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) - 18/04/2023 - Document de base législatif

OBJECTIF : établir des mesures visant à renforcer la solidarité et les capacités de l'Union à détecter les menaces et les incidents liés à la cybersécurité, à s'y préparer et à y répondre (loi de l'UE sur la cybersolidarité).

ACTE PROPOSÉ : Règlement du Parlement européen et du Conseil.

RÔLE DU PARLEMENT EUROPÉEN : le Parlement européen décide conformément à la procédure législative ordinaire et sur un pied d'égalité avec le Conseil.

CONTEXTE : l'ampleur, la fréquence et l'impact des incidents de cybersécurité augmentent, y compris les attaques de la chaîne d'approvisionnement visant le cyberespionnage, les ransomwares ou les perturbations. Ils représentent une menace majeure pour le fonctionnement des réseaux et des systèmes d'information. Compte tenu de l'évolution rapide du paysage des menaces, la menace d'éventuels incidents à grande échelle causant des perturbations ou des dommages importants aux infrastructures critiques exige **une préparation accrue à tous les niveaux du cadre de cybersécurité de l'Union**. Cette menace va au-delà de l'agression militaire de la Russie contre l'Ukraine et devrait persister compte tenu de la multiplicité des acteurs étatiques, criminels et hacktivistes impliqués dans les tensions géopolitiques actuelles.

CONTENU : la proposition de **loi sur la cybersolidarité** vise à établir les capacités de l'UE pour rendre l' Europe plus résiliente et plus réactive face aux cybermenaces, tout en renforçant le mécanisme de coopération existant. Elle contribuera à **assurer un paysage numérique sûr et sécurisé** pour les citoyens et les entreprises et à protéger les entités critiques et les services essentiels, tels que les hôpitaux et les services publics.

Le règlement proposé établit des mesures visant à renforcer les capacités de l'Union à détecter les menaces et les incidents liés à la cybersécurité, à s'y préparer et à y répondre, notamment par les actions suivantes:

Bouclier européen de cybersécurité

Une infrastructure paneuropéenne interconnectée de centres d'opérations de sécurité (cyberbouclier européen) sera mise en place pour développer des capacités avancées permettant à l'Union de **détecter, d'analyser et de traiter les données relatives aux menaces et incidents cybernétiques dans l'Union**. Le cyberbouclier européen sera composé de centres d'opérations de sécurité (SOC) dans toute l'UE, rassemblés dans plusieurs plateformes SOC multinationales, construits avec le soutien du programme pour une Europe numérique (PED) pour compléter le financement national. Le cyberbouclier sera chargé d'améliorer la détection, l'analyse et la réponse aux cybermenaces. Ces SOC utiliseront des technologies avancées telles que l'intelligence artificielle (IA) et l'analyse de données pour détecter et partager les avertissements sur de telles menaces avec les autorités transfrontalières. Ils permettront une intervention plus rapide et plus efficace en cas de menaces majeures.

Mécanisme de cyberurgence

Le mécanisme de cyberurgence améliorera la résilience de l'Union face aux menaces majeures en matière de cybersécurité et permettra de se préparer à l'impact à court terme d'incidents de cybersécurité importants et à grande échelle et de l'atténuer, dans un esprit de solidarité. Il prévoit des actions de **soutien à la préparation**, notamment des tests coordonnés d'entités opérant dans des secteurs hautement critiques (tels que la finance, l'énergie et les soins de santé), une réponse et un rétablissement immédiat en cas d'incidents de cybersécurité importants ou à grande échelle, l'atténuation des cybermenaces importantes et des **actions d'assistance mutuelle**.

Il est également prévu de créer une **réserve européenne de cybersécurité** constituée de services de réaction aux incidents fournis par des fournisseurs de confiance sélectionnés, prêts intervenir, à la demande d'un État membre ou des institutions, organes et agences de l'Union, en cas d'incident de cybersécurité important ou de grande ampleur.

Mécanisme européen d'examen des incidents de cybersécurité

La proposition de règlement prévoit également la mise en place d'un mécanisme d'examen des incidents de cybersécurité, chargé d'évaluer et d'examiner les incidents de cybersécurité spécifiques. À la demande de la Commission ou des autorités nationales (le réseau EU-CyCLONe ou le réseau des CSIRT), l'Agence européenne de cybersécurité (ENISA) sera chargée de l'examen d'un incident de cybersécurité spécifique, important ou à grande échelle, et devra rédiger un rapport comprenant les enseignements tirés et, le cas échéant, des recommandations visant à améliorer la réponse de l'Union en matière de cybersécurité.

Implications budgétaires

Le bouclier de cybersécurité de l'UE et le mécanisme d'urgence en matière de cybersécurité du présent règlement bénéficieront d'un financement au titre de l'objectif stratégique «Cybersécurité» du programme pour une Europe numérique (PED).

Le budget total comprend une augmentation de **100 millions d'euros** que le présent règlement propose de réaffecter à partir d'autres objectifs stratégiques du programme. Cela portera le nouveau montant total disponible pour les actions de cybersécurité dans le cadre du PED à **842,8 millions d'euros**. Une partie des 100 millions d'euros supplémentaires renforcera le budget géré par les CETC pour mettre en œuvre des actions sur les SOC et la préparation dans le cadre de leur(s) programme(s) de travail. En outre, le financement supplémentaire servira à soutenir la mise en place de la réserve de cybersécurité de l'UE.

Il complète le budget déjà prévu pour des actions similaires dans le programme de travail principal du PED et du groupe de travail sur la cybersécurité pour la période 2023-2027, ce qui pourrait porter le total à 551 millions d'euros pour 2023-2027, alors que 115 millions d'euros ont déjà été consacrés sous forme de projets pilotes pour 2021-2022. En incluant les contributions des États membres, le budget global pourrait s'élever à **1,109 milliard d'euros**.