Position ACN/Hexatrust sur la proposition de règlement de la Commission européenne sur l'ENISA et la certification des TIC en matière de cybersécurité (European Cybersecurity Act - COM(2017) 477 final)

2 octobre 2017

A l'occasion du discours sur l'état de l'Union prononcé par le Président de la Commission européenne Jean-Claude JUNCKER, la Commission européenne a présenté le 13 septembre dernier, une série de mesures relatives à la cybersécurité, dont notamment une communication intitulée « *Resilience, Deterrence and Defence : Building strong cybersecurity for the EU* » ainsi qu'une proposition de règlement sur l'ENISA et la certification des TIC en matière de cybersécurité.

Ce projet de règlement ambitionne de redéfinir le mandat et le rôle de l'ENISA et propose de créer un nouveau schéma européen de certification en matière de cybersécurité.

L'ACN et Hexatrust partagent pleinement les objectifs de la Commission européenne d'harmonisation des règles encadrant les dispositifs de cybersécurité en Europe et notamment en matière de certification. En effet, la numérisation de l'ensemble des activités et des secteurs économiques crée un besoin stratégique majeur de cybersécurité.

L'ACN et Hexatrust considèrent que la réponse à cet enjeu doit être coordonnée au niveau européen de manière à obtenir un niveau de sécurité le plus élevé possible face aux menaces cyber dans tous les secteurs. Cette réponse doit pour autant être adaptée aux besoins de sécurité et aux usages considérés, ce qui nécessite la définition de critères de certification de cybersécurité multi-niveaux, qui assurent en fonction du domaine considéré une protection optimale en intégrant la réalité économique du secteur avec des délais et de coûts de certification maitrisés.

Il est primordial de préserver, dans les domaines particulièrement sensibles, par exemple ceux relevant de la souveraineté ou de la sécurité nationale, un système de certification permettant de garantir un niveau maximal de protection tel que celui qui résulte de l'application des Critères communs. Les produits, services et solutions soumis à ce plus haut niveau de certification doivent en outre être soumis à des tests réalisés par des experts, seul moyen de garantir un niveau de protection optimal et réel. Dans d'autres domaines moins exposés ou moins critiques, les exigences en matière de cybersécurité peuvent être moindres, notamment en vue de permettre une meilleure réactivité et de limiter le coût et les délais inhérents à tout processus de certification.

L'ACN et Hexatrust considèrent que la proposition de réglementation de la Commission européenne apporte un progrès indéniable notamment grâce à l'introduction du principe d'une certification unique valable dans l'ensemble des Etats-membres de l'Union européenne. L'ACN et Hexatrust regardent très favorablement l'idée de renforcer le rôle de l'ENISA et de la Commission Européenne en tant que gardiens du temple des schémas européens permettant ainsi la création d'un marché unique de la cybersécurité. La définition légale d'une entité nationale « National Certification Supervision Authority » pour tous les états-membres et leur coordination sont également une avancée utile en vue d'harmoniser les outils à disposition de chaque Etat dans le domaine de cybersécurité.

Pour autant, certains points de cette proposition appellent néanmoins une attention particulière de la part des entreprises du secteur de la confiance numérique qui souhaitent notamment :

1) Conserver les acquis stratégiques majeurs issus de l'accord de reconnaissance mutuelle du certificat de hauts niveaux de sécurité émis par l'ANSSI et ses homologues européens (SOGIS MRA) dans le nouveau modèle

L'ACN et Hexatrust saluent la mise en place d'un schéma unifié pour les certifications en matière de cybersécurité, ainsi que du rôle prépondérant accordé à l'ENISA dans l'initiation, le traitement et la coordination de ces initiatives.

Pour autant, l'ACN et Hexatrust souhaitent que cette transition puisse s'opérer dans une durée assez longue pour éviter toute rupture préjudiciable au marché et dans des conditions compatibles avec la préservation des acquis fondamentaux, construits depuis plus de 20 ans par l'ensemble des acteurs publics et privés du secteur. Plus particulièrement, l'ACN et Hexatrust souhaitent que les exigences édictées notamment par le SOG-IS MRA soient intégralement reconduites dans le nouveau schéma de certification et ainsi étendues à l'ensemble des pays européens dans un souci d'harmonisation.

En effet, les points forts de la cybersécurité européenne (tels que l'encryption, le chiffrement local (éléments sécurisés) ou centralisé (HSM), les logiciels embarqués sécurisés, les puces et composants sécurisés) se sont développés en capitalisant sur l'expérience accumulée en particulier en France grâce aux schémas d'évaluation des produits (critères communs et SOGIS MRA, CSPN, …) mis en place par l'ANSSI. L'ACN et Hexatrust sont extrêmement soucieux de préserver les positions de leaders mondiaux que les industriels européens ont su conquérir sur leurs marchés grâce par exemple au bon fonctionnement du schéma SOG-IS MRA.

