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

2013/0027(COD) - 06/07/2016 - Acte final

OBJECTIF : assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

ACTE LÉGISLATIF : Directive (UE) 2016/1148 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.

CONTENU : la directive établit des mesures visant à **assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information (SRI) dans l'Union** afin d'améliorer le fonctionnement du marché intérieur.

Les réseaux et les services et systèmes d'information jouent un rôle crucial dans la société. Leur fiabilité et leur sécurité sont essentielles aux fonctions économiques et sociétales et notamment au fonctionnement du marché intérieur.

Or, les moyens existants ne sont pas suffisants pour assurer un niveau élevé de sécurité des réseaux et des systèmes d'information dans l'Union. Les niveaux de préparation sont très différents selon les États membres, ce qui se traduit par une fragmentation des approches dans l'Union.

Obligations relatives aux moyens disponibles au niveau national : la directive oblige les États membres à :

- adopter une **stratégie nationale** et à désigner **une autorité SRI nationale** disposant des ressources appropriées pour prévenir et gérer les risques et les incidents SRI et y apporter une réponse;
- mettre sur pied des **centres de réponse aux incidents de sécurité informatique** (CSIRT), chargés de la gestion des incidents et des risques.

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 directive 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 verra confier des tâches telles que l'échange de meilleures pratiques et d'informations sur un certain nombre de questions ou l'examen des capacités et de l'état de préparation des États membres.

Afin de contribuer au renforcement de la confiance entre les États membres et de promouvoir une coopération opérationnelle rapide et effective, **un réseau des CSIRT nationaux** sera établi.

Exigences en matière de sécurité et de notification : la directive vise à créer une **culture de gestion des risques** et à favoriser le partage d'informations entre le secteur privé et le secteur public.

Les entreprises de certains secteurs critiques ainsi que les administrations publiques seront tenues d'évaluer les risques qu'elles courent et d'adopter des mesures appropriées et proportionnées pour garantir la SRI. Ces entités auront l’obligation de signaler aux autorités compétentes tout incident qui compromet

gravement leurs réseaux et systèmes d'information et qui a un impact significatif sur la continuité des services critiques et la fourniture des biens.

L'obligation de signalement des incidents de sécurité concerne :

- **les opérateurs de services essentiels** dans des secteurs tels que les services financiers, les transports, l'énergie et la santé;
- **les fournisseurs de services numériques** 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
- **les administrations publiques** qui sont identifiées en tant qu'opérateurs de services essentiels.

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

ENTRÉE EN VIGUEUR : 8.8.2016.

TRANSPOSITION : au plus tard le 9.5.2018.

APPLICATION : à partir du 10.5.2016.