Rådet for Digital Sikkerhed

08.03.2021

Rådet for Digital Sikkerheds bemærkninger til NIS 2 - Direktiv om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen (NIS2)

Direktivet (NIS2[1]) skal fremme et højt fælles cybersikkerhedsniveau i hele EU og en harmonisering indenfor udvalgte sikkerhedsområder. Dette formål støttes til fulde af Rådet for Digital Sikkerhed, da det kan bidrage til at fremme fokus på sikkerhed i virksomhederne og dermed og mindske økonomiske tab som følge af sikkerhedshændelser og generelt bidrage til at øge trygheden ved digitale løsninger. Rådet mener, der er en række forhold der bør tages i betragtning ved implementering: Implementering af kravene er ressourcekrævende, bøderne er høje og de tekniske krav ikke tilstrækkeligt præcise. De berørte virksomheder skal sikres anonym og fortrolig behandling af deres sager, og endelig er det er helt afgørende, at direktivet samtænkes med nationale initiativer og strategier.

Baggrund

EU-direktivet om sikkerhed i net- og informationssystemer, det såkaldte NIS-direktiv (NIS1) blev vedtaget i 2018. Formålet er at øge cyber- og informationssikkerheden på tværs af EU ved at stille en række tekniske og organisatoriske krav til virksomheder i de berørte sektorer og dermed også sikre en harmonisering af sikkerheden på tværs af EU.

Direktivet stiller krav om, at operatører af samfundskritiske tjenester (tele-, finans-, energi-, sundheds-, transport- og søfartssektoren.) træffer foranstaltninger til at håndtere sikkerheden i de net- og informationssystemer, som de anvender ved levering af deres tjenester. Med NIS 2 ønsker man en yderligere harmonisering af cybersikkerheden på tværs af EU og udvider dermed antallet af berørte sektorer til at inkludere fx post- og kurertjenester, affaldshåndtering, fremstilling og distribution af fødevarer og kemikalier samt flere typer produktion og lægger sig i høj grad op ad GDPR-lovgivningen. Langt flere virksomheder forpligtes til at indgå i samarbejder med myndighederne om indberetning af sikkerhedstrusler og -hændelser m.m. Det har økonomiske konsekvenser for de berørte virksomheder. I nedenstående holdningspapir, redegør Rådet for Digital Sikkerhed for en række synspunkter, der bør tages i betragtning i den videre politiske og implementeringsmæssige proces:

Rådets overordnede holdning

Vi skal skabe en sammenhæng mellem udviklingen indenfor digitalisering og sikkerhed. Derfor er det godt, at der nu kommer en fælles europæisk ramme for sikkerheden med NIS2. NIS2 skal bidrage til, at implementering af informationssikkerhed er ensartethed på tværs af Europa. Derfor bør NIS2 også tage afsæt i eksisterende, anerkendte og internationale standarder indenfor sikkerhed, hvor det er relevant. Det skal bidrage til, at arbejdet med cyber- og informationssikkerhed er gennemsigtigt og dokumenteret. Samtidig bør implementeringen dog tage højde for branchespecifikke forhold på tværs af de berørte virksomheder.

Overordnet set mener vi i Rådet, at implementering af kravene er ressourcekrævende for de berørte virksomheder både når det kommer til investeringer i sikkerhed og medarbejderressourcer. Ligeledes finder vi, at når der skal afgives bøder bør størrelsen på bøden tage afsæt i kritikaliteten i den tjeneste den berørte virksomhed leverer fremfor virksomhedernes størrelse. Når virksomheder indberetter information om hændelser, skal de sikres anonym og fortrolig behandling af deres sager. Endelig er det er helt afgørende, at direktivet samtænkes med nationale initiativer og strategier.

[1] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Revision-of-the-NIS-Directive

Rådets holdning

- *Fremme og harmonisering af EU cybersikkerhed:* Direktivet skal fremme et højt fælles cybersikkerhedsniveau i hele EU og en harmonisering indenfor udvalgte sikkerhedsområdet. Dette formål støttes til fulde af Rådet for Digital Sikkerhed, da det kan bidrage til at fremme fokus på sikkerhed i virksomhederne og dermed og mindske økonomiske tab som følge af sikkerhedshændelser.

