DANSK ERHVERV
Børsen
1217 København K

www.danskerhverv.dk
info@danskerhverv.dk
T. + 45 3374 6000

Forsvarsministeriet
Holmens Kanal 9
1060 København K

Att. Nicklas Schreiber Echsner-Rasmussen, Thomas Balslev Rosenzweig, Nikolaj Højer og Ann-Sofie Koutsis Olsen

Den 3. februar 2021

Høring over Europa-Kommissionens forslag til 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)

Dansk Erhverv takker for høringsmaterialet, som er modtaget d. 20. januar. Med en høringsfrist d. 3. februar skal det bemærkes, at det er en meget kort frist til en reel inddragelse af og dialog med medlemmer, særligt da forslaget berører en række sektorer, der ikke har været omfattet at det gældende NIS-direktiv.

Generelle bemærkninger
Forslaget om at sikre et højt fælles cybersikkerhedsniveau i hele unionen (herefter NIS2) betyder bl.a., at flere sektorer end tidligere bliver forpligtet til at indgå i samarbejder med myndighederne om indberetning af sikkerhedstrusler og -hændelser m.m. Hvor NIS-direktivet primært fokuserede på samfundskritiske sektorer (energi, tele, transport m.m.), dækker det nye forslag langt bredere og inkluderer post- og kurertjenester, affaldshåndtering, fremstilling og distribution af fødevarer og kemikalier samt flere typer produktion.

Dansk Erhverv støtter til fulde hensigten bag NIS2. Virksomheder kan lide meget store økonomiske tab i tilfælde af it-sikkerhedshændelser, som det er sket for flere markante danske virksomheder i de seneste år. Desuden er der store samfundsmæssige risici forbundet med angreb på særligt de kritiske samfundssektorer. Her er Danmark kommet godt i mål med implementeringen af NIS-direktivet med udarbejdelse af sektorstrategier og organisering af faste samarbejder mellem myndigheder og decentrale cyber- og informationssikkerhedsenheder (DCIS'er) i seks udpegede samfundskritiske sektorer.

Dansk Erhverv har deltaget arbejdet med nedsættelse af en Tele-DCIS, der forestår informationsudveksling og validering af information mellem sektorerne og CFCS samt vedligeholdelsen af risiko- og sårbarhedsvurderinger. Det bemærkes, at nedsættelse og drift af en DCIS er en betydelig ressourcekrævende opgave for de berørte virksomheder, organisationer og myndigheder. Til gengæld giver samarbejdet en række sikkerhedsmæssige fordele i form af nyttig udveksling af viden og mulighed for hurtigere reaktioner på trusler.

Forslaget betyder også, at de enheder og sektorer, der er tilføjet i NIS2, vil mærke en øget byrde for at leve op til forpligtelserne og det forhøjede sikkerhedsniveau. Den øgede omkostning for disse sektorer er opgjort til 22 pct. i EU-Kommissionens konsekvensanalyse. Virksomheder, der

er omfattet af den nuværende ramme, forventes at skulle øge udgifterne med 12 pct. Hertil kommer en forøgelse af de offentlige omkostninger på området med 20 pct.

I lyset af de skønnede besparelser på 11,3 mia. EUR ved sikkerhedshændelser i hele EU samt en forventet øget robusthed af væsentlige og vigtige samfundsfunktioner kan en vis forøgelse af omkostningerne til cybersikkerhed være berettiget. Det afgørende er imidlertid, at indsatsen målrettes de virksomheder, der i kraft af deres størrelse og rolle i samfundet, har tilstrækkelig betydning til, at de omkostningerne står i proportion til udfordringernes karakter.

Specifikke bemærkninger
Til de specifikke artikler har Dansk Erhverv følgende foreløbige kommentarer:

Artikel 2 (1) Anvendelsesområde
Dansk Erhverv kan i forlængelse af proportionalitetsprincippet støtte afgrænsningen, hvor direktivet – med visse undtagelser – ikke finder anvendelse på enheder, der betragtes som mikrovirksomheder eller små virksomheder.

Artikel 6 Koordineret offentliggørelse af sårbarheder og et europæisk sårbarhedsregister
I lyset af sikkerhedstruslernes grænseoverskridende karakter, er det relevant, at de nationale CSIRT'er samarbejder på tværs af grænser i CSIRT-netværket, og at lade ENISA udvikle og vedligeholde et europæisk sårbarhedsregister. I forbindelse med offentliggørelser om sårbarheder, er det dog afgørende, at der i videst muligt omfang tages hensyn til beskyttelse af oplysninger, der deles af de i berørte virksomheder, herunder i særlig grad oplysninger, der kan have betydning for virksomhedens konkurrencesituation.

