STOKAB

Remissvar

Datum	2024-04-02
Diarienummer	STOK 2024/100
Sida	1(7)
Handläggare	Patricia Helanow

Stockholms Stadshus AB
remiss@stadshusab.se

Yttrande över delbetänkandet – Nya regler om cybersäkerhet (SOU 2024:18), SSAB:s dnr. 2024/62

Remissen

AB Stokab ("**Stokab**") har erhållit delbetänkandet *Nya regler om cybersäkerhet (SOU 2024:18)* ("**Utredningen**") på remiss från kommunstyrelsen genom underremiss från Stockholms Stadshus AB, för yttrande senast den 2 april efter anstånd.

I Utredningen föreslås de anpassningar av svensk rätt som är nödvändiga för att EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen ("**NIS2-direktivet**") ska kunna genomföras. NIS2-direktivet ställer krav på säkerhet i nätverks- och informationssystem med syftet är att uppnå en högre cybersäkerhet. Det ersätter det tidigare NIS-direktivet från 2016, som genomfördes i svensk rätt genom lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster ("**NIS-lagen**"). Utredningen föreslår att NIS2-direktivet i huvudsak införlivas genom en ny lag, cybersäkerhetslagen, och att den tidigare NIS-lagen upphävs. Utredningen föreslår att den nya lagen ska träda i kraft den 1 januari 2025.

Sammanfattning

Utredningen omfattar ett komplext regelområde. En särskild komplexitet gäller bedömningen av konsekvenserna av att upphäva vissa sektorsspecifika bestämmelser i lagen (2022:482) om elektronisk kommunikation ("**LEK**") för att i stället låta de sektorsövergripande reglerna i förslaget till cybersäkerhetslag gälla. I detta avseende anser Stokab att en mer noggrann analys än vad som har genomförts av Utredningen behövs.

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 viktigt komplement till de skyldigheter som föreslås i den nya cybersäkerhetslagen och Stokab anser att det därför är angeläget att dessa utfärdas skyndsamt.

Inledning

Stockholms stad har, genom Stokab, byggt ett operatörsneutralt fibernät som når drygt 90 procent av hushållen, det vill säga i stort sett samtliga flerfamiljshus, och i princip 100 procent av företagen i Stockholm. Stokab tillhandahåller endast svartfiber med tillhörande passiva installationer som upplåts på likvärdiga villkor till marknadens aktörer (enbart B2B). Stokab är således ett renodlat grossistföretag. Stokab har för närvarande cirka 900 kunder (företag och organisationer), varav över 100 operatörer och tjänsteleverantörer, i sitt nät.

Stokabs dotterbolag, S:t Erik Kommunikation AB ("**STEK**"), driver och administrerar Stockholms stads interna kommunikationsnät enligt uppdrag från Stockholms kommunfullmäktige. Detta nät omfattar alla Stockholms stads verksamheter och bolag, såväl administrativa som tekniska system.

Genom sin verksamhet tillhandahåller Stokab ett allmänt elektroniskt kommunikationsnät i den mening som avses i LEK. Elektroniska kommunikationsnät och -tjänster utgör en grundläggande funktion för att dagens samhälle ska fungera. I princip samtliga sektorer i samhället är beroende av säker och pålitlig elektronisk kommunikation, då allt fler tjänster och samhällsfunktioner förlitar sig på datatrafik via fungerande nät och tjänster för allt från sjukvård till försörjning av livsmedel och dricksvatten.

Elektronisk kommunikation regleras i LEK, vilken även innehåller bestämmelser om säkerhet i nät och tjänster. Med hänsyn till denna reglering är tillhandahållare av allmänna elektroniska kommunikationsnät undantagna den nu gällande NIS-lagen (detta följer även av det underliggande NIS-direktivet). I NIS2-direktivet finns dock inget motsvarande undantag för allmänna elektroniska kommunikationsnät, utan tillhandahållare av dessa omfattas uttryckligen av NIS2-direktivet. Utredningen föreslår därför att tillhandahållare av allmänna elektroniska kommunikationsnät ska omfattas av den nya cybersäkerhetslagen och att motsvarande bestämmelser i LEK ska upphävas. För tillhandahållare av allmänna elektroniska kommunikationsnät, såsom Stokab, innebär detta således att istället för att omfattas av de sektorsspecifika regleringarna i 8 kap. 1–4§§ LEK avseende säkerhet i nät och tjänster, så kommer verksamheten att omfattas av den sektorsövergripande cybersäkerhetslagen.

STEK tillhandahåller DNS-tjänster till verksamheter inom Stockholms stad. Utredningen föreslår att leverantörer av sådana tjänster ska omfattas av cybersäkerhetslagen. Redan av den anledningen omfattas STEK av Utredningens förslag till cybersäkerhetslag.

Nedan följer Stokabs övergripande synpunkter på förslagen i Utredningen och på utvalda avsnitt.

Stokabs synpunkter

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.

Med vänlig hälsning

Joakim Larsson
Verkställande direktör
AB Stokab