Acte législatif sur la cyber-résilience

2022/0272(COD) - 20/11/2024 - Acte final

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

ACTE LÉGISLATIF : Règlement (UE) 2024/2847 du Parlement européen et du Conseil concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) n° 168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828 (règlement sur la cyberrésilience).

CONTENU : le règlement établit:

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

- les exigences essentielles de cybersécurité relatives à la conception, au développement et à la production de produits comportant des éléments numériques, et les obligations qui incombent aux opérateurs économiques en ce qui concerne ces produits eu égard à la cybersécurité;

- les exigences essentielles de cybersécurité relatives aux processus de gestion des vulnérabilités mis en place par les fabricants pour garantir la cybersécurité des produits comportant des éléments numériques durant la période d'utilisation prévue du produit, et les obligations incombant aux opérateurs économiques en ce qui concerne ces processus;

- les règles relatives à la surveillance, y compris le contrôle, du marché et au contrôle de l'application des règles et exigences essentielles.

Champ d'application

Le règlement s'appliquera à **tous les produits qui sont directement ou indirectement connectés à un autre dispositif ou à un réseau**. Les produits de consommation qui sont catégorisés 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 notamment concernés: 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 gestionnaires de mots de passe; iii) les logiciels qui recherchent, suppriment ou mettent en quarantaine des logiciels malveillants; iv) les produits comportant des éléments numériques avec la fonction de réseau privé virtuel (VPN); v) les routeurs, modems destinés à la connexion à l'internet; vi) les assistants virtuels polyvalents pour maison intelligente; vii) les produits domestiques intelligents dotés de fonctionnalités de sécurité, notamment serrures, caméras de sécurité, systèmes de surveillance pour bébé et systèmes d' alarme, viii) les jouets connectés ou ix) les dispositifs portables personnels de santé.

Des exceptions sont prévues concernant les produits pour lesquels des exigences en matière de cybersécurité sont déjà définies dans les règles de l'UE en vigueur, par exemple les dispositifs médicaux, les produits aéronautiques et les voitures.

Consultation des parties intéressées

Lors de l'élaboration des mesures de mise en œuvre du règlement, la Commission consultera 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.

Exigences essentielles

Les fabricants devront veiller à ce que tous les produits comportant des éléments numériques soient conçus et développés conformément aux exigences essentielles de cybersécurité prévues par le règlement.

Les fabricants devront procéder à une **évaluation des risques de cybersécurité** associés à un produit comportant des éléments numériques et tenir compte des résultats de cette évaluation au cours des phases de planification, de conception, de développement, de production, de livraison et de maintenance du produit comportant des éléments numériques, en vue de réduire au minimum les risques de cybersécurité, de prévenir les incidents et d'en réduire au minimum leurs répercussions, y compris en ce qui concerne la santé et la sécurité des utilisateurs.

L'évaluation des risques de cybersécurité devra être documentée et mise à jour au cours d'une **période d' assistance**. Lorsqu'il met sur le marché un produit comportant des éléments numériques, le fabricant devra veiller à ce que les **vulnérabilités** de ce produit 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.

Les fabricants devront i) documenter systématiquement, d'une manière proportionnée à la nature et à l' ampleur des risques de cybersécurité; ii) 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; iii) désigner un point de contact unique pour permettre aux utilisateurs de communiquer directement et rapidement avec lui afin de faciliter le signalement des vulnérabilités du produit; iv) veiller à ce que les produits comportant des éléments numériques soient accompagnés des informations et des instructions destinées à l'utilisateur.

Obligations en matière de communication d'informations

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. Afin de simplifier les obligations de signalement des fabricants, l' ENISA mettra en place une plateforme unique de signalement.

Les produits logiciels et matériels porteront le **marquage «CE»** pour indiquer qu'ils satisfont aux exigences énoncées dans le règlement. Le marquage CE devra être apposé de manière visible, lisible et indélébile sur le produit comportant des éléments numériques.

Le nouveau règlement permettra ainsi aux **consommateurs** de tenir compte de la cybersécurité lorsqu'ils choisissent et utilisent des produits comportant des éléments numériques, car il leur sera plus facile d'identifier les produits matériels et logiciels dotés des caractéristiques de cybersécurité appropriées.

ENTRÉE EN VIGUEUR : 10.12.2024.

APPLICATION : à partir du 11.12.2027.