Regionledningskontoret
Vesna Lucassi

TJÄNSTEUTLÅTANDE
2024-05-07

RS 2024-0256

Regionstyrelsen

Yttrande över delbetänkandet Nya regler för cybersäkerhet (SOU 2024:18)

Regionledningskontorets förslag till beslut

Regionrådsberedningen föreslår att regionstyrelsen beslutar följande.

1. Regiondirektörens tjänsteutlåtande utgör Region Stockholms yttrande till Försvarsdepartementet över delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18).

2. Paragrafen justeras omedelbart.

Sammanfattning

Försvarsdepartementet har remitterat delbetänkandet *Nya regler om cybersäkerhet (SOU 2024:18),* till Region Stockholm för yttrande. Betänkandet innehåller bland annat förslag till införlivning av Europaparlamentets och rådets nya EU-direktiv NIS 2 i svensk rätt genom en ny cybersäkerhetslag som föreslås träda i kraft 2025-01-01. Cybersäkerhetslagen föreslås ersätta lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster som därmed föreslås upphävas. Utredningen kommer i sitt slutbetänkande att lämna förslag på införlivning av även EU:s CER-direktiv om kritiska entiteters motståndskraft. Båda direktiven är s.k. minimidirektiv med innebörd att medlemsstaterna får anta mer långtgående bestämmelser.

Region Stockholm ser i stort positivt på utredningens förslag men lämnar flera synpunkter som samtliga syftar till att underlätta för de som har att tillämpa den föreslagna lagstiftningen. Synpunkterna rör exempelvis definitioner och begrepp, där Region Stockholm pekar på skillnaden i internationell och nationell terminologi för området och betonar vikten av stringens i vilka termer som används i betänkandet och förslaget till lagstiftning.

I yttrandet lyfter Region Stockholm vikten av informationsspridning till NIS-leverantörer utifrån inrapporterade incidenter. Vidare finner Region Stockholm utredningens förslag att lägga tyngdpunkten på informationsplikt till kunder om incidenter snarare än om skyddsåtgärder olycklig och önskar att utredningens förslag harmonieras med andemeningen i NIS 2-direktivet. Region Stockholm pekar även på att regionens verksamhet sträcker sig över flera sektorer och därmed kommer träffas av flera föreskrifter. För att undvika tolkningsproblem ser Region Stockholm istället

att en myndighet borde få ansvar för att utfärda föreskrifter. Följaktligen önskar regionen att samordning sker sinsemellan berörda tillsynsmyndigheter i samband med tillsyn. Region Stockholm menar slutligen att genomförd konsekvensanalys inte i tillräcklig omfattning klarlägger de kostnadsdrivande faktorer som utredningens förslag medför. Region Stockholm bedömer, till skillnad från utredningen, att implementeringen av NIS 2- och CER-direktivet är omfattande och medför kostnadsökningar för regionen.

Bakgrund

Försvarsdepartementet har remitterat delbetänkandet *Nya regler om cybersäkerhet (SOU 2024:18),* till Region Stockholm för yttrande. Remissen innehåller bland annat förslag till cybersäkerhetslag som föreslås träda i kraft 2025-01-01. Cybersäkerhetslagen föreslås ersätta lagen om informationssäkerhet (2018:1174). Cybersäkerhetslagen behöver sedan konkretiseras i myndighetsföreskrifter. Förslag till uppdaterade föreskrifter har ännu inte offentliggjorts av tillsynsmyndigheterna. Många av kraven i lagen om informationssäkerhet omhändertas genom Region Stockholms riktlinjer för informationssäkerhet.

EU-kommissionen presenterade 2020 ett förslag på lagstiftning (NIS 2-direktivet) för att ersätta NIS-direktivet. NIS 2-direktivet ska vara implementerat i medlemsländerna senast den 2024-10-18. Syftet med NIS 2 är att minska fragmenteringen av den inre marknaden och innebär ett mer detaljerat regelverk avseende åtgärder för informationssäkerhet, för att möta rådande och framtida säkerhetsbehov. Tillämpningsområdet för regleringen utvidgas till att omfatta aktörer inom fler sektorer än det tidigare NIS-direktivet. De tillkommande sektorerna är bland annat förvaltning av IKT-tjänster (mellan företag), offentlig förvaltning, post- och budtjänster, digitala leverantörer, forskning och hälso- och sjukvårdssektorn i form av till exempel tillverkning av läkemedel.

