IT-BRANCHENS HØRINGSSVAR TIL LOV OM FORANSTALTNINGER TIL SIKRING AF ET HØJT CYBERSIKKERHEDSNIVEAU

### UDARBEJDET I REGI AF IT-BRANCHENS

### POLICY BOARD FOR CYBERSIKKERHED

****

IT-Branchen har modtaget Forsvarsministeriets udkast til forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (herefter NIS2-lovudkastet) i høring. Af nærværende høringssvar fremgår vores bemærkninger til NIS2-lovudkastet.

Generelle bemærkninger

IT-Branchen vil gerne kvittere for muligheden for at kommentere på det foreliggende danske NIS2-lovudkast, som tydeligt hviler på et omstændeligt lovarbejde, og som i udgangspunktet lægger op til et fornuftigt NIS2-implementeringsniveau i Danmark, selvom de nærmere NIS2-sektorkrav stadig udestår.

Dog vil det være afgørende for en hurtig og effektiv implementering af NIS2-kravene, at NIS2-loven hurtigst muligt følges op af sektorbekendtgørelser og konkret hjælp og vejledning til virksomhederne. Virksomhederne bør i den forbindelse også kunne rette henvendelse til en sektoransvarlig myndighed og modtage et klart og bindende svar på, om de er omfattede af NIS2.

Hvad angår kommunerne, mener IT-Branchen, at de utvetydigt bør omfattes af NIS2, og at dette eksplicit bør fremgå af NIS2-loven.

Endelig savner IT-Branchen nogle klare hegnspæle i NIS2-lovudkastet for CFCS’ ansvars­område og opgaver som CSIRT og en præcisering af snitfladerne til og samarbejdet med de private cybersikkerhedsaktører. CFCS står overfor en markant større, overordnet CSIRT-opgave end tidligere, som der kan sættes spørgsmålstegn ved, om centret har de nødvendige ressourcer til at løfte, og som alt andet lige ikke kan løftes uden omfattende involvering af private aktører.

Vores bemærkninger uddybes i det følgende.

Specifikke bemærkninger

Minimumsimplementering og sektorbekendtgørelser

Der lægges med NIS2-lovudkastet op til en minimumsimplementering af NIS2-direktivet, og lovudkastets krav om foranstaltninger til styring af cybersikkerhedsrisici gengiver, jf. §6, NIS2-direktivets artikel 21 uden uddybelser. IT-Branchen ser frem til, at de konkrete krav til virksomhedernes cybersikkerhed præciseres i sektorbekendtgørelserne udarbejdet af de relevante ressortmyndigheder i samarbejde med FMN/CFCS.

IT-Branchens input:

* Det præciseres ikke i NIS2-lovudkastet, men IT-Branchen henstiller til, at bekendtgørelserne – ligesom NIS2-hovedloven – træder i kraft pr. 1. marts 2025, og at bekendtgørelserne *inden* ikrafttrædelsesdatoen og hurtigst muligt suppleres af konkrete vejledninger til virksomhederne fra de relevante sektoransvarlige myndigheder, så virksomhederne får de bedst mulige betingelser for rettidigt at efterleve NIS2-lovkravene.
* Henset til betydningen og kompleksiteten af indholdet i de kommende sektorbekendt­gørelser henstiller IT-Branchen til, at den vejledende høringsfrist på fire uger som minimum overholdes og også gerne forlænges, hvilket ikke altid er praksis.
* Såfremt sektorbekendtgørelserne og de præciserende vejledninger ikke tilgængelig­gøres inden NIS2-lovens ikrafttræden, bør de sektoransvarlige myndigheder indledningsvis anlægge et dialogbaseret og vejledende tilsyn og ikke gøre brug af deres sanktionsbeføjelser, før de NIS2-omfattede enheder har haft passende mulighed for at sætte sig ind i samt implementere de nærmere sektorlovkrav. Til det formål vil vejledninger og konkrete eksempler på bedste praksis – og ikke blot bekendtgørelser – være nødvendige for at understøtte de omfattede enheder i regelefterlevelsen. Til inspiration ift. konkretiseringsniveau har vi i [IT-Branchens eget NIS2-vejlednings­univers](https://itb.dk/nis2-univers/hvordan-lever-jeg-op-til-nis2/saadan-kommer-du-i-gang-hvis-du-er-indirekte-omfattet-nis2/) listet en række konkrete, tekniske minimumsforanstaltninger, der varierer afhængigt af vurderet risikoprofil.
* Som et af de vigtigste, første fokusområder skal der tilvejebringes vejledning, der kan hjælpe omfattede enheder med en kritikalitetsvurdering – dvs. hjælp og vejledning til at vurdere, hvilken del af en enheds forretning, der ud fra en risikovurdering kan have betydning for anmeldelse af sikkerhedshændelser. Herved opnås en væsentlig forståelse til at sikre en unødig overimplementering af NIS2 i danske virksomheder.
* Herudover efterlyser IT-Branchen – i NIS2-lovudkastet og generelt – en detaljeret oversigt over de forskellige sektoransvarlige myndigheder, som de danske virksomheder kan modtage vejledning fra og rette henvendelse til med tvivlsspørgsmål.

