NATIONELLA BEHOV VID FRAMTAGANDET AV CERTIFIERINGSORDNINGAR ENLIGT EU:S CYBERSÄKERHETSAKT

FMV

Förord

Informations- och cybersäkerheten, generellt i samhället såväl som i säkerhetskänslig verksamhet, är beroende av säkerhetsegenskaper hos kommersiella produkter och tjänster som skulle kunna verifieras inom det europeiska ramverket för cybersäkerhetscertifiering.

Det finns betydande möjligheter att dra nytta av detta ramverk även för nationella ändamål när det gäller att stärka informations- och cybersäkerheten. Men detta är under förutsättning att myndigheter med expertis inom hot, sårbarheter och risker inom cyberområdet i förening med expertmyndigheten inom cybersäkerhets-certifiering samverkar avseende analys och kravställning som Sveriges behov av ökad säkerhet kan mötas och effekterna av samarbetet inom EU kan tillvaratas på ett ändamålsenligt och effektivt sätt.

Av denna anledning bör risk-, hot- och sårbarhetsanalyser för såväl samhället i allmänhet som de säkerhetskänsliga verksamheterna ingå i det analysarbete som sedan kan leda till de nationella krav som Sverige bör verka för att inarbeta i cybersäkerhetsaktens certifieringsordningar. Det är därför av största vikt att myndigheter med ansvar för både hot-, sårbarhets- och riskanalyser för samhället i allmänhet såväl som myndigheter med ansvar för säkerhetskänslig verksamhet ges i uppdrag att aktivt och kontinuerligt samverka i arbetet med att utveckla säkerhetskraven inom det europeiska ramverket för cybersäkerhetscertifiering.

Försvarets materielverk har fått i uppdrag av regeringen att analysera och lämna förslag på hur nationella behov i fråga om cybersäkerhet kan identifieras och omsättas till säkerhetskrav som Sverige bör framhålla i arbetet med att utveckla certifieringsordningar inom EU:s cybersäkerhetsakt.

Denna rapport utgör Försvarets materielverks redovisning av detta uppdrag med tillhörande förslag.

INNEHÅLLSREGISTER

Terminologi

Förkortningar

CA	Certification Authority
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CSA	Cybersecurity Act
CSEC	Sveriges certifieringsorgan för it-säkerhet
CERT	Computer Emergency Response Team
cPP	collaborative Protection Profile
CSIRT	Computer Security Incident Response Team
DIGG	Myndigheten för digital förvaltning
EAL	Evaluation Assurance Level
ECCG	Europeiska gruppen för cybersäkerhetscertifiering
ECSO	European Cyber Security Organisation
ENISA	European Union Agency for Cybersecurity
EU	Europeiska unionen
FIDI	Forum för informationsdelning om informationssäkerhet
FMV	Försvarets materielverk
FRA	Försvarets radioanstalt
ICC	Inspektionen för cybersäkerhetscertifiering
IKT	Informations- och kommunikationsteknik
MISWG	Multinational Industrial Security Working Group
MSB	Myndigheten för samhällsskydd och beredskap
MUST	Militära underrättelse- och säkerhetstjänsten
NCCA	National Cybersecurity Certification Authority
NCSA	National Communications Security Authority
NDA	National Distribution Authority
NLF	New Legislative Framework
PP	Protection Profile
PTS	Post- och telestyrelsen
SAMFI	Samverkansgruppen för informationssäkerhet

SIS	Svenska institutet för standarder
SOG-IS MRA	Senior Officials Group Information Systems Security – Mutual Recognition Agreement
SOU	Statens offentliga utredningar
Swedac	Styrelsen för ackreditering och teknisk kontroll
ST	Security Target

Centrala begrepp

Verksamhetsutövare:

Liksom i NIS2-utredningen[1] definieras i denna rapport verksamhetsutövare som juridisk eller fysisk person som bedriver verksamhet inom ett eller flera områden som omfattas av reglering. Detta kan, men behöver inte, sammanfalla med ”utövare av säkerhetskänslig verksamhet” enligt säkerhetsskyddslagen. Verksamhetsutövare är t.ex. privata företag som teleoperatörer, transportbolag och eldistributörer men omfattar också offentliga organ som bedriver den reglerade verksamheten.

Marknadskontroll och marknadskontrollmyndigheter:

Marknadskontroll innebär att ansvarig myndighet kontrollerar att produkter som finns på marknaden uppfyller gällande lagstiftning och att de är märkta och kontrollerade på föreskrivet sätt. Swedac är ansvarig myndighet för samordning av den svenska marknadskontrollen. Samordningen sker bland annat i Marknadskontrollrådet, där representanter från berörda myndigheter ingår. Marknadskontrollrådet, som i dagsläget består av 17 olika myndigheter.

Samordnande/stödjande myndighet:

Myndighet med roller, uppgifter, ansvar och befogenheter som gäller horisontellt för flera sektorer. Till exempel är Myndigheten för samhällsskydd och beredskap samordnande/stödjande myndighet för NIS-sektorerna medan Säkerhetspolisen och Försvarsmakten är det för säkerhetsskydd.

Sektorsmyndighet:

I denna rapport används begreppet sektorsmyndighet som en samlingsterm för de myndigheter som har föreskriftsrätt, tillsynsuppgifter eller är samordnande/stödjande myndighet inom en viss sektor. Detta inbegriper myndigheterna med olika uppgifter, ansvar och befogenheter enligt NIS-lagen. I begreppet sektorsmyndigheter avses i denna rapport även marknadskontroll- eller marknadsövervakningsmyndigheter[2]. I rapporten utgår vi ifrån att sektorsmyndigheterna motsvaras av de som benämns ”samverkansmyndigheter” i uppdraget till Försvarets materielverk.

[1] SOU 2024:18 Nya regler om cybersäkerhet.

[2] CSA art. 58.7.a. Sedan CSA:s tillkomst har reglerna om marknadsövervakning i Förordning (EG) nr 765/2008 ersatts av regler om marknadskontroll i Förordning (EU) 2019/1020 av den 20 juni 2019 om marknadskontroll […]. Därmed har begreppet övervakningsmyndigheter ersatts av marknadskontrollmyndigheter.

Standard:

Begreppet standard avser inom EU-rätten sådana dokument som utvecklats av erkända standardiseringsorgan under former som definierats enlig Europaparlamentets och rådets förordning (EU) nr 1025/20128 ”Bestämmelser för fastställandet av europeiska standarder och europeiska standardiseringsprodukter för produkter och tjänster till stöd för unionens lagstiftning och politik” som i sin tur är utformad i enlighet med Världshandelsorganisationens (WTO) avtal om tekniska handelshinder (TBT-avtalet[3]). I denna rapport används dock frekvent även ordet standard i en mer informell betydelse och kan då även avse andra tekniska specifikationer som utvecklats i mer eller mindre informella former av olika typer av s.k. de facto-standardiseringsorgan.

[3] Agreement on Technical Barriers to Trade (TBT Agreement)

Sammanfattning av förslaget

Det är en rad faktorer som påverkar hur nationella behov i fråga om cybersäkerhet kan identifieras och omsättas till säkerhetskrav som Sverige bör framhålla i arbetet med att utveckla certifieringsordningar inom EU:s cybersäkerhetsakt.

Det finns ett drygt tiotal EU-regleringar som refererar till cybercertifiering som ett sätt att visa uppfyllnad av krav på cybersäkerhetsegenskaper.

Genom både sådan EU-rätt och tillkommande nationell rätt, inklusive säkerhetsskyddslagstiftningen, styrs ansvar för cybersäkerhet genom ett stort antal sektorsmyndigheter och ett ännu mycket större antal verksamhetsutövare (offentliga såväl som privata).

Verksamhetsutövare ansvarar för att bedöma egna risker och vilka säkerhetsåtgärder som ska införas. Verksamhetsutövare behöver även tillämpa en genomtänkt, sammansatt strategi för vilka kontroller som ska genomföras av t.ex. ledningsystem för informationssäkerhet, nätverks- och informationssystem, systemarkitektur och ingående komponenter, driftövervakning och anlitade tjänster.

Det är en stor utmaning för både den stora gruppen sektorsmyndigheter och det ännu större antalet verksamhetsutövare att var och en etablera och upprätthålla nödvändig kompetens inom informations- och kommunikationsteknik (IKT), cybersäkerhet, risker för sårbarheter och attacker, effektiva säkerhetsåtgärder, effektiva kontrollmetoder och certifiering, samt förmåga att påverka relevanta standarder och certifieringsordningar.

En samlad nationell kompetens- och stödfunktion bör etableras inom staten. Denna ska ha en stark nationell förmåga för analys, samordning, proaktiv och tidig påverkan på utvecklingen av standarder och certifieringsordningar, samt ska kunna stödja sektorsmyndigheter och verksamhetsutövare inom cybersäkerhetsområdet.

Försvarets materielverk föreslår ingen förändring av sektorsmyndigheters och verksamhetsutövares ansvar enligt EU-rätt eller nationell rätt. Den föreslagna funktionen ska utgöra ett stöd till sektorsmyndigheter och verksamhetsutövare, som självständigt fortsatt bär ansvar för sina respektive uppdrag och verksamheter. Det är sektorsmyndigheters och verksamhetsutövares rättsliga ansvar och de behov som följer av detta som ska inrikta stödfunktionens verksamhet.

Stödfunktionen ska i samråd med sektorsmyndigheter utarbeta rekommenderade lösningar för säkerhetsbehov som finns inom en eller flera sektorer, samt i övrigt utgöra ett expertstöd till sektorsmyndigheter och verksamhetsutövare angående effektiva, genomförbara och kostnadseffektiva lösningar som kan adressera respektive sektors behov, avseende bl.a. produkter, arkitektur, drift, tjänster, underhåll, övervakning och kontrollmetoder (inkl. certifiering) samt därtill relaterade standarder. Stödfunktionen ska samverka med sektorsmyndigheterna och tillsammans med dessa bevaka eller proaktivt delta i eller påverka utvecklingen i relevanta standardiseringsorgan och certifieringsordningar.

Inom specifika teknik- eller sakområden, t.ex. kryptering, frågor som rör reglerad avlyssning (eng: ”legal intercept”) eller områden där en enskild sektorsmyndighet är

tongivande kan enskilda myndigheter få i uppdrag att samverka med stödfunktionen samt representera svenska intressen i relevanta organisationer, t.ex. standardiseringsorgan.

I det fall det beslutas att en s.k. Nationell modell för cybersäkerhet med tillhörande cybersäkerhetsnorm etableras, bör den kunna utgöra ett betydande stöd till både sektorsmyndigheter och verksamhetsutövare och tillhandahålla information om certifierade produkter, tjänster och processer och deras säkerhetsnivåer.

Försvarets materielverk förordar att stödfunktionen organiseras inom en redan existerande myndighet, eller inom en ny myndighet för cybersäkerhet, om en sådan etableras i enlighet med Försvarsberedningens förslag. De närmare formerna för stödfunktionens ansvar och uppgifter i relation till sektorsmyndigheterna bör närmare utredas.

Stödfunktionen föreslås vara anslagsfinansierad för sin huvuduppgift. Verksamheten föreslås utöver det kunna finansieras med avgifter för eventuellt tillhandahållet stöd till sektorsmyndigheter och verksamhetsutövare.

1 Inledning

1.1 Uppdraget

Europaparlamentets och rådets förordning (EU) 2019/881 om Europeiska unionens cybersäkerhetsbyrå (Enisa) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (cybersäkerhetsakten) antogs 2019.

Cybersäkerhetsakten etablerar ett ramverk genom vilket certifieringsordningar för cybersäkerhet i produkter och tjänster kan etableras. Certifiering enligt cybersäkerhetsakten är i sig frivillig för leverantörer, men kan göras bindande genom andra regleringar inom EU eller på nationell nivå. Det finns ett flertal andra EU-regleringar under utveckling där certifiering enligt cybersäkerhetsakten endera blir ett sätt att visa efterlevnad eller ett obligatoriskt krav (NIS2, eIDAS2, cyberresiliensakten, m.fl.).

Efter förslag från cybersäkerhetsutredningen 2020 (SOU 2020:58) fick Försvarets materielverk 2021 uppgiften att vara nationell myndighet för cybersäkerhetscertifiering enligt cybersäkerhetsakten. I uppgifterna ingår ansvar för tillsyn över regelsystemets efterlevnad, omvärldsbevakning av området för cybersäkerhet, samverkan med nationella och internationella aktörer samt ansvar för cybersäkerhetscertifiering på den högsta assuransnivån samt.

I cybersäkerhetsutredningens slutbetänkande (SOU 2021:63) föreslog utredaren bl.a. att Försvarets materielverk borde ges i uppdrag att analysera och lämna förslag på formerna för framtagande av ordning för nationell kravställning som utgör grund för evaluering och/eller certifiering av cybersäkerhet i produkter och tjänster i nätverks- och informationssystem i säkerhetskänslig verksamhet. Utredningen föreslog att Försvarets materielverk bl.a. skulle ges i uppdrag att analysera och lämna förslag på vilka resurser som behövs för att inrätta en sådan ordning, vilka samverkansmyndigheter som bör ges till uppgift att bidra till kravställningsarbetet samt hur näringslivsrepresentanter och företag kan beredas möjlighet att delta i arbetet. Våren 2023 fick Försvarets materielverk ett sådant uppdrag, justerat i enlighet med inkomna remissvar.

Som skäl för att ge Försvarets materielverk uppdraget angavs att informations- och cybersäkerheten, generellt i samhället såväl som i säkerhetskänslig verksamhet, ofta är beroende av säkerhetsegenskaper hos kommersiella produkter och tjänster som skulle kunna verifieras genom certifieringsordningar utvecklade inom det europeiska ramverket för cybersäkerhetscertifiering.

Risk-, hot- och sårbarhetsanalyser för såväl samhället i allmänhet som de säkerhetskänsliga verksamheterna bör ingå i det analysarbete som sedan kan omsättas till säkerhetskrav som Sverige bör framhålla i arbetet med att utarbeta certifieringsordningar.

Uppdraget syftar således till att utveckla proaktiva arbetssätt i förhållande till nationella intressen och förhandlingspositioner inom ett alltmer betydelsefullt område för cybersäkerhetsarbetet.

Regeringen bedömer att det är viktigt att myndigheter med ansvar för både hot-, sårbarhets- och riskanalyser för samhället i allmänhet såväl som myndigheter med ansvar för säkerhetskänslig verksamhet bidrar till det arbetet.

Mot bakgrund av att näringslivet både är en konsument och en producent av certifierade produkter är det viktigt ett en dialog förs med dessa under uppdragets genomförande.

Sammanfattningsvis ingår i Försvarets materielverks uppdrag att:

- Analysera och lämna förslag på hur nationella behov i fråga om cybersäkerhet kan identifieras och omsättas till säkerhetskrav som Sverige bör framhålla i arbetet med att utveckla certifieringsordningar inom EU:s cybersäkerhetsakt.
- Beakta behovet av att även kunna certifiera produkter, tjänster och processer i partnerländer utanför EU, särskilt USA.
- Lämna förslag på vilka samverkansmyndigheter som bör ges till uppgift att bidra till arbetet med behovsanalysen samt hur näringslivet kan beredas möjlighet att delta i arbetet.
- Analysera och lämna förslag på hur information om certifierade produkter, tjänster och processer och deras säkerhetsnivåer kan tillgängliggöras för samverkansmyndigheter och andra verksamhetsutövare.
- Samverka med Försvarsmakten och Säkerhetspolisen och vid behov med Försvarets radioanstalt, Myndigheten för samhällsskydd och beredskap, Polismyndigheten, Post- och telestyrelsen och andra berörda samverkansmyndigheter.
- Föra dialog med näringslivet.
- Redovisa uppdraget skriftligt till Regeringskansliet (Försvarsdepartementet) senast den 30 april 2024.

Uppdraget i sin helhet återges i bilaga 1.

1.2 Utgångspunkter

Eftersom uppdragets syfte relaterar till cybersäkerhetsakten, är det rimligt att uppdraget använder aktens definition av cybersäkerhet. Cybersäkerhet definieras där som ”all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot”.

Cyberhot definieras i sin tur som ”en potentiell omständighet, händelse eller handling som kan skada, störa eller på annat negativt sätt påverka nätverks- och informationssystem, användare av dessa system och andra personer”.

Enligt denna definition omfattas därmed både skydd mot olyckor (naturkatastrofer, handhavandefel, felbedömningar, bränder, brister i hårdvara och applikationer) och antagonistiska hot.

Cyberangrepp och -incidenter kan störa tillhandahållandet av nödvändiga tjänster som elektricitet, vatten, hälso- och sjukvård, mobila tjänster, m.m. Möjligheterna till påverkan i nätverks- och informationssystem i demokratiska valprocesser och desinformationskampanjer är också en utmaning. Genom att samhället och människorna blir alltmer beroende av digital infrastruktur och tjänster genom anslutna enheter och utbredd uppkoppling till internet ökar sårbarheten mot cyberattacker till alltmer oroande nivåer. Vidare finns en ökad hotbild avseende antagonistiska aktörer med hög förmåga till cyberattacker. Vikten av fullgod informations- och cybersäkerhet ökar därför i motsvarande grad.[4]

I regeringens försvarspolitiska proposition (prop. 2020/21:30) Totalförsvar 2021–2025 konstaterar regeringen att antalet statsunderstödda cyberangrepp ökar fortlöpande och angriparnas metoder utvecklas. Många stater har byggt upp avsevärda resurser i syfte att kunna verka offensivt genom cyberattacker. Förutom att dessa stater utvecklar avancerade metoder och offensiva verktyg har de skapat förmåga att slå brett mot många mål och att upprätthålla uthållighet över tid. I propositionen framhålls vidare att förmågan att i fredstid hantera antagonistiska hot behöver förbättras, bl.a. vad avser cyberattacker. Sårbarheter behöver minskas och verksamheter av betydelse för Sveriges säkerhet ska stärka sitt säkerhetsskydd. I detta sammanhang betonas vikten av förmågan att kunna agera samlat för att möta utmaningar och hot såväl i fred som vid höjd beredskap, bl.a. vad avser arbetet med att stärka informations- och cybersäkerheten och minska sårbarheten för att säkerställa de viktigaste samhällsfunktionerna. Förmågan att förebygga, identifiera och hantera it-incidenter och antagonistiska attacker behöver därtill förbättras inom alla samhällsviktiga funktioner. De mest skyddsvärda verksamheterna ska dessutom svara upp mot de krav som ställs i säkerhetsskyddslagstiftningen. De hot, sårbarheter och risker som digitaliseringen medför utgör komplexa säkerhetsutmaningar. Hoten blir svårare att upptäcka, beroenden blir svårare att överskåda och sårbarheterna och riskerna blir mer svårbedömda. Exempel på sådana utmaningar är antagonistiska hot som informationsoperationer och cyberangrepp mot skyddsvärda nätverks- och informationssystem, t.ex. i form av spionage, sabotage och dataintrång mot totalförsvarets verksamhet.

Bl.a. mot bakgrund av det föregående fokuseras genomförandet av uppdraget på de risker som följer av antagonistiska hot. Motiven för detta är också, något förenklat, att det är dessa hot som:

- genererar ett stort antal incidenter,
- potentiellt kan leda till störst konsekvenser för samhället och där bättre effekt efterfrågas,
- är fokus för säkerhetsskyddslagen samt säkerhetskänslig verksamhet och totalförsvaret, vilkas behov är övergripande fokus för uppdraget.

Skydd mot antagonistiska hot kan även i de flesta fall ge stöd till skydd mot icke-antagonistiska hot.

[4] SOU 2021:63, s 54.

1.3 Avgränsningar

Uppdraget har avgränsats till nationella behov i fråga om cybersäkerhet som rör säkerhetskänslig verksamhet, certifieringsordningar som utgör tvingande krav för att nå cybersäkerhetsmål enligt EU-reglering, eller certifieringsordningar på frivillig basis kan användas för att uppfylla krav enligt EU-reglering.

Motivet för avgränsningen är att fokusera på cybersäkerhetscertifieringens nytta inom säkerhetskänslig verksamhet och totalförsvaret, samt behov som uppstår genom EU-reglering.

1.4 Försvarets materielverks projektgrupp

Dag Ströman, Senior rådgivare cybersäkerhet, Juridik- och säkerhetsstaben

Jörgen Samuelsson, Rådgivare, Inspektionen för cybersäkerhetscertifiering

Dan Ohlsson, Senior rådgivare, Juridik- och säkerhetsstaben

Mats Engquist, Operativ chef, Sveriges Certifieringsorgan för IT-säkerhet

John Billow, Avdelningschef Cybersäkerhet och certifiering

Madelene Skeppar, Jurist, Juridik- och säkerhetsstaben

Mikaela Rosenlind Magnusson, Tf. Enhetschef, Sveriges Certifieringsorgan för IT-säkerhet

1.5 Genomförandet

Uppdraget har inledningsvis genomförts i samverkan med representanter från Försvarsmakten och Säkerhetspolisen samt inom Försvarets materielverk med Inspektionen för cybersäkerhetscertifiering (ICC) och Sveriges Certifieringsorgan för IT-säkerhet (CSEC).

Huvuddragen av uppdraget och dess inriktning har redovisats inom en arbetsgrupp i det Nationella cybersäkerhetscentret.

Dialog har förts med representanter från Swedac och Kommerskollegium.

Dialog har genomförts med representanter från Säkerhets- och försvarsföretagen, TechSverige, Teknikföretagen, samt företag med erfarenhet av certifiering av IT-säkerhet i produkter.

Försvarsmakten, Säkerhetspolisen, Post- och Telestyrelsen, Myndigheten för samhällsskydd och beredskap, Försvarets radioanstalt, Polismyndigheten, Swedac och Kommerskollegium har givits tillfälle att kommentera ett utkast av rapporten.

Försvarets materielverk tackar de personer som bidragit med värdefulla synpunkter och kommenter i samband med uppdraget och utarbetande av rapporten.

1.6 Disposition

Nätverks- och informationssystem som används allmänt i samhället, även inom säkerhetskänslig verksamhet, baseras generellt på kommersiella produkter och

tjänster som är konstruerade utifrån komplex informations- och kommunikationsteknik. Exempel på sådana teknikområden redovisas i avsnitt 2 ”Informations- och kommunikationsteknik”.

Den informations- och kommunikationsteknik som allmänt utgör grunden för nätverks- och informationssystem och även cybersäkerhetsaktens certifieringsordningar baseras på krav som anges i olika standarder. En närmare beskrivning regelverk för standardisering och de organisationer som utvecklar standarder inom IKT- och cybersäkerhet redovisas i avsnitt 3 ”Standardisering” samt i ”Bilaga 5 - Exempel på standardiseringsorgan och de facto-standardiseringsorgan inom cyberområdet”.

En översiktlig beskrivning av cybersäkerhetsområdet återfinns i avsnitt 4 ”Cybersäkerhet”.

Effektivt arbete med cybersäkerhet förutsätter även kunskap om vilka kontroll- och verifieringsmetoder som är lämpliga, samt förståelse för när och hur certifiering enligt cybersäkerhetsakten är en lämplig metod. Sådana aspekter redovisas i avsnitt 5 ”Cybersäkerhetscertifiering”.

Avsnitt 6 ”EU:s cybersäkerhetsakt och dess certifieringsordningar” beskriver det europeiska ramverket för cybersäkerhetscertifiering, de tre certifieringsordningarna som är under utveckling, samt i bilagorna 5, 6 och 7 tillhörande standarder. I avsnittet beskrivs även processen för utveckling av en certifieringsordning, vilken på olika sätt ger möjlighet för påverkan från svenska intressenter.

Avsnitt 7 ”EU-reglering med referenser till cybersäkerhetscertifiering” beskriver EU-regleringar med koppling till cybersäkerhetscertifiering.

Avsnitt 8 ”Nationell reglering med relevans för uppdraget” ger exempel på nationell reglering med relevans för uppdraget.

Avsnitt 9 ”Försvarets materielverks uppgifter och ansvar” förklarar Försvarets materielverks uppgift, enligt cybersäkerhetsakten och svensk reglering.

Avsnitt 10 ”Näringslivets behov och medverkan” ger en överblick över de behov och förutsättningar som kan anses vara centrala för näringslivet i sin roll som tillhandahållare av produkter och tjänster som kan bli föremål för cybersäkerhetscertifiering.

