La surveillance internationale de masse refait surface | Le Net Expert Informatique

La surveillance internationale de masse refait surface

Après la censure partielle de la très contestée loi sur le renseignement, qui a été validée dans sa quasi-totalité par le Conseil Constitutionnel le 23 juillet dernier, la surveillance des communications internationales refait surface sous la forme d'une proposition de loi. En laissant au parlement le soin de présenter un texte rustine, le gouvernement agit à distance (ni projet de loi, ni étude d'impact) pour autoriser et encadrer la surveillance massive. Ce jeudi 1er octobre 2015 à l'Assemblée nationale, l'examen en séance publique du texte a débuté.

Compléter la loi sur le renseignement

La procédure est accélérée… Le texte relatif aux mesures de surveillance des communications électroniques internationales est présenté par les députés SRC Patricia Adam et Philippe Nauche de la Commission de la défense nationale et des forces armées de l'Assemblée. Ce texte prévoit la création d'un « cadre spécifique » à la surveillance des communications internationales (soit l'émission ou la réception d'une communication depuis l'étranger). Pour ses promoteurs, les services de renseignement français doivent pouvoir assurer, dans un cadre légal, cette surveillance « aux fins de défense et de promotion des intérêts fondamentaux de la Nation ».

Les « correspondances » (contenus) et les « données de connexion » (métadonnées) sont incluses dans la proposition. Par ailleurs, à la différence des interceptions de sécurité, les autorisations de surveillance délivrées par le Premier ministre « ou l'un de ses délégués », ne seront pas soumises à l'avis préalable de la Commission nationale de contrôle des techniques de renseignement (CNCTR). De plus, l'article 1er du texte, qui modifie le chapitre IV du titre V du livre VIII du code de la sécurité intérieure, « autorise l'exploitation non-individualisée des données de connexion interceptées ». La Commission de la défense a repoussé, mercredi 30 septembre, tous les amendements proposés par les députés Les Républicains Laure de La Raudière et Lionel Tardy et par l'écologiste Sergio Coronado (avec d'autres parlementaires). Seuls les amendements de forme ont été conservés.

Prévoir des exceptions… limitées

Amnesty International condamne un texte aux « motifs vastes et peu précis » qui « légalise la surveillance de masse », sans voie de recours. La surveillance à grande échelle, déjà présente dans la loi renseignement du 24 juillet 2015, ne viserait plus seulement l'antiterrorisme mais pourrait « être justifiée pour l'ensemble des finalités mentionnées à l'article 811-3 de la Code de la sécurité intérieure, y compris la défense et la promotion des intérêts majeurs de politique étrangère, économique et scientifique».

Une organisation, une entreprise ou un particulier qui communiquerait en France avec l'étranger ou recevrait une communication émise depuis l'international, pourrait donc tomber sous le coup de cette loi. Seuls les parlementaires, les magistrats, les avocats ou les journalistes qui exercent en France, pourraient théoriquement bénéficier d'une forme de protection…

Dans une tribune, des organisations citoyennes font le même constat. Elles jugent, par ailleurs, que « la période prévue pour la conservation des données est clairement injustifiée, excessive (un an pour le contenu, six ans pour les métadonnées et huit ans pour les communications chiffrées) et en contradiction avec les principes posés par la Cour de justice de l'Union européenne dans son arrêt du 8 avril 2014. » Un point de vue partagé par l'association de défense des droits et libertés La Quadrature du Net. L'Observatoire des Libertés et du Numérique (OLN), dont elle fait partie, appelle les élus à rejeter la proposition de loi et le gouvernement à ouvrir un débat public sur la surveillance internationale.

Source : http://www.silicon.fr/loi-surveillance-communications-electroniques-internationales-127920.html

AVG envisage de vendre certaines données des utilisateurs aux annonceurs en ligne, pour financer ses produits gratuits | Le Net Expert Informatique

	AVG envisage de vendre certaines données des utilisateurs aux annonceurs en ligne, pour financer ses produits gratuits

La firme de sécurité tchèque AVG Technologies a annoncé dans un billet de blog des changements dans la collecte et l'utilisation des données de ses utilisateurs à des fins commerciales. Ces changements s'inscrivent dans une récente révision de la politique de confidentialité d'AVG, qui est censée prendre effet à partir du 15 Octobre prochain.