Ikrafttrædelsesdato 1. marts 2025

Jf. §33 i NIS2-lovudkastet træder loven i kraft den 1. marts 2025, lidt over fire måneder efter NIS2-direktivets implementeringsfrist.

IT-Branchens input:

* IT-Branchen finder det uhensigtsmæssigt, at vi i Danmark ikke overholder NIS2-direktivets implementeringsfrist, og at vedtagelsen af den danske NIS2-lov endnu engang udskydes. Det sender et uheldigt signal – også til de cyberkriminelle – om, at cybersikkerheden ikke tages alvorligt i Danmark, og at vi nedprioriterer området.
* IT-Branchen forudser i henhold til art. 26 stk. 2, at danske virksomheder, der – foruden Danmark – opererer i eller leverer tjenesteydelser til NIS2-omfattede virksomheder i andre EU-lande, hvor den nationale implementeringslovgivning ikke bliver forsinket i samme omfang som i Danmark, kan risikere at være omfattet af jurisdiktionen i andre lande end Danmark i perioden frem til den 1. marts 2025. Det er således uklart, hvilket lands lov der gør sig gældende, og hvad der sker med jurisdiktionsbestemmelsen for omfattede enheder under de i §2 stk. 3-identificerede områder, så længe vi ikke har en vedtaget NIS2-lov i Danmark.
* For at undgå udfordringer og uklarheder som de ovenfor beskrevne – også på sigt – er det ifølge IT-Branchen vigtigt, at Danmark bidrager aktivt til en konsekvent harmonisering af NIS2-reglerne på tværs af EU-medlemslandene.
* For at sikre ensretning og effektiv implementering på tværs af sektorer på nationalt plan, vil det tilsvarende være vigtigt, at de særskilte cybersikkerhedsreguleringer i fx energi- og telesektorerne – der skal tilpasses NIS2-kravene – i videst muligt omfang fremsættes, behandles og træder i kraft på samme tid og parallelt med NIS2-loven og de relaterede sektorbekendtgørelser.

**Omfattede enheder og registreringspligt**

Det fremgår af §9, at det påfalder ”DNS-tjenesteudbydere, topdomænenavneadministratorer, enheder der leverer domænenavnsregistreringstjenester og udbydere af cloudcomputing­tjenester, datacentertjenester, indholdsleveringsnetværk, administrerede tjenester, administrerede sikkerhedstjenester, onlinemarkedspladser, onlinesøgemaskiner og platforme for sociale netværkstjenester” selv at registrere sig hos den relevante, kompetente myndighed. Af §9 stk. 2 følger det, at registreringen skal ske senest den 17. januar 2025.