Avsnitt 11 ”Utgångspunkter, analys och förslag” sammanfattar uppdraget och sätter det i relation till de utgångspunkter som redovisats i rapportens tidigare avsnitt. Därefter följer en analys och Försvarets materielverks förslag på hur nationella behov av cybersäkerhet kan identifieras och omsättas till säkerhetskrav som Sverige bör framhålla i arbetet med att utveckla certifieringsordningar inom EU.

2 Informations- och kommunikationsteknik

Försvarets materielverks bedömning:

Nätverks- och informationssystem som används allmänt i samhället, även inom säkerhetskänslig verksamhet, baseras generellt på kommersiella produkter och tjänster som är konstruerade utifrån komplex informations- och kommunikationsteknik. De olika teknikområdena ger förutsättningar för såväl systemens funktionella egenskaper som deras säkerhetsegenskaper. Dessa teknikområden tillsammans med den snabba digitaliseringen skapar ökad risk för sårbarheter som kan utnyttjas för att genomföra IT-angrepp.

Exempel på sådana teknikområden, som var och en kan medföra cyberrisker på systemnivå, är teknisk design och tillverkning av datachip, teknisk design och tillverkning av hårdvara som exempelvis servrar, mobiltelefoner och persondatorer, utvecklingsprocessen för mjukvara samt teknisk design av olika typer av applikationer.

Öppen källkod, som i sig har inneburit ett paradigmskifte vad gäller kostnadseffektiv tillgänglighet av avancerad kod såväl som applikationer, medför en påtaglig ökad risk för sårbarheter som drabbar många system samtidigt.

Informations- och kommunikationsteknik utgör den tekniska basen och används för att bygga upp komplexa nätverks- och informationssystem, t.ex. molntjänster, 5G-system och ”Sakernas internet”. Att på ett adekvat sätt kunna göra risk-, hot- och sårbarhetsanalyser för nätverks- och informationssystem, som bygger på dessa teknikområden, förutsätter en djup kompetens inom dessa områden, hur de samverkar och hur de påverkar de cyberrisker som detta medför.

2.1 Inledning

Informations- och kommunikationsteknik (IKT) är grunden för de komplexa och sammankopplade system som stöder dagliga samhälleliga verksamheter, håller våra ekonomier igång inom viktiga sektorer som hälso- och sjukvård, energi, finans och transporter.

I denna rapport är det motiverat att ge en översiktlig beskrivning av de olika funktionella delar som kan finns i moderna IKT-system. Dessa olika delar/lager består i sin tur av it-produkter (komponenter) som även dessa i sig kan vara mycket omfattande och bestå av 10-tals eller 100-tals miljoner rader kod. Varje rad kod kan hypotetiskt innehålla konstruktioner som medför mer eller mindre allvarliga sårbarheter.

Syftet med avsnittet är att visa på omfattningen av och komplexiteten i de system och produkter som utgör grunden för digitaliseringen, och där varje del skapar olika typer av risker och möjliga attackvägar. Detta påverkar i sin tur vilka typer av cybercertifieringar som å ena sidan kan vara efterfrågade och å andra sidan kan vara svåra att realisera p.g.a. de olika tekniska utmaningar som finns.

2.2 Hårdvara – datachip

Datachip är centrala komponenter i elektronik och datorer. All exekvering av dataprogram och behandling av data sker genom de oerhörda mängder transistorer som implementeras på varje chip. Dessa chip utgör en förutsättning för avancerade enheter som smartphones, datorer, IoT-enheter, smarta kort och mycket mer. Ett avancerat chip kan idag innehålla 25 miljarder transistorer. De senaste chippen som är ledande för bl.a. AI-tillämpningar kombinerar två chip som tillsammans innehåller 208 miljarder transistorer. Chippen innehåller även avancerande ledningsnät med ibland över 20 lager med ledningar staplade över varandra och som kopplar ihop transistorerna.

Tillverkningen av datachip är en komplex process som involverar flera steg av avancerad teknik. Det inkluderar design av kretsen, skapande av fotomasker, avlagring av olika materialskikt på kiselskivan, fotolitografi för att överföra kretsmönstret, etsning och dopning av kiselsubstratet för att forma komponenter, paketering och testning av de färdiga chippen. Denna tillverkningsprocess kräver hög precision och avancerad teknik för att producera datachip med hög prestanda och pålitlighet.

Datachip är centrala för digitaliseringen genom att möjliggöra utvecklingen av avancerade tekniska lösningar och enheter. Deras tillverkning är en avancerad och sofistikerad process som kräver noggrann planering, implementering och kontroll för att uppnå hög kvalitet och prestanda.

Chippen tillverkas av leverantörer i hela världen. Drivkraften att utveckla allt mer högpresterande chip har lett till att kostnaderna för att bygga de fabriker som kan tillverka av de allra mest kapabla och sofistikerade chipen med de minsta dimensionerna har ökat till extremt höga nivåer. Idag är det tre leverantörer, Intel, Samsung och TSCM som kan sägas ha denna förmåga.

En sådan modern produktionsanläggning kostar oerhörda summor att bygga, i storleksordningen 20–40 miljarder dollar, dvs. en kostnad som motsvarar många länders statsbudget.

Datachippen används sedan för att bygga de olika dedicerade hårdvaror, servrar, routrar och personliga datorer som används för att bygga nätverks- och informationssystem.

Datachippen kan innehålla mer eller mindre allvarliga sårbarheter. Sådana sårbarheter kan vara mycket svåra att finna, inte minst p.g.a. chippens enorma komplexitet och små dimensioner.

2.3 Hårdvara – produkter

Nedan följer exempel på vanligt förekommande hårdvaruprodukter:

Servrar är centrala datorer som hanterar resurser, data och tjänster för att tillhandahålla nätverks- och informationsfunktionalitet. Det kan inkludera filservrar, webbservrar, databasservrar etc.

Switchar används för att ansluta enheter i lokala nätverk och möjliggöra kommunikation mellan dem, medan *routrar* används för att koppla ihop olika nätverk och möjliggöra kommunikation över större avstånd, till exempel mellan lokala nätverk och internet, eller mellan olika organisationer uppkopplade till internet.

Brandväggar är enheter som övervakar och kontrollerar inkommande och utgående nätverkstrafik för att skydda mot obehörig åtkomst och skadlig programvara.

Datalagring utgörs av specialiserad hårdvara som används för att lagra och dela filer över nätverket.

Säkerhetslösningar inkluderar enheter som IDS (Intrusion Detection System) och IPS (Intrusion Prevention System) för att upptäcka och förhindra attacker samt VPN (Virtual Private Network) för krypterad fjärråtkomst till nätverket.

2.4 Mjukvara – programspråk

Datachippen som hanterar data styrs av en stor mängd mycket primitiva och instruktioner, s.k. maskinkod. Denna kod beskriver hur en viss applikation ska bearbeta data som förs mellan chippet och olika typer av minne och lagringsenheter. Att skriva program på denna nivå är dock utmanande och ineffektivt. För att underlätta arbetet med att skapa program definieras s.k. högnivåspråk, där beskrivningen för hur data ska hanteras sker på en mycket högre abstraktionsnivå och som är, jämfört med maskinkod, enklare för människor att använda. Dessa olika högnivåspråk kan sedan m.h.a. speciella program (kompilatorer, interpretatorer) automatiskt översättas till maskinkod, som sedan exekveras på datachippen.

Det finns en mycket stor mängd programspråk som används för olika syften. Varje programspråk kräver stor erfarenhet och expertis för att man ska förstå hur en viss uppgift kan lösas. Varje programspråk är behäftat med olika egenskaper som gör det mer eller mindre lätt för programmeraren att skapa konstruktioner som är funktionellt korrekta, dvs. löser den tänkta uppgiften, men som ändå kan innehålla brister eller sårbarheter som utnyttjas av en angripare. Det krävs för de flesta programmerare många års erfarenhet för att bygga upp nödvändig kunskap för att behärska hur koden ska skrivas för att både leverera rätt funktion och undvika de vanligaste misstagen som kan leda till sårbarheter.

Nedan följer exempel på vanligt förekommande programspråk:

Python är känt för sin läsbarhet och enkelhet. Det används t.ex. för webbapplikationer, dataanalys, artificiell intelligens (AI), maskininlärning, vetenskaplig databehandling och industriautomatisering.

Java är designat för att koden ska kunna exekveras med samma resultat på många olika datorplattformar. Det används t.ex. i företagsapplikationer, Androidappar, webbaserade applikationer, mjukvaruverktyg och stora datasystem.

JavaScript används främst för att skapa interaktiva webbsidor. Det körs på klientens webbläsare men används ibland även på servrar. Det används t.ex. vid webbutveckling, webbapplikationer och på webbservrar.

C++ är en utökning av C-språket som lägger till s.k. objektorienterad programmering. Det används för systemmjukvara, spelutveckling, realtidsapplikationer, inbyggda system högpresterande applikationer.

C är ett av de tidigaste programspråken som låg till grund för t.ex. både de tidiga operativsystemen och senare de många olika Linux-varianterna. C är känt för att vara mycket effektivt och används därför både i system som kräver hög prestanda och i system där beräkningskraften är begränsad, t.ex. i inbyggda system och i IoT-produkter. C är även känt för att programmeraren mycket lätt kan skapa program med rätt funktion, men som samtidigt innehåller många sårbarheter.

PHP är ett skriptspråk som främst används för serversidans utveckling av webbplatser och applikationer. Många webbservrar är baserade på PHP.

Swift är ett programspråk skapat av Apple för iOS- och macOS-utveckling. Det används främst i iOS- och macOS-appar, watchOS, tvOS.

Ruby är känt för sin eleganta syntax och är lätt att läsa och skriva. Det är ett tolkat skriptspråk som främjar snabb utveckling. Det används för webbapplikationer, automatisering och prototyper.

Go är utvecklat av Google och används t.ex. för tillämpningar med många parallella beräkningar samt för systemutveckling, t.ex. webbservrar, nätverksverktyg, distribuerade system och molnbaserade tjänster.

2.5 Mjukvara – applikationer

Nedan följer exempel på vanligt förekommande mjukvaruapplikationer:

Operativsystem är det program som kontrollerar en server eller dator. Vanligtvis används serveroperativsystem som Windows Server, Linux (t.ex. Ubuntu, CentOS) eller Unix för att driva servrar och nätverksenheter.

Nätverksprotokoll, bl.a. TCP/IP, HTTP, FTP, SMTP, SNMP etc., används för att hantera kommunikationen mellan olika enheter på ett lokalt nätverk eller via internet.

Applikationer och tjänster innefattar bl.a. webbserverprogram som Apache eller Nginx, databasprogram som MySQL eller MongoDB, e-postservrar som Exchange eller Postfixoch filhanteringsprogram som Samba etc.

Säkerhetsmjukvara inkluderar brandväggsprogramvara, antivirusprogram, antimalware-program, krypteringsverktyg och andra säkerhetslösningar för att skydda nätverket och dess data.

*Administration och övervakning*kan t.ex. vara mjukvara för att administrera och övervaka nätverks- och informationsresurser, inklusive program för fjärradministration, övervakning av nätverkstrafik, logghantering och rapportering.

Genom att integrera och konfigurera hård- och mjukvarukomponenter på lämpligt sätt kan man skapa robusta och säkra nätverks- och informationssystem som möter organisationens behov och krav.

2.6 Mjukvara – utvecklingsprocessen och dess verktyg

En avsevärd del av de sårbarheter som kan drabba ett it-system beror på olika typer av brister som uppstår vid design och implementering dess mjukvarubaserade applikationer. För att minska dessa risker är det viktigt att integrera säkerhetsprinciper och bästa praxis genom hela utvecklingscykeln. Denna inkluderar säkerhetsgranskningar, penetrationstester och kontinuerlig övervakning av säkerhetsaspekter i koden. Det är därför relevant att återge en kort beskrivning av vilka principiella steg som normalt bör (men långt ifrån alltid) tillämpas vid utveckling av it-produkter och där kompetens, verktyg och arbetsprocesser kan vara föremål för certifiering.

Nedan följer exempel på vanligt förekommande steg vid utveckling av applikationer:

Kravspecificering definierar och dokumenterar användar- och systemkrav. Oklara eller ofullständiga krav kan leda till felaktig implementation som medför risker för sårbarheter. Om kraven inte inkluderar säkerhetsaspekter (t.ex. p.g.a. bristande kompetens och erfarenhet) kan det öka risken för sårbarheter betydligt.

Design skapar arkitekturen och designen för applikationen. Stora produkter kan bestå av 1.000-tals eller 10.000-tals komponenter som samverkar, har inbördes beroenden och kommunicerar med varandra för att etablera de funktioner som är avsedda. Brister i designen, t.ex. felaktig hantering av behörigheter, bristfälliga gränssnitt eller referenser till föråldrade eller olämpliga standarder kan leda till sårbarheter.

Implementering (Kodning) består i att programmerare skriver och testar koden baserat på den godkända designen. Detta är oftast en intensiv och iterativ process, som sker i samverkan via arbetsgrupper, som i sin tur samverkar med varandra. Bristande kodningsregler, oerfarna programmerare, bristande respekt för kodningens risker och tidsbrist, bristande kontroll av indata och bristande uppdatering av tredjepartsprogramvara kan leda till sårbarheter som utnyttjas av angripare. Stora applikationer kan kräva att tusentals programmerare samverkar, ibland under flera års tid.

Källkods- och versionshantering utgör en process med tillhörande verktyg genom vilken programmerare samverkar kring de oftast mycket stora mängder källkodsfiler som flera programmerare behöver utveckla tillsammans. Dessa verktyg ger stöd för hantering av olika kombinationer av källkod, som utgör basen för olika versioner av applikationen. Otillräcklig säkerhet kring vem som har åtkomst till källkoden kan leda till obehörig åtkomst och obehörig manipulering av källkoden. Felaktigt handhavande kan även detta leda till att applikationen baseras på fel källkod, vilket kan medföra sårbarheter.

Byggning och distribution är en process med tillhörande verktyg som bygger den körbara applikationen och distribuerar den till olika miljöer. För stora applikationer kan detta innebära mycket långa byggtider som kräver omfattande datakraft. Byggsystemet brukar vara integrerat med källkods- och versionshanteringen som tillhandahåller rätt källkodsfiler till byggprocessen. Byggverktygen kan bygga hela applikationen, eller instrueras att bara bygga vissa komponenter eller delsystem. Säkerhetsbrister i bygg-

och distributionsprocessen kan möjliggöra insmuggling av skadlig kod eller felaktig konfiguration i produktionsmiljön.

Testning är en process med tillhörande verktyg för att genomföra tester på komponenter, delsystem på olika nivåer, samt slutligen systemtester på den färdiga applikationen. Otillräcklig testning kan leda till att sårbarheter förblir oupptäckta. Även testdata och konfiguration kan vara sårbara för otillbörlig åtkomst.

Dokumentation innebär att man skapar teknisk dokumentation. Otillräcklig dokumentation av säkerhetsåtgärder och konfigurationer kan göra det svårt att hantera och upprätthålla säkerheten över tid.

Underhåll och support utgörs av processer och verktyg för att hantera buggfixar, säkerhetsuppdateringar och support. Dessa baseras ofta på källkod- och versionshanteringen samt byggning och distributionsverktygen. Förseningar i att hantera säkerhetsbrister eller bristande support kan öka risken för sårbarheter. Bristande kvalitet i patchar kan leda till att nya sårbarheter introduceras.

Det finns särskilda utvecklingsprocesser för utveckling av mjukvara som i varje steg av processen ovan innebär att specifika åtgärder vidtas för att förebygga eller hitta design- eller implementationsmisstag som kan innebära att applikationen är behäftad med sårbarheter. En sådan process kallas ofta för *Secure Development Life Cycle*. Ett företag som tillämpar en sådan kan förväntas ha betydligt färre sårbarheter i sina applikationer än företag som inte tillämpar en sådan process.

2.7 Mjukvara – öppen källkod

Öppen källkod (Open Source) refererar till programvara vars källkod är offentligt tillgänglig för alla att använda, modifiera och distribuera. Den bygger på principen om samarbete och delning av resultatet, vilket möjliggör att programmerare från hela världen kan bidra till utvecklingen av programvaran.

Samarbetet sker med hjälp av datorstöd där medverkande utvecklare kan bidra genom att göra ändringar i en egen lokal kopia (t.ex. med stöd av källkods- och samarbetsverktyget Git) och sedan föreslå dessa ändringar tillbaka till de som är ansvariga för huvudprojektet. Genom forum och mailinglistor kan utvecklare och användare diskutera idéer, rapportera buggar och be om funktioner. Många öppen källkodsprojekt har en öppen styrningsmodell där beslut om projektets riktning tas genom gemenskapsomröstningar eller av en styrkommitté som representerar gemenskapens intressen.

I stora öppen källkodsprojekt kan koden bli extremt omfattande. Operativsystem som Linux med tillhörande applikationer omfattar flera hundra miljoner rader kod. Webbläsaren Firefox och databashanteringssystemet MySQL är andra exempel på stora projekt med oerhört omfattande kodbaser och som har mycket stor global spridning.

Öppen källkodsprojekt har haft en enorm påverkan på både teknikindustrin och vardagsanvändare över hela världen. Det är öppen källkod som har gjort att mycket komplicerade och funktionsrika applikationer gjorts tillgängliga på den globala marknaden till mycket låg eller ingen kostnad.

Det finns dock även stora risker med öppen källkod. Eftersom samma källkod ingår som del i så många applikationer kan ett enskilt kodningsmisstag leda till mycket stor spridning där miljontals system i hela världen samtidigt är eller blir sårbara. En annan risk är att statsaktörer och andra organisationer aktivt medverkar vid utveckling av öppen källkod och medvetet för in allvarliga bakdörrar som sedan kan få mycket stor spridning.

Nedan följer exempel på vanligt förekommande framstående öppna källkodsprojekt med global spridning:

Linux är inte bara ett operativsystem utan ett ekosystem av distributioner (distros) som används i smartphones (via Android, som bygger på Linux-kärnan), på servrar, i inbäddade system, på skrivbord och i vetenskapliga datorsystem. Det är ryggraden i mycket av internet och kraften bakom majoriteten av världens servrar.

Apache HTTP Server har varit den mest populära webbserverprogramvaran i världen sedan mitten av 1990-talet. Den spelar en avgörande roll i drift av webben, genom att möjliggöra värdskap för webbsidor på internet.

MySQL och PostgreSQL är två av de mest använda relationsdatabashanteringssystemen (RDBMS) för lagring och sökning av data. Det är genom dessa som stora mängder data organiseras och sedan via olika sökningar kan levereras till applikationer, webbservar och molntjänster.

Git är ett system som används för källkodshantering i mjukvaruutvecklingsprojekt. Git möjliggör effektivt samarbete mellan utvecklare genom att hålla reda på och samordna ändringar i källkoden över tid. Git utgör idag grunden för nästan all utveckling av mjukvara, inklusive den som utvecklas av stora internationella techjättar.

Android är ett mobilt operativsystem baserat på Linux-kärnan och andra öppen källkodsprogramvaror. Det är det mest använda mobila operativsystemet i världen, som driver en myriad av enheter, från smartphones och tabletter till smartklockor och TV-apparater.

Firefox är en webbläsare utvecklad av Mozilla Foundation. Vid sidan av webbläsarna från de stora techföretagen är Firefox en av de mest använda som är baserad på öppen källkod.

WordPress är ett innehållshanteringssystem (CMS) som driver en stor del av internet, från små personliga bloggar till stora nyhetssajter och företagswebbplatser. Det är känt för sin enkelhet, flexibilitet och ett stort utbud av teman och plug-ins.

Docker har revolutionerat utvecklingen av programvara genom att göra det möjligt för utvecklare att paketera sina applikationer med alla deras beroenden i en standardiserad enhet, som sedan väsentligt underlättar att dessa applikationer kan installeras i sina respektive it-system.

TensorFlow och PyTorch är två ledande öppen källkodsramverk för maskininlärning och djupinlärning (AI). TensorFlow utvecklades av Google, medan PyTorch har sitt ursprung från Facebook. Båda används i akademisk forskning och industriell utveckling för att bygga och träna maskininlärningsmodeller.

2.8 Molntjänster

Molntjänster bygger på stora datacenter som är distribuerade över olika geografiska platser för att öka tillgänglighet och redundans.

Virtualisering innebär att en fysisk server kör en särskild programvara, som gör att enskilda användare uppfattar att de får tillgång till en komplett egen hårdvara bestående av de komponenter som beskrivs i föregående avsnitt, medan användaren i själva verket ges tillgång till en ”virtuell dator” där flera olika användare i själva verket kommunicerar med virtualiseringsprogrammet och delar fysisk server med flera andra användare. Dessa användare kan på detta sätt dela på samma fysiska hårdvara. Det är även möjligt att snabbt öka tillgången till datakraft genom att sprida en enskild användarens virtuella konfiguration till flera olika fysiska servrar.

I de virtualiserade datormiljöerna installeras den kombination av simulerad hårdvara och mjukvara som behövs för att etablera det nätverks- och informationssystem som efterfrågats av användaren.

Datacenter där sådana virtualiserade datormiljöer erbjud kan bestå av tusentals fysiska servrar som var och en är virtualiserad för att erbjuda olika tjänster beroende på användarnas behov. För att optimera användningen av hårdvaruresurser används virtualiseringsplattformar som VMware, Microsoft Hyper-V eller OpenStack. Dessa plattformar möjliggör skapandet och hanteringen av virtuella maskiner (VM) på fysisk hårdvara.

Datacenter som erbjuder molntjänster använder sofistikerade nätverksinfrastrukturer för att möjliggöra kommunikation och dataöverföring mellan olika delar av molnet och användare över hela världen. Det inkluderar högpresterande switchar, routrar, lastbalanserare och CDN (Content Delivery Network) för att optimera dataöverföringen.

Data lagras i distribuerade lagringskluster för att säkerställa tillgänglighet och redundans. Tekniker som RAID (Redundant Array of Independent Disks) där flera hårddiskar används för att lagra samma data och skapa redundans används för att skydda mot risken för dataförlust om och när en enskild hårddisk slutar fungera eller på annat sätt skadas.

Via sådana datacenters kan användare erbjudas tillgång till datakraft och tjänster på olika nivåer, t.ex.:

SaaS (Software as a Service) där användare kan få tillgång till och använda programvara via internet. Exempel inkluderar Office 365, Salesforce och Google Workspace. Användaren behöver inte själv förstå hur applikationer, olika servrar och nätverket ska konfigureras eller var datalagringen sker.

PaaS (Platform as a Service) där användare själv kan installera sina egna applikationer och få åtkomst till dessa på ett skalbart sätt i hela världen utan att själv behöva ta hand om hur närverk ska konfigureras eller hur datalagringen ska fungera.

IaaS (Infrastructure as a Service) där användare kan hyra virtualiserade servrar, lagring och nätverksresurser för att bygga och hantera sina egna it-miljöer. I dessa fall kan användaren själv skapa datorresurser som servrar, routrar och

nätverkskonfigurationen som beskriver hur dessa resurser kopplas samman. I denna miljö kan användaren sedan själv även installera sina egna applikationer.

Molntjänster erbjuder elastiska resurser som kan skalas upp eller ned efter behov, vilket möjliggör en flexibel och kostnadseffektiv infrastruktur. Med distribuerade datacenter och redundansmekanismer kan molntjänster erbjuda hög tillgänglighet och geografisk distribution för att minimera nertid och maximera prestanda. Genom att eliminera behovet av att köpa och underhålla egen hårdvara kan företag minska sina kapital- och driftskostnader och istället betala för användningen av molntjänster enligt en förbrukningsbaserad modell. Molntjänster erbjuder automatiserade hanterings- och driftsverktyg för att förenkla hanteringen av infrastruktur och applikationer samt förbättra effektiviteten och skalbarheten. Slutligen kan molntjänster tillhandahåller globala datacenter och nätverksinfrastrukturer för att stödja användare och applikationer över hela världen och optimera prestanda och tillgänglighet, även för små organisationer som annars inte skulle kunna etablera en sådan infrastruktur på egen hand.

Molntjänster kan dock bli ett mycket attraktivt mål för cyberattacker och dataintrång, vilket kan leda till förlust av känslig information och förtroende från användare. I synnerhet om många olika organisationer lagrar sina data i samma molntjänst. Användare är beroende av en pålitlig internetanslutning för att kunna få tillgång till molntjänster och data, vilket kan vara en begränsning i områden med begränsad eller opålitlig anslutning. För stora datavolymer kan kostnaden för att överföra data till och från molntjänster bli betydande, särskilt om det sker över långa avstånd eller över internet. Att förlita sig helt på en molntjänstleverantör kan göra det svårt att byta leverantör eller migrera tillbaka till egen infrastruktur om det behövs, vilket kan resultera i inlåsningseffekter och begränsad flexibilitet.