Dans sa nouvelle politique, le fabricant d'antivirus explique le besoin de collecter certaines données des utilisateurs. En général, les firmes de sécurité à l'instar de la société tchèque collectent certaines données des utilisateurs dans le but d'améliorer les produits et services offerts. Il s'agit entre autres des données relatives aux menaces de logiciels malveillants potentiels, des informations sur la façon dont les produits et leurs caractéristiques sont utilisés, ou encore les informations géographiques des utilisateurs des différentes produits et services.

A cette liste, AVG envisage d'ajouter des informations supplémentaires dans le but de financer certains de ses produits gratuits afin qu'ils le restent toujours. La société s'intéresse particulièrement à l'ID de publicité associé aux terminaux des utilisateurs, les historiques de recherche et de navigation, y compris les métadonnées, ainsi que les informations sur les fournisseurs de services Internet ou les réseaux mobiles utilisés pour se connecter à ses produits. AVG Technologies va également collecter les informations concernant d'autres applications que vous pourriez avoir sur votre appareil et comment vous les utiliser.

Visiblement, la société pourrait les vendre aux annonceurs en ligne qui se présentent comme des demandeurs potentiels de ces informations, qui pourraient leur permettre de diffuser des annonces ciblées. A ce sujet, la société explique dans un billet de blog que c'est une pratique générale pour les produits logiciels et sites web de collecter les données des utilisateurs. « Les données d'utilisation leur permettent de personnaliser l'expérience de leurs clients et partager également des données avec des tiers qui leur permettent d'améliorer ou de développer de nouveaux produits », explique AVG. Le fabricant d'antivirus rappelle d'ailleurs que c'est cette pratique qui permet aux annonceurs de savoir où placer les bannières publicitaires, et que même chez AVG, les données non personnellement identifiables sont recueillies dans le cadre des performances des applications.

AVG précise toutefois que « les données personnellement identifiables ne seront vendues à quiconque, y compris les annonceurs ». Certaines de ces données pourraient toutefois être partagées avec des collaborateurs et filiales de la société à des fins de statistiques et de recherche, mais avec des restrictions.

Face à la possibilité qu'il puisse y avoir une fuite des données personnellement identifiables via les historiques de navigation par exemple, le fabricant d'antivirus dit qu'il va prendre des mesures de précaution pour filtrer ces informations avant de vendre l'historique de navigation des utilisateurs.

Toutefois, cette nouvelle politique ne devrait pas être imposée aux utilisateurs des produits gratuits ciblés par la société. En effet, AVG explique que le délai accordé avant l'entrée en vigueur de sa nouvelle politique de confidentialité a été défini pour permettre aux utilisateurs d'en prendre connaissance afin de décider s'ils veulent participer à ce programme de collecte de données « anonymisées ». Si la société se réserve le droit de modifier sa politique à n'importe quel moment, elle confirme par contre qu'à l'heure actuelle, aucun partage des données ne se fera jusqu'à ce que ses clients soient en mesure de faire ce choix.

Source :
http://www.developpez.com/actu/90118/AVG-envisage-de-vendre-certaines-donnees-des-utilisateurs-aux-annonceurs-en-ligne-pour-financer-ses-produits-gratuits/

Replay de l'émission Infrarouge du 22 septembre : On nous écoute : Cyberguerre,

l’arme fatale ? – 1ère partie | Le Net Expert Informatique

	Replay de l’émission Infrarouge du 22 septembre : On nous écoute : Cyberguerre, l’arme fatale ? – 1ère partie

« Plus rien ne peut rester secret, même nos vies. Parano de grande ampleur ? Complot d'état ?

Quelle est la réalité de la plus grande campagne de surveillance jamais élaborée ? » Edward Snowden, est interviewé en exclusivité à Moscou pour le documentaire. Pour faire suite à notre article « Emission Infrarouge sur France 2 ce mardi à 22h50 : On nous écoute : Cyberguerre, l'arme fatale ? – 1ère partie » du 21 septembre dernier, nous vous mettons à disposition le replay de cette superbe émission.