Artikel 7 (3) Nationale rammer for styring af cybersikkerhedskriser
I forbindelse med vedtagelse af en national cybersikkerhedshændelses- og kriseberedskabsplan bør NIS2 sikre, at det i højst mulig grad er muligt at bygge videre på de værdifulde indsatser, der allerede er iværksat for de kritiske samfundssektorer.

Artikel 10 Krav til CSIRT'er og deres opgaver
Det er en omfattende række opgaver, CSIRT'ere pålægges, fx på anmodning af en enhed at foretage en proaktiv scanning af de net- og informationssystemer, der anvendes til levering af deres tjenester (2 (e)) Det er imidlertid ikke begrundet, hvorfor denne opgave bør udføres af en offentlig aktør frem for private cybersikkerhedsvirksomheder.

Artikel 18 Risikohåndteringsforanstaltninger i forbindelse med cybersikkerhed
Medlemsstaterne skal sikre, at de berørte enheder foretager en lang række omfattende foranstaltninger, herunder politikker for risikoanalyse og informationssystemsikkerhed, håndtering af hændelser m.m. (art. 18 (2)). Kommissionen kan vedtage gennemførelsesretsakter med henblik på at fastlægge de tekniske og metodiske specifikationer for de i stk. 2 omhandlede elementer og tillægges beføjelser til at vedtage delegerede retsakter med henblik på at supplere de elementer, der er fastsat i stk. 2, for at tage hensyn til nye cybertrusler, den teknologiske udvikling eller sektorspecifikke særtræk.

Det bør præciseres nærmere, hvad det er for tekniske og metodiske specifikationer, der kan vedtages ved gennemførelsesretsakter. Beføjelsen til at supplere elementerne, der er fastsat i stk. 2 for at tage hensyn til nye cybertrusler, den teknologiske udvikling eller sektorspecifikke særtræk forekommer temmelig bred. Der ønsker også her en nærmere præcisering og begrænsning af beføjelsen.

Artikel 20 Rapporteringsforpligtelser
Indrapportering af sikkerhedshændelser er forudsætningen for, at fx cybertrusler kan håndteres så tidligt som muligt og spredning forhindres. Det er dog vigtigt, at enhederne ikke risikerer, at der deles oplysninger, der kan skade virksomhedens konkurrenceposition. Det er væsentligt for at sikre virksomhedernes muligheder og fortsatte tillid i forbindelse med deling af oplysninger om sikkerhedshændelser.

Bestemmelsen i artikel 20 (6) om, at de kompetente myndigheder, CSIRT'erne og de centrale kontaktpunkter skal tage vare på den digitale tjenesteudbyders sikkerhed og kommercielle interesser samt fortrolig behandling af de afgivne oplysninger, når den kompetente myndighed eller CSIRT'en informerer de øvrige berørte medlemsstater og ENISA om en relevant hændelse, er yderst vigtig for virksomhederne.

Dette bør også være udgangspunktet ift. hændelser, der blot behandles på nationalt plan. Den kompetente myndighed eller CSIRTen kan dog kræve, at offentligheden bliver informeret om en hændelse, hvis det er nødvendigt for at forebygge eller håndtere en hændelse. I så fald bør deling af konkrete informationer ske i tæt konsultation med den berørte enhed for at forhindre deling af forretningskritiske oplysninger.

Artikel 31 Generelle betingelser for pålæggelse af administrative bøder
Strafferammen for overtrædelser af forpligtelserne i artikel 18 eller artikel 20 er administrative bøder på maksimalt mindst 10 mio. EUR eller op til 2 pct. af den samlede globale årsomsætning i den virksomhed, som den væsentlige eller vigtige enhed tilhører i det foregående regnskabsår, alt efter hvad der er højest.

Bødeniveauet er meget højt. Ofte vil virksomhederne i forvejen lide et økonomisk tab som følge af fx driftsforstyrrelser, manglende mulighed for afsætning eller tab af omdømme. I det lys forekommer bødeniveauet på op til 10 mio. EUR eller 2 pct. af årsomsætningen ude af proportion.

Vi står naturligvis til rådighed, hvis I ønsker nogle af punkterne uddybet.

Med venlig hilsen,

Poul Noer
Chefkonsulent
Dansk Erhverv

Martin Jensen Buch
Chefkonsulent
IT-Branchen