur les bonnes pratiques en matière de conformité et ont envisagé ensemble l'avenir de la profession.

La journée, introduite par la Présidente de la CNIL, Isabelle Falque-Pierrotin, a été ponctuée d'interventions et d'ateliers axés sur la préparation des CIL à un exercice efficace de leurs missions dans un contexte réglementaire renouvelé.

Après la restitution des résultats de l'étude IFOP de juillet 2015 sur la fonction de CIL menée pour la CNIL auprès des correspondants en poste, ont été évoqués les actions, outils, procédures et pratiques contractuelles propres à satisfaire le nouveau principe d' accountability et, plus particulièrement, l'obligation relative à la sécurité des données personnelles à l'heure du tout connecté.

Enfin, un atelier a été consacré aux techniques de valorisation de la conformité auxquelles peut recourir chaque CIL pour installer et pérenniser une culture « Informatique et Libertés » au sein de son organisme.

L'opportunité a été ainsi offerte aux correspondants de partager leurs retours d'expérience et visions opérationnelles sur des sujets désormais incontournables L'objectif a été donc de prendre collectivement une longueur d'avance sur le règlement européen.

CIL aujourd'hui, délégué à la protection des données demain avec le règlement européen

10 ans après sa création, le CIL est devenu un métier clé du paysage de la protection des données personnelles. Cette évolution est consacrée par le projet de règlement européen, qui place les futurs « délégués à la protection des données » (Data Privacy Officers ou DPO) au cœur du prochain dispositif de régulation. Ce texte est actuellement en cours de discussion et devrait être finalisé pour la fin de l'année.

Le projet de règlement prévoit :

• un allègement des formalités préalables à accomplir par les organismes
• un renforcement des droits des personnes concernées,
• une augmentation du montant des sanctions
• la mise en place d'outils et de procédures visant à s'assurer, documenter et ainsi démontrer la prise en compte des principes de protection des données, dans une logique d'engagement responsable (« accountability »).

Dans ce nouveau cadre, la désignation d'un DPO pourrait être rendue obligatoire dans un certain nombre de cas. Son rôle de pilote de la conformité sera consacré au travers d'un renforcement de ses missions et moyens. Il deviendra un véritable « chef d'orchestre » en la matière, chargé :

• de tenir à jour la « documentation Informatique et Libertés »,
• d'informer, de conseiller et de vérifier le respect par l'organisme de ses obligations (en particulier, « privacy by design », études d'impact et notification des violations de données).
• Il sera également le point de contact de l'autorité de régulation, la consultera et coopèrera avec elle si nécessaire.

Qui sont les CIL d'aujourd'hui ?

L'étude IFOP de juillet 2015 menée auprès des CIL sur leur fonction montre que :

53% des CIL font partie du secteur privé et 47% exercent leurs fonctions au sein d'une structure de la sphère publique. La répartition par type d'organisme est la suivante :

• entreprise privée 44%,
• association 9%,
• organisme de sécurité sociale 10%,
• entreprise publique 9%,
• commune 9%,
• établissement de santé 7%,
• Etat 5%,
• EPCI 3%,
• département 2%,
• office HLM 2%,
• région 1%

La quasi-totalité des CIL sont désignés en interne (95%)

Si la plupart des CIL sont issus d'un cursus technique, les profils sont diversifiés :

• 47% sont issus du secteur des TIC/SI,
• 29% occupent ou ont occupé des fonctions juridiques,
• 10% des fonctions administratives
• et 10% des fonctions d'audit ou de conformité.

Les CIL sont principalement rattachés aux instances dirigeantes de leur organismes

• 46% sont rattachés directement au Secrétariat général ou à leur direction générale ou comité exécutif,
• pour 26% ils font partie de la direction informatique
• et 10% de la direction juridique.

Les CIL sont naturellement amenés à collaborer avec de nombreux services qui font appel à leur expertise et à leurs conseils pour la mise en place de traitement de données.

A quoi sert un CIL ?

