Kontaktperson RISE | Datum | Beteckning | Sida

Shahid Raza | 2021-01-25 | Remissyttrande SOU 2020:58 | 1 (4)

shahid.raza@ri.se
076-883 17 97

Remissyttrande från RISE avseende EU:s cybersäkerhetsakt – kompletterande nationella bestämmelser om cybersäkerhetscertifiering, SOU 2020:58

RISE är ett statligt ägt forskningsinstitut. Våra 2800 medarbetare driver och stöder alla typer av innovationsprocesser och erbjuder expertis och ett 120-tal test- och demonstrationsmiljöer. Inom IT-området arbetar RISE med bland annat elektronik, informations- och kommunikationsteknik samt mjukvaruutveckling, mobilitet, systemanalys och interaktionsdesign, cybersäkerhet och artificiell intelligens. RISE bedriver idag certifieringsverksamhet inom flera områden, bl.a. avseende kontrollenheter för kassaapparater, säkra transporter, ledningssystem för informationssäkerhet (ISO/IEC 27001) och produkter kopplade till maskindirektivet.

Det är RISE bedömning att vi som organisation kan spela en viktig roll när olika certifieringsordningar framöver implementeras inom ramen för den europeiska cybersäkerhetsakten.

RISE ser en möjlighet att då agera i olika roller:

- som organ för bedömning av överensstämmelse på de två lägre assuransnivåerna.
- som organ för bedömning av överensstämmelse på den högsta assuransnivån, om delegering för detta erhålls.
- som utvärderare/granskare genom nyttjande av RISE testlaboratorier, på alla tre assuransnivåerna.

I beredningen av detta ärende har Shahid Raza, Mikael Hägglöf, Dag Sjöholm, Pierre Kleberger, Ted Strandberg, Tomas Holm, Martin Bergling, Joakim Jakobsson och Anders Berntson deltagit.

Sammanfattande kommentar

RISE ställer sig bakom utredningen, och tillstyrker därmed utredningens olika förslag.

Några kommentarer följer nedan.

Kommentarer kring frågeställningar i delbetänkandet

7.4.2 Utfärdande och innehav av europeiska cybersäkerhetscertifikat

RISE ser en möjlighet att ta en roll på högsta assuransnivån

Utredningen konstaterar att den högsta assuransnivån ska motsvara höga eller mycket högt ställda krav på cybersäkerhet och som kan antas komma att användas i bl.a. industriella, samhällsviktiga och säkerhetskänsliga verksamhet.

Det kan också konstateras att FMV och FMV/CSEC har lång erfarenhet av säkerhetskänsliga och försvarsanknutna IKT-lösningar.

Utredningen pekar på möjligheten att den nationella myndigheten för cybersäkerhetscertifiering kan besluta om en delegering avseende rätten att utfärda ett cybersäkerhetscertifikat på högsta assuransnivån till ett fristående organ för bedömning av överensstämmelse.

- RISE anser att det finns en möjlighet att RISE här kan ta en viktig roll som organ för bedömning av överensstämmelse, även på den högsta assuransnivån, bland annat avseende IKT-lösningar inom industriella och/eller samhällsviktiga och verksamheter.

Avsnitt 8.3 Nationell myndighet för cybersäkerhetscertifiering

Minimera risker vid FMV:s kontroll av egen verksamhet

Utredningen föreslår att FMV utses till nationell myndighet för cybersäkerhetscertifiering. FMV får därmed ansvar för kontroll och övervakning enligt artikel 58 (tillsyn) som marknadsövervakningsmyndighet, vilket även avser verksamhet som bedrivs av organ för bedömning av överensstämmelse i enlighet med förordningen. Detta innebär tillsynsansvar även över FMV:s egen enhet FMV/CSEC.

- RISE ser risker i att FMV ska utföra kontroll och övervakning av egen organisatorisk enhet FMV/CSEC. RISE vill betona vikten av att minimera de risker som kan uppstå vid kontroll av egen verksamhet, i syfte att säkerställa tilltro till det svenska certifieringssystemet.

Avsnitt 8.3.1 Förslag på nationell myndighet för cybersäkerhetscertifiering

FMV:s ansvar för att bedöma marknadsutvecklingen

Utredningen konstaterar att det inte går att bedöma efterfrågan på marknaden för de föreslagna certifieringsordningarna eller tillhörande assuransnivåer. Utredningen föreslår att de organisatoriska och resursmässiga konsekvenserna bör tas upp till ny bedömning när omfattningen och resursbehovet av certifieringsverksamheten närmare kan bedömas utan att precisera hur detta ska ske.

