COMMISSION
EUROPÉENNE

Bruxelles, le 15.9.2022
SWD(2022) 283 final

DOCUMENT DE TRAVAIL DES SERVICES DE LA COMMISSION

RÉSUMÉ DU RAPPORT D'ANALYSE D'IMPACT

concernant la législation sur la cyberrésilience

accompagnant le document:

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

{COM(2022) 454 final} - {SEC(2022) 321 final} - {SWD(2022) 282 final}

Résumé de l'analyse d'impact (2 pages maximum)

Analyse d'impact relative au règlement sur la cyberrésilience

A. Nécessité d'une action

Quel est le problème et pourquoi se situe-t-il au niveau de l'UE?

Les produits matériels et logiciels font souvent l'objet de cyberattaques fructueuses, ce qui s'est traduit, en 2021, par un coût annuel mondial de la cybercriminalité estimé à 5 500 milliards d'EUR. Ces produits connaissent deux problèmes majeurs qui représentent des coûts supplémentaires pour les utilisateurs et la société: 1) un faible niveau de cybersécurité, reflété par des vulnérabilités généralisées et l'insuffisance et l'incohérence des mises à jour de sécurité pour y remédier, et 2) une compréhension et un accès insuffisants des utilisateurs à l'information, ce qui les empêche de choisir des produits dotés de fonctionnalités de cybersécurité adéquates ou de les utiliser de manière sécurisée.

La cybersécurité des produits comportant des éléments numériques revêt une forte dimension transfrontière, étant donné que les produits fabriqués dans un pays sont souvent utilisés dans l'ensemble du marché intérieur. En outre, les incidents affectant initialement une seule entité ou un seul État membre se propagent souvent en quelques minutes à l'ensemble du marché intérieur.

Si la législation en vigueur dans le marché intérieur s'applique à certains produits comportant des éléments numériques, la cybersécurité de la plupart des produits matériels et logiciels n'est actuellement couverte par aucune législation de l'Union. Plus particulièrement, le cadre juridique actuel de l'UE ne traite pas de la cybersécurité des logiciels non intégrés, même si les attaques de cybersécurité ciblent de plus en plus les vulnérabilités de ces produits, ce qui entraîne des coûts sociétaux et économiques importants. Parmi les exemples récents, citons le logiciel espion Pegasus, qui exploitait des vulnérabilités présentes dans les téléphones portables, ou le ver rançongiciel WannaCry, qui a touché des ordinateurs dans le monde entier en exploitant une vulnérabilité de Windows.

Quels sont les objectifs à atteindre?

Deux objectifs principaux ont été définis en vue de garantir le bon fonctionnement du marché intérieur: 1) créer les conditions pour le développement de produits comportant des éléments numériques sécurisés en faisant en sorte que les produits matériels et logiciels soient mis sur le marché avec moins de vulnérabilités et que les fabricants prennent la sécurité au sérieux tout au long du cycle de vie d'un produit; et 2) créer les conditions permettant aux utilisateurs de prendre en considération la cybersécurité lorsqu'ils sélectionnent et utilisent des produits comportant des éléments numériques. Quatre objectifs spécifiques ont été fixés: i) faire en sorte que les fabricants améliorent la sécurité des produits comportant des éléments numériques dès la phase de conception et de développement et tout au long du cycle de vie; ii) assurer un cadre cohérent en matière de cybersécurité, facilitant la mise en conformité pour les producteurs de matériel et de logiciels; iii) améliorer la transparence des propriétés de sécurité des produits comportant des éléments numériques; et iv) permettre aux entreprises et aux consommateurs d'utiliser les produits comportant des éléments numériques en toute sécurité.

Quelle est la valeur ajoutée de l'action au niveau de l'UE (subsidiarité)?