Pour permettre aux structures publiques et privées d'exercer leur activité tout en protégeant les données personnelles traitées, il est possible depuis l'adoption du décret n° 2005-1309 du 20 octobre 2005 de désigner un CIL et de disposer ainsi d'un précieux acteur de mise en conformité à la loi Informatique et Libertés.

La désignation d'un CIL témoigne également de la part des organismes d'un attachement aux principes de protection de la vie privée, des droits et libertés, et constitue ainsi un facteur de valorisation de l'image de l'organisme.

Cette désignation présente donc plusieurs bénéfices :

Un renforcement de la sécurité juridique : la désignation d'un CIL permet d'identifier un référent sur les questions de protection des données personnelles et s'intègre dans les nouvelles pratiques de gouvernance en termes de mise en conformité. Il en découle une réduction des risques de contentieux contractuel, administratif et judiciaire.

Un renforcement de la sécurité informatique : le CIL conseille l'organisme sur les nouvelles manières d'exploiter les données. Il permet d'éviter les erreurs stratégiques lors du lancement de nouveaux services ou produits, et optimiser en conséquence les investissements, la politique d'archivage et d'externalisation, les procédures internes relatives à la sécurité de l'information.

Un vecteur de confiance avec les parties prenantes : la mise en place d'un CIL est de nature à rassurer les personnes extérieures à l'organisme (clients, citoyens, fournisseurs, étudiants, partenaires potentiels, etc.) et le personnel interne sur les garanties prises pour une collecte et un traitement responsable des données.

Un service dédié au sein de la CNIL

La CNIL propose un accompagnement personnalisé des CIL dès leur désignation, en les préparant à l'exercice de leurs missions et en les guidant dans l'application des textes relatifs à la protection des données :

• réponse rapide aux demandes de conseil juridique,
• ateliers d'information exclusifs et gratuits (en 2014, plus de 1 000 participants ont suivi 34 ateliers),
• outils dédiés (extranet contenant des guides, modèles, réponses-type, référentiels, etc.),
• permanence téléphonique quotidienne.

En 2014, ce sont plus de 2 567 demandes de conseil juridique (+ 17% par rapport à 2013) et 4 808 appels traités par l'équipe du service des CIL, qui concrétise cette volonté forte d'animer et de fédérer le réseau.

Désigner un CIL : une étape vers l'obtention du label « gouvernance » de la CNIL

La désignation d'un CIL fait partie des exigences posées pour obtenir le label CNIL « gouvernance Informatique et Libertés » qui permet d'indiquer au public que la procédure ou le produit proposé par un organisme corresponde aux exigences de la Commission. Un label de la CNIL est destiné à améliorer la confiance des utilisateurs, en termes de protection de la vie privée, envers des produits et des procédures.

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.

Nos domaines de compétence :

• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Source : http://www.cnil.fr/linstitution/actualite/article/article/cil-un-metier-davenir/

Attaque par phishing simulée au PMU : 120 employés piégés | Le Net Expert Informatique

	Attaque par phishing simulée au PMU : 120 employés piégés

La pièce jointe que l'on ouvre et qui diffuse un virus dans toute l'entreprise demeure le vecteur principal des attaques informatiques. Le PMU a testé les réactions de ses collaborateurs en mai dernier en leur envoyant un email de ce type conçu par ses soins. 22% ont cliqué dans la pièce jointe.

Le hack, c'est trop facile. Environ 120 collaborateurs du PMU se sont laissés piéger par un faux email leur proposant de gagner un iPad. Ils ont cliqué dans le lien présent dans l'email et donné leurs coordonnées.

6% ont donné leurs coordonnées

C'est le résultat d'un test mené en vraie grandeur par le PMU en mai dernier pour mesurer la résistance à une attaque par phishing de ses collaborateurs. Résultat : 22% des salariés ont ouvert la pièce jointe associée à un faux email d'invitation à participer à un jeu pour gagner un iPad.

