INTERNET STIFTELSEN

13 maj 2026

Försvarsdepartement

Avdelningen för försvarsunderrättelser, säkerhets- och cyberfrågor,

Enheten för cyber och hybridfrågor

Fö2026/00576

Internetstiftelsens remissvar på Europeiska kommissionens cybersäkerhetspaket med förslag om ändringar i cybersäkerhetsakten (EU 2019/881) samt riktade ändringar i NIS 2-direktivet (EU 2022/2555) KOM (2026)11,13

Stiftelsen för Internetinfrastruktur (”Internetstiftelsen”) har beretts tillfälle att yttra sig över Europeiska kommissionens cybersäkerhetspaket med förslag om ändringar i cybersäkerhetsakten (EU 2019/881) samt riktade ändringar i NIS 2-direktivet (EU 2022/2555) KOM (2026)11,13.

Om Internetstiftelsen

Internetstiftelsen är en oberoende, affärsdriven och allmännyttig organisation som verkar för ett internet som bidrar positivt till människor och samhälle. Organisationen säkerställer en robust och säker internetinfrastruktur som möter dagens och framtidens behov i Sverige, samtidigt som de främjar forskning, utbildning och undervisning med inriktning på internet.

Internetstiftelsen ansvarar för internets svenska toppdomän .se samt drift och administration av toppdomänen .nu. Intäkterna från denna verksamhet finansierar allmännyttiga insatser.

Genom satsningarna bidrar Internetstiftelsen till att öka den digitala kompetensen och resiliensen i samhället, stärka kunskapen om internetanvändning och dess påverkan på individ och samhälle samt utveckla identitets- och behörighetslösningar som förenklar inloggning och stärker säkerheten.

Internetstiftelsens vision är att alla i Sverige vill, vågar och kan använda internet.

Sammanfattning

- Internetstiftelsen välkomnar ambitionen att stärka cybersäkerheten inom EU genom ett harmoniserat certifieringsramverk och åtgärder för säkrare IKT-leveranskedjor. Samtidigt bedömer Internetstiftelsen att flera delar av förslaget riskerar att få långtgående konsekvenser för konkurrens, innovation och den praktiska driften av internetinfrastruktur.

- När det gäller det europeiska ramverket för cybersäkerhetscertifiering finns en risk att certifieringsordningar i praktiken blir nödvändiga för marknadstillträde.

Detta kan skapa betydande kostnader och administrativa bördor, särskilt för små och medelstora företag, och därigenom leda till ökade inträdesbarriärer och marknadskoncentration. Internetstiftelsen anser därför att certifieringskrav måste utformas proportionerligt och med särskild hänsyn till mindre aktörers förutsättningar. Flexibla och riskbaserade modeller för efterlevnad bör möjliggöras, inklusive erkännande av etablerade internationella standarder såsom ISO/IEC 27001.

- Internetstiftelsen framhåller vidare att certifiering inte bör utvecklas till det enda accepterade sättet att visa efterlevnad av NIS2-direktivets krav. Certifiering kan vara ett värdefullt stöd för tillsyn och harmonisering, men kan inte ersätta verksamhetsutövarens eget kontinuerliga och riskbaserade cybersäkerhets-arbete.

- Vad gäller regleringen av säkerhet i IKT-leveranskedjor konstaterar Internetstiftelsen att förslaget innebär en mycket långtgående reglering med potentiellt omfattande konsekvenser för internetinfrastruktur och gränsöverskridande verksamheter. Särskilt oroande är möjligheten att identifiera högriskleverantörer och införa förbud eller begränsningar genom genomförandeakter, utan att det tydligt framgår hur konsekvenserna för internets robusthet och funktion ska bedömas. Internetstiftelsen efterlyser därför djupgående konsekvensanalyser innan sådana åtgärder införs. Aktörer som påverkas av eventuella begränsningar bör involveras i bedömningarna, inklusive analyser av tekniska, operativa och ekonomiska konsekvenser.

- Internetstiftelsen ser även risker för överlappning mellan CSA 2.0 och NIS2, särskilt avseende krav på riskhantering i leveranskedjan.

- Slutligen välkomnar Internetstiftelsen förslaget att undanta leverantörer av DNS-tjänster som är mikro- eller småföretag från tillämpningsområdet.

Inledning
Internetstiftelsens svar begränsas till delar av förslagen enligt nedan.

Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING
om Europeiska unionens cybersäkerhetsbyrå (Enisa), om det europeiska ramverket för cybersäkerhetscertifiering och om säkerhet i IKT-leveranskedjan samt om upphävande av förordning (EU) 2019/881 (cybersäkerhetsakt 2)

Avdelning III – Europeiskt ramverk för cybersäkerhetscertifiering

Certifieringsramverkets utformning och marknadseffekter

Internetstiftelsen noterar att det föreslagna förstärkta europeiska ramverket för cybersäkerhetscertifiering riskerar att i praktiken leda till en certifieringsdriven marknadsmodell. En sådan utveckling kan få betydande konsekvenser för konkurrensen på den inre marknaden.

Särskilt finns en risk att höga kostnader, administrativ komplexitet och kumulativa certifieringskrav skapar oproportionerliga inträdesbarriärer för små och medelstora företag (SME). Detta kan leda till en marknadskoncentration till förmån för ett begränsat antal stora leverantörer, vilket i sin tur riskerar att motverka förordningens övergripande mål om stärkt europeisk cybersäkerhetskapacitet och resiliens.

Mot denna bakgrund bör förordningen, i enlighet med proportionalitetsprincipen säkerställa att certifieringskrav utformas med hänsyn till kostnads- och resursbörda för olika aktörskategorier, att särskilda SME-anpassningar införs, exempelvis genom differentierade krav eller stegvis införande, samt att varje nytt europeiskt certifieringssystem föregås av en strukturerad konsekvensanalys.

Vidare bör det i den fortsatta lagstiftningsprocessen säkerställas att ramverket inte oavsiktligt gynnar aktörer med större finansiella och administrativa resurser, oavsett etableringsland.

Möjligheter till efterlevnad och erkännande av etablerade standarder

Internetstiftelsen framhåller vikten av att det europeiska certifieringsramverket inte utformas på ett sätt som leder till att enskilda certifieringsordningar blir de facto-obligatoriska för marknadstillträde.

För att upprätthålla en välfungerande inre marknad och undvika onödiga inträdesbarriärer bör förordningen möjliggöra flera likvärdiga sätt att visa efterlevnad av säkerhetskrav, förutsatt att en jämförbar säkerhetsnivå kan säkerställas.

Internetstiftelsen anser vidare att i detta avseende bör särskilt erkännande av etablerade internationella standarder, såsom ISO/IEC 27001, möjliggöras, utformningen av europeiska certifieringssystem bör undvika att skapa de facto-monopol för enskilda certifieringsmodeller, samt flexibla certifieringsstrukturer främjas, vilket möjliggör anpassning till olika tekniska lösningar.

Samtidigt är det av vikt att sådana alternativa vägar till efterlevnad utformas på ett sätt som inte underminerar harmonisering och jämförbarhet inom unionen. Det bör därför tydliggöras vilka kriterier som ska vara uppfyllda för att olika metoder ska anses likvärdiga.

Avdelning IV – Säkerhet i IKT-leveranskedjor

Generella synpunkter

EU-kommissionens målsättning är att minska de risker för kritiska IKT-leveranskedjor som orsakas av entiteter som är etablerade i eller kontrolleras av entiteter från tredjeländer som utgör cybersäkerhetsproblem (högriskleverantörer) och minska kritiska beroenden genom att utarbeta en samstämmig och ändamålsenlig ram på EU-nivå för att hantera säkerhetsrisker för IKT-leveranskedjan.

I förslaget anges också den proportionalitetsprincip som görs gällande: Beträffande de lösningar som föreslås i samband med säkerheten i IKT-leveranskedjan föreskrivs det i ramen att man ska samla in bevis på vad som utgör viktiga tillgångar och vilka åtgärder som skulle vara proportionerliga och nödvändiga för att minska riskerna för de kritiska leveranskedjorna. Innan dessa åtgärder fastställs kommer en bedömning av de ekonomiska konsekvenserna att göras, där man bland annat undersöker den ekonomiska genomförbarheten, de tillgängliga alternativen på marknaden och de specifika produkternas livscykel. Denna bedömning kommer att hjälpa till att fastställa vilka riskbaserade åtgärder som behövs och är lämpligast.

Internetstiftelsen välkomnar att EU-kommissionen undersöker sätt att stärka säkerheten i kritiska IKT-leveranskedjor. Förslaget innebär dock en betydande utvidgning av EU:s

reglering av IKT-leveranskedjor, särskilt eftersom det öppnar för EU-gemensamma begränsningsåtgärder mot vissa leverantörer genom genomförandeakter.

