Europol met en garde contre les communications chiffrées | Le Net Expert Informatique

Europol met en garde contre les communications chiffrées

Europol, la police criminelle intergouvernementale, s'est récemment exprimée au sujet des communications chiffrées. Selon les autorités, cela représenterait un réel danger face à la menace terroriste.

Les informations partagés par Edward Snowden, ancien analyste à la NSA, sur les pratiques de surveillance massive orchestrées par les agences de renseignements ont fait l'effet d'une onde de choc. Du jour au lendemain, les plus grosses sociétés Internet ont été directement impliquées dans des affaires de cyber-surveillance. Autant dire que la confiance des internautes vis-à-vis des entreprises, mais également celle de ces dernières face aux gouvernements, en a pris un sacré coup.
Microsoft, Yahoo, Apple ou encore Google ont renforcé leur infrastructure et de plus en plus d'outils surgissent sur la Toile pour sécuriser les communications et la vie privée des internautes. En d'autres termes, la notion de vie privée a le vent en poupe, et ce n'est pas pour plaire à tout le monde. Pour Europol, l'existence de ces technologies est un frein à la lutte contre le terrorisme.

Dans une interview recueillie par la BBC, Rob Wainwright, directeur d'Europol, affirme que les efforts visant à chiffrer les communications par les grandes sociétés high-tech devient problématique. « C'est probablement devenu le plus gros problème pour la police et pour les services de sécurité dans leur lutte contre le terrorisme », affirme-t-il. Et d'ajouter « cela a changé la nature-même du travail contre le terrorisme lequel était jusqu'à présent fiable avec des communications que nous pouvions gérer à un autre qui ne fournit plus rien ».
Apple et Google ont pris le parti de chiffrer leurs systèmes d'exploitation mobiles, au grand dam du FBI. Aussi, Yahoo! a annoncé qu'un dispositif de chiffrement des emails serait proposé d'ici la fin de l'année sur son Webmail. Un mécanisme similaire est déjà disponible avec l'extension Mailvelope pour Chrome et Firefox. Le service sécurisé ProtonMail vient de lever 2 millions de dollars tandis que la messagerie instantanée CryptoCat gagne en popularité.
Pour M. Wainwright, les efforts des sociétés de la Sillicon Valley seraient « motivés par des impératifs commerciaux parce qu'ils perçoivent une demande des consommateurs souhaitant une meilleure vie privée pour leur communications ». D'emblée, ce n'est donc pas la vie privée des internautes qui prime mais les dangers potentiels d'une communication entre terroristes. D'emblée, les efforts des sociétés pour protéger leurs infrastructures et leurs services sont donc replacés à une campagne marketing…
Entre les agences de renseignement et les prestataires de services, le bras de fer ne fait que commencer. Le mois dernier Alex Stamos, responsable de la sécurité chez Yahoo! est monté au créneau contre le directeur de la NSA, lequel souhaite voire la mise en place d'une porte d'accès aux données de l'internaute de manière légale. Les géants du Web se sont rassemblés pour lancer un appel au Congrès américain afin que les services de renseignement cessent leurs collectes de données.

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 protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source :
http://pro.clubic.com/technologie-et-politique/actualite-761041-europol-garde-communications-chiffree.html?&svc_mode=M&svc_campaign=NL_ClubicPro_New_31/03/2015&partner=-&svc_position=91669690B&svc_misc=-&crmID=639453874_91669690B&estat_url=http%3A%2F%2Fpro.clubic.com%2Ftechnologie-et-politique%2Factualite-761041-europol-garde-communications-chiffree.html

---

Un examen médical et pratique pour les pilotes professionnels de drones | Le

Net Expert Informatique

Un examen médical et pratique pour les pilotes professionnels de drones

Les personnes qui souhaitent employer des drones à des fins commerciales seront tenues de passer un examen médical et de démontrer une connaissance théorique et pratique suffisante, indique mardi la ministre de la Mobilité, Jacqueline Galant, dans un communiqué relatif à la publication prochaine d'un arrêté royal organisant l'usage privé et l'exploitation commerciale des drones.

L'arrêté royal garantit par contre que les pilotes de drone à usage commercial devront, au-delà d'un examen médical, démontrer une connaissance théorique suffisante du monde aéronautique et réussir un examen pratique dispensé par un examinateur désigné par la DGTA. Il leur sera également demandé de maintenir leurs compétences puisqu'ils devront voler un minimum de 2 heures par an (6 vols) pour garder leur licence valable.