NIS 2-direktivet har till viss del samordnats och har vissa likheter med EU:s CER-direktiv (Critical Entities Resilience Directive) som syftar till att minska sårbarheter och stärka motståndskraften hos samhällsviktiga verksamheter. CER-direktivet ställer krav på bland annat riskbedömningar, åtgärder för att stärka robusthet och motståndskraft (t.ex. fysiskt skydd av lokaler).

Region Stockholms yttrande

Utifrån ett omfattande och komplext uppdrag och kort tid har utredningen genomfört en betydande insats. Region Stockholm har tagit del av delbetänkandet och ser med fördel att förslagen till lagtext förtydligas i syfte att underlätta för de som har att tillämpa den föreslagna lagstiftningen.

1–2 kap. förslag till cybersäkerhetslag

Region Stockholm konstaterar inledningsvis att utredningen har valt att definiera ”cybersäkerhet” genom att hänvisa till art. 2.1 i Cybersäkerhetsakten,

där cybersäkerhet definieras som all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot.

Region Stockholm förstår vikten av begrepp i största möjliga utsträckning bör ges samma betydelse när de tillämpas nationellt respektive internationellt, och särskilt när det gäller det europeiska samarbetet. Samtidigt bör skillnaden i internationell och nationell terminologi lyftas och svårigheten att anpassa NIS 2-direktivets definitioner till föreslagen lagstiftning. Till exempel kan utredningens nuvarande förslag ”cybersäkerhet” ge upphov till begreppsförvirring om vad som egentligen avses med begreppet i det sammanhang det används.

I nationella sammanhang har oftast informationssäkerhet varit ett paraplybegrepp i betydelsen alla slags hot mot såväl digital som icke-digital information, där cybersäkerhet utgjort en delmängd för att särskilt peka på händelser med antagonistiska hot mot digital information. Region Stockholm önskar därför ett förtydligande i denna del, om hur cybersäkerhet ska förstås, och en stringens i vilka termer som används i betänkandet och förslaget till lagstiftning.

Region Stockholm upplever bestämmelserna gällande kvalificerings-grunder som svåra att tolka när det gäller verksamhet som bedrivs i bolags-form. Utgångspunkten i betänkandet är att all verksamhet inom kommun och region omfattas av den föreslagna lagstiftningen. Samtidigt påtalas att det är varje verksamhetsutövare själv som ska bedöma huruvida denne omfattas. För att utröna om verksamhet som bedrivs i bolagsform omfattas krävs en genomgång och tolkning av NIS 2-direktivet, ibland andra rättsakter från EU och förslaget till cybersäkerhetslag. Även efter en sådan genomgång och tolkning kan det fortfarande vara oklart om verksamhet som bedrivs i bolagsform med säkerhet kan ta ställning i frågan. Av betänkandet framgår att Myndigheten för samhällsskydd och beredskap (MSB) respektive övriga tillsynsmyndigheter via vägledning kan ge stöd vid sådan bedömning. I nuläget har MSB och andra tillsynsmyndigheter inte offentliggjort förslag till föreskrifter eller annat stöd. Detta gör det svårt för verksamheten att ta ställning till huruvida de omfattas av den föreslagna lagstiftningen eller inte och därmed i tid kunna förbereda sig och göra de anpassningar som behövs. Tydlighet och enkelhet att kunna bedöma huruvida verksamhet som bedrivs i bolagsform omfattas behöver eftersträvas. Det är av vikt att arbetet med föreskrifter eller annat stöd från MSB respektive övriga tillsynsmyndigheter påskyndas och att förslagen remitteras.

Verksamhet som bedrivs i form av kommunförbund, och för den delen även kommunalförbund, nämns överhuvudtaget inte i utredningen vilket gör det

än svårare att bedöma och tolka huruvida de omfattas av den föreslagna lagstiftningen.

3 kap. förslag till cybersäkerhetslag
vad gäller incidentrapportering vill Region Stockholm påtala vikten av att tillsynsmyndigheterna inte efterfrågar fler uppgifter än som krävs enligt art. 23 NIS 2-direktivet i syfte att minska den administrativa bördan för rapporterande myndigheter. Region Stockholm önskar även lyfta vikten av informationsspridning till NIS-leverantörer utifrån inrapporterade incidenter (t.ex. kring indikatorer för kompromettering och skyddsåtgärder) samt effektiva och säkra kommunikationsvägar för att möjliggöra det.

