Stockholms stad

**PM Rotel I (Dnr KS 2024/326)**

# Delbetänkandet - Nya regler om cybersäkerhet (SOU 2024:18)

Remiss från Försvarsdepartementet
Remisstid den 28 maj 2024

## Förslag till beslut

Borgarrådsberedningen föreslår att kommunstyrelsen beslutar följande.

Remissen besvaras med hänvisning till vad som sägs i stadens promemoria.

**Föredragande borgarrådet Karin Wanngård**

## Sammanfattning av ärendet

Försvarsdepartementet har remitterat ett delbetänkande - *nya regler om cybersäkerhet* bland annat till Stockholms stad för yttrande.

I delbetänkandet lämnas förslag på hur NIS2-direktivet ska införlivas i svensk lagstiftning. NIS2-direktivet ersätter det tidigare NIS-direktivet från 2016 och ställer krav på säkerhet i nätverks- och informationssystem. Delbetänkandet föreslår att direktivet i huvudsak ska införlivas genom en ny lag som kommer att benämnas som cybersäkerhetslagen. Genom NIS2-direktivet skärps kraven för verksamhetsutövare och direktivet innefattar bestämmelser rörande mer omfattande samverkan inom unionen. Syftet är att uppnå högre cybersäkerhet.

## Beredning

Ärendet har remitterats till stadsledningskontoret och Stockholms Stadshus AB. Stockholms Stadshus AB har underremitterat remissen vidare till AB Stokab och Stockholm Vatten och Avfall AB.

*Stadsledningskontoret* står bakom alla väsentliga delar i det som föreslås i delbetänkandet.

*Stockholms Stadshus AB* har inget att tillägga utan ställer sig bakom dotterbolagens synpunkter.

*AB Stokab* konstaterar att utredningen föreslår en cybersäkerhetslag med övergripande regleringar, men att lagen lär behöva kompletteras med föreskrifter som meddelas av utpekad tillsynsmyndighet. Föreskrifterna från tillsynsmyndigheterna kommer således att utgöra ett mycket viktigt komplement till de skyldigheter som

föreslås i den nya cybersäkerhetslagen och det är angeläget att dessa utfärdas skyndsamt.

*Stockholm Vatten och Avfall AB* anser att implementering av NIS2 kommer leda till stora kostnader och små och långsamma förbättringar och att små organisationer kommer att ha svårt att efterfölja kraven.

## Föredragande borgarrådets synpunkter

Stärkt cybersäkerhet är en angelägen fråga för hela kommunsverige och därför välkomnar jag Försvarsdepartementets delbetänkande *Nya regler om cybersäkerhet SOU 2024:18*.

Inom den offentliga förvaltningen finns det idag olika regleringar på cybersäkerhetsområdet. Utredningen konstaterar att detta skapar en ojämn och fragmenterad implementering av cybersäkerhetsskyddet inom den offentliga förvaltningen. Det i sin tur skapar ojämlika förhållanden mellan verksamheter inom den offentliga förvaltningen, till exempel i situationer av samverkan och informationsutbyte mellan exempelvis kommuner och myndigheter.

Jag ser positivt på ambitionen om en mer enhetlig reglering för hela den offentliga förvaltningen vad gäller informationssäkerhetsarbetet. Men ökade krav och ett ökat ansvar för kommunerna måste komma med ökade resurser. Jag delar därför stadsledningskontorets bild av de finansiella konsekvenserna av utredningens förslag inte är tillräckligt analyserade och behöver utredas vidare.

I övrigt hänvisar jag till stadsledningskontorets och Stockholm Stadshus AB:s tjänsteutlåtanden.

Stockholm den 17 april 2024

Karin Wanngård

## Bilaga

Remiss – Delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18), dnr KS 2024/326-1.1

**Borgarrådsberedningen** tillstyrker föredragande borgarrådets förslag.

## Ärendet

I remissen, benämnd som *Delbetänkande - nya regler om cybersäkerhet,* lämnas förslag på hur NIS2-direktivet ska införlivas i nationell lagstiftning. Den 14 december 2022 antog Europaparlamentet och rådet två nya EU-direktiv, NIS2-direktivet samt CER-direktivet. NIS2-direktivet ersätter det tidigare NIS-direktivet från 2016, och ställer krav på säkerhet i nätverks- och informationssystem.

