STOKAB

Remissvar

Datum	2024-11-10
Diarienummer	STOK 2024/379
Sida	1(4)
Handläggare	Patricia Helanow

Stockholms Stadshus AB
remiss@stadshusab.se

Yttrande över betänkandet Motståndskraft i samhällsviktiga tjänster (SOU 2024:64), SSAB:s dnr. 2024/166

Remissen

AB Stokab (”**Stokab**”) har erhållit betänkandet *Motståndskraft i samhällsviktiga tjänster (SOU 2024:64)* (”**Utredningen**”) på remiss från kommunstyrelsen genom underremiss från Stockholms Stadshus AB, för yttrande senast den 10 november efter erhållet anstånd.

I Utredningen föreslås de anpassningar av svensk rätt som är nödvändiga för att EU:s direktiv om kritiska entiteters motståndskraft (”**CER-direktivet**”) ska kunna genomföras. Direktivets syfte är att stärka kritiska verksamhetsutövares motståndskraft och förmåga att tillhandahålla samhällsviktiga tjänster på den inre marknaden. Utredningen föreslår att CER-direktivet införlivas genom en ny lag, lagen om motståndskraft hos kritiska verksamhetsutövare, samt att denna ska träda i kraft den 1 augusti 2025.

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 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. Genom sin verksamhet tillhandahåller Stokab ett allmänt elektroniskt kommunikationsnät.

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. STEK tillhandahåller inom ramen för sin verksamhet bl.a. DNS-tjänster.

Allmänna elektroniska kommunikationsnät och DNS-tjänster utgör båda tjänster inom sektorn digital infrastruktur vilka enligt utredningens delbetänkande[1] ska omfattas av den nya cybersäkerhetslagen, vilken implementerar det s.k. NIS2-direktivet[2] i svensk rätt och är föreslagen att träda ikraft 1 januari 2025. Såväl Stokab som STEK kommer därför att omfattas av cybersäkerhetslagen.

Nedan följer Stokabs synpunkter på valda avsnitt i Utredningen.

Stokabs synpunkter

Tillämpningsområdet (avsnitt 5)

Lagen om motståndskraft hos kritiska verksamhetsutövare föreslås, i enlighet med CER-direktivet, att tillämpas på enskilda och offentliga verksamhetsutövare som tillhandahåller en samhällsviktig tjänst som omfattas av bilagan till direktivet. Tillhandahållande av allmänna elektroniska kommunikationsnät och DNS-tjänster utgör sådana tjänster inom sektorn digital infrastruktur. Därutöver krävs att verksamhetsutövaren har identifierats som *kritisk* av tillsynsmyndigheten.

Kritiska verksamhetsutövare inom sektorerna bankverksamhet, finansmarknads-infrastruktur och digital infrastruktur är dock uttryckligen undantagna de väsentliga delarna av lagen, innefattande bestämmelserna om riskbedömning och åtgärder för motståndskraft, incidentrapportering samt bakgrundskontroll. Detta innebär även att bestämmelserna om tillsyn och sanktioner inte ska tillämpas för sådana kritiska verksamhetsutövare. Undantaget för digital infrastruktur motiveras av att det av CER-direktivet följer att NIS2-direktivet redan ställer minst likvärdiga krav om åtgärder för att hantera risker som hotar säkerheten i nätverks- och informationssystem samt incidentrapportering.

Som redogjorts för ovan är såväl Stokab som STEK verksamma inom sektorn digital infrastruktur - Stokab genom tillhandahållandet av ett allmänt elektroniskt kommunikationsnät och STEK genom tillhandahållandet av DNS-tjänster till verksamheter inom Stockholms stad. För det fall något av bolagen skulle identifieras av tillsynsmyndigheten som en kritisk verksamhetsutövare, kommer bolaget således endast att omfattas av mycket begränsade delar av lagen, och då snarare av rättigheter än skyldigheter. Mot denna bakgrund är Stokabs synpunkter nedan begränsade till valda delar av det fåtal bestämmelser som föreslås bli tillämpliga för kritiska verksamhetsutövare inom digital infrastruktur.

