Quels changements anticiper ? Le règlement européen sur les données personnelles annoncé pour le printemps :

	Quels changements anticiper Le règlement européen sur les données personnelles annoncé pour le printemps : ?

Ce règlement, dont le premier projet remonte à 2012, est appelé à remplacer la directive de 1995 « relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ». Son objectif est d'uniformiser les règles en matière de protection des données personnelles en Europe, de garantir la libre circulation de ces données sur le territoire de l'Union et de simplifier l'exercice de leurs droits par les citoyens européens.

Après des débats parfois acharnés entre les acteurs en présence, que ce soit les CNIL européennes, les acteurs de l'internet et du Big-Data ou encore les représentants des consommateurs, une version consolidée a été arrêtée et diffusée le 15 décembre 2015.
De la loi du 6 janvier 1978 au futur règlement, la législation en matière de protection des données personnelles est allée dans le sens d'une complexité et d'une incertitude toujours plus grande. Les entreprises peuvent-elles attendre plus de sécurité juridique du futur règlement ? La réponse est contrastée.

Un projet de texte stabilisé… mais pas encore adopté
Il convient tout d'abord de tempérer l'enthousiasme affiché des institutions européennes : le texte définitif n'est pas encore adopté. Après un premier vote du Parlement européen en mars 2014, le Conseil de l'Union européenne donnait mandat au Luxembourg en juin 2015, dans le cadre de la présidence tournante de l'Union européenne, pour parvenir à un consensus sur le projet de règlement au plus tard fin décembre de la même année. Au terme de discussions intenses, Parlement et Conseil sont parvenus à un accord *in extremis* avant la trêve des confiseurs sur un document de pas moins de 200 pages…
Cet accord n'est pour le moment que politique, et la prochaine étape est un vote en deuxième lecture par le Parlement européen pour adoption définitive.
Le règlement européen sera ensuite applicable dans un délai de deux ans après son adoption. La différence essentielle par rapport à la directive de 1995 est que ce texte sera directement applicable au sein de l'Union européenne, sans que chacun des 27 états ne doive adopter des lois nationales de transposition, ce qui aurait nécessairement nui à l'objectif d'harmonisation. Les règles européennes nouvelles remplaceront donc automatiquement les règles nationales existantes incompatibles. Ainsi, pour ses 40 ans, la Loi française du 6 janvier 1978 dite « Informatique et Libertés » va se retrouver fortement vidée de sa substance.
Les entreprises ont donc encore un peu de temps devant elles pour se préparer à la mise en œuvre des nouvelles règles. Quels sont les changements majeurs à anticiper ?

***« Accountability »* et « *Privacy by Design* » sont des termes qui doivent devenir familiers**
Quelles données pourront être traitées ? Quelle durée de conservation appliquer ? Quels outils techniques installer ? Quelles formalités accomplir ?
Si le règlement uniformise la réponse à ses questions au sein de l'Union européenne… il ne les simplifie par nécessairement. Une large place sera faite à l'interprétation des dispositions nouvelles.

