INTERNET STIFTELSEN

Fö2020/00954

Internetstiftelsens remissvar på EU:s cybersäkerhetsakt – kompletterande nationella bestämmelser om cybersäkerhetscertifiering (SOU 2020:58)

Om Internetstiftelsen

Internetstiftelsen är en oberoende, affärsdriven och allmännyttig organisation. Vi verkar för ett internet som bidrar positivt till människan och samhället.

Vi är en stiftelse och vår urkund slår fast att vi ska säkerställa en stark och säker infrastruktur för internet som tillgodoser dagens och framtidens behov i Sverige samt främja forskning, utbildning och undervisning med inriktning på internet. Vi ansvarar för internets svenska toppdomän .se och sköter även drift och administration av toppdomänen .nu. Intäkterna från affärsverksamheten finansierar en rad satsningar i syfte att möjliggöra att människor kan nyttja internet på bästa sätt och att ge kunskap om internetanvändningen i Sverige samt digitaliseringens påverkan på samhället. Vi tillhandahåller evenemang och utbildningsinsatser som gör det enklare att förstå och använda internets tjänster och som bidrar till ökad kompetens och fler möten som främjar internetinnovation. Vi stöttar även olika fristående uppdrags- och forskningsprojekt som på olika sätt gynnar internets utveckling och ger förutsättningar för internetentreprenörer och utvecklare att ta steget från idéstadie till färdig produkt eller tjänst. Med våra identitetsfederationer förenklar vi inloggning och höjer säkerheten i identitets- och kontohantering för både användare och leverantörer av olika tjänster inom skola, hälso- och sjukvård.

Internetstiftelsen har blivit tillfrågade att lämna remissvar på EU:s cybersäkerhetsakt – kompletterande nationella bestämmelser om cybersäkerhetscertifiering (SOU 2020:58). Remissvaret är avgränsat till avsnitt 8.3 Nationell myndighet för cybersäkerhetscertifiering och avsnitt 8.4.3 Nationell myndighet med ansvar för tillsyn.

Övergripande synpunkter

Internetstiftelsen lämnar inga övergripande synpunkter på delbetänkandet och om förslag om kompletterande lagstiftning. Vi har däremot valt att lyfta fram synpunkter på de organisatoriska frågorna.

Avsnitt 8.3 Nationell myndighet för cybersäkerhetscertifiering

Utredningen föreslår att Försvarets materielverk (FMV) ska utses till nationell myndighet för cybersäkerhetscertifiering och att myndighetens certifieringsorgan ska vara nationell myndighet för cybersäkerhetscertifiering enligt artikel 56.5 a och 56.6 i EU:s

cybersäkerhetsakt. Myndigheten ska i sin verksamhet beakta nationella säkerhetsintressen vid tillämpningen av EU:s cybersäkerhetsakt.

Internetstiftelsen konstaterar att uppgifter och ansvar inom informations- och cybersäkerhetsområdet är idag fördelade på flera (för många) myndigheter inom olika samhällssektorer, bland annat gäller det NIS-direktivets tillämpningsområde och verksamheter som omfattas av regleringen om säkerhetsskydd. Utredningen har tolkat direktivens anvisning att förslag till nationell myndighet för cybersäkerhetscertifiering ska utgå från en befintlig myndighet, och att de olika uppgifter, roller och ansvarsområden som enligt cybersäkerhetsakten ska finnas på nationell nivå i och för sig kan fördelas på en eller flera befintliga myndigheter om det är mer ändamålsenligt och effektivt med en sådan lösning.

FMV:s huvuduppdrag och kärnverksamhet är att upphandla varor och tjänster för Försvarsmaktens behov. Det innebär enligt Internetstiftelsens uppfattning att man är i princip att betrakta som beställare/användare i sammanhanget.

Sveriges Certifieringsorgan för IT-säkerhet, CSEC, är en oberoende enhet inom FMV och verkar som Sveriges nationella certifieringsorgan för IT-säkerhet i produkter och system, enligt standarden Common Criteria, CC. CSEC ackrediterades som nationellt certieringsorgan år 2008. FMV/CSEC har således mångårig erfarenhet av certifiering inom informations- och cybersäkerhetsområdet och är idag organiserat inom myndigheten för att möta de krav på oberoende som gäller för ett ackrediterat organ för bedömning. Det är mot bakgrund av att CSEC finns på FMV som man lagt förslaget om att det är FMV som ska vara nationell myndighet för cybersäkerhetscertifiering.

Internetstiftelsen konstaterar att regeringen den 19 november 2009 beslutade att tillkalla en särskild utredare med uppdrag att utreda formerna för och konsekvenserna av att flytta ansvaret för dels Sveriges IT-incidentcentrum (Sitic) från Post- och telestyrelsen (PTS), dels Sveriges certifieringsorgan för IT-säkerhet (CSEC) från Försvarets materielverk (FMV). Utredaren skulle undersöka vilken myndighet av Försvarets radioanstalt (FRA) och Myndigheten för samhällsskydd och beredskap (MSB) som bedömdes bäst lämpad att vara ansvarig utifrån de behov och målsättningar som regeringen angett när det gällde att bland annat samla informationssäkerhetsfrågorna. Utredaren skulle också föreslå en myndighet att vara signatär för både CCRA (Common Criteria Recognition Arrangement) och SOGIS-MRA (Senior Officials Group Information Systems Security – Mutual Recognition Agreement) (SOU 2010:25).

