Une voiture qui devine quand vous allez tourner… | Le Net Expert Informatique

Une voiture qui devine quand vous allez tourner…

On nous promet la voiture qui roule toute seule, la voiture qui réagit à la voix, la voiture connectée… la voiture piratée aussi et la voiture peut tricher aux tests anti-pollution… Voici venir la voiture qui anticipe les mouvements ! Bientôt, elle devinera en effet les manoeuvres du conducteur avant que celui-ci n'ait eu le temps de faire quoi que soit. Tout juste aura-t-il amorcé un mouvement de la tête.

C'est le projet Brain4Cars (« un cerveau pour la voiture ») d'un groupe de chercheurs des universités américaines de Stanford (Californie) et Cornell (Etat de New York). Pour cela, il a fallu littéralement apprendre au système informatique à corréler les mouvements de tête à les manoeuvres. Pour commencer, les chercheurs ont expédié pendant deux mois une dizaine de conducteurs sur les routes, sur voies express ou en ville, à bord de véhicules équipés de caméra filmant à la fois ce qui se passait dans leur champ de vision à l'intérieur et à l'extérieur de l'habitacle. Au total, l'équipe à récupéré deux millions de plans collectés sur 1900 kilomètres et les ont annotés en fonction de ce qu'on y voyait : changement de file, bifurcation, conduite en ligne droite, chronométrage des manœuvres, nombre de voies sur la route empruntée, voie occupée par la voiture, etc.

CORRELATION

La caméra placée dans l'habitacle, sur le tableau de bord, scrutait le visage du conducteur ainsi que les mouvements horizontaux de la tête et l'angle décrit. Les deux jeux de données ont ensuite été corrélés et le logiciel a appris ainsi quels mouvements faciaux et quels angles de rotation de la tête annoncent quelles actions du conducteur. « Nous avons bâti une architecture de « deep learning » (apprentissage profond) en réseaux de neurones récurrents, explique Ashutosh Saxena, membre de l'équipe. Nous nous sommes inspirés des travaux de Andrew Ng [chercheur américain en charge de l'intelligence artificielle chez le moteur de recherche chinois Baidu, ndlr] et de Yann LeCun [chercheur français directeur de l'intelligence artificielle chez Facebook, ndlr] » .

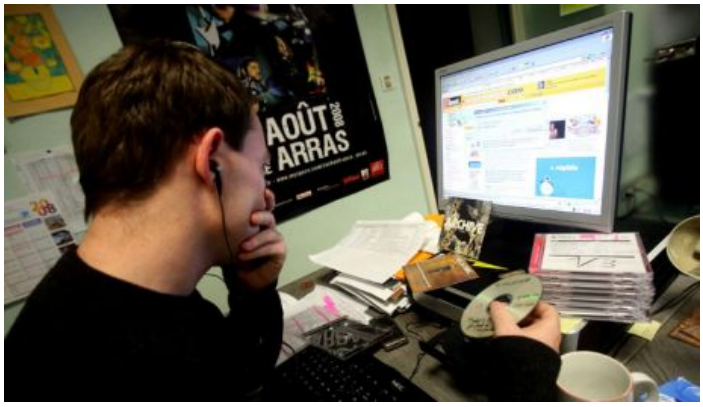
L'équipe s'est concentrée sur quatre événements : changement de file à droite ou à gauche et bifurcation à droite ou à gauche. Une fois la voiture, toujours dotée de ses caméras, de retour sur les routes, l'algorithme compare ce qu'il a « appris » est ce qui se passe en temps réel. Ce calcul s'opère en 3,6 millisecondes. Après quoi il émet une alerte en cas de danger ou d'obstacle (une voiture arrivant derrière mais située dans un angle mort par exemple) quelques secondes avant que le conducteur ne tourne le volant pour faire sa manoeuvre. En l'occurrence, le système a pu réagir entre 1 et 5 secondes à l'avance, pertinent dans plus de 80% des cas.

VIDEO.

Démonstration du système ci-dessous dans une vidéo: à droite, le visage de la conductrice et les différents points observés; à gauche, les actions devinées par l'algorithme:

Source :
http://www.sciencesetavenir.fr/high-tech/transports/20151002.OBS6953/et-la-voiture-devine-que-dans-trois-secondes-vous-allez-tourner-a-droite.html?cm_mmc=EMV-_-SEA-_-20151002_NLSEAACTU-_-et-la-voiture-devine-que-dans-trois-secondes-vous-allez-tourner-a-droite#xtor=EPR-1-SEAActu17h-20151002

Les cybercriminels se faisant passer pour des utilisateurs légitimes représentent le risque de sécurité le plus élevé | Le Net Expert Informatique



Les cybercriminels se faisant passer pour des utilisateurs légitimes représentent le risque de sécurité le plus élevé

Les cyber-attaques consistant à pirater les comptes à privilèges et administratifs, c'est-à-dire les identifiants utilisés pour contrôler et utiliser l'infrastructure IT d'une organisation, constituent la principale menace de sécurité dans les entreprises, selon une récente étude conduite par CyberArk.

