Cyberdéfense : l'Europe doit penser communauté et besoin marché pour réussir

Face à l'explosion des cyberattaques, la Commission européenne (CE) a, en décembre dernier, lancé une nouvelle stratégie de cybersécurité pour la période 2020-2025. Echange d'information inter-pays, formation, réglementation, certification… autant de leviers qui seront mis en place pour que la cybersécurité européenne ait une orientation commune tout en préservant ses souverainetés nationales.

Une stratégie reposant sur plusieurs axes

Premier axe : la réglementation. En adoptant le règlement européen Cybersecurity Act, la CE marque une véritable avancée pour l'autonomie stratégique européenne et tente de promouvoir un schéma de certification à l'échelle européenne afin d'harmoniser les méthodes d'évaluation et les différents niveaux d'assurance de la certification de la cybersécurité.
L'ENISA, Agence européenne pour la cybersécurité, devient un pilier de la coordination et une structure d'autorité européenne. Tout ceci tend à montrer que nous sommes sur la bonne voie, encore faut-il que l'Europe conditionne son marché à utiliser ce règlement !

Dans le cadre de cette stratégie, la CE marque aussi une volonté d'aider les entreprises, quelle que soit leur taille et leur secteur d'activité, à s'organiser pour lutter contre les cyberattaques. Mais si cette initiative est louable, sa concrétisation reste en revanche complexe car le marché souffre d'une forte pénurie de profils spécialisés.

Dans le deuxième axe marqué par l'investissement humain, la CE propose plusieurs actions: développer des cursus préparatoires dédiés à la cybersécurité et généraliser des plateformes d'entraînement. Un souhait, qui espérons-le, ne se résumera pas à une simple lettre d'intention, mais sera soutenue par une véritable politique de formation afin de donner à l'Europe les moyens de gagner son autonomie en cybersécurité. Peut-être aurait-il fallu orienter davantage l'investissement vers la technologie, intrinsèquement plus capable de passer à l'échelle ?

Troisième axe : la coopération inter-pays. La France est l'un des pays européens les plus structurés en matière de cybersécurité, grâce notamment à l'ANSSI et d'autres structures qui insufflent depuis plus de 10 ans une dynamique rigoureuse et initient de nombreux chantiers.
La stratégie nationale proposée par Emmanuel Macron avec un plan de relance d'un milliard d'euros sur la table semble pertinente, tant sur l'articulation avec l'ambition européenne que sur le contenu !

Mais les 27 pays d'Europe ont des degrés de maturité et des capacités d'actions très différents. L'Europe va donc inciter les pays à mettre en place une meilleure circulation des informations afin de se coordonner pour traiter les attaques majeures et développer une cyberdéfense efficiente.
Le terme de communauté apparaît comme un pilier fort de la stratégie européenne. C'est une

bonne chose car la cybersécurité ne fonctionne que si elle est appliquée en réseau, avec des informations qui circulent et son partagées entre les parties prenantes.

Dans cette volonté du concret, le sujet du partage d'informations communautaire doit être creusé en profondeur et rapidement mis en place. Les États-Unis utilisent ceci depuis longtemps à travers des centres de partage sectoriels comme les ISACs. Nos secteurs industriels doivent apprendre à mieux partager de l'information cyber car dans ces domaines, le renseignement diffusé par l'un fait la protection de tous les autres.

Le marché : la composante oubliée de la stratégie européenne !

La stratégie européenne telle que détaillée plus haut semble omettre la composante marché – ou du moins laisser le sujet pour plus tard. S'il est vrai que cette stratégie est bâtie sur de bonnes idées et une orientation bien délivrée, c'est la suite qui risque de bloquer entre des approches trop nationales, trop restrictives et des règles d'allocations budgétaires incohérentes entre les pays.

La cybersécurité existe depuis plus de 20 ans et sur ce terrain l'Europe n'a pas particulièrement brillé en comparaison d'autres blocs. Pour autant tout n'est pas encore perdu mais il faut regarder les choses en face et tirer les constats.

A l'heure actuelle, il faut arrêter les investissements scientifico-scientifiques non appliqués à un besoin marché. Il est important de développer les partenariats publics-privés à l'échelle européenne pour avoir une vraie stratégie d'action dans les domaines qui seront nécessaires demain et dans 10 ans. (l'automatisation orchestrée de la cybersécurité, la modélisation des techniques d'attaques, la détection prédictive des attaques et des anomalies…)

Comme évoqué, le Cybersecurity Act est un bon point de départ mais il nous faut accepter d'aller plus loin dans les programmes de certifications pour les rendre obligatoires pour le marché européen. Cela se traduira notamment pour les entreprises par des obligations à créer des liens avec les industriels cyber autour d'eux et d'offrir une chance aux startups européennes du secteur en leur allouant une partie des budgets cyber…

Enfin, il est nécessaire d'expérimenter des modèles vertueux et pragmatiques dans lesquelles les entreprises expriment des besoins, les fournisseurs candidats calibrent des roadmaps pour y répondre et les organismes publics accompagnent et soutiennent financièrement certains investissements. Les structures académiques ayant elles aussi un rôle majeur à jouer pour les sujets faisant appel à la recherche.