La **définition des données personnelles** ne change pas fondamentalement. Le règlement s'applique aux traitements des données identifiantes ou permettant d'identifier une personne, que ce soit directement ou indirectement. Le projet de règlement ajoute toutefois une série d'exemples de données qui permettent d'identifier une personne : son nom, mais également un numéro d'identification, une donnée de localisation, un identifiant d'un compte en ligne, ainsi que des références à des informations relatives à l'identité physique, génétique, mentale, économique, sociale ou culturelle d'une personne. Ces précisions sont dans la logique de la position actuelle des juridictions européennes et françaises.
S'agissant des **modalités de traitement** des données personnelles, il est abondamment fait référence dans le texte à la notion de *Privacy by Design*.
Qu'est-ce que cela signifie concrètement ? Les entreprises seront désormais tenues d'anticiper les sujets relatifs aux traitements de données dès les premières étapes de leurs projets informatiques, afin qu'il soit vérifié en amont que les développements à intervenir, où les logiciels à implémenter, seront conformes aux exigences imposées par le règlement.
Le responsable du traitement devra ainsi « *implémenter les mesures techniques et organisationnelles appropriées, telles que l'anonymisation, qui sont conçues pour mettre en œuvre les principes de protection des données, […] d'une manière effective et d'intégrer les protections nécessaires dans les traitements de manière à respecter les exigences du règlement et à protéger les droits des intéressés.* »
Une pondération devra en effet être faite entre coûts, état de l'art, contexte, finalités des traitements concernés, risques pour les droits et libertés des individus, etc. Autant de concepts dont la cohabitation laissera une grande place à une appréciation au cas par cas. Le règlement envisage qu'un mécanisme de certification soit mis en place, probablement afin de faciliter cette appréciation, bien que les procédures de certifications pèchent parfois par leur complexité.
Comme en l'état actuel de la législation, le règlement ne prévoit pas expressément de **durée de conservation des données**, et l'on peut le regretter. L'appréciation d'une durée de conservation des données sous une forme identifiante « *qui n'excède pas la durée nécessaire aux finalités pour lesquelles [les données] sont collectées et traitées* », place souvent le responsable de traitement dans une situation d'insécurité juridique. En revanche, dans sa dernière version, le projet de règlement prévoit que cette durée de conservation, ou *a minima* les critères retenus pour fixer cette durée, devront être portés à l'attention de la personne concernée dès la collecte. Les responsables de traitements devront donc apporter une attention particulière à ce sujet avant la mise en œuvre du traitement.
Les **formalités administratives** seront allégées : moins de notifications préalables aux autorités nationales, moins d'interlocuteurs. Un des objectifs principaux de ce texte est de garantir la libre circulation des données au sein de l'Union européenne. Ainsi, pour les groupes ayant des établissements dans plusieurs pays d'Europe, ou une activité ciblant plusieurs Etats-Membres, le principe du « guichet unique » permettra que les formalités requises ne soient effectuées qu'auprès de l'autorité de l'Etat Membre dans lequel le groupe a son établissement principal, les autorités des différents Etats Membres devant ensuite coopérer entre elles.
Les sociétés établies en dehors de l'Union européenne, mais ayant une activité ciblant le public européen, devront quant à elles désigner un représentant sur le territoire de l'Union, qui agira comme point de contact unique, tant pour les autorités que pour les personnes dont la société en question traite les données. A l'instar des pratiques en matière de fiscalité, cette dernière exigence incitera très probablement les grands acteurs du numérique non établis en Europe à désigner un représentant dans un Etat Membre dont l'autorité nationale de protection des données aura des règles réputées plus souples, ou disposera de moins de moyens pour diligenter des contrôles ou engager des procédures de sanction. Ces disparités devraient toutefois être tempérées par la coordination qu'assurera la nouvelle autorité européenne instaurée par le règlement.
En revanche, les **procédures internes seront quant à elles décuplées…** Un contrôleur à la protection des données devra être désigné dans les entités publiques et dans les entreprises traitant des données personnelles à une échelle importante. Il convient de souligner qu'il n'y a pas de seuil chiffré permettant à une entreprise de déterminer si elle doit ou non désigner une telle personne. Sa désignation est requise lorsque l'activité de l'entreprise implique le traitement de données personnelles de manière régulière et systématique sur une large échelle…
Le contrôleur pourra alternativement être salarié ou prestataire de service. Le responsable de traitement devra également tenir à jour des registres des traitements mis en œuvre sur le même modèle que ce qui existe actuellement pour les CIL. Dans la logique du principe d'« *accountability* », ces mesures devront permettre au responsable de traitement de démontrer que les traitements qu'il met en œuvre se font en conformité avec le règlement.
Afin de faciliter aux entreprises la mise en œuvre de telles procédures, et la démonstration de conformité du responsable de traitement à ses obligations, le règlement renvoie ici encore à un mécanisme de certification ou à des codes de conduite.

Et côté personnes physiques, quels droits ? Quelles protections nouvelles ?
Les personnes dont les données sont traitées devront bénéficier d'une **information plus large** sur les traitements qui les concernent. Outre les informations qui doivent déjà être fournies lors de la collecte de données en application de la Loi Informatique et Libertés, le responsable de traitement doit notamment préciser le fondement juridique du traitement, ainsi que la possibilité de déposer plainte auprès d'une autorité compétente d'un Etat Membre. Les mentions d'informations fournies par les responsables de traitement devront donc être ajustées.
Les personnes dont les données sont traitées bénéficieront d'un **droit à la portabilité de leurs données**. Les responsables de traitement devront donc être en mesure de restituer aux personnes dont les données sont traitées lesdites données, et ce dans un format standard et exploitable, afin qu'elles puissent être communiquées à un autre prestataire de services. Cette communication de données pourra même se faire directement au nouveau prestataire sur demande de la personne concernée.
Le projet de règlement prévoit des règles nouvelles encadrant **les traitements de données relatives aux enfants**. Ainsi, l'article 8 du projet de règlement prévoit une disposition visant à interdire aux services de la société de l'information destinés aux mineurs de 16 ans de recueillir leurs données personnelles sans autorisation préalable d'un titulaire de l'autorité parentale. Les Etats Membres pourront décider d'abaisser cette limite d'âge jusqu'à 13 ans. Le texte ajoute que le responsable de traitement devra fournir des efforts raisonnables, au regard des technologies disponibles, pour vérifier que le consentement est bien fourni par le titulaire de l'autorité parentale.
Les éléments détaillés ci-dessus ne sont que quelques points d'attention extraits parmi les 209 pages du projet de règlement dans sa dernière version. Les subtilités se cachent dans les détails et les 4 années de modifications et de reformulations du texte depuis sa première mouture ont pu altérer sa cohérence. Les deux années avant l'entrée en vigueur des dispositions nouvelles ne seront pas de trop pour permettre aux entreprises de se mettre en conformité. D'autant qu'en cas de manquement, les sanctions administratives pourront désormais aller jusqu'à 20 000 000 d'euros ou 4% du chiffre d'affaires mondial… ce qui est sans commune mesure avec les 150 000 euros d'amende que peut à ce jour prononcer la CNIL.

