FORSVARSMINISTERIET

GRUND- OG NÆRHEDSNOTAT TIL FOLKETINGETS EUROPAUDVALG

30. juni

Kommissionens forslag til Europa-Parlamentets og Rådets forordning om foranstaltninger til styrkelse af solidariteten og kapaciteten i Unionen til at opdage, forberede sig og reagere på cybersikkerhedstrusler og-hændelser, KOM (2023) 209

Opdateret notat. Ændringer er markeret med streg i marginen.

Notatet oversendes til Folketingets Forsvarsudvalg til orientering.

1. Resumé

Formålet med forslaget er at styrke den underliggende solidaritet på tværs af EU for bedre at kunne opdage, forberede sig og reagere på cybersikkerhedstrusler og –hændelser. For at opnå dette skal EU styrke det fælles situationskendskab og kapaciteten til at opdage cybertrusler og -hændelser, styrke kritiske enheders beredskab, samt styrke solidariteten og modstandsdygtighed i EU.

Forslaget fastsætter tre hovedforanstaltninger, der har til hensigt at styrke EU's kapacitet til at opdage, forberede sig og reagere på cybersikkerhedstrusler- og hændelser. Først etableringen af et såkaldt 'europæisk cyberskjold', der vil bestå af en paneuropæisk infrastruktur bestående af nationale og grænseoverskridende (cross-border) sikkerhedsoperationscentre (SOC). Dernæst etableringen af en cyberberedskabsmekanisme som skal støtte medlemsstaternes beredskabs- og reaktionsevne, med henblik på at sikre omgående genopretning efter væsentlige eller omfattende cybersikkerhedshændelser. Til sidst oprettelsen af en mekanisme til evaluering af cybersikkerhedshændelser, som Kommissionen, EU-CyCLONe[1] eller CSIRT-netværket[2] vurderer som væsentlige eller omfattende sikkerhedshændelser.

Forslaget har fået en blandet modtagelse i Rådet. Medlemsstaterne har stillet spørgsmål til forslagets juridiske base, finansiering gennem Programmet for et digitalt Europa (DEP), spørgsmål om horvidt Kommissionen bevæger sig

[1] Det europæiske netværk af forbindelsesorganisationer for cyberkriser
[2] Netværket af enheder, som håndterer IT-sikkerhedshændelser

ind på medlemsstaternes kompetenceområde, samt risiko for duplikering af allerede etablerede videndelingsnetværk.

Det vurderes, at forslaget vil få statsfinansielle konsekvenser som følge af nye forpligtelser for myndighederne, såfremt Danmark indgår i et grænseoverskridende SOC-samarbejde.

Regeringen stiller sig overordnet positiv over for forslaget. Regeringen vil arbejde for, at foranstaltninger, der skal styrke situationsbevidsthed, beredskab, modstandsdygtighed og kapaciteter på tværs af EU, anlægger en balanceret tilgang, der både tager højde for nationale kompetencer og behovet for øget understøttelse af EU. Det er centralt for regeringen, at ordlyden af forordningen udarbejdes på en sådan måde, at medlemsstaternes nationale kompetence inden for national sikkerhed og forsvar respekteres. I forlængelse heraf skal sådanne foranstaltninger også tage højde for medlemsstaters forskelligartede offentlige organisering af deres SOC-kapaciteter.

2. Baggrund

Europa-Kommissionen (Kommissionen) har den 18. april 2023 fremsat et forslag til en forordning om foranstaltninger, der skal styrke den underliggende solidaritet og kapacitet til at opdage, forberede sig og reagere på cyberhændelser i EU (KOM(2023) 209) (herefter 'forslaget'). Forslaget er modtaget i dansk sprogversion den 25. maj 2023.

Forslaget har ifølge Kommissionen hjemmel i Traktaten om den Europæiske Unions Funktionsmåde (TEUF) artikel 173, stk. 3 (om industri) samt artikel 322, stk. 1, litra a) (om overførselsregler, der fraviger princippet om etårighed fastsat i Europa-Parlamentets og Rådets forordning[3]). Forslaget skal behandles efter den almindelige lovgivningsprocedure i TEUF artikel 294, hvorefter Rådet træffer afgørelse med kvalificeret flertal.

Det er Kommissionens målsætning, at cybersikkerheden i EU bør styrkes. På den baggrund udarbejdede Kommissionen i 2020 EU's strategi for cybersikkerhed[4]. Der er med afsæt i strategien løbende blevet igangsat en række tiltag for at styrke cybersikkerheden, herunder regulering af kritisk infrastruktur, certificering af cybersikkerhedsprodukter, samt styrkelse af cybersikkerhed på tværs af EU. Strategien etablerer også, at der skal opbygges et europæisk cyberskjold af grænseoverskridende sikkerhedsoperationscentre (SOC), der skal beskytte EU's befolkning, virksomheder og institutioner mod cybertrusler.

[3] Europa-Parlamentets og Rådets forordning (EU, Euratom) 2018/1046 af 18. juli 2018 om de finansielle regler vedrørende Unionens almindelige budget (EUT L 193 af 30.7.2018, s.1).

