La loi sur le renseignement mettra-t-elle en place une « surveillance de masse » ? | Le Net Expert Informatique

	La loi sur le renseignement mettra-t-elle en place une « surveillance de masse » ?

Depuis le début de l'examen, à l'Assemblée nationale puis au Sénat, du projet de loi sur le renseignement, une disposition du texte concentre les critiques et les débats. Il s'agit d'une partie de son article 2, qui permettra aux services de renseignement d'installer des appareils analysant le trafic Internet pour détecter des comportements suspects de terrorisme. Le terme de « boîte noire », d'abord avancé par le gouvernement, est devenu leur nom officieux.

Les détracteurs de la loi y voient, par son caractère systématique et indistinct, l'introduction dans la loi française de la surveillance de masse. Ses partisans refusent le terme. Au Sénat, mardi 2 juin, ils ne sont pas parvenus à trancher ce débat, qui est loin d'être seulement sémantique.

Que dit le projet de loi ?

Le projet de loi sur le renseignement prévoit, en l'état, dans le seul cadre de la lutte contre le terrorisme, la mise en place de « traitements automatisés » sur les réseaux des fournisseurs d'accès à Internet français. Cela signifie que des matériels seront physiquement installés chez les opérateurs, dans lesquels des logiciels – les fameux algorithmes – vont inspecter les flux de données des internautes à la recherche de signaux que les services estiment être avant-coureurs d'un acte terroriste.

Pour les opposants, cela ne fait pas de doute. Si des algorithmes inspectent, automatiquement, l'intégralité des flux qui transitent chez les fournisseurs d'accès à Internet (FAI) à la recherche de comportement suspects, il s'agit d'une mesure de surveillance de masse ; et ce, même s'ils ne sont destinés qu'au repérage de quelques personnes. C'est le cas du sénateur Claude Malhuret (Allier, Les Républicains), joint par Le Monde :

« Ceux qui disent qu'il ne s'agit pas de surveillance de masse disent, à la phrase suivante, qu'il s'agit de chercher une aiguille dans une botte de foin. Mais la botte de foin, c'est l'Internet français ! Les boîtes noires installées chez les FAI analyseront l'intégralité du trafic Internet français. C'est comme les radars sur les principales autoroutes : au bout de quelque temps, tous les Français seront passés devant. Elles cherchent des critères précis, mais en surveillant tout le monde ! »

Difficile en effet de qualifier autrement que « de masse » ce dispositif de surveillance, qui, au minimum, inspectera de très grandes quantités de données pour n'y repérer que quelques activités suspectes.

Ce qualificatif est pourtant violemment récusé par les défenseurs du texte. Le premier ministre, Manuel Valls, a assuré au Sénat mardi 2 juin que le projet de loi « n'exerçait pas de surveillance de masse des Français ». « Le texte n'autorise que de la surveillance ciblée, pas de surveillance de masse » a renchéri son collègue de la défense, Jean-Yves Le Drian.

Pas « d'atteinte à la vie privée »

Le sénateur socialiste du Loiret Jean-Pierre Sueur est du même avis :

« Il ne faut pas faire dire à la loi ce qu'elle ne dit pas. Certains disent que nous pompons les données comme le Patriot Act. C'est faux, c'est quelque chose contre lequel on a toujours été opposés. »

Lorsqu'on lui fait remarquer que pour repérer les suspects dans le flot des connexions, il faudra bien passer en revue toutes les connexions des internautes français, le sénateur dément : « Il ne s'agit pas de tout l'Internet français, mais seulement ceux qui se connectent aux sites terroristes. Notre objectif n'est pas de porter atteinte à la vie privée. » Un exemple d'utilisation des « boîtes noires » qui n'est cependant pas le seul avancé par les promoteurs du dispositif.

La loi ne précise pas les modalités exactes du déploiement de ces « traitements automatisés ». Elle ne limite d'ailleurs pas leur activité à la détection des visiteurs de sites terroristes (dont le blocage est par ailleurs prévu par la loi sur le terrorisme adoptée à la fin de 2014) mais, plus largement, des « connexions susceptibles de révéler une menace terroriste ».

De multiples amendements de suppression des algorithmes

La délicate question des algorithmes dans la loi sur le renseignement a été abordée mercredi soir au Sénat. Des députés issus de tous les groupes politiques, de la gauche à la droite, ont déposé des amendements de suppression du dispositif de « boîtes noires ».

La commission des lois du Sénat a apporté quelques modestes retouches : la Commission nationale de contrôle des techniques de renseignement (CNCTR), l'organisme administratif de contrôle que crée la loi, pourra désormais se prononcer sur les « paramètres » des algorithmes, et non plus sur leurs « critères ». La commission a aussi précisé que l'autorisation du premier ministre, dont la validité sera ramenée de quatre à deux mois, devra préciser les paramètres des algorithmes. L'accès de la CNCTR aux algorithmes ne sera, enfin, pas seulement « permanent », mais également « direct ».

