STORMSHIELD

LIVRE BLANC

PROTECTION DES DONNÉES PERSONNELLES

PETIT PRÉCIS POUR UNE BONNE PRATIQUE DU GDPR (GENERAL DATA PROTECTION REGULATION) EN ENTREPRISE

PAR PASCALE MARIN, PRODUCT MARKETING MANAGER - STORMSHIELD

NETWORK SECURITY | ENDPOINT SECURITY | DATA SECURITY

Introduction

- Rétrospective et contexte
- Révolution numérique
- Crise de confiance

Les textes

- Safe Harbor
- Privacy Shield
- Avènement du GDPR

Le GDPR en pratique

- Limites
- Brexit
- Le GDPR appliqué aux entreprises
- Données personnelles et spéciales
- La question du Shadow IT
- Le Cloud
  - Droits des entreprises
  - Devoirs des entreprises
  - Hébergeurs Cloud
- Les cadres ISO (International Standard Organization)
- Le rôle du responsable du traitement de la donnée
- Code de conduite et certification
- Les accompagnateurs dans la transition vers le GDPR

Cybercriminalité en pratique

- Etat des lieux global
- En France

La Solution Stormshield

- Best Practice
  - Le chiffrement de bout-en-bout
  - Data Loss Prevention
  - Bac à sable
  - Segmentation
  - Formation et sensibilisation
- L'approche MLCS (Multi-Layer Collaborative Security) comme seule stratégie efficace

Glossaire

Depuis le vote du nouveau règlement européen pour la protection des données personnelles (GDPR), le compte à rebours de la transition est lancé pour les entreprises jusqu'à mai 2018. Ces dernières ont 2 ans pour se mettre en règle vis-à-vis du nouveau règlement européen et son corollaire de nouvelles exigences en matière de protection des données : cybersécurité renforcée, responsabilité du collecteur de données et nouvelles procédures obligatoires. Lancé en 2011, les réflexions ont donné lieu à un nouveau texte de loi légiférant sur la protection des données personnelles. Pour les politiques de l'Union européenne (UE), les intentions derrière le GDPR (General Data Protection Regulation) sont simples. Comme l'exprimait l'EU International Cyberspace Policy : « Il est temps pour l'UE de rattraper son retard en matière de cybersécurité et de préparer ses Etats-membres en termes stratégiques, législatifs et opérationnels afin de répondre de manière efficace aux cyber-menaces et d'assurer la cyber-résilience de l'UE pour le futur.[1]"

Le GDPR marque donc l'avènement d'une nouvelle ère où la donnée personnelle devient le centre de tous les intérêts pour les politiques comme pour les entreprises européennes et internationales. Ce qui différencie le GDPR des diverses législations antérieures relatives à la protection des données personnelles, ce sont les aspects dématérialisés et transitoires de ces dernières d'un point de vue légal. On envisage donc enfin la donnée dans un contexte sans frontières et dans sa forme numérisée, en tout cas on essaie. Cela peut sembler être une réflexion anachronique ; pourtant la France, en 2012, parachève seulement son processus de dématérialisation des procédures de marchés publics, initié en 2001. Il marque l'entrée de l'acheteur public dans l'ère de la maîtrise des échanges immatériels[2] ; et le calendrier imposant les factures électroniques pour tous s'échelonne de 2017 à 2020. Force est de constater que l'adoption de la révolution numérique via la digitalisation des données fait apparaître une problématique critique : la cybersécurité. Jusqu'à récemment, ces éléments étaient du ressort des autorités nationales de chaque pays de l'Union européenne. Or, face à la difficulté de légiférer sur un domaine si mouvant et complexe, l'Internet et le numérique constituent actuellement une certaine forme de 'zones grises', comme l'affirme d'ailleurs le directeur général de l'ENISA (Agence européenne chargée de la sécurité des réseaux et de l'information), Udo Helmbrecht : « Internet, aujourd'hui, c'est le Far West. Tout le monde peut faire ce qu'il veut ».

Pour les entreprises, il s'agit à présent de réviser leurs procédures et de s'assurer de leur conformité au nouveau règlement avant que des sanctions ne commencent à pleuvoir. Ce livre blanc se propose de faire le tour de la question en apportant une lecture simplifiée du règlement et des solutions pratiques pour une transition réussie.

1 Source : http://eeas.europa.eu/policies/eu-cyber-security/index_en.htm

2 Source : https://fr.wikipedia.org/wiki/D%C3%A9mat%C3%A9rialisation#Mise_en_.C5.93uvre

Rétrospective et contexte

RÉVOLUTION NUMÉRIQUE

Si l'on considère ces 25 dernières années, il apparaît comme une évidence que les politiques se sont fait surprendre par la rapidité et l'ampleur de la révolution numérique. Ces instances souffraient toutes d'un « décalage alarmant », comme l'écrit Raluca Csernatoni dans son analyse de la stratégie européenne de cybersécurité[1]. D'où un écart important entre la compréhension des enjeux de cybersécurité par les politiques et la réalité pragmatique des nouvelles problématiques engendrées par la révolution numérique et sa structure dématérialisée.

Amorcée en milieu de XX^{ème} siècle et devenue le courant dominant à partir des années 90, la révolution numérique se manifeste par l'adoption de l'ordinateur chez les particuliers, la digitalisation massive des données et l'utilisation démocratisée d'Internet. Si en 1995, seulement 1% de la population mondiale est connectée, aujourd'hui, c'est 40% d'entre nous qui surfent sur le Web[2]. Ceux qui ont connu cette époque se souviendront de l'arrivée du pionnier Yahoo! en 1995. La même année, l'Union européenne vote la Directive 95/46/CE pour légiférer sur les questions numériques émergeantes, et notamment les données personnelles nouvellement dématérialisées. Cette directive est composée de 7 principes fondateurs que sont en substance la notification de l'utilisation des données personnelles, le choix de la personne (à qui appartient ces données), le transfert ultérieur des données, la sécurité, l'intégrité des données, l'accessibilité et les applications. Avec l'adoption du World Wide Web, sa myriade de technologies et autres plateformes en SaaS (Software as a Service ou logiciel en tant que service en ligne) en corollaire, la transformation va s'accélérer en l'espace d'une décennie.

En 2008, Daryl Plummer, MVP (Managing Vice President) Gartner, annonce déjà que « Le Cloud déclenche une évolution pour l'économie qui n'est pas moins influente que ce que le e-business a pu être.[3] » L'Union européenne met à jour sa directive de 1995 par une ultime révision la même année et pour la dernière fois avec une décision-cadre (glossaire). Celle-ci sera relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale. Il s'agit du premier instrument général relatif à la protection des données. A partir de 2011, un grand chantier de réflexion est lancé et le CEPD (Contrôleur européen de la protection des données) accueille favorablement l'intention de réformer le cadre juridique de protection des données personnelles. En effet, il est convaincu que le régime législatif de l'époque n'est pas à même d'assurer une protection suffisante à long terme dans un contexte de société de l'information en développement et de mondialisation[4].

1. Source : http://www.europeanpublicaffairs.eu/time-to-catch-up-the-eus-cyber-security-strategy/
2. Source : http://www.internetlivestats.com/internet-users/
3. Source : http://www.gartner.com/newsroom/id/707508
4. Source : https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2011/EDPS-2011-01_Data_protection_reform_strategy_FR.pdf

Les données personnelles et la loi

Une donnée à caractère personnel représente toute information se rapportant à une personne physique identifiée ou identifiable [...] directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. (Rf. www.cil.cnrs.fr)

CRISE DE CONFIANCE

Pour les vétérans du Web, c'est-à-dire ceux qui en ont connu l'émergence, la propagation et les premiers soucis que la digitalisation et un réseau commun ont posés, les « menaces » se résumaient, à quelques virus et des pourriels proposant des solutions médicamenteuses, remèdes au célibat et autres philtres d'amour. En tout cas, jusqu'à un passé proche. Pas vraiment la priorité numéro 1 des entreprises en pleine adoption de nouvelles technologies type CRM et qui découvrent le Cloud. Dans les années qui suivront, quelques protagonistes vont faire gagner ses lettres de noblesse au « hacktivisme » (glossaire) et ouvrir le bal en matière de fuite de données (pas seulement personnelles).

