COMMISSION
EUROPÉENNE

Bruxelles, le 16.12.2020
SWD(2020) 344 final

DOCUMENT DE TRAVAIL DES SERVICES DE LA COMMISSION

RÉSUMÉ DU RAPPORT D'ANALYSE D'IMPACT

accompagnant le document:

PROPOSITION DE DIRECTIVE DU PARLEMENT EUROPÉEN ET DU CONSEIL

concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148

{COM(2020) 823 final} - {SEC(2020) 430 final} - {SWD(2020) 345 final}

Résumé de l'analyse d'impact

Analyse d'impact du *réexamen de la directive (UE) 2016/1148 du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (ci-après la «directive SRI»)*

A. Nécessité d'une action

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

Malgré des accomplissements notables, la directive SRI, qui a ouvert la voie à une évolution importante des mentalités ainsi que de l'approche institutionnelle et réglementaire de la cybersécurité dans de nombreux États membres, a désormais également montré ses limites. La transformation numérique de la société (intensifiée par la crise de la COVID-19) a étendu le paysage des menaces et apporte de nouveaux défis qui nécessitent des réponses adaptées et novatrices. Le nombre de cyberattaques continue d'augmenter, les attaques sont de plus en plus sophistiquées et proviennent d'un large éventail de sources à l'intérieur et à l'extérieur de l'Union.

À la lumière de l'évaluation du fonctionnement de la directive SRI, l'analyse d'impact a relevé les problèmes suivants: le faible niveau de cyber-résilience des entreprises actives dans l'Union; la résilience inégale en fonction des États membres et des secteurs concernés ainsi que le faible niveau de prise de conscience conjointe de la situation et l'absence de réponse conjointe à la crise. Par exemple, en raison de certains de ces problèmes et facteurs, il existe des situations où certains grands hôpitaux d'un État membre ne relèvent pas du champ d'application de la directive SRI et ne sont donc pas tenus de mettre en œuvre les mesures de sécurité qui en découlent, tandis que dans un autre État membre, la quasi-totalité des hôpitaux du pays sont couverts par les exigences de cette directive en matière de sécurité.

Quels sont les objectifs à atteindre?

Trois objectifs généraux sont envisagés dans le cadre du réexamen de la directive SRI:

1. **relever le niveau de cyber-résilience d'un ensemble exhaustif d'entreprises opérant dans l'Union européenne dans tous les secteurs concernés,** en mettant en place des règles garantissant que toutes les entités publiques et privées du marché intérieur qui exercent des fonctions importantes dans l'économie et la société dans son ensemble soient tenues de prendre des mesures de cybersécurité adéquates;
2. **réduire les incohérences en matière de résilience dans l'ensemble du marché intérieur dans les secteurs déjà couverts par la directive,** en alignant davantage 1) le champ d'application de fait, 2) les exigences en matière de sécurité et de signalement des incidents, 3) les dispositions régissant la surveillance et l'exécution au niveau national et 4) les capacités des autorités compétentes dans les États membres;
3. **améliorer le niveau de connaissance situationnelle conjointe et la capacité collective à se préparer et à réagir**, en prenant des mesures pour renforcer le niveau de confiance entre les autorités compétentes, en partageant davantage d'informations et en établissant des règles et des procédures à suivre en cas d'incidents ou de crises majeurs.

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

La résilience en matière de cybersécurité dans l'ensemble de l'Union ne peut être effective si elle est appréhendée de manière disparate sous l'effet de cloisonnements nationaux ou régionaux. La directive SRI est venue combler cette lacune en établissant un cadre pour la sécurité des réseaux et des systèmes

d'information au niveau national et au niveau de l'Union. Cependant, sa transposition et sa mise en œuvre ont également fait ressortir les insuffisances intrinsèques de certaines dispositions ou approches, telles que la délimitation peu claire de son champ d'application. De plus, avec la crise de la COVID-19, l'économie européenne dépend plus que jamais des réseaux et systèmes d'information et les secteurs et les services sont de plus en plus interconnectés. Le premier réexamen périodique de la directive SRI a donc offert la possibilité d'approfondir l'action de l'Union. Une intervention de l'Union allant au-delà des mesures actuelles de la directive SRI se justifie principalement par: i) la nature transfrontière du problème; ii) le potentiel de l'action de l'Union pour améliorer et permettre des politiques nationales efficaces; iii) la contribution de mesures stratégiques concertées et collaboratives en matière de SRI à la protection efficace des données et de la vie privée.

B. 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?

L'analyse d'impact a examiné quatre options envisageables: 0) maintien du statu quo; 1) mesures non législatives destinées à aligner la transposition; 2) modifications limitées de la directive SRI pour renforcer l'harmonisation; 3) modifications systémiques et structurelles de la directive SRI. L'option 1 a été rejetée à un stade précoce, car elle ne s'éloignait pas beaucoup du statu quo. L'analyse d'impact a conclu que l'**option privilégiée** était l'option 3 (c'est-à-dire les **modifications systémiques et structurelles du cadre SRI**), étant donné qu'elle prévoirait un changement d'approche plus fondamental consistant à couvrir une portion plus large des économies de l'Union, en établissant cependant une surveillance plus ciblée visant les grandes entreprises et les entreprises clés, tout en déterminant clairement le champ d'application. Par ailleurs, elle rationaliserait et harmoniserait davantage les obligations liées à la sécurité pour les entreprises, créerait un cadre plus efficace pour les aspects opérationnels, créerait une base claire pour les responsabilités partagées et l'obligation de rendre compte des acteurs concernés et encouragerait le partage des informations.

