EUROPA-
KOMMISSIONEN

Bruxelles, den 13.9.2017
SWD(2017) 501 final

ARBEJDSDOKUMENT FRA KOMMISSIONENS TJENESTEGRENE

RESUME AF KONSEKVENSANALYSEN

Ledsagedokument til

forslag til EUROPA-PARLAMENTETS OG RÅDETS FORORDNING

om ENISA, "EU's Agentur for Cybersikkerhed", om ophævelse af forordning (EU) nr. 526/2013 og om cybersikkerhedscertificering af informations- og kommunikationsteknologi ("forordningen om cybersikkerhed").

{COM(2017) 477 final}
{SWD(2017) 500 final}
{SWD(2017) 502 final}

A. BEHOV FOR HANDLING

Hvorfor? Hvad er problemstillingen?

Digitale teknologier og Internettet er rygraden i EU's økonomier og samfund. Kritiske økonomiske sektorer såsom transport, energi, sundhed eller finanssektoren er i stadig højere grad afhængige af net- og informationssystemer for at drive deres kernevirksomhed. Tingenes Internet forbinder genstande og personer via kommunikationsnet. Denne nye virkelighed skaber hidtil usete muligheder og også sårbarheder. Cyberhændelser er i kraftig vækst. Deres kompleksitet, hyppighed og "overfladevirkningerne" - fra adgang til væsentlige tjenester til demokratiske processer — forventes at tiltage yderligere.

I denne forbindelse er der konstateret følgende indbyrdes forbundne problemer:

- Opsplitning af politikker og strategier for cybersikkerhed på tværs af medlemsstaterne.
- Spredte ressourcer og tilgange til cybersikkerhed på tværs af EU's institutioner, agenturer og organer.
- Utilstrækkeligt kendskab hos borgerne og virksomhederne for så vidt angår cybertrusler og utilstrækkelig oplysning om sikkerhedsegenskaberne ved de IKT-produkter og -tjenester, som de køber, i sammenhæng med den tiltagende forekomst af flere nationale og sektorielle certificeringsordninger.

Disse problemer har indvirkning på den samlede cybermodstandsdygtighed i EU og det indre markeds effektive funktion.

Hvilke resultater forventes der?

Initiativets specifikke mål er følgende:

1. Øgede kapaciteter og beredskab i medlemsstaterne og virksomhederne, navnlig hvad angår kritiske infrastrukturer.
2. Forbedret samarbejde og samordning mellem medlemsstaterne og EU's institutioner, agenturer og organer.
3. Øget kapacitet på EU-niveau til at supplere medlemsstaternes indsats, navnlig i tilfælde af grænseoverskridende cyberkriser.
4. Øget oplysning til borgere og virksomhederne om cybersikkerhedsanliggender.
5. Øget overordnet gennemsigtighed af cybersikkerhedstillidsniveauet for IKT-produkter og -tjenester med sigte på at styrke tilliden til det digitale indre marked og digital innovation.
6. Undgåelse af opsplitning af certificeringsordningerne i EU og dermed forbundne sikkerhedskrav og evalueringskriterier på tværs af medlemsstater og sektorer.

Hvad er merværdien ved at handle på EU-plan?

Eftersom digitalisering og konnektiviteten af økonomien og samfundet har en global dimension, rækker problemerne langt ud over en enkelt medlemsstats område. Der er derfor

behov for en indsats på EU-plan. I den nuværende situation og med sigte på de fremtidige scenarier ser det ud til, at individuelle tiltag fra medlemsstaternes side og en fragmenteret tilgang til cybersikkerhed, navnlig i lyset af den stærke grænseoverskridende dimension, ikke vil kunne øge Unionens kollektive cybermodstandsdygtighed.

B. LØSNINGER

Hvilke forskellige muligheder er der for at nå målene? Foretrækkes én løsning frem for andre?

I denne konsekvensanalyse undersøges et specifikt sæt politiske løsningsmodeller, som dækker revisionen af Den Europæiske Unions Agentur for Net- og Informationssikkerhed (ENISA) og IKT-sikkerhedscertificering.

ENISA-revisionen

Løsningsmodel 0 - **Referencescenarie** - Denne løsning bibeholder den nuværende situation. ENISA's mandat ville blive forlænget og Agenturets mål og opgaver vil forblive stort set uændret, idet der dog tages hensyn til de opgaver, som ENISA tillægges ved senere EU-lovgivning (f.eks. NIS-direktivet).

