EUROPA-
KOMMISSIONEN

Bruxelles, den 24.9.2020
SWD(2020) 199 final

ARBEJDSDOKUMENT FRA KOMMISSIONENS TJENESTEGRENE

RESUMÉ AF RAPPORTEN OM KONSEKVENSANALYSEN

Ledsagedokument til

Forslag til Europa-Parlamentets og Rådets forordning

om digital operationel modstandsdygtighed i den finansielle sektor og om ændring af forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014 og (EU) nr. 909/2014

{COM(2020) 595 final} - {SEC(2020) 307 final} - {SWD(2020) 198 final}

Resumé

Konsekvensanalyse af forslaget til forordning om digital operationel modstandsdygtighed i den finansielle sektor

A. Behov for handling

Hvorfor? Hvad er problemstillingen?

Den finansielle sektor beror i vid udstrækning af informations- og kommunikationsteknologier (IKT). Den nuværende covid-19-pandemi vil sandsynligvis øge dette fænomen, da det indebærer fordele at sikre løbende fjernadgang til finansielle tjenesteydelser. Afhængighed af digitale teknologier indebærer dog visse problemstillinger: Virksomheder skal være i stand til at modstå potentielle IKT-forstyrrelser, således at digitale hændelser og trusler imødegås og tjenesterne opretholdes. Selv om sårbarheder, der skyldes IKT-afhængighed, gør sig gældende i alle økonomiske sektorer, er de særligt udtalte i den finansielle sektor, hvor der er en høj grad af indbyrdes forbundethed, og hvor der tages grænseoverskridende vigtige tjenester i brug, som realøkonomien er afhængig af. Dette skyldes 1) den dybtgående og udbredte brug af IKT og 2) potentialet for, at virkningerne af en operationel hændelse i en finansiel virksomhed eller finansiel delsektor hurtigt kan sprede sig til andre virksomheder eller dele af den finansielle sektor og i sidste ende til resten af økonomien.

På trods af at den finansielle sektor er meget avanceret på sit marked og med hensyn til lovgivningsmæssig integration, og at den er velfungerende på baggrund af et sæt harmoniserede regler — det fælles EU-regelsæt — har EU's indsats i forhold til behovene for øget operationel modstandsdygtighed både på horisontalt plan og sektorplan været enten:

- baseret på minimumsharmonisering og dermed givet mulighed for nationale fortolkninger og fragmentering i det indre marked eller
- for generel og med begrænset anvendelse, idet den i varierende grad imødegår overordnede operationelle risici, delvist regulerer nogle komponenter af digital operationel modstandsdygtighed (f.eks. IKT-risikostyring, indberetning af IKT-hændelser og IKT-tredjepartsrisici) og samtidig udelader andre (afprøvning).

EU's indsats har indtil videre ikke imødegået operationelle risici på en måde, der modsvarer finansielle virksomheders behov for modstandsdygtighed og indsats over for og genopretning efter IKT-sårbarheder. Den udstyrer heller ikke finansielle tilsynsmyndigheder med de værktøjer, de skal bruge, for at opfylde deres mandat til at dæmme op for finansiel ustabilitet, der opstår som følge af sådanne IKT-sårbarheder.

De nuværende huller og uoverensstemmelser har ført til en udbredelse af ukoordinerede nationale initiativer (f.eks. vedrørende afprøvning) og tilsynsmæssige tilgange (f.eks. til afhængighed af IKT-tredjeparter), som udmønter sig enten i overlapninger, duplikationer af krav og høje administrative omkostninger og overholdelsesomkostninger for grænseoverskridende finansielle virksomheder eller i, at IKT-risici ikke detekteres og imødegås. Overordnet set er der ikke sikret stabilitet og integritet i den finansielle sektor, og det indre marked for finansielle tjenesteydelser er fortsat fragmenteret, hvilket medfører, at forbruger- og investorbeskyttelsen svækkes.

Hvilke resultater forventes der af initiativet?

