ÉCONOMIE

Le marché mondial des solutions de cybersécurité devrait atteindre 80 à 120 md $ d'ici 2018.

LES RETOMBÉES DES DÉCLARATIONS EUROPÉENNES SUR LA CYBERSÉCURITÉ ET L'ACCÈS AU MARCHÉ NUMÉRIQUE

par Mark Skilton

La structure de gouvernance de l'Union européenne est habilitée à adopter des mesures dans le but d'établir ou d'assurer le fonctionnement du marché intérieur. Compte tenue d'une énorme fragmentation du marché des technologies de l'information et de la communication, des produits et des solutions de sécurité TIC, l'action de l'UE est nécessaire pour réaliser un marché unique dans ce domaine, ce qui est également une condition préalable au bon fonctionnement de l'économie numérique.

Plusieurs défis doivent être relevés si l'on veut atteindre l'objectif d'un marché unique numérique dans l'UE. Les 28 États membres actuels de l'UE n'ont pas fait preuve de la même capacité à rivaliser à cause d'un fort effet de levier provenant de leur propre base de fournisseurs contre la concurrence souvent venue de l'extérieur du bloc de l'UE. L'espace informatique est par nature sans frontières et de plus en plus complexe, avec des attaques allant du refus de service aux violations et vols de données, en passant par l'espionnage, la surveillance et le terrorisme. De manière générale, ces attaques ne cessent d'augmenter dans tous les secteurs de l'industrie et entraînent un fort développement de contre-mesures et d'investissements provenant des fournisseurs de

technologie, de l'industrie et des gouvernements de tous les pays.

Etats des lieux de la cybersécurité dans l'UE

Outre les "cybermenaces" et la nécessité de les gérer, il est essentiel d'atteindre une confiance renforcée et sécurisée dans cet espace virtuel pour obtenir un marché harmonieux. Le secteur des solutions en cyber sécurité est un marché à forte croissance qui devrait se développer jusqu'à atteindre 80 à 120 md $ d'ici 2018. Le défi a consisté à investir et coordonner les propres solutions et fournisseurs de l'UE, qui ont eu beaucoup de mal à concurrencer les fournisseurs de TIC extérieurs à leur pays (et surtout à l'UE).

Le marché de l'UE a été dominé par un petit groupe de fournisseurs mondiaux rivalisant avec un grand nombre de fournisseurs européens plus petits. Les cinq principaux fournisseurs contrôlent 20,4 % du marché total (ils proviennent tous de l'extérieur de l'UE). Les fournisseurs de l'UE restent principalement des acteurs nationaux et régionaux. Leur part de marché cumulée a été estimée à environ 16,5 % du total des revenus du marché du Service d'information du réseau (NIS) de l'UE. La fragmentation de l'industrie de l'approvisionnement en cyber sécurité en Europe est l'une des principales raisons des récentes initiatives de l'UE en matière de réglementation de la cyber sécurité.

Comment prévenir les cyberattaques

Parmi les éléments importants qu'un cyber praticien doit retenir, il y a le fait que la cyber sécurité couvre un large éventail d'attaques sur les équipements, les logiciels, les réseaux, et les centres de bases de données qui sont généralement répartis sur plusieurs fournisseurs et services de cloud computing. "Une seule personne ne peut pas tout faire." - il s'agit d'un secteur en constante évolution de personnes et des développements technologiques, et il est nécessaire d'en garder la maîtrise et d'avoir une "approche décloisonnée" entre les entreprises, les autorités publiques et les citoyens afin d'en favoriser l'adoption. "Attaques de plusieurs côtés" - un grand nombre d'attaques proviennent potentiellement des nombreuses "failles" révélées lors de cyber attaques. Les leçons tirées des précédentes cyber attaques : l'ampleur des violations de données (des millions d'enregistrements et le nombre de facteurs de menace). Par exemple, les attaques sur les banques russes en 2015 provenaient de logiciels malveillants introduits furtivement. Les attaques dites "Zéro day", (autrement dit une vulnérabilité n'ayant fait l'objet d'aucune publication connue implique qu'aucune protection n'existe) pourraient bien augmenter en nombre et leurs caractéristiques informatiques devenir plus sophistiquées.

La nécessité d'harmoniser le marché européen

La solution consiste à établir des partenariats permettant de gérer la connaissance et la sensibilisation dans l'UE, ainsi que dans les autres pays et l'industrie. Le taux de renouvellement dans la cyber technologie et les cyber attaques nécessite une approche réactive et évolutive pour garder une longueur d'avance et être en mesure de diriger le marché. L'utilisation de la législation de l'UE progressera pour chercher à établir les fondements d'une réponse conjointe et coordonnée.

L'Article 25 du Règlement du Parlement européen et du Conseil qui établit l'Horizon 2020 fournit le cadre légal de l'établissement d'un partenariat public-privé. L'accord contractuel doit préciser les objectifs du partenariat, les engagements respectifs des partenaires, les indicateurs clés de performance et les résultats. Il faut mettre en œuvre une approche de la cyber sécurité à l'échelle de l'UE et renforcer la coopération actuellement limitée entre les États membres ; les secteurs clés de l'économie seraient soumis à des obligations de sécurité suite à une approche visant à harmoniser le marché interne. Il est donc très probable que la mise en œuvre des exigences commerciales en vertu de la Directive NIS (service d'information du réseau) entraînera une demande accrue des solutions de cyber sécurité.

Ne rien faire maintiendrait le statu quo de l'UE relatif à des approches largement nationales et ne permettrait pas de créer un marché européen efficace pour les produits et services de la cyber sécurité. L'UE ne serait donc pas en mesure de répondre à la demande croissante de services d'information du réseau par les fournisseurs de l'UE, et cela serait une occasion manquée pour l'Europe de devenir un leader mondial dans le domaine de la cyber sécurité. Pour les États membres de l'UE, c'est la direction que doit prendre la stratégie afin de faire face à la nature sans frontières de la cyber sécurité mondial et soutenir les économies mondiales et locales modernes dans tous les secteurs. Les pays non membres de l'UE comme les pays de l'UE ont tous un intérêt particulier à ce que cela fonctionne.

> AUTEUR
Mark Skilton a 30 ans d'expérience en tant que consultant en affaires et en informatique. Il est actuellement professeur en Gestion et innovation des systèmes d'information à la Warwick Business School, au Royaume-Uni. Son dernier ouvrage : 4th Industrial Revolution and A.I. publié par Palgrave Macmillan