Source : http://www.lemonde.fr/pixels/article/2015/06/03/la-loi-sur-le-renseignement-mettra-t-elle-en-place-une-surveillance-de-masse_4646733_4408996.html
Par Martin Untersinger

Les Etats-Unis victimes d’une nouvelle cyber-attaque | Le Net Expert Informatique

Les Etats-Unis victimes d’une nouvelle cyber-attaque

Des pirates chinois seraient à l’origine d’une nouvelle cyber-attaque visant les données de fonctionnaires américains © Reuters/Pichi Chuang

Les données de millions de fonctionnaires américains ont été piratées ces derniers mois, aux Etats-Unis. Des cyber-pirates chinois seraient à l’origine de l’attaque, ils ont réussi selon des officiels américains à s’introduire dans les serveurs de l’Office of Personal Management, qui stocke notamment les profils des employés fédéraux.
Une nouvelle cyber-attaque d’envergure aux Etats-Unis. Les données personnelles de fonctionnaires ont été piratées depuis décembre 2014. Des hackers, apparement chinois, ont réussi à s’introduire dans les serveurs de l’Office of Personal Management (OPM), une agence qui vérifie notamment les profils des employés fédéraux pour le compte de la sécurité nationale.

4 millions de victimes, peut-être plus
Pas moins de quatre millions d’agents fédéraux, en activité ou à la retraite, ont été victimes de cette cyber-attaque. Ils vont devoir s’assurer auprès de leur banque que leurs données privées n’ont pas été utilisés par les pirates. D’autres éléments, comme les numéros de sécurité sociale et autres identifiants personnels sont également tombées aux mains des hackers.
Dans son communiqué, l’OPM n’exclut pas que d’autres personnes aient pu être victimes de cette attaque en ligne, menée au moment même où l’agence se dotait d’un nouveau système de sécurité. Vol de données ou espionnage, l’objectif des pirates reste en revanche incertain.
Le FBI, qui enquête sur l’affaire, dit « prendre au sérieux toutes les attaques potentielles contre les systèmes du secteur public et privé ».

Vulnérabilité du réseau informatique américain
L’attaque a été découverte en avril, mais la pêche aux informations aurait débuté dès la fin 2014. Une affaire de plus qui confirme la vulnérabilité du réseau informatique de l’administration américaine, fragilité dénoncée par le Government Accountability Office (GAO), l’équivalent de la Cour des comptes française.
Il y a quelques jours encore, on apprenait qu’une cybermafia avait réussi à récupérer les déclarations fiscales de plus de 100.000 contribuables. L’an dernier, le Département d’Etat et la Maison Blanche faisaient les frais d’intrusions attribuées à des Russes. A l’époque les courriels du président Barack Obama avaient été compromis.

Source : http://www.franceinfo.fr/vie-quotidienne/high-tech/article/les-etats-unis-victimes-d-une-nouvelle-cyber-attaque-des-hackers-chinois-soupconnes-688588
par Arnaud Racapé

Les pirates ciblent désormais l'Internet of Things | Le Net Expert Informatique

Les pirates ciblent désormais l'Internet of Things

Les assaillants sur internet recourent généralement à des attaques DDos. Mais avec la percée de l'internet des choses (IoT), ils se tournent à présent vers de nouvelles techniques.

DDoS continue de gagner en popularité et évolue aussi. L'année dernière, il s'agissait surtout d'attaques exploitant brièvement une large bande passante. Aujourd'hui, les attaques font moins de 10 Gbps, mais durent plus de 24 heures. Voilà ce qu'affirme Akamai dans son tout dernier rapport State of the Internet.

« Ce type d'attaque de longue durée va souvent de pair avec par exemple des demandes de versement d'une somme d'argent. Car si un site ou un service web est paralysé, le fournisseur perd également de l'argent », déclare Tim Vereecke, senior solutions engineer chez Akamai. L'augmentation des attaques est partiellement due au fait que louer un botnet devient plus abordable pour les criminels. « Le coût initial d'exécution d'une attaque DDoS est à présent inférieur à ce qu'il était avant. Voilà qui explique pourquoi on enregistre aujourd'hui davantage d'attaques de plus longue durée, mais qui sont en moyenne moins puissantes. »

Il n'empêche que les attaques lourdes ne restent pas exceptionnelles. C'est ainsi qu'Akamai a encore enregistré au trimestre dernier huit attaques dépassant les 100 Gbps, dont la plus importante atteignait même 170 Gbps.

Mais les pirates semblent déplacer leur intérêt pour DDos vers SSDP (Simple Service Discovery Platform), un protocole pour l'Internet of Things. Ce protocole s'assure entre autres que votre ordinateur reconnaisse les autres appareils internet dans la maison. « Mais ce protocole est aussi conçu pour recevoir toutes sortes de données, ce qui en fait un candidat idéalement utilisable comme intermédiaire pour une attaque. »

Concrètement, vingt pour cent de l'ensemble des attaques recensées au premier trimestre de cette année ont été lancées via SSDP. Et ce, alors que la technique ne s'était même pas manifestée dans les statistiques jusqu'à la seconde moitié de 2014. La solution pour éviter ces attaques, c'est une bonne sécurisation et configuration des appareils connectés entre eux et à internet.

Source : http://datanews.levif.be/ict/actualite/les-pirates-ciblent-l-internet-of-things/article-normal-397387.html

l’Expert Informatique obligatoire pour valider les systèmes de vote électronique | Denis JACOPINI

La délibération n° 2010-371 du 21 octobre 2010 de la CNIL portant adoption d’une recommandation relative à la sécurité des systèmes de vote électronique indique que tout système de vote électronique doit faire l’objet d’une expertise indépendante.

Le 30 juin dernier, nous avons suivi notre nième formation 8 rue Vivienne à Paris, dans les locaux de la CNIL. Cette fois, c’était un atelier vote électronique consistant à nous enseigner les bonnes pratiques à mettre en oeuvre dans l’expertise d’un système de vote électronique.