Utredaren föreslog då att CSEC tills vidare skulle vara kvar som en organisatorisk enhet inom FMV. Utredarens bedömning var att det saknades goda skäl att flytta CSEC. Verksamheten vid CSEC och placeringen vid FMV fungerade väl, men att lokaliseringen av CSEC på längre sikt bör övervägas i anslutning till det av regeringen aviserade fortsatta arbetet med anledning av Stödutredningens rapport: Ett användbart och tillgängligt försvar – Stödet till Försvarsmakten, och att det vid framtida

överväganden om lokalisering av CSEC bör säkerställas att det finns en långsiktig och hållbar lösning som tillgodoser högt ställda krav på oberoende, säkerhet och effektivitet. Några förslag rörande lokalisering av CSEC presenterades såvitt Internetstiftelsen kan se inte från utredningen. (Rapport från Stödutredningen Fö 2009:A).

Med utredningens förslag att FMV ska vara nationell myndighet för cybersäkerhetscertifiering uppkommer även frågan om CSEC, som alltså i dag är en organisatorisk enhet inom myndigheten FMV, har en sådan organisatorisk ställning och arbetsformer att dessa möter de krav som följer av cybersäkerhetsaktens reglering av ackrediterade organ för bedömning av överensstämmelse för bedömning. Det finns en uppenbar risk för intressekonflikt mellan FMV som användare och FMV som certifieringsorgan. Mot bakgrund av att CSEC har existerat inom FMV under så många år, och att det enligt Internetstiftelsens bedömning fungerat väl så är Internetstiftelsens uppfattning ändå att den ordningen kan fortsätta att råda.

Avsnitt 8.4.3 Nationell myndighet med ansvar för tillsyn

Cybersäkerhetsakten anger också att en tillsynsverksamhet ska finnas på nationell nivå i en medlemsstat. Utredningen lämnar därför förslag om hur den nationella tillsynen ska organiseras för att möta framtida behov av tillsyn med anledning av de europeiska ordningar som kan komma att antas på området. Utredningen bedömer att cybersäkerhetsaktens olika bestämmelser om tillsyn ger utrymme för att med en tillräcklig grad av säkerhet redan vid denna tidpunkt kunna lämna förslag om hur den nationella tillsynsverksamheten bör organiseras och utformas.

Utredningen anser att det finns följande möjliga alternativ för hur ansvaret att lösa de angivna uppgifterna kan organiseras.

1. En och samma myndighet får i uppdrag att vara nationell myndighet för cybersäkerhetscertifiering och att etablera tillsynsfunktionen.
2. En myndighet får i uppdrag att vara nationell myndighet för cybersäkerhetscertifiering och en annan fristående myndighet får i uppdrag att ansvara för den nationella tillsynsfunktionen.
3. En ansvarig sektorsmyndighet får uppdraget att inom sin sektor vara nationell myndighet för cybersäkerhetscertifiering och även ansvara för myndighetens tillsynsfunktion inom sektorn.

Utredningen har valt att lägga fram alternativ 1 som utredningens förslag, det vill säga att FMV ska få rollen både som nationell myndighet för cybersäkerhetscertifiering OCH att etablera tillsynsfunktionen.

Enligt den s.k. Tillsynsutredningens betänkande SOU 2004:100 definieras tillsyn som “oberoende och självständig granskning av tillsynsobjekt som syftar till att kontrollera om tillsynsobjektet uppfyller de krav och villkor som följer av lag, EG-förordning eller annan föreskrift och av särskilda villkor som har meddelats i anslutning till sådana föreskrifter samt beslut om åtgärder som syftar till att vid behov åstadkomma rättelse av den objektsansvarige”.

Internetstiftelsen anser att om det funnits oro för en intressekonflikt för FMV:s generaldirektör som dels beställare/användare, dels certifieringsorgan för IT-säkerhet så finns det än större anledning att vara orolig för det faktum att samma myndighet dessutom ska utöva tillsyn över området. Att samma organisation ska vara nationell myndighet för cybersäkerhetscertifiering och etablera tillsynsfunktionen är enligt Internetstiftelsen olämpligt genom att det riskerar att ytterligare späda på intressekonflikten.

Den organisatoriska lösning som Sverige väljer för att uppfylla kraven i EU:s cybersäkerhetsakt måste inge förtroende, både nationellt och internationellt.

Det skapar enligt Internetstiftelsen mer trovärdighet och borgar för ett vidmakthållet oberoende för CSEC om tillsynsfunktionen läggs utanför FMV, till exempel på MSB.

Sammanfattning

Mot bakgrund av att CSEC har existerat inom FMV under så många år och att det enligt Internetstiftelsens bedömning fungerat väl så är Internetstiftelsens uppfattning att den ordningen kan fortsätta att råda och stödjer därmed utredningens förslag.

Internetstiftelsen delar däremot inte utredningens uppfattning om att tillsynsfunktionen läggs inom samma organisation (FMV). Det skapar enligt Internetstiftelsen mer trovärdighet och borgar för ett vidmakthållet oberoende för CSEC om tillsynsfunktionen läggs utanför FMV, till exempel på MSB.

Stockholm den 2021-01-20

Danny Aerts,

Vd, Internetstiftelsen