A l'heure où la France vient de voter la très contestée Loi sur le Renseignement, où le hacking, le tracking et la cyber-surveillance font partie des grands débats de nos sociétés, où les révélations d'Edward Snowden ont enflammé la planète, les questions que posent ces 2 films deviennent incontournables.
Sommes-nous tous des coupables potentiels à surveiller ? Faudra-t-il abandonner notre présomption d'innocence pour une sécurité dont tout le monde sait qu'elle ne peut pas être totale ? Comment contrôler les services de renseignements sans les empêcher de travailler efficacement ? Et sommes-nous prêts à protéger nos propres lanceurs d'alerte face aux pressions récurrentes d'un Etat-surveillance de plus en plus puissant ?

Une série documentaire inédite (2X52′) écrite et réalisée par Pierre-Olivier François
Une coproduction Artline Films, WGBH Frontline et NOVA
Produit par Olivier Mille
Avec la participation de France Télévisions
Avec le soutien du Centre National du Cinéma et de l'Image Animée
Unité de programmes documentaires de France 2 : Fabrice Puchault et Barbara Hurel
La case Infrarouge invite les téléspectateurs à réagir et commenter les documentaires en direct sur twitter via le hashtag #infrarouge

---

Source : http://www.france2.fr/emissions/infrarouge/diffusions/22-09-2015_341460

L’essor du chiffrement inquiète le renseignement anglais | Le Net Expert Informatique

L’essor du chiffrement inquiète le renseignement anglais

Dans une interview à la BBC, le patron du renseignement intérieur britannique (MI5) a exprimé ses inquiétudes à l'égard de l'évolution des technologies de chiffrement. Selon lui, les entreprises technos ont le devoir éthique d'informer les autorités de menaces potentielles.

Le gouvernement britannique n'en démord pas et veut ses backdoors : dans une interview donnée à la BBC, le dirigeant du MI5, les services de sécurité de la Grande-Bretagne, évoque à nouveau le débat autour des technologies de chiffrement qui se développent à destination du grand public.

Pour Andrew Parker, directeur du MI5, les services de police ont de plus en plus de mal à obtenir des informations en ligne et les entreprises du secteur technologique devraient selon lui informer les agences de renseignement des potentielles menaces détectées via leurs outils. Il explique au micro de la BBC que les services de police sont confrontés à la difficulté croissante d'obtenir « les relevés de communications des utilisateurs suspectés d'activités terroristes, et ce même en disposant d'un mandat de justice. »

Haro sur le chiffrement

Une critique déjà entendue fréquemment et qui fait écho au développement d'outils de chiffrement de bout-en-bout, mouvement qui gagne en intensité dans l'industrie des nouvelles technologies et des services en ligne suite aux révélations d'Edward Snowden.

Et la problématique n'est cantonnée Outre-Manche, où David Cameron a annoncé son intention de légiférer sur le sujet. Aux États Unis, on a ainsi pu voir les dirigeants du FBI exprimer une demande similaire, évoquant la possibilité de mettre en place des backdoors connues des seuls services de renseignement afin de pouvoir accéder aux données échangées sur les plateformes de messagerie en ligne. En France, c'est le procureur de la République de Paris qui s'y colle : celui-ci avait signé en août une tribune dans le New York Times déplorant l'essor du chiffrement et l'obstacle que celui-ci constituait dans les enquêtes judiciaires.

Face à cette offensive, les défenseurs de la cryptographie s'inquiètent tout particulièrement des conséquences que pourrait apporter la mise en œuvre d'une telle volonté politique : pour Bruce Schneier, expert américain de la cryptographie, s'appuyer sur ce type de procédé viendrait immanquablement contredire le principe même de la cryptographie, supposé garantir la sécurité des échanges entre les destinataires. De plus, et l'affaire récente des clefs d'accès aux cadenas TSA le rappelle bien : les backdoors ne sauraient garantir que la personne qui les utilise est bien un représentant des forces de l'ordre, laissant la possibilité à des cybercriminels ou à des pays étrangers de les exploiter.

Source :
http://www.zdnet.fr/actualites/le-renseignement-anglais-s-inquiete-lui-aussi-de-l-essor-du-chiffrement-39825120.htm

---

Cyberespace : les USA et la

Chine font la paix | Le Net Expert Informatique

Cyberespace : les USA et la Chine font la paix

L**e New York Times informe qu'un accord de non-agression contre les sites d'infrastructure critique en temps de paix devrait être signé au cours de la visite du président chinois Xi Jinping aux États-Unis la semaine prochaine.**

Plus tôt, le président américain Barack Obama avait parlé du risque d'aggravation des relations bilatérales en cas d'impossibilité de trouver un terrain d'entente. Au printemps, un tel accord avait déjà été signé entre la Russie et la Chine. Un nouveau régime international de conduite des pays dans le cyberespace pourrait ainsi voir le jour progressivement.

