psm

HORS-SÉRIE
CYBERSÉCURITÉ

Les Solutions pour les Professionnels de la Sûreté - Sécurité

JUILLET 2018 / 18 EUROS

Vidéosurveillance
QUELLES MENACES ?
QUELLES SOLUTIONS ?

Technologies sans contact
LE CONTRÔLE D'ACCÈS SE PROTÈGE DES CYBERATTAQUES

Stockage des données
LE CLOUD, VRAIMENT SÉCURISÉ ?

RGPD

Une priorité : sensibiliser aux cybermenaces P. 16

www.protectionsecurite-magazine.fr

© DR

BIO EXPRESS

1992 Entrée à l'École spéciale militaire de Saint-Cyr

2006 Institut diplomatique du ministère des Affaires étrangères

2007 Directeur délégué à la sécurité et sûreté du groupe Telecom Italia

2015 Directeur à la sécurité et sûreté de la RAI, radio-télévision italienne

2017 Création de Kelony-Cindynics Enterprise

KELONY

Kelony est le premier tiers de confiance pour la vérification et la validation des process de sûreté/sécurité des entreprises. Pour cela, Kelony s'appuie sur un réseau international et multidisciplinaire, composé de spécialistes reconnus dans leur secteur et sur un protocole de calcul des risques intercorrélés (SeVeVa) pour éviter les effets des réactions en chaîne.

Censéric Cantournet

Président directeur général de Kelony

« La protection des données personnelles est un nouveau droit fondamental que le RGPD inscrit dans le marbre. »

Censéric Cantournet a assumé les fonctions de directeur sûreté de grands groupes étrangers, puis fondé le cabinet Kelony. Pour *PSM*, il fait le bilan de l'entrée en vigueur du RGPD et de ce qu'il implique pour les entreprises.

Les sanctions du RGPD sont entrées en vigueur le 25 mai dernier. Quelle étaient, selon vous, la perception de la problématique cybersécurité et de la protection des données dans les entreprises jusqu'alors ?

Avant cette date, que certains considèrent à tort comme « butoir » – et je m'en expliquerai plus loin – un certain nombre d'entreprises était totalement démuni face à ces questions et n'agissait pas toujours en conséquence. Il est incontestable que le 25 mai aura contribué à changer la perception du risque « cyber ». Cela étant, un grand nombre d'entreprises, quelle que soit leur taille, ont perçu la mise en place du RGPD comme un désavantage compétitif sans aller au-delà. De ce fait, elles se sont limitées à le considérer uniquement comme une suite d'obligations qui n'appelait de leur part que des opérations ponctuelles de réponses à des prérequis, suivant des disciplines spécialisées et fragmentées ; à la manière dont on se rend « compliant » pour un certificat ou une check-list à remplir. Il n'en est rien puisque le RGPD pose des principes et n'indique ni quoi faire, ni comment le faire. Il inverse la charge de l'interprétation de la norme et laisse le soin aux entreprises de l'interpréter.

À l'instant, vous considériez que la date du 25 mai était trompeuse. Pourquoi ?

Le RGPD n'est pas un simple règlement auquel souscrire pas à pas, mais le signe tangible d'un changement des attentes de la société qui fait des données personnelles un droit fondamental inaliénable au même titre que l'intégrité physique. C'est la raison pour laquelle le 25 mai 2018 n'était pas une date butoir, mais bien au contraire une ligne de départ.On ne peut pas se contenter de répondre à la menace cyber et à la nécessité de protéger toutes les données collectées et exploitées par une entreprise en publiant une charte et en nommant un délégué à la protection des données personnelles (DPO). pour faire en sorte que ce droit soit respecté. et leur protection. Les cybermenaces ou les risques de non application des droits de ceux à qui appartiennent les ●●●

Gensériс Cantournet
Président directeur général de Kelony

« La protection des données dans l'entreprise ne se limite pas à la publication d'une charte ou à la nomination d'un DPO. »

●●● données, ainsi que la protection de ces dernières vont bien au-delà. En tant que droit fondamental gravé dans le marbre par le RGPD, la protection des données personnelles requiert un travail en profondeur de longue haleine afin de pouvoir mettre en œuvre, de manière coordonnée, des moyens techniques, légaux, culturels et comportementaux. Les entreprises ont tout intérêt à se faire conseiller sur les moyens, méthodes et procédures à mettre en place pour faire en sorte que ce droit soit respecté. Pour ce faire, elles doivent donc changer de culture en ce qui concerne les données personnelles et leur protection.

Que risquent les entreprises qui ne comprennent pas ce caractère « sociétal » de la protection des données ?

Elles risquent de voir leur image fortement écornée, dépréciée, et de ne tout simplement plus répondre aux attentes de leurs clients et usagers. Facebook, soit l'archétype de l'entreprise « sympa et cool » il y a encore quelques mois, en raison de la légèreté avec laquelle ils ont traité les données qu'ils collectent, semble aujourd'hui tomber de Charybde en Scylla.

Que doivent faire les entreprises pour aborder de manière efficace la sécurité des données ?

Les entreprises doivent se faire accompagner pour piloter leur stratégie interne mais aussi celle de leurs fournisseurs. Dans la mesure où d'une part les risques liés au RGPD sont particulièrement critiques pour l'entreprise, et où, d'autre part, il n'existe pas encore de jurisprudence en la matière, il convient d'adopter une stratégie de type « buttom up ». Il serait illusoire et dispendieux d'aborder l'ensemble des aspects du RGPD comme on n'aborderait de façon séquentielle l'ensemble de ses articles. Il faut donc au contraire partir d'une analyse pragmatique des risques afin de pouvoir répertorier et classer les risques Apex* qui pourraient fortement impacter le business de l'entreprise.

Concrètement, comment doivent-elles s'y prendre ?

Les entreprises doivent d'abord faire fi de l'idée trompeuse qu'on peut tout avoir mis en place pour se protéger. Il faut à la suite de l'analyse des risques décrite précédemment, raisonner en termes de vulnérabilités. Cette démarche doit les porter à combler les failles les plus importantes pour remonter ensuite à celles qui, bien que moins visibles de prime abord, n'en constitueraient pas moins une menace potentielle sur le long terme. Les risques liés au RGPD sont d'autant plus à prendre au sérieux que la non protection des données personnelles pourrait donner droit à l'ouverture de « class actions ».

Kelony travaille avec des entreprises qui veulent protéger leurs données. Pourquoi viennent-elles vous voir ?

Nos clients ont en général un niveau de maturité élevé et les entreprises avec lesquelles nous collaborons ont des fonctions plus ou moins bien coordonnées. Pour autant, dans la plupart des groupes nationaux ou internationaux, les directions des risques sûreté, industriels, environnementaux, professionnels et informatiques sont systématiquement séparées et ont parfois des objectifs non concordants. Kelony leur apporte donc la cindynique, une méthode univoque pour faire converger leurs objectifs, un tiers de confiance qui est le meilleur instrument de gouvernance des risques et enfin, à certaines conditions, leur confère la distinction d'excellence Kelony-Assured, comme garantie ultérieure de leur protection vis-à-vis de ces risques. ■

*Risques Apex : terme issu du protocole de cindynique SeVeVa qui décrit les risques intercorrélés qui sont à l'origine des réactions en chaîne et des catastrophes qui les accompagnent.