Un niveau élevé commun de cybersécurité

2020/0359(COD) - 16/12/2020 - Document de base législatif

OBJECTIF : introduire des mesures visant à un niveau commun élevé de cybersécurité dans toute l'Union.

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 : la directive (UE) 2016/1148 du Parlement européen et du Conseil vise à renforcer les capacités de cybersécurité dans l'UE, à atténuer les menaces pesant sur les systèmes de réseaux et d'information utilisés pour fournir des services essentiels dans des secteurs clés et à assurer la continuité de ces services en cas d'incidents de cybersécurité, contribuant ainsi au bon fonctionnement de l'économie et de la société de l'UE.

Toutefois, depuis l'entrée en vigueur de la directive (UE) 2016/1148, des progrès significatifs ont été réalisés pour accroître le niveau de résilience de l'Union en matière de cybersécurité.

CONTENU : la présente proposition vise à remplacer la directive (UE) 2016/1148 relative à la sécurité des réseaux et des systèmes d'information (directive NIS). Il s'agit du premier acte législatif européen en matière de cybersécurité, qui prévoit des mesures juridiques visant à renforcer le niveau général de cybersécurité dans l'UE. La proposition modernise le cadre juridique existant en tenant compte de la numérisation accrue du marché intérieur au cours des dernières années et de l'évolution du paysage des menaces en matière de cybersécurité.

Champ d'application

La proposition devrait s'appliquer à certaines entités essentielles publiques ou privées opérant dans les secteurs énumérés à l'annexe I (énergie ; transports ; banques ; infrastructures des marchés financiers ; santé, eau potable ; eaux usées ; infrastructures numériques ; administration publique et espace) et à certaines entités importantes opérant dans les secteurs énumérés à l'annexe II (services postaux et de courrier ; gestion des déchets ; fabrication, production et distribution de produits chimiques ; production, transformation et distribution de denrées alimentaires ; fabrication et fournisseurs numériques).

Les micro et petites entités seraient exclues du champ d'application de la directive, à l'exception des fournisseurs de réseaux de communications électroniques ou de services de communications électroniques accessibles au public, des fournisseurs de services fiduciaires, des registres de noms de domaine de premier niveau (TLD) et de l'administration publique, ainsi que de certaines autres entités, telles que le fournisseur unique d'un service dans un État membre.

Cadres nationaux de cybersécurité

La proposition prévoit que les États membres seront tenus d'adopter une stratégie nationale de cybersécurité définissant les objectifs stratégiques et les mesures politiques et réglementaires appropriées en vue d'atteindre et de maintenir un niveau élevé de cybersécurité.

Elle établit également un cadre pour la divulgation coordonnée des vulnérabilités et exige des États membres qu'ils désignent des équipes d'intervention en cas d'incident de sécurité informatique qui agiront comme intermédiaires de confiance et faciliteront l'interaction entre les entités déclarantes et les fabricants ou fournisseurs de produits et services de technologies de l'information et de la communication (TIC).

Les États membres seraient tenus de mettre en place des cadres nationaux de gestion des crises de cybersécurité, en désignant des autorités nationales compétentes chargées de la gestion des incidents et des crises de cybersécurité à grande échelle.

Gestion des risques liés à la cybersécurité et obligations d'information

La proposition exige des États membres qu'ils prévoient que les organes de gestion de toutes les entités relevant du champ d'application approuvent les mesures de gestion des risques en matière de cybersécurité prises par les entités respectives et suivent une formation spécifique à la cybersécurité. Les entités relevant du champ d'application devraient des mesures techniques et organisationnelles appropriées et proportionnées pour gérer les risques de cybersécurité posés à la sécurité des réseaux et des systèmes d'information.

Les registres du TLD et les entités fournissant des services d'enregistrement de noms de domaine pour le TLD devraient collecter et conserver des données exactes et complètes sur l'enregistrement des noms de domaine. En outre, ces entités seraient tenues de fournir un accès efficace aux données d'enregistrement de domaine pour les demandeurs d'accès légitimes.

Compétence et enregistrement

En règle générale, les entités essentielles et importantes sont considérées comme relevant de la juridiction de l'État membre où elles fournissent leurs services. La proposition prévoit que certains types d'entités (fournisseurs de services DNS, registres de noms de TLD, fournisseurs de services d'informatique en nuage, fournisseurs de services de centres de données et fournisseurs de réseaux de diffusion de contenu, ainsi que certains fournisseurs numériques) seraient réputés relever de la juridiction de l'État membre dans lequel ils ont leur principal établissement dans l'Union.

Partage d'informations

Les États membres devraient prévoir des règles permettant aux entités de s'engager dans le partage d'informations liées à la cybersécurité dans le cadre d'accords spécifiques de partage d'informations sur la cybersécurité.

Supervision et application

Les autorités compétentes seraient tenues de superviser les entités relevant du champ d'application de la directive proposée, et notamment de veiller à ce qu'elles respectent les exigences en matière de sécurité et de notification des incidents. La proposition exige également que les États membres imposent des amendes administratives aux entités essentielles et importantes et définit certaines amendes maximales.