Réagissez à cet article

Source : *Le règlement européen sur les données personnelles annoncé pour le printemps : Quels changements anticiper ? – Féral-Schuhl Sainte-Marie*

Des règles désormais plus strictes pour la protection des données privées

Des règles désormais plus strictes pour la protection des données privées

La réforme décidée par le Parlement, la Commission et le Conseil européen aura de profondes implications. De plus le texte s'étendra aux pays associés à l'Union : Liechtenstein, Norvège et Islande. La Suisse s'en s'inspirera-t-elle ?

Après 3 ans, Parlement, Commission et Conseil Européen, le « trilogue » bruxellois, sont d'accord sur la réforme de la protection de la vie privée. La directive de 1995 et ses mises à jour étaient obsolètes et furent transposés sans harmonie dans les Etats, d'où l'idée d'un règlement qui s'appliquera tout de suite.

Ce règlement s'applique aux données privées traitées, pas celle qui sont stockées en vrac. Ce sont les résultats qu'on tire de l'exploitation de ces données qui sont dangereuses. Le règlement ne s'appliquera pas aux traitements des données dans un cadre privé (ouf !). Les autorités judiciaires ne seront pas soumises au contrôle des commissions de vie privée

Celui qui gère et traite vos données (le data controller) devra bien être identifié et réel. Celui qui héberge ses données (data processor) tombe aussi sous le règlement : s'il n'est pas établi dans l'Union, le règlement s'applique à lui quand même , surtout s'il s'agit de profiler le comportement en ligne des citoyens européens. Le pays superviseur sera celui du pays du siège principal du data controller et non pas là où les data centers ont été (dé)localisés. C'est à ce prix qu'un Amazon ou Google n'aura plus à dépendre de 28 commissions de vie privée différentes. Si l'entité n'est pas présente dans l'Union, elle doit mandater un représentant.
Le règlement évoque la pseudonymisation, une contraction d'anonymisation et pseudonyme : l'usage de pseudonymes n'exempte pas les sites d'appliquer le règlement, car on peut souvent remonter à qui est derrière. Par contre, le règlement ne s'applique plus après un décès !

Consentement
Le consentement de l'individu au traitement de ses données, qui existe depuis 1995, sera explicite et non tacite). Le data controller doit en garder la preuve: elle sera non valable si l'utilisateur final a subi un petit chantage (par ex. un service dégradé sans ces données privées). Pour la recherche scientifique, on admet qu'il n'est pas facile de demander à l'avance ce consentement, car on ne sait pas toujours ce qui va en sortir.
Si le data controller détecte des crimes ou des menaces à l'ordre public, il doit les communiquer aux autorités. Idem en cas de cybermenace.
Si le traitement des données vise un but humanitaire, de santé publique (épidémies), ou un cas d'urgence pour l'utilisateur final, leur traitement va de soi, consentement ou pas!
Les données sur l'emploi, la protection sociale et les revenus devraient aussi pouvoir être exploitées si le but est, pour l'État, d'augmenter le bien-être public et une politique ad hoc.
Le traitement de données personnelles doit être proportionnel : si on peut l'éviter à service équivalent, c'est mieux. De même, si la société qui a des données de vous ne sait pas vous identifier, elle ne doit pas chercher à le savoir pour… avoir votre consentement.

Les données sensibles : race, religion, opinion politique
Les données liées à l'exercice de droits et de choix fondamentaux, comme la religion, l'appartenance politique ou la race bénéficient d'une protection renforcée. Leur traitement devrait être une exception et soumis, avant leur exécution, à une analyse d'impact du risque encouru d'un tel profilage. Par contre, les photographies ne seront pas protégées saut à contenir des données biométriques.

Accès et rectification de données chez les tiers
Le droit à la rectification doit être aisé à exercer, en ligne par exemple si les données ont été collectées ainsi. Une réponse, oui ou non, sera fournie dans le mois.
À charge pour le data controller de vérifier que celui qui adresse sa demande d'accès est la bonne personne. Le droit à l'oubli à la «Google» devient… un droit à l'effacement si les données collectées ne sont plus nécessaires ou ne sont plus traitées. Ce droit à l'effacement s'opérera en cascade : les entités qui auraient rendu les données publiques seront obligées d'informer les autres qui les exploiteraient ou les auraient copiés.
À une demande d'une copie de ses données personnelles (droit d'accès), c'est un format lisible par un humain qui est exigé, pas du binaire ! D'ailleurs, dit le règlement, ne faudrait-il pas un format de donnes interopérables pour permettre, enfin, la portabilité des données entre sociétés. Il n'est pas précisé si c'est applicable au cloud (car c'est du stockage, pas du traitement). Le règlement évoque les algorithmes qui prennent des décisions sur base des données personnelles ainsi que le profilage.

Fuites et vol des données
Les fuites de données devront être notifiées aux autorités et aux personnes impactées dans les 72 heures à moins que leur chiffrage ne les rendent inviolables. À noter tout de même un relâchement de l'obligation de notifier à la commission de vie privée tous les traitements des données personnelles, uniquement les cas risqués d'atteintes aux droits et libertés fondamentales.