Les représentants de la Chine et des USA mènent des négociations sur un accord les engageant mutuellement à ne pas porter d'attaques cybernétiques contre des sites d'infrastructure critique en temps de paix. Cet accord visera à prévenir les attaques contre les centrales électriques, les systèmes bancaires, les réseaux téléphoniques et les hôpitaux. Les sources du NYT auprès de l'administration du président américain soulignent que ce document devrait contenir peu d'aspects concrets. Il impliquera très probablement des engagements sur le respect des principes et des règles de conduite dans le cyberespace adoptés par un groupe d'experts gouvernementaux de l'Onu en juin dernier.

L'accord en question ne devrait pas concerner l'espionnage industriel des sites commerciaux qui, selon les USA, constituent la grande partie des intrusions chinoises. Ces derniers temps, ce problème est devenu central dans les relations bilatérales. « A un certain moment nous commencerons à considérer les cyberattaques comme une menace à la sécurité nationale et nous y réagirons en conséquence », a déclaré le 11 septembre Barack Obama à Fort Meade devant les militaires américains. Le 16 septembre, il déclarait aussi aux représentants de la communauté d'affaires: « Nous avons préparé plusieurs mesures appelées à montrer que si cette question n'était pas réglée, elle compliquerait considérablement les relations bilatérales ».
Les opinions exprimées dans ce contenu n'engagent que la responsabilité de l'auteur.

Source : http://fr.sputniknews.com/presse/20150921/1018285357/cyberespace-usa-chine.html
Par Kommersant

Emission Infrarouge sur France 2 ce mardi à 22h50 : On nous écoute : Cyberguerre, l'arme fatale ? – 1ère partie | Le Net Expert Informatique

Emission Infrarouge sur France 2 ce mardi à 22h50 : On nous écoute : Cyberguerre, l'arme fatale ? – 1ère partie

« Plus rien ne peut rester secret, même nos vies. Parano de grande ampleur ? Complot d'état ? Quelle est la réalité de la plus grande campagne de surveillance jamais élaborée ? »
Edward Snowden, est interviewé en exclusivité à Moscou pour le documentaire.A l'heure où la France vient de voter la très contestée Loi sur le Renseignement, où le hacking, le tracking et la cyber-surveillance font partie des grands débats de nos sociétés, où les révélations d'Edward Snowden ont enflammé la planète, les questions que posent ces 2 films deviennent incontournables.

Sommes-nous tous des coupables potentiels à surveiller ? Faudra-t-il abandonner notre présomption d'innocence pour une sécurité dont tout le monde sait qu'elle ne peut pas être totale ? Comment contrôler les services de renseignements sans les empêcher de travailler efficacement ? Et sommes-nous prêts à protéger nos propres lanceurs d'alerte face aux pressions récurrentes d'un Etat-surveillance de plus en plus puissant ?

Une guerre d'un nouveau genre a vu le jour, qui bouleverse les règles et les enjeux des conflits traditionnels. Internet est en train de modifier totalement les champs de bataille, de brouiller les frontières entre alliés et ennemis, entre espionnage et sabotage, entre guerre et paix. Pas avec des armes lourdes mais avec des codes et des virus de plus en plus sophistiqués pour déstabiliser, prendre le contrôle ou détruire des centrales électriques ou nucléaires, un réseau ferroviaire, un ministère, des ordinateurs de guidage …

Nos armées se dotent de moyens toujours plus sophistiqués pour lutter contre un ennemi inconnu, invisible et imprévisible. Comment se défendre ? Comment attaquer ?

De nos choix dépendra la société dans laquelle nous vivrons à l'avenir.