Les drones qui sont considérés comme des aéronefs par la législation internationale doivent respecter les règles en vigueur, précise l'arrêté. Ainsi, l'accès à un espace aérien contrôlé leur sera interdit, sauf autorisation. En ce qui concerne les espaces militaires, une gestion dynamique de ceux-ci sera assurée par la Défense.

L'altitude maximale autorisée pour les drones a été fixée à 300 pieds (environ 90 mètres, l'équivalent d'un immeuble d'une trentaine étages). La limite fixée garantit à la fois la sécurité des avions habités et donne aux drones la possibilité de réaliser environ 90% des missions envisagées, peut-on lire dans le communiqué. Des dérogations pourront être demandées lors de missions spéciales.

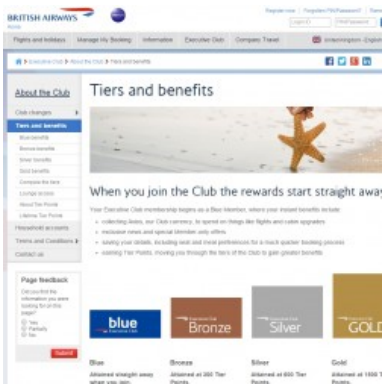
Avec cet arrêté royal, la Belgique rejoint 19 pays européens qui se sont dotés d'une législation en la matière. « Je mettrai de suite en place un groupe de travail, composé de représentants de l'administration, de Belgocontrol, de la Défense et du secteur », a ajouté Jacqueline Galant.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.rtbf.be/info/belgique/detail_un-examen-medical-et-pratique-pour-les-pilotes-professionnels-de-drones?id=8945274

Alerte : Comptes clients

piratés chez British Airways | Le Net Expert Informatique



Alerte : Comptes clients piratés chez British Airways

Une action de piratage a visé de nombreux comptes de clients de la compagnie aérienne British Airways. Les points fidélité amassés tout au long des différents trajets ont été effacés.

Depuis quelques jours, un grand nombre de clients de la compagnie aérienne British Airways ont eu la désagréable surprise de trouver que le solde de points fidélités accumulés grâce à leurs précédents trajets en avion avaient disparu. D'autres n'ont tout simplement plus accès à leur compte fidélité, appelé Executive Club. Une situation qui serait loin d'être le fruit du hasard ou d'un bug informatique, mais qui a plutôt à voir avec une opération de piratage sur un grand nombre de comptes.

Interrogée sur un forum dédié par un utilisateur, British Airways a admis avoir été mis au courant d'une activité non autorisée sur son compte. « Il semble que cela soit le résultat d'un tiers utilisant de l'information obtenue quelque part sur Internet, via un processus automatisé, pour tenter d'accéder aux comptes Executive Club », a indiqué British Airways dans un mail. Bien que les pirates sont parvenus à accéder à des comptes, British Airways n'est pour l'instant pas au courant d'accès à des pages d'information de comptes, historiques de vols ou détails de cartes de paiement.

Selon un message posté par la compagnie, les mots de passe des comptes affectés par ce piratage ont été changés et l'utilisation des points fidélité « Avios » suspendue pour quelques jours. La société a par ailleurs également répondu aux utilisateurs affectés par le problème sur Twitter.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lemondeinformatique.fr/actualites/lire-alerte-aux-comptes-clients-pirates-chez-british-airways-60700.html?utm_source=mail&utm_medium=email&utm_campaign=Newsletter

---

Les 12 outils de communication des commerçants, pme, tpe et professions libérales | Le

Net Expert Informatique

Les 12 outils de communication des commerçants, pme, tpe et professions libérales

Le développement de la communication numérique est une formidable opportunité pour accroître votre visibilité et augmenter votre clientèle. Ce serait dommage de ne pas la saisir ! Vos clients sont au bout de leur smartphone, derrière leurs ordinateurs et leurs tablettes.
Pour vous accompagner dans la mise en place d'actions de communication locale nous avons listé pour vous 12 outils.

