Remissvar

Försvarsdepartementet

Vårt diarienummer:
2026-00904
Ert diarienummer:
Fö2026/00576
Datum:
2026-05-18

Vinnovas remissvar avseende EUs cybersäkerhetspaket

Sammanfattning

Vinnova tillstyrker förslaget på Europeiska kommissionens cybersäkerhetspaket och bedömer att det har god potential att stärka såväl den samlade cybersäkerheten som den digitala motståndskraften i EU. För att uppnå detta är det dock avgörande att genomförandet präglas av ett tydligt innovations-, forsknings- och näringslivsperspektiv. Cybersäkerhet och resilient kritisk digital infrastruktur bör betraktas som horisontella och strategiska möjliggörare för innovation, snarare än enbart som frågor om regelefterlevnad, **särskilt i ljuset av en snabbt föränderlig hotbild där teknikutvecklingen innebär att målet för cybersäkerhet kontinuerligt förskjuts**.

Vinnova framhåller vikten av att regelverk, stödstrukturer och gemensamma europeiska initiativ utformas på ett proportionerligt och flexibelt sätt, så att de stödjer experiment, piloter samt test- och demomiljöer även i tidiga forsknings- och innovationsfaser. Detta är särskilt betydelsefullt för små och medelstora företag, startups och aktörer inom framväxande teknikområden, som utgör centrala drivkrafter för Europas långsiktiga innovations- och konkurrenskraft.

Sammanfattningsvis anser Vinnova att cybersäkerhetspaketet kan bidra till både ökad säkerhet och stärkt innovationsförmåga i Europa, under förutsättning att genomförandet sker med ett sektorsövergripande och systemorienterat angreppssätt där innovation, forskning och näringslivets utvecklingsförutsättningar integreras från början.

Vinnovas ställningstaganden

Testverktyg och testinfrastruktur för cybersäkerhet

Avsnittet behandlar förslagen om att Europeiska unionens cybersäkerhetsbyrå (ENISA) ska kunna tillhandahålla tekniska testverktyg för konformitetsbedömning samt stödja företag, inklusive små och medelstora företag, i frågor som rör test och utvärdering av cybersäkerhet (COM(2026) 11, s. 33).

Vinnova välkomnar att kommissionens förslag uppmärksammar betydelsen av testverktyg och testinfrastruktur inom cybersäkerhet. Vinnova vill särskilt betona vikten av att test- och demomiljöer utformas så att de är lättillgängliga och möjliga att använda med låga trösklar i tidiga forsknings- och innovationsfaser, inklusive för svensk industri.

Skälen för ställningstagandet:
Test och demonstration är avgörande för att kunna utveckla, verifiera och utvärdera nya cybersäkerhetslösningar. Ur ett forsknings- och innovationsperspektiv är det därför positivt att gemensamma testverktyg och testmiljöer lyfts fram i förslagen. Samtidigt visar erfarenheter att test- och

Vinnova
Sveriges innovationsmyndighet

Besöksadress:
Mäster Samuelstgatan 56,
101 58 Stockholm
Telefon: 08 473 30 00
www.vinnova.se

Fakturaadress:
Vinnova, FE 34, 838 73 Frösön
Levaransadress:
Klara Norra Kyrkogata 14, 101 58 Stockholm
Organisationsnummer: 202100-521

demomiljöer inte sällan är tekniskt och organisatoriskt tungrodda, vilket gör insteget kostsamt och förlänger tiden till att relevanta lösningar kan testas i praktiken.

Vinnova vill framhålla att detta särskilt påverkar innovationsförmågan hos SMF och industrin, där behovet av att snabbt kunna testa och demonstrera lösningar i realistiska miljöer är centralt. Test- och demomiljöer behöver därför möjliggöra snabb, flexibel och kostnadseffektiv användning, inte enbart för efterlevnad och certifiering utan även för experiment, piloter och utveckling i tidiga skeden. **För att testinfrastruktur fullt ut ska bidra till innovation och stärkt cybersäkerhet är det därför viktigt att fokus även ligger på tillgänglighet, vidareutveckling och sänkta trösklar för användning.**

Kompetensförsörjning inom cybersäkerhet

Avsnittet behandlar förslagen om ett europeiskt ramverk för cybersäkerhetskompetenser (European Cybersecurity Skills Framework) samt förslaget om europeiska system för individuella cybersäkerhetsattesteringar (COM(2026) 11, s. 33–35 samt artiklarna 198–201).