- RISE anser att det inte är en tillfredställande slutsats från utredningen att FMV:s förmåga att möta en framtida utveckling inom cybersäkerhetscertifiering lämnas till framtida bedömning. Det kan leda till att åtgärder sker för sent samt skada svensk företagsutveckling och konkurrenskraft.

- RISE anser att det finns behov att förtydliga vilket ansvar FMV har för att i god tid tillgodose marknadsutveckling inom nya certifieringsordningar och assuransnivåer. En plan, inklusive finansiering, bör i tidigt skede finnas för att kunna skala upp kompetens och den egna verksamheten i takt med efterfrågan inom olika certifieringsordningar. Alternativt att en kompletterande lösning med andra ackrediterade organ tas fram och tydliggörs. Avsaknad av tillräcklig kapacitet hos ackrediterade organ kan leda till att svenska företag missgynnas gentemot andra EU länder pga. långa ledtider eller obefintlig nationell marknad inom vissa områden och/eller assuransnivåer. Det är särskilt problematiskt om certifieringsordningar, som kan bli obligatoriska inom EU, inte vid behov finns tillgängliga via nationellt ackrediterade organ för svenska företag på grund av brist på bedömning av resursmässiga och organisatoriska konsekvenser.

FMV:s ansvar för att tillhandahålla certifiering inom de lägre assuransnivåerna

Utredningens förslag till FMV och CSEC roll baseras på att de redan anses ha en bred och djup kunskap om cybersäkerhetscertifiering samt lång erfarenhet av både omvärldsbevakning av dessa frågor samt internationell och nationell samverkan med andra berörda aktörer på området. Fokus för både FMV och CSEC har historiskt legat på att certifiera IKT-produkter kopplat till försvar och Sveriges säkerhet.

- RISE anser att det finns behov att tydliggöra vilket ansvar FMV har för, att via ackrediterade organ, tillhandahålla certifiering inom cybersäkerhet för områden som inte är relaterade till högsta assuransnivå eller Sveriges säkerhet. Exempelvis den föreslagna certifieringsordningen för molntjänster är av horisontell karaktär som omfattar alla typer av molntjänster och assuransnivåer. Fler certifieringsordningar väntas komma inom andra områden som i vissa fall ligger långt utanför FMV:s primära intresseområden, men som kan efterfrågas ur ett marknadsperspektiv. Exempel på sådana områden kan vara molntjänster för uppkopplade smarta hem eller fordon i lägre assuransnivåer.

Svensk kompetensbrist kontra brett framtida kompetensbehov

Utredningen konstaterar att det finns en global kompetensbrist inom cybersäkerhet. Detta gäller även Sverige.

FMV och FMV/CSEC har mångårig erfarenhet av certifiering av IKT-produkter inom cybersäkerhetsområdet, men inom ramen för den nya cybersäkerhetsakten kommer många nya typer av IKT-produkter, -tjänster och -processer att vara aktuella. Det kan därför bli svårt för FMV att kompetensmässigt täcka alla de nya certifieringsområden som förväntas implementeras framöver.

- RISE anser att det behövs en ökad nationell samverkan mellan olika typer av aktörer för att på bästa sätt tillgodose behovet av kompetens för olika typer av certifieringar. Här kan det krävas både agila marknadsaktörer och kompetenser på olika nivåer, beroende på vilken assuransnivå som är aktuell.
- RISE har många medarbetare, vilka tillsammans har en både bred och djup kompetens inom många olika IKT-områden – exempelvis 5G, AI/maskininlärning, Internet of Things och molntjänster. RISE ser denna expertis som en mycket viktig kompetensresurs att tillvarata i det fortsatta införandet av cybersäkerhetsakten.

2.4 Definitioner och avgränsning

Olika betydelser av begreppet cybersäkerhet

Utredningen ger en bra redovisning av hur begreppet cybersäkerhet idag definieras i olika sammanhang, och konstaterar därmed också att begreppet cybersäkerhet inte har en enhetlig och fastställd definition.

Det pågår ett arbete inom SIS och MSB avseende en revidering av ”SIS-TR50:2015 Terminologi för informationssäkerhet”, i syfte att skapa en nationell terminologi. Där avses uppdaterade definitioner ges bl.a. för begreppet cybersäkerhet.

- RISE konstaterar att olika terminologier inom informations- och cybersäkerhetsområdet idag inte är samstämmiga. Samtidigt är en gemensam terminologi viktig inom alla teknikområden, inte minst inom områden där det sker en snabb utveckling, såsom sker inom området cybersäkerhet.
- RISE vill därför påpeka vikten av att utredningen i det fortsatta arbetet fortsätter vara uppmärksam på denna problematik.