IT-Branchens input:

* Det er IT-Branchens overbevisning, at det på det eksisterende tekstgrundlag i NIS2-lovudkastet vil blive vanskeligt for mange danske enheder/virksomheder at vurdere, om de er omfattet af NIS2 og proaktivt bør lade sig registrere hos den relevante, kompetente myndighed. Særligt de mange ny-omfattede enheder, der følger af et markant udvidet anvendelsesområde sammenlignet med NIS1, vil blive udfordret.
* For at undgå ovenstående uklarhed/uvished – og en medfølgende tilbageholdenhed i virksomhederne ift. at gå i gang med at styrke cybersikkerhedsniveauet – foreslår IT-Branchen følgende tiltag:
	+ Hurtig tilvejebringelse af konkret vejledningsmateriale og hjælp til enheder/virksomheder med at vurdere, om de er omfattet af NIS2
	+ Hurtig identificering og offentliggørelse af de sektoransvarlige myndigheder, hvorfra virksomheder kan modtage vejledning og rette henvendelse med tvivlsspørgsmål (jf. tidl. input i nærværende høringssvar)
	+ Etablering af en instans/funktion i hver enkel ”relevant kompetent myndighed”, hvor virksomheder løbende kan henvende sig og modtage klart og bindende svar på, om de er omfattet af NIS2. Som inspiration kunne man etablere en ordning, som anvendes inden for skatteområdet, hvor der kan indhentes bindende svar fra myndighederne.
* IT-Branchen finder det desuden problematisk og juridisk uholdbart, at registreringen til relevante kompetente myndighed ifølge lovudkastet skal ske senest den 17. januar 2025 – det vil sige 1,5 måned inden, der er en vedtaget NIS2-lov at falde tilbage på. Kan der være tale om, at datoen fejlagtigt er videreført fra NIS2-direktivet, og at man ikke har indregnet den danske lovforsinkelse? Af §10 stk. 2 følger det, at domæneregistreringstjenester skal registrere sig senest den 17. april 2025.

**Kommunerne**

Det fremgår af §1 stk. 7, at vedkommende minister inden for sit område kan fastsætte regler om, at loven helt eller delvist også finder anvendelse på henholdsvis offentlige forvaltningsenheder på lokalt plan og uddannelsesinstitutioner. Det fremgår videre af bemærkningerne til §1, at det på nuværende tidspunkt ikke er intentionen at fastsætte regler om, at kommunerne omfattes af loven.

IT-Branchens input:

* IT-Branchen er indforstået med, at NIS2-direktivet giver medlemslandene mulighed for selv at vurdere og bestemme, om direktivet skal finde anvendelse på offentlige forvaltningsenheder på lokalt plan, såfremt disse ikke leverer tjenester i kritiske sektorer, som omfatter dem via direktivets anvendelsesområde. IT-Branchen mener imidlertid, at kommunerne utvetydigt bør omfattes af NIS2, og at dette eksplicit bør fremgå af den danske NIS2-lov. For at imødegå cybertruslen og værne om vores samfundssikkerhed, er der behov for, at de offentlige myndigheder lever op til en række skærpede og mere ensartede cybersikkerhedskrav på tværs af stat, regioner og kommuner. Hertil vil NIS2-loven være en kærkommen løftestang til at hæve cybersikkerhedsniveauet i kommunerne. Cybersikkerheden i kommunerne er vital for at bevare borgernes tillid til systemerne og for at sikre opbakning til de effektive, digitale løsninger, der er nødvendige for kritiske, kommunale velfærdsydelser og den gode borgerservice. I yderste konsekvens kan det store antal cyberangreb mod kommunerne, som KL har identificeret (hver fjerde kommune rammes dagligt af over 200 forsøg på angreb), risikere at kompromittere eller skade de samfundsvigtige funktioner, som kommunerne har ansvaret for.
* I forlængelse af ovenstående finder IT-Branchen det nødvendigt, at NIS2-loven præciserer, hvordan og hvor meget kommunerne er omfattet, så der ikke kan opstå uklarheder eller fortolkningstvivl (fx ift. det at være sundhedstjenesteyder), og så ingen kommune kan undslå sig at være omfattet af NIS2. Der skal videre skabes klarhed omkring, hvad det har af betydning ift. ansvarspådragelsen, når kritiske tjenester og velfærdsydelser udliciteres i kommunerne mv. IT-Branchen noterer sig også, at KL selv har ytret ønske om, at kommunerne omfattes af NIS2.
* Af §4 stk. 2 fremgår det, at kommuner og regioner omfattes af loven i det omfang, de måtte udføre opgaver som udbydere af offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester. IT-Branchen henstiller til, at det præciseres og eventuelt eksemplificeres, hvilke typer af sådanne kommunikationsnet og -tjenester i kommunalt og regionalt regi, der her henvises til.

