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

2013/0027(COD) - 13/03/2014 - Texte adopté du Parlement, 1ère lecture/lecture unique

Le Parlement européen a adopté par 521 voix pour, 22 contre et 25 abstentions, une résolution législative sur la proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information (SRI) dans l'Union.

La position en première lecture adoptée par le Parlement européen suivant la procédure législative ordinaire a modifié la proposition de la Commission comme suit :

Champ d'application : le projet de directive vise à imposer des obligations aux administrations publiques et aux acteurs du marché, y compris aux infrastructures critiques et aux services de la société de l'information.

Afin de veiller à la proportionnalité de l'application de la directive, le Parlement est d'avis que les mesures obligatoires prévues au chapitre IV devraient être limitées aux infrastructures qui sont critiques au sens strict. Il a donc suggéré **de ne pas inclure les services de la société de l'information** (ex : passerelles de paiement par internet, réseaux sociaux, moteurs de recherche, services informatiques en nuage etc..) dans la liste des acteurs du marché figurant à l'annexe II de la directive.

En revanche, la directive devrait être **axée sur l'infrastructure critique essentielle au maintien des fonctions économiques et sociétales vitales** dans le domaine de l'énergie, des transports, des services bancaires, des infrastructures de marchés financiers ou des soins de santé. Les développeurs de logiciels et les fabricants de matériel devraient dès lors être exclus du champ d'application de la directive.

Protection et traitement des données à caractère personnel : les députés ont insisté pour que tout traitement de données à caractère personnel dans les États membres en vertu de la directive soit réalisé dans le respect de la directive 95/46/CE et de la directive 2002/58/CE. Toute utilisation des données personnelles devrait être limitée au strict nécessaire et ces données devraient être aussi anonymes que possible, voire totalement anonymes.

Stratégies nationales : le Parlement a proposé que les États membres puissent demander à **l'Agence européenne chargée de la sécurité des réseaux et de l'information** (ENISA) de les aider à élaborer leur stratégie nationale en matière de SRI et leurs plans nationaux de coopération en matière de SRI, à partir d'un modèle minimal commun de coopération en matière de SRI.

Autorités et guichets uniques compétents au niveau national en matière de sécurité des réseaux et systèmes informatiques : les députés ont proposé de modifier la directive afin d'autoriser la désignation de **plusieurs autorités compétentes** par État membre. Toutefois, afin de garantir une application cohérente dans l'État membre et de permettre une coopération efficace et simplifiée au niveau de l'Union, chaque État membre devrait désigner un **guichet unique**. Le guichet unique assurerait, entre autres, la coopération transfrontière avec d'autres guichets uniques.

Équipes d'intervention en cas d'urgence informatique (CERT) : chaque État membre devrait mettre en place **au moins une** équipe d'intervention en cas d'urgence informatique pour chacun des secteurs définis à l'annexe II, chargée de la gestion des incidents et des risques selon un processus bien défini.

Les CERT devraient disposer de moyens humains et financiers adéquats pour participer activement aux réseaux de coopération internationaux, et en particulier au niveau de l'Union.

Les CERT seraient encouragées à initier des exercices conjoints avec d'autres CERT, avec l'ensemble des CERT des États membres et avec les institutions compétentes des pays tiers, ainsi qu'avec les CERT des institutions multinationales et internationales, telles que l'OTAN et les Nations unies, et à y participer.

Réseau de coopération : en vue de renforcer les activités du réseau de coopération, les députés ont estimé que ce dernier devrait envisager **d'inviter les acteurs du marché et les fournisseurs de solutions en matière de cybersécurité** à y participer, si nécessaire. Par ailleurs, le réseau de coopération devrait publier un rapport annuel d'activités.

Les États membres auraient la possibilité de déterminer le **niveau de criticité des acteurs du marché** en tenant compte des spécificités des secteurs et de divers paramètres.

La Commission devrait adopter, au moyen d'actes délégués, un **ensemble de critères communs d'interconnexion et de sécurité** que doivent remplir les guichets uniques pour pouvoir échanger des informations sensibles et confidentielles au sein du réseau de coopération.

Exigences de sécurité et notification d'incidents : la proposition prévoit que la Commission est habilitée à adopter des actes délégués en ce qui concerne la définition des circonstances dans lesquelles les administrations publiques et les acteurs du marché sont tenus de notifier les incidents.

Afin de clarifier la portée des obligations et de les consacrer dans l'acte de base, il est proposé de **remplacer les actes délégués par des critères clairs** permettant de déterminer l'importance des incidents à notifier. Afin de déterminer l'ampleur de l'impact d'un incident, les critères suivants devraient être pris en compte : i) le nombre d'utilisateurs dont le service essentiel est concerné ; ii) la durée de l'incident ; iii) la portée géographique eu égard à la zone touchée par l'incident.

Après avoir consulté l'autorité compétente notifiée et l'acteur du marché concerné, le guichet unique pourrait **informer le public** de chaque incident lorsqu'il juge que la sensibilisation du public est nécessaire pour prévenir un incident ou gérer un incident en cours. Les États membres devraient encourager les acteurs du marché à divulguer les incidents affectant leur activité de leur plein gré dans leurs rapports financiers.

Mise en œuvre et exécution : la proposition prévoit que les acteurs du marché se soumettent à un audit exécuté par un organisme qualifié indépendant ou une autorité nationale et mettent les résultats de cet audit à la disposition de l'autorité compétente. Le Parlement a préconisé pour sa part de **laisser une certaine flexibilité concernant la preuve de la conformité** avec les exigences imposées aux acteurs du marché en matière de sécurité, en admettant d'autres formes de preuve de la conformité que des audits de sécurité.

Les guichets uniques et les autorités chargées de la protection des données devraient mettre au point, en coopération avec l'ENISA, **des mécanismes d'échange d'informations et un formulaire unique** qui seraient utilisés pour les notifications d'incidents.

Sanctions : les députés ont proposé de préciser que lorsque les acteurs du marché ne respectent pas les obligations qui leur incombent en vertu de la directive, mais qu'ils n'ont pas agi de manière intentionnelle ou à la suite d'une négligence grave, aucune sanction ne soit imposée.