En 2013, une affaire éclate et va changer la donne. Un jeune collaborateur de la NSA (National Security Agency), Edward Snowden, révèle les malversations d'espionnage auxquelles s'adonne son employeur, l'agence de renseignements gouvernementale américaine. Ces actions ont une ampleur internationale et visent en particulier les données personnelles européennes. C'est un pavé dans la marre qui fait péniblement prendre conscience aux Etats comme aux entreprises que la cyber guerre a déjà commencé, y compris avec un ancien allié comme les Etats-Unis.

Un autre électrochoc, démarré un peu plus tôt en 2011, arrive la même année avec Max Schrems qui décide de s'attaquer à Facebook. Ce jeune étudiant en droit soulève à nouveau la problématique de la confidentialité des données personnelles européennes et les traitements dont elles font l'objet par le géant américain Facebook. Après les révélations d'Edward Snowden, Max Schrems décide de porter plainte une nouvelle fois contre Facebook, mais aussi contre Apple, Skype, Microsoft et Yahoo!, qu'il accuse d'avoir collaboré avec la NSA. L'affaire est très médiatisée et il gagne son procès en appel contre Facebook à la Cour de justice de l'Union européenne le 6 octobre 2015.

Cette décision entraîne l'invalidation du Safe Harbor, le texte de loi régulant les échanges de données entre l'Europe et les Etats-Unis[1].

1. Source : http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117fr.pdf

Pendant ce temps dans les entreprises…

Si la scène internationale est occupée par ces grandes affaires médiatiques, la cybercriminalité a également changé de visage au cours de ces dernières années pour les entreprises privées.

En cause : le hacking, le ransomware (glossaire), la fuite des données personnelles et le commerce de ces dernières. Plus personne n'est à l'abri et les conséquences vont souvent bien au-delà des dommages faits à la fameuse e-réputation des entreprises.

Le cas du piratage du site internet Ashley Madison, proposant des rencontres extra-conjugales, avait asséné une douche écossaise aux 32 millions de membres dont les données personnelles avaient été volées et publiées en ligne. Parmi eux, des hommes politiques, des personnalités en vue et une entreprise totalement prise au dépourvu qui proposera une prime pour toute information sur les pirates. Ces derniers déclarent que leurs actions avaient 2 motifs.

Le premier était une manifestation de leur désapprobation concernant le service proposé par le site, le deuxième était une dénonciation de la politique de confidentialité du groupe. L'attaque visait à démontrer qu'en dépit des 19 dollars réclamés par le site pour effacer les données des membres qui en faisaient la demande, aucune donnée n'était vraiment effacée.

Autre cas ayant pris des proportions tragiques, celui d'Orange dont le hacking de 1,2 millions de comptes incluant noms, numéros de téléphones et adresses emails a fait boule de neige. Non seulement le groupe de Télécommunication s'est fait pirater mais en plus ses clients sont devenus à leur tour les dindons de la farce, essuyant des tentatives répétées de phishing téléphonique ou par courriel. Quelques mois plus tôt, c'était Vodafone Allemagne qui s'était fait voler 800 000 contacts, et au Royaume-Uni, le fournisseur de Télécom TalkTalk avait vécu la même expérience. En bref, personne n'est à l'abri[1].

Après ces vagues successives de cyber-scandales, les politiques ont publié, souvent dans l'urgence, de nombreux textes, et qui ont généré beaucoup de confusion. Retour sur les fondations légales de la protection des données en Europe.

1. Source : http://www.lemonde.fr/pixels/article/2015/10/06/max-schrems-le-gardien-des-donnees-personnelles-qui-fait-trembler-les-geants-du-web_4783391_4408996.html#B94g8ICsCTK1dAJz.99

Les textes

SAFE HARBOR

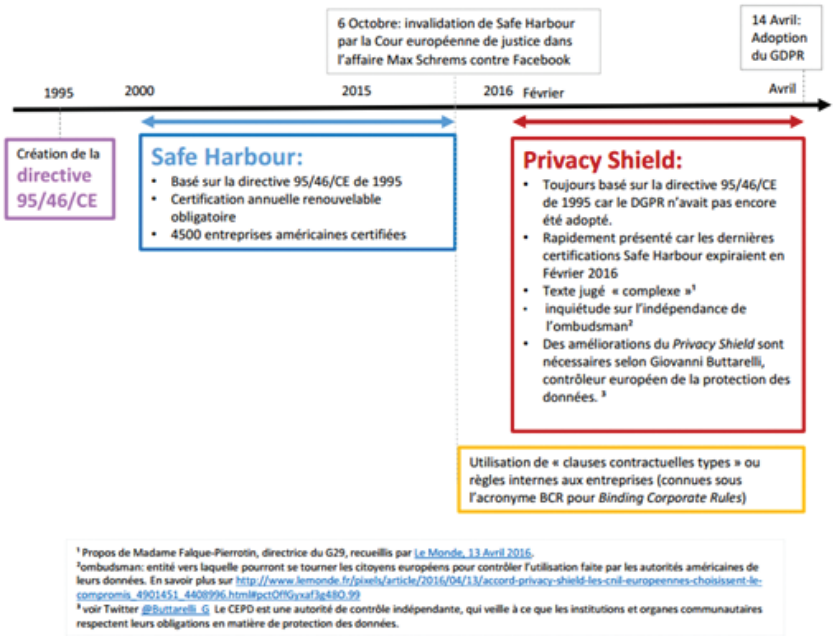
L'accord du « Safe Harbor » (ou « Sphère de Sécurité » en français) avait été validé par la Commission européenne en juillet 2000. En théorie, cela fournissait un socle de confiance pour les échanges de données entre l'Union européenne et les Etats-Unis. En pratique, il s'agissait d'une auto-certification : les entreprises américaines qui adhéraient au Safe Harbor s'engageaient à respecter un cahier des charges, qui devait en principe les hisser à un niveau conforme aux exigences du droit européen en matière de protection des données (basées sur les 7 piliers de la 1ère directive 45/46/CE). Les affaires Snowden et Schrems n'ont fait que précipiter une décision de disqualification du texte que la Cour méditait depuis déjà longtemps. En effet, il avait été constaté de nombreuses insuffisances, et 2 communications avaient déjà été publiées à ce sujet. La première concernait le contenu des obligations prévues au cahier des charges n'ayant pas leur inclusion dans l'ordre juridique américain. Par ailleurs, il subsistait une primauté illimitée des lois américaines sur les règles du Safe Harbor et une possibilité tout aussi illimitée de déroger à ces règles pour des raisons de sécurité nationale, intérêt public ou autre législation interne. Enfin, la Cour avait constaté l'absence de tout recours effectif contre ces interférences, ce qui rendait le texte caduc pour ne pas dire inutile (références COM(2013)846 final et COM(2013)847 final le 27 novembre 2013).