Av 3 kap. 6 § 3 st. förslag till cybersäkerhetslag framgår att skyldigheten att informera kunder vid betydande incidenter och cyberhot är obligatorisk och ska ske inom 72 timmar. Region Stockholm ställer sig frågande till utredningens förslag i denna del och önskar påtala följande. Region Stockholm noterar att tyngdpunkt och reglering lagts på information till kunder om en incident snarare än på information om avhjälpande åtgärder. Kunderna ska enligt utredarens förslag informeras om avhjälpande åtgärder enbart vid behov. Region Stockholm tolkar att NIS 2-direktivet i art.23.2, i motsats till utredningen, i stället tar sikte på informationsplikt om cyberhot snarare än incidenter, med en tyngdpunkt på att informera kunder om möjliga skyddsåtgärder som kan vidtas för att motverka cyberhotet. Information om själva cyberhotet ska enligt art. 23.2 ske där så är lämpligt.

Region Stockholm bedömer att information om själva incidenten till kunder skulle kunna stå i konflikt med till exempel förundersöknings-sekretess. Region Stockholm förespråkar därför att utredningens förslag i 3 kap. 6 § 3 st. ses över och harmonieras med NIS 2-direktivet i denna del.

4 kap. förslag till cybersäkerhetslag
Region Stockholm har i princip inget emot flera tillsynsmyndigheter så länge de samordnar sig vad gäller tolkning av lagstiftning och tidpunkt för tillsyn i syfte att undvika otydliga eller oförenliga föreskrifter. Frågor som är gemensamma för samtliga tillsynsmyndigheter behöver tillämpas och tolkas på likartat sätt för att underlätta för tillsynsobjekten. I syfte att undvika parallella processer behöver tillsynsmyndigheterna samarbeta kring omfattning och separering av tillsynsärenden.

Region Stockholm saknar dock en analys avseende behovet och nyttan gällande föreskrifter för varje tillsynsområde kontra vinsten med enhetliga föreskrifter för samtliga tillsynsområden. Region Stockholm har svårt att se hur föreskrifterna kan komma att skilja sig åt innehållsmässigt mellan olika sektorer/tillsynsmyndigheter utan ser hellre att en myndighet får ansvar för

att utfärda föreskrifter eftersom det annars kan leda till tolkningsproblem hur regionen ska förhålla sig till flera föreskrifter. Som exempel kan nämnas nätverk i regioner som stödjer både sektorerna offentlig förvaltning och hälso- och sjukvård.

Region Stockholm önskar att en verksamhetsutövares anmälan ska ske till en central kontaktpunkt, och att samordning därefter sker sinsemellan de berörda tillsynsmyndigheterna.

Konsekvensanalys
Av konsekvensanalysen, avsnitt 12.7 i delbetänkandet, framgår att utredningen föreslår att ekonomiska konsekvenser finansieras inom verksamhetsutövarens befintliga budgetram. Region Stockholm menar att konsekvensanalysen inte i tillräcklig omfattning klarlägger de kostnadsdrivande faktorer som utredningens förslag medför. Region Stockholm bedömer att implementeringen av såväl NIS 2 som CER är omfattande och kommer att medföra kostnadsökningar för regionen, och hänvisar till den kommunala finansieringsprincipen. Därutöver finns även stort utrymme för tolkning av reglerna och risk för ojämn tillämpning då föreskrifter och konkreta krav ännu saknas.

Implementering av lagförslaget bör följas av riktat stöd för att effekthemtagning ska kunna ske i den takt som är önskvärd. För att underlätta implementeringen av NIS 2 har Region Stockholm identifierat ett behov av tydliga, enhetliga och gemensamma arbetsprocesser. Det rör framför allt områdena systemförteckning, övergripande riskhantering och incidentrapportering.

Ekonomiska konsekvenser
Region Stockholm bedömer att implementering av NIS2-direktivet kommer att leda till kostnadsökningar. Mot bakgrund att utredningens förslag utgör ett delbetänkande samt att föreskrifter och konkreta krav ännu saknas, är dock bedömning av ekonomiska konsekvenser inte möjlig att göra i nuläget.

Emma Lennartsson
Regiondirektör

Susanne Bayard
IT-direktör

Beslutsunderlag

1. Sammanfattning av Nya regler om cybersäkerhet (SOU 2024:18)

Beslutsexpediering

1. Försvarsdepartementet

Godkänd av Emma Lennartsson, 2024-05-07