Løsningsmodel 1 - **Udløb af ENISA's mandat** (ENISA lukkes). Denne løsning indebærer lukningen af ENISA ved afslutningen af dets mandat (juni 2020) og eventuelt en omfordeling af kompetencer/aktiviteter på EU-plan og/eller nationalt plan.

Løsningsmodel 2 - **et "reformeret ENISA"**. Denne løsning ville bygge på det nuværende mandat for ENISA med henblik på at vedtage selektive ændringer, som kan tage højde for udviklingen på cybersikkerhedsområdet. Agenturet ville få et permanent mandat baseret på følgende centrale elementer: støtte til udarbejdelse og gennemførelse af EU-politikker, kapacitetsopbygning, viden og information, markedsrelaterede opgaver, forskning og innovation og operationelt samarbejde og krisestyring.

Løsningsmodel 3 - **et EU-agentur for cybersikkerhed med fuld operationel kapacitet**. Denne løsning indebærer en reform af ENISA ved at samle de tre vigtigste funktioner: 1. En politisk/rådgivende funktion, 2. et viden- og ekspertisecenter, og 3. en IT-beredskabsenhed (Computer Emergency Response Team - CERT). I vidt omfang vil denne løsning indebære samme ændring i omfanget af mandatet som løsningsmodel 2. Der ville komme yderligere opgaver til inden for beredskab og krisestyring, således at Agenturet ville dække hele cybersikkerhedslivscyklussen og håndtere forebyggelse, opdagelse og reaktion på cyberhændelser.

Certificering

Løsningsmodel 0 - Referencescenarie - Ingen foranstaltninger. Denne løsning indebærer, at Kommissionen ville bibeholde den nuværende situation og ikke iværksætte politiske eller lovgivningsmæssige tiltag.

Løsningsmodel 1 - **Ikkelovgivningsmæssige foranstaltninger ("blød lovgivning")**. Denne løsning indebærer, at Kommissionen bruger "bløde" politikinstrumenter (f.eks. fortolkningsmeddelelser, støtte til EU-dækkende selvregulerende initiativer og standardiseringsaktiviteter) for at forbedre gennemsigtigheden og mindske opsplitningen.

<u>Løsningsmodel 2</u> - En EU-retsakt, som udvider SOG-IS-aftalen, så den omfatter samtlige medlemsstater. Denne løsning indebærer, at Kommissionen foreslår en retsakt for at udvide medlemskabet til at være retligt bindende for alle medlemsstater.

<u>Løsningsmodel 3</u> - En **generel EU-ramme for IKT-sikkerhedscertificering**. Denne løsning indebærer oprettelsen af en europæisk certificeringsramme for IKT-sikkerhed (herunder en ekspertgruppe bestående af nationale myndigheder) ved i videst muligt omfang at bygge videre på eksisterende IKT-sikkerhedscertificeringsordninger. Rammen ville gøre det muligt at oprette EU-certificeringsordninger, som accepteres i alle medlemsstater.

Den foretrukne løsning er en kombination af løsningsmodel 2 for ENISA og løsningsmodel 3 for certificering.

Hvem er de forskellige interessenter? Hvem støtter hvilken løsning?

Størstedelen af interessenterne på tværs af alle kategorier (medlemsstater, erhvervslivet, EU-institutioner, forskerkredse), som deltog i høringerne, synes at bifalde den foretrukne løsningsmodel, idet de går ind for en styrkelse af ENISA og oprettelsen af en europæisk ramme for IKT-sikkerhedscertificering.

Der er navnlig enighed om behovet for at have (som minimum) et velfungerende EU-agentur med et permanent mandat, som har tilstrækkelige ressourcer og mandat til at imødegå de nuværende og fremtidige udfordringer inden for cybersikkerhed. Der er også bred enighed blandt interessenterne om at oprette en frivillig skalerbar europæisk ramme.

På erhvervssiden støttes denne løsningsmodel for certificering af virksomheder, som allerede er underlagt certificeringskrav, og som ville have gavn af en EU-dækkende mekanisme, der bygger på gensidig anerkendelse af attester. Den støttes også af SMV, der ellers ville skuldre den største byrde, hvis de allerede skal eller ville skulle iværksætte forskellige certificeringstiltag i forskellige medlemsstater. Nogle medlemsstater, herunder navnlig dem med få ressourcer, og nogle repræsentanter fra erhvervslivet og EU's institutioner udtalte sig også positivt om løsningsmodel 3 for ENISA.