2.9 5G-System

5G (5:e generationens mobilnät eller 5:e generationens trådlösa kommunikationssystem) betecknar den senaste stora generationen av mobila telekommunikationsstandarder som följde på 4G. De första kommersiella systemen startade 2019.

5G innebär att datorer och mobila enheter får snabbare uppkoppling och mindre fördröjning. 5G är avsedd för tillämpningar såsom maskin-till-maskin-kommunikation och sakernas internet, där korta svarstider är till fördel. 5G-tekniken har även visat sig vara lämplig för fast trådlös åtkomst (eng: ”Fixed Wireless Access” - FWA). Nätets kapacitet ökar så att fler enheter ska ha möjlighet att vara uppkopplade samtidigt och till lägre kostnad. Den högre kapaciteten beror dels på att spektrumutrymmen har frigjorts särskild för 5G-nätverk samt möjlighet till att många fler antennelement (så kallad massive MIMO) kan användas för att effektivisera spektrumanvändningen.

Användarenheter består av enheterna som vi använder dagligen, som smartphones, surfplattor och andra IoT-enheter. De är utrustade med teknik för att ansluta till 5G-nätverket och dra nytta av dess höga hastighet och låga fördröjning.

SIM-teknik (baserade på datachip) används för att identifiera och autentisera användarutrustning i nätverket och möjliggöra åtkomst till tjänster och resurser.

Basstationer är placerade runt om i städer och landskap för att ge täckning och anslutning till användarna. Basstationerna tar emot och skickar signaler till och från användarenheter och transporterar trafiken vidare.

Kärnnätverket (eng: ”Core Network”) hanterar all kommunikation och dataöverföring mellan användare, applikationer och andra delar av nätverket. Kärnnätet består av flera olika funktioner som arbetar tillsammans för att möjliggöra kommunikation och dataöverföring. Kärnnätet hantera också säkerhetsfunktionerna såsom autentisering, accesskontroll och debitering (eng: ”Authentication, Authorisaton and Accounting” - AAA).

Slutligen är det de olika applikationerna och tjänsterna som på användarenheter och servrar som drar nytta av 5G-nätverkets hastighet och kapacitet. Det kan vara allt från streaming av video och musik till smarta hemenheter och industriella IoT-lösningar.

Utöver själva applikationerna och tjänsterna sker också en omvandling av nätverksarkitekturen i 5G till en tjänstebaserad arkitektur (service based architecture). Fördelen med detta är att harmonisera arkitekturen mot den bredare IKT-sektorn som redan använder en sådan struktur för att konstruera system. Tidigare 3GPP system har till stor del haft egna protokoll men numera används mestadels http2.

Sammanfattningsvis är 5G-systemet en infrastruktur som möjliggör snabb och tillförlitlig trådlös kommunikation och dataöverföring över långa avstånd. Det är en kombination av olika teknologier och delar som arbetar tillsammans för att leverera en bättre upplevelse för användare och stödja en mängd olika applikationer och tjänster.

2.10 Sakernas internet (Internet of things - IoT)

Sakernas internet (IoT, eller Internet of Things), är en teknik som möjliggör anslutning och kommunikation mellan fysiska enheter och internet. Dessa kan många gånger vara ganska små enheter, utrustade med särskilda chip som förutom förmågan att processa data även har funktioner för inkoppling av sensorer och möjligheter att styra andra enheter (s.k. mikroprocessorer).

IoT-enheter är utrustade med olika typer av sensorer för att samla in data från den fysiska världen. Det kan vara sensorer för mätning av temperatur, luftfuktighet, ljusnivåer, rörelse, vibrationer, och mycket mer.

Sensordata samlas in och behandlas av IoT-enheter för att extrahera relevant information och identifiera mönster eller avvikelser. Denna data kan sedan användas för att fatta beslut, styra enheter eller via olika kommunikationslänkar överföra data till molnbaserade tjänster för ytterligare analys.

IoT kan som ovan nämns m.h.a. s.k. aktuatorer styra olika typer av utrustning, t.ex. dörrlås, styra fordon på vägarna, kontrollera ventiler i processindustri etc.). IoT blir då en del av cyber-fysiska system kan innebära stora risker eftersom sådana attacker kan få en mer eller mindre fysisk effekt.

IoT-enheter använder vanligtvis trådlös kommunikationsteknik, såsom Wi-Fi, Bluetooth, Zigbee, LoRa, eller andra protokoll för att ansluta till internet eller kommunicera med andra enheter i närheten.

För att underlätta kommunikation mellan enheter och molnet använder IoT vanligtvis standardiserade kommunikationsprotokoll som MQTT (Message Queuing Telemetry Transport), CoAP (Constrained Application Protocol), eller HTTP (Hypertext Transfer Protocol).

IoT-enheter kan överföra data till serverbaserade tjänster, ofta implementerade via molntjänster där den kan bearbetas, analyseras och lagra för vidare användning.

IoT-data lagras i en (molnbaserad) server eller lokalt på enheten beroende på kraven och användningsfallet. Det kan vara strukturerad eller ostrukturerad data som lagras i databaser, filsystem eller andra lagringslösningar.

Molnbaserade IoT-plattformar kan använda avancerade analysalgoritmer och maskininlärning för att bearbeta och analysera stora mängder IoT-data. Detta kan inkludera prediktiv analys, anomalidetektion, mönsterigenkänning m.m. för att extrahera insikter och förutsägelser.

Baserat på resultaten av dataanalysen kan IoT-enheter utföra åtgärder eller styra andra enheter i den fysiska världen. Detta kan vara automatiska åtgärder som att justera temperaturer, aktivera larm eller informera användare om specifika händelser.

Genom att kombinera sensorer, trådlös kommunikation och molnbaserad datalagring och analys möjliggör IoT-enheterna en rad olika tillämpningar och användningsfall över olika branscher och sektorer, inklusive smarta hem, industriautomation, hälsovård, transport och mycket mer.

2.11 Artificiell intelligens

Artificiell intelligens (AI) är tekniken bakom datorsystem som kan utföra uppgifter som är svåra att lösa via klassiskt sekventiellt programmerade datorsystem: AI-system kan ges förmågor som annars ofta kräver mänsklig intelligens, såsom att tolka naturligt språk, känna igen mönster, dra slutsatser och lösa problem.

Maskininlärning (ML) är en gren inom AI som fokuserar på att bygga algoritmer och statistiska modeller som låter datorer "lära" sig från och göra förutsägelser eller beslut baserade på data, utan att vara explicit och sekventiellt programmerade för specifika uppgifter.

Det kan krävas väldigt stora datamängder och datorkraft för att träna ett system som baseras på AI/ML för att lära sig att lösa en uppgift.

AI/ML har utvecklats mycket snabbt de senaste åren och har potential att kunna t.ex förutsäga sjukdomsutbrott eller diagnostisera sjukdomar. Det kan även få tillämpning för t.ex detektion av bedrägerier inom finansiella sektorn, eller för att skapa självkörande bilar som mer eller mindre ges förmåga att tolka och reagera på omgivande miljöer.

Användningen av AI/ML innebär både möjligheter och utmaningar.

AI-modeller kan manipuleras genom så kallade adversarial attacks, där små, avsiktliga störningar i indata kan användas för att träna en modell att fatta felaktiga beslut i väldigt specifika situationer. Träning av AI/ML kräver som tidigare nämnts stora mängder data. Det ställs därmed höga krav på dataskydd och säkerhetsåtgärder för att skydda känslig information som används vid träningen från obehörig åtkomst och dataintrång.

AI kan användas både för att automatisera och förbättra skydd mot cyberattacker, så väl som för att genomföra sådana attacker.

En annan allvarlig risk är att AI-system baserat på de data som används vid inlärningen agerar partiskt, vilka kan leda till ojämlik behandling eller diskriminering.

Den nya AI-akten är bl.a. etablerad för att hantera sådana risker. Cybersäkerhetscertifiering enligt cybersäkerhetsakten anges vara en möjlig väg för att indikera uppfyllnad av AI-aktens cybersäkerhetskrav.

3 Standardisering

Försvarets materielverks bedömning:

De krav som etableras i cybersäkerhetsaktens certifieringsordningar baseras till övervägande del på referenser till krav som anges i olika standarder och andra tekniska specifikationer utvecklade av standardiseringsorgan eller andra organisationer. Sådana standarder är sedan i sin tur direkt eller indirekt beroende av ytterligare andra standarder som utvecklas inom IKT-området. Tillsammans bildar dessa standarder det ekosystem av tekniska krav som utgör förutsättningen för samhällets digitalisering.

Sådana standarder kan t.ex. avse funktionella krav, specifika säkerhetskrav, vilka kontroller av funktion eller säkerhet som ska göras eller hur t.ex. organ för bedömning av överensstämmelse ska vara utsedda och organiserade.

Uppdragets uppgift att analysera och lämna förslag på hur nationella behov i fråga om cybersäkerhet kan identifieras och omsättas till säkerhetskrav som Sverige bör framhålla i arbetet med att utveckla certifieringsordningar inom EU:s cybersäkerhetsakt handlar därmed inte bara om hur Sverige kan påverka de direkta certifieringsordningarnas texter (de s.k. genomförandeakterna) eller de utkast som diskuteras under ordningarnas framtagande inom ramen för EU-kommissionens, medlemsstaterna och Enisas arbete. Att omsätta nationella behov till säkerhetskrav inom EU-arbetet handlar även om svensk påverkan på de standarder som refereras i certifieringsordningarna och därmed även om hur svensk medverkan i de standardiseringsorgan som utvecklar dessa standarder kan organiseras.

För att nationella behov av säkerhetskrav i IKT-produkter och tjänster ska kunna tillgodoses inom EU-arbetet är det av fundamental betydelse att de standarder och tekniska specifikationer som direkt eller indirekt har betydelse för EU:s certifieringordningar utvecklas öppet, transparent och i enlighet med EU:s standardiseringsförordning och Världshandelsorganisationens avtal om tekniska handelshinder (TBT-avtalet) och dess principer om öppenhet, transparens, effektivitet, oberoende och ekvivalens[5]. Om så inte sker riskerar svenska intressenter ställas utanför det viktiga kravställningarbetet vid utveckling av dessa standarder. Det kan leda till en påtaglig nackdel för svenska intressen när det gäller harmoniserade krav på den inre marknaden. Det kan även riskera att EU:s certifieringsordningar leder, ur ett nationellt perspektiv, till onödiga tekniska handelshinder med handelspartners utanför EU.

Det är en mycket omfattande uppgift för enskilda myndigheter och andra verksamhetsutövare att ha tillräcklig kompetens och resurser för att bevaka och aktivt medverka i alla de olika standardiseringsorgan (inklusive de facto-standardiseringsorgan) som är av relevans för den egna verksamheten.

Frågan om hurvida de krav som anges i EU:s certiferingsordningar ska baseras på öppna globala standarder, eller på europiska regionala standarder, har både handelspolitiska och

[5] Se Uppförandekod för utarbetande, fastställande och tillämpning av standarder, Bilaga 3 i WTO:s avtal om tekniska handelshinder

säkerhetspolitiska dimensioner och är mycket svåra för enskilda sektorsmyndigheter, verksamhetsutövare och/eller näringslivet att hantera helt på egen hand.

3.1 Inledning

Olika typer av standarder utgör en förutsättning för det globala samhällets snabba digitalisering. Genom att etablera gemensamma krav, protokoll, utvecklingsprocesser och format underlättar standardisering integration, interoperabilitet och cybersäkerhet i nätverks- och informationssystem.

I en värld där företag, offentliga tjänster och konsumenter använder en mängd olika tekniska lösningar, säkerställer standarder att dessa system kan kommunicera och interagera med varandra. Detta är grundläggande för att skapa ett sammanhängande digitalt ekosystem, där data kan delas och tjänster integreras över plattformar och gränser. Utvecklare kan bygga på befintliga standarder för att skapa nya produkter och tjänster, vilket accelererar teknisk utveckling och främjar ekonomisk tillväxt. Standarder kan även hjälpa nya aktörer att komma in på marknaden genom att minska barriärer och göra det lättare att konkurrera med etablerade företag.

Standarder för digital säkerhet, såsom kryptering och autentisering, är avgörande för att skydda information och upprätthålla användarnas integritet. Genom att följa etablerade säkerhetsstandarder kan organisationer och individer minska risken för säkerhetsincidenter och skydda sig mot potentiella hot.

3.2 Genom standardiseringsprocessen samverkar olika intressenter (köpare, leverantörer och experter)

Myndigheter och organisationer som driver samhällsviktig eller säkerhetskänslig verksamhet upphandlar produkter och tjänster från marknaden. Upphandlarna har inte kompetens att själva till alla delar och i detalj beskriva de krav som har relevans för sina nätverks- och informationssystem eller för dess informations- och cybersäkerhet. Därmed behövs stöd för att kunna uttrycka dessa krav.

Leverantörerna å sin sida vill leverera på rättvisa villkor; de vill att andra leverantörer möter samma krav (så att konkurrensen inte snedvrids). De vill också utveckla produkter och tjänster som adresserar flera kunder på marknaden, nationellt såväl som internationellt, samtidigt (dvs. de vill undvika att ställas inför flera olika komplicerade kravsamlingar från olika kunder och marknader eftersom detta är kostnadsdrivande och minskar deras konkurrenskraft).

Genom standardiseringsprocessen kan båda dessa behov adresseras.

3.3 Exempel på IKT- och cyberrelaterad standardisering

Standarder är en förutsättning för att system från olika leverantörer ska kunna utbyta data och kommunicera med varandra, samt kunna tillämpa olika former av säkerhetsprotokoll som t.ex. medger kryptering.

Standarder (eller de facto-standarder) behövs för många olika kategorier av krav som specifikt har bäring på it-säkerheten, t.ex.:

- funktionella krav och säkerhetskrav vid design och implementation av datachips,
- kodningsregler vid programmering av mjukvara,
- hur produkter utvecklas till stöd för säkerhet (utvecklingsprocesser – Secure Development Life Cycle),
- funktionella- och säkerhetskrav på olika typer av mjukvaruprodukter,
- krypteringsalgoritmer och hur dessa kan tillämpas säkert,
- internets funktion, arkitektur och inbyggda (och ofullständiga) säkerhetsmekanismer och som produkter och system måste tillämpa,
- säker autentisering av användare och tjänster, digitala signaturer etc.,
- krav på funktion och säkerhet i kommunikationsprotokoll,
- olika typer av applikationer som operativsystem, brandväggar, webbservrar etc.,
- dataformat vid utbyte av information mellan olika delar av ett system, eller mellan system som interagerar,
- IKT-arkitekturer,
- olika typer av säkerhetsprinciper som ska tillämpas för olika användningsfall (t.ex. defence-in-depth och zero-trust),
- s.k. truststrukturer där säkerhetsfunktioner och associerade roller stämmer med de affärsmodeller som gäller för det specifika användningsfallet,
- hur system driftsätts och förvaltas,
- krav på kompetens hos de som designar, implementerar och driftsätter system,
- krav på hur övervakning av driftsatta system ska ske,
- krav på ledningssystem för informationssäkerhet i de organisationer som driver och ansvarar för systemen,
- hur incidenthantering och felrättning (patchning) ska hanteras internt i en organisation, samt för hur leverantörer av produkter, system och tjänster samverkar med sina kunder,
- krav som anger vilken kvalitetssäkring (kontroller) som ska tillämpas inom respektive kategori av ovan angivna standarder,
- krav på kompetens och förmåga hos de som ska genomföra kontrollerna och hur dessa kompetenskrav verifieras,
- hur den ansvariga ledningen ger ett givet system driftsgodkännande (s.k. systemackreditering),
- hur de organisationer som får genomföra vissa typer av kontrollerna ska godkännas (kompetensackreditering).

Olika it-system är beroende av olika kombinationer av ovan kategorier av standarder. Till exempel leder olika varianter av molntjänster till beroenden av olika kombinationer av standarder, medan telekom och 5G-system är ett annat fall som leder till beroenden av delvis andra standarder.

Det är en stor grupp av organisationer som utvecklar standarder av de slag som exemplifieras ovan. Normalt skiljer man mellan formell standardisering, dvs. standardiseringsorgan som arbetar i enlighet med internationella handelspolitiska principer och de facto-standardisering dvs. privata standarder som ofta tas fram på begränsat tillämpningsområde och bland mindre antal aktörer/intressenter).

I de fall standarder inte tas fram enligt handelspolitiska principer i öppna och transparenta processer kan eventuella handelshinder som t.ex, svenska företag kan mötas av, inte lösas genom de formella processer som etablerats inom ramen för WTO.

Några exempel på standardiseringsorgan listas i senare avsnitt. En del organisationer jobbar bara med en specifik fråga (t.ex. kryptografi), andra jobbar inom ett flertal av ovan kategorier (t.ex. ISO/IEC). Det finns organisationer som fokuserar på olika tillämpningsfall (t.ex. 3GPP, ETSI och Cloud Security Alliance) och som refererar till egna och andra standarder inom flera av ovan kategorier. Samverkan mellan standardiseringsorgan och de facto-standardiseringsorgan är vanligt förekommande, för att undvika dubbelarbete och för att tillse att de olika standarderna kan användas tillsammans.

I kapitel 2 i Union Rolling Work Programme for European cybersecurity certification (URWP)[6] beskrivs cybersäkerhetscertifieringsramverkets strategiska prioriteringar. Standardisering är där det första som tas upp och det beskrivs att ”Rolling Plan for ICT Standardisation” och ”Annual Union Work Programme for European standardisation” är lämpliga instrument för att signalera standardiseringsbehov för cybersäkerhetsaktens certifieringsordningar. Referenser görs i detta sammanhang särskilt till att kommande standarder för eIDAS2 och Cyberresiliensakten bör beaktas i eventuella framtida certifieringsordningar på detta område.

I ”Bilaga 5 - Exempel på standardsorgan och de facto-organ inom cyberområdet” redovisas exempel på tongivande standardiseringsorgan och de facto-standardiserngsorgan som utvecklar standarder och tekniska specifikationer som är av direkt eller indirekt relevans för cybersäkerhetsaktens certifieringsordningar.

De resulterande standarderna refererar frekvent varandra. Tillsammans bildar alla dessa olika organisationer och standarder ett mycket omfattande och komplext ”eko-system” där de i olika kombinationer och varianter utgör förutsättningen för de digitala system som används i hela världen. Standarderna är i ständig förändring. Verksamhetsutövare och sektorsmyndigheter behöver ständigt bevaka utvecklingen för att kunna bedöma hur det påverkar den egna verksamheten och/eller sektorn.

3.4 Standardisering är en säkerhetsåtgärd i sig

Att produkter och tjänster är utbytbara är en förutsättning för fungerande konkurrens. Det är även en viktig säkerhetsegenskap. Om t.ex. förtroende för säkerheten sviktar för en enskild produkt eller tjänst, t.ex. p.g.a. incidenter eller misstankar om otillbörlig påverkan från statsaktörer, är det av fundamental betydelse att sådana produkter och tjänster är utbytbara.

Väl utformade standarder och certifieringsordningar som är till stöd för svenska behov är därmed av mycket stor betydelse för både näringslivet (i egenskap av

[6] Union Rolling Work Programme for European cybersecurity certification | Shaping Europe’s digital future (europa.eu)

konsument och leverantör), för myndigheter (i egenskap av konsument och sektors- och tillsynsmyndigheter) och lagstiftaren.

3.5 Standardisering – konsekvenser av bristande samordning och öppenhet

Företag behöver anpassa sina produkter och tjänster för att möta olika nationella eller regionala standarder. Detta kan innebära olika versioner av en IKT-produkt eller - tjänst, vilket i sin tur kan öka kostnaderna genom behovet av olika anpassningar av produktionslinjer eller specialanpassade komponenter. Detta är inte minst relevant om och när olika marknader utvecklar lokala krav på cybersäkerhet. För varje marknad som har unika krav och standarder måste ofta produkterna genomgå testning och certifiering för att verifiera att de uppfyller dessa krav. Detta är en tidskrävande och kostsam process, särskilt när företag måste upprepa processen för flera marknader. Fragmentering av standarderna kan begränsa företagens tillgång till vissa marknader och vara särskilt problematisk för små och medelstora företag som kanske inte har resurser att anpassa sig till många olika standarder. En fragmenterad standardisering kan leda till utmaningar för intressenter att hitta rätt standard.

En viktig aspekt för alla intressenter (både användare och leverantörer) är att standarder utvecklas så att dessa intressenter har tillgång till standardiseringsprocessen och därmed har möjlighet att både påverka kraven och hur efterlevnad mot dessa krav kan utvärderas (t.ex. via certifiering). Denna möjlighet att påverka är en viktig aspekt både för leverantörerna och för användarna.

Myndigheterna har en viktig roll att säkerställa att centrala risker tas i beaktande vid utformning av standarder, men också att de krav som standarderna ställs kan kontrolleras vid t.ex tillsyn eller certifiering. Myndigheternas deltagande är därför mycket viktig i standardiseringen. Detta förutsätter självklart att standarderna utvecklas på ett sådant sätt att inte minst svenska myndigheter har tillträde till arbetet.

När standarder utvecklas utan insyn eller deltagande från alla relevanta intressenter, kan viktiga innovationer eller säkerhetsmässiga aspekter som skulle kunna göra dem mer effektiva och användbara komma att utlämnas. Brist på öppenhet i standardiseringsprocessen kan lättare leda till att standarder gynnar vissa företag eller teknologier (och i förlängningen: länder) på bekostnad av andra, vilket skapar orättvisa konkurrensförhållanden. Om de som förväntas tillämpa standarderna inte deltagit i deras utveckling kan det leda till bristande förståelse eller t.o.m. misstroende mot standarden, vilket minskar sannolikheten för att industrin som helhet accepterar eller använder den. Detta underminerar standardens värde, som ligger i dess breda acceptans och användning. Det senare är inte minst relevant för standarder som rör IKT och tillhörande cybersäkerhet.

För att hantera dessa utmaningar finns som ovan nämnt det principer och förhållningsregler inom Världshandelsorganisationen med syfte att verka för en harmonisering av tekniska regler (tekniska föreskrifter, standarder och krav på bedömning av överensstämmelse (provning och certifiering) på global nivå som förordar en öppen och inkluderande process för utveckling av standarder.

3.6 Tekniska handelshinder och WTO-TBT

Tekniska handelshinder (eng. ”Technical barriers to trade”) är hinder som tillverkare och leverantörer möter vid mellanstatlig handel genom att varor eller tjänster vid import måste anpassas till obefogade eller omotiverade nationella särkrav på varor som kan finnas i lagar, föreskrifter, standarder och inklusive krav på provnings- och kontrollförfaranden. Den inhemska industrin anpassar sig i första hand till det egna handelsområdets regler och möter därför svårigheter vid export till andra länder som har avvikande regler med t.ex. certifiering som baseras på andra krav än vad som ställts på det egna handelsområdet.

Om det dessutom är flera länder som är intressanta för landets industri att idka handel med, och dessa i sin tur har olika tekniska regler sinsemellan, blir företagens svårigheter mycket stora eftersom det är behäftat med stora kostnader att samtidig uppfylla krav (t.ex. med hjälp av certifiering) från flera länders och handelsområdens olika regleringar och krav.

Världshandelsorganisationens (WTO) avtal om tekniska handelshinder (TBT-avtalet) säger att medlemmarna, när det finns behov av tekniska föreskrifter eller standarder och det finns relevanta internationella standarder, ska använda dessa som grundval.

Syftet är att standarder ska fungera lika överallt (globala standarder). De befintliga handelspolitiska regelverken är till för att definiera vad som konstituerar en standard samt hur standarderna ska utarbetas, fastställas och tillämpas för att inte skapa onödiga handelshinder.

3.7 Världshandelsorganisationens avtal om tekniska handelshinder

WTO:s TBT-avtal inkluderar en uppförandekod för utarbetande, fastställande och tillämpning av standarder (Code of Good Practice) som riktar sig till alla standardiseringsorgan (statliga, lokala som icke-statliga och regionala) som utvecklar standarder[7]. Denna kod syftar till att säkerställa att processen för att skapa tekniska standarder är öppen, transparent och främjar internationell handel för att att förebygga och avveckla onödiga handelshinder.

