Services de sécurité gérés

2023/0108(COD) - 15/01/2025 - Acte final

OBJECTIF : permettre la mise en place de schémas européens de certification de cybersécurité pour les services de sécurité gérés.

ACTE LÉGISLATIF : Règlement (UE) 2025/37 du Parlement européen et du Conseil modifiant le règlement (UE) 2019/881 en ce qui concerne les services de sécurité gérés.

CONTENU : le présent règlement s'inscrit dans le cadre du paquet législatif sur la cybersécurité qui comprend également le nouveau règlement sur la cybersolidarité.

Schémas européens de certification

La présente modification ciblée du règlement sur la cybersécurité vise à renforcer la cyberrésilience de l'UE en permettant l'adoption à l'avenir de schémas européens de certification pour les «**services de sécurité gérés**».

Les services de sécurité gérés tels que les services concernant la gestion des incidents de cybersécurité, les tests d'intrusion, les audits de sécurité et les conseils liés à l'assistance technique, ont gagné en importance en ce qui concerne la prévention et la limitation des incidents.

Les fournisseurs de services de sécurité gérés ont été la cible de cyberattaques et, du fait de leur grande intégration dans les activités des opérateurs, ils représentent un risque particulier. Il est donc important que les entités essentielles et importantes fassent preuve d'une diligence renforcée lorsqu'elles sélectionnent leurs fournisseurs de services de sécurité géré.

La modification ciblée contribuera à **améliorer la qualité des services de sécurité gérés** et à accroître leur comparabilité, elle facilitera l'émergence de fournisseurs de services de cybersécurité fiables, et elle permettra d'éviter la fragmentation du marché intérieur. Elle contribuera à la réalisation de l'objectif consistant à ce que **75%** des entreprises de l'Union commencent à utiliser les services d'informatique en nuage, les mégadonnées ou l'intelligence artificielle ou, à ce que plus de **90%** des PME, y compris les microentreprises, atteignent au moins un niveau élémentaire d'intensité numérique et à ce que les services publics essentiels soient accessibles en ligne.

Rôle de l'Agence de l'Union européenne pour la cybersécurité (ENISA)

L'ENISA jouera un rôle important dans la préparation des schémas européens de certification de cybersécurité candidats. L'ENISA :

- favorisera le recours à la certification européenne de cybersécurité en vue d'éviter la fragmentation du marché intérieur;

- contribuera à l'établissement et au maintien d'un **cadre européen de certification** de cybersécurité;

- favorisera l'élaboration et la mise en œuvre de la politique de l'Union en matière de certification de cybersécurité des produits TIC et services de sécurité gérés;

- facilitera l'établissement et l'adoption de normes européennes et internationales en matière de gestion des risques et de sécurité des produits TIC services de sécurité gérés.

À la suite d'une demande formulée par la Commission, l'ENISA préparera un **schéma candidat** qui satisfait aux exigences applicables énoncées au règlement. 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.

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 et à l'ENISA, de présenter tous les trimestres des informations pertinentes sur un projet de schéma candidat.

Objectifs de sécurité des schémas européens de certification de cybersécurité

Un schéma européen de certification de cybersécurité pour les services de sécurité gérés doit être conçu de façon à réaliser, selon le cas, au moins les objectifs de sécurité suivants:

- que les services de sécurité gérés soient fournis avec la compétence, l'expertise et l'expérience requises;

- que le fournisseur ait mis en place des procédures internes pour garantir que les services de sécurité gérés sont fournis à tout moment à un niveau de qualité suffisant;

- que les données consultées, stockées, transmises ou traitées dans le cadre de la fourniture de services de sécurité gérés soient protégées contre l'accès, le stockage, la diffusion, la destruction ou tout autre traitement accidentels ou non autorisés, ou contre la perte ou l'altération ou l'indisponibilité;

- que la disponibilité des données, services et fonctions ainsi que l'accès à ceux-ci soient rétablis dans les plus brefs délais en cas d'incident physique ou technique;

- qu'un registre soit tenu et disponible pour l'évaluation des données, services ou fonctions qui ont été consultés, utilisés ou traités de toute autre façon, du moment où ils l'ont été et par qui, et faire en sorte qu' il soit possible d'évaluer ces éléments.

La Commission **évaluera régulièrement** l'efficacité et l'utilisation des schémas européens de certification de cybersécurité adoptés ainsi que la question de savoir si un schéma européen de certification de cybersécurité spécifique doit être rendu obligatoire, au moyen de dispositions pertinentes du droit de l'Union.

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

ENTRÉE EN VIGUEUR : 4.2.2025.