Quelle est la position des différentes parties intéressées? Qui soutient quelle option?

La majorité des autorités compétentes et des entreprises se sont montrées favorables à une révision de la directive SRI. Au cours de plusieurs consultations, elles ont signalé qu'une directive SRI révisée devrait couvrir des secteurs et sous-secteurs supplémentaires, ainsi qu'aligner ou rationaliser davantage les mesures de sécurité et les obligations de signalement. Les parties prenantes se sont également montrées favorables à de nouveaux concepts ou à des mesures stratégiques qui ne figurent que dans l'option privilégiée (par exemple, politiques de sécurité relatives à la chaîne d'approvisionnement, institutionnalisation d'un cadre opérationnel de gestion de crise au niveau de l'Union).

C. Incidences de l'option privilégiée

Quels sont les avantages de l'option privilégiée (ou, à défaut, des options principales)?

L'option privilégiée apporterait des avantages considérables: les estimations réalisées sur la base d'une modélisation économique élaborée par une étude d'appui pour le réexamen de la directive SRI indiquent que l'option privilégiée pourrait entraîner une diminution du coût des incidents de cybersécurité de 11,3 milliards d'EUR.

Le champ d'application sectoriel serait considérablement élargi en vertu du cadre SRI, mais à côté des avantages susmentionnés, la charge que les exigences en matière de SRI pourraient créer, notamment du point de vue de la surveillance, serait également équilibrée tant pour les nouvelles entités qui seront

couvertes que pour les autorités compétentes. En effet, le nouveau cadre SRI établirait une approche à deux niveaux, mettant l'accent sur les grandes entités et les entités clés et sur une différenciation du régime de contrôle qui ne permettrait qu'une surveillance ex post (c'est-à-dire réactive et sans obligation générale de documenter systématiquement le respect des exigences) pour un grand nombre de ces entités, notamment celles considérées comme «importantes» mais non «essentielles».

Dans l'ensemble, l'option stratégique privilégiée entraînerait des compromis et des synergies efficaces, le potentiel de toutes les options stratégiques étant analysé pour garantir un niveau accru et cohérent de cyber-résilience des entités clés dans l'ensemble de l'Union, ce qui engendrerait à terme des économies tant pour les entreprises que pour la société.

Quels sont les coûts de l'option privilégiée (le cas échéant, sinon des options principales)?

L'option stratégique privilégiée entraînerait également certains coûts de mise en conformité et d'exécution pour les autorités compétentes des États membres (une augmentation globale d'environ 20 à 30 % des ressources a été estimée). Cependant, le nouveau cadre apporterait également des avantages substantiels grâce à une meilleure vue d'ensemble des entreprises clés et à une meilleure interaction avec celles-ci, à un renforcement de la coopération opérationnelle transfrontière, ainsi qu'à des mécanismes d'assistance mutuelle et d'examen par les pairs. Cela entraînerait une augmentation globale des capacités dans le domaine de la cybersécurité dans l'ensemble des États membres.

Selon les estimations, les entreprises qui relèveraient du cadre SRI devraient augmenter leurs dépenses actuelles consacrées à la sécurité des TIC de 22 % maximum au cours des premières années suivant l'introduction du nouveau cadre SRI (12 % pour les entreprises qui relèvent déjà du champ d'application de la directive SRI actuelle). Cependant, cette augmentation moyenne des dépenses consacrées à la sécurité des TIC donnerait lieu à des avantages proportionnels liés à ces investissements, en raison notamment d'une réduction considérable des coûts des incidents de cybersécurité (estimée à 11,3 milliards d'EUR sur dix ans).

Quelles sont les incidences sur les PME et la compétitivité?

L'option privilégiée prévoit d'exclure les micro et petites entreprises du champ d'application du cadre SRI. Pour les moyennes entreprises, on peut s'attendre à une augmentation des dépenses consacrées à la sécurité des TIC au cours des premières années suivant l'introduction du nouveau cadre SRI. En parallèle, le relèvement du niveau d'exigences de sécurité pour ces entités encouragerait également le renforcement de leurs capacités dans le domaine de la cybersécurité et contribuerait à améliorer leur gestion des risques liés aux TIC.

Y aura-t-il une incidence notable sur les budgets nationaux et les administrations nationales?

Il y aurait une incidence sur les budgets nationaux et les administrations nationales: une augmentation des ressources d'environ 20 à 30 % est prévue à court et moyen terme.

Y aura-t-il d'autres incidences notables?

Aucune autre incidence négative significative n'est attendue. L'option stratégique privilégiée devrait entraîner un renforcement des capacités dans le domaine de la cybersécurité et, par conséquent, elle devrait permettre d'atténuer davantage le nombre et la gravité des incidents, y compris les violations des données. Elle est également susceptible d'avoir une incidence positive sur la mise en place de conditions de concurrence équitables dans l'ensemble des États membres pour toutes les entités relevant du champ d'application du cadre SRI et de réduire les disparités en matière d'information sur la cybersécurité.

Proportionnalité?
L'option privilégiée ne va pas au-delà de ce qui est nécessaire pour réaliser les objectifs spécifiques de manière satisfaisante. L'alignement et la rationalisation envisagés des mesures de sécurité et des obligations d'information sont liés aux demandes formulées par les États membres et les entreprises concernant l'amélioration du cadre actuel.
D. Suivi
Quand la législation sera-t-elle réexaminée?
Le premier réexamen aurait lieu 54 mois après l'entrée en vigueur de l'instrument juridique. La Commission présenterait un rapport au Parlement européen et au Conseil sur son réexamen. Le réexamen serait préparé avec le soutien de l'ENISA et du groupe de coopération.