Centre européen de compétences en matière de cybersécurité

2018/0328(COD) - 17/04/2019 - Texte adopté du Parlement, 1ère lecture/lecture unique

Le Parlement européen a adopté par 480 voix pour, 70 contre et 60 abstentions, une résolution législative sur la proposition de règlement du Parlement européen et du Conseil établissant le Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination.

La position du Parlement européen arrêtée en première lecture suivant la procédure législative ordinaire a modifié la proposition de la Commission comme suit :

Objectifs et missions du Centre de compétences

Le Parlement a rappelé qu'en 2017, 80 % des entreprises européennes ont été confrontées à au moins un incident de cybersécurité, d'où la nécessité d'adopter les normes les plus élevées et des solutions globales en matière de cybersécurité.

Les objectifs du règlement proposé seraient de renforcer la compétitivité et les capacités de l'Union en matière de cybersécurité, et la réduction de sa dépendance numérique en améliorant l'adoption des produits, processus et services de cybersécurité développés au sein l'Union.

Le Centre européen de compétences et le réseau de centres nationaux de coordination établis par le règlement devraient contribuer à la résilience globale et à la prise de conscience, dans l'Union, des menaces en matière de cybersécurité, en tenant compte des implications pour la société.

Les députés ont précisé les missions et tâches du Centre de compétences, à savoir notamment:

- développer les compétences et les capacités d'expertise technologique, industrielle, sociétale, universitaire et de recherche en matière de cybersécurité nécessaires pour sécuriser son marché unique numérique et renforcer la protection des données des citoyens, des entreprises et des administrations publiques de l'Union;
- contribuer à accroître la résilience et la fiabilité des infrastructures des réseaux et des systèmes d' information, y compris l'internet et les autres infrastructures critiques pour le fonctionnement de la société, telles que les transports, la santé et les systèmes bancaires ;
- développer les compétences et les capacités d'expertise technologique, industrielle, sociétale, universitaire et de recherche en matière de cybersécurité ;
- sensibiliser aux menaces en matière de cybersécurité et aux implications et préoccupations d'ordre sociétal et éthique, et réduire le déficit de compétence en matière de cybersécurité dans l'Union;
- développer le leadership européen en matière de cybersécurité en vue de garantir les normes de cybersécurité les plus élevées dans l'ensemble de l'Union;
- renforcer la confiance des citoyens, des consommateurs et des entreprises dans le monde numérique ;
- fournir un soutien financier et une assistance technique aux jeunes entreprises, aux PME, aux microentreprises, aux associations, aux experts individuels et aux projets de technologie civile dans le domaine de la cybersécurité;

- financer des contrôles des codes de sécurité des logiciels et des améliorations connexes des projets de logiciels libres et ouverts, couramment utilisés pour les infrastructures, les produits et les processus;
- faciliter le partage des connaissances en matière de cybersécurité et de l'assistance technique entre autres à la société civile, à l'industrie et aux autorités publiques, ainsi qu'à la communauté universitaire et la communauté scientifique ;
- promouvoir la «sécurité dès la conception» en tant que principe dans le processus de développement, de maintenance, d'exploitation et de mise à jour des infrastructures, des produits et des services, notamment en soutenant des méthodes de développement sûres les plus récentes, des essais de sécurité appropriés et des audits de sécurité ;
- soutenir le développement, la mise en commun et le partage des aptitudes et des compétences en matière de cybersécurité à tous les niveaux d'éducation pertinents ;
- garantir le respect des droits fondamentaux et d'un comportement éthique dans les projets de recherche sur la cybersécurité soutenus par le Centre de compétences ;
- contrôler les rapports de vulnérabilité signalés par la communauté des compétences et faciliter la divulgation de vulnérabilités, le développement et la diffusion des correctifs et des solutions ;
- soutenir la recherche dans le domaine de la cybercriminalité ainsi que le développement de produits et de processus pouvant être librement étudiés, partagés et développés ;
- apporter un soutien spécifique aux PME en facilitant leur accès sur mesure aux connaissances et à la formation ;
- renforcer la coopération entre les sphères civile et militaire en accomplissant des tâches liées à la technologie, aux applications et aux services de cyberdéfense réactive et défensive ;
- contribuer aux efforts de l'Union visant à renforcer la coopération internationale en matière de cybersécurité.

Centres nationaux de coordination

Un centre national de coordination devrait être mis en place dans chaque État membre.

Les relations entre le Centre de compétences et les centres nationaux de coordination devraient se fonder sur un accord contractuel type signé entre le Centre de compétences et chacun des centres nationaux de coordination.

Les centres nationaux devraient coopérer étroitement avec les organismes nationaux de normalisation afin de promouvoir l'adoption des normes existantes et d'associer toutes les parties prenantes concernées, en particulier les PME, à la définition de nouvelles normes. Ils devraient également servir de guichet unique pour les produits et processus financés par d'autres programmes de l'Union et diffuser un programme d' enseignement commun minimal en matière de cybersécurité.

Communauté des compétences en matière de cybersécurité

Celle-ci contribuerait à la mission du Centre de compétences et améliorerait et diffuserait l'expertise en matière de cybersécurité dans toute l'Union.

La communauté des compétences devrait se composer de la société civile, de l'industrie, tant du côté de la demande que de l'offre, y compris les PME, du monde universitaire et scientifique, d'associations d' utilisateurs, d'experts individuels, des organismes européens de normalisation concernés et d'autres associations, ainsi que d'entités publiques et d'autres entités traitant de questions opérationnelles et techniques dans le domaine de la cybersécurité.

Structure de gouvernance

Le conseil de direction se composerait d'un représentant de chaque État membre, d'un représentant nommé par le Parlement européen en tant qu'observateur, et de quatre représentants de la Commission, au nom de l'Union, et viserait la parité hommes-femmes entre les membres du conseil de direction et leurs suppléants.

Le Centre et ses organes devraient veiller à ce que les conflits d'intérêts soient non seulement identifiés, mais résolus et traités de manière transparente et responsable. Les États membres devraient veiller à ce qu' il en soit de même pour les centres nationaux de coordination.

Le comité consultatif industriel et scientifique, composé de 25 membres au maximum, conseillerait régulièrement le Centre de compétences sur l'exécution de ses activités.

Contribution financière de l'Union

Celle-ci s'élèverait à 1.780.954.875 EUR en prix de 2018 (1.998.696.000 EUR en prix courants) provenant du programme pour une Europe numérique, dont jusqu'à 21.385.465 EUR en prix de 2018 (23.746.000 EUR en prix courants) pour les coûts administratifs. Elle comprendrait également un montant du Fonds européen de la défense pour les actions liées à la défense du Centre de compétences.