Une série documentaire inédite (2X52′) écrite et réalisée par Pierre-Olivier François
Une coproduction Artline Films, WGBH Frontline et NOVA
Produit par Olivier Mille
Avec la participation de France Télévisions
Avec le soutien du Centre National du Cinéma et de l'Image Animée
Unité de programmes documentaires de France 2 : Fabrice Puchault et Barbara Hurel
La case Infrarouge invite les téléspectateurs à réagir et commenter les documentaires en direct sur twitter via le hashtag #infrarouge

---

Source : http://www.france2.fr/emissions/infrarouge/diffusions/22-09-2015_341460

Implantation de malwares dans les routeurs Cisco| Le Net Expert Informatique

	**Implantation de malwares dans les routeurs Cisco**

La firme de sécurité Mandiant, filiale de FireEye, a découvert que les firmwares de 14 routeurs d'entreprise de Cisco avaient été remplacés par des versions malveillantes permettant d'ouvrir des backdoors et de compromettre d'autres systèmes.

Remplacer le firmware d'un routeur par une version contaminée n'est plus du tout un risque théorique. Les chercheurs de la société Mandiant, spécialisée dans la sécurité informatique, ont détecté une véritable attaque ayant conduit à installer un faux firmware sur des routeurs d'entreprise dans quatre pays. Le logiciel implanté, désigné sous le nom de SYNful Knock, permet à des attaquants de disposer ainsi d'une porte dérobée, avec des accès à privilèges élevés, pour s'introduire dans les équipements affectés et y rester. La « backdoor » est en effet maintenue, même après un redémarrage du routeur. C'est un élément différentiant et inquiétant par rapport aux malwares que l'on trouve sur les routeurs grand public et qui disparaissent de la mémoire lorsque le périphérique est relancé.

SYNful Knock se présente comme une modification du système d'exploitation IOS (Internetwork Operating System) qui tourne sur les routeurs professionnels et les commutateurs de Cisco. A ce jour, les chercheurs de Mandiant l'ont découvert sur les routeurs ISR (Integrated Service Routeurs) modèles 1841, 8211 et 3825 que les entreprises placent en général dans leurs succursales ou qui sont utilisés par les fournisseurs de services réseaux managés.

Des experts de Mandiant mettent en garde contre de faux firmwares qui implantent des portes dérobées dans plusieurs modèles de routeurs Cisco : ISR 1841 (ci-dessus), 8211 et 3825. (crédit : D.R.)

Défaut ou vol de certificats d'administration

Filiale de la firme de cybersécurité FireEye, Mandiant a trouvé le faux firmware sur 14 routeurs, au Mexique, en Ukraine, en Inde et aux Philippines. Les modèles concernés ne sont plus vendus par Cisco, mais il n'y a aucune garantie que d'autres modèles ne seront pas ciblés à l'avenir ou qu'ils ne l'ont pas déjà été. Cisco a publié une alerte de sécurité en août avertissant ses clients sur de nouvelles attaques sur ses routeurs.

Dans les cas étudiés par Mandiant, SYNful Knock n'a pas été exploité en profitant d'une faille logicielle, mais plus probablement à cause d'un défaut de certificats d'administration ou via des certificats volés. Les modifications effectuées sur le firmware n'ont pas modifié sa taille d'origine. Le logiciel qui prend sa place installe une backdoor avec mot de passe ouvrant un accès Telnet à privilèges et permettant d'écouter les commandes contenues dans des packets TCP SYN (d'où le noom SYNful Knock). La procédure peut être utilisée pour indiquer au faux firware d'injecter des modules malveillants dans la mémoire du routeur. Toutefois, contrairement à la porte dérobée, ces modules ne résistent pas à un redémarrage du périphérique.

Des compromissions très dangereuses

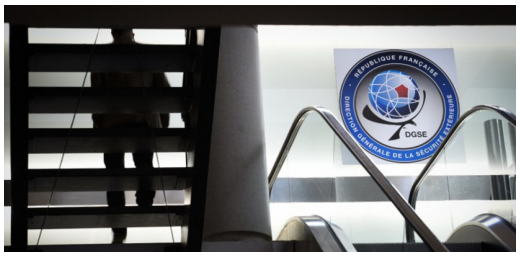
Les compromissions de routeurs sont très dangereuses parce qu'elles permettent aux attaquants de surveiller et modifier le trafic réseau, de diriger les utilisateurs vers de faux sites et de lancer d'autres attaques contre des terminaux, serveurs et ordinateurs situés au sein de réseaux isolés. Généralement, les routeurs ne bénéficient pas du même degré d'attention que d'autres équipements, du point de vue de la sécurité, car ce sont plutôt les postes de travail des employés ou les serveurs d'applications que les entreprises s'attendent plutôt à voir attaqués. Les routeurs ne sont pas protégés par des utilitaires anti-malwares ni par des pare-feux.