La forte nature transfrontière de la cybersécurité et le nombre croissant d'incidents ayant des retombées transfrontières, intersectorielles et sur d'autres produits signifient que les objectifs ne peuvent pas être atteints efficacement par les seuls États membres. Compte tenu du caractère mondial des marchés de produits comportant des éléments numériques, les États membres sont confrontés, sur leur territoire, aux mêmes risques pour un même produit. L'émergence d'un cadre fragmenté de règles nationales

potentiellement divergentes risque d'entraver la création d'un marché unique ouvert et concurrentiel pour les produits comportant des éléments numériques. Une action commune au niveau de l'UE est donc nécessaire pour accroître la confiance des utilisateurs et renforcer l'attractivité des produits comportant des éléments numériques sur le marché de l'Union. Elle profiterait également au marché intérieur en assurant la sécurité juridique et en créant des conditions de concurrence équitables pour les fabricants de produits comportant des éléments numériques.

B. Les solutions

Quelles sont les différentes options pour atteindre les objectifs? Y a-t-il une option privilégiée? Si tel n'est pas le cas, pourquoi?

Quatre options stratégiques et leurs sous-options, allant plus loin que le statu quo, ont été analysées: 1) une approche non contraignante et des mesures volontaires; 2) une intervention réglementaire ad hoc, propre au produit, concernant la cybersécurité des produits matériels comportant des éléments numériques et de leurs logiciels intégrés: 3) une approche mixte, comprenant des règles horizontales contraignantes pour la cybersécurité des produits matériels comportant des éléments numériques et leurs logiciels intégrés et une approche graduelle pour les logiciels non intégrés, avec deux sous-options concernant l'évaluation de la conformité; et 4) une intervention réglementaire horizontale introduisant des exigences de cybersécurité pour un large éventail de produits comportant des éléments numériques, dont les logiciels non intégrés, assortie de sous-options concernant le champ d'application et l'évaluation de la conformité.

L'analyse d'impact a conclu que l'**option à privilégier** est l'option nº 4, qui couvre tous les produits comportant des éléments numériques et prévoit une évaluation obligatoire par un tiers pour les produits critiques, à la lumière de l'évaluation de l'efficacité par rapport aux objectifs spécifiques recherchés, de l'efficacité coûts-bénéfices et de la cohérence.

Quelles sont les positions des différentes parties prenantes? Qui soutient quelle option?

Interrogés sur l'efficacité des interventions envisagées, les répondants à la consultation publique se sont accordés à dire que l'option nº 4 serait la plus efficace (4,08 sur une échelle de 1 à 5). Parmi ces répondants figuraient des organisations de consommateurs (5,00), des personnes se présentant comme utilisateurs (4,22), des organismes notifiés (4,17), des autorités de surveillance du marché (5,00) et des fabricants de produits comportant des éléments numériques (3,85), dont des PME (4,05).

C. Incidences de l'option privilégiée

Quels sont les avantages de l'option privilégiée (le cas échéant; à défaut, des options principales)?

L'option privilégiée présenterait des avantages significatifs pour les différentes parties prenantes. Du point de vue des entreprises, elle permettrait d'éviter l'application de règles de sécurité divergentes aux produits comportant des éléments numériques et de réduire les coûts de conformité à la législation en matière de cybersécurité. Elle diminuerait le nombre de cyberincidents, les coûts liés à la gestion de ces incidents et les atteintes à la réputation des entreprises. Pour l'ensemble de l'UE, la réduction des coûts liés aux incidents affectant les entreprises serait de quelque 180 à 290 milliards d'EUR par an. Qui plus est, cette initiative entraînerait une hausse du chiffre d'affaires des entreprises, grâce à l'augmentation de la demande en produits comportant des éléments numériques. Elle améliorerait en outre la réputation mondiale des entreprises, avec, à la clé, un accroissement de la demande en dehors de l'UE. Du point de vue des utilisateurs finals, l'option privilégiée augmenterait la transparence des propriétés de sécurité des produits et faciliterait l'utilisation des produits comportant des éléments numériques. Les consommateurs et les citoyens bénéficieraient également d'une meilleure protection de leurs droits fondamentaux, tels que

