Acte législatif sur la cyber-résilience

2022/0272(COD) - 27/07/2023 - 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 Nicola DANTI (Renew, IT) sur la proposition de règlement du Parlement européen et du Conseil concernant les exigences horizontales en matière de cybersécurité applicables aux produits comportant des éléments numériques et modifiant le règlement (UE) 2019/1020.

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:

Mises à jour de sécurité

Le texte modifié indique que les fabricants doivent veiller, lorsque cela est techniquement possible, à ce que les produits comportant des éléments numériques fassent clairement la distinction entre les mises à jour de sécurité et les mises à jour de fonctionnalité. Les mises à jour de sécurité, destinées à réduire le niveau de risque ou à remédier à des vulnérabilités potentielles, devraient être **installées automatiquement**, en particulier dans le cas des produits de consommation.

Renforcer les compétences dans un environnement numérique résistant à la cybercriminalité

Les députés ont souligné l'importance des compétences professionnelles dans le domaine de la cybersécurité, en proposant des **programmes d'éducation et de formation**, des initiatives de collaboration et des stratégies visant à améliorer la mobilité de la main-d'œuvre.

Point de contact unique pour les utilisateurs

Afin de faciliter l'établissement de **rapports sur la sécurité des produits**, les fabricants devraient désigner un point de contact unique pour permettre aux utilisateurs de communiquer directement et rapidement avec eux, le cas échéant par voie électronique et d'une manière conviviale, y compris en permettant aux utilisateurs du produit de choisir le moyen de communication, qui ne devrait pas reposer uniquement sur des outils automatisés.

Les fabricants devraient rendre publiques les informations nécessaires aux utilisateurs finaux pour leur permettre d'identifier facilement leurs points de contact uniques et de communiquer avec eux.

Lignes directrices

Le texte modifié comprend des dispositions permettant à la Commission de publier des lignes directrices afin d'assurer la clarté, la certitude et la cohérence des pratiques des opérateurs économiques. La Commission devrait se concentrer sur la manière de faciliter la mise en conformité des microentreprises, des petites entreprises et des moyennes entreprises.

Procédures d'évaluation de la conformité des produits comportant des éléments numériques

Des normes harmonisées, des spécifications communes ou des systèmes européens de certification en matière de cybersécurité devraient être en place pendant six mois avant que la procédure d'évaluation de la conformité ne s'applique.

Accords de reconnaissance mutuelle (ARM)

Afin de promouvoir le commerce international, la Commission devrait s'efforcer de conclure des accords de reconnaissance mutuelle (ARM) avec les pays tiers. L'Union ne devrait établir des ARM qu'avec les pays tiers qui se trouvent à un niveau comparable de développement technique et qui ont une approche compatible en matière d'évaluation de la conformité. Les ARM devraient garantir le même niveau de protection que celui prévu par le présent règlement.

Procédure au niveau de l'UE concernant les produits comportant des éléments numériques présentant un risque important pour la cybersécurité

Lorsque la Commission a des raisons suffisantes de considérer qu'un produit comportant des éléments numériques présente un risque significatif pour la cybersécurité à la lumière de facteurs de risque non techniques, les députés ont estimé qu'elle devrait en informer les autorités de surveillance du marché concernées et adresser des recommandations ciblées aux opérateurs économiques afin de garantir la mise en place de mesures correctives appropriées.

Recettes générées par les sanctions

Les recettes générées par le paiement des sanctions devraient être utilisées pour renforcer le niveau de cybersécurité dans l'Union, notamment en développant les capacités et les compétences liées à la cybersécurité, en améliorant la cyber-résilience des opérateurs économiques, en particulier des micro-entreprises et des petites et moyennes entreprises, et plus généralement en sensibilisant le public aux questions de cybersécurité.

Évaluation et révision

Chaque année, lors de la présentation du projet de budget pour l'année suivante, la Commission devra soumettre une évaluation détaillée des tâches de l'ENISA en vertu du présent règlement telles que définies dans l'annexe VI bis et dans d’autres dispositions pertinentes du droit de l’Union et devra détailler les ressources financières et humaines nécessaires pour accomplir ces tâches.