[4] JOIN (2020) 18 – Final - EU's strategi for cybersikkerhed for det digitale årti

Kommissionen henviser til et behov for, på tværs af EU, at øge informationsdeling og EU's kollektive cybersikkerhedskapaciteter. Dette behov er dels en følge af krigen i Ukraine, hvor Rusland har benyttet fjendtlige cyberoperationer, men også i lyset af, at cyberangreb kan ramme forsyningskæder og have økonomiske konsekvenser. I 2020 berørte angrebet på SolarWinds' forsyningskæde mere end 18.000 organisationer på verdensplan. Væsentlige cybersikkerhedshændelser kan skabe så omfattende forstyrrelser, at en enkelt eller flere berørte medlemsstater ikke kan håndtere dem alene.

Kommissionen mener, at der er begrænset solidaritet medlemsstaterne imellem, og forbinder dette til en afgrænset støtte på EU-niveau til beredskab og reaktion på cybersikkerhedshændelser. Forslaget skal også ses i lyset af Rådets tidligere anmodning til Kommissionen om at forberede et forslag til en ny beredskabsfond for cybersikkerhed.[5]

Kommissionen fremstiller også forslaget for at tilvejebringe langvarigt juridisk og finansielt grundlag for SOC-kapacitetsopbygningsprojekter, som Kommissionen forventer at køre gennem Programmet for et digitalt Europa[6] (DEP) til og med 2027.

Endelig understøtter forslaget ambitionerne i EU's politik for cyberforsvar[7] fra den 10. november 2022 om at opbygge en cybersikkerhedsreserve på EU-plan med tjenester fra betroede leverandører og støtte til test af kritiske enheder.

Kommissionen oplyser, at der på grund af forslagets hastende karakter ikke er foretaget en konsekvensanalyse. Dog oplyser Kommissionen, at forordningens foranstaltninger støttes af DEP og er i overensstemmelse med de foranstaltninger, som var genstand for en DEP-konsekvensanalyse.

Forordningens foranstaltninger støttes med finansiering under den strategiske målsætning "cybersikkerhed" gennem både arbejdsprogrammet for cybersikkerhed og det generelle arbejdsprogram i DEP. Med Forslaget foreslås et øget budget til DEP på ca. 745 millioner kroner (100 mil. EUR), som omfordeles fra andre strategiske målsætninger. Det øgede budget vil bl.a. gå til at Det Europæiske Kompetencecenter for Cybersikkerhed (ECCC) kan implementere handleplaner tilhørende SOC-projekterne under cyberskjoldet. Det øgede budget vil også bidrage til etableringen af cybersikkerhedsreserven.

---

[5] Rådets konklusioner om udviklingen af Den Europæiske Unions cyberposition, 23. maj 2022 (9364/22).

[6] Programmet for et digitalt Europa yder strategisk finansiering med henblik på at bringe digital teknologi til virksomheder, borgere og offentlige forvaltninger (https://digital-strategy.ec.europa.eu/da/activities/digital-programme)

[7] Fælles meddelelse til Europa-Parlamentet og Rådet – EU's politik for cyberforsvar JOIN(2022) 49 final.

3. Formål og indhold

Formålet med forslaget er at styrke solidariteten på tværs af EU for bedre at kunne detektere, forberede sig og reagere på cybersikkerhedstrusler og –hændelser. Dette skal opnås ved at:

- Styrke EU's fælles situationskendskab og kapacitet til at detektere cybertrusler og -hændelser og samtidig bidrage til europæisk teknologisk suverænitet på cybersikkerhedsområdet
- Styrke kritiske enheders beredskab i hele EU ved at udvikle fælles indsatskapaciteter over for væsentlige eller omfattende cybersikkerhedshændelser, herunder også til at støtte associerede tredjelande i DEP
- Øge EU's modstandsdygtighed og bidrage til en effektiv indsats ved at gennemgå og evaluere tidligere væsentlige eller omfattende hændelser, herunder udvikle eventuelle anbefalinger på baggrund af opbyggede erfaringer.

Forslaget bygger på nogle områder videre på Europa-Parlamentet og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele EU (NIS2).

NIS 2-direktivet stiller bl.a. krav om national gennemførelse af cybersikkerhedsforanstaltninger, hændelsesrapportering samt tilsyns- og håndhævelsesbeføjelser, herunder regler om sanktioner. NIS 2-direktivet skal være implementeret i dansk ret senest den 17. oktober 2024. Der vil derfor i den kommende folketingssamling blive fremsat lovforslag, der implementerer direktivet. Arbejdet i de europæiske samarbejdsgrupper, som oprettes med NIS 2-direktivet, vil blive udvidet med nærværende forslag.

Kapitel I – Generelle målsætninger, genstand og definitioner

Forslaget fastsætter foranstaltninger til styrkelse af EU's kapacitet til at detektere, forberede sig og reagere på cybersikkerhedstrusler- og hændelser, navnlig gennem følgende tre tiltag:

- Etablering af en paneuropæisk infrastruktur for sikkerhedsoperationscentre - det europæiske cyberskjold - for at styrke det fælles situationskendskab og kapaciteten til at detektere hændelser.
- Oprettelsen af en cyberberedskabsmekanisme som vil styrke medlemsstaternes beredskabs- og reaktionskapacitetsamt sikre hurtig genopretning efter væsentlige eller omfattende cybersikkerhedshændelser.
- Oprettelse af en europæisk mekanisme til evaluering af cybersikkerhedshændelser med henblik på at evaluere og lære af væsentlige eller omfattende hændelser.

