



Stockholm 2024-05-28

Remissvar

169. Svenska Stadsnätetsföreningen

Handläggare Camilla Jönsson

Tel 08-21 49 31

Camilla.jonsson@stadsnatsforeningen.se

departementet

DNR: Fö2024/00496

fo.remissvar@regeringskansliet.se

visnja.raguz@regeringskansliet.se

Remissvar gällande

Delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18)

Svenska Stadsnätetsföreningen är en bransch- och intresseorganisation som representerar stadsnät i närmare 200 kommuner och 125 leverantörer av tjänster och utrustning inom bredbandsområdet. Föreningen företräder därmed en absolut majoritet av de aktörer som aktivt investerar i ny modern infrastruktur för bredband i Sverige.

Stadsnätetsföreningens medlemmar äger fibernät, som är en grundläggande samhällsviktig infrastruktur och som är fundamental för att dagens samhälle ska fungera. I princip alla branscher och sektorer i samhället är beroende av att robusta och säkra elektroniska kommunikationstjänster fungerar även om samhället drabbas av stora påfrestningar, som en pandemi eller en naturkatastrof. Elektroniska kommunikationer är av stor vikt för Sveriges totalförsvarsförmåga.

Stadsnätetsföreningen tackar för möjligheten att svara på remissen.

Sammanfattning

Stadsnätetsföreningen tillstyrker utredningens förslag om hur Europaparlamentets och rådets direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS2-direktivet) ska implementeras i Sverige.

Stadsnätetsföreningen ser vissa risker med den nya lagen, då det kan komma att finnas en gränsdragningsproblematik när det gäller föreskrifter, efterlevnad och tillsyn, som riskerar att ta omfattande resurser i anspråk. Föreskriftskrav från flera olika myndigheter, som därtill ska göra tillsynsbesök utifrån sina perspektiv, kan komma att öka bördan för både kommuner och företag. Det bör finnas en samordnad hantering för de grundläggande lagkraven.

Stadsnätetsföreningen anser att föreskrifträtten hos de olika sektorsmyndigheterna bör fokuseras på att uttrycka just de unika särdragen som finns inom varje sektor i kompletterande föreskrifter. Det innebär också att föreskrifterna från tillsynsmyndigheterna kommer att utgöra ett viktigt komplement till de skyldigheter som föreslås i den nya cybersäkerhetslagen och därför anser Stadsnätetsföreningen att dessa behöver utfärdas skyndsamt.

När det gäller kravet på incidentrapportering, som enligt den europeiska kodexen för elektronisk kommunikation innehåller mer detaljerade bestämmelser än NIS2-direktivet, föreslår utredningen att utpekad myndighet ska meddela föreskrifter om vad som utgör en betydande incident. Föreskrifträtten avseende vad som utgör en betydande incident och om incidentrapportering föreslås dock ges till MSB och inte till Post, och telestyrelsen, PTS.

Stadsnätsföreningen anser att det bör vara PTS som är mottagare av rapporten för sektorn elektronisk kommunikation. PTS är den myndighet som har kunskap om den sektorsspecifika reglering som omgärdar sektorn för elektronisk kommunikation och som har föreskriftsrätten när det gäller incidentrapportering.

Stadsnätsföreningen tycker att det är bra att utredningen tagit höjd för både den fysiska och logiska säkerheten. Den fysiska säkerheten täcks av den sektorsspecifika lagstiftningen och det är av vikt att den inte glöms bort i gränsdragningen mellan NIS2 och Lagen om elektronisk kommunikation (LEK) och att PTS med sin kompetens säkerställer att de unika riskerna inom sektorn elektronisk kommunikation fångas på det sätt som lagstiftningen avser.

Utredningen lägger förslag om delat tillsynsansvar mellan MSB och olika tillsynsmyndigheter för de olika sektorerna. Stadsnätsföreningen välkomnar utredningens förslag att PTS fortsatt ska vara tillsynsmyndighet för sektorn elektronisk kommunikation och bör vara den myndigheten som har föreskriftsrätt och tillsyn för den sektorspecifika delen.

Yttrandet

NIS2-direktivet ska implementeras i svensk lag och syftet är att öka motståndskraften i samhällsviktig verksamhet inom hela EU. Stadsnätsföreningen bedömer att det är i linje med de intentioner som framkommer av både direktivet och förslaget för att uppnå ett mer robust och motståndskraftigt samhälle. Stadsnätsföreningen tillstyrker utredningens förslag om hur Europaparlamentets och rådets direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS2-direktivet) ska implementeras i Sverige.

Flera myndigheter - gränsdragningsproblem

Stadsnätsföreningen ser vissa risker med den nya lagen, då det kan komma att finnas en gränsdragningsproblematik när det gäller föreskrifter, efterlevnad och tillsyn som riskerar att ta omfattande resurser i anspråk.

Det finns flera myndigheter som har ansvar för olika delar, vilket innebär att det finns risk för fragmentering. Föreskriftskrav från flera olika myndigheter som därtill ska göra tillsynsbesök utifrån sina perspektiv kan komma att öka bördan för både kommuner och företag. Stadsnätsföreningen håller med utredningen om att förslagen ska utformas så att regelbördan och administrationen minimeras för berörda verksamhetsutövare. Därför bör någon typ av samordnad hantering för att förtydliga kraven, föreskrifter och tillsynen för kommunerna och företagen i de delar som är grundläggande processer i lagkraven som gäller lika för alla. Det borde hjälpa till att undanröja en ojämn och fragmenterad implementering av cybersäkerhet nationellt och lätta på bördan för ett flertal föreskrivande myndigheter och tillsynsmyndigheter som inte behöver uttrycka samma krav i sina respektive föreskrifter och antalet föreskrifter minskar för berörda företag och kommuner.