PRIVACY SHIELD, LE NOUVEL ACCORD UE/US :

Depuis l'abrogation de l'accord « Safe Harbor » , qui établissait un cadre législatif clair aux échanges de données personnelles transatlantiques, il existe un flou juridique certain. Le nouvel accord Privacy Shield, en français « Bouclier de Protection », a été vivement critiqué lors de sa présentation le 2 février 2016, puis très mal accueilli par le Contrôleur européen de protection des données (CEPD) en la personne de Giovanni Buttarelli, qui juge le texte trop complexe dans un communiqué de presse de mai 2016[1]. Max Schrems l'a même qualifié de « mort-né » sur son compte Twitter. De nombreuses voix se sont élevées pour dénoncer un accord élaboré dans l'urgence afin de légiférer sur le problème au plus vite sans tenir compte du règlement GDPR à venir et ne répondant pas aux manquements reprochés au Safe Harbor et tant décrié par la *Vox Populi.* Des enjeux économiques certains entre les 2 grandes puissances ont eu une force de levier suffisante pour qu'un texte voit le jour à peine 6 mois après l'invalidation du Safe Harbor. Cependant, l'association Data Rights Ireland a déjà attaqué le text en justice en octobre dernier.

1. Source : CEPD Europe secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2016/EDPS-2016-11-PrivacyShield_EN.pdf

Pendant ce temps, beaucoup d'entreprises utilisent les « clauses contractuelles types » afin de poursuivre leurs échanges avec les Etats-Unis, ce qui était défini dans le cadre de la 1ère directive de 1995, la Directive 95/46/CE. Ces alternatives sont inévitablement vouées à disparaître au profit du GDPR qui impose un seul règlement pour toutes les données européennes et toutes les entreprises qui les collectent, les hébergent et les manipulent.



Pour l'heure, les Etats-Unis ne figurent donc pas dans la liste des pays présentant un niveau de sécurité adéquat en matière de protection des données, et la CNIL (Commission nationale de l'informatique et des libertés) précise que les données personnelles européennes ne doivent pas être transmises aux Etats-Unis, sauf pour les passagers aériens.

En résumé, si la loi bouge avec le texte de Privacy Shield, dans les faits rien ne bouge et il faudra attendre l'avènement de la directive GDPR pour constater une vraie volonté de changement.

Liste des pays présentant un niveau jugé adéquat en matière de protection des données :

- Guernesey,
- les îles Féroé
- l'île de Man
- Jersey,
- Israël
- La Suisse,
- Andorre
- l'Argentine,
- L'Uruguay
- La Nouvelle-Zélande

- Le Canada (pour les traitements soumis à la loi canadienne "*Personal Information Protection and Electronic Documentation Act*")
- l'Australie (pour les données relatives aux passagers aériens),
- Les Etats-Unis (pour les données relatives aux passagers aériens)

Pour les échanges avec d'autres pays, consulter la carte de la CNIL

AVÈNEMENT DU GDPR (GENERAL DATA PROTECTION REGULATION):

C'est dans ce nouveau contexte que l'UE poursuit ses réflexions, entamées depuis 2011, pour légiférer sur la protection des données personnelles européennes. Cette fois-ci, il ne s'agira plus d'une directive (glossaire), comme en 1995, mais d'un règlement (glossaire). Cette dernière, plus coercitive, affiche la volonté de l'UE d'aligner tous les pays membres d'ici à 2020 dans la lignée de 2 grands projets européens : le Marché Digital Unique[1] et Horizon 2020[2].

Ce que cette nouvelle régulation tente d'accomplir, c'est de légiférer sur une donnée personnelle déterritorialisée, transitoire et mondialisée. C'est la donnée qui est au centre de l'attention légale et soumise à cette nouvelle législation, et non pas le pays. Cela veut dire que, du moins théoriquement, l'aspect géographique de son hébergement n'est plus un critère pertinent. Qu'il s'agisse d'un datacenter dans l'Utah (Etats-Unis), à Bangalore (Inde) ou encore à Roubaix dans les Hauts-de-France, la contrainte légale est la même, toujours en théorie. Dans cette tentative, l'UE a joué d'ingéniosité en introduisant une sanction nouvelle pour toute entreprise réticente et qui ne présenterait pas les gages de conformité d'ici à mai 2018. Après les 2 ans accordés pour la mise en place, les entreprises récalcitrantes recevront des amendes pouvant monter jusqu'à 4% de leur chiffre d'affaire mondial et jusqu'à 20 millions d'euros. A noter la subtilité d'une sanction qui ne peut s'exercer que sur un territoire donné et qui, pourtant, va avoir un impact dans un espace géographique étranger. C'est cette sanction qui fait converger tous les regards, surtout celui des américains qui se sont implantés dans l'UE car, si le GDPR est un règlement européen, avoir un pied en Europe signifie devoir potentiellement payer une amende calculée sur le chiffre d'affaire mondial d'un groupe. La maison-mère risque donc de devoir mettre la main au portefeuille de l'autre côté de l'Atlantique. Ça c'est nouveau.

Le GDPR en chiffres :

2 ans : c'est le temps qui est imparti aux entreprises à compter du 24 mai 2016, date de son entrée en vigueur, pour être en conformité avec le GDPR.

4% : c'est le pourcentage du revenu d'une entreprise qui pourra être prélevé sous la forme d'une amende en cas de non-respect de la législation européenne.

5 ans : c'est le nombre d'années de travail qu'il a fallu pour réviser la directive de 1995 qui statuait sur la protection des données jusqu'à présent et dont la dernière mise à jour datait de 2008.

28 : c'est le nombre de pays membres qui bénéficieront de ce nouveau règlement (moins le Royaume-Uni dès lors qu'il sera sorti de l'UE). Pour les Etats et toutes les entreprises, le GDPR s'inscrit dans une démarche coercitive d'uniformisation des lois de protection des données.

42,8 millions : c'est le nombre de cyber-attaques recensées en 2014 à travers le monde.

1. Source : http://ec.europa.eu/priorities/digital-single-market_fr
2. Source : https://fr.wikipedia.org/wiki/Horizon_2020

Le GDPR en pratique

LES LIMITES

On l'aura compris, le GDPR fait peser un risque sur des entreprises étrangères installées physiquement sur le territoire de l'UE. Pour les autres, la coercition est plus subtile. Pour des pays comme la Suisse ou la Norvège, alliés de longue date, le GDPR est une opportunité de renforcer des liens préexistants en s'alignant sur les mêmes contraintes légales. Pour d'autres pays comme les Etats-Unis, le Canada ou l'Australie, ayant leurs propres textes de loi et leurs entreprises qui n'ont pas de présence physique en UE, le GDPR est une épine dans le pied car ils ne sont pas tenus d'y obéir mais leur économie dépend grandement de ces échanges. Rappelons que l'UE ne compte que 7 % de la population mondiale, mais que ses échanges commerciaux avec le reste du monde représentent environ 20 % du volume total des importations et exportations mondiales[1].

Les sanctions prévues par le GDPR ne sont donc applicables que sur le territoire européen. C'est tout le dilemme de cette loi. Ne serait-ce pas l'aveu de l'incapacité des nations à sortir de leurs frontières alors que l'Internet les a fait sauter depuis déjà longtemps ? L'Union européenne n'est maîtresse qu'en sa demeure et les lois européennes ne régulent que l'Union européenne, même si elles sont un signal clair aux autres nations, en particulier aux Etats-Unis, que l'UE se dote d'un arsenal juridique en matière de cybersécurité et prend la question très au sérieux. Personne n'a intérêt à déclencher un nouvel incident diplomatique, car même si l'industrie des technologies informatiques est encore assez largement dominée par des entreprises américaines, l'Europe étant un de leurs principaux partenaires commerciaux avec l'ALENA (alliance USA, Canada et Mexique) et la Chine.