Det fremgår af forslaget, at forordningen ikke berører medlemsstaternes primære ansvar for national sikkerhed, offentlig sikkerhed samt forebyggelse, efterforskning, afsløring og retsforfølgelse af strafbare handlinger.

Kapitel II – Det europæiske cyberskjold
Kommissionen foreslår, at der etableres et europæisk cyberskjold med henblik på at udvikle avancerede kapaciteter til at indsamle, analysere og behandle data om cybertrusler og -hændelser i EU. Skjoldet skal bestå af nationale og grænseoverskridende SOC.

Det europæiske cyberskjold skal:

- samle og dele data om cybertrusler og -hændelser fra forskellige kilder gennem grænseoverskridende sikkerhedsoperationscentre
- udvikle og tilvejebringe anvendelige oplysninger om cybertrusler ved hjælp af bl.a. kunstig intelligens og dataanalyseteknologier
- bidrage til bedre beskyttelse mod og reaktion på cybertrusler
- bidrage til hurtigere detektion af cybertrusler og stærkere situationskendskab i hele EU
- levere tjenester og aktiviteter til cybersikkerhedssektoren i EU, herunder bidrage til udviklingen af den europæiske forsyningskæde for udviklingen af værktøjer inden for avanceret kunstig intelligens og dataanalyse.

Det fremgår af forslaget, at for at deltage i det europæiske cyberskjold skal hver medlemsstat udpege mindst et nationalt SOC, som skal være et offentligt organ. De nationale SOC'er skal fungere som referencepunkt til andre offentlige og private organisationer på nationalt plan med henblik på at indsamle og analysere oplysninger om cybersikkerhedstrusler og -hændelser og bidrage til et grænseoverskridende SOC.

De grænseoverskridende SOC'er organiseres og styres af et konsortium, som skal bestå af mindst tre medlemsstater. Forslaget fastslår, at konsortiemedlemmerne skal udveksle indbyrdes relevante oplyser om fx cybertrusler, hændelser, sårbarheder, teknikker og procedurer, indikatorer for kompromittering, og fjendtlige taktikker.

I forslaget tilskyndes til udveksling af oplysninger mellem grænseoverskridende centre. For at garantere en effektiv udveksling af oplysninger vil kommissionen fastsætte betingelser for interoperabilitet mellem de grænseoverskridende centre. Betingelserne for interoperabilitet fastsættes efter høring af ECCC. Endelig fastsætter forslaget, at såfremt de grænseoverskridende centre indhenter oplysninger om en potentiel eller igangværende væsentlig cybersikkerhedshændelse, skal relevante oplysninger videregives til EU-CyCLONe, CSIRT-netværket og Kommissionen.

Kapitel III – Beredskabsmekanisme for cybersikkerhed
Kommissionen foreslår at etablere en cyberberedskabsmekanisme, der skal forbedre EU's modstandsdygtighed over for større cybersikkerhedstrusler.

Cyberberedskabsmekanismen er også et krisestøtteinstrument, der skal afhjælpe medlemsstaterne med at indkapsle, afbøde og genoprette de kortsigtede virkninger af væsentlige og omfattende cybersikkerhedshændelser.

Cyberberedskabsmekanismen skal sikre, at der er specialiserede ressourcer til rådighed til at støtte forskellige typer af beredskabsforanstaltninger:

- Koordinerede beredskabstest af enheder, der opererer i meget kritiske sektorer i EU. Dette vil overordnet indebære test af sårbarheder hos essentielle enheder, der driver kritisk infrastruktur, støtte til trussels- og risikovurderinger og risikomonitorering af aktiver og sårbarheder. Beredskabstestene skal også sikre en konsekvent tilgang til at teste sikkerheden på tværs af EU. Denne del af mekanismen vil finansieres gennem arbejdsprogrammet for cybersikkerhed i DEP 2023-2024.

- Foranstaltninger der omfatter reaktion på og hurtig genopretning af funktioner og tjenester efter væsentlige eller omfattende hændelser. Forordningen vil også etablere en cybersikkerhedsreserve, der skal bestå af betroede udbydere, som skal kunne levere beredskabstjenester til at understøtte foranstaltningen. De betroede udbydere er udvalgt i overensstemmelse med en række kriterier, som forordningen fastsætter. Udbyderne skal fx have en passende sikkerhedsgodkendelse, have et passende sikkerhedsniveau og kunne dokumentere erfaring med at levere lignende tjenester til nationale myndigheder eller enheder, der opererer i kritiske eller meget kritiske sektorer.

  Det fremgår af forslaget, at brugerne af tjenesterne fra EU's cybersikkerhedsreserve omfatter medlemsstaternes cyberkrisemyndigheder og CSIRT'er[8] samt EU's institutioner, organer og agenturer. Det foreslås, at Kommissionen har det overordnede ansvar for gennemførelsen af EU's cybersikkerhedsreserve og kan helt eller delvist overdrage driften og administrationen af reserven til ENISA. Kommissionen kan i gennemførelsesretsakter præcisere de typer og det antal af beredskabstjenester, der kræves i EU's cybersikkerhedsreserve. For at modtage støtte foreslår Kommissionen, at brugerne af cyberreserven træffer deres egne foranstaltninger for at afbøde virkningerne af den hændelse, som der anmodes om støtte til. Anmodningerne vil blive oversendt til Kommissionen og ENISA. Gennem gennemførelsesretsakter skal de detaljerede ordninger for tildeling af støtte fra EU's cybersikkerhedsreserve fastlægges. Endelig foreslås det, at tredjelande kan anmode om støtte fra EU's cybersikkerhedsreserve, hvis de associeringsaftaler, der er indgået vedrørende deres deltagelse i DEP, indeholder bestemmelser herom.