Vinnova ställer sig i huvudsak positiv till förslagen om att stärka kompetensförsörjningen inom cybersäkerhet genom ett gemensamt europeiskt ramverk för kompetenser och färdigheter (ECSF) samt genom europeiska system för individuella cybersäkerhetsattesteringar. Vinnova betonar att dessa initiativ behöver utformas så att de stödjer ett öppet och innovationsdrivet europeiskt innovationssystem, med särskild hänsyn till små och medelstora företag (SMF), startups, industrin samt akademi- och forskningsaktörer.

Skälen för ställningstagande:
Kompetensförsörjning inom cybersäkerhet är en central förutsättning för att stärka innovationsförmåga, konkurrenskraft och motståndskraft i Europa. Vinnovas erfarenheter från finansiering av forskning och innovationsprojekt visar att brist på relevant och tillgänglig kompetens utgör ett återkommande hinder för såväl utveckling som implementering av nya lösningar, särskilt i projekt där akademi, näringsliv och offentliga aktörer samverkar.

Vinnova bedömer att ECSF kan bidra till ökad transparens och samsyn kring roller, kompetenser och färdigheter inom cybersäkerhet. Ett gemensamt språk och gemensamma referensramar kan underlätta samverkan mellan utbildningsaktörer, forskningsmiljöer och näringsliv samt stödja utvecklingen av relevanta utbildningar och insatser för livslångt lärande. För innovationssystemet är det dock avgörande att ramverket tillämpas med tillräcklig flexibilitet för att även omfatta tvärdisciplinära och föränderliga kompetensbehov.

När det gäller individuella cybersäkerhetsattesteringar ser Vinnova potentiella nyttor, men anser att sådana system måste vara frivilliga och proportionerliga samt inte utformas så att de skapar trösklar för deltagande i forskning och innovation. **Det är särskilt viktigt att attesteringar inte utvecklas till informella inträdeskrav för medverkan i forsknings- och innovationsprojekt**.

Regulatoriska sandlådor (regulatory sandboxes)

Avsnittet behandlar förslagen i COM(2026) 11 (Cybersecurity Act 2) om att stärka ENISA:s kapacitet, inklusive tekniskt stöd till medlemsstaterna, för etablering och drift av regulatoriska sandlådor i syfte att möjliggöra experiment, piloter och innovation i en kontrollerad regulatorisk miljö (jfr artikel om kapacitetsuppbyggnad, s. 70).

Vinnova välkomnar förslaget i COM(2026) 11 att stärka ENISA:s kapacitet att ge tekniskt stöd till medlemsstaterna för etablering och drift av regulatoriska sandlådor inom cybersäkerhet. Vinnova bedömer att regulatoriska sandlådor är ett viktigt instrument för att möjliggöra experiment, piloter och innovation i en kontrollerad regulatorisk miljö, i linje med målen om stärkt cybersäkerhet och europeisk konkurrenskraft. Det är även viktigt att dessa sandlådor snabbt kan anpassas och förändras för att säkerställa kontinuerlig relevans mot marknaden givet cybersäkerhetsområdet föränderliga verklighet.

Skälen för ställningstagandet:
Regulatoriska sandlådor skapar utrymme för kontrollerad testning av nya cybersäkerhetslösningar, tjänster och arbetssätt i verklig miljö, samtidigt som rättssäkerhet och säkerhet upprätthålls. Detta är särskilt relevant inom cybersäkerhetsområdet, där teknikutvecklingen är snabb och regelverken ofta komplexa och sektorsövergripande.

Vinnova bedömer att ENISA:s roll i kapacitetsuppbyggnad är central för att säkerställa likvärdiga förutsättningar mellan medlemsstater och för att sänka trösklarna för deltagande, särskilt för små och medelstora företag, startups och forskningsaktörer.