Et 6% – soit environ 120 personnes – ont cliqué sur le lien présent à l'intérieur et donné leurs coordonnées pour gagner le lot. La pièce jointe affichait un faux message destiné à effrayer durant quelques minutes ceux qui l'avaient ouverte en leur faisant croire que leur PC est en danger et va être vidé.

Le test a été réalisé de façon anonyme, par un prestataire externe, en revanche, on sait que ce sont des personnes de tous les services qui ont cliqué dans l'email.

L'attaque contre TV5 monde

La DRH a donné le feu vert à l'opération car le test a été réalisé juste après les incidents de TV5 Monde qui avait vu la chaîne être bloquée durant une journée à la suite d'une attaque informatique.

Le résultat est à la fois inquiétant et rassurant. Inquiétant car test est intervenu après que le PMU ait procédé à deux ou trois campagnes de sensibilisation au phishing, en expliquant aux collaborateurs qu'il ne faut pas cliquer sur les liens présents dans les emailings. Rassurant, car le fait que le PMU communique de tels résultats permet de sensibiliser l'ensemble des entreprises à ce type de risques.

Le phishing est banal

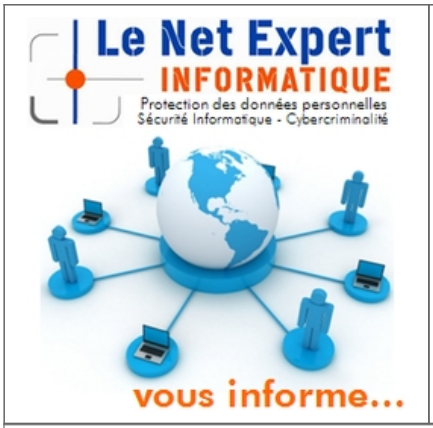
Le phishing est une attaque informatique qui consiste à envoyer des emails imitant ceux de sociétés reconnues – banques, organismes sociaux – afin de recueillir les coordonnées bancaires des personnes ciblées.

Les attaques qui propagent des virus informatiques dans les entreprises – appelées APT (Advanced Persistent Threat) – passent majoritairement par l'ouverture de pièces jointes qui diffusent ensuite un code informatique malveillant entre les machines du réseau de l'entreprise.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source :
http://www.larevuedudigital.com/2015/10/03/simulation-dune-attaque-par-phishing-120-employes-du-pmu-pieges/

CNIL Besoin d'aide ? – Gestion des clients et prospects : quelles formalités à la CNIL ? | Le Net Expert Informatique



Gestion des clients et prospects : quelles formalités à la CNIL ?

Les fichiers relatifs à la gestion de clients et de prospects doivent être déclarés à la CNIL :
• Par une déclaration simplifiée de conformité à la norme n°48, si le fichier correspond aux caractéristiques énoncées dans ce texte;
• Par une déclaration normale si le fichier sort du cadre de cette norme.

A noter : la norme simplifiée n°48 ne s'applique pas aux établissements bancaires ou assimilés, aux entreprises d'assurances, de santé et d'éducation.

Même si remplir un formulaire de déclaration à la CNIL est simple et gratuit, il vous engage cependant, par la signature que vous apposez, à respecter point par point la loi Informatique et Libertés. Cette démarche doit d'abord commencer par une analyse précise et confidentielle de l'ensemble de vos systèmes de traitements de données. Nous pouvons vous accompagner pour une mise en conformité CNIL, former un C.I.L. (correspondant CNIL) ou sensibiliser les agents et salariés à l'hygiène informatique.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

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

Source : http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=DB87C2DC40C5190FF1ABC6E812FA9500?id=541&back=true

Décryptage du Safe Harbor | Le Net Expert Informatique

Décryptage du Safe Harbor

La Cour de justice de l'Union européenne (CJUE) a rendu la semaine dernière une décision historique en invalidant le « Safe Harbor ». Cet accord, concocté par le Département du Commerce des États-Unis, approuvé par la Commission européenne, légalise le transfert de données personnelles de citoyens européens vers les États-Unis. Amazon, Facebook et les autres géants américains du Net pouvaient donc librement exporter nos données et les exploiter à leur guise à des fins publicitaires. Son invalidation va changer la donne, et les défenseurs du respect de la vie privée, parmi lesquels l'UFC-Que Choisir, s'en réjouissent.