Échanges internationaux
Les données peuvent être échangées avec des pays tiers en dehors de l'Union : c'est à la Commission de statuer si le pays répond ou non aux exigences minimales de sécurité. La Commission peut aussi retirer son agrément.
Le data controller peut toutefois continuer à opérer avec un pays « peu sûr » s'il compense avec des mesures de sécurité supplémentaires. Les sociétés peuvent mettre en place entre leurs filiales des règles internes pour atteindre un même niveau de sécurité que le règlement. Attention aux échanges avec des pays tiers (ex : les USA à la demande d'une cour) et donc à l'application extraterritoriale de ses lois à des citoyens européens : ils sont autorisés s'ils sont couverts par un traité d'assistance mutuel.
Le texte s'étendra aux pays associés à l'Union : Liechtenstein, Norvège et Islande. La Suisse s'en s'inspirera-t-elle ?

Réagissez à cet article

Source : *Serrage de vis européen sur la protection des données privées – Le Temps*

Impact sur les entreprises du

règlement général sur la protection des données

Impact sur les entreprises du règlement général sur la protection des données

Dans un autre article, j'ai insisté sur le fait que l'impact du Règlement général sur la protection des données était lourdement sous-estimé. Dans cet article, j'explique pourquoi la conformité est essentielle, et je passe en revue les étapes à suivre pour s'assurer de la conformité au Règlement. Il ne s'agit pas d'une liste de tâches à accomplir, mais d'un virage fondamental dans la mise en place de la conformité.

Pour commencer, il existe de nombreuses définitions de la conformité, mais deux principes clés se dégagent :

Le permis d'exploitation : si votre organisation est une banque, un hôpital ou un service public en particulier, sa mission est de se conformer au respect de la vie privée, surtout si elle manipule des données sensibles sur les citoyens. Ce genre d'organisations est toujours exposé à des lois. Il est donc important d'intégrer les processus sans délai, au quotidien ; il ne peut pas s'agir d'un exercice qu'on effectue une fois par an.

Le comportement et la culture de l'organisation : la conformité doit faire partie de l'ADN de toute l'entreprise, et être le catalyseur d'un changement du comportement des employés, même si les initiatives liées à la conformité émanent du Comité de Direction. Si la Direction est la seule à imposer les changements, les appels à la conformité porteront leurs fruits trois ou quatre fois, mais le processus peut se déliter à la cinquième fois.

Étant donné le caractère vital de la conformité, il est important de ne pas prendre en compte les seuls processus technologiques, mais aussi leur intégration aux processus business et à la mise à disposition d'informations. Voici quelques conseils de base pour aider les organisations à appliquer le futur Règlement général sur la protection des données.

Comprendre la gouvernance des données.

Avant de s'engager dans un projet de conformité, il est important d'avoir des données de qualité, de comprendre leur origine, le système ou l'application où elles sont stockées, et si les informations sont exactes et complètes. Si des tiers sont impliqués, assurez-vous de l'existence d'accords contractuels relatifs à la conservation et à la propriété de ces données.

Faire une analyse des écarts. Les organisations ont généralement déjà mis en place des contrôles concernant la vie privée. Cependant, lorsqu'un nouvel élément législatif tel que le règlement général sur la protection des données entre en vigueur, il est important de déterminer quels contrôles seront suffisants pour appliquer la législation et d'examiner quels points de contrôles doivent être étendus.

Concevoir et développer des contrôles. Après avoir identifié les faiblesses de votre processus de conformité, par exemple au niveau des ressources humaines ou des finances, il vous faudra définir et mettre en place de nouveaux contrôles pour pallier ces manques.

Installer des logiciels de chiffrement. Afin de garantir le transfert sécurisé des données individuelles, qu'elles concernent un client, un fournisseur ou un employé. Il existe toujours un risque potentiel lié à la vie privée, si ces données sont utilisées à des fins non autorisées.

Prouver la conformité et la traçabilité des informations. Il est important que toutes les données soient en place pour répondre aux questions des auditeurs. Il est envisageable d'avoir recours à un tiers pour exercer une fonction d'assurance qualité avant l'arrivée des auditeurs. Nous aidons les entreprises internationales à faire la preuve de leur conformité, informations précises et exhaustives à l'appui.

De plus en plus, le respect de la vie privée devient une préoccupation. Les organisations doivent avoir une vision complète des données en leur possession, de manière à apporter la preuve solide de leur conformité et à établir une relation de confiance avec les fournisseurs, les clients et les citoyens. Le Règlement général sur la protection des données entrera bientôt en vigueur. Il est désormais temps d'évaluer la gouvernance de vos données et les pratiques de sécurité et de confidentialité qui leur sont appliquées.

Réagissez à cet article

Source : *Appliquer le Règlement général sur la protection des données – Abbas Shahim, Atos Consulting*

À partir de quel âge peut-on laisser les ados s'inscrire sur les réseaux sociaux ?

À partir de quel âge peut-on laisser les ados s'inscrire sur les réseaux sociaux ?

Les réseaux sociaux seront-ils bientôt interdits aux moins de 16 ans ? La nouvelle législation européenne sur la protection des données, approuvée le 17 décembre, entend relever l'âge minimum pour pouvoir s'inscrire sans consentement parental.