Delbetänkandet föreslår att NIS2-direktivet i huvudsak ska införlivas genom en ny lag, cybersäkerhetslagen. Genom direktivet skärps kraven för verksamhetsutövare och direktivet innefattar bestämmelser rörande mer omfattande samverkan inom unionen, detta i syfte att uppnå högre cybersäkerhet. Cybersäkerhetslagen föreslås omfatta fler aktörer än den nuvarande lagstiftningen (antalet sektorer ökar från 7 till 18). De sektorer som kommer att omfattas är:

• Energi

• Transporter

• Bankverksamhet

• Finansmarknadsinfrastruktur

• Hälso- och sjukvårdssektorn

• Dricksvatten

• Avloppsvatten

• Digital infrastruktur

• Förvaltning av IKT-tjänster (mellan företag)

• Offentlig förvaltning

• Rymden

• Post- och budtjänster

• Avfallshantering

• Tillverkning, produktion och distribution av kemikalier

• Produktion, bearbetning och distribution av livsmedel

• Tillverkning

• Digitala leverantörer

• Forskning

Lärosäten med examenstillstånd, samtliga kommuner och regioner omfattas av lagens krav, med undantag för region- och kommunfullmäktige. Kraven kommer att omfatta hela verksamheten och inte enbart samhällsviktiga och digitala tjänster. Det föreslås

vidare att cybersäkerhetslagen även ska gälla för majoriteten av Sveriges myndigheter.

Den nya regleringen ställer krav på verksamhetsutövarna att lämna information till sin tillsynsmyndighet. Dessutom ska verksamhetsutövare vidta riskhanteringsåtgärder, i syfte att skydda nätverks- och informationssystem samt systemens fysiska miljö mot incidenter. Det ställs krav på att verksamhetsutövaren ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete. Utöver detta, finns det en skyldighet för verksamhetsutövare att rapportera betydande incidenter till Myndigheten för samhällsskydd och beredskap (MSB), vilket ska ske inom bestämda tidsgränser.

## Remissammanställningen

Ärendet har remitterats till stadsledningskontoret och Stockholms Stadshus AB. Stockholms Stadshus AB har underremitterat remissen vidare till AB Stokab och Stockholm Vatten och Avfall AB.

### Stadsledningskontoret

**Stadsledningskontorets** tjänsteutlåtande daterat den 25 mars 2024 har i huvudsak följande lydelse.

Stadsledningskontoret står bakom alla väsentliga delar i det som föreslås i delbetänkandet. Förslagen innebär att samhällsviktiga verksamheter föreslås träffas i större omfattning än tidigare, detta genom att avsevärt fler sektorer än tidigare omfattas. Detta bedöms vara i linje med de intentioner som framkommer av både direktivet och delbetänkandet för att uppnå ett mer robust och motståndskraftigt samhälle, både nationellt och inom unionen.

Inom den offentliga förvaltningen finns det idag olika regleringar på cybersäkerhetsområdet. Som utredningen konstaterar skapar detta en ojämn och fragmenterad implementering av cybersäkerhetsskyddet inom den offentliga förvaltningen. Det i sin tur skapar ojämlika förhållanden mellan verksamheter inom den offentliga förvaltningen, till exempel i situationer av samverkan och informationsutbyte mellan exempelvis kommuner och myndigheter. Som framgår av direktivet ska tolkningen av cybersäkerhetslagen ha sin grund i direktivets syfte. Effekten av det tidigare NIS-direktivet var inte tillräcklig och cybersäkerhetskraven varierade vilket ledde till en fragmentering av den inre marknaden. Stadsledningskontoret välkomnar en mer enhetlig reglering för hela den offentliga förvaltningen vad gäller de mest grundläggande hygienfaktorerna inom informationssäkerhetsarbetet.

Rätten att forma föreskrifter och genomföra tillsyn är fortsatt tilldelad olika myndigheter för de olika sektorerna som omfattas av NIS2. Stadsledningskontoret anser att lagförslaget inte tillräcklig tar hänsyn till att kommuner, som genom sin

unika uppsättning av olikartade verksamhetsområden inom en och samma organisation, spänner över flera av sektorerna samtidigt.

