Services de sécurité gérés

2023/0108(COD) - 24/04/2024 - Texte adopté du Parlement, 1ère lecture/lecture unique

Le Parlement européen a adopté par 530 voix pour, 5 contre et 33 abstentions, une résolution législative sur la proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) 2019 /881 en ce qui concerne les services de sécurité gérés.

La position du Parlement européen arrêtée en première lecture dans le cadre de la procédure législative ordinaire modifie la proposition comme suit:

Objectif

Le règlement proposé vise à permettre l'adoption de **schémas européens de certification de cybersécurité pour les services de sécurité gérés**. Un service de sécurité géré est défini comme un service fourni à un tiers consistant à effectuer des activités liées à la gestion des risques en matière de cybersécurité, ou à fournir une assistance dans le cadre de ces activités, telles que le traitement des incidents, les tests d'intrusion, les audits de sécurité et le conseil en matière de sécurité, y compris les conseils d'experts, liés à l'assistance technique.

Les schémas de certification faciliteront l'entrée sur le marché et l'offre de services de sécurité gérés, en simplifiant la charge réglementaire, administrative et financière potentielle que les fournisseurs, en particulier les microentreprises ou les petites et moyennes entreprises (PME), pourraient rencontrer lorsqu' ils proposent des services de sécurité gérés.

En outre, afin d'encourager l'adoption de services de sécurité gérés et d'en stimuler la demande, les schémas de certification contribueront à leur accessibilité, en particulier pour les petits acteurs, tels que les microentreprises et les PME, ainsi que pour les collectivités locales et régionales qui disposent de capacités et de ressources limitées, mais qui sont plus exposées aux atteintes à la cybersécurité ayant des implications financières, juridiques, de réputation et opérationnelles.

Le schéma de certification de l'Union pour les services de sécurité gérés devrait contribuer à la disponibilité de services sûrs et de haute qualité qui garantissent une transition numérique sûre et à la réalisation des objectifs fixés dans le programme d'action pour la décennie numérique, en particulier en ce qui concerne l'objectif consistant à ce que 75% des entreprises de l'Union commencent à utiliser l' informatique en nuage, l'IA ou les mégadonnées, à ce que plus de 90% des microentreprises et des PME atteignent au moins un niveau élémentaire d'intensité numérique et à ce que les services publics essentiels soient proposés en ligne.

Préparation, adoption et réexamen d'un schéma européen de certification de cybersécurité

À la suite d'une demande formulée par la Commission, **l'ENISA** préparera un schéma candidat qui satisfait aux exigences applicables énoncées au règlement. À la suite d'une demande formulée par le groupe européen de certification de cybersécurité (GECC) pourra préparer un schéma candidat qui satisfait aux exigences applicables. Si l'ENISA rejette une telle demande, elle devra motiver son refus. Toute décision de rejeter une telle demande sera prise par le conseil d'administration.

Lors de la préparation d'un schéma candidat, l'ENISA consultera en temps utile toutes les parties prenantes concernées au moyen d'un processus de consultation formel, ouvert, transparent et inclusif. Pour chaque schéma candidat, l'ENISA créera un groupe de travail ad hoc afin qu'il lui fournisse des conseils et des compétences spécifiques. Les groupes de travail ad hoc créés à cette fin comprendront, le

cas échéant des experts des administrations publiques des États membres, des institutions, organes et organismes de l'Union et du secteur privé.

Information et consultation sur les schémas européens de certification de cybersécurité

La Commission rendra publiques les informations relatives à sa demande à l'ENISA de préparer un schéma candidat. Au cours de la préparation d'un schéma candidat par l'ENISA, le Parlement européen et le Conseil pourront demander à la Commission, en sa qualité de président du GECC, et à l'ENISA, de présenter **tous les trimestres** des informations pertinentes sur un projet de schéma candidat.

À la demande du Parlement européen ou du Conseil, l'ENISA, en accord avec la Commission, pourra mettre à la disposition du Parlement européen et du Conseil des parties pertinentes d'un projet de schéma candidat d'une manière adaptée au niveau de confidentialité requis et, le cas échéant, de manière restreinte.

Afin de renforcer le dialogue entre les institutions de l'Union et de contribuer à un processus de consultation formel, ouvert, transparent et inclusif, le Parlement européen et le Conseil pourront inviter la Commission et l'ENISA à examiner des questions concernant le fonctionnement des schémas européens de certification de cybersécurité pour les produits TIC, services TIC, processus TIC ou services de sécurité gérés. La Commission devra tenir compte, le cas échéant, des éléments découlant des avis exprimés par le Parlement européen et le Conseil.

Une **nouvelle annexe** contient les exigences auxquelles doivent satisfaire les organismes d'évaluation de la conformité qui souhaitent être accrédités.

Dans une **déclaration**, la Commission rappelle qu'il est reconnu qu'un réexamen approfondi du règlement sur la cybersécurité est de la plus haute importance, y compris l'évaluation des procédures conduisant à l' élaboration, à l'adoption et au réexamen des schémas européens de certification de cybersécurité.

Ce réexamen devrait se fonder sur une analyse approfondie et une vaste consultation sur l'incidence, l' efficacité et l'efficience du fonctionnement du cadre européen de certification de cybersécurité. L'analyse effectuée dans le cadre de l'évaluation établie à l'article 67 du règlement sur la cybersécurité devrait inclure des activités d'élaboration de schémas en cours, telles que celles concernant le schéma européen de certification de cybersécurité pour les services en nuage, ainsi que des activités concernant des schémas adoptés, telles que celles concernant le schéma européen de certification de cybersécurité fondé sur des critères communs.

La Commission, qui est responsable du réexamen du règlement sur la cybersécurité, veillera à ce que ce réexamen tienne compte, le cas échéant, des éléments nécessaires mentionnés à la lumière de l'article 67 lorsqu'elle présente le réexamen aux colégislateurs.