Bruxelles prévoit d'interdire l'accès aux réseaux sociaux aux adolescents de moins de 16 ans, qu'en est-il exactement ?

Pour le moment, il s'agit d'un accord de principe qui devra être soumis au vote du Parlement européen en 2016. Rien n'est donc fait. Cette disposition, ajoutée à la dernière minute au texte sur la protection des données personnelles, fixe à 16 ans l'âge minimum pour s'inscrire sur les réseaux en ligne. Mais chaque État peut ensuite déterminer ses propres limites entre 13 ans et 16 ans.

La règle n'est pas très contraignante, mais c'est tout de même un progrès puisque, à ce jour, aucune loi française ne fixe l'âge d'utilisation pour les mineurs. Actuellement, nous appliquons le droit américain avec la loi COPPA (Children's Online Privacy Protection Act) qui interdit aux sites de recueillir des données d'enfants de moins de 13 ans, sans consentement parental. Si outre-Atlantique, celle-ci est très contraignante, ce n'est pas le cas en France. Les jeunes peuvent s'inscrire en mentant sur leur âge sans conséquences.

À partir de quel âge peut-on les laisser s'inscrire ?

En dessous de 13 ans, ce n'est pas souhaitable car les enfants ne font pas la différence entre vie publique et vie privée. À partir de 13 ou 14 ans, en revanche, ils commencent à acquérir un esprit critique qui leur permet de prendre un peu de recul. Mais la question n'est pas tant l'âge auquel il faut les laisser s'inscrire sur les réseaux sociaux que celui auquel on leur donne un smartphone. Ces petits joujoux sont des réseaux sociaux à eux tout seuls, avec les SMS. Ils donnent en outre accès à tous les sites Internet. Or, la plupart des parents ne pensent pas à installer un contrôle parental.

Il faut donc retarder le plus possible l'acquisition du smartphone, à la fois pour protéger l'enfant des contenus inappropriés et pour qu'il comprenne qu'on peut s'en passer. Un tiers des élèves de CM1-CM2 que je rencontre lors de mes interventions dans les établissements scolaires possède un smartphone. Difficile dans ces conditions de ne pas devenir dépendant.

Smartphone ou ordinateur, comment accompagner les adolescents sur les réseaux sociaux ?

Il faut commencer par installer un contrôle parental, quel que soit le terminal. Les parents doivent ensuite expliquer à l'adolescent la stratégie de ces sites Internet qui revendent les données personnelles à des fins publicitaires. Les contenus sont gratuits, mais l'utilisateur devient en quelque sorte un produit commercial. Une fois cette dimension abordée, il faut l'accompagner dans la phase d'inscription en regardant avec lui les différents paramètres du site. Ainsi, il est primordial de limiter l'accès aux publications aux seuls amis, de même qu'il ne faut pas accepter d'inconnus ou de simples connaissances dans son réseau. Il est également essentiel de rappeler à l'adolescent qu'une fois en ligne, les contenus ne peuvent plus être supprimés, ou alors au prix de démarches complexes sans aucune garantie, puisque n'importe qui peut en faire une copie.

Certains réseaux sociaux sont un peu plus encadrés que d'autres. C'est le cas de Facebook, Instagram et WhatsAPP (qui appartiennent au premier) ainsi que Twitter. En revanche, je déconseille fortement Snapchat. Cette application, qui permet d'échanger des photos de manière instantanée et soi-disant éphémère, est beaucoup plus incontrôlable. Quel que soit le site ou l'application, les parents doivent toujours accompagner les adolescents et, a fortiori, les enfants dans l'univers numérique… comme ils le ferraient dans la rue ou sur la route.

Réagissez à cet article

Source : *À partir de quel âge peut-on laisser les ados s'inscrire sur les réseaux sociaux ? | La-Croix.com – Actualité*

Plus fort que les cookies, découvrez les super-cookies

Plus fort que les cookies, découvrez les super-cookies

Dans un précédent bulletin d'actualité [1], était présenté comment les cookies HTTP (ou témoins de connexion), pouvaient être utilisés à des fins de profilage de l'utilisateur, dans le but notamment de pouvoir lui proposer du contenu ciblé. Après un bref rappel, cet article se propose de parcourir plus largement les mécanismes complémentaires existants à l'heure actuelle, à des fins de sensibilisation aux problématiques de vie privée sur l'Internet, et dans l'optique de permettre la prise des précautions d'usage adaptées à son utilisation au quotidien, dans un contexte professionnel comme personnel.

Techniques de pistage – Cookies – et évolutions

La technique la plus utilisée en matière de pistage d'utilisateurs sur l'Internet repose sur l'exploitation des cookies. Nous rappelons que le terme cookie désigne une variable utilisée par un serveur HTTP pour sauvegarder des informations sur la session HTTP courante. Il est composé d'une paire obligatoire nom/valeur, et d'attributs optionnels, comme la date d'expiration, le domaine et le chemin. Ces informations sont créées et mises à jour lors des échanges entre un serveur et un client Web grâce à des en-têtes dédiés du protocole HTTP (« Set-Cookie », « Cookie ») [2].
Le premier cas d'usage des cookies est tout à fait nécessaire à la navigation sur de nombreux sites Web, par exemple pour le maintien d'une session applicative ou la mémorisation d'un panier d'achats, on parle alors de « cookies de premier niveau ». Il existe cependant d'autres cas d'utilisations controversés sur le plan du respect de la vie privée. En particulier, l'usage de « cookies tiers » (ou « tierce partie ») [1], notamment dans l'optique d'établir des statistiques de consultation, peut permettre par exemple d'offrir des services de publicité ciblée. Ces cookies sont reconnaissables en particulier à leur domaine d'appartenance différent de celui de la page consultée, et peuvent parfois permettre d'identifier finement un utilisateur donné (par exemple cookies Google).