Stockholms stad träffas av nuvarande NIS-reglering inom tre sektorer. Enligt förslagen i utredningen bedöms Stockholms stad istället träffas inom fem sektorer. Inom var och en av de fem sektorerna kommer specifika föreskrifter kunna utformas, precis som idag. Det föreslås att fem olika tillsynsmyndigheter ska få tillsynsansvaret, enligt samma princip som idag. I grunden är det bra att olika myndigheter med sina särskilda uppdrag och kompetenser, genom specifika föreskrifter, får säkerställa att de unika riskerna inom respektive sektor fångas på det sätt som lagstiftningen avser. En erfarenhet från nuvarande föreskrifter är däremot att dessa endast till mycket liten del ställer sektorsunika krav. Däremot förekommer vagt olika nyanser i ordval, vilket bedöms vara naturligt, då det är tre olika författande myndigheter som gett ut föreskrifterna (skillnaderna har ingen påverkan på sakinnehållet). Detta innebär att för en kommun som Stockholms stad, att tre föreskrifter från tre olika myndigheter inom tre olika sektorer idag ställer samma krav på grundläggande processer för ett systematiskt cybersäkerhetsarbete. Konsekvenserna av detta blir merarbete, ineffektivt resursnyttjande och risk för en fragmenterad intern hantering för en kommun som har att förhålla sig till detta.

Stadsledningskontoret kan konstatera att de tre tillsynsmyndigheterna idag ställer samma frågor, om stadens grundläggande verksamhetsprocesser för informationssäkerhet, vid sina respektive tillsynsbesök som genomförs vid tre olika tillfällen. Stadsledningskontoret bedömer att de flesta kraven i det nya förslaget utgör grundläggande processer för ett systematiskt cybersäkerhetsarbete enligt vad som anses vara bästa praxis. Det innebär en risk att kommuner även framöver får ta emot samma föreskriftskrav och tillsynsbesök, fast från fem olika håll istället för tre. Risken är att det leder till en ännu mer suboptimering, både för kommunen och för berörda myndigheter. Stadsledningskontoret efterlyser därför en mer samordnad hantering av föreskrifter och tillsyn som träffar just kommuner, i de delar som gäller grundläggande processer i lagkraven.

Som utredningen framhåller ska förslagen utformas så att regelbördan och administrationen minimeras för berörda verksamhetsutövare. Ur det kommunala perspektivet vore det att föredra ett en samordnande myndighet får föreskriva om de grundläggande och gemensamma cybersäkerhetsprocesser som gäller lika för alla. Det bör stärka intentionen att undanröja en ojämn och fragmenterad implementering av cybersäkerhet nationellt och bespara ett flertal föreskrivande myndigheter och tillsynsmyndigheter resurser att inte behöva uttrycka samma krav i sina respektive föreskrifter. Stadsledningskontoret anser därför att föreskriftsrätten hos de olika sektorsmyndigheterna bör fokuseras på att uttrycka just de unika särdragen som finns inom varje sektor i kompletterande föreskrifter.

Myndigheten för samhällsskydd (MSB) har särskilt framfört risken för att kraven kommer att tillämpas olika om olika myndigheter får meddela föreskrifter. Myndigheten för samhällsskydd (MSB), Säkerhetspolisen, Transportstyrelsen och

Integritetsskyddsmyndigheten (IMY) har föreslagit att det borde ankomma på MSB att meddela föreskrifter med grundläggande krav på säkerhet och att de olika tillsynsmyndigheterna, vid behov, kompletterar dessa föreskrifter genom att meddela föreskrifter med särskilda krav på utökad säkerhet för sin sektor. Utredningen har bedömt att en sådan lösning inte är en framkomlig väg. Stadsledningskontoret delar inte den bedömningen. Delbetänkandet adresserar inte de konsekvenser som uppstår för kommuner som verkar inom flera sektorer samtidigt och således efterfrågas en fortsatt utredning av dessa konsekvenser.

MSB ska enligt delbetänkandet även fortsättningsvis leda ett samarbetsforum där tillsynsmyndigheterna ingår. Syftet med forumet ska vara att underlätta samordning och åstadkomma en effektiv och likvärdig tillsyn. Stadsledningskontoret önskar särskilt understryka vikten av denna samordning när det kommer till föreskrivande och tillsyn av just kommunernas uppdrag, för att undvika resursineffektivitet och suboptimering för både myndigheterna och verksamhetsutövarna.

För de offentliga verksamhetsutövarna föreslår utredningen att kostnaderna ska finansieras inom befintlig ram. Utredningen anser att det är rimligt att offentliga verksamhetsutövare vidtar grundläggande säkerhetsåtgärder. Det konstateras vidare att förslagen innebär en stor förändring jämfört med de nuvarande kraven, eftersom offentliga verksamhetsutövare bara i enstaka fall omfattas av gällande NIS-lag. Utredningen bedömer att kraven inte kan beskrivas som omfattande, men samtidigt är de tillräckligt ingripande för att verksamhetsutövaren ska behöva avsätta resurser.

