COMMISSION
EUROPÉENNE

Bruxelles, le 4.10.2017
COM(2017) 476 final

NOTE
This language version reflects the corrections done to the original EN version transmitted under COM(2017) 476 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 476 final/2 of 4.10.2017

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

Exploiter tout le potentiel de la directive SRI – Vers la mise en œuvre effective de la directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union

FR

Introduction

La directive (UE) 2016/1148 relative à la sécurité des réseaux et des systèmes d'information dans l'Union[1] (ci-après la «directive SRI» ou la «directive»), adoptée le 6 juillet 2016, est la première législation horizontale de l'Union européenne qui aborde les défis liés à la cybersécurité et introduit un véritable changement de paradigme en ce qui concerne la résilience et la coopération en matière de cybersécurité en Europe.

Elle comporte trois objectifs principaux:

- améliorer les capacités nationales en matière de cybersécurité;
- renforcer la coopération au niveau de l'Union européenne; et
- promouvoir une culture de la gestion des risques et du signalement des incidents parmi les principaux acteurs économiques, notamment les opérateurs de services essentiels (OSE), pour le maintien des activités économiques et sociétales, et les fournisseurs de service numérique (FSN).

La directive SRI est une pierre angulaire de la réponse apportée par l'Union aux menaces et défis cybernétiques croissants qui accompagnent la numérisation de notre vie économique et sociale; c'est pourquoi sa mise en œuvre est une composante essentielle du paquet «cybersécurité» présenté le 13 septembre 2017. L'efficacité de la réponse de l'Union européenne sera limitée tant que la directive SRI ne sera pas pleinement transposée dans tous les États membres de l'Union. Cela a également été reconnu comme un point critique dans la communication de la Commission de 2016 sur le renforcement du système européen de cyber-résilience[2].

Le caractère novateur de la directive SRI et la nécessité d'une réaction urgente face à des cybermenaces en évolution rapide justifient d'accorder une attention particulière aux difficultés auxquelles sont confrontés tous les acteurs lorsqu'il s'agit d'assurer une transposition rapide et réussie de la directive. Compte tenu du délai de transposition fixé au 9 mai 2018 et de la date limite du 9 novembre 2018 déterminée pour l'identification des opérateurs de services essentiels, la Commission soutient le processus de transposition des États membres et les travaux qu'ils mènent au sein du groupe de coopération à cette fin.

La présente communication, accompagnée de son annexe, se fonde sur les travaux préparatoires de la Commission et son analyse de la mise en œuvre de la directive SRI à ce jour, sur les contributions de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) et sur les discussions qui ont eu lieu avec les États membres au cours de la phase de transposition de la directive, notamment au sein du groupe de coopération[3]. La

[1] Directive (UE) 2016/1148 du Parlement européen et du Conseil 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. La directive est entrée en vigueur le 8 août 2016.
[2] COM(2016) 410 final.
[3] Un mécanisme de coopération stratégique entre les États membres au titre de l'article 11 de la directive SRI.

présente communication complète les efforts considérables consentis jusqu'à présent, en particulier par les moyens suivants:

- Les travaux intensifs du groupe de coopération, qui est convenu d'un plan de travail axé principalement sur la transposition de la directive SRI, et en particulier sur la question de l'identification des opérateurs de services essentiels et de leurs obligations en matière d'exigences de sécurité et de notification des incidents. Alors que la directive prévoit une marge d'appréciation dans la transposition des dispositions relatives aux opérateurs de services essentiels, les États membres ont reconnu l'importance d'une approche harmonisée à cet égard[4].
- La mise en place et le fonctionnement rapide du réseau composé de centres de réponse aux incidents de sécurité informatique (CSIRT), conformément à l'article 12, paragraphe 1, de la directive. Depuis lors, ce réseau a commencé à jeter les bases d'une coopération opérationnelle structurée au niveau européen.