les droits à la vie privée et à la protection des données.
Quels sont les coûts de l'option privilégiée (ou, à défaut, des options principales)?
L'option privilégiée engendrerait des coûts de mise en conformité et de mise en application pour les entreprises, les organismes notifiés et les autorités publiques, en ce compris les autorités notifiantes, d'accréditation et de surveillance du marché. Pour les développeurs de logiciels et les fabricants de matériel, elle viendra ajouter des coûts de mise en conformité directs liés aux nouvelles exigences de cybersécurité, à l'évaluation de la conformité, aux obligations de documentation et de signalement, portant potentiellement les coûts de mise en conformité globaux à quelque 29 milliards d'EUR pour une valeur de marché estimée à 1 485 milliards d'EUR en chiffre d'affaires. Les utilisateurs finals, en ce compris les entreprises, les consommateurs et les citoyens, pourraient être confrontés à des prix plus élevés pour les produits comportant des éléments numériques. Toutefois, ces coûts sont à considérer dans le contexte des avantages significatifs décrits ci-dessus. Pour les organismes notifiés, les coûts supplémentaires devraient être compensés par une augmentation du chiffre d'affaires.
Quelles sont les incidences sur les PME et la compétitivité?
Les PME seront touchées par les nouvelles exigences à la fois en tant que fabricants et en tant qu'utilisateurs finals. S'agissant des coûts de mise en conformité, les PME seraient en principe plus touchées que les grandes entreprises. Ces dernières bénéficient en effet généralement de meilleures économies d'échelle et sont davantage sensibilisées à la cybersécurité. Toutefois, les PME auraient tout à gagner de cette initiative, car l'intégration de la cybersécurité dans les produits comportant des éléments numériques représenterait des économies significatives pour elles en tant qu'utilisatrices. En tant que fabricants, les PME bénéficieraient d'une plus grande confiance des utilisateurs finals et attireraient de nouveaux clients. Un accès fluide au marché intérieur et une réduction de la fragmentation du marché peuvent se révéler encore plus bénéfiques pour les PME, moins bien dotées pour faire face aux différentes exigences réglementaires. Tout en soulignant la nécessité d'une approche proportionnée et de mesures de soutien, les PME se sont généralement déclarées favorables à des conditions de concurrence équitables entre toutes les entreprises et n'estimaient pas être désavantagées par rapport aux grandes entreprises dans un scénario d'exigences obligatoires horizontales.
Y aura-t-il une incidence notable sur les budgets nationaux et les administrations nationales?
L'initiative aura une incidence sur les autorités nationales, telles que les autorités notifiantes, les autorités d'accréditation et les autorités de surveillance du marché chargées de surveiller et de faire appliquer les mesures proposées. Ces autorités prendront en charge les ajustements supplémentaires (par exemple, formation et ressources humaines) et les coûts de mise en application afin de tenir compte des nouvelles exigences. Les ressources dépensées par les organismes d'accréditation sont toutefois compensées et en grande partie supportées par les organismes d'évaluation de la conformité, par l'achat de services d'accréditation.
Y aura-t-il d'autres incidences notables?
Aucune autre incidence négative significative n'est attendue. L'option privilégiée contribuerait à réduire le nombre et la gravité des incidents, y compris les violations de données à caractère personnel, et aurait des effets sociaux positifs tels que la réduction de la cybercriminalité. La demande de professionnels de la sécurité est susceptible d'augmenter, et l'asymétrie des informations en matière de cybersécurité serait réduite.
Proportionnalité?

L’option privilégiée ne va pas au-delà de ce qui est nécessaire pour réaliser les objectifs spécifiques de manière satisfaisante. L’intervention garantirait que les produits comportant des éléments numériques sont sécurisés tout au long de leur cycle de vie et proportionnellement aux risques encourus.
D. Suivi
Quand la législation sera-t-elle réexaminée?
Au plus tard [36 mois] après la date d’application de l'initiative et tous les quatre ans par la suite, la Commission présente au Parlement européen et au Conseil un rapport sur l’évaluation et le réexamen de l'initiative.