61% des personnes interrogées ont retenu l'usurpation de comptes à privilèges comme étant le type de cyber-attaque le plus difficile à contrer, contre 44% du même avis l'année dernière. En outre, 48% pensent que les violations de données résultent des mauvaises habitudes des employés en matière de sécurité, tandis que 29% attribuent ceci à la sophistication des attaques. Ces conclusions proviennent de la 9e enquête annuelle réalisée par CyberArk sur le panorama mondial des cyber-menaces avancées Threat Landscape Survey, pour lequel l'entreprise a interrogé 673 cadres dirigeants et responsables de la sécurité IT.
CyberArk a analysé les divergences potentielles entre les cyber-menaces préjudiciables et la confiance qu'une organisation accorde à son système de sécurité. Bien que le lien entre la prise de contrôle de comptes à privilèges comme étant le premier vecteur d'attaque et les récentes, et très médiatisées, violations de données soit mieux établit, les entreprises persistent à se concentrer sur une défense « périmétrique ».
Plus de la moitié des interrogés étant convaincus qu'ils pourraient détecter une attaque en quelques jours, CyberArk a indiqué que de nombreux responsables IT et chefs d'entreprises ne disposent pas de la visibilité suffisante sur leurs programmes de sécurité IT. Les défenses périmétriques et les attaques d'hameçonnage (phishing) ne sont que la partie visible de l'iceberg, et les organisations doivent aujourd'hui veiller à se protéger face à des attaques beaucoup plus dévastatrices qui, comme le « Golden Ticket » Kerberos et les attaques « Pass-the-Hash », s'opèrent au cœur-même du réseau.

Les principales conclusions du sondage 2015 incluent : Au-delà de la simple violation – Les pirates cherchent à prendre le contrôle total du réseau
Comme nous avons pu le constater lors des attaques qui ont visé Sony Pictures, le Bureau américain de gestion du personnel et bien d'autres encore, les pirates ayant pris possession des comptes à privilèges peuvent ensuite s'en servir pour prendre de force le contrôle d'une infrastructure réseau ou voler d'importants volumes de données confidentielles. Ces comptes à privilèges permettent en effet aux cybercriminels d'avoir le même niveau de contrôle que les administrateurs IT de haut rang, et ce sur n'importe quel réseau. Grâce à leur capacité de se faire passer pour des utilisateurs légitimes, ces pirates peuvent alors continuer à acquérir des privilèges et à parcourir l'ensemble du réseau afin d'y exfiltrer des données précieuses.

A quelle phase une attaque est-elle la plus difficile à contrer selon les interrogés :
• 61% ont cité la violation des comptes à privilèges, contre 44% en 2014
• 21% mentionnent l'installation du logiciel malveillant
• 12% évoquent la phase de reconnaissance menée par le cybercriminel

Les vecteurs d'attaque représentant les risques de sécurité les plus élevés selon les interrogés sont :
• 38% indiquent la violation de comptes à privilèges ou administratifs
• 27% mentionnent les attaques d'hameçonnage
• 23% citent les logiciels malveillants sur le réseau

Trop de confiance accordée aux stratégies de sécurité dans les entreprises
Le sondage de CyberArk illustre que les interrogés ont entière confiance dans les stratégies de sécurité de leur PDG et de leurs directeurs, mais que les tactiques employées par les organisations sont en contradiction avec les meilleures pratiques en matière de sécurité. Même si les études spécialisées révèlent qu'il faut habituellement une moyenne de 200 jours pour qu'une organisation puisse déceler un pirate sur leurs réseaux, la plupart des interrogés pensent qu'ils sont capables de détecter un pirate endéans quelques jours ou quelques heures. Les interrogés persistent également à croire qu'ils sont parfaitement à même d'empêcher les cybercriminels de pénétrer dans le réseau, malgré de nombreuses preuves indiquant le contraire.
• 55% pensent qu'ils seront capables de détecter une violation en l'espace de quelques jours ; 25% estiment pouvoir détecter une infraction en quelques heures
• 44% continuent de croire qu'ils peuvent parfaitement empêcher les cybercriminels de pénétrer dans un réseau spécifique
• 48% pensent que ce sont les mauvaises habitudes des employés qui sont à la base des violations de données, tandis que 29% mentionnent tout simplement la sophistication des attaques
• 57% des personnes interrogées ont confiance dans les stratégies établies par leur PDG ou leur Conseil d'administration

Les organisations ne semblent toujours pas reconnaître les dangers liés aux attaques de l'intérieur
Les cybercriminels ne cessent de développer de nouvelles tactiques afin de cibler, dérober et exploiter des comptes à privilèges qui leur permettront d'obtenir l'accès aux données les plus sensibles et les plus précieuses d'une organisation. Alors que bon nombre d'entre elles se concentrent sur la défense périmétrique afin de lutter contre des attaques telles que le phishing ou l'usurpation d'identité, ce sont les attaques lancées depuis l'intérieur des organisations qui sont les plus potentiellement dévastatrices. Il a été demandé aux interrogés d'établir un classement des types d'attaques qu'ils redoutent le plus :

• Piratage de mots de passe (72%)
• Attaques d'hameçonnage (70%)
• Piratage de clés SSH (41%)
• Attaques Pass-the-Hash (36%)
• Attaques de Golden Ticket (23%)
• Attaques Overpass-the-Hash (18%)
• Attaques de Silver Ticket (12%)

Les attaques Overpass-the-Hash, Golden Ticket et Silver Ticket sont toutes des attaques Kerberos, permettant d'obtenir un contrôle total d'un réseau spécifique par le piratage du contrôleur de domaine. L'une des attaques les plus dangereuses est celle du Golden Ticket, car elle peut paralyser une organisation entièrement et briser ainsi la confiance accordée à l'infrastructure IT.

