EUROPA-
KOMMISSIONEN

Strasbourg, den 20.1.2026
SWD(2026) 12 final

ARBEJDSDOKUMENT FRA KOMMISSIONENS TJENESTEGRENE

RESUMÉ AF RAPPORTEN OM KONSEKVENSANALYSEN

Ledsagedokument til

forslag til Europa-Parlamentets og Rådets forordning om Den Europæiske Unions Agentur for Cybersikkerhed (ENISA), den europæiske ramme for cybersikkerhedscertificering og sikkerhed i IKT-forsyningskæden og om ophævelse af forordning (EU) 2019/881 (forordningen om cybersikkerhed 2)

og

forslag til Europa-Parlamentets og Rådets direktiv om ændring af direktiv (EU) 2022/2555 for så vidt angår forenklingsforanstaltninger og tilpasning til [forslaget til forordning om cybersikkerhed 2]

{COM(2026) 11 final} - {SEC(2026) 11 final} - {SWD(2026) 11 final}

Resumé af konsekvensanalysen

Formål

Hovedformålet med denne konsekvensanalyse er at vurdere, om de nuværende regler er tilstrækkelige til at håndtere de skiftende cybersikkerhedstrusler i hele EU. Der foreslås et integreret sæt politiske løsningsmodeller, der har til formål at styrke Den Europæiske Unions Agentur for Cybersikkerhed (ENISA), reformere den europæiske ramme for cybersikkerhedscertificering (ECCF) og forenkle overholdelsen af den eksisterende lovgivningsmæssige ramme for cybersikkerhed. Denne vurdering understreger vigtigheden af at tilpasse cyberforvaltningen, så den harmoniseres med teknologiske fremskridt og markedets krav, samtidig med at konkurrenceevnen sikres og miljøpåvirkninger tages i betragtning.

Problemformulering

På trods af den eksisterende indsats står EU's cybersikkerhedslandskab stadig over for betydelige udfordringer i en kontekst med stadig mere komplekse trusler. Utilstrækkelig koordinering mellem medlemsstaterne og andre aktører på EU-plan, fastlåst gennemførelse af politiske værktøjer samt lovgivningsmæssige hindringer og kompleksitet hæmmer en effektiv cybersikkerhedsstyring. Disse problemer medfører øgede omkostninger for virksomheder og offentlige myndigheder, øgede risici for cyberhændelser og uensartede beskyttelsesniveauer for borgerne.

Begrundelse for EU's foranstaltninger

Cybersikkerhedstrusler kender ingen nationale grænser. Derfor er en fælles tilgang afgørende for et effektivt modsvar. En indsats på EU-plan sikrer ensartet beskyttelse, styrker konkurrenceevnen ved at skabe lige vilkår og letter den frie bevægelighed for digitale tjenester og produkter på det indre marked. Harmonisering på EU-plan mindsker også de administrative byrder gennem forenklet efterlevelse og strømlinede procedurer.

Politiske løsningsmodeller og foretrukken løsningsmodel

I denne rapport analyseres fire indsatsområder, som hver især omfatter en række politiske løsningsmodeller, der overvejes i lyset af de specifikke mål, der skal opnås: 1) ENISA's mandat (også en del af den nuværende forordning om cybersikkerhed), 2) ECCF (også en del af den nuværende forordning om cybersikkerhed) og 3) målrettede ændringer af NIS 2-direktivet med sigte på forenkling, samtidig med at de også er indbyrdes forbundne med ENISA's mandat og ECCF. Hvert af disse sæt af løsningsmodeller udgør interventionsområder i sig selv, samtidig med at de er indbyrdes forbundne og relevante for hinanden.

Løsningsmodeller vedrørende afhjælpning af den manglende overensstemmelse mellem Unionens cybersikkerhedspolitiske ramme og interessenternes behov i et stadig mere fjendtligt miljø

Løsningsmodel A.1: *Præcisering af ENISA's mandat og fastlæggelse af prioriteringer* – Denne løsningsmodel vil sikre en klar og stabil ramme for ENISA's opgaver ved at tilføje de opgaver, der er fastsat i anden lovgivning.

Løsningsmodel A.2: *Reform af ENISA's mandat* – Denne løsningsmodel vil ophæve og erstatte forordningen om cybersikkerhed og gennemgribende ændre agenturets mandat.