Utredningen menar att verksamhetsutövarna också kommer erhålla ett stöd till den egna verksamheten genom de förslag som läggs fram. Innebörden av det är att de högre kraven för exempelvis incidenthantering kommer att leda till att incidenter i större utsträckning förebyggs, vilket i förlängningen kommer medföra besparingar. Åtgärderna för att förebygga incidenter antas leda till att incidenter förhindras eller begränsas. Det finns förvisso en logik i det resonemanget som stadsledningskontoret håller med om, det vill säga att syftet med incidenthantering är att identifiera brister som sedan kan åtgärdas och förebyggas. Stadsledningskontoret instämmer i att det leder till en ökad motståndskraft och robusthet för de samhällsviktiga tjänsterna. Det är däremot inte likställt med att besparingar kommer att erhållas. Tvärt om förväntas de högre kraven innebära att fler incidenter identifieras och behöver hanteras samt att fler organisatoriska och tekniska åtgärder kommer krävas. För att skapa förutsättningar för hanteringen behöver verksamheten också säkerställa en ändamålsenligt, effektiv och verksamhetsövergripande incidenthanteringsprocess och många verksamheter behöver även investera i systemstöd. Det innebär således att de ökade kraven leder till både mer arbete, behov av ökade personella resurser och fler investeringar, särskilt för de offentliga verksamhetsutövare som idag bara i enstaka fall omfattas av gällande NIS-lag. Därtill kommer även behov av ökade resurser vid upphandlingar av nätverks- och informationssystem för att säkerställa korrekt kravställning i enlighet med den föreslagna cybersäkerhetslagen.

Stadsledningskontoret bedömer att det finns en inneboende konflikt i resonemanget om finansiella konsekvenser som inte är tillräckligt analyserad och efterlyser därför mer utredning i frågan. Ur det kommunala perspektivet bedöms omställningen till de nya mer omfattande kraven innebära en ökad robusthet i de samhällsviktiga tjänsterna men också en ökad kostnad. Sammantaget gör stadsledningskontoret bedömningen att NIS2-kraven innebär en omställning som kommer att medföra behov av ökade resurser.

En betydande del av Stockholms stads kommunala uppdrag bedrivs i form av kommunala bolag. Stadsledningskontoret bedömer att det är viktigt att klargöra om kommunala bolag omfattas av sektorn offentlig förvaltning eller inte. Det behövs inte minst eftersom kommuner kategoriseras som väsentliga verksamhetsutövare och därmed träffas av högre krav. I delbetänkandets förslag framgår det att kommuner omfattas i sin helhet. Det förtydligas även att det inte enbart är den sektorsspecifika tjänsten som omfattas, utan hela den verksamhet där tjänsten ingår. Innebörden är att den som bedriver verksamhet inom någon av sektorerna, som utgångspunkt omfattas av kraven i cybersäkerhetsregleringen. Det bedöms vara i linje med direktivets och lagens intentioner om att uppnå en högre gemensam cybersäkerhet för samhällsviktig verksamhet inom hela unionen. Utredningen konstaterar dock att i de fall verksamheten bedrivs genom kommunala bolag är det inte kommunen som är verksamhetsutövare. Det innebär att de kommunala bolagen inte ingår i det som avses med ”hela kommunen” eller i den nya sektorn ”offentlig förvaltning”. Stadsledningskontoret instämmer i detta. De kommunala bolagen omfattas bara av kraven om de träffas av någon av de specifikt utpekade sektorerna exempelvis hälso- och sjukvård, transport eller dricksvatten.

Som framgår av delbetänkandet behöver det i lagförslagets tillämpning tas hänsyn till att nätverks- och informationssystem många gånger är sammankopplade inom hela verksamheten samt att incidenter inom en del av verksamheten kan påverka en annan del. Det skulle enligt utredningen leda till gränsdragningsproblem att försöka dela upp verksamheten. Detta talar emot en uppdelning och avgränsning från att även kommunala bolag omfattas när dessa delar infrastruktur med resten av kommunen. Stadsledningskontoret bedömer dock att det är en praktisk fråga som får hanteras av verksamhetsutövaren.

Vid genomgången av delbetänkandet noteras att de riskhanteringsåtgärder som verksamhetsutövare är skyldiga att vidta anges i direktivets artikel 21. I den föreslagna cybersäkerhetslagen, 3 kap. 1 §, är dock inte alla dessa åtgärder medtagna vilket är otydligt och inte tillfredsställande med hänsyn till ledningsansvaret som finns och sanktionerna verksamhetsutövare kan påföras. Ytterst är det en fråga om rättssäkerhet vid lagens tillämpning. Stadsledningskontoret anser att denna otydlighet bör hanteras i det fortsatta arbetet med cybersäkerhetslagen.