« Découvrir que des backdoors ont été placées dans votre réseau peut se révéler très problématique et trouver un implant dans un routeur, encore plus », soulignent les experts en sécurité de Mandiant dans un billet. « Cette porte dérobée fournit à des attaquants d'énormes possibilités pour propager et compromettre d'autres hôtes et des données critiques en utilisant ainsi une tête de pont particulièrement furtive ». Dans un livre blanc, Mandiant livre des indicateurs pouvant être utilisés pour détecter des implants SYNful Knock, à la fois localement sur les routeurs et au niveau du réseau. « Il devrait être évident maintenant que ce vecteur d'attaque est vraiment une réalité et que sa prévalence et sa popularité ne feront qu'augmenter », préviennent les experts. A la suite de l'information diffusée par Mandiant, Cisco a lui aussi communiqué sur le sujet, en fournissant des explications complémentaires.

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.lemondeinformatique.fr/actualites/lire-des-malwares-implantes-dans-les-routeurs-cisco-62359.html?utm_source=mail&utm_medium=email&utm_campaign=LeNetExpert.fr
Par Lucian Constantin / IDG News Service (adapté par Maryse Gros)

En exclusivité, la nouvelle loi sur les écoutes de la DGSE – L'Obs | Le Net Expert Informatique



En exclusivité, la nouvelle loi sur les écoutes de la DGSE

La commission de la Défense de l'Assemblée Nationale rendra publique, jeudi 10 septembre, une proposition de loi très sensible dont « L'Obs » a pu se procurer le texte. Celui-ci définit les modalités d'autorisation et de contrôle des écoutes internationales de la DGSE et de ce fait les légalise pour la première fois.

Cette proposition de loi (dite « relative aux mesures de surveillance des communications électroniques internationales ») fait suite au rejet, le 23 juillet, par le Conseil Constitutionnel des dispositions sur le même sujet inscrites dans la loi sur le renseignement.

L'article avait été retoqué par les Sages au motif notamment qu'il renvoyait à un décret secret (dont « l'Obs » avait révélé l'existence). La représentation nationale n'avait donc pas une idée assez précise du fonctionnement de ces grandes oreilles ni de leur contrôle. Cette nouvelle proposition de loi répond, semble-t-il, à l'exigence de (relative) transparence formulée par le Conseil Constitutionnel.

La proposition de loi apporte les clarifications suivantes :

La France préservée

Il est redit qu'il s'agit des communications « émises ou reçues de l'étranger » et que la DGSE ne peut cibler la France. Plus précisément, le texte stipule que si, du fait du trajet aléatoire des signaux électroniques, le service de renseignement intercepte des communications échangées entre personnes ou équipement « utilisant des numéros d'abonnement ou des identifiants rattachables au territoire national, y compris lorsque ces communications transitent par des équipements non rattachables à ce territoire, ces interceptions sont instantanément détruites. »

Le Premier ministre au centre du dispositif

Cet article est le plus important pour la DGSE. Il stipule que la décision générale d'écouter tel ou tel « système de communication » revient au Premier ministre qui en assume donc la responsabilité. Autrement dit, c'est le chef du gouvernement qui désormais autorise l'interception des flux provenant des satellites de communication et des câbles sous-marins.

Cette disposition oblige également la DGSE à obtenir l'autorisation des Premiers ministres futurs si elle veut écouter de nouveaux moyens de communication. Le but est notamment d'éviter que ne se reproduise l'épisode de 2008. A l'époque, la loi ne permettait pas à la DGSE d'écouter les câbles sous-marins. Pour passer outre, elle avait obtenu à l'insu de la représentation nationale la signature du décret secret évoqué dans la précédente mouture de la loi.