- Gensidige bistandsaktioner i form af bistand fra en medlemsstats nationale myndigheder til en anden medlemsstat.

[8] Computer Security Incident Response Team (CSIRT) i andre sammenhænge betegnet CIRT.

Kapitel IV – Mekanisme til gennemgang af cybersikkerhedshændelser
Kommissionen foreslår, at der skal etableres en mekanisme til evaluering og analyse af cybersikkerhedshændelser. Nærmere foreslås det, at Kommissionen, EU-CyCLONe eller CSIRT-netværket kan anmode ENISA om at vurdere trusler, sårbarheder og afbødende foranstaltninger ved specifikke, væsentlige eller omfattende cybersikkerhedshændelser. Efter afsluttet evaluering, analyse og vurdering af en hændelse, skal ENISA fremsende en rapport om hændelsen til CSIRT-netværket, EU-CyCLONe og Kommissionen. Hvis relevant, kan Kommissionen videresende rapporten til EU's højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik.

Det fremgår af forslaget, at ENISA i forbindelse med udarbejdelsen af rapporterne skal samarbejde med alle relevante interessenter, herunder repræsentanter fra medlemsstater, Kommissionen, andre relevante EU-institutioner, -organer og -myndigheder, udbydere samt brugere af af administrerede sikkerhedstjenester.

I forslaget specificeres det, at rapporterne skal omfatte en gennemgang og analyse af den specifikke cybersikkerhedshændelse, herunder de vigtigste årsager, sårbarheder og opbyggede erfaringer. Fortrolige oplysninger beskyttes i overensstemmelse med EU-retten eller national ret vedrørende beskyttelse af følsomme eller klassificerede informationer. Desuden skal rapporten, hvor det er relevant, indeholde anbefalinger til forbedring af EU's cyberposition. Hvis det er muligt, offentliggøres en udgave af rapporten, som kun vil indeholde oplysninger, der kan offentliggøres.

Kapitel V – Afsluttende bestemmelser
Som følge af forslaget foretages ændringer i forordningen om programmet for DEP mhp. at omprioritere midler fra indsatsområde 2 (Cloud, Data og AI) og indsatsområde 4 (Avancerede digitale kompetencer) til indsatsområde 3 (cybersikkerhed). Der er tale om en reallokering på ca. 745 mio. kr. (100 mio. EUR) fra indsatsområde 2 og 4 til indsatsområde 3. Midlerne vil være øremærket til indsatserne beskrevet i forslaget, hvor der allerede var afsat 857 mio. kr. (115 mio. EUR) til pilotprojekter.

Kommissionen, Europa-Parlamentet og Rådet vil blive forelagt en rapport om evaluering og revision af forordningen senest fire år efter dens vedtagelse.

Gennemførelsesretsakter
Kommissionen har beføjelse til at vedtage gennemførelsesretsakter med det formål at: i) præcisere betingelserne for interoperabilitet mellem grænseoverskridende SOC'er (kapitel II), ii) fastlægge de proceduremæssige ordninger for udveksling af oplysninger mellem grænseoverskridende centre og

relevante EU-enheder vedrørende en mulig eller igangværende væsentlig cybersikkerhedshændelse (kapitel II), iii) fastsætte tekniske krav for at sikre et højt niveau af data og fysisk sikkerhed i infrastrukturen, og beskytte EU's sikkerhedsinteresser, når der udveksles oplysninger med enheder, der ikke er offentlige organer i medlemsstaterne (kapitel II), iv) præcisere, hvilke typer og hvor mange beredskabstjenester der er nødvendige i EU's cybersikkerhedsreserve (kapitel III), og v) yderligere præcisere de detaljerede ordninger for tildeling af støttetjenester under EU's cybersikkerhedsreserve (kapitel III).

4. Europa-Parlamentets udtalelser

Europa-Parlamentet er i henhold til den almindelige lovgivningsprocedure (TEUF art. 294) medlovgiver. Der foreligger endnu ikke en udtalelse.

Det er Europa-Parlamentets udvalg for industri, forskning og energi (ITRE), der behandler forslaget.

5. Nærhedsprincippet

Kommissionen henviser til, at forordningen er fremsat med hjemmel i artikel 173, stk. 3 og artikel 322, stk. 1, litra a), i traktaten om Den Europæiske Unions Funktionsmåde (TEUF).

TEUF artikel 173, stk. 3 giver EU og medlemsstaterne mulighed for at vedtage foranstaltninger til støtte for medlemsstaternes aktioner til virkeliggørelse af målene i artiklens stk. 1. Bestemmelsen tillader dog ikke harmonisering af medlemsstaternes love og administrative bestemmelser. TEUF artikel 173, stk. 1 fastsætter, at EU og medlemsstaterne sørger for, at de nødvendige betingelser for EU-industriens konkurrenceevne er til stede, bl.a. med sigte på, at fremme udnyttelsen af det industrielle potentiale i politikkerne for innovation, forskning og teknologisk udvikling.

Det bemærkes, at deltagelsen i forslagets tre foranstaltninger som udgangspunkt er baseret på frivillighed for medlemsstaterne. Beslutter medlemsstaterne sig dog for at bidrage til eller deltage i de tre foranstaltninger, kan der være forpligtelser forbundet med denne beslutning. Forslaget lægger derfor som udgangspunkt ikke op til en harmonisering af medlemsstaternes love og administrative bestemmelser i forordningen, da det er frivilligt om man benytter sig af foranstaltningerne i forordningen. Hensigten er, at forslaget skal supplere og ikke overlappe de nationale situationskendskab og beredskab, samt kapaciteten til at opdage og reagere på cybertrusler- og hændelser.

TEUF artikel 322, stk. 1, litra a) giver hjemmel til, at Europa-Parlamentet og Rådet kan træffe afgørelse efter almindelig lovgivningsprocedure, efter høring af Revisionsretten, om finansielle regler, der fastsætter retningslinjer for budgettet mv. Det er Kommissionens vurdering, at der i forslaget laves en finansieringsramme for de tre foranstaltninger, hvortil der er behov for en

vis finansiel fleksibilitet. TEUF artikel 322, stk. 1, litra a) giver mulighed for at fravige princippet om etårighed fastsat i Europa-Parlamentets og Rådets forordning (Euratom) 2018/1046. Denne bør benyttes henset til det uforudsigelige cybersikkerheds- og trusselsbillede, da beredskabsmekanismen derfor bør have en vis grad af fleksibilitet med hensyn til budgetforvaltning.

Overordnet set peger Kommissionen på, at cybertruslers udprægede grænseoverskridende karakter gør, at målsætningerne for den nuværende indsats ikke effektivt vil kunne opfyldes af medlemsstaterne alene. Med udgangspunkt i artikel 5 i Traktaten om den Europæiske Union, fastlægger forordningen rammerne for en fælles regulering på tværs af EU for at styrke cybersolidariteten og bedre kunne opdage, forberede sig og reagere på cybersikkerhedstrusler og –hændelser. Der bør til støtte herfor udvikles gensidige støttemekanismer, navnlig samarbejde med den private sektor, for at skabe solidaritet på EU-niveau.

Kommissionen oplyser endvidere, at forordningens formål er at styrke industriens og servicesektorens konkurrenceevner i Europa og støtte den digitale omstilling ved at styrke cybersikkerhedsniveauet på det indre marked. Forordningen har navnlig til formål, at øge modstandsdygtigheden hos borgere, virksomheder og enheder, som opererer i kritiske sektorer over for de tiltagende cybersikkerhedstrusler og dermed kan have ødelæggende samfundsmæssige og økonomiske virkninger. Disse tiltag vurderes at have hjemmel i TEUF artikel 173, stk. 3.

På den baggrund vurderer Kommissionen, at der er behov for tværgående handling på EU-plan, hvorfor forslaget fremsættes med hjemmel TEUF artikel 173, stk. 3 og artikel 322, stk. 1, litra a). Kommissionen oplyser endvidere, at foranstaltningerne ikke går videre, end hvad der er nødvendigt for at opfylde forordningens mål.

Regeringen kan umiddelbart tilslutte sig Kommissionens vurdering og finder på det foreliggende grundlag, at forslaget som udgangspunkt er i overensstemmelse med nærhedsprincippet. Der tages dog forbehold for eventuelle forhold fra analysen af hjemmelsgrundlaget fra Rådets Juridiske Tjeneste, der fortsat udestår, samt afklaring af Kommissionens beføjelser under forslaget til at lave gennemførelsesretsakter med hjemmel i forordningen.

6. Gældende dansk ret

Den danske lovgivning indeholder ikke nærmere regler om etablering af en national SOC eller deltagelse i grænseoverskridende SOC'er som led i et europæisk cyberskjold svarende til det foreslåede.

Center for Cybersikkerhed (CFCS) under Forsvarets Efterretningstjeneste (FE) har til opgave at understøtte et højt informationssikkerhedsniveau i den

informations- og kommunikationsteknologiske infrastruktur, som samfundsvigtige funktioner er afhængige af. I den forbindelse rådgiver CFCS om cybertrusler og beskyttelsesforanstaltninger og bistår efter omstændighederne med håndtering af cyberangreb. CFCS løser således i dag en række opgaver af sammenlignelig karakter, som det, der følger af dele af forslaget. CFCS' virksomhed, herunder rammerne for CFCS' analyse og videregivelse af data, er reguleret i CFCS-loven.

7. Konsekvenser

Lovgivningsmæssige konsekvenser

Forordningen vil være direkte gældende i Danmark.

Det bemærkes indledningsvist, at forslagets nærmere rammer for nationale og grænseoverskridende SOC'er, herunder navnlig deres eventuelle tilvejebringelse, behandling og udveksling af personoplysninger eller fortrolige oplysninger, ikke på nuværende tidspunkt er så konkretiseret, at der kan foretages en tilbundsgående vurdering af alle forslagets lovgivningsmæssige konsekvenser.

Der er eksempelvis flere elementer i forslaget, hvor Kommissionen vil kunne fastsætte nærmere regler ved udstedelsen af gennemførelsesretsakter. Det foreslås således, at Kommissionen kan udstede gennemførelsesretsakter, der 1) fastsætter betingelserne for interoperabilitet mellem de grænseoverskridende SOC'er med henblik på udveksling af oplysninger, 2) fastlægger de proceduremæssige ordninger for udveksling af oplysninger mellem de grænseoverskridende SOC'er og nærmere angivne EU-organer, og 3) fastsætter tekniske krav til medlemsstaternes forpligtigelse til at sikre et højt niveau af datasikkerhed og fysisk sikkerhed i den infrastruktur, der udgør det europæiske cyberskjold.