Uppförandekoden förordar att standardiseringsprocessen är öppen och transparent. Detta innebär att alla relevanta parter, inklusive utländska intressenter, ska ha möjlighet att delta i standardiseringsprocessen. Genom att föreskriva att utkast till standarder ska offentliggöras och att intressenter ska ges tillräckligt med tid för att lämna kommentarer, säkerställer kodexen att processen är inkluderande och rättvis.

Uppförandekoden eftersträvar också oberoende, effektivitet, ekvivalens och beaktande av utvecklingsländer i syfte att förebygga onödiga handelshinder. Detta uppnås genom att uppmuntra till att kravställning av varor, så långt det går, baseras på internationella standarder när sådana finns tillgängliga och är lämpliga. Genom att

[7] De organ som har anslutit sig till eller frånträtt uppförandekoden ska anmäla detta till ISO/IEC Information Centre i Geneve.

harmonisera nationella standarder med internationella standarder minskas risken för att olika länder har inkompatibla krav som kan hindra handeln eller (t.ex) digital interoperabilitet.

Tekniska regler bör utarbetas, fastställas och tillämpas på vetenskaplig grund..

Förutom uppförandekoden innehåller TBT-avtalet sedan ett beslut från år 2000 de så kallade sex principerna för utveckling av internationella standarder (se Artikel 2,5 och Bilaga 3 i avtalet).

Principerna betonar också vikten av att göra standarder lätt tillgängliga för alla intressenter,, bl.a. genom tidig publikation av nya standardiseringsprojekt, tidig notifiering av förslag till nya standarder samt ge andra medlemmar tid för att kommentera förslag till nya standarder.

3.8 Frivilliga standarder v.s. tekniska föreskrifter

Inom ramen för Världshandelsorganisationen (WTO) och särskilt när det gäller tekniska handelshinder, skiljer man mellan frivilliga standardarder och tekniska föreskrifter (bindande myndighetskrav). Dessa koncept är centrala för att förstå hur internationell handel fungerar och dess tämligen stora påverkan även på alla de standarder som berör IKT och/eller cybersäkerhet.

Kravställning på basis att standarder innebär att man använder tekniska specifikationer eller standarder som är utvecklade av standardiseringsorgan på frivillig basis. Dessa standarder kan gälla kvalitet, säkerhet, prestanda, miljöpåverkan och andra aspekter av produkter och tjänster. Frivilliga standarder syftar till att främja effektivitet och innovation, samtidigt som de underlättar internationell handel genom att skapa enhetliga krav som är erkända över landsgränser. Nyckeln till användning av en standard handlar om relevans. Ibland kan fler standarder vara relevanta.

Kravställning på basis av tekniska föreskrifter å andra sidan innebär att det finns lagar, förordningar eller andra myndighetsföreskrifter som ställer tvingande krav på produkter, tjänster eller produktionsprocesser och och måste följas av företag och individer. Syftet med reglering är ofta att skydda konsumenternas hälsa och säkerhet, miljön, eller att upprätthålla rättvisa handelspraktiker. I WTO:s TBT-avtal betonas vikten av att dessa regler inte skapar onödiga handelshinder och att de är transparenta, icke-diskriminerande och baserade på internationella standarder när så är möjligt[8].

TBT-avtalet uppmuntrar medlemsländerna att använda internationella standarder som grund för sina tekniska regleringar för att minska handelshinder. Det kräver också att medlemmar (inklusive EU) anmäler nya förslag tekniska föreskrifter till WTO för att säkerställa att de inte skapar onödiga hinder för internationell handel. Samtidigt erkänner avtalet medlemsländernas rätt att fastställa den skyddsnivå de anser lämplig.. Legitima regulativa mål är bland annat: nationella säkerhetskrav, förebyggande av vilseledande metoder, skydd av människors hälsa eller säkerhet,

[8] Många länder använder standarder (i saknad av tekniska föreskrifter) i kravställning och gör dem bindande. I sådana fall får dessa standarder status av teknisk föreskrift.

djurs eller växters liv eller hälsa, eller miljön. Just cybersäkerhetskrav på IKT motiveras ofta utifrån målet att adressera nationell säkerhet.

3.9 De facto-standardisering

Vid sidan av formell standardisering dvs. erkända organ som följer WTO:s principer finns det ett relativt stort antal andra organisationer som utvecklar standarder och tekniska specifikationer som är av stor betydelse för digitaliseringen. Dessa faller inom privat standardisering och kallas ibland de facto-standarder.

Standardsorgan (Standards Development Organisation – SDO) som följer WTO:s principer i TBT avatalet ska vara öppna för alla intressenter och har konsensusbaserad beslutsfattning vilket borgar för allas möjlighet till inflytande, inklusive svenska myndigheter och företag.

Andra organisationer som utvecklar standarder kan verka mer eller mindre öppet och inkluderande. Vissa organisationer som inte är öppet för samtliga intressenter kan ändå få stort genomslag och påverkan. Det är angeläget att cybersäkerhetsaktens certifieringsordningar enbart refererar standarder och tekniska specifikationer som utvecklats av organ som svenska företag, myndigheter och/eller akademi har tillträde till.

3.10 Standardiseringens roll inom EU

EU utvecklade 1985 ett system för harmonisering där standarder används som komplement till EU-lagstiftningen för att undvika allt för stora detaljkrav i lagstiftningen. Det nya sättet att reglera kallades Nya metoden (eng. ”New approach”). Företag kan genom att använda sig av harmoniserade europeiska standarder (förkortas hEN) visa att de uppfyller EU-lagstiftningens grundläggande krav.

EU:s lagstiftningsram för standardisering och ackreditering, innefattande förordning (EU) nr 1025/2012, förordning (EG) nr 765/2008, samt den Nya metoden, är en viktig del i hur standardisering används för att främja den inre marknaden.

Standardiseringsförordningen utgör grunden för hur europeiska standarder utvecklas och implementeras. Genom förordningen etableras de tre europiska standardsorganen CEN, CENELEC och ETSI, samt att dessa på uppdrag från EU-kommissionen kan ta fram s.k. harmoniserade standarder, som ska ge presumtion om efterlevnad i enlighet med relevanta EU-direktiv eller förordningar. I de områden som harmoniserad standard utvecklats på EU-nivå ska medlemsstaternas standardsorgan avveckla sina ev. överlappande nationella standarder.

Verifikation/Utvärdering huruvida en produkt/tjänst motsvarar krav i en standard kan genomföras av organ för bedömning av överensstämmelse som har ackrediterats (kompetensprövats) av respektive medlemsstats nationella ackrediteringsorgan. Dessa organ (certifieringsorgan, kontrollorgan eller laboratorier) som utför oberoende tredjeparts bedömning av varor enligt krav i EU:s direktiv och förordningar kallas anmälda organ och finns registrerade i Europeiska kommissionens NANDO-databas.

Denna databas övervägs även för att utgöra register över de organ för bedömning av överensstämmelse som bemyndigats att genomföra kontroller i enlighet med cybersäkerhetsakten.

3.11 Cybersäkerhetsfrågorna bidrar till ökad regionalisering och regelfragmentering

Cybersäkerhet är ett tekniskt komplext område som omfattar ett brett spektrum av teknologier, hot och försvarsmetoder. Att utveckla standarder som är tillämpliga över så många olika system och teknologier kan vara utmanande, särskilt när det gäller att hålla jämna steg med snabba tekniska förändringar och utveckling av nya hot. Länder och/eller företag som anser sig ha ett försprång i utvecklingen kan se goda skäl till varför man inte via tidigt deltagande i standardisering vill driva utvecklingen och därmed även konkurrenter framåt.

Flera av de mest tongivande standardiseringsorganen är internationella. Samtidigt finns en tendens inom EU att öka Europas ”digitala suveränitet” och som en följd av detta en drivkraft för utveckling av specifika europeiska standarder. Det finns behov av att på nationell nivå försöka skapa en inriktning för när Sverige ska sträva efter att internationell standard ska tillämpas i certifieringsordningar, och när det är motiverat att skapa regionala standarder som alltså kan utgöra Europiska särlösningar.

Cybersäkerhet är nära knutet till nationella säkerhetsintressen. Många länder kan vara ovilliga att anta internationella standarder som de anser kan kompromettera deras nationella säkerhet eller suveränitet. Risken för cyberangrepp måste ses som en del av den nationella säkerheten. Det rapporteras i stort sett dagligen om cyberangrepp som syftar till spionerі eller sabotage och där statsaktörer eller till sådana associerade organisationer ligger bakom. Det kan finnas betydande svårigheter (eller utmaningar) att samverka i internationell standardisering i en öppet forum där representanter från andra länder har skilda värderingar än västvärldens. Dels för att man helt enkelt inte mer än nödvändigt önskar via standarder vill bidra till detta länders utveckling, dels för att det principiellt är svårt att komma överens om säkerhetsåtgärder med deltagare som man misstänker samtidigt vill hitta svagheter i andra länders nätverks- och informationssystem.

Skillnader i politisk ideologi och strategi mellan länder kan skapa ytterligare hinder för internationell standardisering. Oenighet om hur cybersäkerhetsrisker ska hanteras, eller hur användarnas integritet och dataskydd ska balanseras mot behovet av säkerhet, kan försena eller förhindra antagandet av gemensamma standarder.

Frågan om vilka standarder som bör vara globala och vilka standarder som snarare bör vara regionala nära kopplat till säkerhetspolitiska överväganden, vilket är en utmaning för verksamhetsutövare eller sektorsmyndigheter att hantera på egen hand.

4 Cybersäkerhet

Försvarets materielverks bedömning:

För att kunna skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot omständigheter, händelser eller handlingar som kan skada, störa eller på annat sätt negativt påverka nätverks- och informationssystem, behövs en kombination av och samverkan mellan många olika kompetenser.

Arbetet förutsätter att det finns en god kännedom om tillämpningen för det specifika nätverks- och informationssystemet, verksamhetens mål och hur cybersäkerhetsrisker kan samverka med verksamhetens övriga hot och risker. Det förutsätter därutöver en god kännedom om de rättsliga förutsättningar som råder för den specifika tillämpningen samt en förmåga att bedöma vad de rättsliga kraven innebär för de administrativa och tekniska förhållanden som råder.

Det krävs mycket god kompetens om systemens tekniska funktioner och egenskaper för att kunna bedöma vilka hot, risker och sårbarheter som kan föreligga och för att kunna avgöra vilken kombination av åtgärder som kan vara ekonomiskt och verksamhetsmässigt effektiva.

Det krävs både en omfattande kunskap och erfarenhet för att behärska alla de olika kategorier av standarder som är relevanta och ligger till grund för dagens it- och kommunikationssystem, förstå hur de samverkar säkerhetsmässigt och vad det innebär för cyberriskerna i den specifika verksamheten.

Det behövs kompetens som kontinuerligt kan bevaka hur förändringar, t.ex. beträffande hotbild, teknikutveckling och utveckling av standarder kan påverka cybersäkerheten och de risker och kostnadseffekter förändringar kan medföra för den specifika verksamheten.

Det krävs kunskap om vilka kontroll- och verifieringsmetoder som är lämpliga, samt förståelse för när och hur certifiering enligt cybersäkerhetsakten är en lämplig metod samt vilka kompletterande kontroller som utöver certifieringen som kan behöva genomföras av den egna organisationen eller dess leverantörer.

En enskild verksamhetsutövare eller sektorsmyndighet kan behöva bevaka och/eller deltar i arbetet att utveckla relevanta standarder och certifieringsordningar i syfte att främja behoven för den specifika verksamheten eller sektorn.

Målsättningen för cybersäkerhetsäkerhetsarbetet, både för den enskilde verksamhetsutövaren och för sektormyndigheterna, torde vara att eftersträva den kombination av säkerhetsåtgärder, standarder och regler för kontroll (inklusive eventuell certifiering) där verksamhetsutövaren får de eftersträvade säkerhetsegenskaperna till så låg kostnad som möjligt.

4.1 Inledning

Cybersäkerhet definieras enligt cybersäkerhetsakten som ”all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot”. Cyberhot definieras i sin tur som ”en potentiell omständighet, händelse eller handling som kan skada, störa eller på

annat negativt sätt påverka nätverks- och informationssystem, användare [av] dessa system och andra personer".

Cybersäkerhet syftar därmed till att skydda datorer, nätverk, system och data från oönskade intrång, attacker och skadlig verksamhet. Det består av flera olika aktiviteter och kompetenser, som var och en, eller i kombination, mer eller mindre effektivt kan vara föremål för certifieringsverksamhet.

Framgångsrikt arbete med cybersäkerhet förutsätter förståelse för vilka hot och sårbarheter som finns och vilka åtgärder som kan vidtas för att minska risken för en incident och/eller dess konsekvenser. Det krävs mycket god kompetens om de tekniska systemens egenskaper för att kunna bedöma de risker som kan föreligga och för att avgöra vilken kombination av åtgärder som bör vidtas.

4.2 Vanliga orsaker till sårbarheter

För att förstå vilka åtgärder som kan behöva vidtas för att skydda ett system mot olika former av cyberhot kan det vara en lämplig utgångspunkt att förstå hur de olika bristerna ser ut som kan utnyttjas vid angrepp. Vanliga sårbarheter i it-system uppstår av olika anledningar och kan utnyttjas av angripare för att kompromettera säkerheten.

Både mjuk- och hårdvara (inklusive datachip) som fungerar funktionellt som avsett kan trots det innehålla konstruktioner eller brister som angripare kan utnyttja för att få obehörig åtkomst. Främst avseende mjukvara är detta en orsak till en stor mängd incidenter, men även datachip har varit behäftade med denna typ av sårbarheter som har haft omfattande och allvarliga konsekvenser (se t.ex. beskrivning av Spectre/Meltdown i senare avsnitt). Större datachip innehåller nära nog astronomiskt många tranistorer, delkomponenter och kopplingar. Att i efterhand hitta alla potentiella sårbarheter i dess konstruktion är i de flesta fall inte praktiskt möjligt.

Den ofantligt stora mängden kod (100-tals miljoner rader) som används i enskilda applikationer gör att kvarvarande sårbarheter kan vara mycket svåra att identifiera. Mängden programmerare som utvecklat koden, med varierande uppmärksamhet på kodens säkerhetskvalitet och mängden applikationer som nätverks- och informationssystem består av, gör det till en i praktiken likaledes omöjlig uppgift att hitta alla kvarvarande sårbarheter. Man måste därför anta att varje system innehar ett flertal mer eller mindre allvarliga sårbarheter, detta även efter rigorösa kontroller/certifiering.

Systemen byggs upp genom mycket omfattande anpassningar och konfigurationer av applikationer, servrar, nätverkskomponenter och säkerhetsrelaterade funktioner. En vanlig orsak till incidenter är att applikationerna inte har driftsatts med säkra konfigurationer, vilka därmed kan möjliggöra obehörig åtkomst. De system som är driftsatta är normalt kontinuerligt föremål för olika förändringar som gör att en given konfiguration som tidigare var "säker" kan bli orsak till nya sårbarheter i ett nytt sammanhang. Det kräver mycket hög kompetens och förståelse för det egna systemets inbördes beroenden och egenskaper för att se till att systemets konfigurationer inte öppnar upp för brister som kan utnyttjas av angripare.

De flesta applikationer i nätverks- och informationssystem är föremål för kontinuerlig utveckling med syftet att de ska förses med nya funktioner, effektivare exekvering, felrättningar och/eller fixade sårbarheter. Att ständigt hålla ett systems mjukvara uppdaterad (inklusive alla konfigurationer) med alla dess anslutna servrar, datorer, mobiltelefoner m.m. kan redan för system av ganska modest storlek vara en stor utmaning. I system där kravet dessutom är hög driftsäkerhet kan varje förändring innebära risk för introduktion av felfunktioner. I sådana fall kan det finnas en direkt motvilja mot att installera förändrade applikationer innan de genomgått mer eller mindre omfattande funktionstester för just den tillämpning som gäller i det specifika fallet. Under mer eller mindre lång tid kan ett system därför med avsikt köra gamla applikationer. Oavsett orsak leder ouppdaterade system frekvent till att kända sårbarheter finns kvar och utnyttjas av angripare.

Felaktig tilldelning eller oförsiktig hantering av användarbehörigheter till kritiska data eller systemresurser är även det en mycket vanlig orsak till sårbarheter. Bristande underhåll av gamla konton eller användare som slutar eller får nya arbetsuppgifter utan att de gamla behörigheterna tas bort, tillsammans med att de flesta användare tilldelas väldigt många behörigheter till många olika applikationer, bidrar till denna risk.

Ibland är alla funktioner på plats, korrekt konfigurerade och rätt tillämpade av all personal, men de valda skyddsåtgärderna ger ändå en otillräcklig skyddsnivå. I dessa fall är det bristande skyddet inte en följd av felfunktioner eller felaktig hantering, utan beror att de beslutade säkerhetsåtgärderna är otillräckliga.

Slutligen är användarna i sig en vanlig ingång för attacker. Användning av enkla lösenord som är lätta att gissa, eller lösenord som en angripare (med datorstöd) kan gissa och därmed använda för åtkomst till en användares konto och därifrån arbeta sig vidare in i systemet, underlättar för angripare. Ett många gånger effektivt sätt att motverka denna typ av attacker är s.k. tvåfaktorsautentisering, vilket innebär att användaren behöver styrka sin identitet och behörighet på två olika sätt, ofta dels genom ett lösenord, och dels genom tillgång till en fysisk ”nyckel” (dosa, smartkort, mobiltelefon etc.) som bara användaren har tillgång till. För angriparen räcker det inte att knäcka lösenordet utan att ha tillgång till den fysiska komponenten. Och om angriparen hittar eller stjäl den fysiska komponenten räcker inte det heller utan kännedom om lösenordet. Dock kan användare med starka lösenord eller tvåfaktorsautentisering falla offer för social manipulation (eng: ”social engineering”), luras att dela känslig information, eller luras att ladda ner t.ex. bilagor som innehåller skadlig kod. Olika former av attacker genom social manipulation är mycket vanlig, bl.a. på grund av att de är enkla i sitt genomförande och ofta mycket framgångsrika.

4.3 Exempel på sårbarheter/attacker

För att illustrera den stora variationen av olika sårbarheter, hur de kan utnyttjas i attacker och vilka konsekvenser de kan få, beskrivs i det följande några kända exempel.

Log4Shell (2021) tillåter en angripare att exekvera godtycklig kod på en sårbar server. Log4Shell var särskilt allvarlig p.g.a. dess breda användning i Java-applikationer

världen över, inklusive webbservrar, klientserver-applikationer och andra program som använder Log4j för loggning.

SolarWindshacken (2020) var en sofistikerad cyberattack som riktade sig mot den amerikanska federala regeringen och många stora teknikföretag. Angriparna komprometterade programvaran från SolarWinds, en leverantör av övervaknings- och nätverksadministrationsverktyg, och infekterade den med skadlig kod som användes för att få åtkomst till känslig information och system hos Solarwinds kunder som installerade företagets produkter.

NotPetyaattacken (2017) var en global cyberattack som spreds genom att utnyttja en sårbarhet i Microsoft Windows-operativsystemet. Attacken drabbade företag och organisationer över hela världen och orsakade betydande skador på it-system och affärsverksamhet. NotPetya anses vara en av de mest förödande ransomwareattackerna någonsin och orsakade miljarder dollar i skador.

Spectre och Meltdown (2017) möjliggjordes av en brist i designen av en stor mängd datachip. Sårbarheten innebär att dataläckage kan ske där t.ex. användarens lösenord, bilder, filer eller kryptonycklar läcker via minnet i datachippet till program som exekverar på samma datachip men som står under angriparens kontroll. Nästan alla användare av mobiltelefoner, persondatorer, servrar och molntjänster kan drabbas. Konsekvenserna av Meltdown och Spectre är omfattande eftersom de påverkar centrala hårdvarukomponenter i moderna datorsystem. De tvingade tillverkare och mjukvaruutvecklare att implementera skydd på både hårdvaru- och mjukvarunivå, vilket ofta ledde till prestandaförluster.

ROCA - Return of Coppersmith's Attack - (2017) var en allvarlig sårbarhet som upptäcktes i Infineons RSA-implementering, en populär algoritm för att generera kryptografiska nyckelpar. Sårbarheten gjorde det möjligt för angripare att beräkna den privata RSA-nyckeln från den offentliga nyckeln, vilket underminerade säkerheten i system som använde RSA-kryptering för att skydda känslig information. Den drabbade en bred uppsättning enheter och system, inklusive smartkort, digitala signaturer och krypterade kommunikationskanaler. ROCA-sårbarheten var ett allvarligt hot mot säkerheten och krävde en omfattande åtgärd för att åtgärda.

WannaCry-ransomwareattacken (2017) var en global ransomwareattack som drabbade hundratusentals datorer över hela världen. Attacken utnyttjade en sårbarhet i Windows operativsystem och innebar att angriparna krypterade filer på offrens datorer och krävde offren på lösensumma i utbyte mot återställning av filernas data. Attacken drabbade företag, sjukvårdsorganisationer och offentliga institutioner runt om i världen.

Equifax-dataintrånget (2017) innebar att Equifax, ett av de största kreditupplysningsföretagen i världen, drabbades av ett omfattande dataintrång där personlig information om cirka 147 miljoner människor stals. Angriparna utnyttjade en sårbarhet i Equifax webbapplikationer för att få åtkomst till känslig information, inklusive namn, adresser, kreditkortsnummer och personnummer.

Dyn-DDoS-attacken (2016) innebar att Dyn, en ledande leverantör av DNS-tjänster, drabbades av en massiv DDoS-attack som ledde till omfattande störningar på

internet. Attacken riktades mot Dyns infrastruktur och överbelastade deras servrar med en enorm mängd trafik, vilket resulterade i att många populära webbplatser och onlinetjänster blev otillgängliga för användare runt om i världen.

I *Sony Pictures*-hacket (2014) drabbades Sony Pictures Entertainment av en omfattande cyberattack där angriparna stals stora mängder känslig information, inklusive företagshemligheter, finansiella uppgifter och personlig korrespondens från högt uppsatta företagsledare.

Heartbleed-sårbarheten (2014) var en allvarlig sårbarhet i OpenSSL, en av de mest använda krypteringsbiblioteken på internet. Sårbarheten möjliggjorde för angripare att få åtkomst till känslig information, inklusive användarnamn, lösenord och krypterade kommunikationskanaler, från sårbara servrar.

I *Yahoo*-dataintrånget (2013–2014) drabbades Yahoo av ett massivt dataintrång där uppgifter från uppemot 3 miljarder användarkonton stals. Intrånget var ett av de största och mest omfattande i historien och innefattade personlig information som användarnamn, lösenord, e-postadresser och säkerhetsfrågor.

Target-dataintrånget (2013) innebar att Target Corporation, en av USA:s största detaljhandelskedjor, drabbades av ett dataintrång där uppgifter från cirka 40 miljoner kredit- och betalkort stals. Angriparna fick tillgång till systemen genom en tredjepartsleverantör och kunde sedan stjäla känslig betalningsinformation från Targets kassasystem.

Diginotar-incidenten(2011) innebar att infrastrukturen hos Diginotar, ett företag som utfärdade digitala certifikat för kryptering och autentisering av webbplatser, blev infiltrerad av okända angripare, vilket resulterade i att falska digitala certifikat utfärdades för flera högt profilerade webbplatser, inklusive Google, Yahoo och Microsoft. Angriparna använde dessa falska certifikat för att utföra så kallade "man-in-the-middle"-attacker, där de kunde avlyssna och manipulera kommunikationen mellan användare och de drabbade webbplatserna. Denna incident ledde till att Diginotar förlorade sitt förtroende som certifikatutfärdare och tvingades att gå i konkurs.

Stuxnet (2010) var en sofistikerad och målinriktad malware som utvecklades för att attackera och sabotera Irans kärnenergiprogram. Malwaren utnyttjade flera sårbarheter i Windows operativsystem och SCADA-system (supervisory control and data acquisition) för att infektera och styra industriella processer, vilket resulterade i skador på Irans kärnprogram.

4.4 Skydd mot antagonistiska hot är svårt

Skydd mot antagonistiska hot innebär unika utmaningar jämfört med traditionella metoder för skydd mot olyckor och felfunktion p.g.a. de fundamentalt olika naturerna hos de risker och hot som adresseras. Traditionell teknisk kontroll fokuserar främst på att hantera oavsiktliga fel och brister i produkter, processer och system, medan skydd mot antagonistiska hot därutöver även måste hantera medvetna och avsiktliga försök att utnyttja sårbarheter för skadliga ändamål.

