Des règles européennes plus strictes

De nouvelles règles plus strictes vont s'appliquer à la cyber-résilience et la résilience physique des entités et réseaux critiques.
Deux directives clés sur les infrastructures critiques et numériques entrent en vigueur et renforcent la résilience de l'UE face aux menaces en ligne et hors ligne, des cyber-attaques à la criminalité, aux risques pour la santé publique ou aux catastrophes naturelles.

Les menaces qui pèsent récemment sur les infrastructures critiques de l'UE sont susceptibles de porter atteinte à notre sécurité collective. Déjà en 2020, la Commission européenne avait proposé une mise à niveau significative des règles de l'UE en matière de résilience des entités critiques et de sécurité des réseaux et des systèmes d'information.

Les 2 directives entrées en vigueur sont :

- Directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (Directive SRI 2)[1]
- Directive sur la résilience des entités critiques (Directive CER)[2]

La Directive SRI 2 garantira une Europe plus sûre et plus forte en élargissant considérablement les secteurs et le type d'entités critiques relevant de son champ d'application. Il s'agit notamment des fournisseurs de réseaux et de services publics de communications électroniques, des services de centres de données, de la gestion des eaux usées et des déchets, de la fabrication de produits critiques, des services postaux et de courrier et des entités de l'administration publique, ainsi que du secteur des soins de santé au sens large. En outre, elle renforcera les exigences en matière de gestion des risques de cybersécurité que les entreprises sont tenues de respecter, et rationalisera les obligations en matière de signalement des incidents par des dispositions plus précises concernant le signalement, le contenu et le calendrier.

Face à un paysage de risques de plus en plus complexe, la nouvelle Directive CER remplace la directive sur les infrastructures critiques européennes de 2008[3]. Les nouvelles règles renforceront la résilience des infrastructures critiques face à toute une série de menaces, notamment les risques naturels, les attaques terroristes, les menaces internes ou le sabotage. Onze secteurs seront couverts : l'énergie, les transports, les banques, les infrastructures des marchés financiers, la santé, l'eau potable, les eaux usées, les infrastructures numériques, l'administration publique, l'espace et l'alimentation. Les États membres devront adopter une stratégie nationale et procéder régulièrement à des évaluations des risques afin de recenser les entités considérées comme critiques ou vitales pour la société et l'économie.

Les États membres disposent de 21 mois pour transposer ces deux directives dans leur droit national.

Source : https://digital-strategy.ec.europa.eu/en/news/new-stronger-rules-start-apply-cyber-and-physical-resilience-critical-entities-and-networks

Documentation

Critical Infrastructure: Commission accelerates work to build up European resilience
https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6238

1 *Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (Directive SRI 2)*

2 *Directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil (Directive CER)*

3 *Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection*