FORSVARSMINISTERIET

SAMLENOTAT
TIL FOLKETINGETS EUROPAUDVALG

Vedrørende sager under Forsvarsministeriets ressort, der behandles på rådsmødet (transport, telekommunikation og energi) den 5. december 2023.

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

= Fremskridtsrapport

Revideret udgave af samlenotat af 13. oktober 2023 forud for rådsmødet (transport, telekommunikation og energi) den 5. december 2023. Nye afsnit er markeret med streg i margen.

1. Resumé

På rådsmødet (transport, telekommunikation og energi) den 5. december 2023 forventes EU-formandskabet at gøre status for forhandlingerne om forordningsforslaget om foranstaltninger til styrkelse af solidariteten og kapaciteten i Unionen til at opdage, forberede sig og reagere på cybersikkerhedstrusler- og hændelser (cybersolidaritetsforordningen).

Danmark kan overordnet bakke op om fremskridtsrapporten på baggrund af udviklingen i de foreløbige forhandlinger, herunder angående bl.a. afgrænsningen af Europa-Kommissionens beføjelser til at udstede gennemførelsesretsakter vedrørende bl.a. interoperabilitetskrav for og informationsdeling mellem de grænseoverskridende sikkerhedscentre samt medlemsstaternes inddragelse i etableringen og brugen af EU's cybersikkerhedsreserve. Idet forhandlingerne om forordningsudkastet fortsat pågår, forventes der justeringer i forordningsudkastet frem mod rådsmødet.

2. Baggrund

Europa-Kommissionen har ved KOM (2023) 209 fremsat 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 (cybersolidaritetsforordningen). Med forslaget vil EU styrke det fælles situationskendskab og kapaciteten til at opdage cybertrusler og -hændelser, styrke kritiske enheders beredskab, samt styrke solidariteten og modstandsdygtighed i EU. Det skal ske ved at

der; etableres et "europæisk cybersikkerhedsalarmsystem" bestående af grænseoverskridende cybersikkerhedsoperationscentre; etableres en cyberberedskabsmekanisme, som skal støtte EU-medlemsstaternes beredskabs- og reaktionsevne ift. omfattende cyberhændelser; oprettes en evalueringsmekanisme for cyberhændelser, så man sikrer vidensopsamling og læring.

Forslaget er fremsat under henvisning til traktaten om den Europæiske Unions funktionsmådes artikel 173 om udviklingen af EU-industriens konkurrenceevne, og artikel 322 om overførselsregler, der fraviger princippet om etårighed fastsat i Europa-Parlamentets og Rådets forordning om de finansielle regler vedrørende Unionens almindelige budget.

3. Formål og indhold

På rådsmødet (transport, telekommunikation og energi) den 5. december 2023 forventes EU-formandsskabet at give en status på behandlingen af cybersolidaritetsforordningen. Formandskabet arbejder på at hente mandat på sagen på Coreper hurtigst muligt efter rådsmødet, og inden årets udgang mhp. at indlede trilogforhandlinger med Europa-Parlamentet.

Det forventes, at fokus for formandskabets statusorientering vil være på at beskrive de justeringer, der er foretaget i forordningsudkastet, der ligger inden for formålet med cybersolidaritetsforordningen. Derudover forventes statusorienteringen at fokusere på de foranstaltninger, hvor der fortsat pågår forhandlinger, herunder særligt ønsket fra flere medlemsstater om, at Kommissionens lovgivningsmuligheder ift. interoperabilitet og informationsdeling mellem de grænseoverskridende sikkerhedsoperationscentre via gennemførelsesretsakter afgrænses.

4. Europa-Parlamentets udtalelser

Europa-Parlamentets holdning foreligger endnu ikke.

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. Beredskabsmekanismen bør derfor have en vis grad af fleksibilitet med hensyn til budgetforvaltning.

Overordnet set peger Kommissionen på, at cybertruslers udprægede tværnationale 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 konkurrenceevne 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 et nationalt sikkerhedsoperationscenter eller deltagelse i tværnationale sikkerhedsoperationscentre som led i et europæisk cybersikkerheds alarmsystem 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 tværnationale sikkerhedscentre, 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 tværnationale sikkerhedscentre med henblik på udveksling af oplysninger, 2) fastlægger de proceduremæssige ordninger for udveksling af oplysninger mellem de tværnationale sikkerhedscentre 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 et tværnationale sikkerhedscenter vil blive fastlagt i en såkaldt konsortieaftale, der indgås mellem medlemmerne af det tværnationale *sikkerhedscenter*.

