Acte législatif sur la cyber-résilience

2022/0272(COD) - 12/03/2024 - Texte adopté du Parlement, 1ère lecture/lecture unique

Le Parlement européen a adopté par 517 voix pour, 12 contre et 78 abstentions, une résolution législative sur la proposition de règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et modifiant le règlement (UE) 2019/1020.

Le règlement s'appliquera aux produits comportant des éléments numériques mis à disposition sur le marché dont l'utilisation prévue ou raisonnablement prévisible comprend une connexion directe ou indirecte, logique ou physique, à un dispositif ou à un réseau.

La position du Parlement européen arrêtée en première lecture dans le cadre de la procédure législative ordinaire modifie la proposition comme suit:

Produits importants comportant des éléments numériques (annexe III)

Les produits de consommation qui sont catégorisés, en vertu du règlement, comme des produits importants comportant des éléments numériques devront faire l'objet d'une **procédure plus stricte d' évaluation de la conformité** par un organisme notifié. Sont concernés les produits domestiques intelligents comportant des fonctionnalités de sécurité, tels que i) les systèmes de gestion des identités et logiciels et dispositifs de gestion des accès privilégiés, dont lecteurs d'authentification et de contrôle d' accès et lecteurs biométriques; ii) les assistants virtuels polyvalents pour maison intelligente; iii) les produits domestiques intelligents dotés de fonctionnalités de sécurité, notamment serrures, caméras de sécurité, systèmes de surveillance pour bébé et systèmes d'alarme, iv) les jouets connectés ou v) les dispositifs portables personnels de santé.

La Commission pourra adopter des actes délégués pour **modifier l'annexe III** du règlement en ajoutant une nouvelle catégorie dans chaque classe de la liste des catégories de produits comportant des éléments numériques et en précisant la définition de celle-ci, en déplaçant une catégorie de produits d'une classe à l' autre ou en retirant une catégorie existante de cette liste.

Produits critiques comportant des éléments numériques (annexe IV)

Les catégories de produits critiques comportant des éléments numériques énoncées dans le règlement ont une fonctionnalité liée à la cybersécurité et remplissent une fonction qui comporte un risque important d' effets néfastes du fait de sa capacité à perturber ou endommager un grand nombre d'autres produits avec éléments numériques par le biais d'une manipulation directe.

La Commission pourra adopter des actes délégués afin de déterminer quels produits comportant des éléments numériques dont la fonctionnalité de base est celle d'une catégorie de produits qui figure à l' annexe IV du règlement doivent être tenus d'obtenir **un certificat de cybersécurité européen** au minimum au niveau d'assurance dit «substantiel» dans le cadre d'un schéma européen de certification de cybersécurité, afin de démontrer leur conformité aux exigences essentielles énoncées dans le règlement, à condition qu'un schéma européen de certification de cybersécurité couvrant ces catégories de produits ait été adopté et soit à la disposition des fabricants.

Consultation des parties intéressées

Lors de l'élaboration des mesures de mise en œuvre du règlement, la Commission devra consulter les parties intéressées, telles que les autorités des États membres concernées, les entreprises du secteur privé, y compris les microentreprises et les petites et moyennes entreprises, la communauté des logiciels ouverts, les associations de consommateurs, le milieu universitaire et les organismes et organes compétents de l' Union, ainsi que les groupes d'experts établis au niveau de l'Union.

Afin de répondre aux besoins des professionnels, les États membres, avec, le cas échéant, le soutien de la Commission, du Centre européen de compétences en matière de cybersécurité et de l'Agence de l'Union européenne pour la cybersécurité (ENISA), devront favoriser des mesures et des stratégies visant à développer des **compétences en matière de cybersécurité** et à créer des outils organisationnels et technologiques pour garantir une disponibilité suffisante de professionnels qualifiés afin de soutenir les activités des autorités de surveillance du marché et des organismes d'évaluation de la conformité.

Obligation des fabricants

Le fabricant devra procéder à une évaluation des risques de cybersécurité associés à un produit comportant des éléments numériques. L'évaluation des risques de cybersécurité doit être documentée et mise à jour selon les besoins au cours d'une **période d'assistance**. Lorsqu'il met sur le marché un produit comportant des éléments numériques, et pendant la période d'assistance, le fabricant devra veiller à ce que les vulnérabilités de ce produit, y compris de ses composants, soient gérées efficacement et conformément aux exigences essentielles. Lorsqu'il identifie une vulnérabilité dans un composant, y compris un composant logiciel ouvert, qui est intégré au produit comportant des éléments numériques, le fabricant devra **signaler la vulnérabilité** à la personne ou à l'entité qui assure la maintenance du composant, et s' attaquer et remédier à la vulnérabilité.

Le fabricant devra :

- **fixer la période d'assistance** de sorte qu'elle reflète la durée pendant laquelle le produit est censé pouvoir être utilisé, en tenant compte, en particulier, des attentes raisonnables des utilisateurs, de la nature du produit, y compris de son utilisation prévue, ainsi que du droit de l'Union applicable déterminant la durée de vie des produits comportant des éléments numériques;

- veiller à ce que **chaque mise à jour de sécurité** qui a été mise à la disposition des utilisateurs au cours de la période d'assistance, reste disponible après son émission pendant au moins 10 ans après la mise sur le marché du produit comportant des éléments numériques ou pendant le reste de la période d'assistance;

- désigner un **point de contact unique** pour permettre aux utilisateurs de communiquer directement et rapidement avec lui, notamment afin de faciliter le signalement des vulnérabilités du produit comportant des éléments numériques.

Obligations en matière de communication d'informations incombant aux fabricants

Un fabricant devra notifier toute vulnérabilité activement exploitée contenue dans le produit comportant des éléments numériques dont il prend connaissance simultanément au centre de réponse aux incidents de sécurité informatique (CSIRT) désigné comme coordinateur et à l'ENISA. Le fabricant devra soumettre i) une **alerte précoce** de vulnérabilité activement exploitée, au plus tard 24 heures après en avoir eu connaissance, ii) une **notification de vulnérabilité** au plus tard 72 heures après avoir eu connaissance de la vulnérabilité activement exploitée. Un fabricant devra également notifier tout incident grave ayant un impact sur la sécurité du produit comportant des éléments numériques.

Le fabricant mais aussi d'autres personnes physiques ou morales pourront notifier toute vulnérabilité contenue dans un produit comportant des éléments numériques ainsi que les cybermenaces susceptibles d'

affecter le profil de risque d’un produit comportant des éléments numériques, de manière **volontaire**. Afin de simplifier les obligations de signalement des fabricants, l’ENISA mettra en place une **plateforme unique de notification**.