BREXIT

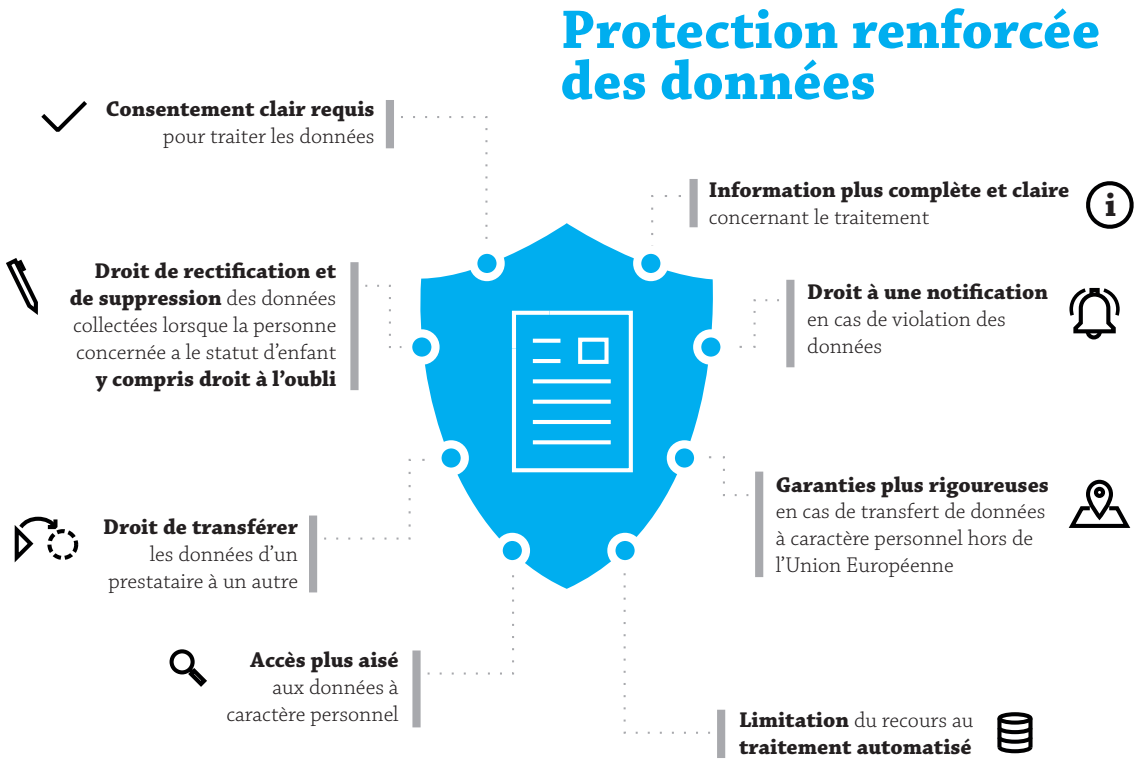
La volonté de sortir de l'Union européenne exprimée par le récent vote du Royaume-Uni, ainsi que la nomination d'un Premier ministre eurosceptique, viennent encore compliquer la situation. Le seul levier pour faire appliquer la loi de l'Union européenne est de sanctionner sur son territoire. Heureusement pour l'application du texte, beaucoup d'entreprises américaines ont un pied physique en Europe. Ces entreprises se sont également installées au Royaume-Uni pour développer leur activité en Europe continentale. Microsoft ou Facebook ont même investi dans des datacenters sur place. Mais qu'adviendra-t-il de l'application de la loi européenne sur le territoire britannique ? C'est un paramètre tout à fait essentiel sur lequel il est nécessaire de méditer avant de choisir ses fournisseurs car, comme nous allons le voir, la responsabilité incombe d'abord à l'entreprise collectrice des données.

1. Source : https://europa.eu/european-union/about-eu/figures/economy_fr

LE GDPR APPLIQUÉ AUX ENTREPRISES

La difficulté des entreprises à intégrer la question de la protection de la donnée personnelle est une réalité qu'il va falloir dépasser rapidement. « A secteur équivalent, une entreprise française y consacre en moyenne un budget dix fois inférieur à ses homologues américaines[1] ». Avec plus de 300 000 arnaques détectées dans l'Hexagone sur les réseaux sociaux, cela positionne la France « dans le rouge » sur ce type de cyber-menaces. Le pays occupe le 2ème rang européen et le 4ème rang mondial dans cette catégorie. La Chine, les Etats-Unis et l'Inde conservant le top 3 en matière de cyber menaces recensées[2].

Dans les faits, le GDPR va obliger les entreprises à remettre de l'ordre dans leurs rangs et à balayer devant leur porte. Cependant, l'Europe met également en avant les bénéfices dont les entreprises vont pouvoir profiter au-delà des contraintes que ce nouveau règlement va leur imposer : Extrait de l'infographie de l'UE



Les nouveaux commandements du GDPR pour les entreprises :

- Le droit à l'oubli numérique (glossaire) pour tous
- Le consentement clair et explicite de la personne concernée quant à l'utilisation de ses données personnelles

1. Source : Olivier Hassid, auteur de Menaces mortelles sur l'entreprise française in Libération.fr
2. Source : InfoDSI

- Le droit de transférer ses données personnelles vers un autre fournisseur de services facilement et rapidement
- Le droit d'être informé en cas de piratage des données personnelles et/ou d'incident lié à la sécurité dans les 24 heures
  - La présentation obligatoire des logs sous 24 heures, une fois l'incident reporté.
  - La garantie que les politiques relatives à la vie privée soient expliquées dans un langage clair et compréhensible
- Nommer un responsable de la donnée personnelle. Le représentant devra agir pour le compte du responsable du traitement et devrait pouvoir être contacté par toute autorité de contrôle (articles 62 et 63)
- S'assurer que le traitement des données est soumis à des procédures documentées, que l'entreprise effectue ce travail elle-même ou que cela soit réalisé pour son compte. Ces documents seront exigés lors d'un audit

DONNÉES PERSONNELLES ET SPÉCIALES

Une notion essentielle à intégrer dans la transition vers le GDPR est que chaque entreprise possède des données personnelles qui tombent sous le joug du règlement européen.

Alors qu'auparavant la protection des données renvoyait principalement aux secteurs bancaires ou médicaux, la notion de « données personnelles » a été considérablement élargie : « On entend par données à caractère personnel toutes les informations relatives à une personne, qu'elles se rapportent à sa vie privée, professionnelle ou publique. Il peut s'agir d'un nom, d'une photographie, d'une adresse de courrier électronique, de coordonnées bancaires, de messages publiés sur des sites de socialisation, de renseignements médicaux ou de l'adresse IP d'un ordinateur. Selon la charte des droits fondamentaux de l'Union européenne, toute personne a droit à la protection, dans tous les aspects de sa vie, des données à caractère personnel la concernant : à son domicile, sur son lieu de travail, lorsqu'elle fait des achats ou reçoit un traitement médical, au poste de police ou sur Internet[1] ». La donnée personnelle commence donc avec le nom d'un client, voire un email, ce qui veut dire que toute entreprise a des données personnelles à protéger. Base des employés, salaires, base clients, tout cela relève de la donnée personnelle, même si l'activité économique de l'entreprise tourne autour d'un secteur a priori non stratégique, comme la vente de chaussures de confort, par exemple. Pour notre vendeur de chaussures de confort qui évolue dans un secteur niche et a fait développer un site de e-commerce pour ses clients à mobilité réduite, les données personnelles de ces derniers ainsi que celles des prospects seront également les adresses IP (statiques ou dynamiques),

1. Source : Rf. Press release EU

ou encore les cookies ou les identifiants biométriques si notre entreprise-exemple décidait d'identifier ses clients en scannant leur plante de pied pour accéder à ses modèles de chaussures compensées et micro aérées en ligne. Dans le cas où notre entreprise souhaiterait se doter d'une application pour appareils mobiles (smartphones et tablettes), les coordonnées GPS, les identifiants personnels de compte (nom d'utilisateur et mot de passe) tombent aussi dans la sacro-sainte « donnée personnelle ». Et plus l'information est intime, plus elle sera considérée spéciale. Dans la notion de donnée spéciale, on trouvera donc, par exemple, le genre de la personne, son orientation sexuelle ou encore son appartenance religieuse. Ces données spéciales sont investies d'un cadre encore plus restrictif, partant du principe que leur traitement est interdit, sauf exceptions (article 9). Il est donc désormais indispensable de protéger toutes les données de l'entreprise, la notion de « données personnelles » ayant des ramifications multiples et étant au cœur de toutes les convoitises cybercriminelles.