Det er endnu ikke konkretiseret, hvilket indhold en eventuel konsortieaftale vil have, og hvordan arbejdet i det tværnationale sikkerhedscenter 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 samarbejde om et tværnationalt sikkerhedscenter, 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 et nationalt sikkerhedscenter eller deltagelse i et tværnationale sikkerhedscenter med placering under FE/CFCS kan således efter omstændighederne medføre et behov for tilpasning af dansk lovgivning.

Det bemærkes afslutningsvist, at det skal vurderes nærmere, om der er et behov for tilpasning af gældende lovgivning for at kunne udføre eventuelle koordinerede beredskabstests af enheder, der opererer i meget kritiske sektorer i EU.

Økonomiske konsekvenser
Statsfinansielle konsekvenser
Det forventes, at forslaget vil få statsfinansielle konsekvenser, såfremt Danmark indgår i et samarbejde om et tværnationalt sikkerhedscenter. 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 et tværnationalt sikkerhedscenter, 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 sikkerhedscentret. 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 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 var fastsat til den 23. juni 2023. Der indkom 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 den 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 opbygge et antal sikkerhedcentre, som er tværnationale, det såkaldte Cyberskjold. ITB mener, at der i det tværnationale samarbejde om sikkerhedscentre 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 tværnationale sikkerhedsoperationscentre skal fungere effektivt i forhold til threat intelligence, er det ikke hensigtsmæssigt, hvis sikkerhedscentrene 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 sikkerhedscentrene 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 sikkerhedscentrene.

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 sikkerhedscentrene 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. Forhandlingssituationen

Forslaget har generelt fået en blandet modtagelse i Rådet.

I EU-kredsen er der overordnet anerkendelse af formålet med forordningen, om end flere medlemsstater har forholdt sig kritisk til elementer i udkastet til forordningen. Medlemsstaterne er overordnet enige i ambitionen om at skabe større solidaritet og understøtte et højt cybersikkerhedsniveau på tværs af EU.

Centralt i forhandlingerne har været en række medlemsstaters skepsis over for Europa-Kommissionens lovgivningsmuligheder ift. interoperabilitet og informationsdeling mellem de grænseoverskridende sikkerhedsoperationscentre via gennemførelsesretsakter. Flere medlemsstater har derudover fremført, at medlemsstaternes nationale kompetence inden for national sikkerhed og forsvar skal respekteres, samt

at det tydeligt skal fremgå af forordningsudkastet, at deltagelse i foranstaltningerne er frivillig for medlemsstaterne. En række medlemsstater har også haft spørgsmål til forordningsforslagets traktatretlige hjemmel, finansiering gennem DEP samt duplikering i forhold til allerede etablerede videndelingsnetværk.

Der forventes yderligere justeringer af forordningsudkastet forud for, at der hentes mandat på sagen på Coreper.

10. Regeringens generelle holdning

Regeringen byder fremskridtsrapporten velkommen.

Regeringen stiller sig overordnet positiv over for cybersolidaritetsforordningen. Regeringen er enig i ambitionen om at styrke medlemsstaternes og EU's kapaciteter til at reagere effektivt og behændigt på cybersikkerhedstrusler og ondsindet aktivitet i cyberdomænet rettet mod EU og medlemsstaterne. Regeringen er ligeledes positiv over for foranstaltninger, der vil styrke solidariteten medlemslandene imellem i tilfælde af væsentlige cybersikkerhedshændelser.

Regeringen er overordnet positiv over for udviklingen i de foreløbige justeringer af forordningsudkastet. Det er centralt for regeringen, at der med forordningen ikke lovgives om interoperabilitetskrav for og informationsdeling mellem de grænseoverskridende sikkerhedsoperationscentre via gennemførelsesretsakter, men at specifikationer for interoperabilitet og informationsdeling skal fastlægges gennem samarbejdsaftaler mellem de medlemsstater, der indgår i et samarbejde om grænseoverskridende sikkerhedsoperationscentre.

11. Tidligere forelæggelse for Folketingets Europaudvalg

Sagen blev forelagt Folketinget Europaudvalg til forhandlingsoplæg den 13. oktober 2023.