- *Ressourcekrævende for de berørte virksomheder:* NIS 1 fokuserede på de samfundskritiske sektorer og med NIS 2 forpligtes flere sektorer som fx affaldshåndtering, fremstilling og distribution af fødevarer og kemikalier til at indgå i samarbejder med myndighederne om indberetning af sikkerhedstrusler og -hændelser m.m. I forlængelse heraf er nedsat en række DCIS'er, der forestår udveksling og validering af information mellem sektorerne indenfor de samfundskritiske sektorer. Nedsættelser og drift af DCIS'er er ressourcekrævende ligesom rapportering og efterlevelse af kravene i NIS 2 er for de berørte virksomheder og myndigheder. Omvendt finder Rådet, at NIS 1 har været en succes og bidraget til at forbedre sikkerheden.

  Endvidere forekommer nogle krav for specifikke ift det er et minimums direktiv.

  Endelig mener Rådet, at hvis små eller mikro virksomheder skal omfattes skal det kun ske hvis deres kritikalitet for samfundet er betydelig. Det fremgår af artikel 2 (anvendelsesområdet) at forpligtelser og krav, som følge af direktivet, målrettes større virksomheder med væsentlig samfundsmæssig betydning, således de øgede omkostninger er proportionelle med formålet

- *NIS2 integration med nationale strategier på området:* NIS 2 direktivet vil sætte rammen for, hvordan den europæiske udvikling indenfor cyber og informationssikkerhed skal være, idet den lægger op til harmonisering og forankring. Rådet mener, at det i en dansk kontekst er helt afgørende, at de krav og tiltag der lægges op til i direktivet følges op i de nationale initiativer. Det gælder
    - Den kommende Nationale Cybersikkerhedsstrategi
    - Den Fælles Offentlige Digitaliseringsstrategi
    - Dataetisk mærke i regi af sikkerhedsmærket

  Danmark skal være på forkant med udviklingen, der kommer, og vi skal sikre sammenhæng og synergi mellem de forskellige nationale og internationale lovkrav og initiativer.

- *Udvikling af metrik for god sikkerhed som grundlag for tildeling af bøder.* Der bør udvikles og beskrives en fælles forståelse og mål for, hvornår de berørte virksomheder er i mål med implementering af de påkrævede sikkerhedsforanstaltninger. Der bør være et objektivt grundlag af målbare (evt. branchespecifikke) parametre – et benchmark ansvarlig myndighed kan tildele bøder ud fra. Ligeledes bør der differentieres mellem kritiske og vigtige enheder. Generelt skal der kun kunne udstedes bøder hvis regelgrundlaget er klart og de aktører som skal virke under NIS 2 ved

hvilke tiltag og foranstaltninger, der forventes iværksat.

- *Brug af internationale standarder til harmonisering:* Det er vigtigt, at der til grund for NIS 2 benyttes internationale standarder (fx ISO 27001), når der skal sikres ensartede og standardiserede tekniske krav, og også at der formuleres tekniske objektive kriterier virksomhederne kan styre efter og for at sikre, at der bygges oven på det sikkerhedsarbejde, som allerede er sat i gang i virksomhederne.

- *Økonomisk byrde for virksomhederne:* Med forslaget øges byrden for de sektorer, der er tilføjet med NIS 2, for at leve op til de nye forpligtelserne og det forhøjede sikkerhedsniveau. De øgede udgifter for de tilføjede sektorerne er opgjort i EU-kommissionens konsekvensanalyse til 22 pct øgede sikkerhedsudgifter og for de allerede omfattede virksomheder til 12 pct øgede sikkerhedsudgifter samt forøgede offentlige omkostninger på 20 pct. Disse omkostninger er i en vis udstrækning berettigede ift. at fremme og harmonisere cybersikkerheden til gavn for øget robusthed i de kritiske sektorer, hvilket også vil mindske tab som følge af hændelser. Der er behov for, at de omkostninger, der væltes over på virksomhederne, er proportionale med effekten af sikkerhedstiltagene. Myndigheder får ganske store beføjelser ift. at give påbud og både til virksomhederne.