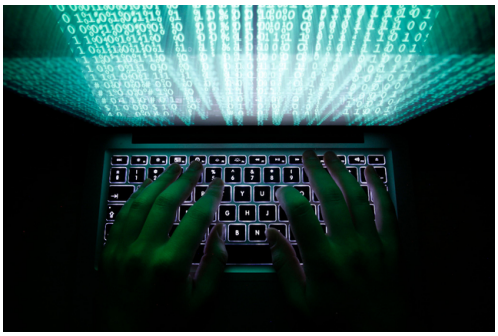
1. L'identité de marque
2. Documents print
3. Le site internet
4. Le référencement
5. Les réseaux sociaux
6. Le micro-blogging
7. Le marketing direct
8. Le marketing relationnel
9. Le street marketing
10. Les relations presse
11. L'achat média
12. Le Sponsoring

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 protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : https://www.1min30.com/ressource/outils-pme-tpe

Les sites Internet trompeurs visent de plus en plus les PME| Le Net Expert Informatique

 Image: Photo d’illustration/Reuters	**Les sites Internet trompeurs visent de plus en plus les PME**

Les petites et moyennes entreprises sont aussi concernées par les attaques sur le web. Les pirates se servent des données des sites pour tromper les clients. La manœuvre la plus courante est d'envoyer des mails aux clients en se faisant passer pour l'entreprise.

Les escrocs opérant via Internet ne s'en prennent plus uniquement à des grandes marques connues: de plus en plus, ils imitent les sites web de petites et moyennes entreprises pour tromper leurs clients. Ils accèdent ainsi à leurs mots de passe ou données de cartes de crédit.
La Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) intervient quotidiennement pour retirer ce type de contenus frauduleux du web, a-t-elle annoncé le mardi 31 mars. Les derniers cas rapportés témoignent même d'une sophistication accrue.
Les attaques de phishing, par lesquelles des escrocs cherchent à accéder à des données sensibles, concernent différents types de PME ayant un site WEB et qui enregistrent des adresses mail de clients, par exemple pour l'envoi d'une newsletter.
Dans un premier temps, les criminels attaquent le site web de l'entreprise. La plupart du temps, ils exploitent une faille sur le site. Cela leur permet d'accéder à une base de données contenant des mails de clients.
Ensuite, ils envoient des mails à ces clients en se faisant passer pour l'entreprise. Les messages font par exemple état d'un remboursement pouvant être demandé par le biais d'un lien indiqué. Derrière ce lien se cache un site web imitant à l'identique celui de l'entreprise et utilisant un nom de domaine très similaire.

Victime en confiance
Le client y est prié de fournir les détails de sa carte de crédit (numéro, validité, cryptogramme), à l'image d'une page de phishing «classique». En usurpant le mail et en imitant le site web d'une entreprise avec laquelle la victime potentielle est en relation, les escrocs augmentent leurs chances de succès, puisque la cible aura plus de chances de se sentir en confiance.
MELANI conseille aux entreprises d'informer rapidement leurs clients lorsqu'elles remarquent le vol d'e-mails. Quant aux utilisateurs, ils sont priés d'effacer les courriels leur enjoignant de fournir des données de cartes de crédit: aucune entreprise sérieuse ne demande de telles informations par mail, rappelle MELANI.
De plus, il faut se méfier des mails évoquant des conséquences (perte financière, plainte pénale, blocage d'un compte ou d'une carte etc) si le destinataire n'agit pas. Enfin, il faut toujours contrôler l'«adresse Internet» (URL) sur laquelle on est redirigé. Pour ce faire, il suffit de positionner la souris sur le lien sans cliquer. (ats/Newsnet)

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.tdg.ch/high-tech/sites-internet-trompeurs-visent-plus-pme/story/15578282

L’armée mène une bataille numérique au cœur des entreprises sensibles | Le Net Expert Informatique

L’armée mène une bataille numérique au cœur des entreprises sensibles

3 mars 2015, les responsables d'une entreprise « sensible » sont inquiets. Il semble clair que la PME est l'une des nombreuses cibles d'une cyberattaque massive lancée contre les industriels français depuis plusieurs semaines maintenant. Face à cette attaque d'ampleur nationale et touchant des entreprises sensibles, le gouvernement fait appel à l'armée.

L'ordre est donc donné par le Premier Ministre d'agir rapidement et efficacement. La cellule de crise du commandement opérationnel de Cyberdéfense du ministère de la Défense va mobiliser dans les meilleurs délais ses équipes pour intervenir directement dans les entreprises touchées. Tous les relais militaires et civils spécialisés dans la cyberdefense sont en alerte.
Leur mission, atténuer la portée de l'attaque et reconstruire le réseau. Dépêchés le plus rapidement possible au cœur de l'entreprise, des équipes d'une quinzaine de spécialistes encadrés par un officier chargé de la logistique prennent place sur les postes informatiques de l'entreprise. Leurs outils ? Aucun, ils viennent dérouler le fil de l'attaque pour pouvoir mieux l'endiguer, colmater les brèches.
Leur difficulté c'est que pour limiter les dégâts, la PME est totalement coupée d'Internet. Les spécialistes s'acharnent à chercher les preuves, nettoyer en profondeur, détecter toutes les failles et verrouiller les portes. Des observateurs de l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) sont présents pour faire remonter les informations auprès de l'organisme et coordonner les actions éventuelles à mener avec les différents ministères du gouvernement.
Une équipe de spécialistes constituée d'étudiants en quatrième année de l'EPITA est déployée par le commandement opérationnel de Cyberdéfense de l'armée pour reconstruire un réseau d'entreprise ayant subi une cyberattaque d'envergure. Dans l'avenir, ces étudiants pourraient faire partie des milliers de réservistes spécialisés que compte recruter le Ministère de la Défense.

