Nya strängare regler börjar gälla för kritiska entiteters och nätverks cyberresiliens och fysiska motståndskraft

Två viktiga direktiv om kritisk och digital infrastruktur har nyligen trätt i kraft och kommer att stärka EU:s motståndskraft mot hot online och offline, från cyberattacker till brottslighet, risker för folkhälsan eller naturkatastrofer.

iStock photo Getty images plus

Den senaste tidens hot mot EU:s kritiska infrastruktur har försökt undergräva vår kollektiva säkerhet. Redan 2020 föreslog kommissionen en betydande uppgradering av EU:s regler om kritiska entiteters motståndskraft och säkerheten i nätverks- och informationssystem.

De 2 direktiv som träder i kraft är följande:

- **Direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS 2-direktivet)** (https://eur-lex.europa.eu/eli/dir/2022/2555)
- Direktivet om kritiska entiteters motståndskraft (https://eur-lex.europa.eu/eli/dir/2022/2557/oj)

NIS 2-direktivet kommer att säkerställa ett säkrare och starkare Europa genom att avsevärt utvidga de sektorer och den typ av kritiska entiteter som omfattas av direktivet. Dessa omfattar leverantörer av allmänna elektroniska kommunikationsnät och kommunikationstjänster, datacentraltjänster, avloppsvatten och avfallshantering, tillverkning av kritiska produkter, post- och budtjänster och offentliga förvaltningsenheter samt hälso- och sjukvårdssektorn i vidare bemärkelse. Dessutom kommer den att **stärka de krav på hantering av cybersäkerhetsrisker som företagen är skyldiga att uppfylla samt** effektivisera incidentrapporteringsskyldigheterna med **mer exakta bestämmelser om rapportering, innehåll och tidsplan**. NIS 2-direktivet ersätter reglerna om säkerhet i nätverks- och informationssystem

(https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG&toc=OJ%3AL%3A2016%3A194%3ATOC), den första EU-omfattande lagstiftningen om cybersäkerhet.

Mot bakgrund av ett allt mer komplext risklandskap ersätter det nya **CER-direktivet** från 2008 direktivet om europeisk kritisk infrastruktur. De nya reglerna kommer att stärka den kritiska infrastrukturens motståndskraft mot en rad hot, däribland naturkatastrofer, terroristattacker, interna hot eller sabotage. 11 **sektorer** kommer att omfattas: energi, transport, bankverksamhet, finansmarknadsinfrastrukturer, hälso- och sjukvård, dricksvatten, avloppsvatten, digital infrastruktur, offentlig förvaltning, rymden och livsmedel. Medlemsstaterna kommer att behöva anta en **nationell strategi** och genomföra **regelbundna riskbedömningar för** att identifiera entiteter som anses vara kritiska eller avgörande för samhället och ekonomin.

Medlemsländerna har 21 månader på sig att införliva båda direktiven i sin nationella lagstiftning. Under denna tid ska medlemsstaterna anta och offentliggöra de åtgärder som är nödvändiga för att följa dem.

I december 2022 antog rådet en **rekommendation** (https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6238) **om en unionsomfattande samordningsstrategi för att stärka motståndskraften hos kritisk infrastruktur**, där medlemsstaterna uppmanas att påskynda det förberedande arbetet för införlivande och tillämpning av NIS 2 och direktivet om kritiska entiteters motståndskraft.

Närmare upplysningar

- NIS2-direktivet (https://digital-strategy.ec.europa.eu/en/news/new-stronger-cybersecurity-rules-kicking-safer-eu-digital-landscape)
- NIS fråga a (https://digital-strategy.ec.europa.eu/en/faqs/revision-network-and-information-security-directive-questions-and-answers)
- Faktablad om nät- och informationssäkerhet (https://digital-strategy.ec.europa.eu/en/library/revised-directive-security-network-and-information-systems-nis2)
- CER-direktivet (https://home-affairs.ec.europa.eu/news/commission-proposes-new-directive-enhance-resilience-critical-entities-providing-essential-services-2020-12-16_en)