Medan den som skyddar komplexa och omfattande närverks- och informationssystem med alla dess komponenter och användare i princip måste hitta alla sårbarheter i all hård- och mjukvara för att systemet inte ska vara möjligt att angripa, så måste angriparen bara hitta en fungerande angreppsväg. Angriparen har ofta tiden på sin sida, medan försvararen hela tiden måste hinna ikapp med utbildning av användare, arbete med systemkonfigurationer och annat säkerhetsarbete.

Antagonistiska hot utvecklas ständigt som svar på nya säkerhetsåtgärder. Angripare anpassar sina metoder och tekniker för att kringgå skydd, vilket skapar ett dynamiskt och ständigt föränderligt hotlandskap. Traditionella tekniska kontroller är ofta statiska, reaktiva och mest baserade på kända problem och fel. Skydd mot antagonistiska hot kräver istället en proaktiv inställning, där potentiella framtida hot och attacker måste förutses och förebyggas.

Angripare kan rikta in sig specifikt på kända sårbarheter eller använda sofistikerade metoder för att hitta nya sätt att penetrera skydd. Detta kräver en djup förståelse och analys av potentiella angreppsvektorer och vilka säkerhetsåtgärder som kan ge ett adekvat skydd. Skydd mot antagonistiska hot innebär även att risken från insiders kan behöva beaktas.

Skydd mot antagonistiska hot kräver att försvararen behöver ha kompetens att bedöma vilka angreppsvägar som den samlade gruppen av hotaktörer kan komma att finna och utnyttja. Detta innebär bl.a. specialiserad kunskap inom områden som kryptografi, nätverkssäkerhet, säker programmering, olika säkerhetsfrämjande arkitekturer, operativ drift och principer för övervakning. Dessa områden kan vara resurskrävande och kräver ständig uppdatering av kunskap och färdigheter i samma takt som angriparna utvecklar sina förmågor. Implementering och upprätthållande av effektiva säkerhetsåtgärder mot antagonistiska hot kan vara betydligt mer resurskrävande än traditionella tekniska kontroller. Detta inkluderar kostnader för säkerhetsteknologi, utbildning av personal och kontinuerlig säkerhetsgranskning.

Många cyberattacker involverar s.k. social manipulation som utnyttjar mänskliga beteenden snarare än tekniska sårbarheter. Detta skapar ytterligare utmaningar som sällan adresseras av traditionella tekniska kontroller, men som måste ingå i skyddsarbetet.

Cybersäkerhet baserad på förhoppningen om frånvaro av sårbarheter och från felkonfigurationer av enskilda produkter bedöms inte i de flesta fall vara en rimlig framgångsfaktor. I dessa fall finns istället behov av stöd för rimliga arkitekturer och krav på övervakning och respons som ger den säkerhet som behövs. Det finns behov av stöd som visar hur kombinationer av certifieringar av produkter, tjänster, utvecklingsprocesser, arkitekturer, övervakning och ledningssystem kan ge hög säkerhet till rimlig kostnad.

4.5 Olika kategorier av säkerhetsåtgärder

Cybersäkerhet är som framgår ett omfattande och mångfacetterat område som strävar efter att säkerställa att datorer, nätverk, system och data skyddas från oönskade intrång, attacker och skadlig verksamhet på internet. För att uppnå denna

önskade säkerhet krävs en kombination av olika åtgärder och strategier som arbetar tillsammans för att minimera risker och skydda mot cyberhot. De olika åtgärderna som vidtas för att skydda system kan delas in i några olika grundläggande kategorier. I det följande ges några viktiga exempel på kategorier av säkerhetsåtgärder.

Förebyggande åtgärder innefattar att vidta åtgärder för att förhindra att säkerhetsincidenter inträffar i första hand. Det kan inkludera att främja god kvalitet vid utveckling av applikationer (för att minska mängden sårbarheter), tillämpning av olika typer av säkerhetsarkitekturer och principer på systemnivå m.h.a. brandväggar, intrusionsskyddssystem (IPS), antivirusprogram, kryptering och säkerhetspolicyer som via flera lager av säkerhetsfunktioner försvårar angrepp, minskar effekten av enskilda sårbarheter och förhindrar obehörig åtkomst.

Detektion och övervakning innebär organisationer använder övervakningsverktyg för att upptäcka och identifiera potentiella hot och säkerhetsincidenter i realtid. Detekteringsåtgärder kan inkludera övervakning av nätverkstrafik, loggfiler, beteendeanalys och andra metoder för att identifiera avvikelser och misstänkta aktiviteter.

Reaktiva åtgärder består i att när en misstänkt säkerhetsincident inträffat agera snabbt för att begränsa skadorna och återställa normal drift. Detta kan innefatta att isolera infekterade system, blockera attacker, återställa data från säkerhetskopior och implementera nödåtgärder för att återställa systemets integritet och tillgänglighet. Om delar av systemen skadas, kan återställning av systemen och data m.h.a. backuper behöva genomföras. En del i de reaktiva åtgärderna kan även vara nödrutiner och lösningar som ingår i så kallad konuitetshantering. Dessa lösningar används tills återställningen är gjord. Detta eftersom vid komplexa system och sofistikerade attacker kan återställningen ta lång tid.

Utbildning och medvetenhet är en viktig del av cybersäkerheten och inebär att man utbildar och höjer medvetenheten bland användare och personal om cyberhot och bästa praxis för att skydda sig mot dem. Det innebär att erbjuda utbildning och träning för att lära användare hur de kan identifiera och undvika vanliga cyberattacker, såsom phishing, malware och social engineering.

Organisationer bör etablera tydliga och robusta *säkerhetspolicyer och förfaranden* för att vägleda användare och personal i säkerhetsfrågor. Detta kan inkludera regler för lösenordskomplexitet, åtkomsthantering, användning av företagsresurser och reaktion på säkerhetsincidenter.

Vart och ett av ovan områden består i sig av ett stort antal olika säkerhetsåtgärder som beroende på omständigheterna kan vara lämpliga att tillämpa. Genom att kombinera olika åtgärder inom ovan kategorier kan organisationer skapa ett cybersäkerhetsprogram med införda säkerhetsåtgärder som står i balans med de värden som ska skyddas. Det finns dock alltid en reell risk för mer eller mindre framgångsrika attacker. Risk för allvarliga incidenter måste ingå i beredskapen och en god förmåga att upptäcka och hantera attacker är mycket viktig.

4.6 Val av säkerhetsåtgärder, ansvarstagande och ”säkra system”

Syftet med cybersäkerhetsarbetet är att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot. Men som framgår är det i det generella fallet inte möjligt att vare sig definiera eller verifiera en serie säkerhetsåtgärder för ett givet system, som innebär att systemet fortfarande inte är sårbart.

Cyberområdets komplexitet gör att det till skillnad från många andra områden är mycket svårt att etablera en tydlig, gemensam uppfattning om vilka åtgärder det är som måste etableras för att ge ett tillräckligt skydd i en given situation.

Vad som utgör en ”tillräcklig” lista av säkerhetsåtgärder är i högsta grad subjektivt och beror på en rad faktorer. En verksamhetsutövare har därmed i uppgift att göra en bedömning av vilka olika säkerhetsåtgärder som ska genomföras. Denna bedömning kan utgå från verksamheten, hotbilden, vilken riskvillighet som finns, rättsliga krav, krav som etablerats via avtal eller kunders förväntningar etc. Alla dessa aspekter varierar för olika organisationer. I slutändan leder arbetet till genomförandet av en serie säkerhetsåtgärder. Men även i det skedet kan systemet antas innehålla mer eller mindre allvarliga sårbarheter (se exemplen i tidigare avsnitt).

Det är en viktig del av välordnat säkerhetsarbete att de som ansvarar för organisationen, dess ekonomi och resultat, är de som ytterst ansvarar för den valda ambitionsnivån och tillser att den upprätthålls.

I denna bemärkelse kan alltså ett säkert system sägas vara ett system där den som är verksamhetsansvarig har tillsett att det genomförts en bra och kompetent analys av verksamheten, dess hot och risker, rättsliga krav etc., infört beslutade säkerhetsåtgärder, verifierat att dessa är korrekt införda och därefter bär ansvar för de incidenter som därefter ändå inträffar.

En annan aktör (tillsynsmyndighet, rättsinstans, oberoende expert etc.) kan naturligtvis göra en annan bedömning och komma fram till en annan slutsats än den ansvarige verksamhetsutövaren. Detta p.g.a. nätverks- och informationssystems inneboende komplexitet, olika kompetens och riskvillighet, olika kunskap om hot och potentiella attackvägar samt cybersäkerhetsområdets allmänna snabba utveckling.

Det är därmed en utmaning att etablera en harmoniserad och tydlig beskrivning av vad som egentligen avses med ett ”säkert system” eftersom systemen är så komplexa, hotbilden snabbt föränderlig och att det är svårt att etablera regler som tolkas lika av olika personer och organisationer.

4.7 Cybersäkerhet förutsätter kontroll och verifiering

Inom säkerhetsområdet räcker det inte med att ha en strategi för vilka säkerhetsåtgärder som ska införas. Det är av fundamental betydelse att de säkerhetsegenskaper som ett system är designat för också kan kontrolleras och verifieras. Det krävs en genomtänkt, sammansatt strategi för vilka kontroller som ska genomföras av ledningsystemet för informationssäkerhet, de tekniska systemens

arkitektur med ingående komponenter, använda tjänster och personalens kompetens. Eftersom komponenter, system och personal mer eller mindre kontinuerligt förändras behöver denna kontrollstrategi utformas så att den upprätthåller kvalitet och säkerhet över tiden. System som saknar en sådan genomförd kontrollstrategi kan inte anses vara säkra - ”no security without control”.

Ett system som ska användas för ett givet område behöver därför omfattas av en kontrollstrategi, dvs. principer och planer för hur systemet, dess komponenter och personalen kompetens (och i förekommande fall tillförlitlighet). En väldefinierad kontrollstrategi borgar för att de olika åtgärderna och kontrollerna sammantaget ger det skydd som eftersträvas.

Certifiering enligt någon av cybersäkerhetsaktens ordningar, kan vara verktyg i den processen, men certifiering fråntar inte verksamhetsutövaren ansvaret för att känna till det egna systemets alla olika delar och vilka kontroller som bör genomföras.

Vanligtvis räcker inte certifieringen i sig. Ytterligare kontroller av det färdiga systemet måste genomföras, dels för att certifiering inte omfattar alla kontroller som kan behövas för ett system, dels för att kontrollerna måste anpassas till det specifika systemet och dess förutsättningar.

Kontroller kan ske på olika sätt bl.a.:

- Leverantörernas egenkontroller
- Oberoende tredjepartsgranskning (t.ex. certifiering)
- Verksamhetsutövarens egna kontroller
- Myndigheters tillsyn.

Ofta (inte alltid) är det svårigheterna att kontrollera som leder till utmaningar. Det är t.ex. oerhört svårt (omöjligt i de flesta praktiska fall) att kontrollera att det inte finns kvarvarande sårbarheter i en produkt eller i ett system. Svårigheten att via kontroller hitta varje brist som kan leda till sårbarheter på en nivå kan leda till behov av andra, kompletterande säkerhetsåtgärder på en annan nivå. Svårigheterna med att etablera en genomförbar och effektiv kontrollstrategi på komponentnivå kan ha en direkt påverkan på behovet av nya och tillkommande säkerhetsåtgärder med t.ex. krav på arkitektur och driftövervakning och tillhörande kontroller på en annan nivå.

Vad som är lämplig kombination av säkerhetsåtgärder och tillhörande kontrollmetoder är olika för olika tillämpningsområden, beroende på de olika områdenas förutsättningar. Det varierar p g a många faktorer, t.ex. med vilken typ av kompetens som verksamhetsutövaren själv har (eller kan upphandla), möjliga attackvägar för ett givet system, ekonomiska förutsättningar, leveranstider, tillgängliga resurser, riskvillighet, gällande reglering etc.

Det är en stor utmaning för organisationer att etablera och upprätthålla all den IKT-kompetens, cybersäkerhetskompetens, kompetens om attackvägar och effektiva säkerhetsåtgärder, kompetens om standarder och de olika kontrollmetoder som man direkt eller indirekt är beroende av eller själv behöver tillämpa.

4.8 Cybersäkerhet och certifiering

Målsättningen med arbetet med cybersäkerhet kan sägas vara att säkra förmågan att skydda IKT-system och dess information, dess integritet samt att upprätthålla verksamhetsutövarens förmåga att driva sin verksamhet i enlighet med dess syfte och huvudmål. Trots förebyggande insatser, som välutbildade användare och härdade, segmenterade, pentestade system, kommer incidenter att inträffa. En del attacker kommer att lyckas. Därför behövs reservsystem samt rutiner för effektivt återställande av drabbade system.

Kontrollåtgärder bör införas så att det skapas en balans mellan åtgärdernas effekt på säkerheten och den totala kostnaden för kontroll av t.ex.

- datachippens säkerhetsegenskaper
- enskilda produkter och tillhörande assuransnivå (där hög assuransnivå är kostnadsdrivande utan att nödvändigtvis minskar effekten av kvarvarande sårbarheter)
- produkters utvecklingsprocess
- ledningssystem hos verksamhetsutövaren
- it-systemens säkerhetsarkitektur (zero trust, defence-in-depth)
- övervakning och förmåga att agera,
- incidenthantering och patchning.

Samtliga exempel i listan ovan är områden där certifiering kan vara mer eller mindre lämpligt. Vad som anses vara en väl motiverad balans i dessa olika områden ger grund för vilken typ av krav som är adekvata och när certifiering med fördel kan användas för att möta kraven.

Detta kan sedan styra sektorsmyndigheternas hållning inom cybersäkerhetsakten, både vad gäller fortsatt inriktning på de certifieringsordningar (och tillhörande standarder) som är under utveckling, och även skapa efterfrågan på sådana certifieringsordningar som skulle vara i Sveriges intresse, men som inte täcks av de nuvarande ordningarna. Detta kan också styra Sveriges hållning i förhandlingar rörande annan EU-lagstiftning än certifieringsordningarna.

4.9 Cybersäkerhetscertifiering är ett verktyg till stöd för verksamhetsutövare

Ett cybersäkerhetscertifikat representerar ett intyg från en tredje part att en produkt, tjänst eller organisation har genomgått vissa säkerhetskontroller och uppfyller specifika säkerhetsstandarder vid tidpunkten för bedömningen. Det är av central betydelse att förstå att värdet av ett sådant certifikat främst ligger i intygandet av att dessa kontroller har utförts, snarare än ett oberoende intyg om att produkten eller tjänsten är absolut säker eller lämplig för alla möjliga användningsområden.

De säkerhetskontroller som ett cybersäkerhetscertifikat baseras på kan vara omfattande och grundliga, men de är nödvändigtvis begränsade till de specifika kriterierna för den standard eller ramverk som certifieringen avser. Dessa kontroller

kan inte förutsäga eller täcka alla tänkbara säkerhetsutmaningar som en produkt eller tjänst kan stöta på i skiftande och specifika användningsmiljöer.

Cybersäkerhetshot utvecklas kontinuerligt, och en produkt eller tjänst som anses säker idag kan anses sårbar imorgon. Detta följer av att nya attacker och tekniker utvecklas eller av att sårbarheter som länge funnits i systemen upptäcks och blir kända. Ett certifikat visar att skydd funnits mot vissa attacker vid tidpunkten för certifieringen, men det garanterar inte att samtliga sårbarheter hittades eller att det finns skydd mot nya angreppssätt som utvecklas efter tidpunkten för certifiering.

Certifikatinnehavaren kan i enlighet med cybersäkerhetsakten hållas ansvarig för att produkten, tjänsten eller processen motsvarar de krav och kontroller som det specifika certifikatet representerar. Certifieringsorganet kan hållas ansvarigt för om de kontroller som åligger dem att göra inte blivit genomförda enligt certifieringsordningens regelverk.

Det är viktigt att poängtera att vare sig certifikatinnehavaren eller certifieringsorganet kan hållas ansvarigt för att en certifierad produkt eller tjänst är lämplig för ett givet ändamål i ett nätverks- eller informationssystem. Om en produkt eller tjänst är lämplig i en given situation kan enbart verksamhetsutövaren ansvara för.

Varje organisation har unika säkerhetsbehov baserade på hur produkten eller tjänsten används i det enskilda fallet, organisationens riskprofil, affärsmodell, regleringskrav och andra faktorer. En produkt eller tjänst som är certifierad kan vara lämplig i en kontext men olämplig i en annan, beroende på de specifika säkerhetsriskerna och kraven i den miljön.

Att förstå de underliggande kontrollerna som genomförs vid en certifiering och deras relevans för den egna organisationens säkerhetsbehov är avgörande för att effektivt använda cybersäkerhetscertifikat som en del av ett riskbaserat säkerhetsarbete. Användare av certifikatet måste:

- förstå vilka säkerhetskontroller och standarder certifieringen baseras på och hur dessa relaterar till de egna säkerhetskraven,
- utvärdera hur väl certifieringens omfattning och de testade säkerhetsaspekterna överensstämmer med de egna riskerna och säkerhetsbehoven,
- använda certifieringen som en del av en större säkerhetsstrategi, och vid behov implementera ytterligare säkerhetsåtgärder för att adressera områden som inte täcks av certifieringen.

I slutändan är cybersäkerhetscertifikat värdefulla verktyg som kan bidra till en organisations riskhanteringsprocess, men de ska ses som en del av en större helhet snarare än en fullständig lösning i sig på en verksamhetsutövares cybersäkerhetsutmaningar. En djup förståelse för de underliggande kontrollerna och en kritisk bedömning av certifikatets relevans för de egna behoven är nödvändig.

5 Cybersäkerhetscertifiering

Försvarets materielverks bedömning:

Ett cybersäkerhetscertifikat som utfärdas av en behörig organisation utgör ett intyg om att kontroller av krav eller egenskaper på en produkt, tjänst eller process har prövats i enlighet med en överenskommen metod, av en organisation som bedömts vara kompetent att genomföra dessa kontroller. De krav på egenskaper som ställs på produkten, tjänsten eller processen, liksom den metod för hur kontrollerna ska genomföras, samt kompetenskraven på den som genomför kontrollerna utrycks oftast via standarder. Certifieringsordningen och de standarder som refereras, utgör tillsammans de krav som ställs på en certifierad produkt, tjänst eller process, samt på de organ för bedömning av överensstämmelse som genomför kontrollerna.

Certifiering kan tillämpas för många olika aspekter inom cyberområdet.

Certifiering av it-produkters cybersäkerhetsegenskaper innebär att produkternas förmåga att upprätthålla informationssäkerhet granskas och bedöms mot etablerade standarder.

Certifiering av s.k. säkra utvecklingsprocesser (eng; ”Secure Development Lifecycle”, SDL), syftar till att hjälpa utvecklare att skapa säkrare programvara genom att integrera säkerhetstänkande och åtgärder i alla faser av programvarans utvecklingscykel.

Certifiering av ledningsystem innebär att ett standardiserat arbetssätt tillämpas för att bedöma en verksamhets olika risker och de åtgärder som bör vidtas.

Bland fördelarna med certifiering kan nämnas att det kan leda till betydligt fler certifieringar än vad certifieringskapaciteten hos en enskild medlemsstat kan åstadkomma. EU-gemensam certifiering är dessutom mer fördelaktigt för leverantörer jämfört med alternativet att genomgå olika certifieringar i respektive medlemsstat. Leverantören får lägre kostnader och sparar mycket tid. EU-certifikat kan, för det fall certifiering krävs för marknadstillträde, ge svenska leverantörer tillgång till en större EU-marknad än vad enskilda nationella certifikat kan ge, eftersom nationell certifiering oftast måste genomföras i respektive land.

Samtidigt finns det flera utmaningar med certifiering av cybersäkerhet. Som en konsekvens av hur IKT-produkter och system är uppbyggda är det inte tekniskt eller resursmässigt möjligt att genom certifiering hitta varje tänkbar sårbarhet. Samtidigt är det just behovet av frånvaro av sårbarheter som är det centrala behovet som efterfrågas. Certifiering kan inte heller ”kontrollera fram” säkerhet i produkter eller tjänster när det råder bristande tilltro till leverantören. Även leverantörer med mer eller mindre illasinnade avsikter kan uppfylla kraven som ställs i certifieringsordningarna. En övertro till värdet av certifieringar, framför allt avseende frånvaro av kvarvarande sårbarheter, kan leda till felaktiga riskhanteringsbeslut hos användare. Processen att utveckla certifieringsordningar och refererade standarder, och processen att certifiera enskilda produkter eller tjänster, långsam och kostnadsdrivande.

Sektorsmyndigheters och verksamhetsutövares förmåga att identifiera behov av cybersäkerhet som kan adresseras av EU:s certifieringordningar förutsätter stor kompetens om IKT, cybersäkerhet, standardisering och principer för teknisk kontroll.

Sådan kompetens är en förutsättning för att certifiering används som instrument endast när så är lämpligt, och att andra alternativa kontrollmetoder annars väljs och tillämpas.

5.1 Allmänna principer för teknisk kontroll

Teknisk kontroll innefattar inspektioner, testning och certifiering för att verifiera att produkter, tjänster och system uppfyller utpekade standarder och andra lagstadgade krav. Syftet till att säkerställa säkerhet, kvalitet och prestanda, i vissa fall även andra typer av krav (avseende miljö, hållbarhet m.m.).

Teknisk kontroll bör baseras på standarder och tekniska specifikationer som klart definierar de krav som produkter eller tjänster måste uppfylla. Ramverket för teknisk kontroll ska ange hur den tekniska verifieringen ska utföras och kraven på de aktörer som genomför kontrollerna. De som utför teknisk kontroll måste vara tekniskt kvalificerade och ha relevant kunskap och erfarenhet. Det är även vanligt att det finns standarder som anger kompetenskrav hos den personal som genomför kontrollerna För att säkerställa att standarderna fortsätter att upprätthållas över tid kan det krävas regelbundna eller slumpmässiga inspektioner efter den initiala utvärderingen.

Ackreditering är processen genom vilken ett erkänt ackrediteringsorgan (i Sverige det nationella ackrediteringsorganet Swedac) intygar att ett organ för bedömning av överensstämmelse är kompetent att utföra specifika uppgifter. Dessa uppgifter kan inkludera testning, kalibrering, systemcertifiering och inspektion.

Ackreditering intygar att ackrediterade organ för bedömning av överensstämmelse har den tekniska kompetens och opartiskhet som krävs för att kontrollera produkters och tjänsters överensstämmelse med tillämpliga nationella och internationella standarder. I EU utförs ackreditering av nationella ackrediteringsorgan som utses av medlemsstaten i enlighet med förordning (EG) nr 765/2008.

De organ som söker ackreditering måste visa att de har nödvändig kompetens, inklusive utbildad personal, lämplig utrustning och metoder samt ett effektivt kvalitetsledningssystem. Ackrediterade organ ska vara oberoende och opartiska i sina utvärderingar. De ska inte ha något intresse i resultatet av deras utvärderingar förutom att säkerställa rättvisa och objektivitet gentemot de krav som anges i den underliggande standarden. Ackrediterade organ måste upprätthålla sekretessrörande information som erhållits under utvärderingsprocessen. Ackreditering kan inom vissa tillämpningsområden vara frivillig, medan den inom andra kan vara lagstadgad.

Inom cybersäkerhetsakten ska alla organ för bedömning av överensstämmelse vara ackrediterade. Inom cybersäkerhetsakten ska organ för kontroll av överensstämmelse även stå under tillsyn av den nationella myndigheten för cybersäkerhetscertifiering (NCCA). För certifieringar på assuransnivå ”Hög” ska organen dessutom bemyndigas av NCCA. Den senare ska även samverka med den nationell ackrediteringsmyndigheten.

För att främja att de olika standarderna tolkas på ett likvärdigt sätt och därmed att organ för kontroll av överensstämmelse kommer till likvärdiga slutsatser, kan s.k. peer review (inbördes kvalitetsgranskning mellan ackrediteringsorgan) tillämpas. Vid

sådan peer review granskar olika ackrediteringsorgan varandras verksamheter i syfte att nå ett likvärdigt resultat från de organ för kontroll av överensstämmelse som respektive ackrediteringsorgan ackrediterat. I vissa fall, t.ex. inom ramen för certifiering inom cybersäkerhetsakten, är det även möjligt att genomföra peer review direkt mellan organ för kontroll av överensstämmelse, samt mellan respektive nationell myndighet för cybersäkerhetscertifiering.