« C'est du vécu »
Rapidement, les experts comprennent que le cybermissile s'est introduit tout simplement via une vulnérabilité WordPress du blog de l'entreprise. L'attaquant a installé un relai de scripts sur le serveur du blog qui lui permet d'aller plus avant dans ses funestes objectifs. Il pouvait même prendre la main sur l'ERP de l'entreprise. L'organisation pirate en a profité pour absorber la base de données de la société.
Mais voilà, ce scénario catastrophe est ce que l'armée appelle un « jeu », avec des « joueurs ». En réalité, ce jeu fait partie d'un exercice en grandeur nature réalisé par 600 personnes et encadré par le Ministère de la Défense et l'ANSSI. Baptisé DEFNET, l'expérimentation consiste à mettre en place des équipes constituées de dix à 15 élèves provenant de grandes écoles spécialisées dans le domaine de l'informatique et des télécommunications (Epita, Insa, Télécom Paris Tech, Ensta Bretagne, CentraleSupélec,…).
Encadré par un enseignant et un militaire, l'idée consiste à former à partir de ces ressources, les réservistes dédiés à la cyberdéfense de demain. L'armée compte disposer de plusieurs milliers de réservistes dans les prochaines années.
Lors de l'exercice, auquel ZDNet.fr a pu assister, le contre-Amiral Riban, Directeur Général adjoint de l'ANSSI a tenu à préciser que cette expérimentation repose sur « du vécu », sans en dire beaucoup plus, secret défense oblige. Dans ce genre de situation de crise, l'ANSSI est le chef d'orchestre. En élaguant les vagues de cyberattaques et les défacements de sites web en janvier, qui, pour lui étaient d'un niveau faible, il souligne qu'une véritable cyberattaque ne se résumerait pas forcément uniquement à des conséquences tragiques en termes de vol de données.
Ainsi, si les réseaux informatiques des banques, des aéroports, des réseaux de transport (SNCF, Ratp,…), ou les opérateurs de téléphonie étaient victimes d'une cyberattaque, la France pourrait être paralysée en quelques heures, avec tous les dangers que cela peut représenter. Enfin, interrogé sur une riposte éventuelle suite à une cyberattaque, le contre-amiral a précisé que l'article 21 de la loi de programmation militaire oblige à faire cesser l'attaque, mais pas d'aller au-delà. Le sujet est donc bien la défense…

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.zdnet.fr/actualites/cyberdefense-quand-l-armee-mene-une-bataille-numerique-au-coeur-des-entreprises-sensibles-39817126.htm

---

Vote électronique :

précisions sur la sécurité et la confidentialité | Le Net Expert Informatique

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

Opter pour un prestataire pour l'organisation des élections professionnelles par vote électronique ne dédouane pas l'employeur de sa responsabilité en cas d'irrégularités. C'est ce que rappelle le Conseil d'Etat dans cette affaire. Il en profite pour apporter quelques précisions sur les garanties essentielles gouvernant ce dispositif en termes de confidentialité et de sécurité des données (Conseil d'Etat, 11.03.15, n°368748).

Pour élire ses délégués du personnel, la société X a décidé de mettre en place le vote électronique. Ayant déjà recouru à ce dispositif lors des précédentes élections professionnelles (en 2012), elle s'adresse au même prestataire extérieur.
Mais voilà qu'un syndicat conteste le bon déroulement des opérations et saisit la CNIL d'une plainte. Après enquête, cette dernière relève effectivement un certain nombre d'irrégularités. Aussi, elle prononce à l'encontre de l'entreprise, un avertissement et rend publique cette décision sur internet.
Contestant les manquements reprochés, et non contents de cette (mauvaise) « publicité », l'entreprise et le prestataire saisissent le Conseil d'Etat pour demander l'annulation la délibération de la CNIL.
Mais le Conseil d'Etat va approuver en tous points les manquements soulevés par la CNIL, et confirmer ainsi la sanction prise à l'encontre de la société requérante.

