Agence de cybersécurité de l'UE (ENISA) et certification de cybersécurité des TIC ("Cybersecurity Act")

2017/0225(COD) - 07/06/2019 - Acte final

OBJECTIF : réformer l'actuelle Agence européenne pour la sécurité des réseaux et de l'information (ENISA) en vue de doter l'UE d'une capacité accrue en matière de cybersécurité et définir un cadre pour la mise en place d'un système européen de certification en matière cybersécurité.

ACTE LÉGISLATIF : Règlement (UE) 2019/881 du Parlement européen et du Conseil relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité).

CONTENU : en vue d'assurer le bon fonctionnement du marché intérieur tout en cherchant à atteindre un niveau élevé de cybersécurité, de cyber-résilience et de confiance au sein de l'Union, le règlement fixe:

- les objectifs, les tâches et les questions organisationnelles concernant l'ENISA (l'Agence de l' Union européenne pour la cybersécurité); et
- un cadre pour la mise en place de schémas européens de certification de cybersécurité dans le but de garantir un niveau adéquat de cybersécurité des produits TIC, services TIC et processus TIC dans l' Union, ainsi que dans le but d'éviter la fragmentation du marché intérieur pour ce qui est des schémas de certification dans l'Union.

Agence de l'Union européenne pour la cybersécurité (ENISA)

Le règlement renforce l'actuelle Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA) pour en faire un organe permanent, l'Agence de l'UE pour la cybersécurité.

L'ENISA exécutera les tâches qui lui sont assignées par le règlement dans le but de parvenir à un niveau commun élevé de cybersécurité dans l'ensemble de l'Union. Elle servira de point de référence pour les conseils et compétences en matière de cybersécurité pour les institutions, organes et organismes de l' Union ainsi que pour les autres parties prenantes concernées de l'Union.

Les tâches de l'ENISA consisteront entre autres à :

- assister les institutions, organes et organismes de l'Union, ainsi que les États membres, dans l' élaboration et la mise en œuvre des politiques de l'Union liées à la cybersécurité et à les aider à accroître la protection de leurs réseaux et systèmes d'information, à améliorer les capacités de cyber-résilience et de cyber-réaction, et à développer des aptitudes et des compétences dans le domaine de la cybersécurité ;
- soutenir la politique de l'UE en matière de certification de la cybersécurité, par exemple en jouant un rôle central dans l'élaboration des systèmes de certification ;
- promouvoir l'utilisation du nouveau système de certification, par exemple en créant un site web fournissant des informations sur les certificats ;

- favoriser la coopération, notamment le partage d’informations et la coordination au niveau de l’ Union ;
- soutenir les actions des États membres pour prévenir les cybermenaces et réagir à celles-ci, notamment en cas d’incidents transfrontières ;
- promouvoir un niveau élevé de sensibilisation des citoyens, des organisations et des entreprises aux questions liées à la cybersécurité, y compris en matière d’hygiène informatique et d’habileté numérique ;
- organiser des exercices réguliers de cybersécurité à l'échelle de l'UE, y compris un exercice global à grande échelle une fois tous les deux ans ;
- produire des analyses stratégiques à long terme des cybermenaces et des incidents afin d’identifier les tendances émergentes et contribuer à prévenir les incidents.

Le mandat prévoit aussi un réseau d'agents de liaison nationaux afin de faciliter l'échange d'informations entre l'ENISA et les États membres.

Un groupe consultatif de l’ENISA composé d’experts reconnus représentant les parties prenantes concernées, ainsi qu’un groupe des parties prenantes pour la certification de cybersécurité seront établis.

Cadre européen de certification de cybersécurité

Le règlement crée un mécanisme pour l'établissement de systèmes européens de certification de cybersécurité afin de garantir que les produits, les processus et les services TIC vendus dans les pays de l’ UE soient conformes aux normes de cybersécurité. Les certificats délivrés dans le cadre de ces systèmes seront valables dans tous les pays de l'UE.

La Commission devra publier un programme de travail de l'Union pour la certification européenne de cybersécurité qui recense les priorités stratégiques pour les futurs schémas européens de certification de cybersécurité. Elle devra tenir à jour un site internet dédié fournissant des informations sur les schémas européens de certification de cybersécurité, les certificats de cybersécurité européens et les déclarations de conformité de l'UE.

Les systèmes de certification eux-mêmes s'appuieront sur ce qui existe déjà aux niveaux international, européen et national. Les systèmes seront adoptés par la Commission et mis en œuvre et contrôlés par des autorités nationales de certification de cybersécurité.

La certification sera volontaire, sauf disposition contraire dans le droit de l'UE ou des États membres. La Commission surveillera régulièrement l'impact des systèmes de certification et évaluera leur niveau d'utilisation par les fabricants et les fournisseurs de services.

Il existera trois niveaux d'assurance différents, selon le niveau de risque associé à l'utilisation prévue du produit, à savoir «élémentaire», «substantiel» ou «élevé». Au niveau le plus élémentaire, les fabricants ou les fournisseurs de services pourront effectuer eux-mêmes l'évaluation de conformité.

Dans un souci d’équivalence des normes, dans l’ensemble de l’Union, en ce qui concerne les certificats de cybersécurité européens, les autorités nationales de certification de cybersécurité feront l’objet d’un examen par les pairs.

ENTRÉE EN VIGUEUR : 27.6.2019. Certaines dispositions s’appliqueront à partir du 28.6.2021.