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) - 15/01/2025 - Acte final

OBJECTIF : renforcer la solidarité et les capacités dans l'UE en matière de détection, de préparation et de réaction face aux menaces et incidents de cybersécurité.

ACTE LÉGISLATIF : Règlement (UE) 2025/38 du Parlement européen et du Conseil établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les cybermenaces et incidents, de s'y préparer et d'y réagir et modifiant le règlement (UE) 2021/694 (règlement sur la cybersolidarité).

CONTENU : le présent règlement s'inscrit dans le cadre du paquet législatif sur la cybersécurité qui comprend également une modification ciblée du règlement sur la cybersécurité.

Le règlement établit des mesures destinées à renforcer les capacités dans l'Union afin de **détecter les cybermenaces et incidents, de s'y préparer et d'y réagir**. Il poursuit les objectifs généraux consistant à renforcer la position concurrentielle 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.

Le règlement établit :

1) Un système d'alerte en matière de cybersécurité

Un système européen d'alerte en matière de cybersécurité est 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. Il s' agit d'un **réseau paneuropéen d'infrastructures** composé de cyberpôles nationaux et de cyberpôles transfrontières y adhérant sur une base volontaire. Ces entités seront chargées de partager des informations et de détecter les cybermenaces et d'y réagir.

Les cyberpôles utiliseront des technologies de pointe, telles que l'intelligence artificielle (IA) et l'analyse avancée des données, pour détecter et partager en temps utile les avertissements sur les menaces et incidents de cybersécurité au niveau transfrontière. Ils renforceront le cadre européen existant, tandis que les autorités et les entités concernées, de leur côté, seront en mesure de réagir de manière plus efficiente et efficace aux incidents en matière de cybersécurité.

2) Un mécanisme d'urgence dans le domaine de la cybersécurité

Ce mécanisme d'urgence est 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 effets à court terme d' incidents de cybersécurité importants, d'incidents de cybersécurité majeurs ou d'incidents de cybersécurité assimilés à des incidents majeurs.

Le mécanisme d'urgence soutient les types de mesures suivantes:

- **des actions de préparation**, à savoir les tests de préparation coordonnés des entités actives dans des secteurs hautement critiques dans l'ensemble de l'Union pour détecter des vulnérabilités potentielles, sur la base de méthodes et de scénarios de risque communs;

- **une réserve de cybersécurité de l'Union** composée de services de réaction aux incidents fournis par le secteur privé et prêts à intervenir, à la demande d'un État membre ou des institutions, organes et agences de l'UE et des pays tiers associés, en cas d'incident de cybersécurité important ou à grande échelle. Pour bénéficier de l'aide de la réserve de cybersécurité de l'Union, les utilisateurs doivent prendre toutes les mesures appropriées pour atténuer les effets de l'incident pour lequel ils demandent de l'aide. Les demandes d'aide doivent être évaluées par le pouvoir adjudicateur. Une réponse doit être transmise aux utilisateurs sans retard et, en tout état de cause, au plus tard 48 heures après la présentation de la demande afin de garantir l'efficacité du soutien;

- **une assistance mutuelle** sur le plan technique.

3) Un mécanisme d'analyse des incidents de cybersécurité

Afin de soutenir les objectifs de promotion d'une appréciation commune de la situation et de réaction efficace aux incidents de cybersécurité importants et incidents de cybersécurité majeurs, la Commission ou le réseau européen pour la préparation et la gestion des crises cyber (EU-CyCLONe), sera en mesure de demander à l'ENISA, avec le soutien du réseau des CSIRT et avec l'approbation des États membres concernés, d'analyser et d'évaluer les cybermenaces, les vulnérabilités exploitables constatées et les mesures d'atténuation relatives à un incident de cybersécurité important ou majeur spécifique.

Après l'analyse et l'évaluation d'un incident, l'ENISA devra établir un **rapport d'analyse**, en collaboration avec l'État membre concerné, les parties prenantes concernées, notamment les représentants du secteur privé, la Commission ainsi que les autres institutions, organes ou organismes de l'Union concernés. En s'appuyant sur la collaboration avec les parties prenantes, les rapports d'analyse portant sur des incidents spécifiques serviront à évaluer les causes et les conséquences de ces incidents ainsi que leur atténuation, après qu'ils se sont produits.

ENTRÉE EN VIGUEUR : 4.2.2025.