D'autres mécanismes permettent la conservation de données utilisateur, qui exploitent d'autres modes de création et de stockage que les cookies HTTP. On regroupe généralement ceux-ci sous le terme « supercookie ». Ils s'appuient notamment sur l'utilisation :
• mécanismes de stockage local dédiés à des applications Web au-dessus du protocole HTTP, comme Adobe Flash (« Local Shared Objects », également appelés « cookies Flash »), Microsoft Silverlight (« Silverlight Isolated Storage ») ou encore HTML5 (« HTML5 storage ») ;
• d'objets dans le contenu des pages Web, comme la propriété « window.name » en JavaScript, qui peut être détournée pour stocker temporairement des informations ;
• du cache du navigateur et de l'historique de navigation, pour stocker sous forme encodée des informations ;
• de HSTS (« HTTP Strict Transport Security ») [3], mécanisme de politique de sécurité pour HTTP, permettant à un serveur de demander le passage vers HTTPS via un champ d'en-tête HTTP (« Strict-Transport-Security »), mais dont une utilisation détournée permet à tiers contrôlant plusieurs domaines d'identifier de façon unique un utilisateur [4].

Cette liste, non exhaustive, montre bien qu'il existe de nombreuses façons de stocker des données issues de la navigation Web, et qu'un simple nettoyage des cookies HTTP via le navigateur ne peut pas suffire à effacer proprement l'ensemble de celles-ci. D'ailleurs, on parle de « cookie zombie » pour désigner des cookies HTTP qui sont régénérés après leur suppression grâce à l'utilisation des supercookies. L'application Evercookie [5], par exemple, illustre cela, permettant la propagation des cookies HTTP dans autant que mécanisme de stockage que possible afin d'assurer la résilience de l'information.

Autres techniques
Si les cookies (et assimilés) permettent d'obtenir une masse d'informations très intéressante, ils ne sont pas pour autant la seule source considérée par les entités cherchant à pister l'utilisateur. Il existe en particulier de nombreuses autres méthodes permettant d'identifier de façon unique un utilisateur, parfois à la granularité du terminal utilisé (téléphone, ordinateur, téléviseur connecté, tablette, etc.).
Ces méthodes peuvent être classées en cinq catégories [6] :
• entification générée par le client : certains terminaux ou applications clientes génèrent un identifiant unique pouvant être accessible par les services tiers à des fins publicitaires (advertising identifiers).
• Identification via des éléments réseau : certains équipements réseau situés entre le client et le serveur insèrent des éléments permettant, volontairement ou non, d'identifier l'utilisateur. Par exemple, l'utilisation du champ « X-Forwarded-For » dans l'en-tête HTTP précise l'adresse IP d'origine d'un client se connectant à travers un serveur mandataire.
• Identification par le serveur : certains serveurs ajoutent des pixels-espions [7], images de très petite taille généralement non repérables par l'utilisateur, qui permettent la génération de cookies tiers.
• Identification unique : certains services permettent à l'utilisateur de s'authentifier pour accéder à un ensemble de ressources (sites, applications), induisant ainsi la création d'un identifiant unique, censé faciliter la navigation (unique portail d'authentification, gestion des préférences utilisateur, etc.). On peut citer par exemple Facebook Connect, Windows Live ID, Google Account, etc.
• Identification statistique : certaines données issues du navigateur, de l'application ou encore du système d'exploitation permettent le calcul d'une empreinte entraînant la capacité à singulariser l'utilisateur. Ce calcul peut par exemple s'appuyer sur le User-Agent, la valeur du champ HTTP Accept, la politique de gestion des cookies, la résolution de l'écran, ou encore les extensions installées [8].

La directive 2002/58 du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques [9][10] précise que l'utilisation de cookies est autorisée à condition que l'utilisateur se voie donner des informations claires et précises sur la finalité de ces cookies ainsi que les informations placées sur l'équipement terminal qu'il utilise. L'utilisateur pourra refuser l'utilisation de ces dispositifs, cependant cette disposition ne fait pas obstacle au stockage de données utilisées à des fins exclusivement techniques.
Techniquement, des solutions amont ont été proposées, comme l'en-tête HTTP « Do Not Track » (DNT, 2009), pour permettre d'indiquer à un site web qu'un utilisateur ne souhaite pas être tracé. Cependant, bien qu'intégré dans tous les navigateurs modernes, il est purement déclaratif et peut être ignoré par le site visité.
D'un point de vue pratique, une des solutions les plus simples afin de limiter ces traces est de bloquer les cookies tiers. Ces cookies ne sont généralement pas utiles pour la navigation et il est recommandé de les refuser par défaut [11].
Enfin, de nombreuses extensions pour navigateur permettent de limiter le suivi d'un utilisateur existant. Elles ont principalement pour effet :
• blocage des traceurs (DoNotTrackME, Disconnect, uBlock Origin, AdBlock),
• le blocage des scripts (NoScript, ScriptNo),
• la génération de fausses informations afin de brouiller le calcul des empreintes numériques (Random Agent Spoofer),
• le basculement automatique vers HTTPS si disponible (HTTPS Everywhere).