Sur les plans tant politique qu'opérationnel représentés par ces deux structures, l'engagement total de tous les États membres est essentiel pour atteindre l'objectif d'un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

La présente communication, accompagnée de son annexe, consolidera ces efforts en rassemblant et en comparant les bonnes pratiques des États membres qui sont pertinentes pour la mise en œuvre de la directive, en formulant de nouvelles orientations sur la manière dont la directive devrait être mise en œuvre et en fournissant des explications plus détaillées sur des dispositions spécifiques. L'objectif général est d'aider les États membres à parvenir à une mise en œuvre efficace et harmonisée de la directive SRI dans l'ensemble de l'Union européenne.

La présente communication sera également complétée par le futur règlement d'application de la Commission sur les spécifications supplémentaires des éléments et paramètres relatifs aux exigences en matière de sécurité et de notification des incidents applicables aux fournisseurs de service numérique, conformément à l'article 16, paragraphe 8, de la directive SRI. Le règlement d'application facilitera la mise en œuvre de la directive en ce qui concerne les obligations des fournisseurs de service numérique[5].

La communication présente les principales conclusions de l'analyse des questions considérées comme des thèmes de référence importants et une source d'inspiration potentielle du point de vue de la transposition en droit national. L'accent est principalement mis ici sur les dispositions relatives aux capacités et obligations des États membres concernant les entités

[4] Le groupe de coopération travaille actuellement sur des documents d'orientation de référence concernant entre autres: les critères définissant le caractère critique d'un opérateur conformément à l'article 5, paragraphe 2, de la directive; les circonstances dans lesquelles les opérateurs de services essentiels sont tenus de notifier les incidents sur la base de l'article 14, paragraphe 7, de la directive; et les exigences de sécurité applicables aux opérateurs de services essentiels, conformément à l'article 14, paragraphes 1 et 2.

[5] Le projet de règlement d'application est actuellement consultable par le public à l'adresse: https://ec.europa.eu/info/law/better-regulation/have-your-say_fr

qui relèvent du champ d'application de la directive. L'annexe fournit un examen plus détaillé des domaines dans lesquels la Commission estime qu'il est le plus utile de fournir des orientations pratiques en matière de transposition en explicitant et en interprétant certaines dispositions de la directive, ainsi qu'en décrivant de bonnes pratiques et l'expérience acquise jusqu'à présent.

Vers une mise en œuvre effective de la directive SRI

L'objectif de la directive SRI est d'atteindre un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union. Il faut, autrement dit, accroître la sécurité de l'internet et des réseaux et systèmes informatiques privés sur lesquels reposent les services dont dépend le fonctionnement de notre société et de nos économies. Le premier élément important à cet égard est l'état de préparation des États membres, qui devrait être assuré par la mise en place de stratégies nationales de cybersécurité, telles que décrites dans la directive, par les travaux des CSIRT et par ceux des autorités nationales compétentes.

Exhaustivité des stratégies nationales

Il est important que les États membres profitent du processus de transposition de la directive SRI pour revoir leur stratégie nationale en matière de cybersécurité à la lumière des lacunes, des bonnes pratiques et des nouveaux défis traités en annexe.

Bien que la directive se concentre naturellement sur les entreprises et les services qui revêtent une importance critique particulière, c'est la cybersécurité de l'économie et de la société dans son ensemble qui doit être abordée de manière globale et cohérente, étant donné le recours toujours plus fréquent aux TIC. Par conséquent, l'adoption de stratégies nationales globales allant au-delà des exigences minimales de la directive SRI (c'est-à-dire couvrant plus que les secteurs et les services énumérés, respectivement, aux annexes II et III de la directive) augmenterait le niveau global de sécurité des réseaux et des systèmes d'information.

Dans la mesure où la cybersécurité est un domaine des politiques publiques encore relativement nouveau et en pleine expansion, de nouveaux investissements sont nécessaires dans la plupart des cas, même si la situation générale des finances publiques exige des réductions et des économies. La prise de décisions ambitieuses visant à garantir des ressources financières et humaines adéquates, indispensables à la mise en œuvre effective des stratégies nationales, y compris l'affectation de ressources suffisantes aux autorités nationales compétentes et aux CSIRT, est donc fondamentale pour la réalisation des objectifs de la directive.