Le big data légalisé

Le Premier ministre « autorise l'exploitation non individualisée des données de connexion interceptées ». Il s'agit de la reconnaissance publique que la DGSE intercepte des flux et pas seulement des communications individuelles et qu'elle analyse les « big data » ainsi récoltées. Le texte ajoute que « ces autorisations [délivrées pour un an] déterminent la ou les finalités poursuivies ainsi que les types de traitements automatisés pouvant être mis en œuvre. »

Les pays cibles des grandes oreilles

Le paragraphe le plus novateur stipule que le Premier ministre autorise l'écoute de « zones géographiques [donc des pays ou des régions] », d' »organisations », de « personnes » ou de « groupes de personnes ». C'est la première fois qu'un texte officiel confirme que la France écoute elle aussi le monde, que la DGSE agit comme la NSA (avec, certes, moins de moyens). On remarquera que le législateur n'interdit pas l'écoute de dirigeants étrangers, ennemis ou amis…

Contrôle théorique

La Commission Nationale de Contrôle des Techniques de Renseignement (CNCTR) « dispose d'un accès permanent, complet et direct aux renseignements collectés, aux transcriptions et extractions réalisées […] et peut contrôler à sa demande les dispositifs techniques ». Sur le papier, les écoutes de la DGSE sont donc bien contrôlées. Tout dépendra des moyens dont la future CNCTR va disposer.

Destruction possible

La CNCTR peut recommander au Premier ministre la destruction d'écoutes non conformes. Si celui-ci refuse, elle peut saisir le Conseil d'Etat pour trancher. Une disposition originale.

Recours individuel

Comme pour les écoutes intérieures, « toute personne souhaitant vérifier qu'aucune mesure de surveillance [par la DGSE] n'est irrégulièrement mise en œuvre à son égard » peut saisir la CNCTR. Celle-ci notifie à la personne en question qu'il a procédé aux vérifications nécessaires « sans confirmer ou infirmer la mise en œuvre de mesures de surveillance ».

Délais de conservation

La loi définit des délais de conservation des interceptions qui s'étalent entre un an pour les communications à huit pour les renseignements chiffrés en passant par six pour les données de connexion.

Le texte du projet de loi :
proposition loi surveillance publié par NouvelObs.com

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://tempsreel.nouvelobs.com/monde/20150909.OBS5547/exclusif-la-nouvelle-loi-sur-les-ecoutes-de-la-dgse.html
Par Vincent Jauvert

Le certificat électronique est une arme efficace contre la Cybercriminalité | Le Net Expert Informatique

	Le certificat électronique est une arme efficace contre la Cybercriminalité

Lutter contre la cybercriminalité est un axe stratégique pour les entreprises et les institutions. En effet, nous assistons quotidiennement à des attaques toujours plus sophistiquées qui viennent durablement compromettre l'intégrité et la confidentialité des échanges réalisés sur le net. Bien entendu, nombre d'entreprises et d'institutions mettent en place des dispositifs pour se protéger, mais en laissant «certains trous dans la raquette» qui sont immédiatement utilisés par les pirates pour mener à bien leurs actions.

Très répandues, ces pratiques créent des désastres financiers et montrent bien que les flux sortants sont tout aussi exposés que les flux entrants. Il est donc nécessaire de les prendre en compte dans la mise en œuvre de dispositifs de protection efficace.

L'usage du certificat électronique ID (pour personne physique) est la piste à privilégier. Il est d'ailleurs largement plébiscité par l'Etat et les collectivités avec la norme RGS. Véritable rempart contre l'usurpation d'identité, il permet au destinataire d'un mail d'en vérifier l'émetteur, il permet également de garantir la confidentialité des données échangées. L'autre avantage tient à sa simplicité d'utilisation sur les mobiles et tablettes. Avec un certificat, les envois de mails à partir d'un smartphone ne représentent plus une faille de sécurité mais sont protégés efficacement.

Au regard de ces éléments, institutions et entreprises doivent accélérer le déploiement de certificats pour sécuriser leurs échanges de données. Une prise de conscience dans ce domaine permet de colmater des brèches importantes et complète des dispositifs traditionnels de type Firewall qui jouent pour leur part un rôle de filtrage pour les données entrantes. Avec les certificats électroniques, les flux sortants sont parfaitement sécurisés, leur apport dans la lutte contre la cybercriminalité est donc stratégique, d'autant que leur coût d'acquisition n'est pas onéreux.

Source : http://www.edubourse.com/finance/actualites.php?actu=89518

Votre frappe au clavier vous identifie tout aussi efficacement qu'une écriture

à la main | Le Net Expert Informatique

Votre frappe au clavier vous identifie tout aussi efficacement qu'une écriture à la main

Des chercheurs français ont mis au point un logiciel capable de reconnaître avec précision un utilisateur qui tape au clavier d'ordinateur. Une possibilité qui permet de sécuriser des opérations mais qui supprime aussi l'anonymat sur Internet.