EU:s verktygslåda för cybersäkerhet har stärkts gradvis de senaste åren, men förslagen i CSA 2.0 går längre. Kommissionen skulle för första gången kunna peka ut tredjeländer som cybersäkerhetsrisker, förbjuda eller gradvis fasa ut vissa leverantörer och införa EU-gemensamma begränsningar för hur produkter och tjänster får användas genom genomförandeakter. Det är svårt att fullt ut förstå och därmed bedöma följden av detta.

Vi delar uppfattningen att leverantörsberoenden som innebär reella cybersäkerhets-risker måste kunna hanteras kraftfullt. Vår invändning gäller inte behovet av sådana åtgärder, utan att besluten måste föregås av transparenta, riskbaserade och tekniskt välgrundade konsekvensanalyser så att åtgärderna stärker, och inte oavsiktligt försvagar, internets robusthet.

Risken med överlappning av NIS2

I NIS2 ställs krav på de entiteter som omfattas av lagstiftningen, att genomföra riskanteringsåtgärder avseende leveranskedjan. Det finns således risk för överlappning med NIS2, samt till följd av det, oklar ansvarsfördelning som riskerar att leda till dubbla krav på riskhantering och dubbla tillsyner. Det är av vikt att det är en tydlig gränsdragning mellan regelverken.

Begränsningsåtgärder i relation till gränsöverskridande verksamheter

EU-kommissionen anger i konsekvensbedömningen att efter en omfattande analys framkom alternativet att utarbeta en heltäckande och övergripande ram för att hantera cybersäkerhetsrisker för IKT-leveranskedjor som det rekommenderade alternativet. Kommissionen menar att genom detta alternativ skulle en övergripande, teknik- och sektorsneutral ram inrättas för att hantera icke-tekniska cybersäkerhetsrisker för IKT-leveranskedjor.

Vad som inte framgår i EU-kommissionens förslag är hänsyn till den struktur som internet är uppbyggd med, och som är högst relevant för aktörer i internetinfrastruktur-kedjan, där bland annat en toppdomänadministratör som är klassad som en väsentlig enhet enligt NIS2.

Internets infrastruktur är i praktiken en sammanhängande kedja där varje del är beroende av aktörer i flera länder. En datatrafik från Sverige till en digital tjänst kan exempelvis passera kablar, nät och knutpunkter som ägs eller drivs av företag i andra jurisdiktioner, inklusive ett tredje land. Även centrala funktioner som DNS, molntjänster och innehållsdistribution hanteras ofta av globala aktörer med verksamhet spridd över flera länder.

Detta innebär att internets funktion och tillgänglighet är beroende av både fysisk infrastruktur och ett fungerande samarbete mellan ett stort antal oberoende aktörer världen över. Störningar, regleringar eller konflikter i en del av denna kedja kan få konsekvenser även i andra länder, vilket understryker internets gränsöverskridande och ömsesidigt beroende karaktär.

Internetstiftelsen saknar en djupgående konsekvensbedömning av vad en begränsning i IKT-kedjan skulle kunna få för konsekvenser för den typ av gränsöverskridande verksamhet som sker i internets infrastrukturkedja. En sådan konsekvensanalys bör åtminstone omfatta effekter på tillgänglighet, redundans, DNS-resolution,

incidenthantering, migreringstider, avtalsrättsliga konsekvenser, kostnader, alternativa leverantörer, interoperabilitet samt risken för koncentration till ett fåtal godkända leverantörer.

Identifiering av viktiga IKT-tillgångar

I artikel 102 framgår de punkter som Kommissionen ska beakta vid identifieringen av viktiga IKT-tillgångar. Vidare framgår i artikel 103 att Kommissionen ges befogenhet att anta genomförandeakter för att fastställa att väsentliga och viktiga entiteter enligt NIS2, ska vara förbjudna att i någon form använda, installera eller integrera IKT-komponenter eller komponenter som innehåller IKT-komponenter från högriskleverantörer som identifierats.

Internetstiftelsen vill lyfta att det kan få stora konsekvenser för internets robusthet, med hänvisning till den beskrivning om internets infrastrukturkedja enligt ovan.

Internetstiftelsen anser vidare att det saknas utrymme för involvering i bedömningen av de aktörer som i praktiken kommer att påverkas av dessa eventuella förbud. Det bör tydliggöras att de aktörer som kommer att påverkas, måste involveras i bedömningen och särskilt i bedömningen av de konsekvenser ett sådant förbud skulle få för entitetens förmåga att leverera sin tjänst eller produkt, inklusive de ekonomiska konsekvenserna att finna ny leverantör, lämna ingångna avtal etc.

Som lyfts tidigare är det följaktligen svårt att förstå konsekvenserna av förslagen. En djupgående konsekvensanalys är obligatoriskt, i vilken de aktörer som i praktiken kommer att påverkas av lagförslagen måste involveras.