La pleine responsabilité de l'employeur, même en présence d'un sous-traitant

Pour rappel, l'employeur a la possibilité de confier à un prestataire la mise en place du système de vote électronique dans son entreprise. C'est l'option retenue par la société en l'espèce et c'est précisément grâce à ce sous-traitant qu'elle va tenter de s'affranchir de sa responsabilité. Elle estime en effet que le prestataire présentait des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité. Pour résumer, sa responsabilité se limitait au choix d'un « bon » prestataire. Elle n'était donc pas responsable des irrégularités commises par ce dernier.
Le Conseil d'Etat ne l'a pas entendu ainsi. Il considère au contraire que « la circonstance que des opérations de traitement de données soient confiées à des sous-traitants ne décharge pas le responsable de traitement de la responsabilité qui lui incombe de réserver la sécurité des données ». Le sous-traitant agissant « sur instruction du responsable de traitement », c'est bien sur ce dernier que repose l'obligation de veiller au respect de la sécurité et de la confidentialité des données personnelles. Les manquements constatés étaient donc imputables à la société requérante en sa qualité de responsable de traitement.

L'exigence d'une expertise préalable indépendante à chaque scrutin

Le Code du travail (1) soumet le système de vote électronique à une expertise indépendante préalable à sa mise en place ou à toute modification de sa conception. En l'espèce, le système ayant déjà été utilisé lors des dernières élections, et n'ayant fait l'objet d'aucune modification depuis, il n'a pas été jugé nécessaire de renouveler cette expertise préalable. Première erreur, car le Conseil d'Etat a interprété un peu plus largement les dispositions légales : si la réalisation d'une expertise indépendante est nécessaire au moment de la conception initiale du système et à chaque modification de la conception de ce système, elle l'est également « avant chaque scrutin recourant au vote électronique ». Afin de garantir la sincérité des opérations électorales par voie électronique, l'expertise aurait donc dû être renouvelée avant le scrutin.

Une transmission des moyens d'identification aux électeurs sécurisée

Au moment de voter électroniquement, l'électeur doit se connecter et se faire connaître par le moyen d'authentification qui lui a été transmis selon des modalités garantissant sa confidentialité (2). Ce moyen permet au serveur de vérifier l'identité de l'électeur et de garantir ainsi l'unicité de son vote. Il se trouve qu'en l'espèce, la transmission aux électeurs des identifiants et mots de passe, leur permettant de participer au vote, a été faite par simple courriel. Seconde erreur.
La CNIL a estimé que ce mode de transmission n'avait pas fait l'objet de mesures de sécurité spécifiques permettant de s'assurer que les électeurs en étaient les seuls destinataires(3).

Un chiffrement des bulletins de vote ininterrompu

Enfin, un arrêté ministériel (4) impose que le chiffrement (ou cryptage) et l'anonymat des bulletins de vote soit ininterrompu de l'émission du vote sur le poste de l'électeur, jusqu'à la transmission au fichier dénommé « contenu de l'urne électronique ». Voici donc le troisième manquement commis par la société : la CNIL a relevé que le système de chiffrement ayant été interrompu à un moment donné, il ne présentait pas un niveau de sécurité suffisant.

Ce rappel des règles était nécessaire. On peut ajouter que le Conseil d'Etat pousse plus loin encore la responsabilité de l'employeur dans le respect des règles relatives au vote électronique en approuvant la sanction infligée par la CNIL alors même que ces irrégularités n'ont entraîné ici aucune atteinte effective aux données personnelles des électeurs, ni aux principes du droit électoral ou encore aux libertés publiques.

(1) Art. R. 2314-12 du Code du travail.
(2) Art. R. 2324-5 du Code du travail.
(3) Cette solution n'est pas nouvelle, elle avait déjà été retenue par la chambre sociale de la Cour de Cassation dans un arrêt du 27 février 2013, n°12-14.415.
(4) Art. 2 de l'arrêté du ministre de l'Emploi, de la cohésion sociale et du logement pris en application du décret n°2007-602 du 25 avril 2007.
[block id="24761" title="Pied de page HAUT"]

