Mesures visant à renforcer la solidarité de l'Union et ses capacités de détection, de préparation et de réaction face aux menaces et aux incidents de cybersécurité

2023/0109(COD) - 24/04/2024 - Texte adopté du Parlement, 1ère lecture/lecture unique

Le Parlement européen a adopté par 470 voix pour, 23 contre et 90 abstentions, une résolution législative sur la proposition de règlement du Parlement européen et du Conseil établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir.

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

Objectifs

Le règlement proposé établit des mesures destinées à renforcer les capacités dans l'Union afin de **détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir**, notamment par les actions suivantes:

- l'établissement d'un **réseau paneuropéen de cyberpôles** («système européen d'alerte en matière de cybersécurité») dans le but de mettre en place et de développer des capacités de détection coordonnée et d' appréciation commune de la situation;

- la mise en place d'un **mécanisme d'urgence** dans le domaine de la cybersécurité pour aider les États membres et les autres utilisateurs à se préparer aux incidents de cybersécurité importants, majeurs et assimilés à des incidents majeurs, à y réagir, à en atténuer les retombées et à s'en rétablir;

- la mise en place d'un **mécanisme européen d'analyse des incidents de cybersécurité** afin d'analyser et d'évaluer les incidents importants ou majeurs.

Le règlement poursuit les objectifs généraux consistant à renforcer la position concurrentielle des secteurs de l'industrie et des services dans l'ensemble de l'économie numérique de l'Union, y compris les microentreprises et les petites et moyennes entreprises ainsi que les jeunes pousses, et à contribuer à la souveraineté technologique et à l'autonomie stratégique ouverte de l'Union dans le domaine de la cybersécurité, notamment en stimulant l'innovation dans le marché unique numérique.

Ces objectifs seront poursuivis en **renforçant la solidarité au niveau de l'Union**, en consolidant l' écosystème de cybersécurité, en accroissant la cyberrésilience des États membres et en développant les aptitudes, le savoir-faire, les capacités et les compétences de la main-d'œuvre dans le domaine de la cybersécurité.

Le règlement est sans préjudice des fonctions essentielles des États membres, notamment celles d'assurer l'intégrité territoriale de l'État, de maintenir l'ordre public et de préserver la sécurité nationale. En particulier, la sécurité nationale reste de la seule responsabilité de chaque État membre.

Création du système européen d'alerte en matière de cybersécurité

Réseau paneuropéen d'infrastructures **composé de cyberpôles nationaux et de cyberpôles transfrontières** y adhérant sur une base volontaire, le système européen d'alerte en matière de cybersécurité sera mis en place pour soutenir le développement de capacités avancées permettant à l' Union de renforcer les capacités de détection, d'analyse et de traitement des données en rapport avec les cybermenaces et la prévention des incidents dans l'Union.

Lorsqu'un État membre décide de participer au système européen d'alerte en matière de cybersécurité, il désignera ou, le cas échéant, mettra en place un cyberpôle national. Les cyberpôles nationaux pourront coopérer avec des entités du secteur privé pour échanger des données et des informations pertinentes aux fins de la détection et de la prévention des cybermenaces et incidents, y compris avec les communautés sectorielles et transsectorielles d'entités essentielles et importantes.

Cyberpôles transfrontières.

Lorsqu'au moins trois États membres s'engagent à veiller à ce que leurs cyberpôles nationaux collaborent pour coordonner leurs activités de détection des incidents de cybersécurité et de surveillance des cybermenaces, ces États membres pourront créer un consortium d'hébergement.

Un cyberpôle transfrontière est une plateforme multinationale établie par un accord de consortium écrit. Il sera conçu pour améliorer la surveillance, la détection et l'analyse des cybermenaces, pour prévenir les incidents et pour contribuer à l'obtention de renseignements sur les cybermenaces, notamment par l' échange de données et d'informations pertinentes et, le cas échéant, anonymes, ainsi que par le partage d' outils de pointe et le développement conjoint de capacités de détection, d'analyse, de prévention et de protection des cybermenaces dans un environnement de confiance.

Mécanisme d'urgence

Un mécanisme d'urgence dans le domaine de la cybersécurité sera mis en place afin de favoriser l' amélioration de la résilience de l'Union face aux cybermenaces et d'anticiper et d'atténuer, dans un esprit de solidarité, les incidences à court terme d'incidents de cybersécurité importants, majeurs ou assimilés à des incidents majeurs.

Le mécanisme d'urgence soutiendra i) des actions de préparation, telles que des **tests coordonnés de préparation** des entités opérant dans des secteurs hautement critiques dans l'ensemble de l'Union, ii) d' autres actions de préparation pour les entités opérant dans des secteurs critiques; iii) les mesures prévues par les fournisseurs de services de sécurité gérés de confiance participant à la réserve de cybersécurité de l' Union qui soutiennent la réaction aux incidents de cybersécurité importants, majeurs ou assimilés à des incidents majeurs et permettent d'amorcer le rétablissement suite à ces incidents; iv) les actions d' assistance mutuelle, apportée sous forme de subventions et aux conditions fixées dans les programmes de travail correspondants visés au règlement établissant le programme pour une Europe numérique.

Réserve de cybersécurité de l'UE

Une réserve de cybersécurité de l'Union sera créée afin d'aider, à leur demande, les utilisateurs à réagir aux incidents de cybersécurité importants, majeurs ou assimilés à des incidents majeurs, ou à fournir une assistance à cet effet, et à entreprendre le rétablissement immédiat après de tels incidents.

L'ENISA préparera, au moins tous les deux ans, une cartographie des services nécessaires aux utilisateurs des services de la réserve de cybersécurité. Les demandes d'aide adressées à la réserve de cybersécurité de l'UE seront transmises au pouvoir adjudicateur qui les évaluera. Une réponse sera transmise aux

utilisateurs en tout état de cause, au plus tard 48 heures après la présentation de la demande afin de garantir l'efficacité de l'action de soutien. Le pouvoir adjudicateur informera le Conseil et la Commission des résultats du processus.

Un **pays tiers** associé au programme pour une Europe numérique pourra demander une aide à la réserve de cybersécurité de l'Union lorsque l'accord par lequel il est associé au programme pour une Europe numérique prévoit sa participation à la réserve.

Évaluation et réexamen

Au plus tard deux ans à compter de la date d'application du règlement et au moins tous les quatre ans par la suite, la Commission procèdera à une évaluation du fonctionnement des mesures définies dans le règlement et présentera un rapport au Parlement européen et au Conseil.