Un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l’Union

2022/0085(COD) - 10/03/2023 - Rapport déposé de la commission, 1ère lecture/lecture unique

La commission de l’industrie, de la recherche et de l’énergie a adopté le rapport d’Henna VIRKUNEN (PPE, FI) sur la proposition de règlement du Parlement européen et du Conseil établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l’Union.

La commission compétente a recommandé que la position du Parlement européen adoptée en première lecture dans le cadre de la procédure législative ordinaire modifie la proposition comme suit:

Objet

Le règlement devrait établir des mesures qui ont pour but d’obtenir un niveau élevé commun de cybersécurité au sein des entités de l’Union. À cette fin, le règlement fixerait:

- les obligations qui imposent aux entités de l’Union de mettre en place un cadre de gestion des risques, de traitement des incidents, de gouvernance et de contrôle des risques de cybersécurité;

- les obligations incombant aux entités de l’Union en ce qui concerne la gestion des risques de cybersécurité et la communication d’informations;

- les règles sous-jacentes aux obligations de partage d’informations et à la facilitation des modalités de partage volontaire d’informations pour les entités de l’Union;

- les règles relatives à l’organisation, aux missions et au fonctionnement du centre de cybersécurité des entités de l’Union (CERT-UE) et à l’organisation et au fonctionnement du conseil interinstitutionnel de cybersécurité (IICB).

Cadre de gestion des risques, de traitement des incidents, de gouvernance et de contrôle des risques

Sur la base d’un audit de cybersécurité exhaustif, **chaque entité de l’Union** devrait établir son propre cadre de gestion des risques, de traitement des incidents, de gouvernance et de contrôle des risques de cybersécurité. L’établissement de ce cadre devrait être placé sous la supervision du **niveau hiérarchique le plus élevé** de l’entité de l’Union et se trouver sous sa responsabilité.

Le cadre de gestion des risques devrait i) définir les objectifs stratégiques permettant d’assurer un niveau élevé de cybersécurité au sein des entités de l’Union; ii) définir des mesures de cybersécurité pour la sécurité des réseaux et des systèmes d’information englobant la totalité de l’environnement TIC et déterminer les rôles et les responsabilités du personnel des entités de l’Union chargé d’assurer la bonne mise en œuvre du règlement; iii) comporter les indicateurs de performance clés (IPC).

Le cadre devrait être **réexaminé régulièrement** et au moins tous les trois ans.

Mesures de gestion des risques de cybersécurité de gestion des risques

Les mesures de gestion des risques devraient garantir, pour les réseaux et les systèmes d’information de la **totalité de l’environnement TIC**, un niveau de sécurité adapté aux risques identifiés dans le cadre de

gestion des risques en tenant compte de l'état des connaissances et, s'il y a lieu, des normes européennes et internationales applicables ou des certificats de cybersécurité européens disponibles.

Lors de l'évaluation de la **proportionnalité** de ces mesures, il conviendrait de tenir compte du degré d' exposition de l'entité de l'Union aux risques, de sa taille et de la probabilité de survenance d'incidents et de leur gravité, y compris leurs conséquences sociétales, économiques et interinstitutionnelles.

Évaluations de la maturité en matière de cybersécurité

Chaque entité de l'Union devrait procéder, au plus tard 18 mois après la date d'entrée en vigueur du règlement, puis au moins tous les deux ans par la suite, à une évaluation de la maturité en matière de cybersécurité portant sur l'ensemble des éléments de son environnement TIC. Les petites entités de l' Union dont les tâches ou la structure sont similaires pourraient effectuer une évaluation combinée de la maturité en matière de cybersécurité.

Compte tenu des conclusions tirées de l'évaluation de la maturité en matière de cybersécurité et des risques identifiés, le niveau hiérarchique le plus élevé de chaque entité de l'Union devrait approuver un **plan de cybersécurité** dans les meilleurs délais après l'établissement du cadre et l'adoption des mesures de gestion des risques de cybersécurité.

Conseil interinstitutionnel de cybersécurité - IICB

L'IICB a pour but d'aider les entités à améliorer leurs postures de cybersécurité respectives grâce à la mise en œuvre du règlement. Afin d'aider les entités de l'Union, l'IICB devrait i) adopter les **orientations et les recommandations** requises pour les évaluations de la maturité en matière de cybersécurité et les plans de cybersécurité des entités de l'Union, ii) réexaminer les interconnexions éventuelles entre les environnements TIC des entités de l'Union et iii) soutenir la mise en place d'un **groupe de responsables de la cybersécurité** relevant de l'ENISA, comprenant les responsables locaux de la cybersécurité de toutes les entités de l'Union, avec pour objectif de faciliter le partage de bonnes pratiques et d'expériences découlant de la mise en œuvre du règlement.

Lorsque l'IICB considère qu'une entité de l'Union n'a pas appliqué ou mis en œuvre le règlement avec efficacité, il pourrait i) demander la documentation pertinente et disponible portant sur la bonne mise en œuvre des dispositions du règlement, ii) faire part de son **avis motivé** relatif aux lacunes observées dans la mise en œuvre du règlement, iii) inviter l'entité de l'Union concernée à fournir une auto-évaluation de son avis motivé et iv) publier, en coopération avec le CERT-UE, des **orientations** destinées à rendre conformes au règlement son cadre de gestion, de gouvernance et de contrôle des risques, ses mesures de gestion des risques de cybersécurité, ses plans de cybersécurité et ses obligations de communication d' information.

Mission et tâches du CERT-UE

La mission du CERT-UE, centre interinstitutionnel autonome de cybersécurité au service de l'ensemble des entités de l'Union serait de contribuer à la sécurité de l'environnement TIC non classifié de l' ensemble des entités de l'Union et de leur fournir des conseils concernant la cybersécurité, en les aidant à prévenir, à détecter et à traiter les incidents, ainsi qu'à en atténuer les effets, à y répondre et à s'en remettre. Le CERT-UE serait un fournisseur interinstitutionnel autonome de services destinés à l' ensemble des entités de l'Union. Il serait intégré à la structure administrative d'une direction générale de la Commission, afin de bénéficier des structures d'appui de la Commission en matière administrative, financière, de gestion et de comptabilité.

Obligations en matière de communication d'informations

Le règlement définit une approche de la **notification des incidents importants** en plusieurs étapes. L’ ensemble des entités de l’Union devraient informer le CERT-UE de tout incident ayant un impact important. Un incident est considéré comme important si: a) il a causé ou est susceptible de causer une perturbation opérationnelle grave du service ou des pertes financières pour l’entité concernée; b) il a affecté ou est susceptible d’affecter d’autres personnes physiques ou morales en causant des dommages matériels, corporels ou moraux considérables.

Les entités de l’Union devraient notifier, entre autres, toute information qui permet au CERT-UE de déterminer toute conséquence inter-entités, transfrontière ou pour l’État membre hôte de l’incident important. L’ensemble des entités de l’Union devraient transmettre au CERT-EU:

a) sans retard injustifié et en tout état de cause dans les **24 heures** après avoir eu connaissance de l’ incident important, une alerte précoce qui, le cas échéant, indique si l’on suspecte l’incident important d’ avoir été causé par des actes illicites ou malveillants ou s’il pourrait avoir un impact inter-entités ou transfrontière;

b) sans retard injustifié et en tout état de cause dans les **72 heures** après avoir eu connaissance de l’ incident important, un rapport d’incident.

Le CERT-UE devrait coordonner le traitement des **incidents majeurs** entre les entités de l’Union.