TechSverige

Datum
2026-04-22

Vår referens
FSD

Finansdepartementet
fi.remissvar@regeringskansliet.se

Remissvar avseende betänkandet Kompletterande bestämmelser till EU:s cyberresiliensförordning (SOU 2025:115)

TechSverige har givits möjlighet att avge remissvar avseende betänkandet Kompletterande bestämmelser till EU:s cyberresiliensförordning (SOU 2025:115) med dnr Fi2026/00065.

TechSverige är en bransch- och arbetsgivarorganisation för alla företag inom tech-sektorn. TechSveriges uppdrag är att tillsammans med medlemmarna skapa bästa möjliga förutsättningar för en konkurrenskraftig svensk techbransch som driver innovation och utveckling i hela samhället. TechSverige samlar cirka 1 400 företag – som sammantaget har närmare 100 000 medarbetare i Sverige. Bland dessa finns allt från startupföretag till multinationella bolag.

Sammanfattning

TechSverige

- påminner om behovet av en informationssäkerhetspolitik där staten
    - skapar goda villkor för cybersäkerhetsföretag
    - lämnar bidrag där den verkligen kan bidra, som till exempel kompetensförsörjning och brottsbekämpning
- tillstyrker utredningens skrivningar om sekretess, tystnadsplikt och regulatoriska sandlådor
- efterfrågar samordning med övriga cybersäkerhetsregleringar
- efterfrågar gemensam rapportering för samma cyberincident
- tillstyrker utredningens förslag om stödåtgärder till företag
    - om de inte stör privata aktörernas möjligheter
    - ser en risk att stödåtgärdernas betydelse överskattas i förhållande till de faktiska utmaningar som små och medelstora företag står inför.

Utveckla informationssäkerhetspolitiken

Staten bör bidra till goda villkor för cybersäkerhets företag där dess roll är särskilt betydelsefull.

De säkerhetsbrister eller svagheter som i dag finns inom cyberområdet beror i de allra flesta fall inte på brister i förmågor hos leverantörer av cybersäkerhetstjänster. Därav följer att det mest angelägna är att lyfta finansiering, mognad och kompetens på kundsidan.

Den svenska cybersäkerhetsmarkanden omsätter ca 16 mdkr om året – med i vissa fall världsledande företag. I ljuset av det har betydelsen av statliga satsningar och regleringar begränsningar. Det viktigaste staten kan göra är att skapa goda möjligheter för fler och växande cybersäkerhetsföretag som kan bistå kunder i privat och offentlig sektor.

Detta är en större fråga i informationssäkerhetspolitiken. Staten bör vidta ytterligare åtgärder för att minska kompetensbristen inom informations- och cybersäkerhetsområdet. Inom det området och till exempel brottsbekämpning har staten särskilda roller som inte privata aktörer har samma möjligheter att påverka.

Sekretess och tystnadsplikt

TechSverige tillstyrker införande av sekretess i enlighet med CRA artikel 14 och 15 samt förslaget om tystnadsplikt för att inte röja eller utnyttja information om affärs- eller driftförhållanden.

Regulatoriska sandlådor och testmöjligheter

TechSverige välkomnar möjligheten att använda regulatoriska sandlådor som ett verktyg för att främja innovation och samtidigt säkerställa regelefterlevnad.

Sandlådorna bör kompletteras med testmöjligheter under verkliga förhållanden, särskilt vid utveckling och införande av mer komplexa produkter och system. Mot denna bakgrund är det positivt att ansvariga myndigheter ges utrymme att vidareutveckla och anpassa sådana verktyg i nära dialog med näringslivet. En praktisk och flexibel tillämpning är avgörande för att sandlådor och testmiljöer ska utgöra ett verkligt stöd och inte medföra onödiga administrativa bördor.

Incidentrapportering och tillsyn

Det är av stor vikt för näringslivet att tillsynsprocesser och rapporteringskrav samordnas för att undvika parallella granskningar av samma förhållanden eller incidenter.

Detta gäller tillsyn enligt EU:s cyberresiliensförordning (CRA), cybersäkerhetslagen (NIS2), säkerhetsskyddslagstiftningen, GDPR, förordningen om digital operativ motståndskraft (DORA), eIDAS-förordningen och CER-direktivet.

Det skulle kunna uppstå en situation där ett fysiskt intrång eller olycka sker i energisektorn (CER) och leder till cyberintrång hos tjänsten (NIS2), ska incidenten rapporteras enligt dessa två regelverk. Vidare, om intrånget möjliggjordes genom en offentligt känd utnyttjad sårbarhet i en produkt integrerad i systemet ska en rapport om detta också göras enligt CRA till tillverkaren. Har dessutom personuppgifter läckt måste enheten rapportera enligt GDPR. Till detta ska även nationella regler läggas, som säkerhetsskyddslagen.

I det fortsatta arbetet bör prioriteringen vara en ytterligare harmonisering av de centrala rapporteringsskyldigheterna, med utgångspunkt i exempel från DORA och NIS2, som ett led i att förenkla rapporteringen.

En ytterligare observation kan vara att för höga och komplicerade krav på rapportering kan leda till minskad rapportering av incidenter.

TechSverige efterfrågar förenkling genom en väg in och med en tydlig instruktion om att en rapport om en betydande incident räcker.

Sverige borde kunna ta ett första steg och införa en gemensam incidentrapporteringsportal där samtliga ovan nämnda regleringar ingår på åtminstone det sätt som Danmark och Luxemburg redan genomfört. De överlappande rapporteringsskyldigheterna innebär onödiga ekonomiska och administrativa bördor.

I väntan på en väg in för incidentrapportering finns behov av ytterligare förtydliganden kring hur rapporteringskraven enligt cyberresiliensförordningen ska förhålla sig till befintliga incidentrapporteringskrav enligt den svenska cybersäkerhetslagen.

Vidare bör det beaktas att svenska företag kan ha krav att lämna rapporter som inte ska lämnas vidare från i svenska myndigheter. Det kan också finnas situationer där det inte är uppenbart i ett första läge. Dessa förhållanden bör ligga till grund för hur en mer samlad rapportering utformas och i vilken ordning rapporter ska delas mellan svenska och europeiska myndigheter.

Den tekniska lösningen och behandlingen av rapporter måste utformas på ett sätt som inte leder till försvagad cybersäkerhet och motståndskraft, och som inte riskerar att äventyra den information som företag lämnar.

Stöd till företag

Förslagen i betänkandet om stöd till företag i samband med genomförandet av CRA är i grunden positiv. Särskilt välkomnas fokus på vägledning, samordning mellan myndigheter och tidiga stödinsatser till företag – så länge det inte leder till otillbörlig konkurrens med till exempel säkerhetsföretag eller andra som kan bistå på marknadsmässiga grunder.

TechSverige ser en risk att stödåtgärdernas betydelse överskattas i förhållande till de faktiska utmaningar som små och medelstora företag står inför. För dessa företag är det inte i första hand brist på stöd som utgör hindret, utan de ökade kostnader, den administrativa börda och den komplexitet som följer av regelverket.

Stödåtgärder kan vara ett viktigt komplement, men kan inte ersätta behovet av förenklade regler, minskad administrativ belastning och krav som är anpassade efter mindre företags förutsättningar. Än mindre kan det ersätta goda villkor för den svenska cybersäkerhetsmarknaden som kommer att vara helt nödvändiga för att höja informations- och cybersäkerheten i Sverige.

För TechSverige

Christina Ramm-Ericson
näringspolitisk chef

Fredrik Sand
näringspolitisk expert