Finanstilsynet

FINANS DANMARK

Positivt med et styrket cyberforsvar i den finansielle sektor i EU

Resumé

Finans Danmark glæder sig over forslaget fra EU-Kommissionen. Forslaget har fokus på at sikre en harmoniseret ramme for operationel modstandsdygtighed i den finansielle sektor i EU's indre marked. Det er positivt, at der med forordningen kommer fælles harmoniserede minimumskrav til sektoren i forhold til cyberforsvar. Generelt set er det vigtigt, at fordelene ved risikoreduktion opvejer omkostningerne ved de foranstaltninger, der træffes.

Det er væsentligt, at der fokuseres på en risikobaseret tilgang og proportionalitet i reguleringen på området. Dermed kan der skabes et reelt indre marked og sikres en bedre koordinering på tværs af medlemsstaterne.

Bestræbelserne på at etablere ensartede spilleregler for beskyttelse af alle dele af modstandskæden hilses velkommen.

Høringssvar

7. oktober 2020

Dok: FIDA-151247800-694946-v1

Kontakt Mette Stürup

Digital Operational Resilience Act (DORA)

Digital Operational Resilience

Finans Danmark glæder sig over forslaget fra EU-Kommissionen. Forslaget har fokus på at sikre en harmoniseret ramme for operationel modstandsdygtighed i den finansielle sektor i EU's indre marked. Der er imidlertid tale om et meget omfattende forslag, derfor er der behov for at analysere detaljerne nærmere i den kommende tid. Generelt set er det vigtigt, at fordelene ved risikoreduktion opvejer omkostningerne ved de foranstaltninger, der træffes.

Høringssvar

7. oktober 2020
Dok. nr.:
FIDA-151247800-694946-v1

Det er væsentligt, at der fokuseres på en risikobaseret tilgang, og at der skabes sammenhængende lovgivningskrav og bedre koordinering på tværs af medlemsstaterne. Bestræbelserne på at etablere ensartede spilleregler for beskyttelse af alle dele af modstandskæden hilses velkommen.

Det er væsentligt, at der ikke fremadrettet vil blive iværksat nationale initiativer parallelt. Dette kan resultere i uoverensstemmelser, overlappende krav og høje administrations- og efterlevelsesomkostninger. Som EU-Kommissionen påpeger i forslaget, kan dette føre til, at IKT-risici forbliver uopdagede og dermed uløste.

Et positivt resultat af Covid-19-krisen har været det øgede samarbejde mellem finansielle institutioner i forbindelse med bekæmpelse af cyberkriminalitet. Mens de navigerede i pandemien, mødtes bankerne på en hidtil uset måde for at udveksle trusselsefterretninger og bedste praksis, ikke mindst gennem Nordic Financial CERT (NFCERT). Finance Denmark glæder sig over, at EU-Kommissionen som led i loven om operationel modstandsdygtighed præciserer forudsætningerne for, at institutionen kan udveksle oplysninger, herunder myndigheder. Det er væsentligt at sikre, at det bliver lettere at udveksle oplysninger.

Specifikke bemærkninger

Proportionalitet

Proportionalitet og risikobaseret tilgang er helt central. Dette synes dog ikke til stede i hele forslaget, f.eks. i afsnittet om kontrol af robusthed, da det indeholder en forpligtelse til at sikre, at alle identificerede svagheder og mangler, fuldstændig er løst. Dette synes ikke at være i overensstemmelse med anvendelsen af kvalitative og kvantitative vurderingskriterier. Et af formålene med retsakten er: *"reducing regulatory complexity, fosters supervisory convergence and increases*

legal certainty, this Regulation also contributes to limit financial entities' compliance costs, especially for those operating on a cross-border basis, which in turn would help remove competitive distortions". Men det er ikke klart, hvordan det rent faktisk vil fungere, da det umiddelbart er vurdering, at der bliver indført mange nye krav. Det kræver dog en nærmere analyse.

Målet om at harmonisere digitale modstandstest i hele EU er meget positivt, især gensidig anerkendelse af testresultater i forskellige jurisdiktioner.

Omfang

Passende med fokus på sammenhængende anvendelse og ensartede spilleregler til beskyttelse af alle dele af forsvarskæderne. Det er imidlertid vigtigt, at store organisationer kan stole på og engagere sig i mindre organisationer uden at skulle bekymre sig om eller påtage sig et stort ansvar for sikkerheden i den mindre organisation, som måske ikke er omfattet af forslaget.