Expert informatique assermenté, Denis JACOPINI peut vous accompagner dans cette démarche d’expertise de systèmes de votes électroniques.

Cette journée de formation, à destination des Experts Informatiques et Experts Judiciaires en Informatique, portait sur le vote électronique. Vous trouverez ci-dessous un résumé de ce que nous considérons essentiel.

Le vote électronique, souvent via internet, connaît un développement important depuis plusieurs années, notamment pour les élections professionnelles au sein des entreprises.

La mise en place des traitements de données personnelles nécessaires au vote doit veiller à garantir la protection de la vie privée des électeurs, notamment quand il s’agit d’élections syndicales ou politiques.

La CNIL souligne que le recours à de tels systèmes doit s’inscrire dans le respect des principes fondamentaux qui commandent les opérations électorales : le secret du scrutin (sauf pour les scrutins publics), le caractère personnel, libre et anonyme du vote, la sincérité des opérations électorales, la surveillance effective du vote et le contrôle a posteriori par le juge de l’élection. Ces systèmes de vote électronique doivent également respecter les prescriptions des textes constitutionnels, législatifs et réglementaires en vigueur.

Les mesures de sécurité sont donc essentielles pour un succès des opérations de vote mais mettent en œuvre des mesures

compliquées, comme par exemple l'utilisation de procédés cryptographiques pour le scellement et le chiffrement.

La délibération n° 2010-371 du 21 octobre 2010 de la CNIL portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique indique que **tout système de vote électronique doit faire l'objet d'une expertise indépendante**.

Par ailleurs, l'article R2314-12 du Code du Travail créé par Décret n°2008-244 du 7 mars 2008 – art. (V) fixe très clairement que préalablement à sa mise en place ou à toute modification substantielle de sa conception, **un système de vote électronique est soumis à une expertise indépendante**. Le rapport de l'expert est tenu à la disposition de la Commission nationale de l'informatique et des libertés.

Information complémentaire : Les articles R2314-8 à 21 et R2324-4 à 17 du Code du Travail indiquent de manière lus générale les modalités du vote électronique lors du scrutin électoral de l'élection des délégués du personnel et des délégués du personnel au comité d'entreprise.

Ces dispositions ont été complétées par la délibération 2010-371 de la CNIL du 21 octobre 2010 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique.

L'expertise doit couvrir l'intégralité du dispositif installé avant le scrutin (logiciel, serveur, etc.), l'utilisation du système de vote durant le scrutin et les étapes postérieures au vote (dépouillement, archivage, etc.).

L'expertise doit porter sur l'ensemble des mesures décrites dans la présente délibération et notamment sur :

- le code source du logiciel y compris dans le cas de l'utilisation d'un logiciel libre,
- les mécanismes de scellement utilisés aux différentes

étapes du scrutin (voir ci-après),
- le système informatique sur lequel le vote va se dérouler, et notamment le fait que le scrutin se déroulera sur un système isolé ;
- les échanges réseau,
- les mécanismes de chiffrement utilisé, notamment pour le chiffrement du bulletin de vote sur le poste de l'électeur.

L'expertise doit être réalisée par un expert indépendant, c'est-à-dire qu'il devra répondre aux critères suivants :

- Être un informaticien spécialisé dans la sécurité ;
- Ne pas avoir d'intérêt financier dans la société qui a créé la solution de vote à expertiser, ni dans la société responsable de traitement qui a décidé d'utiliser la solution de vote ;
- Posséder une expérience dans l'analyse des systèmes de vote, si possible en ayant expertisé les systèmes de vote électronique d'au moins deux prestataires différents ;
- Avoir suivi la formation délivrée par la CNIL sur le vote électronique.

Le rapport d'expertise doit être remis au responsable de traitement. Les prestataires de solutions de vote électronique doivent, par ailleurs, transmettre à la CNIL les rapports d'expertise correspondants à la première version et aux évolutions substantielles de la solution de vote mise en place.

Si l'expertise peut couvrir un champ plus large que celui de la présente recommandation, le rapport d'expertise fourni au responsable de traitement doit comporter une partie spécifique présentant l'évaluation du dispositif au regard des différents points de la recommandation.

L'expert doit fournir un moyen technique permettant de

vérifier a posteriori que les différents composants logiciels sur lesquels a porté l'expertise n'ont pas été modifiés sur le système utilisé durant le scrutin. La méthode et les moyens permettant d'effectuer cette vérification doivent être décrits dans le rapport d'expertise.

[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

Vous souhaitez organiser des élections par voie électronique ?
Cliquez ici pour une demande de chiffrage d'Expertise

Vos expertises seront réalisées par **Denis JACOPINI** :

- Expert en Informatique **assermenté et indépendant** ;
- **spécialisé dans la sécurité** (diplômé en cybercriminalité et certifié en Analyse de risques sur les Systèmes d'Information « ISO 27005 Risk Manager ») ;
- ayant suivi la **formation délivrée par la CNIL sur le vote électronique** ;
- qui n'a **aucun accord ni intérêt financier** avec les sociétés qui créent des solution de vote électronique ;
- et possède une expérience dans l'analyse de nombreux systèmes de vote de prestataires différents.

Denis JACOPINI ainsi **respecte l'ensemble des conditions recommandées** dans la Délibération de la CNIL n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.