### AB Stokab

**AB Stokabs** uttrande daterat den 3 april 2024 har i huvudsak följande lydelse.

Utredningen omfattar ett komplext regelområde. En särskild komplexitet gäller bedömningen av konsekvenserna av att upphäva vissa sektorsspecifika bestämmelser i LEK för att istället låta de sektorsövergripande reglerna i förslaget till cybersäkerhetslag gälla, se närmare nedan under avsnitt NIS2-direktivet och LEK.

Det kan vidare konstateras att Utredningen föreslår en cybersäkerhetslag med övergripande regleringar, men att lagen lär behöva kompletteras med föreskrifter som meddelas av utpekad tillsynsmyndighet. Föreskrifterna från tillsynsmyndigheterna kommer således att utgöra ett mycket viktigt komplement till de skyldigheter som föreslås i den nya cybersäkerhetslagen och Stokab anser därför att det är angeläget att dessa utfärdas skyndsamt.

#### Cybersäkerhetslagens tillämpningsområde (avsnitt 5)

##### *Verksamhetsutövare (avsnitt 5.2.2)*

Utredningen har tagit ställning till frågan om verksamhetsutövarens verksamhet i dess helhet, eller om bara delar av verksamheten, behöver uppfylla NIS2-direktivets krav. Utredningen har funnit att det i direktivet saknas en uttrycklig begränsning om att endast delar av den fysiska eller juridiska personens verksamhet skulle omfattas av direktivet. Utredningens slutsats är med hänsyn därtill att hela verksamheten omfattas. Stokab har inget att invända mot detta förslag och förstår de gränsdragningsproblem som en uppdelning av verksamheten skulle kunna leda till. Stokab anser dock att det är viktigt att det tydligt framgår att de riskhanteringsåtgärder som ska vidtas enligt cybersäkerhetslagen ska vara proportionerliga i förhållande till risken, se vidare nedan under avsnitt Riskhanteringsåtgärder.

##### *Undantag för säkerhetsskyddsklassificerade uppgifter och för enskilda verksamhetsutövare (avsnitt 5.5.3 och 5.5.5)*

Stokab instämmer med och välkomnar Utredningens förslag avseende undantag för enskilda verksamhetsutövare i den del som de bedriver egen säkerhetskänslig verksamhet, oberoende av om verksamhetsutövaren även bedriver annan icke säkerhetskänslig verksamhet.

När det gäller enskilda verksamhetsutövares tillhandahållande av tjänster till aktörer som bedriver säkerhetskänslig verksamhet föreslår Utredningen dock att endast de tjänster som erbjuds till myndigheter som är helt undantagna från cybersäkerhetslagen också undantas från krav om riskhanteringsåtgärder, incidentrapportering samt tillsyn- och sanktionsbestämmelser som hänför sig till dessa krav.

Innebörden för enskilda verksamhetsutövare blir således att de undantas från cybersäkerhetslagens krav i den delen som de själva bedriver säkerhetskänslig verksamhet samt i den delen som de erbjuder tjänster till myndigheter som är

undantagna från cybersäkerhetslagen, exempelvis till Försvarsmakten eller Polismyndigheten. De undantas dock inte i den del de erbjuder tjänster till en myndighet, region eller kommun som bedriver säkerhetskänslig verksamhet i mindre utsträckning.

Stokab anser att utgångspunkten bör vara att säkerhetskänslig verksamhet ska undantas från cybersäkerhetslagen. Detta bör gälla såväl när det rör sig om egen säkerhetskänslig verksamhet som när den enskilde verksamhetsutövaren utför tjänster inom ramen för en kunds säkerhetskänsliga verksamhet. Stokab anser att den senare situationen bör vara oberoende av om kunden bedriver säkerhetskänslig verksamhet i större eller mindre utsträckning. Det är viktigt att säkerhetskänslig verksamhet inte belastas av krav i olika regelverk och att Utredningens förslag att skyldighet att lämna uppgifter enligt cybersäkerhetslagen inte ska gälla för säkerhetsskyddsklassificerade uppgifter får fullt genomslag i tillämpningen av lagen.

