Un niveau élevé commun de cybersécurité

2020/0359(COD) - 27/12/2022 - Acte final

OBJECTIF : renforcer la cybersécurité et la résilience dans l'ensemble de l'Union.

ACTE LÉGISLATIF : Directive (UE) 2022/2555 du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l’ensemble de l’Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2).

CONTENU : la directive établit des mesures qui ont pour but d’obtenir **un niveau commun élevé de cybersécurité** dans l’ensemble de l’Union en vue 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. La nouvelle directive, appelée «SRI 2», remplacera l'actuelle directive sur la sécurité des réseaux et des systèmes d'information (directive SRI).

Objectifs

La directive révisée a pour objectif **d'harmoniser les exigences en matière de cybersécurité** et la mise en œuvre des mesures de cybersécurité dans les différents États membres. À cette fin, elle fixe les règles minimales d'un cadre réglementaire et définit les mécanismes d'une coopération efficace entre les autorités compétentes de chaque État membre.

La directive SRI 2 constituera la base des mesures de **gestion des risques** en matière de cybersécurité et des obligations en matière de **signalement** dans tous les secteurs essentiels couverts par la directive, à savoir 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 dans les 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.

Champ d’application

La nouvelle directive SRI 2 introduit comme règle générale pour l'identification des entités réglementées **une règle associée à un plafond**. Cela signifie que 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.

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 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.

La directive comprend des dispositions supplémentaires visant à garantir **la proportionnalité**, un niveau plus élevé de gestion des risques et des **critères clairs** relatifs au caractère critique des entités pour permettre aux autorités nationales d'inclure d'autres entités.

Cadres coordonnés en matière de cybersécurité

La 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).

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

Un mécanisme volontaire d'apprentissage par les pairs renforcera la confiance mutuelle et les enseignements à tirer des bonnes pratiques et des expériences dans l'Union, contribuant ainsi à un niveau élevé commun de cybersécurité.

Le groupe de coopération établira, au plus tard le 17 janvier 2025, 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 en vue de tirer des enseignements des expériences partagées, de renforcer la confiance mutuelle, de parvenir à un niveau élevé commun de cybersécurité, ainsi que de renforcer les capacités et les politiques des États membres en matière de cybersécurité qui sont nécessaires à la mise en œuvre de la directive.

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, 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.

ENTRÉE EN VIGUEUR : 16.1.2023

TRANSPOSITION : au plus tard le 17.10.2024. Les dispositions sont applicables à partir du 18.10.2024.