Son expérience dans l'expertise de systèmes de votes électroniques, son indépendance et sa qualification en sécurité Informatique (ISO 27005 et cybercriminalité) vous apporte l'assurance d'une qualité dans ses rapport

d'expertises, d'une rigueur dans ses audits et d'une impartialité et neutralité dans ses positions vis à vis des solutions de votes électroniques.

Correspondant Informatique et Libertés jusqu'en mai 2018 et depuis Délégué à La Protection des Données, nous pouvons également vous accompagner dans vos démarches de mise en conformité avec le RGPD (Règlement Général sur la Protection des Données).

Contactez-nous

Les atteintes aux libertés de la Loi Renseignement | Le Net Expert Informatique

Les atteintes aux libertés de la Loi Renseignement

Hier, le Sénat a commencé l'examen du projet de loi sur le renseignement par l'inévitable discussion générale. Chacun des groupes et sénateurs a pu ainsi donner « sa » religion sur ce texte, contesté par bon nombre d'organisations de la société civile, tout comme la CNIL ou le défenseur des droits. Compte rendu.

D'entrée, Manuel Valls a jugé le texte comme indispensable afin d'apporter la précision et l'encadrement nécessaire aux activités des services du renseignement, dans un contexte d'évolution technologique : « Il faut pouvoir suivre les terroristes sur leurs réseaux, car ils utilisent tous les outils du numérique pour leurs actions de propagande et d'embrigadement, ainsi que pour échanger. C'est pourquoi nous autorisons le recours aux algorithmes : afin de détecter des terroristes jusqu'alors inconnus et des individus connus qui recourent à des techniques de dissimulation. Moins d'un djihadiste sur deux avait été détecté avant son départ en Syrie ; nous devons pouvoir faire mieux. »

Quand Philippe Bas s'attaque aux « inoculations toxiques »

Des propos à comparer à ceux de Philippe Bas (UMP), rapporteur du texte : « **Le texte confronte les intérêts fondamentaux de la Nation et la sauvegarde de la vie humaine aux exigences aussi fortes que sont le respect de la vie privée et la garantie des libertés fondamentales. Il donne un cadre légal aux services de renseignement** » s'est-il félicité, en pleine phase avec le gouvernement. S'en prenant aux détracteurs, il jure cependant que ce projet « ne renforce pas les moyens des services de renseignement, ce n'est pas son objet. Il n'a rien à voir avec la caricature qui en a été faite. Les critiques qui lui sont faites, cependant, sont autant d'anticorps pour que l'État de droit résiste à des inoculations toxiques pour les libertés ».
Une erreur d'analyse patente puisque le projet de loi vise bien à décupler les moyens des services du renseignement, au motif ou prétexte de leur encadrement.

Renseignement, Google, même combat

Yves Detraigne (UDI-UC) s'en est tout autant pris aux opposants à ce texte qui condamnent l'usage des algorithmes, « dont l'utilisation quotidienne, à des fins mercantiles, par les géants du web tels que Google, ne provoque pas les mêmes réactions ». Comme si Google pouvait vous envoyer en prison… Jean-Jacques Hyest (UMP) a pris pour cible la presse et les discours anxiogènes amplifiés lors d'une précédente loi sécuritaire: « On annonçait une catastrophe pour les libertés publiques, c'était « l'horreur » – alors que l'article 13 est plus protecteur des libertés publiques que le droit qui prévalait jusque-là. » Tellement protecteur que cet article (devenu l'article 20), qui autorise l'aspiration de données de connexion par le renseignement, est actuellement en voie de QPC au Conseil d'État. La Quadrature du Net, FDN et FFDN ayant victorieusement fait valoir aux yeux du rapporteur que certains droits et libertés fondamentaux étaient un peu trop menacés par ces mécanismes, qui servent de socles juridiques à la loi Renseignement.

Il y aura des faux positifs et des atteintes aux libertés

Pierre Charon (UMP) admet sans sourciller que des « faux positifs » seront possibles avec les boites noires (algorithme détectant les premières traces de menace terroriste). Mais pas grave : « Cela confirme que nos services ont aussi besoin de moyens humains » et que « les citoyens doivent avoir des voies de recours ». Analyse similaire chez Jean-Pierre Sueur (PS) qui explique que les atteintes aux libertés sont nécessaires : « Vous savez qu'il existe des sites dangereux parce qu'ils encouragent à l'oeuvre de mort. Je crois l'atteinte aux libertés nécessaire pour combattre le terrorisme, pourvu qu'elle soit limitée par le droit ». La question du terrorisme cependant n'est qu'un petit versant de ce texte qui autorise l'espionnage pour d'autres fins, notamment celle de la défense ou la promotion des intérêts français.

Le germe d'une collecte massive débouchant sur une surveillance généralisée

La sénatrice Michelle Demessine (CRC) sera pour sa part plus critique : « ce texte porte en lui le germe d'une collecte massive et indifférenciée de données qui débouche inévitablement sur une surveillance généralisée de la société. ». Claude Malhuret (UMP) embraye, plus réservé encore : « On nous dit que ne seraient concernées que les métadonnées. Cela relève de l'escroquerie intellectuelle. M. X, marié, se connecte tous les quinze jours à un site de rencontres extra-conjugales ; M. Y, dans la même situation, visite toutes les semaines un site de rencontres homosexuelles. Les métadonnées contiennent toute l'information intéressante. Point besoin de connaître aussi le contenu ».