Det overordnede mål er at styrke den digitale operationelle modstandsdygtighed i EU's finansielle sektor ved at strømline og ajourføre EU's nuværende finansielle lovgivning og indføre nye krav de steder, hvor der er huller, for at

- forbedre finansielle virksomheders styring af IKT-risici
- øge tilsynsmyndigheders kendskab til trusler og hændelser
- forbedre finansielle virksomheders afprøvning af deres IKT-systemer og
- sikre en overvågning af risici, der opstår som følge af finansielle virksomheders afhængighed af tredjepartsudbydere af IKT-tjenester.

Mere specifikt vil forslaget skabe mere sammenhængende og konsekvente mekanismer til indberetning af hændelser og dermed reducere den administrative byrde for finansielle institutioner og styrke effektiviteten af tilsynet.

Hvad er merværdien ved at handle på EU-plan?

EU's indre marked for finansielle tjenesteydelser er reguleret af et omfattende sæt regler, der er fastsat på EU-plan, hvorved finansielle virksomheder, der er meddelt tilladelse i en medlemsstat, har mulighed for at levere tjenester i hele det indre marked takket være en EU-pasordning. Som resultat udgør regler på nationalt plan ikke en effektiv metode til at styrke den operationelle modstandsdygtighed i finansielle virksomheder, som anvender pasordningen. Derudover indeholder det fælles EU-regelsæt som følge af den finansielle krise meget detaljerede og præskriptive regler, der tager sigte på mere "traditionelle" risici, f.eks. kredit-, modparts-, markeds- og likviditetsrisici. De eksisterende regler om operationelle risici er fortsat generelle. Styrkelse af digital operationel modstandsdygtighed kræver tilpasninger af de bestemmelser om operationelle risici, der allerede er

fastsat på EU-plan — og som derfor kun kan ajourføres og suppleres på EU-plan.

B. Løsninger

Hvilke lovgivningsmæssige og ikkelovgivningsmæssige løsninger er overvejet? Foretrækkes en bestemt løsning frem for andre? Hvorfor?

Foruden et basisscenarie, hvor der ikke træffes nogen foranstaltninger med hensyn til EU-lovgivningen om finansielle tjenesteydelser, tages tre løsninger op til overvejelse i konsekvensanalysen. Nærmere bestemt:

- **"Ingen foranstaltninger"**: Der vil fortsat blive fastsat regler om operationel modstandsdygtighed i henhold til det nuværende, divergerende sæt EU-bestemmelser om finansielle tjenesteydelser, delvist under NIS-direktivet, og i henhold til eksisterende eller fremtidige nationale ordninger.
- **Løsning 1 — Styrkelse af kapitalbuffere**: Der vil blive indført en supplerende kapitalbuffer for at øge finansielle virksomheders evne til at dække tab, der kan opstå som følge af manglende operationel modstandsdygtighed.
- **Løsning 2 — Indførelse af en retsakt om digital operationel modstandsdygtighed i forbindelse med finansielle tjenesteydelser**: Der vil blive indført en udførlig ramme på EU-plan, som fastsætter regler om digital operationel modstandsdygtighed for alle regulerede finansielle institutioner, og som
  - vil imødegå IKT-risici på mere omfattende vis
  - vil give finansielle tilsynsmyndigheder mulighed for at få adgang til oplysninger om IKT-relaterede hændelser
  - vil sikre, at de finansielle virksomheder vurderer effektiviteten af deres forebyggende foranstaltninger og foranstaltninger vedrørende modstandsdygtighed og identificerer IKT-sårbarheder
  - vil styrke de regler om outsourcing, der regulerer det indirekte tilsyn med tredjepartsudbydere af IKT-tjenester
  - vil give mulighed for at føre direkte tilsyn med de aktiviteter, som tredjepartsudbydere af IKT-tjenester udfører, når de leverer deres tjenester til finansielle virksomheder, og
  - eventuelt vil give incitament til udveksling af trusselsefterretninger i den finansielle sektor.
- **Løsning 3 — En retsakt om modstandsdygtighed kombineret med et centraliseret tilsyn med kritiske tredjepartsudbydere**: Foruden en retsakt om operationel modstandsdygtighed (løsning 2), oprettes der en ny myndighed, som skal føre tilsyn med IKT-tredjepartsudbydere, som leverer kritiske IKT-tjenester til finansielle virksomheder. Det vil også sikre en klarere afgrænsning af den finansielle sektor i forhold til anvendelsesområdet for NIS-direktivet.