Au-delà de ce bilan économique, ce sont aussi les notions stratégiques de souveraineté et de conservation de la capacité européenne de cyberprotection que l'ACN et Hexatrust souhaitent voir sanctuarisées. En effet, alors que cette proposition de règlement affiche l'ambition d'augmenter le niveau de cybersécurité de l'Europe, la définition de la nouvelle organisation des schémas d'évaluation/certification aboutira, de facto, à une diminution du niveau d'expertise et donc de confiance, finalement contraire aux objectifs initiaux.

Proposition

- **Reprendre le contenu et les principes du SOG-IS – MRA en annexe du règlement pour en faire le schéma de certification de référence sans préjudice du développement d'autres schémas de certification avec des exigences moindres adaptées aux besoins de domaines moins stratégiques.**

2) Capitaliser sur les autorités nationales pour garantir une plus grande homogénéité

Les sujets de cybersécurité ayant un lien consubstantiel avec les domaines de la souveraineté et de la sécurité nationale, les acteurs industriels de l'ACN et d'Hexatrust souhaitent que cette dimension nationale puisse avoir une traduction dans les nouveaux schémas proposés.

Aussi, il est essentiel que dans le processus conduisant à l'élaboration de nouveaux schémas, le EU Cybersecurity certification Group et les Etats membres aient, au côté de l'ENISA, un pouvoir de codécision tant pour initier que pour valider les nouveaux schémas de certification.

Par ailleurs, dans la mise en œuvre des schémas au niveau national, l'ACN et Hexatrust proposent, afin notamment d'améliorer la diffusion des bonnes pratiques, que les National Certification Supervisory puissent être validés par l'ensemble des autorités nationales européennes, dans un système de peer review.

Propositions

- Soumettre l'initiation et la validation formelle des nouveaux schémas de certification à une validation formelle des entités nationales de sécurité (via le European Cyber security Certification group) pour les niveaux élevés de sécurité (correspondant actuellement aux niveaux supérieurs à EAL4+) avant la finalisation des schémas par l'ENISA et la publication des actes d'implémentation.
- Instituer un trilogue entre la Commission européenne, l'ENISA et l'European Cybersecurity Certification group permettant de faire émerger des compromis dans la création des schémas.
- Instaurer un système de peer review entre les « National Certification supervisory » qui devraient être revus par leurs pairs avant de pouvoir accréditer les laboratoires de façon à pouvoir garantir une parfaite homogénéité des niveaux de sécurité.

3) Renforcer le niveau de dialogue entre les représentants des entreprises de la confiance numérique et l'ENISA

La transversalité et l'évolutivité sont des caractéristiques inhérentes à la notion de cybersécurité. Aussi, la définition des mesures adéquates de cybersécurité résulte de la combinaison des plus fortes expertises en matière de cybersécurité mais aussi de celles propres au domaine à sécuriser. Cette synergie ne peut s'obtenir que par une représentation des entreprises du domaine de la confiance numérique à laquelle il est utile d'associer également les représentants du secteur à sécuriser.

Toutefois, afin de garantir une cohérence et une légitimité à ce dialogue entre les entreprises et l'ENISA, il est essentiel de s'assurer de la légitimité des parties prenantes associées au processus et de manière à s'assurer que les messages émis soient bien ceux d'une profession légitime et non les intérêts particuliers d'une entreprise ou de toute autre entité souhaitant exercer une influence dans ce domaine extrêmement stratégique qu'est la définition des exigences de cybersécurité.

L'ACN et Hexatrust se félicitent ainsi que la réglementation proposée accorde une place d'importance à la consultation des acteurs privés mais demande instamment que la participation à ces instances soit soumise à un contrôle rigoureux des interlocuteurs sollicités.

Proposition

- Soumettre les parties prenantes, représentants des entreprises, à un agrément qui pourrait être délivré par chaque autorité nationale ou par le EU Cybersecurity certification Group.

Position ACN/Hexatrust
European Cybersecurity Act
2 octobre 2017

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 CoFIS (Comité de filière des Industries de Sécurité). Par ailleurs, l'ACN est également membre fondateur de l'ECSO (European CyberSecurity Organisation).

A propos d'Hexatrust :

HEXATRUST est née de la volonté commune de PME et ETI françaises, acteurs complémentaires experts de la sécurité des systèmes d'information, de la cybersécurité et de la confiance numérique.
Editeurs et Intégrateurs de solutions innovantes représentatifs de l'excellence française, ils se sont rassemblés pour fournir une gamme de produits et de services performante, cohérente et complète de sécurisation des infrastructures critiques. Cette alliance répond aux besoins des Entreprises, des Administrations et des organisations de toutes tailles, publiques et privées, soucieuses de bénéficier d'offres innovantes d'origine française, couvrant l'ensemble de leurs besoins en matière de sécurité informatique. Forts de leur implantation sur le marché européen, les membres d'HEXATRUST souhaitent également accélérer leur développement international en partageant leur expérience, leurs réseaux et leurs moyens d'accès aux marchés mondiaux.

Alliance pour la Confiance Numérique - 17 rue de l'amiral Hamelin, 75783 Paris cedex 16 - http://www.confiance-numerique.fr
Contact : Yoann KASSIANIDES, Délégué général - Tel : 06 26 78 57 55, ykassianides@confiance-numerique.fr - SIRET : 797 543 550 00017