**Risikovurdering**

§6 i NIS2-lovudkastet angiver, at væsentlige og vigtige enheder skal træffe en række ”passende” og ”forholdsmæssige” tekniske, operationelle og organisatoriske minimums­foranstaltninger til styring af cybersikkerhedsrisici.

IT-Branchens input:

* IT-Branchen vil gerne påpege vigtigheden af, at proportionaliteten af de angivne minimumsforanstaltninger tager udgangspunkt i en samlet risikovurdering, der også indebærer de samfundsmæssige og økonomiske indvirkninger af en hændelse. Derfor foreslås det, at andet led/afsnit i Artikel 21 stk. 1 i NIS2-direktivet tilføjes i starten af §6 i den danske NIS2-lov, ligesom første led/afsnit i Artikel 21 stk. 1 i NIS2-direktivet allerede er gengivet i starten af §6. Det manglende led lyder: ”Under hensyntagen til det aktuelle teknologiske stade og i givet fald til relevante europæiske og internationale standarder samt gennemførelsesomkostningerne skal de i første afsnit omhandlede foranstaltninger tilvejebringe et sikkerhedsniveau i net- og informationssystemer, der står i forhold til risiciene. Ved vurderingen af proportionaliteten af disse foranstaltninger tages der behørigt hensyn til graden af enhedens eksponering for risici, enhedens størrelse og sandsynligheden for hændelser og deres alvor, herunder deres samfundsmæssige og økonomiske indvirkning.” Leddet er gengivet i betragtningerne til §6 nederst på side 229, men der må ikke lovgives i betragtningerne, hvorfor det bør være en del af selve lovteksten.

**Underretningspligter og frivillig indberetning**

§12,13, 14, 15, 16.

IT-Branchens input:

* IT-Branchen undrer sig over, at det kun er frivillige indberetninger af hændelser under §14, som er undtaget aktindsigt. De almindelige indberetninger som følge af §12 er ikke undtaget aktindsigten. Dette bør genovervejes, eller også bør man som minimum begrænse aktindsigten i de almindelige indberetninger under §12, da der allerede under databeskyttelsesreglerne har været hændelser, hvor der af Datatilsynet er givet aktindsigt i sager, hvor dette har skadet efterforskningen og skabt problemer for de omfattede organisationer.
* Af §16 fremgår det, at myndighederne kan vælge at offentliggøre væsentlige hændelser, hvis det er nødvendigt for at forebygge og håndtere andre hændelser, eller hvis det er i offentlighedens interesse. Dette skal ifølge NIS2-udkastet fornuftigvis ske efter høring af den pågældende enhed, men IT-Branchen efterlyser, at det nærmere præciseres, hvornår/hvor hurtigt en hændelse kan offentliggøres – fx om der vil være tilstrækkelig tid til, at den pågældende enhed kan have håndteret hændelsen – eller hvor lang høringen af den pågældende enhed kan/vil være.
* IT-Branchen efterlyser en utvetydig melding om, hvem underrettelsespligten påfalder i tilfælde, hvor leverandører er involveret, og hvorvidt tidsrammen gælder fra det tidspunkt, den NIS2-omfattede enhed bliver opmærksom på hændelsen, eller fra det tidspunkt enhedens leverandør bliver det. Her savner vi sondring mellem eksempelvis ”data processor” og ”data controller” som kendt fra GDPR.
* For at lette de administrative omkostninger for erhvervslivet og fremme den generelle indberetning, vil det være vigtigt, at der faciliteres én indberetning/indgang/formular – også for væsentlige og vigtige enheder, der er beskæftiget i mere end én af de NIS2-omfattede sektorer (à la Virk.dk i dag).