Governance

Det er relevant og passende med aktiv og større rolle for ledelsesorganet for at sikre fokus på IKT-sikkerhed og -risiko. Denne større rolle for ledelsesorganet skal være mere detaljeret, f.eks. hvad regelmæssigt betyder, så forventninger er klare. Endvidere er der behov for klare regler for delegation.

It-risikostyring

Positivt med fokus på harmonisering. Det ser ud til, at der vil blive brugt betydelige ressourcer på rapportering til myndighederne. Dog ser det ikke ud til, at proportionaltetes princippet er implementeret it-risikostyringen. Det bør nærmere analyseres. Som led i artikel 14 vil der blive udarbejdet udkast til tekniske standarder. Disse vil sandsynligvis få stor indvirkning på de finansielle institutioner. Det er derfor vigtigt, at den finansielle sektor inddrages i udviklingen af disse tekniske standarder.

ICT-hændelser

Det er vigtigt og meget positivt med harmonisering af rapporteringsindhold og skabeloner, det er i dag meget komplekst. Det er ikke klart, om denne harmonisering vil fjerne indberetningspligten i henhold til f.eks. PSD2, NIS eller andre landespecifikke bestemmelser. Det bør afdækkes. Det er væsentligt at sikre en fuld harmonisering af alle EU-regler.

Test af digital driftsfleksibilitet

Det er relevant og hensigtsmæssigt at styrke test. I den danske implementering af TIBER er Nationalbanken myndighed for testprogrammet og gennemfører testene ud fra et hensyn om at understøtte den finansielle stabilitet. Der bør derfor være mulighed for videreføre den danske implementering. Derfor bør det fremgå at det kan være *relevante myndigheder* kan have myndighedsrollen. Det fremgår også at der skal testes mindst hvert tredje år. Dette er godt i tråd med forventningen i sektoren, men der kan være gode grunde til at afvige fra dette (fx corona). Det kunne i stedet formuleres med en "comply or explain"-tilgang. Derudover kunne der i DORA stilles krav om at kritiske leverandører deltager i testen, hvis de fx systemunderstøtter samfundskritiske funktioner.

Cloud/Tredjeparts IKT-risiko

Finans Danmark hilser det velkomment, at der sker en balanceret regulering af kritiske tredjeparts IKT-udbydere til den finansielle sektor, såsom udbydere af cloudtjenester.

Finans Danmark hilser forslaget om, at EU's tilsynsmyndigheder skal føre tilsyn med kritiske tjenesteudbydere, velkomment. Der er behov for at standardisere og strømline processer omkring tredjepartsudbydere. For at høste fordelene ved brug af tredjeparter er det afgørende, at overlapninger undgås mellem tilsynskontrol og de enkelte finansielle institutioners gennemførelse af kontrollen med tredjepartsudbydere. Vil en "certificering" af en kritisk udbyder kunne hjælpe banker af med visse byrder? I den forbindelse er det væsentlig at sikre, at der ikke er overlapninger over til andre regelsæt. Det er umiddelbart vurderingen, at det kræver en nærmere analyse.

Navnlig med hensyn til dialogen med store online platforme ("bigtechs") vil EU-regler om kontraktklausuler hjælpe med at skabe magtbalancen mellem mindre banker og de store modparter. Fra tredjepartsperspektiv mener vi også, at en revision/inspektion fra en EU-myndighed, i stedet for at alle skal have adgang, vil være enklere. Det er afgørende, at reglerne er proportionale og baseret på en risikobaseret tilgang, så mindre udbydere kan fortsætte med at servicere finansielle institutioner uden at blive overreguleret. I dag benytter finansielle institutter sig at mange forskellige små og store it-leverandører. Det er væsentligt, at fintech miljøet ikke afskæres fra at være leverandør med forslaget.

Tredjepart risikostyring er vigtig med hensyn til proportionalitet og risiko for ordningen og afhængigheden. Her savnes definitionerne af "kritiske og vigtige funktioner" for at undgå usikkerhed. Der er behov for klarer definitioner for udtryk som

"mikrovirksomheder" og politik. Formuleringerne omkring politikken skaber usikkerhed om, på hvilket Governance niveau forskellige krav bør tages op og godkendes.

Med venlig hilsen

Mette Stürup

Mail: 27152020

Høringssvar

7. oktober 2020
Dok. nr.:
FIDA-151247800-694946-v1