- **För att sandlådor ska få full innovationspolitisk effekt är det viktigt att de utformas så att de kan användas även i tidiga forsknings- och innovationsfaser och inte enbart för efterlevnad eller certifiering.**

- **Vinnova ser vidare ett behov av tydlig nationell organisering och strukturer för systematiskt lärande, så att erfarenheter från regulatoriska sandlådor kan tas tillvara och bidra till långsiktig regel- och policyutveckling inom cybersäkerhetsområdet.**

- **För att maximera nyttan bör erfarenheter från sandlådor systematiskt återföras inte enbart till nationell policyutveckling utan även till EU-nivån, i syfte att bidra till mer sammanhängande och ändamålsenlig regelutveckling. Detta är särskilt angeläget i ljuset av att närliggande regelområden, såsom cybersäkerhet och artificiell intelligens, i praktiken samverkar men ofta utvecklas i parallella processer. En stärkt horisontell kunskapsöverföring, exempelvis i relation till genomförandet av AI-förordningen, kan därmed bidra till att motverka fragmentering och skapa mer innovationsfrämjande och koherenta regelverk inom EU.**

Ransomware-data och incidentinformation

Avsnittet behandlar förslagen om harmoniserad insamling av ransomware-relaterad data inom EU, inklusive närmare specifikation av vilken incidentinformation som ska rapporteras samt hur denna information ska struktureras och delas mellan behöriga myndigheter, i syfte att stärka lägesbild, analys och samordning (COM(2026) 13 – Direktiv om harmoniserad insamling av ransomware-data och specificering av vilken information som ska rapporteras, s. 9–11 och 13–14).

Vinnova välkomnar förslagen om harmoniserad insamling av ransomware-data och tydligare specificering av incidentinformation. Ur Vinnovas perspektiv är detta ett viktigt steg för att stärka kunskapsuppbyggnad, analys samt forskning och innovation inom cybersäkerhetsområdet i Europa.

Skälen för ställningstagandet
Harmoniserad insamling av ransomware-data skapar ett jämförbart och sammanhållet kunskapsunderlag på EU-nivå, vilket är en viktig förutsättning för förbättrad analys av hotbilden och för utveckling av effektiva cybersäkerhetslösningar.

Vinnova
Sveriges innovationsmyndighet

Besöksadress:
Mäster Samuelstgatan 56,
101 58 Stockholm

Telefon: 08 473 30 00

www.vinnova.se

Fakturaadress:
Vinnova, FE 34, 838 73 Frösön

Levaransadress:
Klara Norra Kyrkogata 14, 101 58 Stockholm

Organisationsnummer: 202100-521

Ur ett forsknings- och innovationsperspektiv möjliggör tillgång till strukturerade och kvalitativa incidentdata avancerad analys samt utveckling av nya metoder och verktyg. Särskilt värdefullt är om data, i aggregerad eller anonymiserad form och med fullt beaktande av säkerhet och sekretess, kan göras relativt enkelt tillgänglig för forskning och innovation. Samtidigt är det viktigt att detta sker utan att ytterligare rapporteringskrav åläggs företagen.

Nya krav bör utformas så att de inte skapar onödig administrativ trögrörlighet eller byråkrati för sakens skull, eller riskerar att hämma innovation, nytänkande och tekniska paradigmskiften. Standardiserade format, tydlig vägledning samt möjligheter till automatiserad rapportering är viktiga verktyg för att säkerställa hög datakvalitet och god rapporteringsgrad, utan att varje enskild åtgärd bidrar till att bromsa utvecklingstakten.

- **Det är därför avgörande att rapporteringskraven är proportionerliga, ändamålsenliga och tydliga, särskilt för små och medelstora företag.**

I detta ärende har generaldirektör Darja Isaksson beslutat. Programledaren Frédéric Pillot har varit föredragande. I den slutliga handläggningen har också handläggare Johan Lindberg, Åsa Moum, Erik Borälv, och Göran Marklund deltagit.

Darja Isaksson

Vinnova
Sveriges innovationsmyndighet

Besöksadress:
Mäster Samuelstgatan 56,
101 58 Stockholm

Telefon: 08 473 30 00

www.vinnova.se

Fakturaadress:
Vinnova, FE 34, 838 73 Frösön

Levaransadress:
Klara Norra Kyrkogata 14, 101 58 Stockholm

Organisationsnummer: 202100-521