## Riskhantering och incidentrapportering (avsnitt 7)

### *Övergripande lagreglering om riskhanteringsåtgärder (avsnitt 7.1)*

Stokab delar Utredningens bedömning att kraven om riskhanteringsåtgärder ska regleras övergripande i cybersäkerhetslagen och att lagen bör kompletteras med föreskrifter som meddelas av tillsynsmyndigheten. Den förslagna avvägningen mellan vad som föreslås regleras direkt i cybersäkerhetslagen (grundläggande men inte alltför detaljerade krav) och vad som bör meddelas i föreskrifter (mer detaljerade och sektorsanpassade krav) är väl genomförd.

Det kan redan i detta sammanhang påpekas att Stokab instämmer med Utredningens förslag om delat tillsynsansvar mellan Myndigheten för samhällsskydd och beredskap (”**MSB**”) och olika tillsynsmyndigheter för de olika sektorerna, se vidare under avsnittet nedan angående Tillsyn. Liksom Utredningen anser Stokab att det är angeläget att föreskrifterna kan sektorsanpassas och att den myndighet som har tillsyn också har föreskriftsrätten.

### *Riskhanteringsåtgärder (avsnitt 7.1.2)*

När det gäller Utredningens förslag avseende vilken typ av riskhanteringsåtgärder som ska vidtas, anser Stokab att det är viktigt att det på så sätt som föreslås är tydligt att riskhanteringsåtgärderna ska utgå från ett allriskperspektiv och en riskanalys och vara proportionerliga i förhållande till risken. Som påpekats ovan blir denna proportionalitetsbedömning särskilt viktig när verksamhetsutövarens hela verksamhet omfattas.

Utredningen anger vidare att åtgärderna ska ske hos verksamhetsutövaren och syftet är att förhindra eller minimera incidenters påverkan på mottagaren av tjänsterna eller andra tjänster. Detta tydliggör enligt Stokabs uppfattning vikten av att utgå från verksamhetsutövarens olika nätverks- och informationssystems påverkan på den tillhandahållna tjänsten vid proportionalitetsbedömning avseende riskhanteringsåtgärderna.

Enligt förslaget till lagtext ska riskhanteringsåtgärderna vidtas för att skydda nätverks- och informationssystem och systemens fysiska miljö mot incidenter. I detta avseende hänvisas till avsnittet nedan angående NIS2-direktivet och LEK.

Stokab välkomnar Utredningens klargörande avseende att säkerhet i leveranskedjan innebär att varje verksamhetsutövare endast behöver vidta riskhanteringsåtgärder i förhållande till sin direkta leverantör och alltså ansvarar för ett led i kedjan. Vidare anges i Utredningen att de närmare bestämmelserna för detta bör följas av föreskrifter. Stokab anser att ytterligare vägledning kring hur sådan säkerhet i leveranskedjan uppnås kommer att vara viktig. Detta gäller särskilt avseende sådana leverantörer som inte själva omfattas av cybersäkerhetslagen.

## Tillsyn (avsnitt 8)

### *Tillsynsmyndigheter i Sverige (avsnitt 8.4.2)*

Som angivits ovan instämmer Stokab med Utredningens förslag om delat tillsynsansvar mellan MSB och olika tillsynsmyndigheter för de olika sektorerna. När det gäller sektorn digital infrastruktur, omfattande bland annat tillhandahållande av allmänna elektroniska kommunikationsnät, önskar Stokab framföra följande. Post- och telestyrelsen (”**PTS**”) är den myndighet som bevakar området elektronisk kommunikation i Sverige och har således god kännedom om sektorn. Stokab välkomnar därför Utredningens förslag att PTS även fortsatt ska vara tillsynsmyndighet för sektorn inklusive de nya verksamhetsutövare som kommer att omfattas.

### *Föreskrifter (avsnitt 8.4.5)*

När det gäller föreskriftsrätten föreslår Utredningen att tillsynsmyndigheten inom sitt tillsynsområde får meddela föreskrifter om riskhanteringsåtgärder, systematiskt och riskbaserat informationssäkerhetsarbete samt utbildning. Dock föreslås att MSB får meddela föreskrifter om vad som utgör en betydande incident och om incidentrapportering. Som angivits ovan anser Stokab att det är viktigt att föreskrifterna kan sektorsanpassas och att den myndighet som har tillsyn också har föreskriftsrätten. Detta gäller även incidentrapporteringen, se vidare nedan under avsnitt NIS2-direktivet och LEK. Föreskrifterna från tillsynsmyndigheterna kommer att utgöra ett mycket viktigt komplement till de skyldigheter som föreslås i den nya cybersäkerhetslagen och de bör därför utfärdas skyndsamt. I detta avseende bör det framhållas att det hos PTS finns en inarbetad praxis med föreskrifter för tillhandahållare av allmänna elektroniska kommunikationsnät innehållande incidentrapportering.

