Stockholm 2026-05-18

Remissvar

Försvarsdepartementet
DNR: Fö2026/00576
fo.remissvar@regeringskansliet.se
fo.ech.remissvar@regeringskansliet.se

Yttrande gällande

Europeiska kommissionens förslag på cybersäkerhetspaket

Svenska Stadsnätsföreningen är en bransch- och intresseorganisation som representerar stadsnät i närmare 200 kommuner och 120 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.

Stadsnätsföreningen tackar för möjligheten att lämna synpunkter på Europeiska kommissionens förslag på cybersäkerhetspaket.

Bakgrund

EU-kommissionen presenterade i början av året ett cybersäkerhetspaket för att stärka EU:s motståndskraft mot cyberangrepp och hybridpåverkan mot kritisk infrastruktur och samhällsviktiga tjänster. Som nu Försvarsdepartementet har skickat ut på remiss.

Förslaget rör tre huvuddelar: (1) uppdaterat mandat för EU:s cybersäkerhetsbyrå ENISA, (2) förenklat och tydligare ramverk för cybersäkerhetscertifiering (ECCF), samt (3) ett nytt ramverk för säkerhet i IKT-leveranskedjor med fokus på leverantörsrisker.

Bakgrunden är en förvärrad hotbild och ökade sårbarheter i cyberrymden. EU har därför de senaste åren antagit bl.a. NIS2 och ”5G-verktygslådan” samt aviserat en mer samlad ansats för inre säkerhet och motståndskraft i strategin ProtectEU. CSA 2 är ett led i detta och ska stärka genomförandet och samspelet mellan regelverken, med tydlig koppling till NIS2 och ett ökat fokus på säkerhet i digitala leveranskedjor.

ENISA

Kommissionens förslag innebär en översyn av mandatet för EU:s cybersäkerhetsbyrå ENISA, med syfte att förtydliga och i vissa delar utöka byråns ansvar och uppgifter. Förslaget stärker ENISA:s roll som stödjande aktör i genomförandet av unionens cybersäkerhetsram, samtidigt som byrån ges en mer framträdande roll i operativt samarbete, särskilt vid gränsöverskridande incidenter, samt utökade uppgifter inom bland annat certifiering, sårbarhetshantering och stöd till marknadsaktörer.

Stadsnätsföreningen är positiv till att ENISA:s nuvarande uppgifter förtydligas och stärks, särskilt avseende policyutveckling, kunskapsuppbyggnad och kunskapsspridning samt stöd till standardisering och övningar.

Svenska Stadsnätsföreningen | *Swedish Local Fibre Alliance*
Wallingatan 22 | 111 24 Stockholm | Sweden
+46 8 214 930 | kansli@ssnf.org | www.ssnf.org

Stadsnätsföreningen delar den svenska regeringens bedömning i sin promemoria[1] att den föreslagna utvidgningen av ENISA:s mandat, särskilt en mer operativ roll och möjligheten att ta ut avgifter, behöver analyseras ytterligare och tydliggöras. Utan ett sådant förtydligande finns en risk att ENISA:s uppgifter går in i medlemsstaternas ansvar, inklusive nationella team som tar emot och hanterar it-säkerhetsincidenter (CSIRT) och behöriga myndigheter. Detta riskerar att leda till otydliga roller, dubbelrapportering och ökade administrativa bördor. Förslag som syftar till att förenkla incidentrapportering är positiva, men kräver gemensamma och tydliga krav samt att risken för dubbelrapportering minskar. Föreningen vill även betona vikten av en säker och rättssäker hantering av känslig information.

IKT-leveranskedjor (supply chain security)

Stadsnätsföreningen delar uppfattningen att cybersäkerhet är av central betydelse och stödjer ambitionen att stärka säkerheten i Europas digitala infrastruktur, särskilt för samhällsviktig verksamhet.

Förslaget innebär bl.a. att Europeiska kommissionen kan få en tydligare roll i att identifiera och analysera risker kopplade till tredjeländer. Bedömningar kan omfatta faktorer som statlig kontroll och styrning, rättssystemets utformning och geopolitisk kontext. Leverantörer med koppling till sådana länder kan i vissa fall klassificeras som högriskleverantörer, vilket kan medföra krav på riskreducerande åtgärder. Det framgår även att komponenter från högriskleverantörer kan behöva begränsas eller fasas ut i så kallade nyckeltillgångar, och att detta kan omfatta både mobila och fasta nät.

Stadsnätsföreningen delar inriktningen att högriskleverantörer ska kunna fasas ut när det krävs för att skydda samhällsviktig digital infrastruktur. Samtidigt behöver beslut om begränsningar eller förbud föregås av noggranna konsekvensbedömningar och risk- och sårbarhetsanalyser, där säkerhetsnyttan vägs mot kostnader och genomförandeeffekter.

En utfasning i befintliga nät kan bli kostsam, särskilt om redan installerad utrustning måste ersättas. Om omfattande utbyteskrav tränger undan investeringar i ny infrastruktur, exempelvis fortsatt fiberutbyggnad, kan det försvaga både utbyggnadstakt och investeringsklimat. Förutsebara krav, realistiska tidsplaner och tydlighet kring vilka tillgångar som omfattas är därför centralt.

Den föreslagna maxperioden om 36 månader kan vara kort med hänsyn till tekniska beroenden samt upphandlings- och genomförandeprocesser. Kraven behöver därför utformas så att de stärker säkerheten utan att skapa oplanerade driftstörningar eller försvåra långsiktiga investeringar.

Fasta nätet – flera lager

Stadsnätsföreningen noterar att kommissionens förslag i mindre utsträckning analyserat hur leverantörsbegränsningar ska tillämpas i fasta nät än i mobilnäten.