Løsning 2 er den foretrukne løsning. I sammenligning med de andre løsninger er det den løsning, der opfylder flest af initiativets mål, samtidig med at den tager hensyn til kriterierne om effektivitet og sammenhæng. Det er også denne løsning, der nyder størst opbakning blandt interessenterne.

Hvem støtter hvilken løsning?

De fleste interessenter (private, offentlige) er enige i, at der er behov for en EU-indsats for bedre at beskytte finansielle virksomheders operationelle modstandsdygtighed. Mange mener også, at en EU-indsats er nødvendig for at afhjælpe den reguleringsmæssige byrde, der skyldes, at finansielle virksomheder underkastes overlappende eller inkonsekvente regler, som er fastsat i NIS-direktivet, EU-retten om finansielle tjenesteydelser og nationale ordninger (f.eks. med hensyn til indberetning af hændelser). Ganske få interessenter støtter således, at der ikke træffes foranstaltninger. Nogle få interessenter ser en fordel i at lade den operationelle modstandsdygtig beskytte ved hjælp af øgede kapitalbuffere (løsning 1). Dette er imidlertid den traditionelle tilgang til operationelle risici, navnlig inden for bankvirksomhed, og betragtes som sådan af f.eks. internationale standardiseringsorganisationer. Den type kvalitative foranstaltninger, som fastsættes i løsning 2, og som vil strømline og ajourføre den finansielle EU-lovgivning og indføre nye krav de steder, hvor der er huller, samtidig med at forbindelserne til det horisontale NIS-direktiv opretholdes, høster bred opbakning blandt de interessenter, der besvarede den offentlige høring. Mens nogle interessenter (navnlig offentlige) ser en fordel i et øget tilsyn med tredjepartsudbydere af IKT-tjenester som i løsning 3, nyder oprettelsen af en ny EU-myndighed til dette formål kun begrænset opbakning blandt interessenterne, og det samme gør et mere fuldstændigt brud med NIS-rammen.

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)?

Løsning 2 tager sigte på **IKT-risici** i hele den finansielle sektor ved at øge finansielle institutioners kapaciteter til at modstå IKT-hændelser. Dette vil reducere risikoen for, at en cyberhændelse hurtigt spreder sig på tværs af finansielle markeder. Det er vanskeligt at foretage et skøn over de omkostninger, der er forbundet med

operationelle hændelser i den finansielle sektor (ikke alle hændelser indberettes; omfanget af omkostninger er usikkert), men vurderinger i sektoren tyder på, at omkostningerne i EU's finansielle sektor ligger et sted mellem 2-27 mia. EUR om året. Den foretrukne løsning vil afhjælpe disse omkostninger og eventuelle bredere virkninger, som større cyberhændelser kan få for den finansielle stabilitet. Afskaffelse af overlappende **krav til indberetning** vil mindske den administrative byrde. For eksempel kan de dermed forbundne besparelser for nogle af de største banker udgøre et sted mellem 40-100 mio. EUR om året. Direkte indberetning vil også øge tilsynsmyndighedernes kendskab til IKT-hændelser. **Harmoniserede afprøvningsmetoder** vil sikre øget detektion af ukendte sårbarheder og risici. De vil også medføre et fald i omkostningerne, navnlig for grænseoverskridende virksomheder. For eksempel vil de samlede forventede fordele ved en fælles tilgang for de 44 største grænseoverskridende banker udgøre et sted mellem 11-88 mio. EUR. Ved at indføre et sammenhængende sæt regler om styring af risici forbundet med **tredjepartsudbydere af IKT-tjenester** vil finansielle virksomheder kunne udøve mere kontrol med, hvordan tredjepartsudbydere af IKT-tjenester efterlever lovrammen, hvilket kan give tilsynsmyndighederne sikkerhed. Det vil også indebære tilsynsmæssige fordele som følge af tilsynet med tredjepartsudbydere af IKT-tjenester. Overordnet set udmønter den foretrukne løsning sig i bredere samfundsmæssige fordele som følge af et mere modstandsdygtigt operativmiljø for alle finansielle markedsdeltagere samt styrket forbruger- og investorbeskyttelse.