### *Tillsynsmyndighetens undersökningsbefogenheter (avsnitt 8.4.6)*

När det gäller riktade säkerhetsrevisioner välkomnar Stokab Utredningens förslag, samt därtill underliggande motivering, att tillsynsmyndigheten endast får besluta om en riktad säkerhetsrevision utförd av ett oberoende organ, och som bekostas av verksamhetsutövaren, om det finns särskilda skäl.

## NIS2-direktivet och LEK (avsnitt 11)

### *Inledning*

Genom NIS2-direktivet upphävs de sektorsspecifika artiklarna 40 och 41 i den europeiska kodexen för elektronisk kommunikation (”**Kodexen**”), implementerad i svensk rätt genom LEK, och ersätts med bestämmelserna som följer av NIS2-direktivet. Utredningen har därför utrett om de motsvarande individuella bestämmelserna om säkerhet i nät och tjänster i LEK (8 kap. 1–4§§) även innehåller andra bestämmelser än de som är avsedda att genomföra artiklarna 40 och 41 i Kodexen.

### *Riskhanteringsåtgärder och ramen för vad riskhanteringsåtgärder kan avse (avsnitt 11.2.3 och 11.2.4)*

Utredningen gör en jämförelse mellan tillhandahållares skyldighet att vidta risk-hanteringsåtgärder i NIS2-direktivet med relevanta bestämmelser i Kodexen och finner att säkerhetsbegreppet i de två direktiven är att betrakta som likvärdiga. Utredningen finner även att bestämmelsen i LEK korresponderar med det materiella innehåll som följer av motsvarande bestämmelse i Kodexen, och att NIS2-direktivets bestämmelser inte är begränsande i förhållande till Kodexen i denna del.

Stokab anser dock att den genomförda analysen inte är tillräcklig och alltför översiktlig. Som Utredningen också konstaterar så anger Kodexen och LEK att det som ska skyddas genom riskhanteringsåtgärderna är ”näts och tjänsters säkerhet”, medan NIS2-direktivet och förslaget till cybersäkerhetslag talar om ”säkerheten i nätverks- och informationssystem”. En fundamental skillnad mellan de olika lagstiftningarna är att NIS2-direktivet ställer krav på säkerhet i nätverks- och informationssystem, medan den sektorsspecifika lagstiftningen i Kodexen och LEK inte har nätverks- och informationssystem som utgångspunkt utan tillhandahållandet av det allmänna elektroniska kommunikationsnätet (och kommunikationstjänsterna) som helhet.

När det gäller allmänna elektroniska kommunikationsnät är exempelvis den fysiska säkerheten i nätet avgörande för att skydda mot incidenter. En kabelskada kan få mycket stora konsekvenser på tillhandahållandet av tjänsten, men kan inte undvikas genom att vidta åtgärder för att skydda nätverks- och informationssystem. Detta omfattas idag av den sektorsspecifika lagstiftningen, men det är enligt Stokabs uppfattning inte självklart att dessa delar avseende säkerhet i nättjänster kommer att omfattas av cybersäkerhetslagen. Stokab anser i detta avseende att det är oklart vad som avses med ”systemens fysiska miljö”. Enligt Stokabs uppfattning utgör inte det allmänna elektroniska kommunikationsnätet bestående av, i Stokabs fall, fiberkablar och kanalisation en fysisk miljö för nätverks- och informationssystem. Sammanfattningsvis anser Stokab att gränsdragningen mellan den föreslagna cybersäkerhetslagen och LEK måste analyseras och utredas ytterligare i detta avseende. Det är avgörande att en sådan gränsdragning är både tydlig och ändamålsenlig.

### *Incidentbegreppet, kravet på incidentrapportering och föreskriftsrätt (avsnitt 11.2.6, 11.2.7 och 11.2.11)*

Vad som har angivits ovan avseende skillnaden mellan skyddsföremålet enligt Kodexen (”säkerhet för nät och tjänster”) respektive NIS2-direktivet (”säkerhet i nätverks- och informationssystem”) gör sig gällande även när det gäller hantering av incidenter. I Utredningen anges att NIS2-direktivet förvisso omfattar incidentbegreppet fysisk infrastruktur och fysisk påverkan, men kräver att den aktuella händelsen ska ha någon form av påverkan på uppgifter eller tjänster. Av samma skäl som har angivits i ovanstående stycke anser Stokab att det är oklart huruvida en kabelskada ska anses utgöra en incident i cybersäkerhetslagens bemärkelse. Stokab instämmer därför med vad som anges i Utredningen att det i det fortsatta lagstiftningsarbetet bör övervägas om skillnaden i omfattning mellan lagstiftningarna medför ett behov av vidare åtgärder.

