D'incertitudes en bonnes résolutions !

Stéphane MEYNET
Président
CERTitude NUMERIQUE

Une nouvelle année démarre avec comme toujours son lot de résolutions, de bilans et autres vœux. Un éternel recommencement. Les vœux, un exercice délicat pour ne pas répéter chaque année les mêmes banalités, constituent pourtant un moment fort, essentiel, qui permet de faire un bilan des actions engagées et des difficultés rencontrées, et de dresser des perspectives pour la nouvelle année.

Sur le plan de la sécurité numérique, l'année 2022 fut une fois de plus marquée par le nombre accru de cyberattaques, d'avancées… et de manifestations en tout genre.

Inutile de revenir sur les nombreuses cyberattaques qui ont perturbé entreprises, collectivités, hôpitaux, écoles, etc. Si le monde actuel est rempli de doutes et d'incertitudes, l'(in)sécurité numérique, elle, nous offre la certitude que les incidents (défaillances et cyberattaques) continueront de ponctuer notre quotidien. Comme le dit cette phrase si souvent répétée par les professionnels de la cybersécurité qu'elle en devient un mantra : « la question n'est pas de savoir si cela va arriver, mais quand ».

Une augmentation de la réglementation sur la sécurité numérique

En revanche, les travaux réglementaires méritent un regard attentif quant à leurs futures déclinaisons et mises en œuvre.

L'approbation de la directive NIS2 fin 2022 par exemple ouvre de belles perspectives avec probablement en France de nouvelles mesures de sécurité numérique pour de nouvelles catégories d'opérateurs ainsi que l'élargissement du nombre d'Opérateurs de Service Essentiel. La mise en place de cette directive pourrait conduire à établir 3 niveaux / 3 classes d'opérateurs (vitaux, importants et essentiels) pour lesquels s'appliqueront des mesures cohérentes et proportionnées à leur criticité. Il sera intéressant d'en suivre la transcription dans notre droit et ceux de nos partenaires européens.

Autres points d'intérêt : la LOPMI, votée en fin d'année 2022, dans laquelle figurent le très attendu 17 cyber (même si ce futur dispositif ne nécessite pas de mesure législative) et une accentuation du rôle des préfets en matière de sécurité numérique des territoires ; ou encore la loi du 3 mars 2022 qui crée le CyberScore, certification de cybersécurité des plateformes numériques destinées au grand public. Autant de sujets prometteurs qui constituent autant d'avancées, dont la concrétisation présente un certain nombre de défis.

DSA, DMA, Cyber Resilience Act… ces autres textes

européens viennent là encore compléter l'arsenal réglementaire destiné à renforcer la sécurité et la confiance numériques des états membres et leur résilience face au risque numérique. Ajoutons à cela le RGPD, en vigueur depuis 2016 : les contraintes sont croissantes pour un nombre toujours plus important d'acteurs dont les entreprises et les collectivités territoriales…

Pour résumer, une année riche en réglementations. Peut-être même trop riche.

Le Plan de Relance Cyber en action

Dans le prolongement de l'annonce faite par le Président de la République le 18 février 2021, les actions du Plan de Relance Cyber continuent de se déployer : développement du Campus Cyber ; soutien aux projets pour renforcer la sécurité numérique des collectivités, des établissements dans les domaines de la santé et le portuaire, et à la filière pour favoriser l'innovation et créer les licornes de demain ; création des CSIRT régionaux sur les territoires dont les préfigurations laissent néanmoins craindre une forte disparité entre les régions et interrogent sur la pérennité du modèle. Au-delà du chiffre d'un milliard du Plan de Relance Cyber, il sera intéressant de suivre l'efficacité des mesures conduites et donc de la dépense publique dans ce domaine.

La multiplication des événements sur la sécurité numérique

L'intérêt grandissant pour la sécurité numérique des institutions n'a pas été un phénomène isolé, comme le montre le nombre croissant d'événements de tous types qui ont ponctué l'année 2022. Les nombreuses manifestations sur la cybersécurité sous de multiples formes (forums, séminaires, workshops, webinaires, journées de rencontres, conférences...) montrent, et c'est une avancée, l'intérêt grandissant du monde de la cybersécurité pour les PME /TPE, les collectivités territoriales ou d'autres sujets thématiques comme les femmes et la cybersécurité, qui jusqu'alors n'avaient pas été forcément au centre des préoccupations. Elles montrent également l'abondance, voire la surabondance, d'acteurs se positionnant sur la cybersécurité, par opportunisme et sans le niveau de confiance nécessaire, ainsi que la surabondance d'événements dont la finalité et les contenus laissent parfois dubitatifs. Que penser également de ceux qui plagient mot pour mot sans vergogne les présentations et les travaux engagés depuis des années par d'autres pour bricoler du reconditionné…

Ces trois points dans ce qu'ils constituent de côtés positifs devraient nous rassurer quant à la prise en compte de la sécurité numérique par de nombreux acteurs, sur l'ensemble des territoires et au plus haut niveau de l'État et de l'Union européenne. Et donc logiquement nous rassurer quant à la sécurité de nos systèmes numériques dans les années à venir.