A Lire aussi :
Nouveautés dans l'organisation des votes électroniques pour les élections professionnelles
3 points à retenir pour vos élections par Vote électronique
Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique
Modalités de recours au vote électronique pour les Entreprises
L'Expert Informatique obligatoire pour valider les systèmes de vote électronique
Dispositif de vote électronique : que faire ?
La CNIL sanctionne un employeur pour défaut de sécurité du vote électronique pendant une élection professionnelle
Notre sélection d'articles sur le vote électronique

Source : http://www.cfdt.fr/portail/le-carnet-juridique/fil-d-actualites/vote-electronique-precisions-sur-la-securite-et-la-confidentialite-srv1_255996

La Commission européenne conseille de quitter Facebook | Le Net Expert Informatique

La Commission européenne conseille de quitter Facebook

Un avocat de la Commission européenne a conseillé au procureur général de la Cour de Justice de l'Union Européenne (CJUE) de fermer son compte Facebook pour éviter que ses données personnelles soient exploitées aux Etats-Unis.

« Vous devriez envisager de fermer votre compte Facebook si vous en avez un » a conseillé Bernhard Schima, l'avocat de la Commission européenne, au procureur général de la JUE Yves Bot la semaine dernière. Une recommandation lancée dans le cadre d'une audience concernant la confidentialité des données des Européens vis-à-vis de l'utilisation qu'en fait le géant américain. La question avait été soulevée il y a plusieurs années par Max Schrems, un étudiant en droit autrichien qui a déclenché en août 2014 une procédure d'action collective mondiale à l'encontre de Facebook.
Mais le procès actuellement en cours oppose Max Schrems à l'équivalent irlandais de la CNIL, contre laquelle l'Autrichien a porté plainte, refusant de voir ses données personnelles stockées par Facebook – dont le siège européen se trouve en Irlande – transférées aux Etats-Unis pour alimenter le ciblage publicitaire de l'entreprise. Le réseau social n'est pas le seul concerné : Microsoft, Apple ou encore Yahoo sont également pointés du doigt.

Ciblage et espionnage
Max Schrems considère que les révélations d'Edward Snowden concernant l'espionnage des données pratiqué par la NSA met les Européens en danger à partir du moment où leurs données personnelles transitent aux Etats-Unis. Une accusation qui remet en question l'application du Safe Harbor, un ensemble de principes de protection des données personnelles, négociés entre les autorités américaines et la Commission européenne en 2001. Les entreprises qui adhèrent à ces principes peuvent recevoir des données en provenance de l'UE, mais la surveillance généralisée de la NSA remettrait en question l'application de ces règles.
On comprend mieux en quoi la petite phrase de l'avocat de la Commission européenne est lourde de sens : elle semble donner raison à la théorie de Max Schrems, engagé depuis longtemps contre la collecte d'information, jugée abusive, par Facebook.
Le commissaire irlandais à la protection des données considère quant à lui qu'il n'existe aucune preuve que le transfert des données de Max Schrems aux Etats-Unis lui a porté préjudice. « Ce n'est pas étonnant dans la mesure où la NSA n'est pas intéressée par les essais écrits par les étudiants en droit autrichiens » a-t-il ironisé. L'avocat général devrait rendre son avis sur l'affaire le 24 juin prochain.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://pro.clubic.com/blog-forum-reseaux-sociaux/facebook/actualite-760937-protection-donnees-personnelles-commission-europeenne-conseille-quitter-facebook.html

---

HoloLens, l'ordinateur du futur ? | Le Net Expert Informatique

HoloLens, l'ordinateur du futur ?

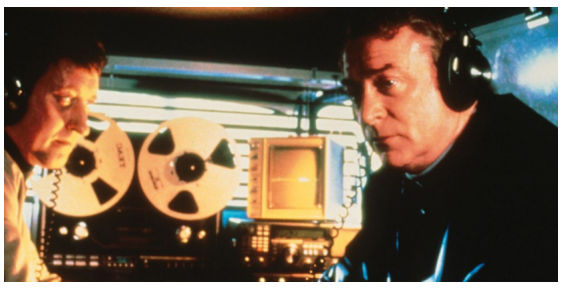
Le projet « Windows Holographic », avec son masque HoloLens, permettra de manipuler des objets virtuels dans un environnement réel.Microsoft assure que ce dispositif ambitieux préfigure « l'ordinateur du futur ».

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 protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.01net.com/editorial/642445/hololens-lordinateur-du-futur-video-du-jour/

Les 8 techniques les plus ahurissantes des espions d'aujourd'hui | Le Net Expert Informatique



Les 8 techniques les plus ahurissantes des espions d'aujourd'hui

Un projet de loi entend multiplier les possibilités de surveillance des agents du renseignement français. Tour des outils à disposition des services secrets dans le monde. Les services de renseignement français vont bientôt voir leurs possibilités d'espionnage multipliées, avec le projet de loi concocté par le gouvernement. L'occasion de faire le point sur l'éventail des outils à disposition des services secrets à travers le monde.