När det gäller kravet på incidentrapportering konstaterar Utredningen att Kodexen innehåller mer detaljerade bestämmelser än NIS2-direktivet om vad som ska beaktas vid bedömningen av om en incident har haft betydande påverkan och därmed är rapporteringspliktig. Som angivits ovan är dessa sektorsspecifika bestämmelser utformade utifrån tillhandahållandet av det allmänna elektroniska kommunikationsnätet (och kommunikationstjänsterna) som helhet och är därför enligt Stokabs uppfattning mer ändamålsenliga och tydliga för tillhandahållare av allmänna elektroniska kommunikationsnät. Utredningen analyserar dock inte detta närmare utan konstaterar att denna diskrepans mellan direktiven sannolikt kommer att sakna betydelse i den svenska tillämpningen eftersom Utredningen föreslår att närmare föreskrifter om vad som utgör en betydande incident ska få meddelas av utpekad myndighet. På så sätt undviker Utredningen att närmare analysera frågan och konsekvenserna av den konstaterade diskrepansen för att istället överlämna ett klargörande till kommande föreskrifter.

Föreskriftsrätten avseende vad som utgör en betydande incident och om incidentrapportering föreslås dock ges till MSB och inte till PTS. Det skulle alltså vara MSB som genom föreskrifter skulle behöva klargöra de konstaterade diskrepanserna som till stor del beror på den sektorsspecifika regleringen. Stokab anser att det är av stor vikt att föreskrifterna för tillhandahållare av allmänna elektroniska kommunikationsnät är sektorsanpassade, eller åtminstone att de särskilda förutsättningar som gäller inom denna sektor beaktas vid utformandet av föreskrifterna om vad som utgör en betydande incident och om incidentrapportering.

## Stockholm Vatten och Avfall AB

**Stockholm Vatten och Avfall AB:s** yttrande daterat den 3 april 2024 har i huvudsak följande lydelse.

Delar av Stockholm Vatten och Avfalls verksamhet träffades av NIS redan 2020 i och med att vattenproduktion och vattendistribution räknas som samhällsviktig verksamhet.

Stockholm Vatten och Avfalls kontrollinstans, Livsmedelsverket, skrev ett förslag till föreskrifter som bolaget besvarade. Kritiken handlade om att förslaget i stort sätt enbart baserades på att identifiera säkerhetsbrister med hjälp av risk- och sårbarhetsanalyser. Metoden är både resurs- och tidskrävande och långt från optimal om det övergripande målet är att snabbt få verksamheten robust och resilient. Remissvaret innehöll en checklista med standardåtgärder som alltid behöver utföras för att skydda en kritisk IT-miljö mot olika typer av angrepp. De färdiga föreskrifterna hade till vissa delar tagit hänsyn till Stockholm Vatten och Avfalls remissförslag.

#### Remissvar på NIS2

NIS2 har tagit ytterligare ett steg ifrån att prioritera skyddet av den del av verksamheten som levererar den samhällsviktiga tjänsten. Kraven i förslaget liknar till stor del kraven i ISO/IEC 27001/27002. Dessa är bra om målet är att förbättra det generella informationssäkerhetsarbetet. Om målet är att snabbt och effektivt säkra leveransen av den samhällsviktiga tjänsten så har man inte lyckats. Bolaget bedömer att en implementering av NIS2 kommer få följande konsekvenser:

• Införandet kommer leda till stora kostnader och små och långsamma förbättringar.

• I och med att konkreta krav saknas blir det mycket svårt att granska efterlevnaden på ett rättvist sätt.

• Små organisationer kommer att ha oerhört svårt att uppfylla kraven.

Syftet borde vara att kunna upprätthålla den samhällsviktiga leveransen även under kriser/allvarliga störningar. Det finns redan standarder som leder till en generell förbättring av informationssäkerhetsarbetet. ISO/IEC 27001/27002 gör det möjligt för organisationen att till viss del välja vilka krav som är tillämpliga för den egna verksamheten. NIS2 riskerar att tvinga de som träffas av lagstiftningen att införa krav som enbart genererar kostnader.