Communiqué de presse ACN
12 mars 2019

Adoption par le Parlement européen du *Cybersecurity Act* : Vers un cadre clair et harmonisé de la cybersécurité au niveau européen !

Après deux ans de travaux intenses, le Parlement européen a adopté aujourd'hui en session plénière, le European Cybersecurity Act. Ce texte vient compléter les bases réglementaires qui permettront à terme de rehausser le niveau de cybersécurité à travers toute l'Europe. L'Alliance pour la Confiance Numérique (ACN) s'est fortement mobilisée tout au long du parcours législatif de ce texte et a proposé de nombreux commentaires et amendements à ce projet afin notamment qu'il intègre les acquis et les savoir-faire développés les industries de la confiance numérique depuis plus de 20 ans préserve une ambition forte de cybersécurité globale pour l'Europe.

C'est pourquoi, l'ACN se félicite de ce nouvel outil qui définit un cadre clair et harmonisé pour la mise en œuvre de la cybersécurité dans tous les secteurs économiques. En effet, l'édiction de règles communes en matière de certification en cybersécurité au niveau européen constitue une avancée primordiale pour permettre le développement d'un marché unifié Européen au bénéfice des PME et des grands groupes de la confiance numérique.

L'Alliance pour la Confiance Numérique (ACN) salue l'adoption par le Parlement européen de la proposition de règlement relatif à l'ENISA (Agence européenne chargée de la sécurité des réseaux et de l'information) et à la certification des technologies TIC, dite « *European Cybersecurity Act* ». Ce texte, qui devra désormais être adopté par le Conseil européen, donne un mandat permanent à l'ENISA et créé un cadre européen de certification de cybersécurité. Le *Cybersecurity Act* devrait contribuer à réduire la fragmentation du marché européen grâce à la mise en place des futurs schémas européens de certification. Dorénavant, un fournisseur de produits, services et processus TIC ne sera plus obligé de passer par plusieurs schémas de certification nationaux. « *Les schémas européens de certification devraient renforcer la transparence du marché des produits TIC en donnant des indications sur le niveau d'assurance d'un produit. Depuis des années, nous œuvrons pour que les certifications de cybersécurité aient une portée européenne, sans que cela ne se traduise par un nivellement par le bas, et s'adaptent aux besoins des clients en équilibrant le niveau de protection recherché en fonction de l'analyse des risques avec la réalité économique du produit/service concerné. Cela permettra de créer de la confiance, d'augmenter la cybersécurité générale et de créer un marché européen atteignant ainsi la taille critique pour nos entreprises, et notamment les plus petites d'entre-elles.* » déclare Jean-Pierre Quémard, Président de l'ACN.

Le *Cybersecurity Act* établit un système de certification multi-niveaux qui prend en compte, grâce à une analyse préalable des risques, la bonne adéquation entre les exigences de sécurité et le besoin de protection, ce qui correspond aux besoins du marché. Les produits, services et processus TIC peuvent être certifiés à un niveau d'assurance élémentaire, substantiel ou élevé. Le niveau élémentaire correspond aux produits les moins critiques et est assorti d'une simple procédure déclarative. A l'autre bout du spectre, les produits et services dont la résistance aux cyberattaques est cruciale, tels que des puces électroniques, peuvent être certifiés au niveau d'assurance élevé par le biais d'une procédure plus robuste. La version finale du *Cybersecurity Act* introduit une exigence de tests de pénétration pour le niveau d'assurance élevé. « *Les tests de sécurité sont indispensables pour garantir la résistance à des attaquants expérimentés et dotés de ressources conséquentes. En cybersécurité, la conformité à un cahier des charges ne garantit jamais l'infaillibilité des systèmes de protection : si l'on veut s'assurer d'un niveau réel de sécurité, il faut impérativement soumettre le produit à du hacking éthique et des tests de pénétration* en vraie grandeur» explique Jean Pierre-Quémard.