Le sénateur s'est d'ailleurs appuyé sur les (pseudos) reculades aux États-Unis en matière de renseignement pour justement torpiller le pas de danse français. « Nous ne sommes plus loin des horreurs décrites par Orwell après la révélation par Edward Snowden des pratiques de la NSA » ajoute Catherine Morain-Desailly (UDI-UC). « Ce texte est bien un Patriot Act à la française, pris en hâte après les attentats de janvier. Les algorithmes sont source d'erreur, on le sait. Pourquoi les légaliser quand le Congrès américain le refuse désormais ? Supprimons le contrôle par les boites noires qui fragilisent la sécurité des données des entreprises et des institutions à cause des failles que les cybercriminels savent exploiter. Instituons un contrôle de la CNIL, le seul rempart contre l'arbitraire, l'hypersurveillance et l'hypervigilance ».

C'est quoi le programme ?

Les sénateurs débattront véritablement des articles et des amendements à partir de 14 h 30 aujourd'hui jusqu'au 9 juin. Ensuite « leur » texte sera arbitré avec celui des députés en Commission mixte paritaire. Si le gouvernement le souhaite, c'est l'Assemblée nationale qui pourra avoir le dernier mot, du moins si la disharmonie perdure. Après cela, le projet de loi devrait être contrôlé par le Conseil constitutionnel, avant sa publication au Journal officiel. Une promesse de François Hollande, alors que plus de 60 députés se sont déjà réunis pour doubler cette saisine par une action parlementaire en ce sens. Ajoutons que le Conseil constitutionnel pourrait dans le même temps examiner le recours précité, initié par la Quadrature du Net, la FDN et FFDN, si du moins le Conseil d'État suit l'avis du rapporteur général en ce sens (notre compte rendu et l'interview de Me Spinosi)

Source : http://www.nextinpact.com/news/95299-loi-renseignement-faux-positifs-atteintes-aux-libertes-pas-grave.htm
Par Marc Rees

L'analyse comportementale, la nouvelle cyber-arme ? | Le Net Expert Informatique

IdentityGRC 2015 est la dernière offre de détection comportementale de la fraude et de la fuite de données de Brainwave, co-fondée par Sébastien Faivre. (crédit : D.R.)

L’analyse comportementale, la nouvelle cyber-arme ?

C’est bien connu, en matière de sécurité les risques ne proviennent pas seulement de l’extérieur du périmètre de l’entreprise mais bien de l’intérieur. Téléchargement de fichiers non autorisés, vol de données confidentielles ou encore accès à des informations par un collaborateur ayant quitté depuis des mois l’entreprise sont, malheureusement, une réalité qui dépasse – parfois – de loin la fiction. Et bien souvent, à la base de cette problématique, on trouve une gestion et/ou une politique de gestion des droits d’accès défaillante ou en tout cas plus en mesure de répondre à une évolution malsaine des comportements.
« Le constat que l’on fait aujourd’hui est que d’une façon générale la sécurité des accès et la configuration des droits d’accès pour accéder à des applications ou données sont souvent les parents pauvres de la sécurité informatique », explique Sébastien Faivre, co-fondateur de Brainwave. « En général, le département informatique et les métiers se renvoient la balle en termes de responsabilités dans les cas où on se rend compte que des personnes qui ont quitté l’entreprise ou changé de département ont toujours accès à des informations sensibles ou que d’autres encore ont des droits d’accès excessifs à des données critiques ».

Des jeux d’API couplés à des algorithmes d’analyse
Pour faire face à ce type de menace, le jeune éditeur francilien Brainwave (créé en 2010) a développé IdentityGRC qui permet de récupérer toutes les informations de configurations de l’ensemble des systèmes de l’entreprise afin de proposer une cartographie de l’ensemble des droits d’accès aux applications. Et ce, des systèmes CRM, ERP, gestion financière (SAP, Salesforce.com, Microsoft Dynamics CRM…) que des solutions cloud de sauvegarde et de partages documentaires (Google Drive, Dropbox…) ou encore des grands systèmes (AS400, RACF, CA Top Secret…). Pour y parvenir, plusieurs jeux d’API ont été développés, couplés à des algorithmes d’analyse, brevetés depuis fin 2010, afin de pouvoir poser des questions en langage naturel de type « Quelles sont les personnes ne faisant pas partie des ressources humaines qui ont accès aux fiches de paye des salariés ? ».
Aujourd’hui, Brainwave va plus loin en matière de détection mais surtout de prévention de la fraude et de fuite des données. « La version 2015 d’IdentityGRC propose de l’analyse comportementale permettant de mettre sous surveillance des comportements anormaux comme par exemple identifier une personne qui récupère bien plus de fichiers que ses collègues, mais également d’automatiser le diagnostic et la résolution des comportements suspects », fait savoir Sébastien Faivre. Une approche différente selon Brainwave des traditionnelles offres de sécurité centrées davantage sur les flux de comportements au niveau des postes de travail que sur le comportement du point de vue des applications, indépendamment du reste de tout terminal.