Förslag till EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV om ändring av direktiv (EU) 2022/2555 vad gäller förenklingsåtgärder och anpassning till [förslag till cybersäkerhetsakt 2]

Cybersäkerhetscertifiering

Internetstiftelsen välkomnar ambitionen att genom europeiska cybersäkerhets-certifieringsordningar skapa en ökad harmonisering av hur efterlevnad av NIS2-direktivets krav kan påvisas. Gemensamma certifieringsramverk kan bidra till ökad tydlighet, jämförbarhet och förutsebarhet mellan medlemsstaterna, vilket är särskilt värdefullt för verksamheter som verkar gränsöverskridande.

Internetstiftelsen anser samtidigt att certifiering bör användas med försiktighet som bevismedel för efterlevnad av artikel 21. NIS2-direktivet bygger på ett riskbaserat och proportionellt förhållningssätt där säkerhetsåtgärder ska anpassas utifrån verksamhetens risker, storlek, exponering och samhällsviktiga funktion. Även genomförandeförordningen betonar proportionalitet och behovet av att kunna beakta alternativa eller kompenserande åtgärder. Mot denna bakgrund bör certifiering inte införas som ett generellt krav eller utvecklas till det enda accepterade sättet att visa efterlevnad.

Ett certifikat kan vara ett relevant stöd för att visa att vissa delar av kraven i NIS2 uppfylls, förutsatt att certifieringsordningen faktiskt omfattar relevanta delar av direktivets krav. Certifiering kan även underlätta tillsyn och uppföljning genom att vissa kontroller redan har granskats av en extern och oberoende part samt följs upp genom återkommande revisioner och omcertifieringar. För de delar där certifieringen ger faktisk

täckning skulle detta kunna minska behovet av att återkommande lämna in motsvarande underlag till tillsynsmyndigheter.

Samtidigt bör det tydliggöras att certifiering inte är liktydigt med faktisk cybersäkerhet eller fullständig efterlevnad av NIS2. Certifieringar fångar inte nödvändigtvis alla verksamhetsspecifika risker och kan inte ersätta verksamhetsutövarens eget ansvar för att bedriva ett kontinuerligt och riskbaserat cybersäkerhetsarbete. Certifiering bör därför ses som ett komplement till andra former av efterlevnadsarbete och inte som ett fullständigt bevis på att samtliga krav i direktivet är uppfyllda.

Internetstiftelsen vill även understryka vikten av att eventuella certifieringsordningar utformas med hänsyn till sektorsspecifika förhållanden. Generiska certifieringsmodeller riskerar att inte fullt ut spegla de särskilda hot, beroenden och säkerhetskrav som kännetecknar DNS-ekosystemet och annan viktig internetinfrastruktur. Det finns därmed en risk att fokus förskjuts från effektiva och verksamhetsanpassade säkerhetsåtgärder till formell efterlevnad av standardiserade kontrollkrav.

Det är vidare viktigt att tydliggöra att certifiering inte begränsar tillsynsmyndigheternas ansvar eller befogenheter och inte heller innebär någon form av ansvarsfrihet vid incidenter eller brister i säkerhetsarbetet. Verksamheter utan certifiering måste fortsatt kunna visa efterlevnad genom andra relevanta och ändamålsenliga metoder.

Internetstiftelsen vill också framhålla att obligatoriska eller de facto nödvändiga certifieringar riskerar att skapa inträdesbarriärer, särskilt för mindre aktörer med begränsade resurser i form av personal, tid och ekonomi. Detta kan på sikt påverka konkurrensen och innovationsförmågan negativt inom sektorn.

Mot denna bakgrund anser Internetstiftelsen att förslaget bör justeras för att säkerställa proportionalitet, flexibilitet och en tydlig koppling till verksamhetsspecifika risker. Certifiering kan vara ett värdefullt verktyg för att stödja efterlevnad och underlätta tillsyn i vissa delar, men bör inte utformas eller tillämpas på ett sätt som tränger undan andra rimliga och riskbaserade sätt att uppnå och visa en hög nivå av cybersäkerhet.

Leverantörer av DNS-tjänster som är mikroföretag eller små företag

Internetstiftelsen instämmer i bedömningen att leverantörer av DNS-tjänster som är mikroföretag eller små företag ska strykas från tillämpningsområdet.

Ärendet har beretts av senior legal counsel Filippa Murath, CISO Catharina Ankre och Information Security Specialist Nicklas Larsson.

För Internetstiftelsen

Carl Piva, vd