LA QUESTION DU SHADOW IT

Rappelons que pour être conforme aux préceptes édictés par le GDPR, il faut pouvoir démontrer un niveau de sécurité adéquat pour toute donnée européenne collectée et hébergée par une société, c'est-à-dire « La mise en œuvre de politiques appropriées en matière de protection des données par le responsable du traitement » (article 24.2). La question du Shadow IT va donc (re)devenir prépondérante en 2018 car l'idée que des collaborateurs décident d'utiliser un service non référencé par l'entreprise (un outil de Web conférence, un SaaS métier type plateforme de mass emailing, etc.) va présenter un nouveau danger légal et ajouter une couche de complexité à un problème déjà bien connu. Il y a déjà plusieurs écoles de pensées pour traiter le Shadow IT. Certaines entreprises ont tout bonnement verrouillé leur réseau et rien ne peut être installé sur les postes des collaborateurs sans l'intervention de l'équipe IT. Un processus générateur de frustrations évidentes chez les collaborateurs, comme pour le responsable IT. **Le chiffrement (glossaire) de la donnée peut constituer une alternative moins radicale et néanmoins très efficace pour minimiser l'exposition des données personnelles** vers des applications externes non répertoriées.

Le Cloud

Dans un contexte de migration vers le Cloud amorcée depuis une dizaine d'années, la question de la protection des données européennes prend une autre dimension. En effet, le Cloud implique de prendre plusieurs aspects en considération pour être en conformité avec le GDPR :

1. La donnée est confiée à un partenaire externe (sous-traitant). Elle est *de facto* hébergée ailleurs et sort du cadre physique de l'entreprise. Cela oblige à se poser les bonnes questions et à s'assurer que l'hébergeur sera en mesure d'assurer un niveau de sécurité

adéquat, de pouvoir présenter des logs en temps voulu en cas d'incident. Car le GDPR exige une présentation des informations liées à un incident dans les 72 heures (article 33). Cela offre une garantie à l'entreprise cliente et obliger les hébergeurs Cloud à se doter des technologies d'enregistrement des logs, d'alerte et de tout l'arsenal de cybersécurité qui, de toute façon, devrait être explicitement inclus dans toute offre Cloud sérieuse et qui se respecte.

2. Déterritorialisation et menace d'espionnage. Puisque la donnée est dématérialisée, sa migration dans le Cloud peut lui faire passer des frontières. C'est en réalité un risque majeur auquel il faut s'intéresser de près et pour lequel des solutions existent. Même dans le cadre du GDPR et dans le contexte international actuel très tendu, certaines entreprises peuvent néanmoins avoir des données hébergées ailleurs qu'en Europe, parfois à cause de leur modèle économique (entreprises en « Follow the sun » qui transmettent de la donnée autour de la planète au rythme des rotations de leurs équipes internationales), parfois à cause de leur structure intrinsèque (entreprises ayant délocalisé une partie de leur activité hors d'Europe ou ayant racheté une autre société à l'étranger, etc.), parfois parce qu'une application à valeur ajoutée ne propose pas d'autre hébergement qu'hors des frontières de l'Union européenne (un CRM ou un outil d'automatisation marketing, par exemple).

Le cas d'Office 365 :

Beaucoup d'entreprises choisissent de migrer sur Office 365 pour bénéficier des réductions de maintenance et de coûts que le stockage et les applications externalisées peuvent offrir en mode Cloud. C'est une solution de choix, particulièrement quand l'IT ne fait pas partie du métier de l'entreprise ; car la sophistication des systèmes, des technologies et des attaques potentielles nécessitent aujourd'hui un savoir-faire tout à fait unique et que la plupart des entreprises ne peuvent pas gérer en local. Cette démarche de migration sur le Cloud doit nécessairement amener à se poser la question de la sécurité de ses données.

Ainsi, le cadre coercitif du GDPR va imposer aux entreprises qui migrent ainsi qu'aux hébergeurs Cloud de conduire la réflexion suivante :

Pour les entreprises :

Choisir l'hébergement en France ou dans un des pays de l'Europe (il est conseillé d'exclure le Royaume-Uni de cette équation car leur sortie de l'UE a été votée) pour s'assurer que l'hébergeur Cloud sera tenu de respecter les contraintes imposées par le GDPR dans le traitement qu'il fera de la donnée qui lui est confiée. Choisir un hébergement Cloud sur le territoire de l'UE, quand cela est possible, permet de s'assurer que l'hébergeur est astreint au GDPR et applique donc une politique conforme aux prescriptions du règlement.

Droits des entreprises vis-à-vis des hébergeurs Cloud :

- Changement d'hébergement facile ;
- Remontée d'incident sous 72 heures ;
- Présentation des logs sous 72 heures ;
- Procédures écrites et présentables sur demande ;
- Garantie absolue que la donnée ne sera pas traitée par l'hébergeur sans l'autorisation de l'entreprise cliente et collectrice ;
- S'assurer que le traitement des données est soumis à des procédures documentées, que l'entreprise effectue ce travail elle-même ou que cela soit réalisé pur son compte. Ces documents seront exigés lors d'un audit.

Devoirs des entreprises vis-à-vis des personnes dont les données personnelles sont collectées :

- Nommer un responsable de la donnée (en interface avec l'hébergeur Cloud potentiel et les autorités en cas d'audit)
- Le consentement clair et explicite de la personne concernée quant à l'utilisation de ses données personnelles. Là encore, l'entreprise doit exprimer clairement ses intentions quant à l'usage qu'elle compte faire des données qu'elle collecte ou qui lui sont confiées
- Le droit à l'oubli pour les personnes qui en font la demande. Cette nouveauté instaurée par le GDPR oblige l'entreprise à assurer « la possibilité claire et explicite » de voir les données d'un particulier ou d'une autre entreprise effacées sur simple demande; ce qui veut dire que les bases prospects et clients existent tant que l'entreprise en reçoit le consentement par ses contacts et qu'elle doit impérativement fournir un moyen simple de proposer l'effacement des données de ses contacts si cela est leur volonté
- Le droit de transférer ses données vers un autre fournisseur de services. L'entreprise prendra la responsabilité de cette procédure qui devra être aisée, rapide et sur demande du contact
- Une information claire du collecteur concernant les traitements effectués sur la donnée personnelle collectée. La protection des données personnelles est un droit fondamental en vertu de l'article 8 de la Charte des droits fondamentaux de l'Union européenne, intimement lié au respect de la vie privée, prévu à l'article 7
- Le droit d'être informé en cas de piratage des données et/ou d'incident lié à la sécurité dans les 72 heures. Voilà un des nouveaux points du GDPR qui sera échu à l'entreprise qui choisira un service Cloud en dehors des frontières de l'Union européenne ou qui ne sera pas hébergée en mode Cloud. Pour les autres, c'est l'hébergeur Cloud

européen qui prendra cette contrainte en charge, mais il faudra la négocier au moment de la signature du contrat car aux yeux du règlement européen, c'est le collecteur de données le responsable,

- La garantie que les politiques relatives à la vie privée soient expliquées dans un langage clair et compréhensible. Cela s'appliquera à toutes les entreprises.

Sortir de ce périmètre géographique où le GDPR doit et sera appliqué, c'est s'exposer à de nouveaux risques que l'hébergeur hors de l'Union européenne ne portera pas et qui basculeront sur l'entreprise européenne qui collecte la donnée.