Myndigheten för samhällsskydd (MSB) har särskilt framfört risken för att kraven kommer att tillämpas olika om olika myndigheter får meddela föreskrifter. Därför har MSB, Säkerhetspolisen, Transportstyrelsen och Integritetsskyddsmyndigheten (IMY) 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 specifika föreskrifter med särskilda krav på utökad säkerhet för sin sektor. En kompetens som den sektorspecifika myndigheten besitter. Stadsnätsföreningen stödjer MSBs förslag och anser att föreskriftsrätten bör ligga hos de olika sektorsmyndigheterna som kan fokusera på de unika särdragen som finns inom varje sektor i kompletterande föreskrifter.

Skälet till det är att olika myndigheter med sina särskilda uppdrag och kompetens kan säkerställa, genom specifika föreskrifter, att de unika riskerna inom respektive sektor fångas på det sätt som lagstiftningen avser.

Samordning

MSB ska enligt delbetänkandet fortsätta leda ett samarbetsforum där tillsynsmyndigheterna ingår. Syftet med forumet ska vara att underlätta samordning och åstadkomma en effektiv och likvärdig tillsyn. Stadsnätsföreningen tillstyrker förslaget och understryker vikten av samordning för att harmonisera föreskrivandet och tillsynen.

NIS2 och lagen om elektronisk kommunikation

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 föreslår en cybersäkerhetslag med övergripande regleringar, men att lagen behöver kompletteras med föreskrifter som meddelas av utpekad tillsynsmyndighet. Föreskrifterna från tillsynsmyndigheterna kommer därför att utgöra ett mycket viktigt komplement till de skyldigheter som föreslås i den nya cybersäkerhetslagen. Stadsnätsföreningen anser att dessa därför behöver utfärdas skyndsamt.

Fysisk och logisk säkerhet

Stadsnätsföreningen tycker det är bra att utredningen tagit höjd för både den fysiska och logiska säkerheten. Den fysiska säkerheten för exempelvis kablar och noder är avgörande för att skydda elektroniska kommunikationer mot incidenter. Den fysiska säkerheten täcks av den sektorsspecifika lagstiftningen och det är av vikt att den inte glöms bort i gränsdragningen mellan NIS2 och LEK och att PTS med sin kompetens säkerställer att de unika riskerna inom vår sektor fångas på det sätt som lagstiftningen avser.

Verksamhetsutövare och riskhanteringsåtgärder

Utredningen har kommit fram till att det i direktivet saknas en uttrycklig begränsning om att endast delar av den fysiska eller juridiska personens verksamhet skulle omfattas av direktivet. Utredningen har därför tagit ställning och anser att hela verksamheten ska omfattas. Stadsnätsföreningen förstår gränsdragningsproblematiken. Det är dock viktigt att det tydligt framgår att de riskhanteringsåtgärder som ska vidtas enligt cybersäkerhetslagen ska vara proportionerliga i förhållande till risken så att det inte blir onödigt betungande.

Enligt utredningen ska kraven om riskhanteringsåtgärder regleras övergripande i cybersäkerhetslagen och 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 bra. Men återigen vill Stadsnätsföreningen lyfta att det är angeläget att de tillsynsmyndigheter som har sektorskompetensen också omhändertar och anpassar föreskrifterna och har tillsynsansvaret för det.

Stadsnätsföreningen välkomnar ett klagörande 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 att de närmare bestämmelserna för detta bör följas av föreskrifter.

Incidentrapportering

Utredningen konstaterar att kravet på incidentrapportering enligt 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.

Utredningen föreslår att föreskrifter om vad som utgör en betydande incident ska få meddelas av utpekad myndighet. Föreskriftsrätten avseende vad som utgör en betydande incident och om incidentrapportering föreslås dock ges till MSB och inte till PTS.

Stadsnätsföreningen anser att det bör vara PTS som är mottagare av rapporten för sektorn elektronisk kommunikation. PTS är expertmyndighet som har kunskap om sektorn för elektronisk kommunikation och har dessutom föreskriftsrätten när det gäller incidentrapportering enligt LEK.

Stadsnätsföreningen håller också med MSB bedömning att cybersäkerhetslagens krav på incidentrapportering och tillsyn bör undantas när det gäller den säkerhetskryddade verksamheten för att undvika överlappning och otydlighet när det gäller tillsyn och rapportering enligt säkerhetskryddslagen.

Tillsynsmyndigheter

Utredningen lägger förslag om delat tillsynsansvar mellan MSB och olika tillsynsmyndigheter för de olika sektorerna. PTS är den myndighet som bevakar området elektronisk kommunikation i Sverige och har god kännedom om sektorn. Stadsnätsföreningen välkomnar utredningens förslag att PTS fortsatt ska vara tillsynsmyndighet för sektorn och bör vara den myndigheten som har föreskriftsrätt och tillsyn för den sektorspecifika delen.

Gemensam kontaktpunkt

Utredningen föreslår att en verksamhetsutövers anmälan om att den omfattas av NIS2-regleringen ska göras till respektive tillsynsmyndighet. Varje tillsynsmyndighet ska inom sitt tillsynsområde upprätta ett register över väsentliga och viktiga verksamhetsutövare. Tillsynsmyndigheterna ska sedan dela dessa uppgifter med MSB vars uppgift i egenskap av den gemensamma kontaktpunkten också ska dela dessa uppgifter med EU-kommissionen och NIS samarbetsgruppen.

Stadsnätsföreningen välkomnar utredningens förslag att MSB fortsatt utgör gemensam kontaktpunkt och får rollen som nationell cyberkrishanteringsmyndighet.

Mikael Ek

Vd Stadsnätsföreningen

Elin Bertilsson

Ordf. Stadsnätsföreningen