Le Safe Harbor en deux mots

Europe et États-Unis ont une vision différente de la protection des données personnelles des citoyens. Leurs politiques respectives en la matière sont donc divergentes. L'Europe interdit notamment le transfert des données personnelles vers des pays qui offrent un niveau de protection inférieur au sien (1). Pour ne pas priver les entreprises américaines de cet « or numérique » en provenance de l'Europe, le Département du Commerce des États-Unis (l'équivalent d'un ministère du Commerce) a concocté un cadre juridique qui légalise le transfert de données personnelles : le Safe Harbor, aussi appelé Sphère de sécurité. Les entreprises qui souhaitent en profiter doivent garantir certaines conditions (information des consommateurs sur l'exploitation de leurs données, droit de rectification, sécurité des données, etc.) et obtenir une certification. 4 000 entreprises américaines en sont titulaires, parmi lesquelles Microsoft, Amazon, Google ou encore Facebook.

De quelles données parle-t-on ?

Les données personnelles sont au centre de la plupart des modèles économiques des entreprises du Net. Vos achats, les messages que vous publiez sur les réseaux sociaux, vos habitudes de navigation sur Internet, les mots que vous saisissez dans les moteurs de recherche, ou bien encore les livres et les films que vous achetez en ligne sont autant d'indicateurs qui permettent de définir finement des profils de consommation et de vous envoyer des publicités ciblées, donc efficaces, donc vendues à prix d'or.

Quels sont les fondements de la décision de la CJUE ?

Tout est parti d'une plainte de Maximillian Schrems, un citoyen autrichien, auprès de l'autorité irlandaise de contrôle, l'Office of the Data Protection Commissioner, l'équivalent de notre Cnil (2). Maximillian Schrems utilise Facebook et sait qu'en vertu du Safe Harbor, ses données sont traitées aux États-Unis. Mais les révélations d'Edward Snowden, en 2013, sur la surveillance opérée par la NSA (National Security Agency) prouvent que le pays n'offre pas un niveau de protection suffisant des données. Or le Safe Harbor engage les États-Unis à fournir un niveau de protection au moins équivalent à celui de l'Europe.

La CJUE s'est prononcée sur deux points. D'abord, elle a confirmé qu'une autorité nationale (la Cnil et les autres) a le droit d'enquêter lorsqu'elle est saisie par un citoyen sur le sujet, et ce malgré l'existence du Safe Harbor. Ensuite, elle estime que la Commission européenne a eu tort d'accepter cet accord sans vérifier que les États-Unis n'interdisaient pas les opérations de surveillance généralisée (comme celles de la NSA). Du coup, 15 ans après son entrée en application, la justice suspend le Safe Harbor. Une décision historique.

Cette décision va-t-elle changer quelque chose ?

À court terme, les entreprises du Safe Harbor se retrouvent dans un trou juridique. Elles doivent subitement gérer une situation passée de légale à illégale du jour au lendemain. Les grandes entreprises disposent des armes suffisantes pour poursuivre leurs activités à coup de bras de fer juridiques. Mais quid des entreprises plus modestes ?

À moyen terme, l'Europe réaffirme son attachement à la protection des données personnelles. Cette décision de la CJUE pèsera sans doute dans les discussions sur le projet de Règlement européen sur les données personnelles. Ce texte, actuellement au stade des négociations tripartites entre le Parlement, le Conseil et la Commission, constituera à l'avenir le socle de la politique européenne en matière de protection de la vie privée.

(1) Directive 95/46/CE sur la protection des données personnelles.
(2) Commission nationale de l'informatique et des libertés.