Les règles du GDPR concernant directement les hébergeurs Cloud

- Le droit pour le client (entreprise) de transférer ses données vers un autre fournisseur de services,
- Nommer un responsable de la donnée. Le représentant devra agir pour le compte du responsable du traitement et devrait pouvoir être contacté par toute autorité de contrôle (articles 62 et 63),
- Le droit, pour le client, d'être informé en cas de piratage des données et/ou d'incident lié à la sécurité sous 24 heures,
- La mise à disposition des logs après incident sous 24 heures,
- S'assurer que le traitement des données est soumis à des procédures documentées, que l'entreprise effectue ce travail elle-même ou que cela soit réalisé pour son compte. Ces documents seront exigés lors d'un audit.

LES CADRES ISO COMME SOUTIEN AU NOUVEL ORDRE EN MARCHE

Qu'il s'agisse de procédures ou de gouvernance informatique, les normes ISO seront d'un grand soutien. Les normes ISO 2700x (gouvernance informatique) et ISO 9001 (procédures liées aux produits et aux services) seront des cadres normatifs qui faciliteront la transition des entreprises dans leur démarche de conformité au GDPR. Il est conseillé de s'y reporter et, pourquoi pas, de se certifier. L'exercice permettra de faire un audit des structures en place et de construire un modèle d'architecture de l'information et de l'entreprise garantissant l'assurance de sa conformité avec le règlement européen dans une philosophie d'amélioration continue. Outre ces bénéfices liés aux contraintes imposées par le GDPR, rappelons que les normes ISO sont toujours un gage de procédures et méthodologies intra-entreprise cohérentes. Cela va dans le sens de l'optimisation des entreprises et doit être considéré comme une opportunité d'amélioration et non une contrainte.

LE RÔLE DU RESPONSABLE DU TRAITEMENT DE LA DONNÉE

Pour les grands groupes, le concept n'est pas nouveau. En 2011, une enquête réalisée par PricewaterhouseCoopers révélait que 80% des entreprises avaient un CISO (Chief

Information & Security Officer) ou équivalent. Il prendra peut-être aussi la nouvelle casquette du responsable de la protection des données personnelles. On voit déjà également apparaître des DPO (Data Protection Officer) qui sont des postes spécifiques pour cette fonction.

De manière générale, le rôle du responsable du traitement est de mettre en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au règlement (article 24.1). Dans le cadre du GDPR, la fonction devient obligatoire au sein des entreprises.

Pour les plus petites entreprises, il faudra donc nommer une personne responsable du traitement de la donnée qui puisse assumer les fonctions suivantes :

- Etre correctement informé(e) sur le GDPR et ses contraintes. Le règlement parle de Code de Conduite et de certifications qui verront bientôt le jour pour former ses collaborateurs.
- Vérifier et valider les propositions commerciales des sous-traitants (hébergeur, fournisseur, etc.) ainsi que leur niveau de services contractuels (SLA ou « Service Level Agreement » en anglais, voir le glossaire),
- S'assurer que le sous-traitant n'effectue aucun traitement des données, excepté sur instruction du responsable du traitement,
- Vérifier et valider les pratiques de traitement des données en interne (avec le marketing et les ressources humaines en particulier) et s'assurer de la mise en œuvre de politiques appropriées en matière de protection des données. Il veillera en particulier à faire respecter le fameux « droit à l'oubli » (politique de rétention de la donnée) qui oblige toute entreprise à effacer les données d'un prospect ou d'un client sur simple demande de ce dernier,
- Etre l'interlocuteur dédié pour les fournisseurs et pouvoir être joignable facilement (sous 72 heures) en cas d'incident,
- Vérifier la pertinence des procédures liées au traitement des données, tenir à jour des procédures écrites et consultables (l'UE se réserve le droit de les consulter sur simple demande),
- S'assurer que la déclaration d'un incident a bien lieu, et ce dans un délai de 72 heures maximum,
- S'assurer de la mise en place d'un outil de lecteur et d'enregistrement des logs afin de pouvoir les présenter sur demande après un incident sous 72 heures (article 35),
- S'assurer qu'un plan de continuation, de reprise de l'activité et de rétablissement après désastre a été mis en place et validé avec les sous-traitants potentiels et au sein de

l'entreprise,

- Effectuer des analyses d'impact, en particulier dans le cadre de traitement à grande échelle (article 35). Cela entraîne une préparation à la gestion des risques (analyse, mitigation, déroulement). Certaines formations courtes (telles que la certification M_o_R®, Risk Management, Practitioner, par exemple) proposent des méthodologies spécifiques qui peuvent aider les entreprises à adopter de bonnes pratiques en matière de gestion du risque.

CODE DE CONDUITE ET CERTIFICATION

Pour soutenir l'effort des entreprises dans la transition vers mai 2018, l'UE propose 2 éléments : le code de conduite et la certification.

Dans son article 40, le règlement encourage la mise en place d'un code de conduite par les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants pour s'assurer de la bonne application du règlement. Ces codes devraient promouvoir les notions de traitement loyal et transparent, les intérêts légitimes poursuivis par les responsables du traitement dans des contextes spécifiques, la collecte des données à caractère personnel, l'utilisation de pseudonymes pour ces dernières, les informations communiquées au public et aux personnes concernées, ou encore l'exercice des droits des personnes concernées, pour n'en citer que quelques-unes.

L'existence de ce code de conduite peut servir d'élément attestant du respect des obligations incombant au responsable du traitement (article 24.3).

Le GDPR annonce également la mise en place de mécanismes de certification en matière de protection des données ainsi que de labels et de marques en la matière, aux fins de démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent le présent règlement (article 42).

Les accompagnateurs dans la transition vers le GDPR

Dans ce tourbillon de nouvelles contraintes légales compliquées par la situation politique internationale (sortie de l'Europe du Royaume-Uni, tensions très sérieuses avec la Russie, conflits armés dans certains pays du Machrek), il faut s'appuyer sur l'aide de professionnels :

1. Ne pas hésiter à faire appel à des cabinets d'avocats spécialisés. Il en existe plusieurs qui se sont fait une spécialité du GDPR et seront capables d'accompagner les entreprises qui le souhaitent pendant les 2 années de mise en conformité juridique octroyées. Il existe même des outils juridiques en ligne dédiés au GDPR, comme celui du cabinet Ulys permettant de surfer au gré des articles, faire des recherches par mots clé et comprendre la législation actuelle et celle à venir.

2. Solliciter des cabinets de consultation qui pourront apporter une analyse après audit et un conseil pour gérer au mieux sa transition digitale en intégrant toutes les contraintes du GDPR. Dans cette mesure, les architectes d'entreprises seront de bons conseils car leur action s'applique en considérant l'entreprise dans sa globalité et pas uniquement la donnée ou les systèmes informatiques[1].

3. Exiger des garanties de la part des hébergeurs Cloud. Certains hébergeurs Cloud tel qu'OVH, par exemple, proposent l'application Office 365 hébergée dans l'un de leurs datacenters en France. Que l'hébergeur Cloud soit physiquement en Europe ou non, il devra apporter la garantie d'une conformité au GDPR, et c'est à l'entreprise de s'en assurer sous peine d'être considérée responsable légalement si un incident n'est pas géré de manière adéquate.

4. Se doter des meilleures solutions en matière de cybersécurité. Après les différentes affaires de partenariats entre certains fournisseurs d'équipement de sécurité informatique et la NSA qui ont défrayé la chronique, l'heure est à la prudence. Car si un équipement étranger de cybersécurité est à l'origine d'une fuite de données, c'est l'entreprise victime qui en sera responsable aux yeux de la nouvelle loi. L'entreprise qui collecte et héberge la donnée doit s'assurer qu'elle apporte un niveau adéquat de sécurité pour préserver l'intégrité de ses données. Il vaut mieux toujours choisir une solution certifiée par des organismes garantissant un haut niveau de qualité tels que l'ANSSI, l'Agence nationale de sécurité des systèmes d'information, en France, le BSI en Allemagne ou l'OCSTI en Espagne pour garantir l'efficacité d'une solution de cybersécurité. Toutes ces agences nationales auront d'ailleurs bientôt des certifications uniformisées dans toute l'Europe. Se souvenir également qu'une donnée chiffrée volée n'est pas considérée comme une fuite si les clés de déchiffrement ne sont pas accessibles. Le chiffrement reste donc le meilleur moyen d'être en conformité.