Mais tout ceci favorise-t-il vraiment le développement d'un numérique de confiance ?

En écoutant les bruits de fond, ces fameux signaux faibles, ce qui se dit hors des estrades ou webinaires, il semblerait que le tableau ne soit pas aussi lisse.

En effet, plutôt que de rassembler, fédérer, éclairer, nombre d'actions menées en 2022 conduisent davantage à disperser, concurrencer, égarer voire ennuyer faute de cohérence et de coordination.

L'abondance des réglementations, ou des normes et standards pour lesquels le constat est le même, risque de noyer encore d'avantage les acteurs de la cybersécurité et les utilisateurs qui peinent déjà aujourd'hui à « y voir clair ». Sans parler du manque de moyens, tant humains que financiers, qui sont au cœur des enjeux de sécurité numérique des entreprises et des collectivités, notamment les plus petites, que les réglementations ne comblent pas.

Chaque jour nos messageries électroniques regorgent d'invitations et d'informations pour des événements sur la cybersécurité, très souvent sur les mêmes thèmes et avec le même angle d'attaque. Comment identifier parmi cette masse les événements et informations pertinentes, les acteurs et les paroles de confiance ?

Certes, la sécurité numérique est aujourd'hui un marché, parfois lucratif, avec des perspectives plutôt attrayantes contrairement à d'autres domaines, et c'est tant mieux ! Mais le marché, surtout lorsqu'il s'agit de sécurité numérique, ce qui sous-entend des questions de confiance numérique, de souveraineté et de sécurité nationales, de viabilité de nos sociétés, ne peut s'affranchir d'une certaine éthique, une vision au-delà d'un résultat commercial immédiat, surtout entre des organisations battant même pavillon. Il est ainsi dommageable que le terme de « far west » revienne désormais fréquemment dans les discussions à propos du marché de la sécurité numérique.

Le constat est que nous avons progressivement perdu l'esprit qui animait l'écosystème cybersécurité à ses débuts et dans ses premières années. J'ai en mémoire cette phrase, forte : « la cybersécurité est l'école de l'humilité ». Certains reconnaîtront son auteur. Malheureusement, notre ère, et cela ne concerne pas que la cybersécurité, consacre davantage la communication plutôt que les travaux, la forme, voire les paillettes, plutôt que le fond. La course aux « buzzwords » tels qu' « innovation », « IA », « blockchain », « start-up », « licornes » et tant d'autres, nous détourne du fond et des valeurs essentielles de la cybersécurité. L'IA, l'innovation, etc. représentent bien évidemment des sujets majeurs, mais demandent une approche de fond, raisonnée et cohérente. Une vision qui dépasse le court terme et qui s'appuie sur de la coopération.

Tout cela positionne-t-il la France parmi les leaders en la matière comme l'a souhaité le Président de la République lors de la présentation de la Revue Stratégique Nationale ? Sommes-nous mieux préparés, mieux armés que d'autres pays au regard des moyens mis en œuvre ? Un parangonnage international pourrait apporter un éclairage fort utile pour la définition et l'évolution de nos politiques publiques.

Alors que nous souhaiter pour 2023 en termes de bonnes résolutions pour la sécurité numérique ?

- Revenir aux fondamentaux, c'est-à-dire, au risque de ne pas être original, revenir aux métiers au service desquels est la cybersécurité : les métiers de la santé, de l'industrie, de l'agriculture, de la défense, etc. La cybersécurité pour la cybersécurité n'a pas d'intérêt.
- En faire moins, moins précipitamment, moins de réglementations, moins de normes et standards, moins d'initiatives tous azimuts pour faire mieux tout en gardant un cap et une visibilité clairs pour tous.
- Intégrer plus de sciences humaines et sociales dans les réflexions et les travaux sur la sécurité numérique : nos grands scientifiques, ceux qui ont marqué notre histoire, n'étaient-ils pas souvent en même temps philosophes voire théologiens ?
- Replacer les valeurs d'éthique et d'humilité au cœur de la sécurité numérique.
- S'attacher à la coordination, au pragmatisme, à la continuité et à la cohérence des actions engagées aux niveaux européen, national et local.
- Travailler ensemble, mettre nos forces respectives au service de l'intérêt général.

L'année 2023 sera-t-elle l'année qui permettra d'« agir efficacement ensemble pour une culture de sécurité numérique partagée » ? ©CyberCercle

En tous cas, bonne année 2023 à tous !