A partir de 75 000 euros la licence perpétuelle
Distingué par le Gartner dans la catégorie des « cool vendors » dans son rapport Magic Quadrant 2013 en Identity Analytics and Intelligence, Brainwave n’a pas attendu pareille reconnaissance pour se tailler une place dans les entreprises. Surtout les grandes, avec des clients comme PSA Peugeot-Citroën, Natixis, Crédit Agricole, BNP Paribas, ou encore Aéroports de Paris et Eutelsat qui utilisent ses solutions. En tout, l’éditeur revendique une cinquantaine de références en France mais également au Bénélux, en Suisse, au Royaume-Uni, au Magrehb ou encore au Canada où il a ouvert récemment un bureau commercial. Autofinancée jusqu’en 2014, la société a levé 2,5 millions d’euros fin 2014 afin de donner un nouvel élan à sa croissance internationale mais également renforcer ses équipes R&D (une dizaine de personnes sur 30 collaborateurs au total). Brainwave a réalisé l’année dernière un chiffre d’affaires de 2 millions d’euros et indique être rentable.
IdentityGRC 2015 est proposée à partir de 75 000 euros en licence perpétuelle, auquel vient s’ajouter près de 20 000 euros de maintenance annuelle. Deux modes de tarification sont proposées : nombre de personnes sur lequel un audit sécurité est réalisé ou bien en fonction du nombre d’applications. Quant à la disponibilité de l’offre, elle est pour le moment uniquement en on-premise. « Nous ne proposons pas d’offre en mode cloud public. Nos clients considèrent que ce type de données est sensible et préfèrent donc un déploiement sur site. Cependant, certains clients ont choisi un déploiement dans un cloud privé chez un infogéreur », explique Sébastien Faivre.

Source : http://www.lemondeinformatique.fr/actualites/lire-avec-identitygrc-2015-brainwave-s-ouvre-a-l-analyse-comportementale-61157.html
Par Dominique Filippone

Les dernières fuites de données mettent en évidence la nécessité de sécuriser les e-mails | Le Net Expert Informatique

	Les dernières fuites de données mettent en évidence la nécessité de sécuriser les e-mails

Peut-on se passer de l'e mail dans le cadre de ses activités professionnelles ? Pratique et instantanée, la communication par e-mail s'est imposée au quotidien dans l'entreprise. Certaines études évaluent à plus de 100 milliards le nombre d'e-mails professionnels qui sont échangés chaque jour(1).

Nos e mails risquent-ils de laisser échapper des données sécurisées ?
Malgré ses nombreux atouts, l'e-mail présente également certains risques. Des récits de fuites de données sensibles font régulièrement la une des médias. Un des derniers incidents en date : la récente divulgation des numéros de passeport de 31 leaders mondiaux. En cause ? La fonctionnalité de saisie automatique à partir du carnet d'adresses d'Outlook. Cette fonctionnalité – aussi pratique soit-elle – ne fait qu'accentuer le risque de diffuser, par erreur, des données confidentielles.
Malgré l'augmentation du nombre d'erreurs d'aiguillage d'e-mails et l'évolution du contexte législatif – comme en atteste la récente loi australienne sur l'obligation de conserver des métadonnées et d'autres textes réglementant la transmission de données confidentielles (HIPAA, FIPPA et PCI) –, on peut s'étonner que les entreprises ne soient pas plus nombreuses à choisir de sécuriser le contenu de leurs e mails.
L'e mail est sans doute un peu trop pratique à en juger par la facilité avec laquelle des informations sensibles peuvent être envoyées, au risque de tomber dans les mauvaises mains.

Quelques chiffres :
• 53 % des employés ont déjà reçu des données sensibles d'entreprise non cryptées par e mail ou en pièces jointes (2).
• 21 % des employés déclarent envoyer des données sensibles sans les chiffrer(2). Les coûts liés à la perte de données s'envolent, sans parler des conséquences sur la réputation des entreprises et des éventuelles répercussions sur le plan juridique en cas de violation de la réglementation sur la transmission et le stockage de données confidentielles (notamment dans le cadre des lois HIPAA et FIPPA, et du standard PCI).
• 22 % des entreprises sont concernées chaque année par la perte de données via e-mail(3).
• 3,5 millions de dollars : coût moyen d'une violation de données pour une entreprise(4).

La solution
Il existe heureusement des solutions de sécurité des e-mails qui mettent les utilisateurs et leur entreprise à l'abri de ces menaces. La signature numérique et le chiffrement des e-mails garantissent la confidentialité d'un message et évitent que des données sensibles ne tombent dans de mauvaises mains. Le destinataire a également l'assurance de l'identité réelle de l'expéditeur de l'e-mail et que le contenu du message n'a pas été modifié après son envoi.
Le chiffrement d'un e-mail revient à sceller son message puis à le déposer dans un dossier verrouillé dont seul le destinataire prévu possède la clé. Il est alors impossible pour une personne interceptant le message, pendant son transit ou à son emplacement de stockage sur le serveur, d'en voir le contenu. Sur le plan de la sécurité, le chiffrement des e mails présente les avantages suivants :
• Confidentialité : le processus de chiffrement requiert des informations de la part du destinataire prévu, qui est le seul à pouvoir consulter le contenu déchiffré.
• Intégrité du message : une partie du processus de déchiffrement consiste à vérifier que le contenu du message d'origine chiffré correspond au nouvel e-mail déchiffré. Le moindre changement apporté au message d'origine ferait échouer le processus de déchiffrement.
Avant de choisir une solution, il est important d'avoir en tête plusieurs choses. L'utilisateur est le mieux placé, car il connaît son entreprise mieux que personne. Phishing, perte de données… quels sont ses principaux sujets de préoccupation ? Quelle est l'infrastructure de messagerie en place dans l'entreprise ? Quel est le cadre réglementaire ? Les réponses propres à chaque entreprise orienteront les choix vers la solution la plus appropriée.

