Niveau élevé commun de sécurité des réseaux et de l'information dans l'Union

2013/0027(COD) - 17/05/2016 - Position du Conseil

Le Conseil a adopté sa **position en première lecture** en vue de l'adoption de la directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

La directive proposée établit des mesures visant à assurer un niveau commun élevé de sécurité des réseaux et des systèmes d'information dans l'Union afin d'améliorer le fonctionnement du marché intérieur.

Les principaux éléments de la position du Conseil portent sur les points suivants :

Obligations relatives aux moyens disponibles au niveau national en matière de cybersécurité : aux termes de la position du Conseil, les États membres seraient tenus :

- d'adopter une **stratégie nationale** définissant les objectifs stratégiques et les mesures politiques et réglementaires appropriées en vue de parvenir à un niveau élevé de sécurité des réseaux et des systèmes d'information et de le maintenir ;
- de **désigner une ou plusieurs autorités nationales compétentes** en matière de sécurité des réseaux et des systèmes d'information chargées de contrôler l'application de la directive au niveau national ;
- de **désigner un guichet unique national** en matière de sécurité des réseaux et des systèmes d'information exerçant une fonction de liaison pour assurer une coopération transfrontière entre les autorités des États membres, ainsi qu'avec les autorités pertinentes des autres États membres, le groupe de coopération et le réseau des centres de réponse aux incidents de sécurité informatiques (CSIRT). Le guichet unique fournirait également au groupe de coopération un rapport annuel concernant les notifications reçues ;
- de **désigner une ou plusieurs équipes de réactions aux incidents touchant la sécurité informatique dénommées «CSIRT»**, chargées de la gestion des incidents et des risques. Le texte prévoit dans son annexe I des obligations et des tâches incombant aux CSIRT.

Coopération : pour soutenir la coopération stratégique entre les États membres, renforcer la confiance et parvenir à un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, la position du Conseil prévoit :

- **l'institution d'un groupe de coopération** composé de représentants des États membres, de la Commission et de l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA). Ce groupe se verrait confier des tâches spécifiques énumérées dans le texte, telles que l'échange de meilleures pratiques et d'informations sur un certain nombre de questions ou que l'examen des capacités et de l'état de préparation des États membres ;
- **la mise en place d'un réseau des CSIRT nationales** afin de contribuer au renforcement de la confiance entre les États membres et de promouvoir une coopération opérationnelle rapide et efficace. Le texte définit une liste de tâches imparties au réseau, telles que l'échange d'informations sur les services, les opérations et les capacités de coopération des CSIRT, le soutien aux États membres dans la gestion d'incidents transfrontières ou, dans certaines conditions, l'échange et l'évaluation d'informations liées à des incidents et aux risques correspondants.

Exigences en matière de sécurité et de notification : aux termes de la position du Conseil, la directive fixerait certaines obligations à deux types d'acteurs du marché, à savoir i) aux **opérateurs de services essentiels** et ii) aux **fournisseurs de services numériques**.

Selon une **approche différentiée**, les exigences en matière de sécurité et de notification imposées aux fournisseurs de services numériques seraient moins strictes que celles appliquées aux opérateurs de services essentiels.

Les deux types d'acteurs du marché seraient tenus de prendre des **mesures organisationnelles et techniques en vue de gérer les risques** qui menacent la sécurité des réseaux et systèmes d'information, ainsi qu'en vue de prévenir les incidents qui compromettent la sécurité de ces systèmes et d'en limiter l'impact. Par ailleurs, les incidents ayant un certain degré d'impact sur les services en question devraient être notifiés aux autorités nationales compétentes ou aux CSIRT.

Services essentiels (annexe II) : dans un certain nombre de secteurs importants d'un point de vue social et économique, dont ceux de l'énergie, des transports, de la banque, des infrastructures des marchés financiers, de la santé, de la fourniture et de la distribution d'eau potable et des infrastructures numériques, les États membres devraient identifier, sur la base de critères précis énoncés dans la directive, les opérateurs de services essentiels.

Services numériques (annexe III) : tous les fournisseurs de services numériques (à l'exception des micro et petites entreprises) offrant **trois types de services**, à savoir : i) les places de marché en ligne, ii) les moteurs de recherche en ligne et iii) les services d'informatique en nuage, devraient se conformer aux exigences de la directive.

Des entités qui n'ont pas été recensées en tant qu'opérateurs de services essentiels et qui ne sont pas des fournisseurs de services numériques pourraient notifier, à titre volontaire, certains incidents.

Transposition : les États membres devraient transposer la directive dans un délai de 21 mois à compter de sa date d'entrée en vigueur et disposeraient de 6 mois supplémentaires pour le recensement de leurs opérateurs fournissant des services essentiels.