

Services de sécurité gérés

2023/0108(COD) - 18/04/2023 - Document de base législatif

OBJECTIF : proposer une modification ciblée du règlement sur la cybersécurité, afin de permettre l'adoption future de schémas de certification européens pour les «services de sécurité gérés».

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 : le règlement (UE) 2019/881 du Parlement européen et du Conseil relatif à l'ENISA (l'Agence de l'Union européenne pour la cybersécurité) et à la certification en matière de cybersécurité des technologies de l'information et des communications établit un cadre pour la mise en place de systèmes européens de certification en matière de cybersécurité dans le but d'assurer un niveau adéquat de cybersécurité pour les produits d'information et de technologie TIC, les services TIC et les processus TIC dans l'Union, ainsi que dans le but d'éviter la fragmentation du marché intérieur en ce qui concerne les systèmes de certification en matière de cybersécurité dans l'Union.

Les **services de sécurité gérés**, qui sont des services consistant à mener des activités liées à la gestion des risques de cybersécurité de leurs clients, ou à fournir une assistance à cet égard, ont pris **une importance croissante dans la prévention et l'atténuation des incidents de cybersécurité**. En conséquence, les prestataires de ces services sont considérés comme des entités essentielles ou importantes appartenant à un secteur de haute criticité conformément à la directive (UE) 2022/2555 du Parlement européen et du Conseil relative à des mesures visant à assurer un niveau commun élevé de cybersécurité dans l'Union.

Les fournisseurs de services de sécurité gérés dans des domaines tels que la réponse aux incidents, les tests de pénétration, les audits de sécurité et le conseil, jouent un rôle particulièrement important pour aider les entreprises et autres organisations à prévenir, détecter, réagir ou se remettre des cyberincidents. Cependant, ils ont également été la cible de **cyberattaques** et présentent un risque particulier en raison de leur intégration étroite dans les opérations de leurs clients.

Certains États membres ont déjà commencé à adopter des systèmes de certification pour les services de sécurité gérés. Il existe donc **un risque concret de fragmentation du marché intérieur** de ces services, auquel la présente proposition vise à remédier.

CONTENU : la modification ciblée proposée vise à permettre, au moyen d'actes d'exécution de la Commission, **l'adoption de schémas européens de certification de cybersécurité pour les «services de sécurité gérés»**, en plus des produits d'information et de technologie (TIC), des services TIC et des processus TIC, qui sont déjà couverts par le règlement sur la cybersécurité.

La proposition introduit une définition de ces services, qui est très étroitement alignée sur la définition des «fournisseurs de services de sécurité gérés» au sens de la directive NIS 2 (article 2 du règlement sur la cybersécurité). Elle ajoute également une nouvelle disposition sur les objectifs de sécurité de la certification européenne de cybersécurité adaptée aux «services de sécurité gérés». Enfin, un certain nombre de modifications techniques sont apportées afin de garantir que les articles pertinents s'appliquent également aux «services de sécurité gérés».