C. DEN FORETRUKNE LØSNINGS VIRKNINGER

Hvilke fordele er der ved den foretrukne løsning (hvis en bestemt løsning foretrækkes – ellers fordelene ved de vigtigste af de mulige løsninger)?

Den foretrukne løsningsmodel giver EU et agentur, der er fokuseret på at yde støtte til medlemsstaterne, EU-institutioner og virksomheder på områder, hvor det vil give størst merværdi. Disse omfatter: støtte til gennemførelse af NIS-direktivet, udvikling og gennemførelse af politikker, information, viden og højnet oplysningsniveau, forskning, operationelt samarbejde og krisestyring, indre marked. ENISA vil navnlig støtte EU's politik inden for IKT-sikkerhedscertificering ved at sikre det administrative vedligehold og den tekniske forvaltning af en europæisk ramme for IKT-sikkerhedscertificering. En sådan ramme vil i praksis indføre et sæt regler for forvaltning af IKT-sikkerhedscertificering i EU, hvilket vil fremme et system med gensidig anerkendelse af attester udstedt i medlemsstaterne. Den løsningsmodel, som kombinerer disse muligheder, er vurderet som den mest effektive for EU til at nå de identificerede mål: øget cybersikkerhedskapacitet, beredskab, samarbejde, højnet

oplysningsniveau, transparens og undgåelse af markedsopsplitning. Denne løsningsmodel er også den, der hænger bedst sammen med de politiske prioriteter i EU's strategi for cybersikkerhed og de tilknyttede politikker (f.eks. NIS-direktivet) samt strategien for det digitale indre marked. Denne løsning ville ydermere nå målene gennem en fornuftig brug af ressourcer.

Hvilke omkostninger er der ved den foretrukne løsning (hvis en bestemt løsning foretrækkes – ellers omkostningerne ved de vigtigste af de mulige løsninger)?

Til trods for at det får nye roller, vil et "reformeret ENISA" forblive en omstilingsparat organisation. Det nødvendige finansielle bidrag fra EU's budget ville være større end i dag, men vil fortsat ligge under bidraget til andre agenturer, som også opererer på kritiske områder.

Oprettelsen af en europæisk ramme for IKT-sikkerhedscertificering vil ikke indebære ekstra startomkostninger for erhvervslivet (herunder SMV). Den vil snarere give betydelige besparelser for de virksomheder, der allerede certificerer deres produkter, eller som er villige til at få foretaget sikkerhedscertificering, hvilket gavner deres konkurrenceevne på verdensplan. Den vil dog på den anden side indebære visse budgetmæssige forpligtelser for at sikre, at rammen vedligeholdes, hvilket først og fremmest vil skulle gøres via den "reformerede ENISA"-løsning, hvad angår tekniske opgaver og sekretariatsopgaver.

Vil det have stor indvirkning på de nationale budgetter og myndigheder?

Nej. Omkostningerne ved at styrke ENISA vil primært blive afholdt over EU-budgettet, medens medlemsstaterne stadig har mulighed for at yde frivillige finansielle bidrag til Agenturet. Hvad angår certificering, vil den vigtigste indvirkning på de nationale budgetter og myndigheder følge af oprettelsen af en certificeringsmyndighed, når det er relevant.

Vil den foretrukne løsning få andre væsentlige virkninger?

Nej.

Proportionalitet?

Den foretrukne løsning omfatter afbalancerede foranstaltninger, som alle vurderes at være nødvendige for at nå de relevante mål uden at pålægge de pågældende interessenter for store byrder. I dette lys anses initiativet for at være i overensstemmelse med proportionalitetsprincippet.

D. OPFØLGNING

Hvornår vil foranstaltningen blive taget op til fornyet overvejelse?

Det foreslås, at den første evaluering finder sted fem år efter retsaktens ikrafttræden. Kommissionen aflægger efterfølgende beretning til Europa-Parlamentet og Rådet om evalueringen, i givet fald ledsaget af et forslag til revision. Yderligere evalueringer foretages hvert femte år.