Même si remplir un formulaire de déclaration à la CNIL est simple et gratuit, il vous engage cependant, par la signature que vous apposez, à respecter point par point la loi Informatique et Libertés. Cette démarche doit commencer par une analyse précise et confidentielle de l'ensemble de vos systèmes de traitements de données. Nous pouvons vous accompagner pour vous mettre en conformité avec la CNIL, former ou accompagner un C.I.L. (correspondant CNIL) ou sensibiliser les agents et salariés à l'hygiène informatique.

Besoin d'informations complémentaires ?

Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

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

Source : http://www.quechoisir.org/telecom-multimedia/internet/actualite-donnees-personnelles-decryptage-du-safe-harbor
Par Camille Gruhier

Un nouveau logiciel malveillant cible les iPhone | Le Net Expert Informatique

	Un nouveau logiciel malveillant cible les iPhone

Décidément, les terminaux à la pomme intéressent de plus en plus les pirates. Après la découverte le 4 février par les experts du cabinet de sécurité informatique Trend Micro du premier logiciel espion baptisé « XAgent » exploitant des failles sur les téléphones Apple non débridés (dits « non jailbreakés »), c'est au tour de l'unité de recherche 42 de l'entreprise de sécurité informatique Palo Alto Networks de publier dimanche 4 octobre une alerte sur un nouveau logiciel malveillant (malware) affectant les iPhones du commerce.

Baptisé « YiSpecter », il attaque sans distinction les iPhone du commerce vendus avec le système d'exploitation officiel iOS d'Apple et ceux qui ont été débridés. Apple, qui a reconnu l'existence de ce malware, a indiqué lundi 5 octobre que les utilisateurs d'iOS 8.4 et d'iOS 9 étaient désormais protégés. La particularité de ce programme – qui serait actif depuis plus de 10 mois à Taïwan et en Chine continentale d'où il proviendrait – est d'utiliser des failles que l'on pensait impossible à exploiter, et de se propager de façon inédite, selon Palo Alto Networks.

Un fonctionnement et une propagation inédits

Détournant certaines interfaces de programmation propres au système d'exploitation iOS, cette nouvelle forme de logiciel malveillant ne laisse rien présager de bon pour l'avenir des terminaux mobiles à la pomme selon la firme de sécurité à l'origine de la découverte : « C'est le premier malware que nous avons vu en circulation qui abuse les API [interfaces de programmation] privées dans le système iOS pour mettre en œuvre des fonctionnalités malveillantes. »

En se propageant seul soit grâce à « Lingdun », un ver informatique sous Windows (qui se charge d'envoyer des liens malicieux de téléchargement d'YiSpecter à tous ses contacts), soit par le piratage des connexions WiFi des boîtiers des fournisseurs d'accès à Internet, cette nouvelle variante de malware inquiète la société californienne. Ses quatre composants, tous authentifiés par des certificats d'entreprises réels émanant de sociétés comme Verisign ou Symantec, s'installent de façon furtive sur les iPhone, en masquant ses programmes, mais aussi en dupliquant les noms et les logos des icônes système (Game Center, Météo, Notes, PassBook, Téléphone, etc.), piégeant même les utilisateurs les plus avertis.

Une fois installé, YiSpecter peut télécharger, installer et lancer des applications de l'App Store, mais aussi les modifier, par l'affichage de publicités en plein écran par exemple. Il permet également de collecter les données des utilisateurs, notamment celles utilisées dans le navigateur Internet Safari. S'il est découvert, sa suppression par méthode classique ne fonctionnera pas car il se réinstalle automatiquement après un redémarrage système. Enfin, peu d'espoir du côté des antivirus, qui ne détectent toujours pas sa présence sur les terminaux infectés.

Des malwares aux origines peu claires

Certains indices repérés par Palo Alto Networks font converger les soupçons vers « YingMob », une entreprise chinoise de publicité mobile ayant pignon sur rue, qui aurait programmé et diffusé ce malware à des fins publicitaires, n'hésitant pas à en faire sa promotion au grand jour. Mais la complexité et les méthodes de propagation de YiSpecter cachent peut-être des visées plus opaques.

