Acte législatif sur la cyber-résilience

2022/0272(COD) - 15/09/2022 - Document de base législatif

OBJECTIF : établir des exigences horizontales en matière de cybersécurité applicables aux produits comportant des éléments numériques.

ACTE PROPOSÉ : Règlement du Parlement européen et du Conseil.

RÔLE DU PARLEMENT EUROPÉEN : le Parlement européen décide conformément à la procédure législative ordinaire et sur un pied d'égalité avec le Conseil.

CONTEXTE : les produits matériels et logiciels font de plus en plus l'objet de cyberattaques réussies, ce qui a entraîné un coût annuel mondial de la cybercriminalité estimé à 5.500 milliards d'euros en 2021. Ces produits souffrent de deux problèmes majeurs qui entraînent des coûts supplémentaires pour les utilisateurs et la société : i) un **faible niveau de cybersécurité**, reflété par des vulnérabilités généralisées et la fourniture insuffisante et incohérente de mises à jour de sécurité pour y remédier, et ii) **une compréhension et un accès insuffisants aux informations par les utilisateurs**, ce qui les empêche de choisir des produits présentant des propriétés de cybersécurité adéquates ou de les utiliser de manière sécurisée.

Dans un environnement connecté, un incident de cybersécurité sur un produit peut affecter toute une organisation ou toute une chaîne d'approvisionnement, et se propager souvent au-delà des frontières du marché intérieur en quelques minutes. Cela peut entraîner une grave perturbation des activités économiques et sociales, voire mettre des vies en danger.

Si la législation existante de l'Union s'applique à certains produits comportant des éléments numériques, il n'existe pas de cadre réglementaire horizontal de l'Union établissant des exigences complètes en matière de cybersécurité pour tous les produits comportant des éléments numériques. Il est donc nécessaire d'établir un **cadre juridique uniforme** pour les exigences essentielles en matière de cybersécurité pour la mise sur le marché de l'Union de produits comportant des éléments numériques.

CONTENU : la proposition de la Commission vise à introduire des **exigences obligatoires en matière de cybersécurité** applicables aux produits comportant des éléments numériques, sur l’ensemble de leur cycle de vie.

Objet

Fondée sur le **nouveau cadre législatif** applicable à la législation sur les produits dans l’UE, la proposition établit :

- des règles relatives à la **mise sur le marché** de produits comportant des éléments numériques afin de garantir la cybersécurité de ces produits;

- des exigences essentielles pour **la conception, le développement et la production** de produits comportant des éléments numériques, et des obligations pour les opérateurs économiques concernant ces produits en matière de cybersécurité;

- des exigences essentielles relatives aux **processus de gestion de la vulnérabilité** mis en place par les fabricants pour garantir que les produits comportant des éléments numériques sont conformes aux exigences de cybersécurité tout au long de leur cycle de vie, et des obligations incombant aux opérateurs économiques en ce qui concerne ces processus;

- des règles relatives à la **surveillance du marché** et au contrôle de l'application des règles.

Champ d'application

Le règlement proposé s'appliquerait à **tous les produits qui sont connectés directement ou indirectement à un autre appareil ou réseau**. Il ne s'appliquerait pas aux produits pour lesquels des exigences en matière de cybersécurité sont déjà définies dans des règles européennes existantes, tels que les dispositifs médicaux, l'aviation ou les voitures.

Objectifs

La proposition poursuit deux objectifs principaux visant à assurer le bon fonctionnement du marché intérieur :

- créer les conditions propices au **développement de produits sûrs** comportant des éléments numériques en veillant à ce que les produits matériels et logiciels mis sur le marché présentent moins de vulnérabilités et que les fabricants prennent la sécurité au sérieux tout au long du cycle de vie d'un produit;

- créer les conditions permettant aux **utilisateurs** de tenir compte de la cybersécurité lorsqu'ils choisissent et utilisent des produits comportant des éléments numériques.

Obligations pour les fabricants, importateurs et distributeurs

Des obligations seraient imposées aux opérateurs économiques, à partir des fabricants jusqu'aux distributeurs et aux importateurs, en ce qui concerne la mise sur le marché de produits contenant des éléments numériques, en fonction de leur rôle et de leurs responsabilités dans la chaîne d'approvisionnement.

Les **exigences et obligations essentielles en matière de cybersécurité** stipulent que tous les produits contenant des éléments numériques ne seront mis à disposition sur le marché que si, lorsqu'ils sont fournis de manière obligatoire, correctement installés, entretenus et utilisés aux fins auxquelles ils sont destinés ou dans des conditions raisonnablement prévisibles, ils satisfont aux exigences essentielles en matière de cybersécurité énoncées dans le règlement.

Les exigences et obligations essentielles **obligeraient les fabricants** à i) tenir compte de la cybersécurité dans la conception, le développement et la production des produits comportant des éléments numériques, ii) faire preuve de diligence raisonnable en ce qui concerne les aspects de sécurité lors de la conception et du développement de leurs produits, iii) faire preuve de transparence en ce qui concerne les aspects de cybersécurité qui doivent être portés à la connaissance des clients, iv) assurer un support de sécurité (mises à jour de sécurité) de manière proportionnée et v) se conformer aux exigences en matière de traitement des vulnérabilités.

Notification des organismes d'évaluation de la conformité

Le bon fonctionnement des organismes notifiés est crucial pour assurer un niveau élevé de cybersécurité et pour la confiance de toutes les parties intéressées. C'est pourquoi la proposition définit des exigences pour les autorités nationales responsables des organismes d'évaluation de la conformité (organismes

notifiés). Les États membres désigneraient une autorité notifiante qui serait chargée de mettre en place et d'appliquer les procédures nécessaires à l'évaluation et à la notification des organismes d'évaluation de la conformité et au contrôle des organismes notifiés.

Processus d'évaluation de la conformité

Les fabricants devraient se soumettre à un processus d'évaluation de la conformité pour démontrer si les exigences spécifiées relatives à un produit ont été respectées. Lorsque la conformité du produit aux exigences applicables a été démontrée, les fabricants et les développeurs établiraient une **déclaration UE de conformité** et pourraient apposer le marquage CE.

Surveillance du marché

Les États membres devraient désigner des **autorités de surveillance du marché**, qui seraient chargées de faire respecter les obligations de la loi sur la cyberrésilience.

En cas de non-conformité, les autorités de surveillance du marché pourraient exiger des opérateurs qu'ils mettent fin à la non-conformité et éliminent le risque, qu'ils interdisent ou restreignent la mise à disposition d'un produit sur le marché ou qu'ils ordonnent que le produit soit retiré ou rappelé. Chacune de ces autorités pourrait infliger des amendes aux entreprises qui ne respectent pas les règles.

Application

Afin de laisser aux fabricants, aux organismes notifiés et aux États membres le temps de s'adapter aux nouvelles exigences, le règlement proposé deviendra applicable 24 mois après son entrée en vigueur, à l'exception de l'obligation de déclaration des fabricants, qui s'appliquerait à partir de 12 mois après la date d'entrée en vigueur.