**CFCS som CSIRT**

Center for Cybersikkerhed (CFCS) skal ifølge NIS2-lovudkastet varetage rollen som CSIRT. Af §17-19 følger CSIRT’ens opgaver.

* IT-Branchen henstiller til, at CFCS’ ansvarsområde og opgaver som CSIRT præciseres yderligere i NIS2-loven, herunder ikke mindst hvad angår snitfladerne til og samarbejdet med de private cybersikkerhedsaktører. Med et markant øget anvendelsesområde sammenlignet med NIS1 – og et estimeret antal omfattede enheder i Danmark, der stiger fra 130 til 2.000 – vil der blive tale om en markant større, overordnet opgave for en CSIRT end tidligere, som der kan sættes spørgsmålstegn ved, om CFCS har de nødvendige ressourcer til at løfte, og som alt andet lige ikke kan løftes uden omfattende involvering af private aktører. Der er ydermere behov for nogle klare hegnspæle for en offentlig CSIRT’s aktiviteter i NIS2-loven, så der ikke opstår unfair konkurrence og skævvridning af det private marked. Endelig vil det være væsentligt for de NIS2-omfattede enheder at få klarhed over, hvad der forventes løftet af en offentlig CSIRT, og hvornår og hvordan der henvises til hjælp fra private aktører.

**Tilsyn og håndhævelse**

IT-Branchen finder det positivt, at lovudkastet lægger op til en fælles tilgang til tilsyn og en tæt koordinering mellem de forskellige sektoransvarlige myndigheder – særligt for at tilgodese enheder, der indgår i forskellige sektorer - med mulighed for fælles tilsynsbesøg og deling af tilsynsressourcer/-sekretariater på tværs af ressortmyndigheder.

IT-Branchens input:

* Der henvises i NIS2-lovudkastet til et forestående analysearbejde – og det foreslås, at vedkommende ressortminister bemyndiges til at fastsætte nærmere regler i bekendtgørelsesform – men IT-Branchen efterlyser en præcisering af, hvilke certificeringer og godkendelser der kan blive genstand for suspension ved manglende NIS2-regelefterlevelse. Samtidig er det i NIS2-lovudkastet ikke beskrevet, om/hvordan en midlertidig suspension vil have opsættende virkning, hvis suspensionen påklages til en rekursmyndighed, eller der anlægges en sag ved domstole.

Øvrige, tekstnære bemærkninger

* Definitionen på side 231 af, hvilke net- og informationssystemer, der er omfattet ud fra en betragtning af, hvordan de kan påvirke enhedens levering af de tjenester eller aktiviteter, som er baggrunden for at enheden er omfattet af direktivet, bør fremhæves og gøres til en del af de fleste vejledninger, da den manglende forståelse af dette skaber forvirring mange steder.
* På side 255 nævnes muligheden for at DCIS’erne kan komme med tilbagemeldinger på indberetning af hændelser. Hvis dette skal være en mulighed, bør det så ikke fremgå mere tydeligt af lovteksten, at DCIS’erne kan spille en myndighedsrolle i forhold til implementeringen af direktivet i dansk lovgivning?
* På side 280 står der, at væsentlige enheder vil blive underlagt ”*løbende tilsyn*”. Dette bør uddybes eller konkretiseres, således at det er tydeligt om dette fx betyder at alle væsentlige enheder skal underlægges mindst et tilsyn om året.
* Af artikel 32 stk. 4 litra g fremgår det at den kompetente myndighed kan udpege en overvågningsansvarlig, men på side 282 (og § 22 punkt 5) fremgår det, at den kompetente myndighed kan opbyde enheden at udpege en person med ansvar for i en nærmere fastsat periode at føre tilsyn med enhedens overholdelse af §§ 6, 12, 13, 15 og 16, samt regler udstedt i medfør heraf. Det virker som om, der ikke helt er sammenhæng mellem direktivets tekst og lovens tekst på dette punkt.

På vegne af IT-Branchen og IT-Branchens Policy Board for Cybersikkerhed,

Med venlig hilsen

Troels Johansen

Chefkonsulent

IT-Branchen

Mobil: 9384 9383

Mail: tjoh@itb.dk