Références

Bulletin d'actualité CERTA-2010-ACT-005 (05 février 2010)
http://www.cert.ssi.gouv.fr/site/CERTA-2010-ACT-005/CERTA-2010-ACT-005.html
RFC 6265 (HTTP State Management Mechanism) (avril 2011)
https://www.rfc-editor.org/rfc/rfc6265.txt
RFC 6797 (HSTS) (novembre 2012)
https://tools.ietf.org/html/rfc6797##section-14.9
How HSTS supercookies make you choose between privacy or security (02 février 2015)
https://nakedsecurity.sophos.com/2015/02/02/anatomy-of-a-browser-dilemma-how-hsts-supercookies-make-you-choose-between-privacy-or-security/
Evercookie (github)
https://github.com/samyk/evercookie
IAB Cookie White Paper (janvier 2014)
http://www.iab.net/media/file/IABPostCookieWhitepaper.pdf
Web beacon (9 janvier 2014)
https://www.iab.net/wiki/index.php/Web_beacon
Browser uniqueness
https://panopticlick.eff.org/browser-uniqueness.pdf
Directive 2002/58/CE (12 juillet 2002)
http://eur-lex.europa.eu/legal-content/fr/TXT/?uri=CELEX:32002L0058
Sites web, cookies et autres traceurs (CNIL)
http://www.cnil.fr/vos-obligations/sites-web-cookies-et-autres-traceurs/que-dit-la-loi/
Conseils aux internautes (CNIL)
http://www.cnil.fr/vos-droits/vos-traces/les-cookies/conseils-aux-internautes/

Vulnérabilités critiques au sein de Juniper ScreenOS

Contexte

Le 18/12/2015, le CERT-FR a émis l'alerte CERTFR-2015-ALE-014 [1] concernant plusieurs vulnérabilités critiques impactant le système ScreenOS des équipements Juniper. D'après le bulletin de sécurité publié par Juniper [2], ces vulnérabilités ont été découvertes suite à un audit de code interne et auraient été introduites volontairement pour affaiblir la sécurité de ScreenOS. Il s'agit en l'occurrence de deux portes dérobées qui permettent de :
– contourner le mécanisme d'authentification en place au niveau des services SSH et Telnet,
– déchiffrer les communications entre un client et le service VPN d'un équipement Juniper vulnérable.

Marqueurs de détection

La société Fox-It propose des signatures au format Snort afin d'identifier toute tentative de connexion à un équipement Juniper vulnérable via la porte dérobée. Ces signatures sont cependant limitées au service Telnet. De plus, la vulnérabilité liée au service VPN étant exploitable après une interception passive du trafic chiffré, il n'est pas possible de détecter son exploitation.
Versions affectées
La porte dérobée permettant d'accéder à l'interface d'administration de l'équipement via le protocole Telnet ou SSH impacte le logiciel Juniper ScreenOS de la version 6.3.0r17 à 6.3.0r20.
La vulnérabilité permettant de déchiffrer les communications réseau liées au service VPN impacte le logiciel Juniper ScreenOS versions 6.2.0r15 à 6.2.0r18 et les versions 6.3.0r12 à 6.3.0r20.
Ces vulnérabilités permettant un accès illégitime sont respectivement référencées par les identifiants CVE-2015-7755 et CVE-2015-7756.

Description des portes dérobées

CVE-2015-7755
La porte dérobée permettant d'accéder à l'interface d'administration d'un équipement Juniper vulnérable est localisée au sein du code de vérification des identifiants de connexion. Ce code compare le mot de passe saisie par l'utilisateur avec une chaîne de caractère codée en dur dans le système ScreenOS. Si elles sont identiques, l'accès est autorisé.
CVE-2015-7756
La seconde porte dérobée reposait sur une faiblesse du générateur de nombres aléatoires utilisé par l'algorithme de chiffrement et permettait à un attaquant d'accéder au contenu des communications VPN, obtenues à partir d'une écoute passive du trafic réseau.

Corrections

Le CERT-FR recommande d'appliquer les mesures préconisées dans le bulletin d'alerte CERTFR-2015-ALE-014.