Webcam débranchée, pare-feu, IP masquée, VPN… Les internautes aguerris et concernés par leur anonymat sur internet connaissent le minimum requis pour se fondre dans les méandres du web. Qu'ils soient honnêtes ou malhonnêtes, ils pourront bientôt être identifiés et cela n'a plus rien à avoir avec un quelconque logiciel de pistage. Ce qui va trahir les internautes, ce sont leurs doigts. Ou plutôt la façon dont ils vont les utiliser sur leur clavier. Des chercheurs français du Groupe de recherche en informatique image automatique et instrumentation de Caen (Greyc) ont ainsi développé un petit logiciel pilote qui permet de différencier avec une grande précision les différents internautes qui tapent sur leur clavier.
Pour cela, le programme repère la pression exercée sur les touches, le temps d'appui et surtout les délais, très courts, entre chaque touche. Telle une graphologie moderne, tous ces critères s'avèrent très différents en fonction des personnes et permet de donner un profil précis.
« Ce n'est pas nouveau » remarque Jean-Paul Pinte, docteur en information scientifique et technique et maître de conférences à l'Université Catholique de Lille. « Avant l'arrivée des claviers, pendant la Seconde Guerre Mondiale, les opérateurs de renseignement britanniques écoutaient les opérateurs de code morse allemands. La vitesse de code, les erreurs de frappe permettait de différencier les opérateurs. »
Au cours des années 2000, avec l'avènement d'internet, la « frappologie » a été de plus en plus étudiée, dans le même esprit que la graphologie, censée apporter des informations sur la personnalité d'une personne. « C'est surtout dans l'espionnage que cette biométrie dite douce a pris racine mais elle est de plus en plus pratiquée dans le monde du recrutement » souligne Jean-Paul Pinte. Sauf que les techniques se sont largement améliorées et les recherches du Greyc et d'autres chercheurs dépassent le cadre du simple profiling de personnes.

Le but est avant tout de toujours mieux crypter les données. Ainsi, même en connaissant le mot de passe de sa victime, un usurpateur ne passerait pas entre les mailles du filet sécuritaire puisque sa façon de taper le mot magique serait forcément différente de celle du véritable utilisateur.

Mais ce système offre aussi des perspectives plus sombres car il permet d'identifier une personne à coup sûr, malgré tous ses efforts pour rester anonymes.

Il suffit que plusieurs gros sites s'y mettent et les voilà en possession de toutes les pages visitées par une même personne, identifiée par son clavier. Dans ce cas, l'adresse IP n'aurait plus vraiment d'enjeu. Et ce ne sont pas les réseaux masqués, comme le célèbre TOR qui empêcheront cela. Runa Sandvik, un chercheur indépendant interrogé par le site Arstechnica, a tenté l'expérience et s'est rendu compte que le système chargé normalement de le maintenir anonyme, n'a pas pu lutter. « Aujourd'hui, tout est possible même avec TOR » souligne Jean-Paul Pinte. « La recherche évolue dans le domaine car il faut savoir que l'anonymat n'existe pas vraiment sur la toile. »

L'entreprise suédoise BehavioSec met d'ailleurs à disposition un site d'essai pour évaluer l'efficacité du système pour un site de vente en ligne. Au bout de 3 formulaires (similaires) remplis, le programme était capable de retrouver l'utilisateur dans 75% des cas ultérieurs… Cela concerne les internautes attachés à leur anonymat mais aussi les dissidents politiques de certains pays qui surveillent la toile.

Mais d'ores et déjà, la riposte s'organise. Les chercheurs Per Thorsheim et Paul Moore ont développé un petit plugin pour le navigateur de Google Chrome qui permet de crypter les informations liées au clavier. Si le programme est encore en phase de test, il pourrait être une nouvelle protection à ajouter pour qu'internet reste un espace de liberté.

Source : http://www.atlantico.fr/decryptage/comment-maniere-dont-tapez-votre-clavier-identifie-tout-aussi-efficacement-qu-ecriture-main-2268834.html
Illustration : On peut désormais vous identifier à la manière dont vous tapez sur le clavier de votre ordinateur. Crédit Reuters