Två vanliga former av teknisk kontroll inom cybersäkerhet är evaluering, där en produkt eller tjänst genomgår t.ex. testning, inspektion, kalibrering i syfte att bedöma om kraven är uppfyllda, samt certifiering, vilket innebär ett intyg om att en evaluering skett på ett riktigt sätt och att resultatet överensstämmer med de krav som har ställts. Evaluering och certifiering sker normalt oberoende av varandra, dvs. de som genomförde evalueringen får inte delta i beslutet om att ge ut ett certifikat.

Genom att ackreditering av organ för kontroll av överensstämmelse baseras på samma eller likvärdiga standarder mellan olika nationella ackrediteringsorgan kan ett förtroendet etableras för att teknisk kontroll genomför av organ ackrediterat i ett land är likvärdigt kontrollerna i ett annat.

För ett givet område anger en certifieringsordning alla förutsättningar som gäller för vilka krav som gäller, vilka standarder eller tekniska specifikationer som ska tillämpas, hur kontroller ska ske, regler för hur ackreditering ska genomföras med t.ex. krav på kompetens hos den personal som ska genomföra evaluering, samt regler för hur konflikter mellan parterna ska hanteras.

Certifieringsordningen förvaltas av en ”ägare”, vilken inom för cybersäkerhetsakten kan sägas vara EU-kommissionen och medlemsstaterna som beslutar om reglerna via ett s.k. kommittologiförfarande. Själva certifieringsordningarna med regler och utpekade standarder och tekniska specifikationer materialiseras genom genomförandeakter.

5.2 Certifiering

Ett certifikat utgör ett intyg utfärdas av en behörig organisation om att kontroller att krav eller egenskaper på en produkt, tjänst eller process har prövats i enlighet med en överenskommen metod av en organisation som bedömts vara kompetent att genomföra dessa kontroller.

De krav eller egenskaper som ställs på produkten, tjänsten eller processen, liksom den metod för hur kontrollerna ska genomföras, samt kompetenskraven på den som genomför kontrollerna utrycks oftast via standarder:

- Standard(er) för att ange krav/egenskaper på produkten/tjänsten
- Standard(er) som anger hur kontrollerna av produkten/tjänsten ska genomföras
- Standard(er) som anger krav på den organisation som genomför kontrollerna
- Standard(er) som anger hur en organ för bedömning av överensstämmelse ska godkännas (ackrediteras).

Dessa standarder, refererade direkt eller indirekt via certifieringsordningen, utgör tillsammans de krav som ställs på en certifierad produkt, tjänst eller process, samt på de som genomför kontrollerna.

5.3 Olika typer av certifiering av cybersäkerhet

5.3.1 Cybersäkerhetscertifiering av it-produkter

Certifiering av it-produkters cybersäkerhetsegenskaper innebär att produkternas förmåga att upprätthålla informationssäkerhet granskas och bedöms mot etablerade standarder. Exempel på denna typ av certifiering är Common Criteria (ISO/IEC 15408) som ligger till grund för EUCC, och FIPS-140 som är en standard för certifiering av kryptomoduler.

Vid en sådan produktcertifiering granskas produktens förmåga att skydda mot obehörig åtkomst, förlust eller ändring av data. Detta inkluderar krav på autentisering, auktorisation, dataintegritet, konfidentialitet och spårbarhet. För vissa produkter, särskilt de som innehåller hårdvara, kan det finnas krav på fysiska säkerhetsåtgärder för att skydda mot fysisk manipulation eller dataläckage. Det kan finnas krav på säker utvecklingsprocess (se nedan), incident- och patchhantering och säkerhetsuppdateringar för att säkerställa att produkten förblir säker över tid. Krav på s.k. penetrationstestning är vanligt, dvs. testning för att aktivt söka och utnyttja säkerhetssvagheter i produkten för att bedöma dess motståndskraft mot attacker. Andra tester som vanligen ingår är s.k. funktionella tester, dvs. kontroller för att säkerställa att de säkerhetsfunktioner som specificeras faktiskt fungerar som avsett i olika användningsfall. Sökning efter kända sårbarheter i den källkod som ingår i produkten är vanligt förekommande.

Även efter en certifiering av en IT-produkt måste det antas att det kan finnas kvarvarande brister eller sårbarheter som kan utnyttjas för angrepp. Certifiering av it-produkter kan utgöra ett bra verktyg för att säkerställa att produktens säkerhetsfunktioner är korrekt implementerade och att produkten allmänt är utvecklad under kontrollerade former. Men det innebär inte att produkten är felfri. Verksamhetsutövare av nätverks- och informationssystem behöver förstå vad de enskilda certifikaten representerar, vilka kontroller som är gjorda, samt vilka andra kompletterande säkerhetsåtgärder som behöver göras på arkitektur- eller driftsnivå för att hantera risken för att återstående sårbarheter kan utnyttjas vid angrepp.

5.3.2 Certifiering enligt Ledningssystem för informationssäkerhet – ISO/IEC 27001

Ett ledningssystem för informationssäkerhet (LIS) utgör ett regelverk för hur en verksamhet systematiskt och över tiden organiserar arbetet med att skydda verksamhetens informationstillgångar. ISO/IEC 27001 är en internationell standard som specificerar krav för ledningssystem för informationssäkerhet (eng: ”Information Security Management System”, ISMS).

Certifiering enligt ISO/IEC 27001 innebär att ett oberoende ackrediterat certifieringsorgan har granskat organisationens ISMS och bekräftat att det uppfyller standardens krav. Certifieringsordningen som oftast tillämpas finns definierad i

ISO/IEC 27006. Tillämpning av dessa standarder är därmed ensad på global nivå. Att man uppfyller kraven (dvs. erhållit ett certifikat) innebär att det systematiska säkerhetsarbetet finns på plats. Ett certifikat innebär i sig dock inte nödvändigtvis att säkerheten i organisationens system allmänt kan sägas vara tillräcklig eller adekvat i alla avseenden (sic).

ISO/IEC 27001 innebär att riskhantering är den systematiska grunden. Standarden ställer krav på att verksamheten ska identifiera, bedöma och hantera informationssäkerhetsrisker. Organisationer ska genomföra regelbundna riskbedömningar för att identifiera t.ex. hot och sårbarheter som kan påverka deras informationstillgångar och baserat på dessa implementera lämpliga säkerhetsåtgärder. Exakt vilka säkerhetsåtgärder som måste införas är dock inte hårt styrt, utan valet av åtgärder ska följa organisationens egen policy för riskbedömning. ISO/IEC 27001 anger dock att verksamheten ska övervaka och revidera sina säkerhetsåtgärder för att säkerställa att de förblir effektiva över tid. Högsta ledningen för verksamheten ska tillhandahålla nödvändiga resurser, definiera säkerhetspolicyn och säkerställa att säkerhetsmålen är i linje med organisationens övergripande verksamhetsmål. Standarden anger att fysisk säkerhet, HR-processer, it-infrastruktur och organisatoriska säkerhetsåtgärder såsom hantering av underleverantörer beaktas vid utformningen av ledningssystemet. Genom att följa standardens krav på regelbunden rapportering av riskstatus och riskbehandlingsplaner till högsta ledningen, kan organisationer systematiskt identifiera och hantera säkerhetsrisker, vilket möjliggör ett informerat beslutsfattande.

Certifiering enligt ISO/IEC 27001 innebär att det finns en ledningsstyrd arbetsprocess och ett arbetssätt för att bedöma verksamhetens olika risker som stämmer med standardens krav.

Dock kan olika organisationer som har erhållit en certifiering enligt ISO/IEC 27001, beroende på kompetens, förståelse för it-systemens risker, kunskap om aktuell hotbild, resurstilldelning, ledningens riskvillighet och många andra faktorer etablera nätverks- och informationssystem med mycket varierande mängd säkerhetsåtgärder och varierande faktiskt skydd. Syftet med ISO/IEC 27001 kan snarare sägas vara att etablera en upptäckande och förbättrande process, snarare än att alla verksamheter som erhållit ISO/IEC 27001 certifiering ska ha en likartad nivå av faktiskt säkerhet.

5.3.3 Certifiering av säkra utvecklingsprocesser

Säkra utvecklingsprocesser (eng; ”Secure Development Lifecycle”, SDL) syftar till att hjälpa utvecklare att skapa säkrare programvara och att minska risken för säkerhetsbrister och angrepp. SDL-processen fokuserar på att integrera säkerhetstänkande och -åtgärder i alla faser av programvaruutvecklingscykeln.

Inom ramen för en SDL-process definieras säkerhetskrav och policyer tidigt i utvecklingsprocessen. Under designfasen analyseras och modelleras säkerhetsrisker genom metoder som hotmodellering, vilket hjälper till att identifiera och mitigera potentiella säkerhetsproblem innan kodning börjar. SDL kan inkludera riktlinjer och bästa praxis för säker kodning för att minska antalet säkerhetsbrister i koden införda av enskilda programmerare. Utvecklare uppmuntras att använda säkra

programmeringstekniker och verktyg som kan identifiera säkerhetsproblem. I slutfasen ingår säkerhetstestning, inklusive statisk och dynamisk kodanalys, fuzzing och penetrationstestning för att identifiera och åtgärda säkerhetsbrister innan programvaran släpps. Säkerhetsgranskning av kod och arkitektur utförs regelbundet av grupper av erfarna utvecklare för att säkerställa att säkerhetskrav och standarder upprätthålls genom hela utvecklingscykeln. En plan för säkerhetsincidenthantering tas fram för att snabbt kunna hantera och åtgärda säkerhetsproblem som upptäcks efter att programvaran har släppts. Utbildning och medvetenhet om säkerhet för utvecklingsteamet är en central del av SDL. Detta säkerställer att teamet är väl förberett för att integrera säkerhet i sitt arbete.

5.3.4 Hybrider av certifiering av produkt/tjänst/process/ledningssystem

De certifieringsprinciper som redovisats i föregående avsnitt är oftast kombinerade inom en och samma standard eller certifieringsordning.

Till exempel omfattar EUCC både krav på själva produkten (produktcertifiering), såväl som krav på hur produkten utvecklas (processcertifiering), samt hur det fysiska skyddet av de it-system och de lokaler där utvecklingen pågår ska vara beskaffat (vilket delvis kan sägas överlappa regler för certifiering av ledningssystem).

Den föreslagna certifieringsordningen för 5G (EU5G) är ett exempel på när två olika typer av certifiering (produkt och process) ingår i certifieringsordningen, jfr. avsnitt 6.16.

5.4 Certifiering av cybersäkerhet – Fördelar och styrkor

EU-gemensam certifiering kan leda till betydligt fler certifieringar än certifieringskapaciteten hos en enskild medlemsstat. Genom cybersäkerhetsakten blir kapaciteten potentiellt den sammanlagda förmågan att certifiera hos alla certifieringsorgan i hela EU, att jämföra med ett enskilt lands förmåga att certifiera gentemot ett nationellt regelverk. Detta är en av cybersäkerhetsaktens största fördelar.

EU-gemensam certifiering är mycket fördelaktigt för leverantörer jämfört med alternativet att genomgå olika certifieringar i respektive medlemsstat. Leverantören får lägre kostnader och sparar mycket tid.

EU-gemensamma certifikat kan, i de fall certifiering är tvingande, ge svenska leverantörer tillgång till större (EU-)marknad, än vad enskilda nationella certifikat kan ge, eftersom nationell certifiering oftast måste genomföras av leverantören i respektive land.

I de fall certifiering efterfrågas kan verksamhetsutövare lättare få tillgång till större urval av leverantörer som kan möta kravet, samtidigt som verksamhetsutövaren kan få lättare att förstå värdet av certifikaten (jämfört med olika nationella certifieringar).

Certifieringsordningarna kan, rätt utformade, leda till jämnare villkor för leverantörer inom hela EU.

EU:s certifieringsordningar kan bli ett verktyg som gör det möjligt för svenska intressenter att påverka och styra leverantörer som verkar inom både EU:s inre

marknad och på den globala marknaden på ett sätt som annars inte skulle kunna vara möjligt.

EU-gemensam certifiering och de underlag som produceras i samband med en certifiering kan utgöra ett viktigt stöd för både verksamhetsutövare och leverantörer.

För verksamhetsutövare och leverantörer som saknar egen kompetens eller förmåga på området, kan EU-certifiering kan ge ett mycket bra stöd att kontrollera produkters och tjänsters säkerhetsegenskaper.

Väl utformade certifieringsordningar kan leda till IKT-produkter, tjänster och/eller -processer med kända egenskaper som utgör värdefulla underlag i verksamhetsutövares och tillsynsmyndigheters arbete att bedöma risker, regelefterlevnad och eventuella behov av kompletterande säkerhetsåtgärder.

Väl utformade krav på cybersäkerhet genom EU:s certifieringsordningar som sedan efterfrågas vid upphandling eller genom reglering kan leda leverantörer till att förbättrade säkerhetsegenskaperna i sina produkter och tjänster.

Kraven på incident- och sårbarhetshantering enligt cybersäkerhetsakten kan, rätt utformade, bli en tillgång för användarna, i synnerhet om sådan hantering kan samordnas med nationella processer för incidenthantering.

Kraven på kontinuerligt stöd från leverantörer under certifikatets giltighetstid kan bli en tillgång för användarna och motverkar risken att verksamhetsutövare använder produkter som inte längre underhålls av leverantören.

Certifiering som verktyg fungerar väl för verifiering av existens av säkerhetsfunktioner – ”funktionella tester”, men det är fortsatt en utmaning att via certifiering finna alla sårbarheter.

EU-gemensam certifiering skulle kunna leda till ökat fokus på kontroll av leverantörers utvecklingsprocesser, underhåll och förmåga att till operativ övervakning. Detta kan leda till både färre brister och bättre skalbarhet avseende EU:s kapacitet för antalet certifierade produkter.

EU-certifiering kan starkt bidra till att ta hand om ”långsamma” krav, dvs. krav som är stabila och lika över tiden, och där standarder är väl definierade, certifieringarna är möjliga att genomföra inom rimlig tid/kostnad för användarna och där det finns tillräcklig kompetens hos certifieringsorganen.

5.5 Certifiering av cybersäkerhet – Utmaningar

Det är i de flesta praktiska fall omöjligt att uppnå en status där IKT-produkter och system saknar sårbarheter. Detta är en konsekvens av hur dessa system är uppbyggda av komplicerade dataship, mjukvaror och arkitekturer. Att testa ett system eller en produkt i sin helhet för att hitta varje tänkbar sårbarhet är i de flesta fall inte tekniskt eller resursmässigt möjligt; det är en gränslös uppgift. Detta till skillnad från kontroll av existens (”funktionella krav”) som annars är en vanlig grund för certifiering av säkerhet i samband med t ex CE-märkning. Samtidigt är det just behovet av frånvaro av sårbarheter som är det centrala behovet som efterfrågas. Certifiering kan inte antas

hitta alla sårbarheter och det är rimligt att anta att varje certifierad produkt/tjänst är behäftad med kvarvarande sårbarheter som kan utnyttjas av en angripare.

Certifiering kan inte heller ”kontrollera fram” säkerhet i produkter/tjänster när det råder bristande tilltro till leverantören; även leverantörer som kan ha mer eller mindre illasinnade intressen, kan uppfylla kraven som ställs i certifieringsordningarna. Bristande tilltro till leverantörer och många andra riskfaktorer måste hanteras via riskbedömning och olika former av kompenserande säkerhetsåtgärder vid utformningen av det specifika nätverks- och informationssystemet. Beslut om en produkts/tjänst lämplighet för en viss given användning kan inte enbart baseras på certifikat.

Certifieringarna kommer genomföras i enlighet med krav som anges i certifieringsordningen och i denna refererade standarder och/eller tekniska specifikationer. Om svenska intressenter inte kunnat delta på lika villkor som andra aktörer vid utformning av certifieringsordningar eller de standarder som dessa refererar, kan de bli utformade så att de är till nackdel för svenska intressen (t.ex. omotiverat försvårar för svenska leverantörer att uppfylla kraven) och samtidigt gynna andra intressenter. Direkta utlåsningseffekter kan uppstå för både svenska verksamhetsutövare och leverantörer om kraven i certifieringsordning eller standarder är ”orättvist” utformade eller för dyra att efterleva.

Vid framtagning av certifieringsordningars relaterade standarder måste svenska intressenter förhandla med andra, vilket kan leda till att eventuella specifika svenska behov inte adresseras i certifieringsordningarna. Därmed kan i många fall produkter/tjänster vara behäftade med egenskaper som behöver kompletteras via andra åtgärder. Sådan komplettering kan både komma att behövas på nationell nivå, så väl som för enskilda sektorer eller enskilda system.

En övertro till värdet av certifieringar, framför allt avseende risken för kvarvarande sårbarheter, kan leda till felaktiga riskhanteringsbeslut hos användaren. Detta är en risk för svenska intressenter och något som bör adresseras. [9]

Processen att utveckla certifieringsordningar och refererade standarder är långsam och kan ta många år i anspråk. Det samma gäller uppdateringar av standarder och certifieringsordningen över tiden. Därmed kan teknik och säkerhetskrav som följer av snabb utveckling och snabba förändringar inte komma att täckas väl av certifieringsprocesserna. Certifiering passar bättre för aspekter som objektivt verifierbara och är stabila över tiden.

Certifieringsprocessen kan vara mycket långsam och kostsam visavi behovet av att göra produkter/tjänster tillgängliga på marknaden.

---

[9] Cybersäkerhetsakten definition av assuransnivå: assuransnivå: förtroendegrund för att en IKT-produkt, IKT-tjänst eller IKT-process uppfyller säkerhetskraven i en särskild europeisk ordning för cybersäkerhetscertifiering och anger på vilken nivå en IKT-produkt, IKT-tjänst eller IKT-process har utvärderats, men som i sig inte mäter säkerheten i den berörda IKT-produkten, IKT-tjänsten eller IKT- processen.

Bristande tillgång till kompetenta granskare kan leda till bristande kvalitet i genomförda certifieringar och leda till snedvriden konkurrens och svårbedömda risker för användarna. Detta förstärks av att verksamheten att kontrollera andras resultat i form av utvecklade produkter och tjänster av många personer kan ses som mindre intressant och attraktivt än att delta i utveckling av samma produkter/tjänster

Certifiering kan innebära en ”pappersbaserad kontrollverksamhet”, dvs. en kostsam administrativ påbyggnad som inte bidrar till ökad säkerhet. Detta gäller inte minst för underhåll av ett certifikat över tid, där nya patchar och versioner av produkter/tjänster kan vara mycket frekventa.

Olämpligt utformade eller tillämpade certifieringsordningar kan leda till ojämn kvalitet mellan olika länder. Detta kan leda till mer eller mindre allvarlig snedvridning av konkurrensen och att vissa leverantörer medvetet väljer att söka certifiering i de medlemsländer där man får denna tjänst billigast. Eftersom cybersäkerhetsakten anger att utgivna certifikat ska erkännas av alla medlemsstater och behandlas lika vid t.ex. statlig upphandling kan detta mer eller mindre allvarligt både snedvrida konkurrensen och leda till att t.ex. svenska myndigheter via LOU-upphandling tvingas välja sådana produkter eller tjänster som erhållit certifikat efter en undermålig process.

Överdrivet centraliserad incidenthantering inom ramen för cybersäkerhetsakten kan innebära säkerhetsrisker för svenska intressen. Central incidentrapportering behöver inte vara tekniskt detaljerad för att kunna utgöra en risk; blotta kunskapen om att en sårbarhet existerar i viss produkt/tjänst kan vara av värde för en angripare och inrikta dennas sökande efter nya attackvägar.

Cybersäkerhetsaktens regelverk medger undantag för medlemsstaterna då det gäller nationella säkerhetsintressen. Detta innebär att andra länder, liksom Sverige, kan underlåta att meddela kända sårbarheter i de fall man ser en risk för den nationella säkerheten om sådan kunskap sprids. Därmed innebär förmodligen cybersäkerhetsakten att inte att alla sårbarheter av allvarligt slag rapporteras. Detta i sig kan få konsekvenser för det värde som kan ges till enskilda certifieringar och för de säkerhetsåtgärder som Sverige bör tillämpa för att tillvara ta svenska behov.

Långtgående krav på certifiering av produkter och tjänster via EU-reglering, nationell reglering eller av upphandlande organisation kan leda till allvarliga säkerhetsrisker om inte certifiering och underhåll av certifiering sker till en kostnad och tid som bedöms vara rimlig. Annars riskerar certifiering försena leveranser av certifierade produkter/tjänster och/eller leda till motvilja från både leverantörer och verksamhetsutövare att använda nya (presumtivt säkrare) versioner av produkter/tjänster men som ännu inte certifierats p.g.a. av de kostnader som detta innebär. Men i de fall certifieringsreglerna är ändamålsenliga och verkligen leder till önskade säkerhetsegenskaper, så kan detta samtidigt lättare leda till exakt vad som eftersträvas, dvs. att produkter/tjänster som ännu inte visats motsvara kraven inte tas i drift.

Alltför långtgående krav på certifiering kan leda till att valet står mellan sämre, certifierade EU-lösningar i stället för bättre produkter/tjänster från leverantörer som inte haft resurser och/eller tid att genomföra certifieringen.

Krav på certifiering kan öka risken för monokulturer, dvs. minskad variation av produkter och tjänsteleverantörer på inre marknaden. Detta kan förenkla för angripare att framgångsrikt attackera många system via en och samma sårbarhet eftersom antalet system och tillhörande variationer kan begränsas.

EU-certifiering kan starkt bidra till att ta hand om ”långsamma” krav, dvs. krav som är stabila och lika över tiden, och där standarder är väl definierade, certifieringarna är möjliga att genomföra till tid/kostnad som är till värde för användarna och där det finns tillräcklig kompetens hos certifieringsorganen.

6 EU:s cybersäkerhetsakt och dess certifieringsordningar

Försvarets materielverks bedömning:

Cybersäkerhetsakten beskriver ett ramverk genom vilket certifieringsordningar för cybersäkerhet kan utvecklas i samverkan mellan bland annat EU-kommissionen, medlemsstaterna, Enisa och näringslivet. EU-kommissionens prioriteringar för vilka ordningar som ska utvecklas ska som huvudregel anges via ”Unionens löpande arbetsprogram för europeisk cybersäkerhetscertifiering” (eng: ” Union Rolling Work Programme for European cybersecurity certification” - URWP). Främst baserat på URWP ska EU-kommissionen ge Enisa i uppdrag att utarbeta förslag till certifieringsordningar.

Vid utarbetandet av förslag till certifieringsordningar ska Enisa samråda med alla berörda intressenter genom en öppen, transparent och inkluderande samrådsprocess. Enisa ska ha ett nära samarbete med medlemsstaternas NCCA-myndigheter. Baserat på Enisas förslag utarbetar EU-kommissionen därefter ett utkast till genomförandeakt. Genom ett kommittéförfarande och förhandlingar med medlemsstaterna når slutligen genomförandetakten sitt slutliga innehåll, efter omröstning av medlemsstaterna i genomförandekommittén.

Den första certifieringsordningen för certifiering av IT-produkter (EUCC) antogs genom kommittéförfarande i december 2023. En certifieringsordning för certifiering av molntjänster (EUCS) är i slutfasen av sin utveckling. Utveckling pågår även av en certifieringsordning relaterade till användaridentifiering i 5G-system, samt för de nätverkskomponenter som ingår i 5G-system.

Dessa tre certifieringsordningar avser komplicerad och omfattande informations- och kommunikationsteknik med bred, allmän användning i samhället. Det är en omfattande lista av standarder som ligger till grund för certifieringsordningarna, utvecklade av en stor mängd olika standardiseringsorgan.

För att kunna påverka utvecklingen av dessa certifieringsordningar behöver sektorsmyndigheter, verksamhetsutövare och näringsliv medverka inom ramen för EU-kommissionen och Enisas arbetsprocess, samt inom alla de olika organ som utvecklar de standarder och tekniska specifikationer som refereras i certifieringsordningarna.

Utveckling av certifieringsregelverk förutsätter omfattande kompetens med nödvändig bred och djup kompetens rörande IKT, cybersäkerhet, olika principer för teknisk kontroll, relevanta standarder, samt kunskap om behov av cybersäkerhet som finns i de specifika sektorer och verksamheter i vilka certifikaten är avsedda att användas.