Documentation

1
Bulletin d'alerte du CERT-FR :
http://cert.ssi.gouv.fr/site/CERTFR-2015-ALE-014/index.html
2
Bulletin de sécurité de l'éditeur :
http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10713&cat=SIRT_1&actp=LIST
3
Versions de ScreenOS vulnérable :
https://isc.sans.edu/diary/Infocon+Yellow%3A+Juniper+Backdoor+(CVE-2015-7755+and+CVE-2015-7756)/20521
1 – Rappel des avis émis
Dans la période du 21 au 27 décembre 2015, le CERT-FR a émis les publications suivantes :
CERTFR-2015-ALE-015 : Campagne de messages électroniques non sollicités de type TeslaCrypt
CERTFR-2015-AVI-554 : Multiples vulnérabilités dans le noyau Linux de Debian
CERTFR-2015-AVI-555 : Vulnérabilité dans VMWare
CERTFR-2015-AVI-556 : Multiples vulnérabilités dans Citrix XenServer
CERTFR-2015-AVI-557 : Multiples vulnérabilités dans Cisco IOS et IOS XE
CERTFR-2015-AVI-558 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
CERTFR-2015-AVI-559 : Vulnérabilité dans Xen
CERTFR-2015-AVI-560 : Vulnérabilité dans Cisco IOS XE
CERTFR-2015-AVI-561 : Multiples vulnérabilités dans le noyau Linux de Fedora
CERTFR-2015-AVI-562 : Multiples vulnérabilités dans ISC Bind
CERTFR-2015-AVI-563 : Multiples vulnérabilités dans le noyau Linux de SUSE
Durant la même période, les publications suivantes ont été mises à jour :
CERTFR-2015-ALE-014-1 : Vulnérabilité dans Juniper ScreenOS (ajout de règles Snort dans les contournements provisoires.)
Gestion détaillée du document
28 décembre 2015 version initiale.
Dernière version de ce document : http://cert.ssi.gouv.fr/site/CERTFR-2015-ACT-052
CERT-FR
2015-12-28

Réagissez à cet article

Source : *Bulletin d'actualité CERTFR-2015-ACT-052*

Les principales mesures du nouveau règlement européen sur la protection des données

Les principales mesures du nouveau règlement européen sur la protection des données

---

L'UE a approuvé le 15 décembre au soir le règlement sur la protection des données, qui renforce considérablement les pouvoirs de sanction des Cnil nationales.
La Commission européenne, le Parlement européen et le Conseil européen, qui travaillent depuis cet été à la constitution d'un compromis, se sont entendus le 15 décembre au soir sur un règlement européen sur la protection des données, qui harmonise des législations nationales très variées (voire inexistantes) pour donner aux citoyens un meilleur contrôle sur la façon dont leurs données sont collectées et utilisées. Comme tout règlement, celui-ci n'aura pas besoin d'être transposé en droit national et s'appliquera directement à partir du début 2017.

Parmi les principales mesures approuvées, on trouve :
Un important pouvoir de sanction accordé aux différentes « Cnil » nationales, qui pourront infliger des amendes allant jusqu'à 4% du chiffre d'affaires mondial (jusqu'à un certain plafond) des entreprises qui utilisent à mauvais escient les données numériques des gens, notamment en y accédant sans leur consentement. Autrement dit, des amendes pouvant atteindre plusieurs millions d'euros qui devraient a minima constituer une bonne dissuasion. Toutefois, pour ne pas empêcher les entreprises de tirer profit du big data, elles pourront traiter librement les données une fois effacée l'identité précise des utilisateurs.
L'obligation, pour les entreprises victimes de fuite de données, de signaler leur cas aux régulateurs nationaux sous trois jours, sous peine là encore de fortes amendes.
Le droit à l'oubli, entériné par le règlement, qui permet aux citoyens européens de demander à supprimer des informations en ligne qui les concernent mais ne sont plus pertinentes.
La portabilité des données, qui permet aux utilisateurs de demander le transfert de leurs données d'une plateforme vers une autre.
L'obligation, pour les moins de 16 ans, de demander une autorisation parentale avant de pouvoir utiliser des services tels que Facebook, Snapchat ou Instagram. Bruxelles proposait 13 ans comme aux Etats-Unis, mais certains pays dont la France ont poussé pour relever cette majorité numérique. Chaque Etat membre est toutefois libre d'y déroger.

L'extension de ces nouvelles règles à toutes les sociétés qui comptent des utilisateurs dans l'Union européenne, même si elles sont basées hors de l'UE. Dans la Silicon Valley par exemple.
Autrement dit, le règlement se fait beaucoup plus protecteur des citoyens européens que la législation équivalente aux Etats-Unis, mais également bien plus sévère à l'égard des sociétés qui y contreviendraient.
Naturellement, les géants américains ont protesté en accusant l'Union de les cibler injustement, au détriment de leurs petits rivaux européens. Ils estiment en particulier que lier les sanctions au chiffre d'affaires mondial n'a pas de sens. Mais l'UE, qui a toujours rejeté ces accusations, est restée ferme. Les grandes plateformes US ont donc sans doute du souci à se faire, à l'instar d'un Facebook qui a déjà eu maille à partir avec les régulateurs nationaux en France, en Espagne, en Allemagne, aux Pays-Bas et encore récemment en Belgique.

Réagissez à cet article

Source : *Les principales mesures du nouveau règlement européen sur la protection des données | CHABERT CATHERINE*

Des amendes plus lourdes de la part de la Cnil ? – Denis JACOPINI Expert informatique

Des amendes plus lourdes de la part de la Cnil ?