Déjà le mois dernier, 344 applications iOS officielles présentes dans l'App Store, la boutique d'applications d'Apple, avaient été retirées en urgence car infectées par le malware « XcodeGhost », découvert le mercredi 16 septembre par les équipes sécurité du groupe chinois Alibaba. L'origine de ce malware est encore incertaine, mais les méthodes utilisées sont très similaires aux techniques de programmation qu'emploie la CIA – selon des documents publiés en mars par The Intercept.

Tout début septembre, c'était le logiciel malveillant « KeyRaider » également découvert par la société Palo Alto Networks, qui faisait parler de lui : selon la société de sécurité, plus de 225 000 comptes et identifiants Apple auraient été dérobés, uniquement sur des iPhone et iPad débridés.

La société de sécurité américaine est également à l'origine de la chute d'un mythe : c'est elle qui annonçait il y a moins d'un an, en novembre 2014, la découverte, toujours en Chine, de « Wirelurker », le tout premier malware pour iPhone touchant des téléphones non débridés. Depuis, il ne se passe pas un mois sans qu'une nouvelle alerte concernant les terminaux mobiles d'Apple ne soit lancée.

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Source :
http://www.lemonde.fr/pixels/article/2015/10/07/un-nouveau-logiciel-malveillant-cible-les-iphone_4784509_4408996.html

Que peuvent faire les entreprises en attendant un Safe Harbor II | Le Net Expert Informatique

Que peuvent faire les entreprises en attendant un Safe Harbor II

La décision de la CJUE étant d'application immédiate, depuis le 6 octobre 2015, tous transferts vers les Etats-Unis fondés sur le Safe Harbor sont invalides. Marc d'Haultfoeuille (Avocat Associé) et Nadège Martin (Avocat Of Counsel) de l'Equipe Technologie & Innovation de Norton Rose Fulbright, explique quoi faire en attendant un Safe harbor II.

Ce que les entreprises peuvent faire en attendant un Safe Harbor II

Force est d'admettre que la décision du 6 octobre 2015 par laquelle la Cour européenne de justice (CJUE) a déclaré invalide la décision Safe Harbor, sème un trouble auquel il n'existe aucune réponse juridique unanimement valable pour l'ensemble des entreprises concernées. Cette situation tient au fait qu'au-delà du contenu de cette décision, dont la portée demeure encore difficilement mesurable en l'absence de positionnement officiel des autorités de protection des données, d'autres paramètres doivent être pris en compte : le transfert est-il déjà effectif ? quelles sont ses finalités ? la loi nationale impose-t-elle des formalités préalables ?

AUDIT DES TRANSFERTS EN COURS

La décision de la CJUE étant d'application immédiate, depuis le 6 octobre 2015, tous transferts vers les Etats-Unis fondés sur le Safe Harbor sont invalides. Il est ainsi recommandé d'identifier rapidement les contrats et formalités déclaratives existants (ces transferts étaient soumis à simple notification auprès de la CNIL) afin de disposer des détails pertinents sur ces transferts.

Cet audit est nécessaire à l'identification des solutions alternatives envisageables à plus ou moins court terme, en l'état de la loi Informatique et Libertés ou sur la base des mesures qui pourraient être annoncées dans l'intervalle par la CNIL. A plus long terme, la décision Safe Harbor II en cours de discussion devrait être une solution pertinente mais il est difficile de prévoir sous quels délais elle sera adoptée.