Løsningsmodel A.3: *Reform af ENISA's mandat med et stærkt fokus på operationel støtte* – Denne løsningsmodel bygger på løsningsmodel A.2. ENISA vil desuden udvikle kapaciteter til at støtte enheder omfattet af NIS 2-direktivet direkte i deres håndtering af og genopretning efter cybersikkerhedshændelser efter anmodning fra en medlemsstat.

Løsningsmodeller vedrørende den europæiske ramme for cybersikkerhedscertificering

Løsningsmodel B.1: *Præcisering af ECCF's anvendelsesområde, elementer og mål samt indførelse af en vedligeholdelsesmekanisme* – Denne løsningsmodel vil indføre en ny vedligeholdelsesmekanisme for ordningerne, som efter deres vedtagelse skal gennemføres af ENISA.

Løsningsmodel B.2: *Reform af ECCF ved at revidere dens procedurer og udvide anvendelsesområdet for at gøre det lettere at overholde lovgivningen* – Denne løsningsmodel vil ophæve forordningen om cybersikkerhed og erstatte den med en ny forordning. Ud over løsningsmodel B.1 vil proceduren i forbindelse med anmodning om, udvikling og vedtagelse af ordninger blive revideret for at forbedre ansvarlighed og effektivitet.

Løsningsmodel B.3: *Reform af ECCF som under løsningsmodel B.2 og indførelse af obligatorisk sikkerhedsstatuscertificering* – Denne løsningsmodel vil bygge videre på løsningsmodel B.2, men har til formål yderligere at øge rammens virkning ved at indføre obligatorisk certificering af væsentlige enheder, der er omfattet af NIS 2-direktivet, under hensyntagen til specifikke risikoscenarier i stedet for udelukkende at basere sig på frivillig certificering af enheder.

Løsningsmodeller vedrørende forenkling

Løsningsmodel C.1: *En tilgang med blød lovgivning og ikkelovgivningsmæssige instrumenter, herunder anvendelse af eksisterende beføjelser (vedtagelse af gennemførelsesretsakter i henhold til artikel 21, stk. 5, og artikel 23, stk. 11, i NIS 2-direktivet)* – Denne løsningsmodel omfatter vedtagelse af gennemførelsesretsakter ved brug af de eksisterende beføjelser i henhold til NIS 2-direktivet for at sikre en højere grad af harmonisering af foranstaltninger til styring af cybersikkerhedsrisici, tærskler for indberetning af hændelser samt typen af oplysninger, formaterne og proceduren for underretninger, samt vedtagelse af retningslinjer for at styrke retssikkerheden og harmoniseret gennemførelse.

Løsningsmodel C.2: *Målrettet indsats – yderligere forenkling af overholdelsen af den relevante EU-lovgivningsramme for cybersikkerhed* – Denne løsningsmodel indebærer en begrænset indsats gennem ændringer af forordningen om cybersikkerhed og NIS 2-direktivet med det formål at forenkle specifikke aspekter af cybersikkerhedsrammen, herunder tilpasning af anvendelsesområdet, maksimal harmonisering for gennemførelsesretsakter,

dokumentation for overholdelse gennem certificering og vedtagelse af det sæt retningslinjer, der er omhandlet i løsningsmodel C1.

Løsningsmodel C.3: *Harmonisering af cybersikkerhedsrelaterede foranstaltninger fastsat i EU-lovgivningen* – Denne løsningsmodel vil bygge på løsningsmodel C.2 og fjerne alle foranstaltninger til styring af cybersikkerhedsrisici samt beføjelser i relation til foranstaltninger i sektorlovgivning. I stedet vil NIS 2-direktivets økosystem blive ændret for at fastsætte strømlinede krav for alle typer enheder med henblik på at sikre bedre harmonisering.

Løsningsmodeller vedrørende sikkerhed i IKT-forsyningskæden

Løsningsmodel D.1: En *tilgang med blød lovgivning til håndtering af cybersikkerhedsrisici for IKT-forsyningskæder* – Denne løsningsmodel vil ikke indebære lovgivningsmæssige indgreb på EU-plan. I stedet vil Kommissionen øge antallet af koordinerede risikovurderinger og frivillige værktøjskasser.

Løsningsmodel D.2: *Ad hoc-reguleringsindgreb, der kodificerer 5G-værktøjskassen* – Denne løsningsmodel vil kodificere foranstaltningerne i 5G-værktøjskassen. Den vil indføre en forpligtelse for medlemsstaterne til at sikre, at komponenter fra højrisikoleverandører ikke anvendes i netværkets nøgleaktiver.