5. Puiser de l'information auprès de la CNIL qui a mis en ligne une page résumant les bonnes pratiques et ce qui change[2]. Le gouvernement français[3] a mis à disposition la plateforme « Pharos » pour signaler des contenus illicites ainsi que des liens utiles vers tous les organismes de confiance susceptibles de conseiller et d'accompagner les entreprises dans leur effort de protection des données[4].

1. Source : https://www.opengroup.fr/architecture-dentreprise/
2. Source : https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels
3. Source : http://www.gouvernement.fr/risques/risques-cyber
4. Source : https://www.internetsignalement.gouv.fr/PortailWeb/planets/LiensUtiles.action

Cybercriminalité en pratique

ETAT DES LIEUX GLOBAL

Le terme de « cybersécurité » émerge au milieu du XX^{ème} siècle. Quant aux attaques, elles vont connaître une croissance exponentielle. En 2015, la très sérieuse enquête sur l'état de la cybersécurité actuelle publiée sur le site www.pwc.com[1] relevait une hausse de 38% des incidents de sécurité en entreprise comparé à l'année précédente. Ce chiffre monte à 56% pour les attaques liées aux vols et piratages de propriétés intellectuelles. Depuis le 1er janvier 2016, c'est près de 28 millions d'attaques qui ont été recensées[2] et on en comptait au total 42,8 millions en 2014. Au Royaume-Uni, l'Office for National Statitstics (ONS) a déclaré en 2015 que le cybercrime était à présent la première menace pour les citoyens britanniques avec 6,8 millions d'incidents répertoriés.

Pour certains pays, l'hacktivisme et le cybercrime sont devenus des sports nationaux. En tête du palmarès des agrégés du pourriel, les Etats-Unis[3].

Depuis 2009, les incidents détectés ont progressé en moyenne de 66% par an[4].

EN FRANCE

Selon InfoDSI, 500 millions d'informations personnelles ont été volées ou perdues en 2015 dans le monde. La France serait à l'origine de plus de 9,9 millions d'attaques réseaux et connaît un grand nombre d'attaques ciblées qui concernent à plus de 57% les PME, et à 28,9% les entreprises de plus de 1 500 employés. Et avec plus de 300 000 arnaques sur les réseaux sociaux détectées, l'Hexagone se positionnent en tête sur ce type de cyber-menaces, occupant le 2ème rang européen et le 4ème rang mondial dans cette catégorie. Si les arnaques partagées par les utilisateurs eux-mêmes constituent encore l'écrasante majorité de ce type de menaces, les fausses offres sont en forte progression[5].

Virus, phishing, rootkit, backdoor et autre malware, la cybercriminalité a à sa disposition un éventail d'outils variés pour nuire aux entreprises, que le but poursuivi soit politique ou lucratif. Depuis 2013, le ransomware, ou « rançongiciel » en français, sévit dans les entreprises. Ce dernier a augmenté de 260% en France en 2015. Enfin, mention spéciale au RaaS –

1. Source : The Global State of Information Security®, a registered trademark of International Data Group, Inc. http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html

2. Source : http://www.planetoscope.com/Internet-/1852-cyberattaques-dans-le-monde.html

3. Source : http://www.journaldunet.com/ebusiness/crm-marketing/1172848-origine-du-spam-dans-le-monde-statista/

4. Source : http://www.pwc.fr/fr/espace-presse/communiques-de-presse/2014/octobre/cybersecurite-alors-que-les-incidents-augmentent-et-sont-toujours-plus-couteux.html

5. Source : InfoDSI http://www.infodsi.com/articles/162318/france-figure-top-10-pays-cyber-criminalite-est-plus-active.html

Ransomware as a service (vous ne rêvez pas). Il s'agit d'un nouveau business model du crime où certain cybercriminels proposent la diffusion du malware en mode « service » contre un pourcentage de la rançon[1]. Un business très lucratif et en pleine effervescence.

C'est d'abord contre tout cela que le GDPR veut protéger les entreprises. Quelques bonnes pratiques simples et efficaces vont aider à les rendre conformes aux règlements.

La Solution Stormshield

BEST PRACTICES :

Chiffrement de bout-en-bout

Que l'on choisisse un hébergement sur le territoire de l'UE, astreint au GDPR, ou ailleurs parce qu'on n'a pas le choix, il faut impérativement se préoccuper de l'intégrité de la donnée personnelle. L'article 32.a précise même que « des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation et le chiffrement, sont destinées à mettre en œuvre les principes relatifs à la protection des données personnelles […] de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée ». Le chiffrement répond à ces exigences. C'est une solution peu onéreuse, clé en main et souvent assez transparente pour l'utilisateur. Assurer le chiffrement de sa donnée n'est plus l'apanage de secteurs tels que la Défense ou la Banque, mais bien l'affaire de tous. Stormshield Data Security (SDS) propose un produit très simple d'utilisation et efficace pour protéger les données de l'entreprise, qu'elles soient hébergées localement ou dans un Cloud. SDS s'installe sur le poste de travail de l'utilisateur et va chiffrer emails et fichiers de manière transparente, garantissant ainsi la possibilité de déplacer les fichiers d'un Cloud à un autre, ou d'un ordinateur à une clé USB en toute tranquillité. SDS permet de chiffrer la donnée, et c'est une solution certifiée par un organisme européen (l'ANSSI) et développée en France. Elle offre donc la garantie d'une technologie saine et dénuée de tout dessein d'espionnage informatique ou industriel. Enfin, une donnée chiffrée volée n'étant pas considérée comme une brèche tant que les clés de déchiffrement sont inaccessibles et maîtrisées par l'entreprise, on garde l'esprit tranquille.

DLP

Il existe également des solutions dites de DLP (Data Loss Prevention ou « prévention de la perte des données » en français). Ces technologies sont basées sur de la reconnaissance comportementale et agissent en corrélant différents éléments fournis par les équipements de

1. Source : http://www.riskcompliance.be/news/la-belgique-dans-le-top-3-mondial-des-victimes-de-ransomware/

cybersécurité disséminés dans l'infrastructure, les réseaux et postes de travail pour déclencher une politique de sécurité, stopper un chiffrement « sauvage » ou agir contre un comportement jugé suspect. Ce comportement peut être celui d'un malware qui aurait réussi à infiltrer le réseau ou encore celui d'un collaborateur. Ces solutions sont des outils très puissants et doivent aujourd'hui être considérées par les entreprises pour garantir une meilleure imperméabilité autour des données personnelles à protéger. Stormshield propose un connecteur compatible avec toutes les solutions de DLP.

Bac à sable (Sandboxing)

Dans un contexte digital ou l'utilisateur est perpétuellement sollicité par des emails et ses attachements, les technologies de sandboxing (entendez « bac à sable » en français) vont également participer à la réduction du risque d'infection et de corruption des réseaux des entreprises et donc de leurs données. La mise en place d'environnements étanches permettant effectivement de jouer un fichier, une pièce jointe ou encore un lien de manière isolée et sans permettre d'interaction entre cet environnement de test et le reste du réseau de l'entreprise préviendra la contamination possible à tout un réseau. On ne peut pas empêcher l'utilisateur de cliquer mais on peut éviter la propagation des fichiers malicieux dans l'ensemble de son réseau. Breach Fighter de Stormshield est une solution de sandboxing sûre et qui fonctionne de concert avec les autres technologies Stormshield. Si, par exemple, le pare-feu Stormshield Network Security (SNS) détecte un fichier suspect, il est capable de l'envoyer automatiquement sur Breach Fighter, l'environnement imperméable de test hébergé dans le Cloud. Ce fichier est ensuite analysé en utilisant la technologie des moteurs de prévention de Stormshield Endpoint Security (solution de protection des postes de travail). Le résultat de l'analyse viendra enrichir la base de données partagée par la communauté Stormshield, si bien qu'à la prochaine apparition de ce fichier dans la messagerie de n'importe quel client Stormshield, le pare-feu saura automatiquement si le fichier est bon ou mauvais.