« Il est inacceptable qu'une organisation continue de penser que ses programmes de sécurité sont en mesure d'empêcher les cybercriminels de pénétrer dans leur réseau. En outre, le fait de se retrancher derrière la sophistication des attaques et les mauvaises habitudes des utilisateurs ne fait qu'aggraver le problème, déclare John Worrall, Directeur du marketing chez CyberArk. Les attaques les plus dévastatrices sont celles où les pirates volent des identifiants à privilèges et administratifs afin d'obtenir les mêmes droits d'accès que les administrateurs systèmes en interne. Une organisation se retrouve ainsi à la merci du cybercriminel, que ses motivations soient financières, liées à des activités d'espionnage ou visent à causer la fermeture de l'entreprise. Alors que le sondage souligne que les organisations sont de plus en plus conscientes des effets dévastateurs des violations de comptes à privilèges, celles-ci consacrent encore trop d'efforts à vouloir stopper les attaques périmétriques telles que le hameçonnage. »

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.globalsecuritymag.fr/Etude-les-cybercriminels-se,20150930,56282.html

---

Les sites Web du gouvernement thaïlandais attaqués | Le Net Expert Informatique

Les sites Web du gouvernement thaïlandais attaqués

Plusieurs sites gouvernementaux thaïlandais ont été la cible, dans la nuit de mercredi 30 septembre à jeudi 1er octobre, d'attaques dites de « déni de service », qui les ont rendus inaccessibles pendant plusieurs heures. Ce type d'attaque, appelée DDoS, consiste à multiplier les requêtes inutiles sur un site afin de le saturer. Parmi les sites visés, celui du gouvernement, du ministère de l'information et du ministère de la défense. Certains étaient encore difficiles d'accès jeudi matin.

Ces attaques sont généralement automatisées, mais mercredi, des appels à surcharger ces sites ont été relayés sur les réseaux sociaux, incitant les internautes à s'y connecter et à rafraîchir les pages au maximum. Objectif : dénoncer les projets du gouvernement sur l'avenir d'Internet.

« Grande muraille »

Les Thaïlandais s'inquiètent en effet de la censure grandissante exercée par la junte militaire au pouvoir sur Internet, qui a amplifié sa politique de censure, et multiplié les poursuites contre les internautes ayant émis des critiques sur la famille royale.

L'inquiétude est montée d'un cran la semaine dernière, après l'annonce discrète, sur un site gouvernemental, d'un projet de mise en place d'une gateway (« passerelle ») unique. Une gateway est une sorte de porte d'entrée permettant à un pays de se connecter au réseau mondial. La Thaïlande en possède actuellement une dizaine, gérées par des opérateurs publics ou privés. Se limiter à une seule gateway, opérée par la junte, pourrait faciliter la surveillance et la censure, dénoncent les détracteurs du projet.

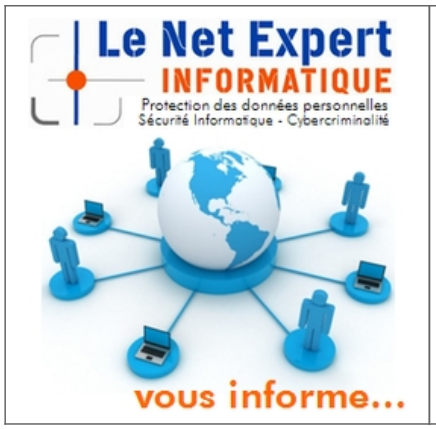
Ceux-ci ont réussi à réunir plus de 130 000 signatures sur une pétition en ligne contre ce projet surnommé « Great firewall of Thaïlande », en référence au Great firewall of China, cette « Grande Muraille » de l'Internet érigée en Chine.

Source :

http://www.lemonde.fr/pixels/article/2015/10/01/les-sites-web-du-gouvernement-thailandais-attaques-pour-protester-contre-la-censure_4779521_4408996.html

---

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

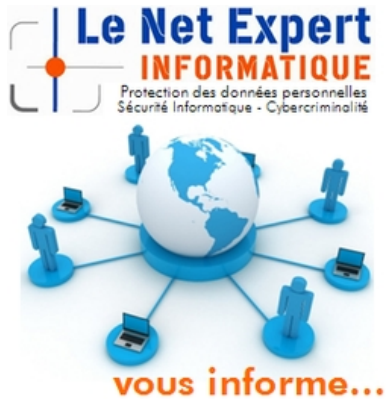
Amnesty International condamne un texte aux « motifs vastes et peu précis » qui « légalise la surveillance de masse », sans voie de recours. La surveillance à grande échelle, déjà présente dans la loi renseignement du 24 juillet 2015, ne viserait plus seulement l'antiterrorisme mais pourrait « être justifiée 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

Comment protéger au mieux les données clients des cyberattaques ? | Le Net Expert Informatique



Comment protéger au mieux les données clients des cyberattaques ?