Løsningsmodel D.3: *Omfattende og horisontal ramme til håndtering af cybersikkerhedsrisici i IKT-forsyningskæder* – Denne løsningsmodel vil etablere en horisontal, teknologi- og sektorneutral lovgivningsmæssig ramme til at håndtere ikketekniske cybersikkerhedsrisici i IKT-forsyningskæder.

Efter omfattende analyser er den foretrukne politikpakke følgende: Løsningsmodel A.2 – Reform af ENISA's mandat, løsningsmodel B.2 – Reform af ECCF ved at revidere dens procedurer og udvide anvendelsesområdet for at gøre det lettere at overholde lovgivningen, og løsningsmodel C.2 – Målrettet indsats – yderligere forenkling af overholdelsen af den relevante EU-lovgivningsramme for cybersikkerhed, og løsningsmodel D.3 – Omfattende og horisontal ramme til håndtering af cybersikkerhedsrisici i IKT-forsyningskæder.

Denne kombination giver en velafbalanceret reaktion på identificerede politiske udfordringer og øger i væsentlig grad virkningen, effektiviteten og sammenhængen på tværs af EU.

Vigtigste virkninger

Cost-benefit-analyse: Overgangen til den foreslåede lovgivningsramme vil medføre omkostninger både for ENISA, der anslås til op til 161,3 mio. EUR over fem år til at varetage sine nye opgaver, og for offentlige myndigheder i hele EU på op til 80 mio. EUR over fem år til tilsyn (under hensyntagen til relevante omkostningsbesparelser). Hvad angår virksomheder, kan udfasning af specifikt højrisikoudstyr over en overgangsperiode på tre år føre til årlige omkostninger på 3,4-4,3 mia. EUR for mobilnetoperatører, mens investeringer i pålidelige leverandører samtidig kan stige til op til 2 mia. EUR om året. Desuden forventes strømlinede og reducerede overholdelsesforpligtelser at skabe omkostningsbesparelser for virksomheder

på op til 14,6 mia. EUR. Desuden vil der være betydelige fordele for borgere, offentlige myndigheder og virksomheder ved at forbedre EU's overordnede cybersikkerhed og teknologiske suverænitet samt ved at stimulere innovation og konkurrenceevne, hvilket på lang sigt forventes i vid udstrækning at opveje de indledende udgifter.

Konkurrenceevne: Ved at mindske fragmenteringen på markedet og harmonisere reglerne fremmer de foretrukne løsningsmodeller lige konkurrencevilkår i hele Unionen og giver virksomhederne klarere veje til overholdelse og innovation.

Klimaoverensstemmelseskontrol: I vurderingen blev der taget hensyn til hver løsningsmodels potentielle miljøpåvirkning. Der blev lagt særlig vægt på energieffektivitet, rejserelaterede emissioner og konsolidering af infrastrukturen. De foretrukne løsningsmodeller A.2, B.2 og C.2 har begrænset miljøpåvirkning, mens D.3 tager højde for miljøneutralitet under hensyntagen til produkters livscyklus og overgangsperioder for udskiftning af nøgleaktiver. Dette er i overensstemmelse med EU's forpligtelse til bæredygtighed.

Digitalt som standard: Forslagets fokus på strømlinede digitale processer demonstrerer Unionens engagement i en "digital først"-tilgang, hvilket sikrer hurtigere og mere pålidelig dataudveksling og beslutningstagning. Løsningsmodel D.3 kan også have stor indvirkning på digitaliseringen, da den vil indebære udskiftning af komponenter fra enheder, der er etableret i eller kontrolleret af enheder fra tredjelande, som udgør en cybersikkerhedsrisiko.

Forenkling og reduktion af byrder: De foretrukne løsningsmodeller bidrager til forenkling ved at indføre præciseringer af anvendelsesområdet og foranstaltninger til at strømline overholdelse og tilsyn, hvilket mindsker de administrative byrder. "Én ind, én ud"-princippet tages i betragtning ved at sikre, at nye forpligtelser opvejes af færre forpligtelser andre steder.

Konklusion

Denne konsekvensanalyse præsenterer en omfattende strategi for at styrke EU's cybersikkerhed, afhjælpe lovgivningsmæssig ineffektivitet og forberede det digitale landskab på fremtidige udfordringer. Der anbefales en samarbejdsorienteret og sammenhængende tilgang, hvor politiske reformer forankres i eksisterende rammer, samtidig med at der sikres tilpasning til den nye teknologiske virkelighed. Gennem disse foranstaltninger har EU til formål at sikre en modstandsdygtig, konkurrencedygtig og bæredygtig digital økonomi.