6.1 Certifieringsramverket och dess syften

EU:s cybersäkerhetsakt (CSA) är uppdelad i två delar. Den första delen behandlar mål, uppgifter och organisatoriska frågor som rör Europeiska unionens cybersäkerhetsbyrå (Enisa). Den andra delen fastställer ett europeiskt ramverk för cybersäkerhetscertifiering av IKT-produkter, -tjänster och -processer. Certifikat som

utfärdas enligt ramverkets certifieringsordningar blir giltiga och skall erkännas i alla medlemsstater. Tillsyn över efterlevnaden införs också.

Det huvudsakliga syftet med cybersäkerhetsakten är att säkerställa en väl fungerande inre marknad och samtidigt sträva efter att uppnå en hög nivå av cybersäkerhet, cyberresiliens och förtroende inom unionen.

Det europeiska ramverket för cybersäkerhetscertifiering är avsett att bl.a. ge följande fördelar för företag och enskilda:

- Cybersäkerhetsakten ska stödja och underlätta utvecklingen av en europeisk cybersäkerhetspolitik genom att harmonisera villkoren och de materiella kraven för cybersäkerhetscertifiering av IKT-produkter, IKT-tjänster och IKT-processer i EU,
- certifieringsordningar ska hänvisa till gemensamma standarder eller kriterier för utvärderings- och test-metoder, vilket bidrar till användningen av gemensamma säkerhetslösningar i EU och undanröjer hinder för den inre marknaden,
- Cybersäkerhetsakten ska stödja och komplettera genomförandet av direktiv så som NIS-direktivet genom att förse de företag som omfattas av direktivet med ett verktyg för att visa att nät- och informations-säkerhetskraven uppfylls i hela unionen,
- de europeiska ordningarna för cybersäkerhetscertifiering ska ha företräde framför motsvarande nationella system och ersätter befintliga parallella nationella ordningar avseende samma IKT-produkter, -tjänster eller -processer,
- företag ska bara behöva genomgå en certifiering en gång, och certifikat som utfärdas enligt de europeiska ordningarna ska erkännas i alla medlemsstater,
- företag ska få en kontaktpunkt för cybersäkerhetscertifiering inom EU,
- en produkt , tjänst eller process ska – beroende på cybersäkerhetsbehov – kontrolleras och certifieras till en anpassad ambitionsnivå.

För närvarande pågår utveckling av tre certifieringsordningar:

- Certifiering av it-produkter (EUCC)
- Certifiering av molntjänster (EUCS)
- Certifiering komponenter (IKT-produkter) relaterade till användaridentifiering i 5G-system, samt certifiering av nätverkskomponenter som ingår i 5G-system och dessas utvecklingsprocess 5G-system (EU5G)

EU-kommissionen har föreslagit en utvidgning av cybersäkerhetsakten till förvaltade cybersäkerhetstjänster (i princip såsom dessa tjänster definierats i NIS2-direktivet). Förhandlingen om denna begränsade uppdatering av cybersäkerhetsakten är i sitt slutskede. Cybersäkerhetsakten stipulerar också att en övergripande översyn skall göras inom fem år från ikraftträdandet. Den översynen har påbörjats.

6.2 Unionens löpande arbetsprogram för europeisk cybersäkerhetscertifiering - URWP

I unionens löpande arbetsprogram för europeisk cybersäkerhetscertifiering (eng: ”Union Rolling Work Programme for European cybersecurity certification” –

URWP) fastställs strategiska prioriteringar för framtida certifieringsordningar. I URWP ska det särskilt ingå en förteckning över IKT-produkter, IKT-tjänster och IKT-processer eller kategorier av sådana som kan gagnas av att omfattas av en europeisk ordning för cybersäkerhetscertifiering.

6.3 Intressentgruppen för cybersäkerhetscertifiering – SCCG

En intressentgrupp för cybersäkerhetscertifiering ska inrättas (eng: ”Stakeholder Cybersecurity Certification Group” – SCCG). Gruppen ska bestå av medlemmar som ska väljas bland erkända experter som företräder berörda intressenter, t.ex. näringsliv, akademi och andra experter.

SCCG ska:

- ge kommissionen råd i strategiska frågor om den europeiska ramen för cybersäkerhetscertifiering,
- på begäran ge Enisa råd om allmänna och strategiska frågor om Enisas uppgifter när det gäller marknaden, cybersäkerhetscertifiering och standardisering,
- bistå kommissionen vid utarbetandet av unionens löpande arbetsprogram (URWP),
- yttra sig över unionens löpande arbetsprogram (URWP), och
- i brådskande ärenden ge kommissionen och europeiska gruppen för cybersäkerhetscertifiering råd om behovet av ytterligare certifieringsordningar.

Ordförandeskapet i SCCG ska innehas gemensamt av företrädare för kommissionen och Enisa, och Enisa ska tillhandahålla sekretariatet.

6.4 Certifiering – Säkerhetsmålsättningar

En certifieringsordning syftar till att, när så är tillämpligt, att åtminstone följande säkerhetsmålsättningar uppnås av föremålet för certifiering för vald assuransnivå:

- Att skydda data som lagras, överförs eller på andra sätt behandlas, mot oavsiktlig eller otillåten lagring, behandling eller åtkomst eller oavsiktligt eller otillåtet offentliggörande under hela IKT-produktens, -tjänstens eller -processens livscykel.
- Att skydda data som lagras, överförs eller på andra sätt behandlas, mot oavsiktlig eller otillåten förstöring eller förlust, oavsiktliga eller otillåtna ändringar eller bristande tillgänglighet under hela IKT-produktens, -tjänstens eller -processens livscykel.
- Att behöriga personer, program eller maskiner kan få åtkomst endast till de data, tjänster eller funktioner som omfattas av deras åtkomsträttigheter.
- Att identifiera och dokumentera kända beroenden och sårbarheter.
- Att registrera vilka data, tjänster och funktioner som någon haft åtkomst till, som använts eller på andra sätt behandlats, vid vilken tidpunkt och av vem.

- Att det är möjligt att kontrollera vilka data, tjänster eller funktioner som någon haft åtkomst till, eller som använts eller på andra sätt behandlats, vid vilken tidpunkt och av vem.
- Att kontrollera att IKT-produkter, -tjänster och -processer inte innehåller några kända sårbarheter.
- Att återställa tillgängligheten och tillgången avseende data, tjänster och funktioner i rätt tid vid en fysisk eller teknisk incident.
- Att IKT-produkter, -tjänster och -processer är säkra i sitt grundutförande och är säkra genom sin konstruktion.
- Att IKT-produkter, -tjänster och -processer tillhandahålls med uppdaterad programvara och maskinvara som inte innehåller publikt kända sårbarheter, och med funktioner för säkra uppdateringar.

6.5 Assuransnivåer

Cybersäkerhetscertifieringar ska ske enligt en av tre assuransnivåer (”förtroendenivåer” eller ” ambitionsnivåer”): Grundläggande, Betydande och Hög.

Assuransnivån anger en förtroendegrund för att en IKT-produkt, IKT-tjänst eller IKT-process uppfyller säkerhetskraven i certifieringsordning och anger i vilken omfattning en IKT-produkt, IKT-tjänst eller IKT-process har utvärderats. Assuransnivån ska stå i proportion till nivån på den risk som är förenad med den avsedda användningen av en IKT-produkt, IKT-tjänst eller IKT-process, i form av sannolikhet för och inverkan av en eventuell incident. Assuransnivåerna avspeglar motsvarande stringens och djup i fråga om utvärdering av IKT-produkten, IKT-tjänsten och IKT-processen. Nivåerna fastställs genom hänvisning till tekniska specifikationer, standarder och förfaranden med koppling till detta, inbegripet tekniska kontroller, som ska mildra eller förhindra incidenter. En assuransnivå i sig mäter dock inte säkerheten i den berörda IKT-produkten, IKT-tjänsten eller IKT-processen, utan anger ambitionsgraden av den granskning som är genomförd.

Assuransnivå Grundläggande innebär att föremålet för certifieringen har utvärderats på en nivå som avser att minimera kända grundläggande risker för incidenter och cyberattacker. Den utvärdering som ska göras ska innefatta åtminstone en granskning av den tekniska dokumentationen.

Assuransnivå Betydande innebär att föremålet för certifieringen har utvärderats på en nivå som avser att minimera kända cyberrisker, och risken för incidenter och cyberattacker som genomförs av aktörer med begränsade kunskaper och resurser. Utvärderingen ska visa att allmänt kända sårbarheter inte föreligger och omfattar testning för att visa att IKT-produkter, -tjänster och -processer på ett korrekt sätt omfattar nödvändiga säkerhetsfunktioner.

Assuransnivå Hög innebär att föremålet för certifieringen har utvärderats på en nivå som avser att minimera risken för avancerade cyberattacker som genomförs av aktörer med omfattande kunskaper och resurser. Utvärderingen som ska göras omfattar åtminstone testning för att visa på korrekta och nödvändiga

säkerhetsfunktioner enligt senast känd teknik (eng: ”state-of-the-art”) och en bedömning av motståndskraften mot kunniga angripare genom så kallade penetrationstester.

6.6 Självbedömning

En certifieringsordning kan ge tillverkaren eller leverantören av IKT-produkter, IKT-tjänster eller IKT-processer möjlighet att göra en självbedömning av överensstämmelse. Detta kan dock endast tillåtas i förhållande till IKT-produkter, -tjänster och -processer med låg risk som då endast motsvarar assuransnivån grundläggande.

6.7 Certifieringsordningarnas innehåll

En certifieringsordning enligt cybersäkerhetsakten (eng: ”certification scheme” eller bara ”scheme”) utgör en vittomfattande uppsättning regler, tekniska krav, standarder och förfaranden som fastställs på unionsnivå och som beskriver krav på hur bedömning av överensstämmelse av IKT-produkter, -tjänster och -processer ska ske.

En certifieringsordning består normalt bl.a. av regler för:

- Den typ eller kategori av IKT-produkter, -tjänster och -processer som kan omfattas av certifieringsordningen.
- En hänvisning till de standarder eller tekniska specifikationer som ska tillämpas.
- Vilka assuransnivåer som omfattas.
- Kraven på teknisk kompetens hos de organ för bedömning av överensstämmelse som ska utvärdera cybersäkerhetskraven.
- Villkor för utfärdande, bibehållande, fortsättande och förnyelse av europeiska cybersäkerhetscertifikat.
- Bestämmelser om hur tidigare oupptäckta sårbarheter i fråga om cybersäkerhet hos IKT-produkter, -tjänster och -processer ska rapporteras och hanteras.
- Giltighetstid för europeiska cybersäkerhetscertifikat som utfärdats enligt ordningen.
- Villkor för ömsesidigt erkännande av certifieringsordningar med tredjeländer.
- Regler för ömsesidig inspektion av nationella myndigheter för cybersäkerhetscertifiering (eng: ”National Cybersecurity Certification Authority” – NCCA) eller certifieringsorgan (så kallat peer review).

Ett cybersäkerhetscertifikat utgör ett dokument, utfärdat av behörigt certifieringsorgan, som intygar att en viss IKT-produkt, -tjänst eller -process, har utvärderats genom kontroll av överensstämmelse med specifika säkerhetskrav som fastställs i en certifieringsordning.

6.8 Nationella certifieringsordningar

De nationella ordningarna för cybersäkerhetscertifiering som omfattas av en europeisk ordning för cybersäkerhetscertifiering ska upphöra att ha verkan när en motsvarande europeisk certifieringsordning etablerats. Medlemsstaterna får inte

införa nya nationella ordningar för cybersäkerhetscertifiering som redan omfattas av en befintlig europeisk ordning för cybersäkerhetscertifiering.

6.9 Nationell myndighet för cybersäkerhetscertifiering

Varje medlemsstat ska utse en eller flera nationella myndigheter för cybersäkerhetscertifiering (eng: ”National Cybersecurity Certification Authority” – NCCA). I Sverige är Försvarets materielverk som har fått denna uppgift. Se närmare om Försvarets materielverks roll som NCCA i avsnitt 9 ”FMV:s uppgifter och ansvar”

6.10 Organ för bedömning av överensstämmelse

Organ för bedömning av överenstämmelse (eng: ”Conformity Assessment Body” - CAB) kan utgöras av både ett certifieringsorgan (eng ”certification body” - CB), samt i förekommande fall (beroende på villkoren i certifieringsordningen), av de särskilda organ som ansvarar för att genomföra kalibrering, tester och/eller provning (”laboratorium”, ”labb”, ”Information Technology Security Evaluation Facility” – ITSEF). Resultatet av sådana tester rapporteras till certifieringsorganet.

Ett organ för bedömning av överensstämmelse ska vara ackrediterat av det nationella ackrediteringsorganet i respektive EU-medlemsstat. I Sverige har myndigheten Swedac denna uppgift.

En sådan ackreditering utgör en förklaring från det nationella ackrediteringsorganet att ett organ för bedömning av överensstämmelse uppfyller de krav som ställs på dem, samt besitter den kompetens som är nödvändig för att genomföra specifika tekniska kontroller enligt relevant(a) cybersäkerhetscertifieringsordning(ar).

En certifieringsordning kan även ange att ett organ för bedömning av överensstämmelse dessutom ska bemyndigas av den Nationella Myndigheten för Cybersäkerhetscertifiering (eng ”National Cybersecurity Certification Authority” – NCCA). I Sverige är det Inspektionen för Cybersäkerhetscertifiering (ICC) vid Försvarets materielverk som har denna roll. Denna extra nivå av behörighetskontroll är avsedd för certifieringsorgan för bedömning av överensstämmelse som avser verka på assuransnivå Hög.

Certifikat på assuransnivå Hög får enbart utfärdas av ett nationellt certifieringsorgan inordnat vid NCCA eller annan myndighet eller av ett kommersiellt organ för bedömning av överensstämmelse endera genom att NCCA förhandsgodkänner varje enskilt certifikat, eller genom allmän delegering ger ett sådant förtroende till ett (eller flera) kommersiella organ för bedömning av överensstämmelse.

Cybersäkerhetsakten ställer krav på leverantören att tillhandahålla all relevant information nödvändig för certifieringen, information till användarna av den certifierade IKT-produkten/-tjänsten/-processen samt tämligen långtgående krav på rapportering om potentiella sårbarheter.

6.11 Inbördes granskning (peer review)

De nationella myndigheterna för cybersäkerhetscertifiering omfattas av inbördes granskning i syfte att uppnå likvärdig tillämpning i hela unionen för europeiska cybersäkerhetscertifikat. En sådan inbördes granskning ska utföras av minst två nationella myndigheter för cybersäkerhetscertifiering från andra medlemsstater och kommissionen och ska utföras minst vart femte år. Enisa får delta i den inbördes granskningen.

6.12 Europeiska gruppen för cybersäkerhetscertifiering (ECCG)

Europeiska gruppen för cybersäkerhetscertifiering består av företrädare för nationella myndigheter för cybersäkerhetscertifiering eller företrädare för andra berörda nationella myndigheter. Gruppen har i uppgift att bl.a. ge råd till och bistå kommissionen i dess arbete för att säkerställa ett konsekvent genomförande och en konsekvent tillämpning av det europeiska ramverket för cybersäkerhetscertifiering, särskilt när det gäller frågor som rör unionens löpande arbetsprogram, cybersäkerhetscertifiering, strategisamordning och utarbetandet av de europeiska ordningarna för cybersäkerhetscertifiering. ECCG ska:

- ge råd till och bistå kommissionen avseende cybersäkerhetscertifiering, strategisamordning och utarbetandet av certifieringsordningar
- ge råd till, bistå och samarbeta med Enisa när det gäller utarbetande av förslag till certifieringsordning
- anta ett yttrande om förslag till, eller ändring av, certifieringsordning som utarbetats av Enisa
- bevaka utvecklingen på området cybersäkerhetscertifiering och utbyta information och god praxis om ordningar för cybersäkerhetscertifiering,
- delta i ömsesidig granskning av medlemsstaternas NCCA.
- verka för att certifieringsordningar baseras på internationellt erkända standarder.

6.13 Utveckling av certifieringsordningar och möjligheter till påverkan

6.13.1 Inledning

Svenska intressenter har flera olika möjligheter att direkt eller indirekt påverka cybersäkerhetsakten och dess certifieringsordningar via de olika utvecklingssteg som föreskrivs i akten. Bara vissa steg i utvecklingen är öppna för t.ex. näringsliv eller andra experter. I de fall kraven och reglerna för kontroll utvecklas via öppna standardiseringsorgan så är dock även dessa forum tillgängliga. Följande avsnitt ger en beskrivning av stegen för hur certifieringsordningarna utvecklas och möjligheten för svenska intressenter att medverka och påverka.

6.13.2 Via standardiseringsorganen och andra arbetsgrupper

Som tidigare angivits refererar certifieringsordningarna direkt och indirekt olika former av standarder och tekniska specifikationer som utvecklats av

standardiseringsorgan och de facto-standardiseringsorgan. Dessa standarder och andra dokument har en mycket stor betydelse för de faktiska krav som ställs via certifieringsordningarna, reglerna för hur kontrollerna ska genomföras samt kraven på kompetens hos de organ för bedömning av överensstämmelse som ska göra dessa kontroller.

I avsnittet om standardisering anges ett antal framträdande standardiseringsorgan inom IKT- och cybersäkerhetsområdet.

I Bilaga 6 – EUCC: Standardsorganisationer och standarder, Bilaga 7 – EUCS: Standardsorganisationer och standarder och Bilaga 8 – EU5G: Standardsorganisationer och standarder framgår exempel på standardiseringsorgan och relaterade standarder som är av betydelse för respektive certifieringsordning.

6.13.3 Via URWP

Via unionens löpande arbetsprogram för europeisk cybersäkerhetscertifiering (URWP) ska strategiska prioriteringar fastställas för framtida certifieringsordningar. Svenska intressenter kan påverka denna strategiska inriktning genom dialog med NCCA som sedan för dialog med EU-kommissionen, deltagande i Intressentgruppen för cybersäkerhetscertifiering (”Stakeholder Cybersecurity Certification Group” – SCCG), eller med den nationella representanten i ECCG.

6.13.4 Via Enisas arbetsgrupper och Enisas öppna samråd

Efter en begäran från kommissionen ska Enisa utarbeta ett förslag till certifieringsordning.

I arbetet skapar Enisa för varje certifieringsordning en tillfällig arbetsgrupp (s.k. Ad-hoc Working Group) bestående av ca 20 experter från medlemsstaternas offentliga förvaltningar, unionens institutioner, organ och byråer samt den privata sektorn, inklusive industrin, användare och akademiska experter på nät- och informationssäkerhet. Dessa20-talet experter Enisa väljer att medverka till detta arbete har mycket goda möjlighet att påverka innehållet i förslaget till certifieringsordning. En begränsad grupp innebär begränsad insyn från övriga intressenter.

Vid utarbetandet av ett förslag till certifieringsordning ska Enisa samråda med alla berörda intressenter genom en formell, öppen, transparent och inkluderande samrådsprocess. När Enisa utvecklat ett förslag publiceras detta på myndighetens hemsida för öppet samråd. Vid detta tillfälle har allmänheten, dvs. företag och andra experter möjlighet att kommentera förslaget. Men det är Enisa som tar beslut på vad som ska presenteras för ECCG vilket i sin tur påverkas av det som det 20-tal deltagarna i Enisas Ad-hoc-Working Group anser.

6.13.5 Via ECCG

Enisa ska ha ett nära samarbete med ECCG, där medlemsstaternas NCCA-myndighet medverkar. Därmed har Sverige genom sin NCCA-myndighet stor möjlighet över tiden följa arbetet och påverka inriktningen på arbetet. NCCA-myndigheterna tar del av i Enisas arbetsgruppers resultat, vilket också andra svenska

myndigheter kan göra i samverkan med NCCA-myndigheten. Dock har inte näringslivet eller andra experter tillträde till detta forum, men de kan söka dialog med sin respektive NCCA-myndighet eller sektorsmyndighet.

6.13.6 Via kommittologiförfarandet

EU-kommissionen utarbetar därefter ett förslag till genomförandeakt baserat på Enisas förslag. Genom ett kommittéförfarande och förhandlingar med medlemsstaterna får slutligen genomförandeaktens sitt slutliga innehåll, efter omröstning av medlemsstaterna i genomförandekommittén. Det går att lämna synpunkter till EU-kommissionen medan de tar fram sitt förslag samt under hela kommittologiförfarandet. Man kan också under förfarandet lämna synpunkter till svenska företrädare i kommittén (vilket ofta är bl.a. NCCA:n). Intressenter kan också försöka påverka under den öppna samråd som KOM måste ha om genomförandeakten.

6.14 EU:s certifieringsordning för it-säkerhet i it-produkter – EUCC

6.14.1 Översiktlig beskrivning

EUCC baseras på standarden Common Criteria (ISO/IEC 15408) och tillhörande evalueringsmetodik (ISO/IEC 18405). Totalt består standarden av sex dokument på sammanlagt över 1000 sidor text.

Enligt Common Criteria ska en s.k. säkerhetsmålsättning (eng: ”Security Target” - ST) utvecklas i enlighet med standardens regler för varje specifik produkt som ska certifieras. Detta dokument ska visa vilka tillgångar som ska skyddas, vilka hot och angripare som ska mötas, samt de krav på säkerhetsfunktioner och granskning som ska borga för att tillgångarna kan skyddas mot angripare med en viss attackförmåga. Produkter ska sedan granskas av ackrediterat (och för assuransnivå hög bemyndigat) organ för bedömning av överensstämmelse (CAB/ITSEF) i enlighet med den tillhörande evalueringsmetodiken. Granskningsresultatet ska granskas och godkännas av ett ackrediterat (och för assuransnivå hög bemyndigat) certifieringsorgan (CAB/CB). Om certifieringsorganet anser sig kunna godkänna resultatet kan organet utfärda ett certifikat.

Enligt EUCC kan certifiering ske på assuransnivå Betydande (vilket motsvarar CC EAL3 i det etablerade regelverket Common Criteria) och/eller Hög (motsvarar CC EAL4 eller högre). I EUCC tillämpas inte assuransnivå Grundläggande.

Enligt Common Criteria kan även säkerhetskrav för en viss typ av produkt definieras, t.ex. för brandväggar eller för operativsystem. Sådana krav utvecklade för en specifik typ av produkt kallas för skyddsprofil (eng ”Protection Profile” – PP). En leverantör av till exempel en brandvägg kan sedan utveckla sin produkts säkerhetsmålsättning så att den matchar kraven angivna i en skyddsprofil som är utvecklad för att ange krav på brandväggar. I själva certifieringsprocessen kontrolleras sedan att den specifika leverantörens produkt (t.ex. brandvägg) motsvarade kraven i en sådan skyddsprofil. Vid överenstämmlse så utfärdas och anges detta i certifikatet.

Skyddsprofiler är ett mycket vanligt och användbart verktyg för att användare verksamhetsutövare och kravställare ska kunna formulera vilka krav man vill ställa på en produkt som ska användas för ett visst syfte. Det finns 100-tals sådana skyddsprofiler definierade för vanliga typer av produkter. Dessa skyddsprofiler kan i sig betraktas som standarder för den givna produkttypen.

I ” Bilaga 10 – Exempel på internationella Skyddprofiler enligt Common Criteria” finns en lista över sådana skyddsprofiler. Kraven på en produkt vid certifiering enligt Common Criteria (t.ex. inom ramen för EUCC) styrs i sådana fall helt av kraven som anges i sådana Skyddsprofilen. Sådana dokument är mycket komplicerade texter utformade för att adressera specifika säkerhetsproblem.Det finns ett behov av att Sverige inom ramen för cybersäkerhetsakten får tillgång till produkter med standardiserade funktioner, baserade på skyddsprofiler. Detta dels för att produkternas funktioner då förväntas bättre bidra till säkerhet i den arkitektur de är den del av, dels för att det då medger för verksamhetsutövare att välja mellan fler leverantörer som erbjuder produkter vilka då har likvärdig säkerhetsfunktionalitet och kan bli utbytbara. Detta i sin tur bidrar till ökad möjlighet till variation mellan verksamhetsutövare och därmed bidra till minskad risk för s.k. monokulturer avseende sådana produkter. Det är dock mycket få (eller inga?) svenska verksamhetsutövare eller sektorsmyndigheter som har tillgång till sådan kompetens och samtidigt har resurmässigt utrymme för att delta vid utveckling av dessa dokument.