Les derniers piratages des données bancaires de plus de 1,3 millions de clients Orange, les 83 millions de données de clients volées à la banque américaine JP Morgan Chase ou les menaces d'hackers de divulguer l'identité de 36 millions d'utilisateurs du site de rencontres canadien Ashley Madison… Tous ces épisodes démontrent que les cyber-attaques menacent aujourd'hui fortement la liberté individuelle et les données personnelles.

Elles viennent également rappeler qu'aucune entreprise, même bien protégée, n'est aujourd'hui en mesure de garantir à 100% la sécurité des données qu'elle manipule. Face à ce constat, les entreprises doivent changer la façon dont elles peuvent rapidement détecter et répondre en utilisant de nouvelles solutions plus précises, plus actionnables pour les équipes de sécurité. C'est un véritable enjeu pour les entreprises d'assurer à leurs clients la protection la plus fiable possible.

Voici 4 conseils aux entreprises pour protéger au mieux les données sensibles de leurs clients et les actions à mettre en place lors d'une attaque :

· Toute organisation chargée de la gestion des données personnelles très sensibles de leurs clients doit prendre ses responsabilités très au sérieux et protéger ainsi les données contre les accès non autorisés indésirables. Cela impliquerait de multiples niveaux de contrôles de sécurité au niveau de l'IT, peut-être en commençant par le cryptage des données personnelles alors qu'elles sont actives et en cours d'utilisation. Cette approche peut être efficace à la protection des données hautement sensibles, même si le réseau dans lequel elles résident est compromis. Cela peut paraître couteux à mettre en œuvre mais c'est une méthode de protection efficace.

· Il est capital d'avoir des processus et procédures internes qui garantissent l'accès physique aux centres de stockage de données sécurisées y compris de CLOUD. Les comptes d'utilisateurs inutilisés devraient être supprimés rapidement et les restrictions d'accès gérés de façon stricte pour s'assurer que tous les employés n'aient pas accès aux données de n'importe quel autre utilisateur.

· Nous pouvons également parler d'une nouvelle génération, solide dans son approche, permettant d'atténuer les menaces (en constante évolution) d'attaques malveillantes des réseaux d'entreprise provenant de l'extérieur. Les organisations "pirates" peuvent percevoir cela comme une énorme opportunité financière à voler les données personnelles détenues par quelque organisme que ce soit. Le fait d'avoir des défenses périmétriques fortes mises en place comme un pare-feu, des anti-virus sur toutes les stations de travail , d'une solution de filtrage d'e-mail, ou encore d'une solution IPS / IDS et un SIEM offrant la possibilité de surveiller les événements de toutes ces technologies en un seul endroit, ne restent malheureusement pas les plus fiables et beaucoup de sociétés ayant mis en place ces solutions ont quand même été attaquées, des brèches ont été exploitées car toutes ces solutions ne permettent pas d'arrêter tous les logiciels malveillants persistants qui vont compromettre un réseau en offrant la possibilité de se déplacer librement afin de trouver des données ciblées à voler.

· Là où les entreprises doivent se focaliser (en plus d'autres options internes déjà mentionnées), c'est de déployer une solution de détection des menaces plus intégrée qui peut extraire des informations à partir de plusieurs points dans le réseau, d'analyser ce qui se passe en temps réel (sur les stations de travail et sur le réseau) et défendre activement les réseaux d'entreprise avec la possibilité d'automatiser les réponses défensives générées en temps réel et 24 heures sur 24. Il y a encore à ce jour une réticence au niveau des comités exécutifs des entreprises de reconnaître la nécessité d'avoir un budget propre à la « Cyber Sécurité » mais qui permettrait de continuer à investir sur les dernières générations de solutions qui sont adaptées aux nouvelles menaces. Jusqu'à ce que cela change ; les cyber attaques vont continuer, les hackers utilisant des outils automatisés de pointe. Et nous continuerons de découvrir de nouvelles attaques de grandes ampleurs, quasiment tous les jours !

Par Bernard Girbal, Vice-Président EMEA chez Hexis Cyber Solutions

---

Source : http://www.infodsi.com/articles/157575/proteger-mieux-donnees-clients-cyberattaques-bernard-girbal-vice-president-emea-chez-hexis-cyber-solutions.html

---

Safe Harbor remis en question – Et si le transfert de

données personnelles aux US cessait ? | Le Net Expert Informatique

Safe Harbor remis en question – Et si le trans

Pour l'avocat général de la CUJE, la disposition autorisant les transferts de données vers les Etats-Unis (Safe Harbor) est invalide car le pays ne garantit pas la protection de ces données du fait de la surveillance par la NSA. Une Cnil européenne a de plus tout pouvoir pour suspendre ces transferts.

Entre Maximilian Schrems et Facebook, c'est une longue histoire d'amour (vache). C'est notamment à ce dernier qu'on doit d'avoir découvert l'ampleur de la collecte de données personnelles effectuée par le réseau social.
Remonté contre les pratiques de Facebook, le jeune autrichien l'est tout autant à l'encontre de la surveillance massive par les Etats-Unis. Pour accéder aux données des Européens, la NSA pourrait compter sur un dispositif : le Safe Harbor.