Da de nærmere regler vedrørende overstående skal fastsættes ved gennemførelsesretsakter, er det på nuværende tidspunkt ikke muligt at vurdere de eventuelle lovgivningsmæssige konsekvenser heraf.

Den nærmere ordning for deltagelsen i en grænseoverskridende SOC vil blive fastlagt i en såkaldt konsortieaftale, der indgås mellem medlemmerne af den grænseoverskridende SOC.

Det er endnu ikke konkretiseret, hvilket indhold en eventuel konsortieaftale vil have, og hvordan arbejdet i den grænseoverskridende SOC vil blive udmøntet i praksis. Derfor er det ikke muligt på nuværende tidspunkt at vurdere de lovgivningsmæssige konsekvenser af denne del af forslaget.

Såfremt Danmark indgår i et grænseoverskridende SOC-samarbejde, vil der være behov for nærmere at regulere eksempelvis den behandling af personoplysninger, der i givet fald vil finde sted.

En vedtagelse af forslaget og en efterfølgende etablering af en national SOC eller deltagelse i en grænseoverskridende SOC med placering under FE/CFCS kan således efter omstændighederne medføre et behov for tilpasning af dansk lovgivning.

Økonomiske konsekvenser
Statsfinansielle konsekvenser
Det forventes, at forslaget vil få statsfinansielle konsekvenser, såfremt Danmark indgår i et grænseoverskridende SOC-samarbejde. De statsfinansielle konsekvenser er således ikke en direkte effekt af forordningens vedtagelse og direkte virkning i Danmark. Omkostningerne kan omfatte nye opgaver til eksisterende myndigheder i form af etablering og drift af en SOC, som vil indgå i det europæiske cyberskjold. Etableringen vil omfatte deltagelse i det fælles indkøb, som bliver organiseret af ECCC, og skal indkøbe software og hardware, som skal udgøre SOC'en. Driften indebærer løbende udgifter til personel, aktiviteter, rejser, eventuelle udbud og vedligeholdelse af udstyr. Der er gennemført et udgiftsskøn på baggrund af overvejelser om dansk deltagelse i cyberskjoldet med seks øvrige medlemsstater, hvilket skønnede etableringsomkostninger til ca. 4,5 mio. kr. og driftsomkostninger over 3 år til ca. 4,5 mio. kr.

Det bemærkes, at afledte nationale udgifter som følge af EU-retsakter afholdes inden for de berørte ministeriers eksisterende bevillingsramme, jf. budgetvejledningens bestemmelser herom.

Samfundsøkonomiske og erhvervsøkonomiske konsekvenser
Forslaget vurderes ikke at have samfundsøkonomiske eller erhvervsøkonomiske konsekvenser.

Andre konsekvenser og beskyttelsesniveauet
Det forventes, at forslaget på sigt vil øge cybersikkerheden i Danmark til gavn for både virksomheder og forbrugere og for den nationale sikkerhed. Cybersikkerhedslovgivning, der stiller krav til deling af informationer om cybertrusler, støtte til medlemsstaterne ved omfattende cybersikkerhedshændelser samt efterfølgende evaluering af disse hændelser, vil bidrage til at myndigheder og virksomheder i Danmark er bedre beskyttet i cyberspace. Forslaget skønnes derudover ikke i sig selv at medføre administrative eller miljømæssige konsekvenser.

8. Høring
Forslaget har været i høring i specialudvalget for Civilbeskyttelse samt hos Erhvervsministeriet og Digitaliserings- og Ligestillingsministeriet fra 9. juni til 13. juni.

Forslaget er hertil sendt i ekstern høring hos Dansk Industri, Dansk Erhverv, CENSEC, Danske Maritime, Navalteam, Dansk Metal, DigitalLead, IDA og It-Branchen. Høringsfristen er fastsat til den 23. juni 2023. Der er indkommet høringssvar fra Dansk Industri og IT-Branchen.

Dansk Industri (DI) bemærker, at cybertruslen er alvorlig og forventes i lyset af den sikkerhedspolitiske situation kun at blive mere alvorlig. Derfor er det afgørende, at man både nationalt og internationalt styrker cybersikkerhed og samarbejde herom. Dog finder DI ikke at forslaget er svaret.

DI bemærker, at der er meget regulering på det digitale område og inden for cybersikkerhed, og at forslaget bygger oven på NIS2-direktivet, der først får virkning til oktober 2024. DI pointerer, at der derudover allerede eksisterer forskellige former for videndeling mellem cybersikkerhedsenheder på tværs af EU, og ikke mindst på tværs af vores allierede, der også omfatter lande uden for EU. DI finder derfor, at der ikke er brug for nye lignende tiltag, før man har fået erfaringer fra NIS2-implementeringen og analyseret, hvad der konkret er brug for i forhold til fx videndeling. DI bemærker, at kræfterne bør fokuseres på de rigtige initiativer.