Segmentation

La micro segmentation est également une bonne pratique qui renforcera la sécurité des réseaux et des équipements (serveurs, automates, etc.), et donc minimisera le risque d'accès pernicieux aux données. L'idée est d'installer un pare-feu devant chaque serveur et de segmenter chaque réseau pour éviter la propagation de codes malicieux ou de virus au réseau dans sa globalité.

Formation et sensibilisation

Parce qu'il est bien connu que la première vulnérabilité informatique des entreprises se situe entre la chaise et le clavier, il est indispensable de mettre en place des formations internes pour informer ses collaborateurs, leur apprendre à construire un bon mot de passe, se méfier des noms de domaines suspects et de l'émetteur lorsqu'on reçoit une pièce jointe douteuse, avoir

les bons réflexes quand ils sont sollicités pour obtenir des informations ou installer quelque chose sur leur poste de travail, etc. La formation « Menace interne » (mieux connue sous son nom anglais « Insider Threat ») est aujourd'hui une activité à considérer absolument pour tous les collaborateurs de l'entreprise afin de se prémunir contre les désagréments du cyber crime. Des programmes, tels qu'entre autres RESALIA™ proposé par Axelos (propriétaire de certification ITIL, entre autres), peuvent aider les entreprises à former leurs collaborateurs aux bonnes pratiques de cybersécurité en interne.

L'approche Multi-layer Collaborative Security comme seule stratégie de défense efficace

Dans l'approche Stormshield, la cybersécurité est l'affaire de tous, et la seule façon d'être efficace, c'est la collaboration. Partant de cette idée maîtresse, le groupe a développé une stratégie innovante : la Multi-Layer Collaborative Security (sécurité collaborative multi-couches), mieux connue sous l'acronyme MLCS. Cette stratégie propose une redéfinition des paradigmes de la cybersécurité pour entrer dans une ère de collaboration et de convergence.

On peut définir la stratégie MLCS en 3 couches collaboratives :

Tout d'abord, la convergence de technologies au sein d'un seul et même équipement. C'est notamment le cas de la gamme de produits Stormshield Network Security (SNS) qui a un pare-feu multifonctions ou UTM (Unified Threat Management ; entendez « gestion unifiée des menaces »). Les différents moteurs de sécurité de ces produits échangent des informations pour prendre des décisions de blocage, si nécessaire. Dans la perspective du GDPR, cela va permettre non seulement de détecter mais également d'arrêter les tentatives d'intrusion, de vols de données ou de prise de contrôle à distance (rootkit, backdoor, etc.).

Ensuite, tous les équipements et logiciels dédiés vont également collaborer et échanger de l'information entre eux. Ainsi, chaque élément de cybersécurité devient un capteur qui va enregistrer de l'information et la redistribuer aux autres éléments afin de synchroniser les politiques de défense. Ce peut être une alerte de l'UTM SNS qui va déclencher automatiquement une règle de flux avec SES. Il peut également s'agir d' anticiper la fuite de données quand SES va déclencher l'arrêt de SDS afin de conserver les données chiffrée en fonction du réseau utilisé.

Enfin, la dernière couche de cet arsenal de cybersécurité à l'avant-garde consiste en le fait que l'entreprise devient partie prenante de sa propre défense en entrant dans la communauté Stormshield. Chaque réseau, chaque utilisateur, vont permettre de répertorier les menaces rencontrées et en faire bénéficier les autres car, dans cette guerre, il n'est pas question de faire cavalier seul. La solution est d'abord collaborative et technologique, et c'est cette approche que Stormshield a choisi de privilégier.

Stormshield, fournisseur de technologies innovantes vous accompagne dans une transition réussie vers le GDPR. Contactez-nous pour en savoir davantage et pour comprendre comment nos technologies peuvent vous aider à mieux protéger vos données personnelles.

Stormshield, filiale à 100% d'Airbus Defence and Space, propose des solutions de sécurité de bout-en-bout innovantes pour protéger les réseaux (Stormshield Network Security), les postes de travail (Stormshield Endpoint Security) et les données (Stormshield Data Security).

Ces solutions de confiance de nouvelle génération, certifiées au plus haut niveau européen (EU RESTRICTED, OTAN et ANSSI EAL4+), assurent la protection des informations stratégiques et sont déployées au travers d'un réseau de partenaires de distribution, d'intégrateurs et d'opérateurs dans des entreprises de toute taille, des institutions gouvernementales et des organismes de défense partout dans le monde.

Contact : commercial@stormshield.eu

Glossaire

SaaS

Software as a Service ou logiciel en tant que service en ligne. Service proposé directement sur Internet, dont certaines applications sont parfois gratuites (Skype, MailChimp), généralement grâce à un abonnement (Dropbox, WebEx) ou un droit de licence (Office 365, Suite Adobe, Salesforce.com). Ces logiciels sont hébergés dans le Cloud et aucune donnée n'est conservée au sein de l'entreprise. C'est le fournisseur du SaaS qui propose également un hébergement des données. La question du lieu d'hébergement de ces données devient prépondérante dans le cadre du GDPR.

Décision-cadre

Dans le cadre de la coopération policière et judiciaire en matière pénale de l'Union européenne, elle permet au Conseil de l'Union européenne statuant à l'unanimité d'agir « aux fins du rapprochement des dispositions législatives et réglementaires des États membres »

Hacktivisme

Le hacktivisme est une contraction de hacker (pirate informatique) et activisme (politique). Des individus choisissent des actions référencées comme des cyber-crimes (piratage informatique) comme méthode d'engagement politique en divulguant, par exemple, des données confidentielles d'Etat, comme Julian Assange avec WikiLeaks ou en militant pour la confidentialité sur Internet comme les Anonymous.

Ransomware

Cela a été le cas du ransomware Chimera où les pirates se targuaient de pouvoir publier en clair, et sur un site public, les données qu'ils avaient chiffrées sur les machines de l'entreprise victime.

Directive

Acte juridique européen pris par le Conseil de l'Union européenne avec le Parlement ou seul dans certains cas. Elle lie les États destinataires de la directive quant à l'objectif à atteindre, mais leur laisse le choix des moyens et de la forme pour atteindre cet objectif dans les délais qu'lle a fixés au préalable.

Règlement

Acte juridique européen, de portée générale dont toutes les dispositions sont obligatoires: les États membres sont tenus de les appliquer telles qu'elles sont définies par le règlement. Celui-ci est donc directement applicable dans l'ordre juridique des États membres. Il s'impose à tous les sujets de droit : particuliers, États, institutions.

Droit à l'oubli numérique

Selon l'article 17 du GDPR, la personne concernée a le droit d'obtenir du responsable du traitement l'effacement des données à caractère personnel la concernant, ainsi que la cessation de la diffusion de ces données.

Chiffrement (des données)

Procédé de cryptographie permettant de rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé)chiffrement. Ce principe est généralement lié au principe d'accès conditionnel qui nécessite une autorisation préalable.

WWW.LINKEDIN.COM

TWITTER.COM/STORMSHIELD_

WWW.FACEBOOK.COM/STORMSHIELDOFFICIAL/

STORMSHIELD

Téléphone
+33 9 69 32 96 29
(Numéro Cristal)

WWW.STORMSHIELD.EU