Un niveau élevé commun de cybersécurité

2020/0359(COD) - 10/11/2022 - Texte adopté du Parlement, 1ère lecture/lecture unique

Le Parlement européen a adopté par 577 voix pour, 6 contre et 31 abstentions, une résolution législative sur la proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148.

La position du Parlement européen arrêtée en première lecture dans le cadre de la procédure législative ordinaire modifie la proposition comme suit:

Renforcer la cybersécurité et la résilience à l'échelle de l'UE

La directive établit des mesures qui ont pour but d'obtenir un **niveau commun élevé de cybersécurité** dans l'ensemble de l'Union, afin d'améliorer le fonctionnement du marché intérieur et d'améliorer encore la résilience et les capacités de réaction aux incidents du secteur public comme du secteur privé et de l'UE dans son ensemble. À cette fin, la présente directive fixe:

- **des obligations** qui imposent aux États membres d'adopter des stratégies nationales en matière de cybersécurité, de désigner ou de mettre en place des autorités compétentes, des autorités chargées de la gestion des cybercrises, des points de contact uniques en matière de cybersécurité et des centres de réponse aux incidents de sécurité informatique (CSIRT);

- **des mesures de gestion des risques** en matière de cybersécurité et des obligations d'information pour les entités relevant des secteurs «essentiels» comme l'énergie, les transports, la banque, les infrastructures des marchés financiers, la santé, l'eau potable, l'infrastructure numérique, les administrations publiques et le secteur de l'espace, ainsi que des secteurs «importants» comme les services postaux, la gestion des déchets, les produits chimiques, l'alimentation, la fabrication de dispositifs médicaux, l'électronique, les machines, les moteurs de véhicules et les fournisseurs numériques;

- des règles et des obligations pour le **partage d'informations** en matière de cybersécurité;

- les obligations des États membres en matière de surveillance et d'exécution.

La directive fixe les **règles minimum** d'un cadre réglementaire et ne fait pas obstacle à l'adoption ou au maintien par les États membres de dispositions assurant un niveau plus élevé de cybersécurité.

Champ d'application

Toutes **les moyennes et grandes entités** opérant dans les secteurs couverts par la directive ou fournissant des services qui en relèvent rentreront dans son champ d'application.

Les **administrations publiques** étant souvent la cible de cyberattaques, la directive s'appliquera aux entités de l'administration publique aux niveaux central et régional. En outre, les États membres pourront décider de l'appliquer également à ce type d'entités au niveau local ainsi qu'aux établissements d'enseignement, en particulier lorsqu'ils mènent des activités de recherche critiques.

La directive ne s’appliquera pas aux entités de l’administration publique qui exercent leurs activités dans les domaines de la sécurité nationale, de la sécurité publique, de la défense ou de l’application de la loi, y compris la prévention et la détection des infractions pénales, ainsi que les enquêtes et les poursuites en la matière. Les parlements et les banques centrales sont également exclus du champ d'application.

La directive comporte des dispositions supplémentaires visant à garantir la **proportionnalité**, un niveau plus élevé de gestion des risques ainsi que des **critères clairs** relatifs au caractère critique des entités afin de déterminer celles qui sont couvertes.

Coopération au niveau de l’Union

La directive définit les mécanismes d'une coopération efficace entre les autorités compétentes de chaque État membre. Elle institue un **groupe de coopération** afin de soutenir et de faciliter la coopération stratégique et l’échange d’informations entre les États membres et de renforcer la confiance. Un **réseau des CSIRT nationaux** est institué afin de contribuer au renforcement de la confiance et de promouvoir une coopération opérationnelle rapide et effective entre les États membres.

La directive instaure également officiellement le réseau européen pour la préparation et la gestion des crises de cybersécuriyé (**UE-CyCLONe**), qui soutiendra la gestion coordonnée des incidents de cybersécurité majeurs.

Mécanisme volontaire d'apprentissage par les pairs

Des évaluations par les pairs seront introduites afin de contribuer à tirer les enseignements des expériences partagées, de **renforcer la confiance mutuelle** et d’atteindre un niveau commun élevé de cybersécurité. Le groupe de coopération établira, au plus tard 2 ans après la date d’entrée en vigueur de la directive, avec l'aide de la Commission et de l’ENISA et, s’il y a lieu, du réseau des CSIRT, la méthodologie et les aspects organisationnels des évaluations par les pairs. La participation aux évaluations par les pairs s’ effectuera à titre volontaire.

Simplification des obligations de signalement

La directive rationalise les obligations en matière de signalement afin d'éviter d’engendrer un phénomène de surdéclaration et de créer une charge excessive pour les entités concernées.

Afin de simplifier la communication des informations requises en vertu de la directive et de réduire la charge administrative pesant sur les entités, les États membres devront fournir des moyens techniques, tels qu’un point d’entrée unique, des systèmes automatisés, des formulaires en ligne, des interfaces conviviales, des modèles et des plateformes dédiées à l’utilisation des entités, indépendamment du fait qu'elles relèvent ou non du champ d’application de la directive, pour la communication des informations pertinentes à transmettre.

Enfin, la directive prévoit **des voies de recours et des sanctions** pour assurer le respect de la législation.