DI påpeger, at forslaget lægger op til at etablere en europæisk cybersikkerhedsreserve bestående af udvalgte betroede udbydere af cybersikkerhedstjenester, der skal reagere på væsentlige eller omfattende cybersikkerhedshændelser og omgående genopretning efter sådanne hændelser. Tjenesterne kan indsættes i alle medlemsstater. DI bemærker, at der lægges op til, at udvalgte it-sikkerhedsfirmaer vil kunne udføre hændelsesberedskabstjenester på EU's vegne i alle medlemsstater.

DI vurderer umiddelbart, at det kun vil være de største europæiske it-sikkerhedsleverandører, der vil være i spil til at vinde et sådant udbud. DI foreslår derfor, at det i stedet skal være op til medlemsstaterne selv at udvælge it-sikkerhedsleverandører med eksisterende kendskab til det enkelte medlemsstats digitalisering og it-sikkerhed, som betroede udbydere finansieret af cybersikkerhedsreserven.

DI mener, at det giver bedre muligheder for en hurtig afhjælpning med nationalt kendskab og et allerede eksisterende tillidsforhold, og derudover vil det skabe bedre muligheder for, at flere it-sikkerhedsleverandører vil kunne være betroede udbydere, herunder at udvikle markedet for cybersikkerhedstjenester i det enkelte medlemsstat, i stedet for at styrke enkelte allerede store cybersikkerhedsleverandører med det fremsatte forslag.

IT-Branchen (ITB) bakker overordnet op om forslaget, der har som grundformål at styrke EU landenes indbyrdes solidaritet med hinanden ved at op-

bygge et antal SOC'er som er grænseoverskridende, det såkaldte Cyberskjold. ITB mener at der i det grænseoverskridende samarbejde om SOC'er bør tages højde for at ikke alle EU lande er lige digitaliserede.

I forhold til den pulje af midler, der afsættes til at hjælpe virksomheder der bliver ramt af cyberangreb, og som virksomhederne kan bede om midler fra til at afbøde konsekvenser af cyberangreb, mener ITB, at det fjerner noget af incitamentet til at sikre sine systemer, da der ikke stilles krav til hvordan man kan gøre sig fortjent til midlerne. ITB påpeger derudover, at hvis midlerne skal gøre nytte, skal de være tilgængelige meget hurtigt efter at der er konstateret et succesfuldt angreb. Her er der behov for meget hurtige administrative processer, og lovforslaget redegør ikke umiddelbart for processen for at få midlerne.

ITB mener, at for at de grænseoverskridende SOC'er skal fungere effektivt i forhold til threat intelligence, er det ikke hensigtsmæssigt, hvis SOC'erne bliver begrænset fra at afsøge "leaks" på darknet. Her vil de finde lækkede databaser med passwords og personoplysninger. ITB finder derudover, at der som et minimum bør være en forpligtelse til at offentliggøre daglige trusselsvurderinger, som har en karakter af rådata, som andre virksomheder kan anvende i deres arbejde med sikkerhedskunder.

ITB mener, at hvis SOC'erne opdager noget, der ikke er samfundskritisk, bør de stadig kunne dele deres viden med deres nationale efterforskningsenheder, således at den generelle sikkerhed og kriminalitetsbekæmpelse bliver forbedret. Det bør derudover være muligt at dele data anonymt i realtid blandt SOC'erne.

ITB påpeger, at det i dag er muligt at lave en national null routning. ITB bemærker, at det i Danmark tager et sted imellem et par timer og flere dage. I Norge er det muligt at lave det på fem minutter. ITB mener derfor at det bør indføres i alle lande og testes, således at man i en krise kan lukke ned for visse IP´er/ URL´er eller landes trafik. ITB mener at det generelt set bør være ISP'ernes ansvar.

ITB bemærker, at det i forslaget anbefales, at der konstrueres et antal minimumskrav til virksomheder, der byder ind til cybersikkerhedsberedskabet. Der anvises dog ikke hvad kravene bør være, eller hvordan de etableres. Det anføres i forslaget at der bør lægges særlig vægt på erfaringer, ekspertise, faglig integritet og upartiskhed. For at det skal være effektivt, mener ITB, at kravene til dette bør være kendte, så virksomheder kan lægge en plan for at imødekomme dem. ITB mener, at kravene i artikel 16 i forslaget ikke er entydige, men i stedet inviterer til en subjektiv vurderingsproces.

ITB finder, at for at opnå succes med cybersikkerhedsreserve initiativet er det essentielt, at de private udbydere, der indgår i reserven, holdes orienteret af SOC´erne løbende, og ikke først tilkaldes når en krise indtræffer, og herefter skal sætte sig ind i tingene.

ITB mener, at der bør være mulighed for at ting kan blive driftet af ens konkurrenter eller samarbejdspartnere. ITB påpeger, at bankerne i Danmark fx har en aftale om, at datacentrene kan overtage trafik for hinanden, hvis der sker en hændelse.

9. Generelle forventninger til andre landes holdninger

Der har i Rådets horisontale arbejdsgruppe for cyber (HWPCI) indtil videre været en tematisk drøftelse af sikkerhedsoperationscentrene i forslaget, samt en session, hvor medlemsstaterne har kunnet stille spørgsmål til forslaget til Kommissionen. Samtlige lande har taget undersøgelsesforbehold, og ikke givet officielle holdninger til kende. Der er således indtil nu fortrinsvist stillet tekniske spørgsmål til forslaget.