1. Ecouter les téléphones
Il s'agit de la pratique la plus évidente : l'écoute des conversations. En France, n'importe quel particulier peut être mis sur écoute dans le cadre d'une affaire portant « sur la sécurité nationale, la prévention du terrorisme, de la criminalité et de la délinquance organisée ».
Cette capacité s'est généralisée (pour atteindre un budget de 43 millions d'euros en 2013) et va parfois très loin. L'agence de renseignement américaine NSA s'est dotée d'une gigantesque capacité d'interception, avec son programme Mystic. En 2011, celui-ci aurait même servi à enregistrer 100% des appels passés dans un pays.
Pour simplifier les interceptions, la NSA a également des millions de données, notamment de Français, en se branchant directement sur le câble sous-marins ou les infrastructures internet par lesquels transitent 99% des télécommunications. L'agence était ainsi capable de récupérer en moyenne chaque jour 3 millions de données concernant des Français (conversations téléphoniques, SMS, historiques de connexions internet, e-mails échangés…).


Une écoute téléphonique dans le film « Le quatrième protocole » de John Mackenzie (1987) (AFP)

2. Ecouter Skype, Whatsapp et BBM
Les autorités françaises peuvent mettre en place des écoutes, sur simple décision administrative. Mais cette capacité d'écouter aux portes devrait s'étendre. Le projet de loi souhaite étendre les interceptions également aux SMS et aux e-mails. De plus, un discret amendement au projet de loi Macron va permettre d'étendre les écoutes aux services internet. A terme, les services pourront écouter/lire les conversations sur Skype, Hangout de Google, Whatsapp, WeChat, Line, Facebook Messenger, Viber, BBM, etc.
Microsoft aime à rappeler que, sur son service Skype, deux clefs de chiffrement aléatoires et inconnues de l'entreprise sont créées à chaque conversation, rendant techniquement impossible de brancher des écoutes. Seulement, l'argumentaire a été mis à mal à la suite d'une polémique en 2012 où le site Slate expliquait que des dispositifs techniques avaient été mis en place pour faciliter les interceptions de communication. L'année suivante, le « New York Times » révélait que Skype aidait les forces de l'ordre américaines à accéder aux données de ses clients.

3. La mallette qui écoute tout
Si l'écoute classique ne suffit pas, les services peuvent faire appel à une précieuse mallette : l'IMSI-catcher (parfois aussi désignée par sa marque, StingRay). Cet appareil permet de capter et d'enregistrer toutes les communications (appels, SMS) des téléphones à proximité. Techniquement, il se fait passer pour l'antenne de l'opérateur pour faire transiter par son disque dur toutes les conversations. Il suffit alors de se trouver à portée d'un suspect pour l'écouter.
Une solution largement utilisée par les agences de renseignement dans le monde entier. Aux Etats-Unis, pas moins de 46 agences locales dans 18 Etats y ont recours. Il faut dire que l'IMSI-catcher est plus accessible que jamais : il faut compter 1.800 dollars pour acquérir une mallette prête à l'emploi sur internet, selon « Wired ».

Le projet de loi du gouvernement prévoit d'autoriser leur utilisation par les services français, après avoir reçu l'aval d'un juge.
La NSA aurait même poussé le concept d'IMSI-catcher plus loin puisque, selon des documents d'Edward Snowden, la police fédérale américaine (US Marshall) utilise de petits avions de tourisme dotés de la même technologie afin de capter les communications de suspects.

4. L'aide des hackers
A l'image de James Bond, les services secrets peuvent utiliser micros et caméras pour surveiller des suspects. Ils peuvent aussi utiliser des balises GPS afin de les géolocaliser « en temps réel ». Des dispositifs que le projet de loi français entend légaliser. Mais il souhaite aller plus loin et permettre l'usage de logiciels espions.

Intitulés « keyloggers », ces logiciels-mouchards permettent de recopier en temps réel tout ce qui se passe sur un ordinateur, un smartphone ou une tablette. La navigation internet, les mots de passe saisis, les fichiers stockés… tout est accessible. Le texte du gouvernement précise que « des agents spécialement habilités » pourront « poser, mettre en œuvre ou retirer les dispositifs de captation ». Concrètement, des hackers des services de renseignement pirateront en toute légalité les machines des suspects pour mieux les espionner.