Sekretess (avsnitt 13)

I Utredningen identifieras ett behov av att stärka sekretesskyddet för sådana uppgifter som kan komma att behandlas enligt CER- och NIS2-direktiven, exempelvis uppgifter i incidentrapporter. Anledningen till detta är att Utredningen anser att befintliga

---

[1] Nya regler om cybersäkerhet (SOU 2024:18)

[2] EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen

bestämmelser i offentlighets- och sekretesslagen (2009:400) ("**OSL**") inte ger ett tillräckligt skydd för sådana uppgifter. Stokab delar Utredningens bedömning i detta avseende. Vidare instämmer Stokab med vad som anförs i Utredningen när det gäller vikten av att sådana känsliga uppgifter som typiskt sett ingår i incidentrapporter ges ett fullgott skydd.

Utredningen föreslår att en ny sekretessbestämmelse införs i 18 kap. OSL för uppgift i incidentrapporter enligt lagen om cybersäkerhet och lagen om motståndskraft hos kritiska verksamhetsutövare samt för uppgift om åtgärd som följer av en sådan incident. Bestämmelsen föreslås utformas med ett omvänt skaderekvisit. Vidare föreslås att rätten att meddela och offentliggöra uppgifter begränsas. Stokab anser att förslaget till ny sekretessbestämmelse är väl utformat och instämmer i övrigt med Utredningens förslag.

Ändringar i säkerhetsskyddsregleringen (avsnitt 14)

I Utredningens uppdrag har även ingått att föreslå ändringar som behövs för att uppnå en mer sammanhållen systematik mellan säkerhetsskyddslagen (2018:585), lagen om cybersäkerhet och lagen om motståndskraft hos kritiska verksamhetsutövare, särskilt vad gäller tillsynsmyndigheternas befogenheter och sanktionsavgifternas storlek.

När det gäller sanktionsavgiften för enskilda verksamhetsutövare föreslår Utredningen att denna ska höjas och bestämmas till lägst 25 000 kronor och högst till det högsta av 120 000 000 kronor eller 2 procent av verksamhetsutövarens totala globala årsomsättning under föregående räkenskapsår. Förslaget innebär en signifikant höjning av det maximibelopp för sanktionsavgiften på 50 miljoner kronor som gäller idag. Förslaget till höjning motiveras utifrån en jämförelse med de föreslagna sanktionsavgifternas storlek i lagen om cybersäkerhet och lagen om motståndskraft hos kritiska verksamhetsutövare. Eftersom maximibeloppen för sanktionsavgift i de lagförslagen uppgår till det högsta av 10 000 000 euro eller 2 procent av verksamhetsutövarens totala globala årsomsättning under föregående räkenskapsår, konstaterar Utredningen att en överträdelse av de lagarna skulle kunna leda till mer kännbara sanktionsavgifter än en överträdelse av säkerhetsskyddslagstiftningen, vilket Utredningen inte anser är önskvärt.

Stokab instämmer med vad som anförs i Utredningen att skyddet av Sveriges säkerhet är grundläggande för vår säkerhet som nation samt att säkerhetsskyddslagen är central för skyddet av dessa intressen. Av denna anledning behöver sanktionerna vara av sådan art att det är avskräckande att bryta mot lagen. Stokab anser förvisso att nu gällande maximibelopp för sanktionsavgiften på 50 miljoner kronor är tillräckligt avskräckande, men har förståelse för förslaget om höjning utifrån jämförelsen med de föreslagna sanktionsavgifternas storlek i lagen om cybersäkerhet och lagen om motståndskraft hos kritiska verksamhetsutövare. Stokab önskar dock framföra att möjligheten till utfärdande av så höga sanktionsavgifter också ställer höga krav på tydliga regler och vägledning för reglernas tillämpning. I detta avseende kan konstateras att bestämmelserna om sanktioner och ingripande i säkerhetsskyddslagen inte har varit i kraft någon längre tid och det saknas vägledande praxis vad gäller reglernas tillämpning. Det är därför viktigt att åtgärda identifierade brister bland annat genom att omhänderta de åtgärdsförslag för förbättrat tillsynsarbete som framkommit inom ramen för regeringens uppdrag att redovisa hur arbetet med tillsyn inom säkerhetsskyddsområdet har bedrivits och fungerat under perioden 1 januari 2021–31 december 2023.

Stockholm som ovan

Joakim Larsson
Verkställande direktör
AB Stokab