Une « des voies » des agences US pour accéder « à la collecte des données »

Le Safe Harbor prévoit le transfert automatique de données par les entreprises entre l'Europe et les Etats-Unis. C'est cet accord qui est visé par Maximilian Schrems au travers de sa plainte contre Facebook devant la justice irlandaise.
Le justiciable européen conteste le transfert de données à caractère personnel de Facebook Ireland à Facebook USA au motif que la protection de ses données n'est pas garantie du fait du programme PRISM de la NSA.
Saisie par la Haute Cour de Justice d'Irlande, la Cour de Justice européenne est appelée à se prononcer sur plusieurs points de droit. Pour l'heure, c'est l'avocat général de la CUJE, Yves Bot, qui a livré son analyse juridique.

Et en substance, ce dernier souligne le manque de garanties entourant le Safe Harbor et estime qu'une autorité nationale de protection peut enquêter sur les transferts de données réalisées dans ce cadre.

Plus encore, écrit l'avocat général, une autorité, au terme de ses investigations, « a le pouvoir de suspendre le transfert de données en cause » dès lors qu'elle estime qu'il « porte atteinte à la protection dont doivent bénéficier » les citoyens de l'UE.
Le Safe Harbor part du postulat que les Etats-Unis apportent un niveau de protection adéquat. Une obligation cependant qui se doit d'être continue, souligne Yves Bot. Cela « suppose qu'aucune circonstance intervenue depuis ne soit de nature à remettre en cause l'évaluation initiale effectuée par la Commission. »
Or, les révélations d'Edward Snowden au sujet de la surveillance par la NSA pourraient justement constituer une remise en cause. La Commission de l'UE elle-même estimait que le Safe Harbor était « l'une des voies par lesquelles les autorités américaines de renseignement ont accès à la collecte des données à caractère personnel initialement traitées au sein de l'Union. »

La « décision 2000/520 doit être déclarée invalide »

Pour l'avocat général de la CUJE, le « droit et la pratique des États-Unis permettent de collecter, à large échelle, les données à caractère personnel de citoyens de l'Union qui sont transférées dans le cadre du régime de la sphère de sécurité, sans que ces derniers bénéficient d'une protection juridictionnelle effective. »
C'est donc le principe même du Safe Harbor et des transferts automatisés de données qui est contesté. « Nous sommes, dès lors, d'avis que la décision 2000/520 doit être déclarée invalide dans la mesure où l'existence d'une dérogation qui permet d'une manière aussi générale et imprécise d'écarter les principes du régime de la sphère de sécurité empêche par elle-même de considérer que ce régime assure un niveau de protection adéquat aux données à caractère personnel qui sont transférées aux États-Unis depuis l'Union » va jusqu'à considérer le représentant de la CUJE.
« C'est formidable de voir que l'avocat général a utilisé cette affaire pour rendre un avis général sur les transferts de données vers des pays tiers et la surveillance de masse » réagit Maximilian Schrems.
« Si le système du Safe Harbor disparaît, il est très probable que les autorités de protection dans les 28 Etats membres de l'UE n'autoriseront pas les transferts de données des entreprises US soumises à des lois de surveillance de masse » ajoute-t-il.
Les géants américains du Web comme Facebook pourraient ainsi se voir interdire le droit de transférer les données des utilisateurs européens de leurs services vers les Etats-Unis. Les juges de la Cour de Justice de l'UE doivent toutefois rendre leur décision, en tenant compte ou non de l'avis de l'avocat général.

Source : http://www.zdnet.fr/actualites/safe-harbor-et-si-le-transfert-de-donnees-personnelles-aux-us-cessait-39825358.htm
Par Christophe Auffray

L’Europe pourrait revoir le transfert de données personnelles vers les Etats-Unis | Le Net Expert Informatique

L’Europe pourrait revoir le transfert de données personnelles vers les Etats-Unis

La justice européenne met un coup de canif dans le processus permettant aux services américains de puiser dans les informations personnelles d’internautes européens. Suite à une plainte concernant Facebook, l’avocat général de la CJUE demande qu’un pays puisse en demander l’arrêt.

Le Safe Harbor est un texte datant de 2000 autorisant, sous certaines conditions, des entreprises américaines à transférer des données personnelles présentes en Europe vers leur territoire. Un principe qui soulève des polémiques depuis les révélations autour de systèmes américains (NSA via le dispositif PRISM) permettant de consulter ces informations.
La justice européenne souhaite à présent revoir ce dispositif. L’avocat général de la Cour de Justice de l’Union européenne (CJUE) vient à ce titre de rendre un avis dans lequel il demande à ce que n’importe quel Etat membre puisse mettre en pause ce transfert de données. En conséquence, les services américains du renseignement ne pourraient plus puiser dans ce vaste vivier d’informations.
S’il ne s’agit ici que d’un avis (http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-09/cp150106fr.pdf) émis par l’avocat général Yve Bot sur l’épineuse question de la protection des données personnelles, le document demeure clair à l’encontre de la pratique. Il motive son avis en évoquant les cas de « défaillances systémiques constatées dans le pays tiers vers lequel des données à caractère personnel sont transférées, les États membres doivent pouvoir prendre les mesures nécessaires à la sauvegarde des droits fondamentaux protégés par la Charte des droits fondamentaux de l’Union européenne, parmi lesquels figurent le droit au respect de la vie privée et familiale et le droit à la protection des données à caractère personnel ».
Autrement dit, la justice considère que ce principe de transfert automatique de données constitue une « ingérence dans le droit au respect de la vie privée et dans le droit à la protection des données ». Elle demande donc à ce que les autorités nationales de protection des informations personnelles puissent conserver la main sur ce type d’activité.