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

Den foretrukne løsning vil give anledning til både engangsomkostninger og tilbagevendende omkostninger. Med hensyn til førstnævnte skyldes disse investeringer i IT-systemer og er vanskelige at sætte tal på, da virksomhedernes nedarvede systemer er i forskellig stand. I mangel af reguleringsmæssige indgreb har nogle virksomheder allerede foretaget væsentlige investeringer i IT-systemer. Dette betyder, at omkostningerne for større finansielle virksomheder i forbindelse med gennemførelse af foranstaltningerne i dette forslag sandsynligvis vil være begrænsede. For mindre virksomheder forventes omkostningerne også at være begrænsede, da de vil være omfattet af mindre strenge foranstaltninger, som står i rimeligt forhold til deres lavere risici. For så vidt angår afprøvning har de europæiske tilsynsmyndigheder vurderet, at de omkostninger, der er forbundet med trusselsbaserede penetrationstest, udgør et sted mellem 0,1 % og 0,3 % af de berørte virksomheders samlede IKT-budget. Omkostninger forbundet med indberetning af hændelser vil blive drastisk reduceret, da der ikke vil være nogen overlapninger med indberetningen under NIS-direktivet. Tilsynsmyndigheder vil også pådrage sig nogle omkostninger som følge af de yderligere opgaver, som de vil påtage sig. For eksempel kan stigningen i antallet af FTÆ'er for tilsynsmyndigheder, der deltager i det direkte tilsyn med tredjepartsudbydere af IKT-tjenester, forventes at ligge et sted mellem 1-5 FTÆ'er pr. ledende tilsynsførende og på ca. 0,25 FTÆ'er pr. deltagende myndighed.

Hvordan påvirker den foretrukne løsning virksomhederne, herunder de små og mellemstore virksomheder og mikrovirksomhederne?

Den foretrukne løsning vil dække alle finansielle virksomheder for at øge den operationelle modstandsdygtighed i sektoren som helhed. Dette brede anvendelsesområde er vigtigt i lyset af den indbyrdes forbundethed i den finansielle sektor og det dertil svarende behov for at have en forsvarlig grad af overordnet operationel modstandsdygtighed overalt. Når der defineres centrale krav på tværs af de primære indsatsområder, finder proportionalitetsprincippet imidlertid både anvendelse på tværs af delsektorer og inden for den enkelte delsektor. Hermed tages der hensyn til bl.a. forskelle i form af forretningsmodeller, større, risikoprofil, systemisk betydning osv. Foranstaltninger vedrørende indberetning af hændelser og afprøvning vil for eksempel være mindre strenge for mindre finansielle virksomheder.

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

Nej. Dette supplerende tilsyn kan som påvist ovenfor kræve et begrænset antal yderligere tilsynsmæssige ressourcer, som helt eller delvist (hvis der indføres tilsynsgebyrer) kan afholdes over de offentlige budgetter.

Vil den foretrukne løsning få andre væsentlige virkninger?

De socioøkonomiske konsekvenser af covid-19-pandemien illustrerer, præcis hvor vigtige de finansielle markeder og deres operationelle modstandsdygtighed er. Den foretrukne løsning vil danne et solidt grundlag for at høste fordelene ved den digitale omstilling, idet der sikres operationel modstandsdygtighed for finansielle tjenesteydelser, herunder i bankunionen og kapitalmarkedsunionen, på grundlag af et sæt regler og krav, som skal skabe sikkerhed, gode resultater, stabilitet og lige vilkår. Dette vil også styrke Europas stilling som en førende finansiel og digital aktør på globalt plan, som er et mål, der er fastsat af Kommissionen i meddelelsen "Europas digitale fremtid i støbeskeen".

D. Opfølgning

Hvornår vil foranstaltningen blive taget op til fornyet overvejelse?
Den første revision gennemføres tre år efter det retlige instruments ikrafttræden. Kommissionen aflægger rapport til Europa-Parlamentet og Rådet om sin revision. Revisionen kan underbygges ved hjælp af en offentlig høring, undersøgelser, ekspertdrøftelser, spørgeundersøgelser, seminarer, alt efter hvad der er relevant.