Contact presse: Yoann KASSIANIDES – ykassianides@confiance-numerique.fr – 06.26.78.57.55

L'ACN souligne que le succès du volet certification du *Cybersecurity Act* dépendra essentiellement de la capacité de la Commission et de l'ENISA à créer des schémas qui soient susceptibles d'être adoptés par le plus grand nombre. Les schémas de certification sont volontaires et ils ne seront utilisés que s'ils sont adaptés aux réalités du marché.

Aussi, pour l'ACN, les recommandations suivantes permettront de faire du *Cybersecurity Act* un succès en matière de certification :

- **Impliquer toutes les parties prenantes**

Le nouveau règlement créé un *Stakeholder Cybersecurity Certification Group*. Celui-ci a pour mission de conseiller la Commission et l'ENISA sur les points stratégiques relatifs à la certification de cybersécurité. L'ACN recommande à la Commission et à l'ENISA de tirer le plus grand profit de cette expertise. Les consultations publiques et les travaux effectués par les groupes de travail *ad hoc* doivent également aiguiller le travail des institutions.

- **Préserver les acquis stratégiques en matière de certification**

Dès le début de la procédure législative, l'ACN a eu à cœur d'insister sur la nécessité de préserver les acquis stratégiques en matière de certification issus de plus de vingt d'expertise et de savoir-faire des acteurs du secteur. Le SOG-IS MRA, par exemple, a démontré au cours des années qu'il était un outil adapté pour la certification des produits stratégiques à un niveau d'assurance élevé**. L'ACN se félicite d'ores et déjà de la décision de l'ENISA de créer un premier schéma européen sur la base du SOG-IS MRA.**

- **S'appuyer sur les normes existantes**

Les futurs schémas de certification ne pourront être adaptés par le marché que s'ils reposent sur les normes existantes. Les travaux des organisations européennes de normalisation, telles que le CEN/CENELEC et l'ETSI, de même que ceux de l'organisation internationale ISO/IEC, doivent être utilisés dans les futurs schémas.

- **Assurer une approche harmonisée de la certification**

Malgré la volonté de créer un cadre européen harmonisé, le risque de disparité entre Etats membres subsiste. Les processus d'accréditation et de supervision des organismes d'évaluation de la conformité continueront de relever de la compétence des autorités nationales de contrôle de certification. En outre, les autorités nationales seront en charge de délivrer certains certificats de cybersécurité. Des approches différentes pourraient donc donner lieu à des certificats qui n'auraient *de facto* pas la même valeur en termes d'assurance. Ces certificats seront pourtant reconnus dans tous les Etats membres. Une telle disparité conduirait à un manque de transparence et diminuerait la confiance que des utilisateurs pourraient avoir en ces certificats. **L'ACN salue l'introduction d'un système de *peer review* entre autorités nationales dans la version finale du *Cybersecurity Act*. Ce système devrait limiter ce risque de disparité. L'ACN encourage les Etats membres à tout mettre en œuvre pour que ce système de *peer review* conduise effectivement à une approche harmonisée de la certification européenne.**

A propos de l'ACN :

L'Alliance pour la Confiance Numérique (ACN) représente les entreprises (leaders mondiaux, PME, et ETI) du secteur de la confiance numérique notamment celles de la cybersécurité, de l'identité numérique, des communications sécurisées, de la traçabilité / lutte anti-contrefaçon et de la safe city. La France dispose dans ce domaine d'un tissu industriel très performant et d'une excellence internationalement reconnue grâce à des leaders mondiaux, des PME, des ETI et aux différents acteurs dynamiques du secteur. On dénombre environ 850 entreprises réalisant en France près de 9 Milliards d'euros de chiffre d'affaires dans ce secteur en forte croissance (plus de 12% de croissance chaque année depuis 2014). L'ACN est membre de la FIEEC (Fédération des Industries Electriques, Electroniques et de Communication) et participe activement à ce titre aux travaux du Comité Stratégique de filière des Industries de Sécurité. Par ailleurs, l'ACN est également membre fondateur de l'ECSO (European CyberSecurity Organisation).

Contact presse: Yoann KASSIANIDES – ykassianides@confiance-numerique.fr – 06.26.78.57.55