Forslaget har generelt fået en blandet modtagelse, hvor en række medlemsstater har haft spørgsmål til forslaget, blandt andet vedrørende forslagets juridiske base, finansiering gennem DEP, national kompetence samt duplikering i forhold til allerede etablerede videndelingsnetværk.

Danmark har sammen med 23 andre medlemsstater fremsendt et non-papir den 31. marts 2023 (inden forslagets fremsættelse), med fokus på at medlemsstaterne skal indgå i tæt dialog med Kommissionen om udarbejdelsen og vedtagelsen af forslaget, at den kommende EU-cybersikkerhedsreserve skal tilpasses medlemsstaternes behov, samt at medlemsstaterne skal være med til at bestemme krav til reserven og være inde over beslutning om aktivering af reserven.

10. Regeringens generelle holdning

Regeringen stiller sig overordnet positiv over for forslaget.

Regeringen er enig med Kommissionen i, at der er behov for at styrke medlemsstaternes og EU's kapaciteter til at reagere effektivt og behændigt på cybersikkerhedstrusler og ondsindet aktivitet i cyber-domænet rettet mod EU og medlemsstaterne. Regeringen er ligeledes positiv over for foranstaltninger, der vil styrke solidariteten medlemslandene imellem i tilfælde af væsentlige cybersikkerhedshændelser.

Det er centralt for regeringen, at ordlyden af forordningen udarbejdes på en sådan måde, at medlemsstaternes nationale kompetence inden for national sikkerhed og forsvar respekteres efter Traktaten om Den Europæiske Union (TEU) artikel 4, stk. 2.

Ligeledes er det centralt for regeringen, at Kommissionens beføjelser til at udstede gennemførelsesretsakter skal afgrænses. Regeringen er skeptisk over for, at den nærmere specificering af interoperabilitetskrav, informationsdeling samt tildeling af støttetjenester skal ske igennem gennemførelsesretsakter. Regeringen mener også, at der bør udarbejdes en konsekvensanalyse af forslaget, for at der bedst muligt kan tages stilling til forslaget.

Regeringen støtter den foreslåede finansiering af forslaget igennem DEP arbejdsprogrammet. Prioriteringer af midler indenfor DEP bør generelt foretages på en sammenhængende, inkluderende og transparent måde frem for i områdespecifikke retsakter.

Regeringen mener, at der er behov for mere forudsigelighed for aktørerne ift. finansieringen af cyberinitiativerne under DEP, og at disse i højere grad bør formuleres som frivillige rammer igennem det eksisterende samarbejde imellem medlemsstaterne og det Europæiske Kompetencecenter for Cybersikkerhed (ECCC).

Regeringen vil arbejde for, at foranstaltninger, der skal styrke situationsbevidsthed, beredskab, modstandsdygtighed og kapaciteter på tværs af EU overfor cybersikkerhedstrusler og -hændelser, anlægger en balanceret tilgang, der både tager højde for nationale kompetencer og behovet for øget understøttelse af EU.

Regeringen støtter foranstaltninger, der sikrer effektiv informationsudveksling og situationsbevidsthed, fx etableringen af en paneuropæisk-infrastruktur for sikkerhedsoperationscentre, der tilsammen skal udgøre et europæisk cyberskjold. Det er centralt for regeringen, at arbejdet med at højne informationsdeling på fælleseuropæisk niveau ikke samtidig forpligter medlemsstaterne til at dele klassificerede eller følsomme oplysninger.

Regeringen finder det vigtigt, at centrale begreber i forslaget afklares. Der er behov for yderligere at præcisere afgrænsningen af bl.a. et nationalt sikkerhedsoperationscenter og et grænseoverskridende sikkerhedsoperationscenter, for at skabe transparens og en fælles forståelse for centrenes samt forordningens anvendelse. Det bør være tydeligt beskrevet, hvordan sikkerhedsoperationscentrene vil blive reguleret i henhold til forordningen.

Regeringen finder, at beredskabsforanstaltninger, der skal forbedre EU's modstandsdygtighed over for større cybersikkerhedstrusler og –hændelser, skal tage højde for nationale forhold. Først bør det afklares, om det rette nationale juridiske grundlag for beredskabstest er på plads.

Regeringen er positivt indstillet over for foranstaltninger, der bidrager til styrkelsen af EU's kollektive cyberforsvar- og sikkerhed. I forbindelse med

oprettelsen af en EU cybersikkerhedsreserve, samt dennes eventuelle deployering, finder regeringen det vigtigt, at der tages højde for nationale individuelle forhold med henblik på at sikre kompabilitet.

Regeringen byder ligeledes foranstaltninger og samarbejde med ligesindede partnere og tredjelande, der bidrager til EU's evne til at afskrække og reagere på ondsindet adfærd i cyberspace, velkommen. Regeringen finder, at medlemsstaterne bør være inddraget i beslutningen om at støtte tredjelande gennem EU's cybersikkerhedsreserve.

Regeringen mener, at der bør sikres sammenhæng og undgås unødvendige overlap mellem gældende og fremtidig regulering og indsatser. Regeringen finder det her vigtigt, at der ikke skabes unødige administrative og økonomiske byrder for virksomheder og offentlige myndigheder. Derudover vil regeringen arbejde for at forslaget tilrettelægges så det i videst muligt omfang kommer dansk cyberindustri til gode.

11. Tidligere forelæggelse for Folketingets Europaudvalg

Sagen har ikke tidligere været forelagt for Folketingets Europaudvalg.