DES DÉLAIS À ANTICIPER POUR LES TRANSFERTS À COURT TERME

La situation s'avère plus délicate pour les contrats en voie de conclusion pour lesquels le transfert était censé être fondé sur le Safe Harbor. En effet, sauf à pouvoir remplacer ce fondement par une exception légale ou des BCRs également soumis à simple notification préalable auprès la CNIL, les parties devront non seulement conclure des clauses contractuelles types (CCT) mais le responsable de traitement devra solliciter l'autorisation préalable de la CNIL au transfert. Or, obtenir cette autorisation peut prendre jusqu'à deux mois, voire plus, selon la loi. De plus, au vu des motifs de la décision rendue par la CJUE, le traitement de ces demandes par la CNIL est susceptible d'en être complexifié et en tout état de cause, allongé. Ces projets seront ainsi, pour beaucoup, dépendants des orientations qui seront prises par les autorités de protection des données.

Même si remplir un formulaire de déclaration à la CNIL est gratuit et enfantin, il vous engage cependant, par la signature que vous apposez, à respecter scrupuleusement la loi Informatique et Libertés. Cette démarche doit d'abord commencer par un Audit de l'ensemble de vos systèmes de traitements de données. Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

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

Source : http://www.usine-digitale.fr/article/ce-que-les-entreprises-peuvent-faire-en-attendant-un-safe-harbor-ii.N356084

Le secret professionnel des avocats menacé par la Loi renseignement ? | Le Net Expert Informatique

 Le Conseil de l’ordre des avocats de Paris va saisir la Cour européenne des droits de l’Homme (CEDH) contre la loi controversée sur le renseignement. | AFP	Le secret professionnel des avocats menacé par la Loi renseignement ?

Le Conseil de l'ordre des avocats de Paris va saisir la Cour européenne des droits de l'Homme (CEDH) contre la loi controversée sur le renseignement.

« Nous allons saisir la CEDH contre cette loi qui repose à nos yeux sur deux mensonges d'État », a expliqué vendredi le bâtonnier de Paris Pierre-Olivier Sur, confirmant une information du site Next INpact.

« Le premier mensonge, c'est que cette loi ne vise pas simplement à protéger la société contre le terrorisme, elle concerne toute la matière pénale. Le second, c'est qu'il n'y a pas dans le texte de véritable juge pour protéger les libertés publiques car le seul juge habilité à le faire, c'est le juge judiciaire. Et le législateur a choisi un juge administratif, très éloigné des questions de liberté », a-t-il fait valoir.

« Ce secret professionnel a une valeur sacrée »

Pour le représentant des avocats parisiens, la loi sur le renseignement porte également atteinte « au secret professionnel des avocats ».

« Ce secret professionnel a une valeur sacrée. Il ne place pas l'avocat au-dessus des lois mais on doit prendre en compte la spécificité de son travail, ne pas aller chercher, en fracturant le secret, des renseignements sur des actes qu'il aurait pu commettre et qui, par capillarité, risque de nuire à la défense de son client. Il faut donc que les premiers actes d'investigation soient particulièrement contrôlés, notamment par le président du TGI », a-t-il fait valoir.

Cette saisine intervient quelques jours après celle de l'Association de la presse judiciaire (APJ) qui estimait, elle, que la loi sur le renseignement menaçait la liberté de la presse et le secret des sources.

Ecoutes, caméras, logiciel-espion…

De la prévention d'attentats à l'espionnage économique, le texte définit un large éventail des missions des services de renseignement ainsi que le régime d'autorisation et de contrôle de techniques d'espionnage (écoutes, pose de caméra ou de logiciel-espion, installation chez les opérateurs de télécommunications de dispositifs pour collecter les données de connexion, etc.).

Fin juin, le Parlement a adopté définitivement la loi à une large majorité gauche-droite, mais avec des voix dissidentes dans presque chaque groupe.

Face à la controverse, François Hollande a saisi le Conseil constitutionnel. Ce dernier a validé la loi en juillet estimant notamment que « le législateur (avait) prévu des garanties suffisantes pour qu'il ne résulte pas » du texte contesté « une atteinte disproportionnée au droit au respect de la vie privée, au droit de la défense et au droit à un procès équitable, y compris pour les avocats et les journalistes ».

Source :
http://www.ouest-france.fr/loi-renseignement-le-secret-professionnel-des-avocats-menace-3752413