Un niveau élevé commun de cybersécurité

2020/0359(COD) - 04/11/2021 - Rapport déposé de la commission, 1ère lecture/lecture unique

La commission de l'industrie, de la recherche et de l'énergie a adopté le rapport de Bart GROOTHUIS (Renew Europe, NL) sur la proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148

La commission compétente a recommandé que la position du Parlement européen adoptée en première lecture dans le cadre de la procédure législative ordinaire modifie la proposition comme suit:

Objet et champ d'application

La directive s'appliquerait aux entités publiques et privées essentielles et importantes d'un type appelé « **entités essentielles**» à l'annexe I et «**entités importantes**» à l'annexe II, qui fournissent leurs services ou mènent leurs activités au sein de l'Union. Elle ne s'appliquerait pas aux petites entreprises ou aux microentreprises. Au plus tard 6 mois après le délai de transposition, les États membres devraient établir une **liste des entités essentielles et importantes**. Cette liste devrait être mise à jour régulièrement et au moins tous les deux ans.

Les entités essentielles et importantes devraient **soumettre au moins les informations suivantes aux autorités compétentes**: i) le nom de l'entité, ii) l'adresse et les coordonnées actualisées, y compris les adresses électroniques, iii) les plages d'IP, iv) les numéros de téléphone et v) le ou les secteurs et sous-secteurs concernés mentionnés aux annexes I et II. Les entités devraient informer les autorités compétentes de toute modification de ces informations.

À cette fin, l'Agence de l'Union européenne pour la cybersécurité (ENISA), en coopération avec le groupe de coopération, devrait publier dans les meilleurs délais des **lignes directrices** et des modèles concernant les obligations de notification. Le traitement de données à caractère personnel au titre de la directive serait effectué conformément au règlement général sur la protection des données (RGPD).

Stratégie nationale en matière de cybersécurité

Cette stratégie devrait également comprendre un cadre pour la répartition des rôles et des responsabilités des organismes et entités publics ainsi que des autres acteurs concernés, un point de contact unique en matière de cybersécurité pour les PME ainsi qu'une évaluation du niveau général de sensibilisation des citoyens à la cybersécurité.

Les États membres devraient par ailleurs adopter :

- une politique en matière de cybersécurité pour chaque secteur couvert par la directive;

- des prescriptions relatives au cryptage et l'utilisation de produits de cybersécurité à code source ouvert;

- une politique liée au maintien de la disponibilité générale et de **l'intégrité du noyau public de l' internet ouvert**, y compris la cybersécurité des câbles de communications sous-marins;

- une politique visant à promouvoir le développement et l'intégration de technologies émergentes, telles que **l'intelligence artificielle**, dans les outils et applications de renforcement de la cybersécurité;

- une politique de promotion de **l'hygiène informatique** augmentant la sensibilisation générale des citoyens aux menaces et aux meilleures pratiques en matière de cybersécurité;

- une politique de promotion de la **cyberdéfense** active;

- une politique pour aider les autorités à développer des compétences et à mieux comprendre les aspects de sécurité nécessaires pour concevoir, construire et gérer des lieux connectés;

- une politique traitant spécifiquement de la menace des **logiciels rançonneurs** et s'efforçant de désorganiser le modèle économique de ces derniers;

- une politique comprenant des procédures et des **cadres de gouvernance** pour soutenir la mise en place de partenariats public-privé en matière de cybersécurité.

L'ENISA devrait fournir des conseils aux États membres afin d'aligner les stratégies nationales de cybersécurité sur les exigences et les obligations énoncées dans la directive.

Divulgation coordonnée des vulnérabilités et base de données européenne des vulnérabilités

L'ENISA devrait élaborer et tenir à jour une base de données européenne des vulnérabilités qui exploite le registre mondial Common Vulnerabilities and Exposures (CVE). À cette fin, l'ENISA devrait adopter les mesures techniques et organisationnelles nécessaires pour assurer la sécurité et l'intégrité de la base de données.

Centres de réponse aux incidents de sécurité informatique (CSIRT)

Les États membres devraient garantir la possibilité d'un échange d'informations efficace et sécurisé à tous les niveaux de classification entre leurs propres CSIRT et les CSIRT de pays tiers au même niveau de classification. Les CSIRT devraient développer au moins les capacités techniques suivantes:

- mener une surveillance en temps réel ou quasi-réel des réseaux et des systèmes d'information, et à détecter les anomalies;

- soutenir la prévention et la détection des intrusions;

- collecter et analyser les données de police scientifique;

- filtrer le trafic malveillant;

- mettre en œuvre une authentification poussée et des privilèges et contrôles d'accès forts;

- analyser les cybermenaces.

Les CSIRT devraient assumer la surveillance des cybermenaces, des vulnérabilités et des incidents au niveau national et **l'acquisition de renseignements sur les menaces en temps réel**, la réaction aux incidents et l'assistance aux entités concernées ainsi que la contribution au déploiement d'outils de partage d'informations sécurisés.

L'ENISA devrait publier, en coopération avec la Commission, un rapport bisannuel sur l'état de la cybersécurité dans l'Union et le soumettre au Parlement européen.

Obligations en matière de communication d'informations

Les États membres devraient mettre en place un **point d'entrée unique** pour toutes les notifications requises en vertu de la directive et d'autres actes pertinents de l'Union.

Les entités essentielles et importantes devraient informer les CSIRT des incidents importants qui ont une incidence sur la disponibilité de leur service **dans les 24 heures** suivant la prise de connaissance de l' incident. Elles devront informer les CSIRT des incidents importants qui portent atteinte à la confidentialité et à l'intégrité de leurs services **dans un délai de 72 heures** à compter de la prise de connaissance de l' incident.

Amendes

Afin de garantir une application efficace des obligations prévues par la directive, chaque autorité compétente pourrait imposer ou demander l'imposition d'amendes administratives si la violation a été commise délibérément ou par négligence ou si l'entité concernée avait été informée de son infraction.