Max Schrems, un étudiant autrichien au début de la polémique

Depuis à présent 4 ans, Max Schrems, un jeune autrichien s’attaque aux pratiques de Facebook en matière de conservation et de protection des données de ses utilisateurs. Après avoir en premier lieu reproché au réseau social de créer des profils fantômes de personnes inexistantes, il avait attaqué le service pour avoir communiqué à la NSA des informations sur ses inscrits, notamment dans le cadre du programme PRISM.
L’affaire avait été portée devant la Data Protection Commissioner (DPC), l’équivalent de la Cnil en Irlande puis auprès de la Haute Cour du pays (Etat dans lequel le siège de Facebook Europe se trouve). Le cas est ensuite remonté jusqu’à la CJUE.
Suite à la remise de cet avis, la question de la suspension du Safe Harbor se pose à nouveau. La Cour de justice peut désormais suivre ou non l’avis de l’avocat général avant de remettre sa décision définitive. Celle-ci devrait survenir dans les prochains mois.

Source :
http://pro.clubic.com/blog-forum-reseaux-sociaux/facebook/actualite-780512-facebook-europe-cour-justice.html?estat_svc=s%3D223023201608%26crmID%3D639453874_1165961926#pid=22889469

Stopper les attaques informatiques avant qu’elles ne bloquent l’entreprise | Le Net Expert Informatique

	Stopper les attaques informatiques avant qu’elles ne bloquent l’entreprise

Une récente étude de Gartner révèle que seulement 40 % des grandes organisations auront mis en place des plans de sécurité globaux afin de se prémunir contre les cyberattaques d'ici 2018. Cela signifie que 60 % des entreprises n'auront pas mis en place de stratégie d'ici trois ans, prenant un risque considérable face à des attaques de plus en plus sophistiquées qui pourraient atteindre un niveau supérieur au cours des prochaines années. Il ressort notamment de ce rapport que la priorité serait donnée à l'adoption de solutions de détection des attaques de manière réactive plutôt que proactive. Jean-François Pruvot, Regional Director France chez CyberArk, nous livre son analyse.

A l'heure où les cyberattaques sont de plus en plus nuisibles, les entreprises qui stockent des données sensibles figurent parmi les principales cibles. Le fait que la plupart des sociétés n'aient pas prévu de stratégie globale de sécurité d'ici à trois ans, et ce malgré les récentes attaques perpétrées contre de grands noms, témoigne souvent d'un manque de connaissances sur la manière de hiérarchiser les priorités dans le cadre de leurs programmes de sécurité ; cela laisse présumer que le hacker se trouve déjà à l'intérieur du réseau. Selon le général chinois Sun Tzu, dans son traité de stratégie militaire « L'art de la guerre », le succès de celle-ci repose sur la préparation mais également sur une bonne connaissance du terrain. Les entreprises doivent donc impérativement identifier l'ensemble des portes permettant d'accéder au « royaume IT », en particulier les comptes administrateurs ou à hauts pouvoirs qui conduisent à l'intégralité du système et des données qu'il renferme ; il est en effet impossible de protéger un espace sans connaître son étendue et ce qu'il contient.

La mise en place d'une stratégie globale de sécurisation de ces comptes et des systèmes d'information est donc indispensable pour limiter les vols et pertes de données, et se fait en plusieurs étapes clés.

Tout d'abord, partant du constat que la menace est peut-être déjà à l'intérieur, les RSSI doivent s'équiper d'outils de détection d'activités inhabituelles dans leurs systèmes. Cela leur permettra de contenir les menaces et de se prémunir contre l'infiltration progressive et malveillante de hackers dans le réseau en stoppant leur déplacement latéral. Une fois que les mesures de sécurité sont prises pour protéger les données, les comptes à privilèges difficilement détectables restent l'accès principal aux informations pour les pirates. Il est par exemple possible de les contourner pour pénétrer dans le système à l'aide de techniques de phishing classiques ; une fois à l'intérieur, le hacker peut s'y déplacer insidieusement et y installer des logiciels malveillants qui lui permettront de collecter autant de données que nécessaires sur des périodes pouvant se compter en années, et ce sans être détecté. Les comptes à hauts-pouvoirs qui ne sont pas suivis, gérés et protégés sont en effet l'une des vulnérabilités les plus répandues dans le cas de cyberattaques.

Enfin, une fois la stratégie établie, bien qu'il ne faille pas négliger la faille humaine, il est essentiel aujourd'hui que les entreprises ne se réfugient plus derrière cette excuse pour justifier les faiblesses des systèmes. En effet, que la menace vienne de l'intérieur ou de l'extérieur, les conséquences sont les mêmes pour les entreprises encore nombreuses à ne pas posséder les bases pour sécuriser leurs données ; elles doivent en effet commencer par mettre en place des correctifs, assurer leur mise à jour régulière, et surtout veiller au renforcement des contrôles sur les comptes à privilèges et administrateurs. Il est donc essentiel d'anticiper la présence de l'ennemi dans l'organisation et d'adopter ainsi une posture de gestion des risques concentrée sur la proactivité.

