Europaudvalget 2020
KOM (2020) 0823
Offentligt

EUROPA-
KOMMISSIONEN

Bruxelles, den 16.12.2020
SWD(2020) 344 final

ARBEJDSDOKUMENT FRA KOMMISSIONENS TJENESTEGRENE

RESUMÉ AF RAPPORTEN OM KONSEKVENSANALYSEN

Ledsagedokument til

forslag til Europa-Parlamentets og Rådets direktiv

om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen og om ophævelse af direktiv (EU) 2016/1148

{COM(2020) 823 final} - {SEC(2020) 430 final} - {SWD(2020) 345 final}

Resumé

Konsekvensanalyse af evalueringen af Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (NIS-direktivet).

A. Behov for handling

Hvad er problemet, og hvorfor er det et problem på EU-niveau?

På trods af dets bemærkelsesværdige resultater har NIS-direktivet, som banede vejen for en betydelig ændring i tankegangen vedrørende samt den institutionelle og lovgivningsmæssige tilgang til cybersikkerhed i mange medlemsstater, nu også vist sine begrænsninger. Den digitale omstilling af samfundet (intensiveret af covid-19-krisen) har udvidet trusselsbilledet og skaber nye udfordringer, som kræver tilpassede og innovative løsninger. Antallet af cyberangreb er fortsat stigende, idet der kommer stadig mere sofistikerede angreb fra en bred vifte af kilder i og uden for EU.

På grundlag af evalueringen af, hvordan NIS-direktivet fungerer, blev der i konsekvensanalysen identificeret følgende problemer: Den lave grad af cyberrobusthed hos virksomheder, der opererer i EU; den inkonsekvente modstandsdygtighed på tværs af medlemsstater og sektorer og det lave niveau af fælles situationsbevidsthed og manglen på fælles kriserespons. Som følge af nogle af disse problemer og drivkræfter opstår der f.eks. situationer, hvor større hospitaler i en medlemsstat ikke er omfattet af NIS-direktivets anvendelsesområde og derfor ikke er forpligtet til at gennemføre de deraf følgende sikkerhedsforanstaltninger, mens næsten alle landets hospitaler i en anden medlemsstat er omfattet af NIS-sikkerhedskravene.

Hvad bør opnås?

Der er planlagt tre generelle mål for evalueringen af NIS:

1. **Øge cyberrobustheden i et omfattende sæt af virksomheder, der opererer i Den Europæiske Union, på tværs af alle relevante sektorer** ved at indføre regler, der sikrer, at alle offentlige og private enheder i hele det indre marked, som varetager vigtige funktioner for økonomien og samfundet som helhed, er forpligtet til at træffe passende cybersikkerhedsforanstaltninger.
2. **Mindske inkonsekvens i modstandsdygtigheden på tværs af det indre marked i de sektorer, der allerede er omfattet af direktivet,** ved yderligere at tilpasse 1) det faktiske anvendelsesområde, 2) kravene til sikkerheds- og hændelsesrapportering, 3) bestemmelserne om nationalt tilsyn og håndhævelse og 4) de kompetente myndigheders kapacitet i medlemsstaterne.
3. Forbedre **niveauet af fælles situationsbevidsthed og den kollektive evne til at forberede sig og reagere** ved at træffe foranstaltninger, der skal øge tilliden mellem de kompetente myndigheder, udveksle flere oplysninger og fastsætte regler og procedurer i tilfælde af en omfattende hændelse eller krise.

Hvad er merværdien ved at handle på EU-plan (nærhedsprincippet)?

