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

2022/0085(COD) - 22/03/2022 - Document de base législatif

OBJECTIF : établir des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l’Union.

ACTE PROPOSÉ : Règlement du Parlement européen et du Conseil.

RÔLE DU PARLEMENT EUROPÉEN : le Parlement européen décide conformément à la procédure législative ordinaire et sur un pied d'égalité avec le Conseil.

CONTEXTE : l’évolution de la technologie ainsi que la complexité et l’interdépendance croissantes des systèmes numériques amplifient les risques de cybersécurité et **rendent l’administration de l’Union plus vulnérable aux cybermenaces et aux incidents**.

Les institutions, organes et organismes de l’Union sont devenus des cibles très attrayantes pour les cyberattaques sophistiquées. Entre 2019 et 2021, le nombre d’incidents importants touchant des institutions, organes et organismes de l’Union et perpétrés par des acteurs de menaces persistantes avancées a considérablement augmenté. Au cours du premier semestre de 2021, on a enregistré autant d’ incidents importants que sur l’ensemble de l’année 2020.

Le Centre pour la cybersécurité des institutions, organes et organismes de l’Union (CERT-UE) a évalué les principales cybermenaces auxquelles les institutions, organes et organismes de l’Union sont actuellement exposés ou sont susceptibles de l’être dans un avenir prévisible. L’analyse a examiné l’ influence des grands changements en cours sur la façon dont les institutions de l’Union gèrent et utilisent leurs infrastructures et services informatiques. Parmi ces changements figurent l’augmentation du télétravail, la migration des systèmes vers le nuage et l’externalisation accrue des services informatiques.

L’analyse des vingt institutions, organes et organismes de l’Union concernés fait apparaître **des disparités considérables** en ce qui concerne leur gouvernance, leur hygiène informatique, leurs capacités globales et leur maturité. Par conséquent, pour remédier à cette hétérogénéité des niveaux de maturité en matière de cybersécurité, il est nécessaire que les institutions, organes et organismes de l’Union atteignent **un niveau élevé commun de cybersécurité** grâce à une base de référence en cybersécurité, à l’échange d’ informations et à la collaboration.

La présente proposition s’appuie sur la stratégie de l’UE pour l’union de la sécurité et sur la stratégie de cybersécurité de l’UE pour la décennie numérique.

CONTENU : la présente proposition établit **un cadre destiné à assurer des règles et des mesures communes en matière de cybersécurité au sein des institutions, organes et organismes de l’Union** afin de leur permettre d’accomplir leurs missions respectives de manière ouverte, efficace et indépendante. Elle vise à améliorer la résilience de toutes les entités ainsi que leurs capacités de réaction aux incidents.

Le règlement proposé :

- oblige les institutions, organes et organismes de l’Union à i) établir **un cadre interne** pour la gestion, la gouvernance et le contrôle des risques de cybersécurité, garantissant une gestion efficace et prudente de

tous ces risques, ii) adopter une **base de référence** en cybersécurité pour faire face aux risques identifiés au moyen de ce cadre, iii) procéder, au moins tous les trois ans, à une **évaluation de la maturité** en matière de cybersécurité portant sur l'ensemble des éléments de son environnement informatique et iv) à adopter un **plan de cybersécurité**;

- institue un **conseil interinstitutionnel de cybersécurité** chargé de suivre la mise en œuvre du présent règlement par les institutions, organes et organismes de l'Union, ainsi que de surveiller la mise en œuvre des priorités et des objectifs généraux par le CERT-UE et de fournir à ce dernier des orientations stratégiques;

- définit la tâche et les missions du CERT-UE, centre interinstitutionnel autonome de cybersécurité au service de l'ensemble des institutions, organes et organismes de l'Union. Le CERT-UE contribuera à la sécurité de l'environnement informatique de l'ensemble des institutions, organes et organismes de l'Union en les conseillant, en les aidant à prévenir, à détecter et à limiter les incidents, ainsi qu'à y répondre, et en faisant office de plateforme d'échange d'informations et de coordination des réponses aux incidents dans le domaine de la cybersécurité;

- garantit la coopération et l'échange d'informations entre le CERT-UE et les institutions, organes et organismes de l'Union afin de renforcer la confiance. À cette fin, le CERT-UE pourrait demander aux institutions, organes et organismes de l'Union de lui fournir des informations pertinentes et il pourrait échanger des informations spécifiques à un incident avec les institutions, organes et organismes de l' Union afin de faciliter la détection des cybermenaces ou incidents similaires sans le consentement de la partie concernée. Le CERT-UE ne pourrait échanger des informations spécifiques à un incident qui révèlent l'identité de la cible de l'incident de cybersécurité qu'avec le consentement de la partie concernée;

- oblige l'ensemble des institutions, organes et organismes de l'Union à **notifier au CERT-UE** les cybermenaces importantes, les vulnérabilités importantes et les incidents importants dans les plus brefs délais et, en tout état de cause, au plus tard 24 heures après en avoir eu connaissance.

INCIDENCE BUDGÉTAIRE : d'après les études, les dépenses directes en matière de cybersécurité représentent généralement entre 4 et 7% du total des dépenses informatiques des organisations. Toutefois, l'analyse des menaces menée par la CERT-UE indique que les organisations politiques et organismes internationaux sont confrontés à des risques accrus et qu'il semblerait plus approprié de consacrer **10%** des dépenses informatiques à la cybersécurité.

Le coût exact de ces efforts est impossible à déterminer en raison du manque d'informations détaillées sur les dépenses informatiques des institutions, organes et organismes de l'Union et sur la part que représentent les dépenses de cybersécurité.

Le CERT-UE aura besoin de ressources supplémentaires pour mener à bien sa mission élargie et ces ressources devraient être réaffectées à partir des institutions, organes et organismes de l'UE bénéficiant des services du CERT-UE.