Sources :
(1) Email Statistics Report 2013-2017, The Radicati Group, Inc.
(2) SilverSky Email Security Habits Survey Report, SilverSky, 2013
(3) Best Practices in Email, Web, and Social Media Security, Osterman Research, Inc., January 2014
(4) Global Cost of Data Breach St'sudy, Ponemon Institute,

Source : http://www.globalsecuritymag.fr/Les-dernieres-fuites-de-donnees,20150601,53078.html
par GlobalSign

Protection des données. Un accord européen possible le 15 juin | Le Net Expert Informatique

Un accord pour adapter la législation européenne sur la protection des données personnelles à l'essor de l'internet est à portée de main et peut être conclu le 15 juin.

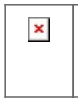
Jeudi soir à Bruxelles, l'Allemagne, la France, le Luxembourg et la Commision européenne ont assuré qu'un accord sur la protection des données pourrait voir le jour d'ici à trois semaines.
« Nous sommes dans la dernière ligne droite et nous voulons aboutir », a déclaré le ministre allemand de l'Intérieur, Thomas de Maizière, au cours d'un débat sur la protection des données avec les ministres de la Justice de la France, du Luxembourg et la commissaire européenne Vera Jourova.
« Nous sommes sur la voie d'un accord général. Le texte est inachevé, mais il est bon », a confirmé Mme Taubira. « Nous avons en perspective un accord le 15 juin » lors de la réunion des ministres européens de la Justice à Luxembourg, a renchéri la commissaire Jourova.

Protéger les citoyens européens

L'objectif de cette nouvelle législation est d'empêcher les données personnelles des citoyens de l'UE de quitter l'espace européen sans leur consentement explicite.
Thomas de Maizière a préconisé une longue journée de discussion pour aboutir. « Il va falloir faire des compromis et tempérer les attentes », a-t-il insisté.
Deux textes sont en discussion depuis février 2012: un règlement pour les données personnelles à caractère civil et commercial, et une loi pour les fichiers du secteur privé.

Source : http://www.ouest-france.fr/un-accord-europeen-possible-le-15-juin-3436970

La voiture autonome vulnérable aux cyber-attaques, selon des experts | Le Net Expert Informatique



La voiture autonome vulnérable aux cyber-attaques, selon des experts

Le risque de voir des pirates informatiques prendre le contrôle de voitures autonomes est bien réel, estiment des experts américains, une hypothèse d'ores et déjà prise en compte par les constructeurs et les assureurs aux Etats-Unis.

Annoncées sur les routes en 2020, voire même dès 2017, la voiture sans conducteur devrait disposer des technologies dernier cri comme des capteurs numériques –caméras, radars, sonars, lidars (guidage par laser)– gérées à distance par des logiciels permettant de reconnaître des limites de chaussées, des panneaux ou encore des obstacles.
Mais, comme pour les automobiles connectées et leurs systèmes multimédias embarqués, ces nouvelles technologies de pointe censées rendre les véhicules plus sûrs et fiables, pourraient aussi les rendre vulnérables aux attaques de hackers, selon les sociétés de sécurité informatique américaines Mission Secure Inc (MSi) et Perrone Robotics Inc.
Un pirate informatique s'est récemment vanté d'avoir pénétré les systèmes électroniques d'un avion de ligne dans lequel il voyageait, et d'en avoir modifié la trajectoire. Ceci en utilisant le système wifi proposé aux passagers.
Les deux sociétés de sécurité ont effectué, en collaboration avec l'Université de Virginie (est) et le ministère américain de la Défense, des tests en situation réelle qui ont montré, selon elles, qu'il était possible de désorganiser le système.
L'un des essais consistait à modifier le comportement de la voiture face à un obstacle: le piratage «oblige la voiture à accélérer au lieu de freiner même si l'obstacle a été détecté par le Lidar, entraînant une collision à grande vitesse», selon le rapport consultable sur le site internet de MSi (missionsecure.net).
Une autre cyber-attaque «provoque un freinage d'urgence inapproprié plutôt qu'un freinage en douceur, pouvant entraîner la perte de contrôle du véhicule», peut-on encore lire.
Selon ces experts, les pirates pénètrent le système grâce aux connexions sans fil, bluetooth et wifi.
MSi et Perrone Robotics, qui développent un système payant pour parer les cyber-attaques, estiment que «cette situation pose des défis importants et des risques pour l'industrie automobile ainsi que pour la sécurité publique».
– Primes d'assurances revues ? –
La plupart des constructeurs automobile s'attelant à la fabrication de leur voiture autonome n'ont pas donné suite aux sollicitations de l'AFP sur le sujet.
Mais, selon des sources proches de l'industrie, les éventualités de cyber-attaques ont été prises en compte et testées tout au long du processus de fabrication.
Le géant de l'internet Google, par exemple, aurait une équipe d'informaticiens de haut vol chargée de défier les logiciels destinés à sa propre voiture autonome qui va être testée sur la voie publique à partir de cet été, selon des sources industrielles.
Contacté par l'AFP, le groupe de Mountain View (Californie) s'est refusé à tout commentaire.
Cette question de sécurité préoccupe les assureurs américains qui sont dans l'expectative face à ces nouvelles technologies et à leur capacité à réduire réellement les risques d'accidents. Cela pourrait les obliger à repenser leurs contrats et à recalculer les primes.
Dans un premier temps, ces dernières pourraient augmenter à cause du prix des voitures autonomes, qui sera élevé en raison du coût des technologies embarquées et des réparations éventuelles, a expliqué l'assureur Nationwide à l'AFP.
Mais, a-t-il ajouté, cela pourrait être en partie compensé avec la généralisation de ces véhicules supposés éviter les accidents. Pour State Farm, autre assureur américain, il est nécessaire d'avoir une «vue d'ensemble».
«Certes les technologies des voitures autonomes et connectées réduisent ou éliminent certains risques auxquels font face aujourd'hui les conducteurs, mais de nouveaux risques vont probablement apparaître», a argumenté la compagnie.
Selon un important assureur américain ayant requis l'anonymat, il sera essentiel de bien baliser les responsabilités en cas d'accidents. Celles-ci seront établies en fonction des instructions des constructeurs automobiles sur ce que la voiture pourra faire ou non de manière autonome.

