La pandémie de COVID-19 a plongé nos sociétés mondialisées dans une crise sanitaire et économique sans précédent. Le télétravail est devenu en quelques semaines la norme de fait pour la quasi-totalité d'une population planétaire confinée au même instant. Cette résilience immédiate, inimaginable il y a encore quelques dizaines d'années, a été rendue possible par le numérique et la cybersécurité, outils indispensables à la continuité d'activité des entreprises.

En France, les adhérents d'Hexatrust ainsi que de nombreux acteurs de la filière ont répondu à l'appel du Gouvernement dans un «acte de citoyenneté» visant à fournir des solutions et des conseils gracieux aux acteurs de notre économie.

Quel serait le premier grand enseignement de cette crise ? La dépendance de notre industrie a été démontrée quand le besoin en équipements de protection individuels et en dispositifs de santé s'est fait criant. Or, la cybersécurité est au numérique ce que les masques, les tests, les respirateurs artificiels ou les vaccins sont à notre appareil de santé. Il est une partie intégrante de la résilience de la Nation. C'est pourquoi il est désormais de notre devoir d'anticiper la prochaine pandémie… Et celle-ci sera potentiellement numérique.

L'industrie de cybersécurité est critique et indispensable à la souveraineté de la nation. Elle est de surcroît véhicule d'emplois, de croissance et d'inclusion sociale.

En France, nous constatons que tous les secteurs d'activités ne sont pas également équipés en matière de numérique et insuffisamment préparés au risque inhérent. Nos entreprises et organisations consomment essentiellement des produits numériques importés, sans réelle prise en compte des implications qu'ils ont en matière de respect de protection des données ou de maîtrise de notre autonomie stratégique. Ainsi, les solutions de télétravail mises en œuvre sont essentiellement étrangères et ont entrainé une fuite massive d'informations confidentielles hors d'Europe.

Cette ultra-dépendance aux outils et plateformes étrangères doit constituer un avertissement pour notre secteur. Elle doit amorcer une réflexion en profondeur de nos approvisionnements tout en restant vigilant au prix de la souveraineté pour les utilisateurs finaux ! La souveraineté doit devenir un avantage concurrentiel sur le marché mondial, en proposant des solutions souveraines à un prix compétitif et à un niveau de fonctionnalité équivalent.

En ce sens, nous formulons **cinq vœux pour une autonomie stratégique européenne sur le plan du numérique** pour lesquels il faudra préalablement définir les critères exhaustifs qui fonderont la souveraineté européenne.

5 VŒUX Pour une autonomie stratégique Européenne

1. Initier un « plan d'équipement cyber »
2. Instaurer une proportion d'achats fléchés vers les PME françaises de confiance
3. Participer à l'émergence d'une Europe de la Cybersécurité
4. Accroître l'investissement dans les entreprises cyber stratégiques notamment les **ETI** de croissance
5. Instaurer une « assurance Cyber »

Club des Directeurs CDSE de Sécurité des Entreprises

HEXATRUST CLOUD CONFIDENCE & CYBERSECURITY

En association avec le club des juristes