Issue du monde du piratage informatique, la pratique a fait des émules dans les services de renseignement. La NSA aurait ainsi développé un ver informatique, caché dans les disques durs vendus, capable d'espionner tous les faits et gestes, mais aussi de voler n'importe quel document de dizaine de milliers d'ordinateurs à travers le monde.

Mais la France n'est pas en reste puisque deux rapports indiquent que les services de renseignement hexagonaux ont développé leur propre logiciel malveillant, baptisé « Babar », qui renferme un keylogger. Objectif : écouter les conversations en ligne sur Skype, Yahoo Messenger et MSN, mais aussi de savoir quels sites ont été visités.

5. Ecouter autour du téléphone, même éteint
Le téléphone portable est décidément devenu le meilleur ami des agences de renseignement. Outre les écoutes et la géolocalisation, le mobile peut facilement se transformer en micro, même s'il est éteint.

Des documents d'Edward Snowden ont ainsi mis en lumière que la NSA (encore et toujours) est capable d'installer à distance un programme fantôme sur un portable afin de le transformer en espion. Le magazine « Wired » qui rapporte l'information n'entre pas dans les détails, mais ce ver permet de faire croire que l'appareil s'éteint alors qu'il continue de transmettre des informations (sur son contenu notamment). Pour s'en prémunir, la seule solution est de retirer la batterie.

Des hackers ont fait savoir depuis longtemps qu'il est possible de pirater un téléphone et d'en faire un véritable mouchard : écoute des appels, copie des SMS, géolocalisation, écouter les sons environnant (dans un rayon de 5 à 8 mètres), enregistrer la vidéo captée par l'objectif… Et la fonction micro fonctionne même si l'appareil est éteint (mais conserve sa batterie). Une fonction qui a sûrement déjà séduit des agences de renseignement à travers le monde.

6. La carte des interactions humaines
La NSA a aussi un appétit vorace pour les métadonnées. Tous les échanges électroniques (appels, SMS, e-mails, surf sur internet) colportent également des détails sur ceux-ci : qui communique avec qui, à quelle heure, pendant combien de temps, depuis où, etc. Des données qui se rapprochent des fadettes (les factures téléphoniques détaillées) et qui intéressent grandement la NSA.

L'agence a mis en place un programme visant à collecter et à stocker l'ensemble des métadonnées obtenues par les opérateurs télécoms américains. Objectif : constituer une gigantesque base de données permettant, à tout moment, de connaître les interactions entre personnes sur le sol américain. Une idée qui plaît aussi aux renseignements français, déjà experts des fadettes. Le projet de loi souhaite que les autorités puissent avoir accès aux métadonnées d'une personne ciblée sans demander l'avis d'un juge, il suffira d'une autorisation administrative.

Afin de mieux appréhender ce que les métadonnées peuvent dire de nous et de nos interactions, le Massachusetts Institute of Technology (MIT) propose l'outil Immersion qui permet de visualiser sa galaxie de relations basée sur son adresse Gmail de Google.

7. La constitution d'une banque de photos
Toujours selon des documents de Snowden, la NSA collecte chaque jour une quantité astronomique de photos (« des millions d'images ») afin de s'en servir dans le cadre de reconnaissance faciale. Le tout est récupéré dans des e-mails, SMS, sur les réseaux sociaux, via les outils de vidéo-conférences, etc.
Quotidiennement, l'agence obtiendrait 55.000 photos permettant d'identifier des individus, afin d'alimenter une immense banque d'images. L'objectif étant de pouvoir identifier rapidement un suspect, en particulier quand la banque d'images des photos de passeports ne suffit pas.

8. Fouiner dans les téléchargements illégaux
Les téléchargements illégaux peuvent aussi aider les autorités, ou du moins les aiguiller. Un document d'Edward Snowden a révélé que les services secrets canadiens ont chaque jour scruté l'ensemble des téléchargements réalisés sur des plateformes comme MegaUpload ou RapidShare, afin de repérer les manuels et documents édités par des groupes terroristes, afin d'identifier leurs auteurs et ceux qui les consultent. Ils produisaient alors une liste de suspects, transmise à leurs alliés, dont les Etats-Unis. En somme, une aiguille dans une botte de 10 à 15 millions de téléchargements quotidiens.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://tempsreel.nouvelobs.com/tech/20150317.OBS4818/les-8-techniques-les-plus-ahurissantes-des-espions-d-aujourd-hui.html
Par Boris Manenti