Cyberveiligheid - Strengere Europese regels

Strengere regels gaan van toepassing voor de cyber- en fysieke veerkracht van kritieke entiteiten en netwerken.
Twee belangrijke richtlijnen inzake kritieke en digitale infrastructuur treden in werking treden en maken de EU beter bestand tegen online- en offline-dreigingen, van cyberaanvallen tot criminaliteit, risico's voor de volksgezondheid of natuurrampen.

Recente bedreigingen voor de kritieke infrastructuur van de EU hebben geprobeerd onze collectieve veiligheid te ondermijnen. Reeds in 2020 had de Europese Commissie voorgesteld de EU-regels inzake de veerkracht van kritieke entiteiten en de beveiliging van netwerk- en informatiesystemen aanzienlijk te verbeteren.

De 2 richtlijnen die in werking treden, zijn:

- Richtlijn betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie (NIS 2-richtlijn) ;
- Richtlijn betreffende de weerbaarheid van kritieke entiteiten (CER-richtlijn) .

De NIS 2-richtlijn zal zorgen voor een veiliger en sterker Europa door de sectoren en soorten kritieke entiteiten die onder het toepassingsgebied ervan vallen aanzienlijk uit te breiden. Het gaat onder meer om aanbieders van openbare elektronische-communicatienetwerken en -diensten, datacentra, afvalwater- en afvalbeheer, de productie van kritieke producten, post- en koeriersdiensten en overheidsinstanties, alsook de gezondheidszorg in ruimere zin. Voorts zullen de vereisten inzake risicobeheer op het gebied van cyberbeveiliging waaraan bedrijven moeten voldoen, worden aangescherpt en zullen de verplichtingen inzake melding van incidenten worden gestroomlijnd met preciezere bepalingen inzake rapportage, inhoud en tijdschema.

Tegen de achtergrond van een steeds complexer risicolandschap vervangt de nieuwe CER-richtlijn de richtlijn Europese kritieke infrastructuur van 2008. De nieuwe regels zullen kritieke infrastructuur weerbaarder maken tegen een reeks bedreigingen, waaronder natuurrampen, terroristische aanslagen, dreigingen van binnenuit of sabotage. Er zullen 11 sectoren worden bestreken: energie, vervoer, bankwezen, infrastructuur van de financiële markten, gezondheid, drinkwater, afvalwater, digitale infrastructuur, openbaar bestuur, ruimtevaart en voedsel. De lidstaten zullen een nationale strategie moeten vaststellen en regelmatig risicobeoordelingen moeten uitvoeren om vast te stellen welke entiteiten als cruciaal of essentieel voor de samenleving en de economie worden beschouwd. De lidstaten hebben 21 maanden de tijd om beide richtlijnen in nationaal recht om te zetten.

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

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

© Irina Strelnikova / Adobe Stock