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.infodsi.com/articles/158490/gestion-risques-stopper-attaques-avant-bloquent-entreprise.html

Nouveau règlement européen sur la protection des données personnelles : Les changements pour les entreprises | Le Net Expert Informatique

Nouveau règlement européen sur la protection des données personnelles : Les changements pour les entreprises

Fin juillet, le Contrôleur Européen de la Protection des Données a publié ses recommandations sur le futur règlement européen portant à quatre le nombre de versions du document. L'occasion de faire le bilan sur les trois évolutions du règlement qui auront le plus d'impact pour les entreprises.

QUEL CHANGEMENT POUR LES ENTREPRISES ?

Mise en place du Privacy by Design (Articles 23, 30, 32a, 33a et 33)

Première nouveauté, les entreprises devront définir et mettre en œuvre des procédures permettant d'intégrer les problématiques liées à la manipulation des données personnelles dès la conception de nouveaux services.

Cette démarche s'accompagne de l'obligation de réaliser des analyses de risques relatives à la vie privée des personnes (discrimination, diffusion de données confidentielles, etc.) préalablement à la mise en place des traitements les plus sensibles et à chaque modification du traitement.

Face aux risques sur la vie privée des personnes induits par ces traitements, il sera imposé aux entreprises d'adopter des mesures de sécurité adéquates en vue de les maitriser.

Concrètement que retenir du Privacy by Design ?

Une mise à jour de la méthodologie projet afin d'identifier au plus tôt les traitements sensibles et une méthode d'analyse de risques à définir et outiller.

Il sera pour cela possible de s'inspirer des guides pratiques de la CNIL intitulés « Etude d'impact sur la vie privée », qui seront à simplifier et contextualiser aux besoins spécifiques de l'entreprise.

Responsabilisation ou « Accountability » (Articles 22 et 28)

Toute entreprise devra désormais être capable de prouver sa conformité vis-à-vis du règlement.

Cette exigence se traduit par :

• l'adoption d'une politique cadre de gestion des données à caractère personnel ;

• une organisation associée ;

• des procédures opérationnelles déclinant les thèmes du règlement (information, respect des droits des personnes, transfert à des sous-contractants, etc.).

L'entreprise devra également être en capacité de prouver l'application de ces politiques et donc, de mettre en place des processus de contrôle.

L'occasion de parler de la personne qui illustrera ce principe d' « Accountability » : le DPO (pour Data Protection Officer). Il devient quasiment obligatoire et remplace le CIL actuel.

Concernant ce DPO, le texte entérine l'obligation de lui fournir le personnel, les locaux, les équipements et toutes les autres ressources nécessaires pour mener à bien ses missions. Encore une fois le parlement souhaite aller au-delà de cette exigence : il propose de nommer au sein de la direction une personne responsable du respect du règlement.

Comment appliquer ce principe ? Il sera nécessaire de définir a minima une politique avec des règles de protection des données ainsi qu''un plan de contrôle et de formation. Cette politique pourra par exemple s'inspirer du modèle des BCR « Binding Corporate Rules », dont le principe a été entériné dans le futur texte, pour lesquelles des modèles types et des premiers retours d'expérience existent déjà.

Obligation de notification des fuites (articles 31 et 32)

L'ensemble des parties s'accordent sur l'obligation de notification des fuites aux autorités. Le Parlement propose même que les entreprises mettent en ligne un registre listant les types de brèches de sécurité rencontrées. Il sera intéressant de constater comment cette exigence cohabitera avec les législations nationales en matière de sécurité et la protection des intérêts de la nation qui tendent à limiter la diffusion de ce type d'information.

La notification de fuites aux personnes concernées, quant à elle, n'est obligatoire que si l'entreprise n'est pas en mesure de démontrer qu'elle a mis en œuvre des mesures afin de rendre cette fuite sans conséquence. D'où l'intérêt d'effectuer correctement l'analyse de risques, de définir et d'implémenter des mesures appropriées.

Au final, deux recommandations afin d'anticiper le futur règlement sur ce point :

• un processus de gestion des fuites de données à définir en l'orchestrant avec les dispositifs de gestion de crise existants et les processus de relation client,

• la réalisation d'exercices réguliers afin de tester son efficacité avec tous les acteurs concernés.

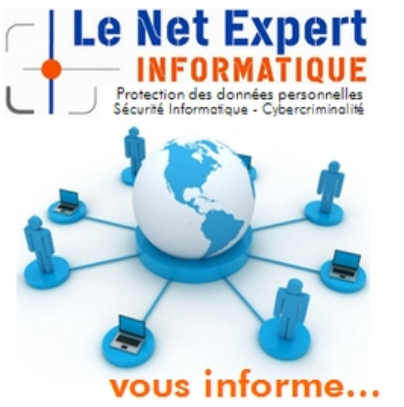
UNE MISE EN CONFORMITÉ À ANTICIPER

Au-delà de ces trois nouveautés majeures, d'autres modifications plus limitées en termes d'impacts organisationnels sont également à prendre en compte, comme la création du droit à la portabilité ou l'extension de la liste des données sensibles. On peut par ailleurs noter le renforcement d'obligations existantes comme le droit à l'information et le recueil du consentement. Le diable se nichera dans les détails.

Pour conclure, les deux années de mise en application du règlement ne seront pas de trop (soit une mise en conformité d'ici début 2018) et nous ne pouvons que conseiller d'initier la mise en conformité dès 2016, avec le cadrage et le lancement des premiers chantiers majeurs. D'autant plus que le sujet devient de plus en plus visible médiatiquement (condamnation récente de Boulanger, Google et l'application du droit à l'oubli, etc.) et que les sanctions financières deviennent réellement significatives (entre 2 et 5% du chiffre d'affaire mondial). L'occasion pour toutes les entreprises de communiquer largement sur les principes de respect de la vie privée effectivement appliqués.

Source : http://www.solucominsight.fr/2015/09/nouveau-reglement-europeen-sur-la-protection-des-donnees-personnelles-anticiper-les-3-impacts-majeurs/

Multiples vulnérabilités dans Apple iTunes | Le Net Expert Informatique



Multiples vulnérabilités dans Apple iTunes

1 – Risque(s)exécution de code arbitraire à distance
déni de service à distance
atteinte à la confidentialité des données

2 – Systèmes affectés
Apple iTunes version antérieure à 12.3

3 – Résumé
De multiples vulnérabilités ont été corrigées dans Apple iTunes. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et une atteinte à la confidentialité des données.

4 – Solution
Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 – Documentation
Bulletin de sécurité Apple HT205221 du 16 septembre 2015
https://support.apple.com/fr-fr/HT205221
Référence CVE CVE-2010-3190
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3190
Référence CVE CVE-2014-8146
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8146
Référence CVE CVE-2015-1152
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1152
Référence CVE CVE-2015-1153
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1153
Référence CVE CVE-2015-1157
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1157
Référence CVE CVE-2015-1205
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1205
Référence CVE CVE-2015-3686
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3686
Référence CVE CVE-2015-3687
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3687
Référence CVE CVE-2015-3688
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3688
Référence CVE CVE-2015-3730
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3730
Référence CVE CVE-2015-3731
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3731
Référence CVE CVE-2015-3733
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3733
Référence CVE CVE-2015-3734
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3734
Référence CVE CVE-2015-3735
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3735
Référence CVE CVE-2015-3736
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3736
Référence CVE CVE-2015-3737
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3737
Référence CVE CVE-2015-3738
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3738
Référence CVE CVE-2015-3739
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3739
Référence CVE CVE-2015-3740
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3740
Référence CVE CVE-2015-3741
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3741
Référence CVE CVE-2015-3742
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3742
Référence CVE CVE-2015-3743
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3743
Référence CVE CVE-2015-3744
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3744
Référence CVE CVE-2015-3745
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3745
Référence CVE CVE-2015-3746
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3746
Référence CVE CVE-2015-3747
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3747
Référence CVE CVE-2015-3748
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3748
Référence CVE CVE-2015-3749
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3749
Référence CVE CVE-2015-5755
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5755
Référence CVE CVE-2015-5761
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5761
Référence CVE CVE-2015-5789
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5789
Référence CVE CVE-2015-5790
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5790
Référence CVE CVE-2015-5791
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5791
Référence CVE CVE-2015-5792
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5792
Référence CVE CVE-2015-5793
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5793
Référence CVE CVE-2015-5794
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5794
Référence CVE CVE-2015-5795
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5795
Référence CVE CVE-2015-5796
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5796
Référence CVE CVE-2015-5797
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5797
Référence CVE CVE-2015-5798
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5798
Référence CVE CVE-2015-5799
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5799
Référence CVE CVE-2015-5800
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5800
Référence CVE CVE-2015-5801
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5801
Référence CVE CVE-2015-5802
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5802
Référence CVE CVE-2015-5803
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5803
Référence CVE CVE-2015-5804
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5804
Référence CVE CVE-2015-5805
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5805
Référence CVE CVE-2015-5806
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5806
Référence CVE CVE-2015-5807
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5807
Référence CVE CVE-2015-5808
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5808
Référence CVE CVE-2015-5809
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5809
Référence CVE CVE-2015-5810
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5810
Référence CVE CVE-2015-5811
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5811
Référence CVE CVE-2015-5812
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5812
Référence CVE CVE-2015-5813
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5813
Référence CVE CVE-2015-5814
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5814
Référence CVE CVE-2015-5815
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5815
Référence CVE CVE-2015-5816
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5816
Référence CVE CVE-2015-5817
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5817
Référence CVE CVE-2015-5818
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5818
Référence CVE CVE-2015-5819
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5819
Référence CVE CVE-2015-5821
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5821
Référence CVE CVE-2015-5822
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5822
Référence CVE CVE-2015-5823
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5823
Référence CVE CVE-2015-5874
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5874
Référence CVE CVE-2015-5920
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5920
Gestion détaillée du document

18 septembre 2015
version initiale.
Dernière version de ce document : http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-398