Modstandsdygtigheden over for cybertrusler i hele Unionen kan ikke være effektiv, hvis der gribes ind på en uensartet måde gennem nationale eller regionale siloer. NIS-direktivet har til formål at afhjælpe denne mangel ved at fastlægge en ramme for net- og informationssystemernes sikkerhed på nationalt plan og EU-plan. Omsætningen og gennemførelsen af direktivet afslørede imidlertid også iboende mangler ved visse bestemmelser eller fremgangsmåder, såsom den uklare afgrænsning af NIS-direktivets anvendelsesområde. Siden covid-19-krisen er den europæiske økonomi desuden blevet mere afhængig af

net- og informationssystemer end nogensinde før, og sektorer og tjenester er i stigende grad indbyrdes forbundne. Den første periodiske evaluering af NIS-direktivet skabte derfor mulighed for yderligere EU-tiltag. En EU-indsats, der går videre end de nuværende foranstaltninger i NIS-direktivet, er primært begrundet i: i) problemets grænseoverskridende karakter, ii) EU-indsatsens potentiale til at forbedre og fremme effektive nationale politikker og iii) bidraget fra samordnede og samarbejdsbaserede politiske foranstaltninger vedrørende net og informationssikkerhed til effektiv beskyttelse af databeskyttelse og privatlivets fred.

B. Løsninger

Hvilke forskellige løsninger er der for at nå målene? Foretrækkes en bestemt løsning frem for andre? Hvis ikke, hvorfor?

Konsekvensanalysen behandlede fire politiske løsningsmodeller: 0) bevarelse af status quo, 1) ikkelovgivningsmæssige foranstaltninger til tilpasning af gennemførelsen, 2) begrænsede ændringer af NIS-direktivet med henblik på yderligere harmonisering og 3) systemiske og strukturelle ændringer af NIS-direktivet. Løsningsmodel 1 blev forkastet på et tidligt tidspunkt, da den ikke afviger væsentligt fra status quo. I konsekvensanalysen konkluderes det, at den **foretrukne løsningsmodel** er løsningsmodel 3 (dvs. **systemiske og strukturelle ændringer af NIS-rammen**), da den vil indebære en mere grundlæggende ændring af tilgangen med henblik på at omfatte et større segment af økonomierne i hele Unionen, men dog med et mere fokuseret tilsyn, der er proportionalt målrettet store og centrale virksomheder, samtidig med at anvendelsesområdet fastlægges klart. Den vil også strømline og yderligere harmonisere virksomhedernes sikkerhedsrelaterede forpligtelser, skabe en mere effektiv ramme for operationelle aspekter samt fastlægge et klart grundlag for de relevante aktørers fælles ansvar og ansvarlighed samt tilskynde til udveksling af oplysninger.

Hvad er de forskellige interessenters holdning? Hvem støtter hvilken løsning?

De fleste kompetente myndigheder og virksomheder udtrykte støtte til en revision af NIS-direktivet. Gennem flere høringer gav de udtryk for, at et revideret NIS-direktiv bør omfatte yderligere (under)sektorer samt tilpasse eller strømline yderligere sikkerhedsforanstaltninger og rapporteringsforpligtelser. Interessenterne udtrykte ligeledes støtte til nye koncepter eller politikrelaterede foranstaltninger, som kun er en del af den foretrukne løsningsmodel (f.eks. politikker for forsyningskædesikkerhed, institutionalisering af en operationel EU-krisestyringsramme).

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 vil medføre betydelige fordele: Skøn foretaget på grundlag af en økonomisk model, der er udviklet inden for en støtteundersøgelse til evalueringen af NIS-direktivet, viser, at den foretrukne løsning kan føre til en reduktion af omkostningerne ved cybersikkerhedshændelser på 11,3 mia. EUR.

Det sektorspecifikke anvendelsesområde vil blive udvidet betydeligt inden for rammerne af NIS-rammen, men ud over ovennævnte fordele vil den byrde, der kan opstå som følge af NIS-kravene, navnlig ud fra et tilsynsperspektiv, også være afbalanceret for såvel de nye enheder, der skal dækkes, som de kompetente myndigheder. Dette skyldes, at den nye NIS-ramme vil indføre en tostrenget tilgang med fokus på store og centrale enheder og en differentiering af tilsynsordninger, der kun tillader efterfølgende tilsyn (dvs. reaktivt og uden en generel forpligtelse til systematisk at dokumentere overholdelse) for et stort antal

enheder, navnlig dem, der betragtes som "vigtige", men som endnu ikke er "væsentlige".