- *Videndeling og udveksling af viden og erfaringer:* Koordineret offentliggørelse af sårbarheder og et europæisk sårbarhedsregister er nogle af de gevinster, der kan høstes i forlængelse af NIS2 (Jf artikel 6). De nationale CSIRTer bør i CSIRT netværket samarbejde og udveksle erfaringer om sikkerhedstrusler, ligesom det er oplagt at ENISA udvikler og vedligeholder et europæisk sårbarhedsregister.

- *CSIRT'ers opgaver bør tilfalde private virksomheder:* CSIRT'ere (jf artikel 10) pålægges en bred vifte af opgaver, fx på anmodning at foretage en scanning af net- og informationssystemer, der anvendes til levering af en given enheds tjenester. Denne opgave kan lige så vel tilfalde private *cybersikkerhedsvirksomheder fremfor offentlige.*

- *Nationale rammer for styring af cybersikkerhedskriser:* Når der etableres nationale cybersikkerhedshændelses- og kriseberedskabsplaner, bør disse bygge videre på det arbejde, der er igangsat, og de erfaringer der er gjort, i de samfundskritiske sektorer i forbindelse med NIS 1 (artikel 7 (3)).

- *Behov for præcisering af tekniske risikohåndteringsforanstaltninger:* Myndighederne i medlemsstaterne skal sikre, at virksomheder og organisationer i de berørte sektorer foretager en række omfattende tekniske og organisatoriske foranstaltninger (fx politik for risikoanalyse og informationssystemsikkerhed, håndtering af hændelser m.m. (art. 18 (2)).

- *Myndighederne får store beføjelse*: En ansvarlig myndighed skal sikre, at de berørte virksomheder foretager de nødvendige foranstaltninger. Det bør præciseres og afgrænses, hvilke tekniske specifikationer, der kan vedtages gennemførelsesretsakter jf art. stk 2.

- *De berørte virksomheder skal sikres anonym/fortrolig behandling af deres oplysninger ifm. indrapportering af en hændelse*. Indrapportering af sikkerhedshændelser (art. 20 (6) Rapporteringsforpligtelser) er fundamentet for videndeling om cybertrusler og dermed formindsket risiko for andre. Når CSIRT (eller kompetent myndighed) behandler og deler oplysninger om hændelser og trusler, skal dette ske således den enkelte virksomhed ikke lider skade fx ift. virksomhedens sikkerhed eller konkurrenceposition jf artikel 20 (6). Det er afgørende for, at man som virksomhed kan have tillid til fortsat at dele oplysninger om sikkerhedshændelser. I tilfælde, hvor det alligevel kræves at offentligheden informeres om en hændelse, for at forebygge eller håndtere en hændelse, bør deling af konkrete informationer ske i tæt konsultation med den berørte virksomhed.

- Ansvarlig myndighed: Når der udpeges en ansvarlig myndighed, der også skal tildele bøder, er det vigtigt at denne er uvildig og ligeledes at bøderne tildeles på baggrund af en objektiv og målbar vurdering – gerne ud fra branchespecifikke kriterier. Hvis f.eks. den ansvarlige myndighed bliver CFCS, skal det overvejes, om det giver problemer at en myndighed under forsvaret kan uddele bøder til aktører i civilsamfundet.

- *Højt bødeniveau*: Bøder bør gives udfra kritikaliteten og dette skal ikke vurderes af den enkelte branche, men af en uvildig myndighed. Strafferammen for overtrædelser af forpligtelserne i artikel 18 eller artikel 20 er administrative bøder på maksimalt 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. Det fremgår af Artikel 31, ”Generelle betingelser for pålæggelse af administrative bøder”. Bødeniveauet er for højt. I tilfælde af et sikkerhedsbrud vil den berørte virksomhed i forvejen have haft udgifter til driftsforstyrrelser, manglende mulighed for afsætning eller opleve tab af omdømme.