Efficacité de la mise en œuvre et de l'application.

La nécessité de désigner des autorités nationales compétentes et des points de contact uniques est soulignée à l'article 8 de la directive et constitue un élément essentiel pour garantir une mise en œuvre de la directive SRI et une coopération transfrontalière efficaces. À cet égard, des approches tantôt centralisées, tantôt décentralisées ont vu le jour dans les États membres. Lorsque les États membres adoptent une approche plus décentralisée en ce qui concerne la

désignation des autorités nationales compétentes, il s'avère essentiel d'assurer une coopération étroite entre de nombreuses autorités et le point de contact unique (*voir tableau 1 de la section 3.2 de l'annexe*). Cela augmenterait l'efficacité de la mise en œuvre et faciliterait l'application.

Sur la base de l'expérience acquise dans le domaine de la protection des infrastructures d'information critiques (PIIC), il est possible d'élaborer un modèle optimal de gouvernance pour les États membres, garantissant à la fois une mise en œuvre sectorielle efficace de la directive SRI et une approche horizontale cohérente (*voir la section 3.1 de l'annexe*).

Renforcement des capacités des CSIRT nationaux

Faute de CSIRT nationaux efficaces et dotés de ressources suffisantes dans toute l'Union, comme le prévoit l'article 9 de la directive SRI, l'Union européenne restera trop vulnérable face aux menaces cybernétiques transfrontalières. Les États membres pourraient donc envisager d'étendre les compétences des CSIRT au-delà des secteurs et services couverts par la directive (*voir les sections 3.3 de l'annexe*). Cela permettrait aux CSIRT nationaux d'apporter un soutien opérationnel en cas de cyberincidents dans des entreprises et des organisations qui ne relèvent pas du champ d'application de la directive mais qui sont également importantes pour la société et l'économie. En outre, les États membres pourraient tirer pleinement parti des possibilités de financement supplémentaires offertes par le programme du mécanisme pour l'interconnexion en Europe (MIE) relatif aux infrastructures de services numériques (DSI) dans le domaine de la cybersécurité, conçu pour renforcer les capacités des CSIRT nationaux et la coopération entre eux (*voir la section 3.5 de l'annexe*).

Cohérence du processus d'identification des OSE

Conformément à l'article 5 de la directive SRI, les États membres sont tenus d'identifier les entités qui seront considérées comme des opérateurs de services essentiels au plus tard le 9 novembre 2018. En ce qui concerne cette tâche, les États membres pourraient envisager d'utiliser, de manière cohérente, les définitions et les orientations contenues dans la présente communication afin de veiller à ce que des entités similaires jouant un rôle similaire sur le marché intérieur soient systématiquement identifiées comme des opérateurs de services essentiels dans d'autres États membres. Les États membres pourraient également envisager d'étendre le champ d'application de la directive SRI aux administrations publiques, compte tenu du rôle qu'elles jouent en faveur de la société et de l'économie dans son ensemble (*voir sections 2.1 et 4.1.3 de l'annexe*).

Il serait très utile d'harmoniser, dans la mesure du possible, les approches nationales en matière d'identification des opérateurs de services essentiels, notamment en suivant les orientations élaborées par le groupe de coopération (*voir section 4.1.2 de l'annexe*), car cela

contribuerait à une application plus harmonisée des dispositions de la directive et réduirait ainsi le risque de fragmentation du marché. Dans les cas où les opérateurs de services essentiels fournissent des services essentiels dans deux États membres ou plus , il est crucial que les États membres s'efforcent de parvenir à un accord dans le cadre du processus de consultation prévu à l'article 5, paragraphe 4, sur l'identification cohérente des entités (*voir la section 4.1.7 de l'annexe*), car cela permettrait d'éviter qu'une même entité fasse l'objet d'un traitement réglementaire différent dans des juridictions d'États membres différents.