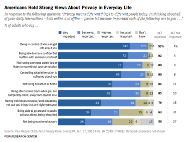
Source : http://www.liberation.fr/economie/2015/05/31/la-voiture-autonome-vulnerable-aux-cyber-attaques-selon-des-experts_1320239

90% internautes US veulent garder le contrôle sur leurs données privées | Le Net Expert Informatique

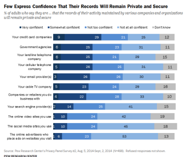
- 90% internautes US veulent garder le contrôle sur leurs données privées

Outre-Atlantique, le manque de confiance concernant la protection de la vie privée en ligne est plus que majoritaire. D'après de récents chiffres publiés par le Pew Research Center, les Américains souhaitent contrôler leurs données tout en évitant d'être traqués sur la Toile.

Aux États-Unis, d'un côté les utilisateurs tiennent à leur vie privée, de l'autre le gouvernement et les grandes entreprises du web collectent des données. Voilà le paradoxe que met en avant la dernière enquête du Pew Research Center ! En matière d'intimité en ligne, les consommateurs sont toujours plus septiques. Nombreux sont ceux qui veulent être en mesure de contrôler leurs informations en ligne et surtout l'accès à ces dernières.



L'étude du Pew Research Center porte sur le dernier trimestre 2014 et le premier trimestre 2015. Il s'agit là du troisième sondage sur la vie privée depuis les révélations d'Edward Snowden en 2013. Sur cette période, 93% de sondés ont déclaré qu'il était « très important » ou « assez important » de pouvoir contrôler qui peut obtenir et consulter des informations personnelles. Chose intéressante, dans le cadre professionnel, les attentes et besoins de confidentialité sont beaucoup plus bas, à savoir 56%.
Au final, les personnes interrogées font le plus confiance aux entreprises du marché des cartes de crédit pour la conservation de données privées et sécurisées. On trouve ensuite les entreprises publiques et téléphoniques. À l'inverse, la méfiance est bien plus élevée pour ce qui est du secteur publicitaire et des médias sociaux. Une importante part d'internautes américains (44%) estime également que les plateformes vidéo ne devraient pas suivre leur activité et 40% n'approuvent pas le business modèle de Google.
Le rapport explique que « les internautes pensent que leur activité sur internet ne reste pas privée et sécurisée ». De manière générale, 80% des sondés ne font pas confiance aux annonceurs quant à la gestion de leurs données en ligne, 70% pour ce qui est des médias sociaux et 66% concernant les moteurs de recherche.



L'écart se creuse entre la volonté des citoyens américains et les actions du gouvernement en faveur des grandes firmes du Net. La lutte contre le terrorisme est un argument de poids, mais 65% de la population croit aujourd'hui qu'il n'y a pas de limite à la collecte de données privées. Tout en soulignant le fait que les internautes sont conscients d'être surveillés, Pew révèle que les utilisateurs US réclament des limites concernant la durée de consultation de leur activité en ligne. Pour faire simple, ceux-ci souhaitent que leurs données de navigation ne soient conservées par les sites que pour un temps défini et non archivées pour un ciblage futur.
Les consommateurs américains ont ici un avis peu favorable à l'égard des géants du web. Pour Facebook, Google et de nombreux autres, le ciblage, la collecte et le suivi de données sont un exercice délicat. Idéalement, l'objectif premier serait de regagner la confiance des utilisateurs, mais le problème est à la fois économique, éthique et technique.
Selon Pew, 9% des sondés pensent qu'ils ont « beaucoup » de contrôle sur la quantité d'informations collectées à leur sujet. En revanche, seulement 7% d'entre eux ont déclaré avoir pris des mesures pour garder la main sur leurs données personnelles. Le constat est troublant ! D'un côté, le manque de confiance saute aux yeux, mais de l'autre les utilisateurs ne prennent pas de mesure pour tenter d'éviter le tracking ; qu'il s'agisse du gouvernement ou de sociétés commerciales. Malheureusement, tout le monde n'est pas capable de sécuriser ses données. Le sentiment d'impuissance des internautes face à une surveillance constante explique en partie cette passivité quant au contrôle de leur vie privée !

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

Source : http://www.zdnet.fr/actualites/90-internautes-us-veulent-garder-le-controle-sur-leurs-donnees-privees-39819740.htm
Par Pierrick Aubert pour Watch IT