Det fasta elektroniska kommunikationsnätet är inte en sammanhållen teknikplattform, utan består av flera lager och nätdelar (t.ex. accessnät och transportnät) med olika typer av nätutrustning i respektive del. Tillgången till europeiska leverantörer som kan bedömas som ”säkra” eller godtagbara varierar mellan dessa lager. I vissa delar av den fiberbaserade infrastrukturen saknas europeiska alternativ helt eller är mer begränsade, vilket kan göra krav på att begränsa eller ersätta leverantörer som bedöms utgöra en säkerhetsrisk svåra att genomföra och förenade med betydande kostnader och tekniska utmaningar, särskilt när antalet alternativa leverantörer är litet. Jämfört med detta finns i mobilnäten etablerade

europeiska leverantörer och EU:s 5G-verktygslåda utgör en etablerad referensram för hantering av leverantörsrisker.

Stadsnätsföreningen anser därför att kommissionens analys behöver utvecklas och att förslaget bör föregås av en fördjupad analys av tillämpningen i fasta nät. Mot bakgrund av fasta nätens tekniska komplexitet behöver det tydliggöras vilka lager, nätdelar och komponenttyper som avses (inklusive vilka "nyckeltillgångar" som kan omfattas), samt hur eventuella krav ska kunna genomföras i befintlig infrastruktur på ett proportionerligt och praktiskt genomförbart sätt.

Rådighet, ägande och driftansvar
Säkerhet i samhällskritisk digital infrastruktur handlar inte bara om enskilda tekniska komponenter eller leverantörer. Minst lika viktigt är vem som har rådighet över infrastrukturen – alltså kontroll över drift, underhåll, förvaltning och den långsiktiga utvecklingen.

Förslaget har ett tydligt fokus på risker kopplade till leverantörer och tredjeländer. Föreningen anser att analysen därför behöver kompletteras med strukturella faktorer: vem som äger infrastrukturen, vilka aktörer som ansvarar för drift och underhåll, och vilka rättsliga och organisatoriska förutsättningar som styr deras arbete. Dessa förutsättningar påverkar i praktiken möjligheten att genomföra säkerhetsåtgärder och att upprätthålla tydligt ansvar över tid. Föreningen vill också lyfta risken för oavsiktlig koncentration: om åtgärderna i praktiken leder till att få leverantörer eller aktörer återstår kan konkurrensen minska och den samlade motståndskraften försvagas.

Bredare analys och tydliga definitioner
Föreningen anser att kommissionens analys behöver breddas: dels genom att tydligare belysa möjliga tekniska, riskbaserade sätt att minska sårbarheter och beroenden, dels genom att centrala begrepp definieras på ett sätt som ger rättssäkerhet och förutsebarhet i tillämpningen.

Föreningen saknar exempelvis en analys av om säkerhet och resiliens kan stärkas genom riskbaserade tekniska åtgärder som komplement till leverantörsbegränsningar, till exempel leverantörsdiversifiering (multivendor, det vill säga olika leverantörer i olika delar av nätet), teknisk segmentering och redundans.

Föreningen ser också ett behov av att centrala begrepp såsom högriskland, högriskleverantör och nyckeltillgångar definieras tydligt för att säkerställa rättssäkerhet och förutsebarhet samt minska risken för att beslutsfattande uppfattas som politiskt eller godtyckligt.

Därtill är det viktigt med en tydlig ansvarsfördelning mellan EU-nivå och nationell nivå, där EU kan bidra med samordning och gemensam inriktning när det ger mervärde. Samtidigt är det avgörande att nationell kompetens och lokal kännedom tas till vara i den praktiska tillämpningen och genomförandet, inte minst när det gäller kunskap om hotbild, säkerhetsarbete och hur nät och verksamheter fungerar i praktiken.

Sammanfattande behov av analys och proportionalitet
Mot denna bakgrund anser Svenska Stadsnätsföreningen att de föreslagna åtgärderna avseende leverantörsbegränsningar och högriskklassificering behöver analyseras vidare, särskilt med avseende på proportionalitet, rättssäkerhet och praktisk genomförbarhet. Det är centralt att åtgärderna stärker den faktiska säkerheten utan att skapa oproportionerliga

kostnader eller hinder för fortsatt utbyggnad och förvaltning av robust, samhällskritisk fiberinfrastruktur i hela landet.

Samordning och förenkling av krav

Cybersäkerhetspaketet kommer att verka parallellt med andra regelverk, såsom exempelvis NIS2-direktivet (direktivet om åtgärder för en hög gemensam nivå av cybersäkerhet i hela EU) och CRA (Cyber Resilience Act, EU:s cybersäkerhetskrav för produkter med digitala inslag). Om regelverken inte samordnas finns en risk att de sammantaget skapar ett komplext system där resurser i allt större utsträckning läggs på att hantera formella krav, snarare än att stärka säkerheten i praktiken. Därför är det viktigt att cybersäkerhetspaketet utformas i linje med befintliga regelverk, så att det inte leder till mer administration, överlapp och dubbelarbete.

Säkerhetsfrågor präglas samtidigt av starka nationella intressen, vilket innebär att EU-regelverk ofta kompletteras med nationella åtgärder. Den samlade regleringen behöver därför utformas så att risken för överlapp, motstridiga krav och dubbelrapportering begränsas.

För att bidra till förenkling är det vidare viktigt att certifiering utformas som ett frivilligt verktyg, och att kraven på certifiering och efterlevnad blir tydliga, proportionerliga och möjliga att tillämpa i praktiken.

Elin Bertilsson

VD, Svenska Stadsnätsföreningen

Camilla Jönsson

Sakkunnig samhälle och politik,
Svenska Stadsnätsföreningen