Overordnet set vil den foretrukne løsningsmodel føre til effektive afvejninger og synergier med det bedste potentiale blandt alle de analyserede politiske løsningsmodeller og sikre en øget og konsekvent grad af cyberrobusthed hos centrale enheder i hele Unionen, hvilket i sidste ende vil føre til omkostningsbesparelser for både virksomheder og samfundet.

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

Den foretrukne løsningsmodel vil medføre visse overholdelses- og håndhævelsesomkostninger for de relevante myndigheder i medlemsstaterne (der blev anslået en samlet stigning på ca. 20-30 % af ressourcerne). Den nye ramme vil imidlertid også medføre betydelige fordele takket være et bedre overblik over og interaktion med centrale virksomheder, øget grænseoverskridende operationelt samarbejde samt gensidig bistand og peerevalueringsmekanismer. Dette vil føre til en generel forøgelse af cybersikkerhedskapaciteterne på tværs af medlemsstaterne.

For de virksomheder, der vil være omfattet af NIS-rammen, anslås det, at deres nuværende udgifter til IKT-sikkerhed vil skulle øges med 22 % i de første år efter indførelsen af den nye NIS-ramme (dette vil være 12 % for virksomheder, der allerede er omfattet af det nuværende NIS-direktiv). Denne gennemsnitlige stigning i udgifterne til IKT-sikkerhed vil imidlertid medføre en forholdsmæssig fordel ved sådanne investeringer, navnlig på grund af en betydelig reduktion af omkostningerne ved cybersikkerhedshændelser (som anslås til 11,3 mia. EUR over 10 år).

Hvad er indvirkningerne på SMV'er og konkurrencedygtighed?

Små virksomheder og mikrovirksomheder vil blive undtaget fra NIS-rammens anvendelsesområde under den foretrukne løsningsmodel. For mellemstore virksomheder kan det forventes, at der vil ske en stigning i udgifterne til IKT-sikkerhed i de første år efter indførelsen af den nye NIS-ramme. Samtidig vil en styrkelse af sikkerhedsniveauet for disse enheder også kunne tilskynde dem til at styrke deres cybersikkerhedskapaciteter og bidrage til en forbedring af deres IKT-risikostyring.

Vil den foretrukne løsning få væsentlige virkninger for de nationale budgetter og myndigheder?

Den foretrukne løsning vil have virkninger for de nationale budgetter og myndigheder: Der forventes en stigning på omkring 20-30 % af ressourcerne på kort og mellemlang sigt.

Vil den foretrukne løsning få andre væsentlige virkninger?

Der forventes ingen andre væsentlige eller negative virkninger. Den foretrukne løsningsmodel forventes at føre til mere robuste cybersikkerhedskapaciteter og vil derfor have en større afbødende virkning på antallet og alvoren af hændelser, herunder brud på datasikkerheden. Den vil sandsynligvis også have en positiv indvirkning med hensyn til at sikre lige vilkår på tværs af medlemsstaterne for alle enheder, der er omfattet af anvendelsesområdet for net- og informationssikkerhed, og mindske asymmetrier i cybersikkerhedsoplysninger.

Proportionalitet?

Den foretrukne løsning går ikke ud over, hvad der er nødvendigt for at opfylde de specifikke mål på tilfredsstillende vis. Den planlagte tilpasning og strømlining af sikkerhedsforanstaltninger og rapporteringsforpligtelser vedrører medlemsstaternes og virksomhedernes anmodninger om at forbedre den nuværende ramme.

D. Opfølgning
Hvornår vil foranstaltningen blive taget op til fornyet overvejelse?
Den første evaluering gennemføres 54 måneder efter retsaktens ikrafttræden. Kommissionen aflægger rapport til Europa-Parlamentet og Rådet om sin evaluering. Evalueringen vil blive udarbejdet med støtte fra ENISA og samarbejdsgruppen.