Soumission d'informations sur l'identification des OSE à la Commission

Conformément à l'article 5, paragraphe 7, les États membres sont tenus de fournir à la Commission des informations sur les mesures nationales permettant l'identification des OSE, la liste des services essentiels, le nombre d'OSE identifiés et l'importance de ces opérateurs pour le secteur. En outre, les États membres sont invités à fournir les seuils, pour autant qu'ils existent, utilisés dans le processus d'identification pour déterminer le niveau de l'offre pertinent ou l'importance de l'opérateur concerné pour maintenir un niveau d'offre suffisant. Les États membres pourraient également envisager de partager avec la Commission les listes d'opérateurs de services essentiels identifiés et, le cas échéant, à titre confidentiel, car cela contribuerait à améliorer l'exactitude et la qualité de l'évaluation de la Commission (*voir les sections 4.1.5 et 4.1.6 de l'annexe*).

Approches harmonisées concernant les exigences en matière de sécurité et de notification des incidents applicables aux OSE

En ce qui concerne les obligations relatives aux exigences de sécurité et aux notifications d'incidents pour les opérateurs de services essentiels (article 14, paragraphes 1, 2 et 3), une approche harmonisée en la matière afin de faciliter la conformité des OSE par-delà les frontières des États membres de l'Union favoriserait, dans toute la mesure du possible, un effet de marché unique. La référence reste ici les travaux portant sur un document d'orientation menés au sein du groupe de coopération (*voir les sections 4.2 et 4.3 de l'annexe*).

Dans le cas d'un incident cybernétique à grande échelle qui affecte plusieurs États membres, il est très probable qu'une notification d'incident obligatoire soit soumise par un OSE ou un FSN conformément à l'article 14, paragraphe 3, et à l'article 16, paragraphe 3, ou par une autre entité qui ne relève pas du champ d'application de la directive sur une base volontaire conformément à l'article 20, paragraphe 1. Conformément à la recommandation de la Commission sur la coordination des réactions aux incidents et crises de cybersécurité majeurs, les États membres pourraient envisager d'aligner leurs approches nationales afin de pouvoir fournir dès que possible des informations pertinentes fondées sur ces notifications aux autorités compétentes ou au CSIRT des autres États membres concernés. Des informations précises et exploitables seraient essentielles pour réduire le nombre d'infections ou remédier aux vulnérabilités avant qu'elles ne soient exploitées.

Dans un esprit de partenariat visant à tirer le meilleur parti de la directive SRI, la Commission a l'intention d'accorder un soutien au titre du mécanisme pour l'interconnexion en Europe à

toutes les parties prenantes concernées par cette législation. Bien que l'accent ait été mis sur le renforcement des capacités des CSIRT et sur une plateforme favorisant une coopération opérationnelle rapide et efficace destinée à renforcer le réseau CSIRT, la Commission va maintenant examiner comment le financement au titre du mécanisme pour l'interconnexion en Europe peut également bénéficier aux autorités nationales compétentes ainsi qu'aux opérateurs de services essentiels et aux fournisseurs de service numérique.

Conclusion

Compte tenu des échéances imminentes du 9 mai 2018 pour la transposition de la directive SRI dans la législation nationale et du 9 novembre 2018 pour l'identification des opérateurs de services essentiels, les États membres devraient prendre des mesures appropriées pour veiller à ce que les dispositions et les modèles de coopération de la directive SRI fournissent les meilleurs outils possibles au niveau de l'Union pour parvenir à un niveau élevé commun de sécurité des réseaux et des systèmes d'information. La Commission invite les États membres à examiner, dans le cadre de ce processus, les informations, orientations et recommandations pertinentes contenues dans la présente communication.

La présente communication peut être complétée par d'autres actions, y compris celles qui découlent des travaux en cours dans le cadre du groupe de coopération.