Produkter som hör till CC EAL5 eller högre ska enbart kunna certifieras inom EUCC Nivå hög om de endera hör till specifika teknikområden (smartcard och ”security boxes” som är avsedda att motstå angrepp från angripare som har fysisk tillgång till produkten), eller till mjukvaruprodukter för vilka en särskild skyddsprofil (Protection Profile, PP) med tillhörande metodik har godkänts och införlivats i genomförandeakten.

En viktig cybersäkerhetsapsekt i EUCC är att leverantörer är skyldiga att rapportera potentiella sårbarheter i certifierade produkter inom tre dagar till sitt certifieringsorgan, som ska analysera sårbarheten och rapportera till NCCA.

Certifieringsorgan på assuransnivå Hög ska minst vart 5:e år genomgå en s.k. peer review, för att borga för hög och jämn tillämpning mellan medlemsländernas certifieringsorgan på denna nivå.

För att förtydliga tillämpningen av standarden som ligger till grund för EUCC (ISO/IEC 15408) standarden och anpassa den till aktuellt läge avseende teknisk utveckling av både skyddsåtgärder och attack-teknik, finns ett ganska stort antal s.k. ”state-of-the-art”-dokument etablerat inom ramen för utvecklingen av certifieringsordningen, tänkta att införlivas i denna.

Ett sådant ”state-of-the-art”-dokument är inte rättsligt bindande, men i de fall ett organ för bedömning av överensstämmelse av någon anledning inte följer dokumentets regler, ska detta rapporteras till NCCA som in sin tur ska rapportera detta till EU-kommissionen. EU-kommissionen kan sedan överväga om det finns skäl att göra kravet obligatoriskt genom att lyfta in det i certifieringsordningens genomförandeakt.

Totalt är det ett tjugotal olika ”state-of-the-art” dokument som är under utveckling. Dessa beskriver t.ex. krav på kompetens hos organ för kontroll av överensstämmelse, hur olika typer av attacker kan genomföras som ingår i testningen som ska genomföras vid en certifiering och hur säkerheten ska upprätthållas hos leverantörerna av certifierade produkter.

6.14.2 Relation till andra standarder än CC

Vad gäller säkerhetsmålsättningar och skyddsprofiler i CC så refereras det ofta till många typer av standarder för att ange t.ex. krav på kommunikationsprotokoll, dataformat eller vilka krypteringslösningar som får användas.

Dessa refererade standarder blir därmed i sig delar av de krav som EUCC blir beroende av och som mycket väsentligt kan styra både de funktionella krav och de krav på granskning och kontroll som kan omfattas av EUCC.

Som tidigare nämnts är ofta skyddsprofiler i sig att betrakta som standarder och sådana utvecklas av en stor mängd olika standardiseringsorgan eller de facto-standardiseringsorgan.

I ”Bilaga 5 - Exempel på standardsorgan och de facto-organ inom cyberområdet”finns en lista över standardiseringsorgan och de facto-standardiseringsorgan som utvecklar standarder och tekniska specifikationer som är direkt eller indirekt av betydelse för kraven som ställs via EUCC.

Det är ett tjugotal olika organ som utvecklar standarder och tekniska specifikationer som är av stor relevans för EUCC.

6.14.3 Utvecklingsläget

Genomförandeförordningen för EUCC är antagen och har trätt i kraft. Vissa av bestämmelser är dock inte tillämpliga ännu. Det är även ett stort antal ”state-of-the-art”-dokument under utveckling.

6.15 EU:s certifieringsordning för cybersäkerhet i molntjänster – EUCS

6.15.1 Översiktlig beskrivning

EUCS syftar till att förbättra villkoren för EU:s inre marknad och att höja nivån på cybersäkerhet i olika typer av molntjänster som omfattar molnfunktioner som är implementerade av molntjänstleverantören, inklusive applikationer, infrastruktur och plattformstjänster.

EUCS täcker ett brett spektrum av cybersäkerhetskrav genom att erbjuda utvärderingsnivåer som motsvarar alla tre assuransnivåer definierade i cybersäkerhetsakten (”grundläggande”, ”betydande” och ”hög”).

Användare av EUCS kan inkludera:

- molntjänsteleverantörer (CSP) som vill bedöma cybersäkerheten för sina molntjänster genom tredjepartcertifiering;

- molntjänstkunder (CSC) som vill dra nytta av bevisen från certifierade molntjänster till att fatta välgrundade beslut relaterade till cybersäkerheten för dessa molntjänster;
- tillsynsmyndigheter som vill inkludera krav på cybersäkerhet och försäkran om molntjänster inom sina förordningar och direktiv.

De säkerhetsåtgärder som ska genomföras varierar beroende på vald assuransnivå. Även om säkerhetsåtgärderna har vissa likheter med ISO/IEC 27000 serien så har deinte organiserats för att underlätta för organisationer som redan har en ISO/IEC 27001-certifiering. EUCS är genom de olika assuransnivåerna i vissa avseenden mer normerande än vad ISO/IEC 27001-certifiering i sig kan anses vara.

Säkerhetsåtgärderna kan grupperas i olika kategorier. Nedan är en listning av de kategorier som finns definierade i EUCS:

- Organisation för informationssäkerhet
- Policy för informationssäkerhet
- Riskhantering
- Hantering av personal (Human Resources)
- Hantering av tillgångar
- Fysisk säkerhet
- Säker drift
- Kryptografi och hantering av kryptonycklar
- Säker kommunikation
- Portabilitet och interoperabilitet
- Ändrings- och konfigurationsstyrning
- Utveckling av informationssystem
- Upphandling
- Incidenthantering
- Kontinuitetshantering
- Regelefterlevnad
- Användardokumentation
- Hantering av tillsyn från myndigheter
- Produktsäkerhet

Var och en av ovan kategorier utvecklas till specifika krav på säkerhetsåtgärder som en molntjänstleverantör ska ha infört.

En särskild del av EUCS är utvecklad som definierar kraven på de organ för bedömning av överensstämmelse som ska certifiera en molntjänst enligt EUCS.

6.15.2 Relation till standarder

Se Bilaga 7 – EUCS: Standardsorganisationer och standarder

6.15.3 Utvecklingsläget

Enisa har tidigare lämnat ett utkast till EUCS för offentligt samråd och yttrande från ECCG. Emellertid har Enisas senare utkast ändrats betydligt och Enisa har ännu inte lämnat något formellt förslag till EUCS till EU-kommissionen. Enisas arbete har försvårats och försenats p.g.a. Kommissionens och några medlemsstaters vilja att EUCS ska innehålla regler för s.k. digital suveränitet, eller skydd mot olovlig tillgång till data (protection of unlawful access (PUA) to data) som det senare kommit att kallas, vilket innebär att EUCS på högsta nivån skulle innehålla krav på åtgärder som syftar till att hindra att tredje lands lagstiftning skulle tvinga en certifierad molntjänst att lämna ut data. EU-kommissionens rättstjänst har emellertid nyligen presenterat en rättslig analys kring PUA-kraven för ECCG. Enligt denna analys ger cybersäkerhetsakten inte något mandat att ställa PUA-krav i certifieringsordningarna. Därmed menar EU-kommissionen att ordningen kommer att kunna antas i ungefär det skick som ECCG redan yttrat sig kring och att det kan ske under våren/sommaren, innan nuvarande kommissions mandat löper ut. Men analysen öppnar fortfarande för att man kan kräva att en riskanalys kring PUA-frågor görs och publiceras i samband med en CSA-certifiering. Detta är fortfarande omdiskuterat. Ett nytt omarbetat utkast skickades till medlemsstaterna den 28 mars 2024.

6.16 EU:s certifieringsordning för IKT-säkerhet i 5G-system – EU5G

6.16.1 Översiktlig beskrivning

Certifieringsordningen för 5G avses bestå av flera olika delar och kunna leda till olika typer av certifikat, dels för vissa IKT-produkter, dels vissa IKT-processer.

Baserat på de GSMA-ordningar för certifiering, vilka pekats ut av EU-kommissionen, avser man för det första certifiera vissa IKT-produkter, baserat på GSMA:s NESAS-ordning. Här handlar det i princip om den nätverksutrustning som behövs för hanteringen av övriga delar av ordningen.

En annan typ av IKT-produkt som avses certifieras är det som kallas eUICC, eller eSIM, grovt förenklat den mjuk- och/eller hårdvara som förr var det klassiska SIM-kortet.

Utöver det avser man certifiera två IKT-processer;

- dels distanshantering av eSIM, grovt förenklat 5G-användarnas profiler i telefonen, baserat på GSMA:s SAS-SM-ordning,
- dels, återigen grovt förenklat, konfigureringen av eUICC/eSIM för att kunna hantera eUICC-utvecklarnas distanskonfigurering av eSIM, baserat på GSMA:s SAS-UP-ordning.

Därmed består EU5G av tre olika delar.

- eUICC: Certifiering av s.k. Embedded Universal Integrated Circuit Card, en lösning där en användare kan ladda ner en eller flera abonnemang från olika operatörer över internet.

- SAS: Certifiering av utvecklare/tillhandahållare av eUICC till operatörerna (SAS-UP), samt certifiering av eUICC-användare och deras abonnemang (SAS-SM).
- NESAS: Certifiering av utvecklingsprocess och komponenter i 5G-system.

I följande avsnitt följer lite mer detaljerade beskrivningar av de i EU5G ingående delarna.

6.16.2 eUICC

eUICC hänvisar till de arkitekturstandarder som publicerats av GSMA eller implementeringar av dessa standarder. Med eUICC kan en enhet säkert lagra en eller flera SIM-kortsprofiler, som är de unika identifierare och kryptografiska nycklar som används av leverantörer av mobilnätstjänster för att unikt identifiera och säkert ansluta användare till mobila nätverksenheter. eUICC kan finnas i bl.a. mobila nätverksenheter (mobiltelefoner, surfplattor, bärbara datorer, säkerhetskontroller, medicinsk utrustning, etc.) som använder mobilnätverk som följer 3GPP-standarder (2G, 3G, 4G och 5G).

Certifiering av eUICC föreslås genomföras genom ett antal certifieringar av komponenter som ingår i en eUICC-implementation enligt skyddsprofiler (Protection Profiles) inom ramen för EUCC, bl.a.:

- eUICC chip: BSI-CC-PP-0084 (uppdatering av skyddsprofil:n krävs)
- eUICC java card platform (JCP): BSI-CC-PP-0099 (uppdatering av skyddsprofil:n krävs)
- eUICC RSP: BSI-CC-PP-0100: (uppdatering av skyddsprofil:n krävs)
- Secure application on mobile (SAM): skyddsprofil saknas(men kan komma att behövas för certifiering av e-plånböcker, vilka regleras i eIDAS2-förordningen[10])[11].
- Cryptographic abstraction layer (CSP): BSI-CC-PP- 0104 (kan komma att behövas för certifiering av e-plånböcker, vilka regleras i eID-förordningen)[12].

6.16.3 SAS

GSMA:s Security Accreditation Scheme (SAS) gör det möjligt för mobiloperatörer att bedöma säkerheten hos sina UICC- och eUICC-leverantörer och för deras tjänsteleverantörer av eUICC-abonnemang.

Två certifieringsordningar är etablerade inom SAS:

[10] REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework

[11] Det finns dock också förslag att hantera autentiseringen för e-plånboken via molnbaserade lösningar, t.ex. HSM-modul.

[12] Det finns dock också förslag att hantera autentiseringen för e-plånboken via molnbaserade lösningar, t.ex. HSM-modul.

- SAS för UICC-produktion (SAS-UP): Detta är ordning genom vilken UICC- och eUICC-tillverkare låter sina produktionsplatser och processer genomgå en säkerhetsrevision.
- SAS for Subscription Management (SAS-SM): Detta är en ordning genom vilken tjänsteleverantörer av eUICC-abonnemang kan genomgå en säkerhetsrevision.

Vid säkerhetsrevisionen granskas bl.a. följande delar:

- Säkerhetspolicy, strategi och dokumentation
- Säkerhetsorganisation och ansvar
- Informationssäkerhet
- Personalens säkerhet
- Fysisk säkerhet
- Certifikat- och nyckelhantering
- Hantering av känsliga processdata
- Logistik och produktionsledning
- Dator- och nätverkshantering

6.16.4 NESAS

GSMA NESAS (GSMA Network Equipment Security Assurance Scheme) är ett samarbete och leds gemensamt av 3GPP och GSMA. NESAS är öppet för alla leverantörer av nätverksutrustningsprodukter som stöder 3GPP-definierade funktioner. NESAS har utvecklats för att stärka säkerhetsnivån i 5G- och LTE-nätverk enligt etablerade bästa praxis och system som ger säkerhetsförsäkring.

NESAS består av två olika typer av granskningar:

- Granskning av leverantörens utvecklingsprocess och säkerhetsrutiner.
- Granskning av enskilda produkter mot specificerade krav för den givna produkttypen.

Vid bedömning av leverantörens utvecklingsprocess och säkerhetsrutiner ingår:

- Definition av en produkts utvecklings- och livscykel
- Definition av tillgångar som ska skyddas
  - Källkod
  - Mjukvarubiliotek
  - Färdiga produkter
  - Säkerhetsrelaterad dokumentation
  - Driftsatta produkter
  - Stödsystem vid produktutveckling
- Identifiering av hot och risk
- Identifiering av säkerhetsmålsättningar
- Säkerhetskrav vid utveckling och leverans:
  - Security by Design
  - Implementation/kodning
  - Granskning av källkod

- Källkodshantering
- Automatiserad byggprocess
- ”Byggprocesshantering”
- Säkerhetstestning
- Integritetsskydd
- Unik versionsidentifierare
- Dokumentationskvalitet
- Säkerhetsdokumentation
- Kontaktperson Säkerhet
- Hantering av information om sårbarheter
- Lösningsprocess för sårbarhet
- Sårbarhetsåtgärd Oberoende
- Säkerhetspatchning - information
- Versionskontrollsystem
- Ändringsspårning
- Personalutbildning
- Informationsklassificering och hantering
- Ständiga förbättringar
- Underleverantörer och livscykelhantering för leveranser från tredje part

För granskning/certifiering av enskilda komponenter finns tekniska specifikationer (Security Assurance Specification - SCAS). Det finns ett stort antal sådana tekniska specifikationer som ska tillämpas när sådana komponenter certifierar inom EU5G.

6.16.5 Relation till standarder

Se Bilaga 8 – EU5G: Standardsorganisationer och standarder.

6.16.6 Utvecklingsläget

Ett förslag till certifieringsordning för 5G-system är fortfarande under utveckling av Enisa. Enisa har aviserat att de avser presentera (för offentligt samråd) ett första utkast till förslag i slutet första kvartalet 2024.

Mycket arbete återstår, t.ex. att:

- klargöra omfattningen av certifieringarna,
- skriva överenskommelser om tillgång till ett flertal av de underliggande dokumenten, vilka utvecklats av andra (t.ex. GSMA), samt
- klargöra hur de omfattande och komplicerade regelverken ska underhållas.

7 EU-reglering med referenser till cybersäkerhetscertifiering

Försvarets materielverks bedömning:

Det finns ett drygt tiotal EU-regleringar (se bilaga 3) där cybersäkerhetscertifiering kan visa uppfyllnad av respektive reglerings krav på cybersäkerhetsegenskaper. CSA-certifiering kan således på nationell nivå få påverkan inom alla sektorer som omfattas av eller på annat sätt är beroende av dessa EU-regleringar. Dels som ett verktyg för verksamhetsutövare som en del av arbetet att tillämpa det egna arbetet att verifiera sina säkerhetsåtgärder, dels för att visa att man uppfyller regleringarnas stipulerade cybersäkerhetskrav. Ibland ställs tvingande krav på cybersäkerhetscertifiering direkt i den grundläggande EU-rättsakten på området, t.ex. rörande e-plånböcker (i eIDAS2-förordningen) och färdskrivare (i färdskrivarförordningen).

För de fall certifiering inte är ett tvingande krav är CSA-certifikat ändå av betydelse eftersom sådana certifikat enligt ett flertal EU-förordningar kan användas för att påvisa överensstämmelse med kraven, s.k. presumtion. Att certifiering i dessa fall är ett frivilligt sätt att visa kravuppfyllnad mot sådana regleringar skulle kunna leda till slutsatsen att aktiv medverkan vid utveckling av relaterade standarder och certifieringsordningen inte är en nödvändighet och kan hanteras ”i mån av tid”.

Det ska dock noteras att i flera av dessa förordningar har EU-kommissionen fått mandat att via s.k. delegerade akter med kort förvarning och med begränsat inflytande från medlemsstater, leverantörer eller verksamhetsutövare (privat eller offentliga) göra certifiering obligatorisk. Inom sektorer som omfattas av sådana EU-förordningar, t.ex. telekommunikation, transport, energi, hälsa, eID, AI, m.fl., kan det vara ett misstag om sektorsmyndigheter och/eller verksamhetsutövare väntar med att påverka relevant standard och certifieringsordning till dess att EU-kommissionen annonserar en avsikt att via delegerad akt göra certifiering obligatorisk.

Sektorsmyndigheter och verksamhetsutövare med ansvar inom EU-förordningar där EU-kommissionen har mandat att införa sådana delegerade akter bör därför tidigt i utvecklingsarbetet sätta sig in i de certifieringsordningar som berör deras ansvarsområden och överväga medverkan vid utveckling och uppdateringar av såväl dessa ordningar som relevanta standarder.

Detta illustreras av den nyligen antagna certifieringsordningen för cybersäkerhet i it-produkter (EUCC) som (liksom alla kommande ordningar), tillsammans med relaterade standarder ständigt kommer att kompletteras och uppdateras. Genom delegerade akter beslutade av EU-kommissionen kan EUCC kan komma att bli obligatorisk inom t.ex. NIS2-direktivet.

Vidare är ytterligare två certifieringsordningar nästan klara, en för molntjänster (EUCS) och en för 5G-nätverk (EU5G). EU-kommissionen har därutöver (i nyligen antagna URWP) pekat på några stora komplexa områden där de i närtid kommer att begära

utveckling av nya certifieringsordningar (AI, e-plånböcker i eIDAS2[13] och förvaltade säkerhetstjänster).

Ytterligare en aspekt att beakta och bevaka är att cybersäkerhetsakten ger enskilda medlemsstater möjlighet att reglera krav genom att göra certifiering enligt aktens certifieringsordningar obligatorisk på nationell nivå. I dessa fall får certifiering direkta marknadstillträdeeffekter i dessa länder. Till exempel har Tyskland redan idag en nationell certifieringsordning för 5G-utrustning[14] baserad på GSMA-NESAS, vilken EU5G också till stor del baseras på. Således kan certifiering enligt den kommande certifieringsordningen för 5G-system bli en förutsättning för att svenska leverantörer ska få tillträde till den stora tyska marknaden om Tyskland gör EU5G obligatorisk, även om ingen tvingande sådan reglering genomförts på EU-nivå.

Slutsatsen blir att sektorsmyndigheter, verksamhetsutövare och leverantörer av produkter och tjänster som berörs, eller kan beröras, av EU-regleringar som nämns i detta avsnitt blir intressenter av de certifieringsordningar och standarder som utvecklas inom ramen för cybersäkerhetsakten.

Leverantörer av produkter och tjänster som kan komma att omfattas av enskilda medlemsstaters reglering med referens till cybersäkerhetsakten blir intressenter även i dessa fall.

7.1 Inledning

Cybersäkerhetsakten (CSA) stipulerar att om det föreskrivs i en viss unionsrättsakt, får ett certifikat eller en EU-försäkran om överensstämmelse som utfärdats enligt en europeisk ordning för cybersäkerhetscertifiering användas för att påvisa presumtion om överensstämmelse med kraven i den rättsakten. I detta kapitel presenteras kort ett antal EU-rättsakter som innehåller cybersäkerhetskrav och referenser till olika typer av certifiering eller annan reglering med någon form av tredjepartsbedömningar av uppfyllnad av i akterna stipulerade cybersäkerhetskrav, med eller utan tydliga kopplingar till cybersäkerhetsakten. Omvänt torde resultat av granskningar av cybersäkerhet i enlighet med andra EU-rättsakter, under specifika betingelser, kunna användas som bevis vid CSA-certifiering.

EU-rättsakter med krav på CSA-certifiering (eller annan certifiering mot motsvarande cybersäkerhetskrav) kan innebära att sådana certifieringar blir en dominerande faktor för dessa cybersäkerhetskrav (inkl. krypto). Dessa krav kan påverka förutsättningarna för såväl svenskt genomförande av dessa rättsakter (som NIS2-direktivet m.fl.) samt även hur de produkter och tjänster som används inom säkerhetskänslig verksamhet utformas, vilket i sin tur kan påverka svenska leverantörers marknadstillträdelse inom EU.

[13] REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework

[14] https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-NESAS/NESAS-CCS-GI_node.html

I avsaknad av harmoniserad unionsrätt får en medlemsstats nationella rätt också föreskriva att en europeisk ordning för cybersäkerhetscertifiering får användas för fastställande av presumtionen om överensstämmelse med de rättsliga kraven. Det finns en rad EU-rättsakter med cybersäkerhetskrav samt referenser till CSA-certifiering (eller annan liknande certifiering) som presumtion för uppfyllnad av dessa krav (t.ex. NIS2, CRA och eIDAS2 (för ”e-plånboken”)).

Utöver eventuell EU-reglering ger cybersäkerhetsakten enskilda länder möjlighet att reglera certifiering på nationell nivå, varför certifiering då kan få direkt marknadstillträdeeffekter i dessa länder. T.ex. har Tyskland redan idag en nationell certifieringsordning för 5G-utrustning baserad på GSMA-NESAS, vilket EU5G också till stor del avser basera sig på. Således kan certifiering enligt den kommande certifieringsordningen för 5G-system bli en förutsättning för att svenska leverantörer ska få tillträde till den stora tyska marknaden om Tyskland gör EU5G obligatorisk, även om ingen tvingande sådan reglering genomförts på EU-nivå.

7.2 Vem berörs av EU:s cybersäkerhetskrav och cybersäkerhetscertifiering?

Det är väldigt många olika typer av organisationer som berörs av cybersäkerhetskrav och cybersäkerhetscertifiering för att uppfylla dessa krav i EU-rättsakterna som beskrivs i denna rapport. Med lite variation per EU-rättsakt berörs dessa organisationer:

- Standardiseringsorgan, eftersom det är de som tar fram standarder, ofta på begäran från Europeiska kommissionen;
- Alla företag, myndigheter och andra organisationer som deltar i framtagande av standarder;
- Alla företag, myndigheter och andra organisationer som verkar som organ för bedömning av överensstämmelse utifrån standarder;
- Lagstiftare, som t.ex. kan vilja kräva att certifieringar används eller att standarder följs, antingen som direkt lagstiftningskrav eller som presumtion för uppfyllnad av lagkrav, eller mer indirekt som krav som måste ställas vid vissa upphandlingar.
- Alla myndigheter som bedriver tillsyn, har föreskriftsrätt eller andra uppgifter i respektive EU-rättsakts genomförande. Det finns dels myndigheter med dessa uppgifter för respektive relevant sektor, t.ex. NIS-sektorerna, samt Myndigheten för samhällsskydd och beredskap som för NIS avses få både sektorbaserade uppgifter och ansvar men också vissa sektorsövergripande uppgifter och ansvar. Utöver det har Försvarets materielverk och Swedac uppgifter och ansvar för cybersäkerhetsakten och för varje CSA-certifieringsordning i enlighet med lagen (2021:553) respektive förordningen (2021:555) med kompletterande bestämmelser till EU:s cybersäkerhetsakt.

7.3 EU-rättsakter med referens till cybersäkerhetscertifiering

EU-rättsakter med referenser till cybersäkerhetscertifiering redovisas i tabellen nedan (kolumn 1) inklusive om rättsakten kräver certifiering eller ger KOM mandat att kräva certifiering (kolumn 2), eller om rättsakten mer eller mindre explicit stipulerar

att CSA-certifiering utgör presumtion för uppfyllande av respektive akts cybersäkerhetskrav (kolumn 3)[15]:

EU-rättsakt	**(x): CSA-cert. krävs [x]: KOM kan kräva CSA-cert.**	**x: explicit presumtion (x): förmodad presumtion**
NIS2 – Nät- och informationssäkerhetsdirektivet	[x]	x
CER-direktivet – Critical Entities Resilience Directive		(x)
CRA – Cyberresiliensakten	[x]	x
AI-akten – Akten om artificiell intelligens		x
eIDAS2 – Bl.a. certifiering av e-plånböcker	(x)	
DORA – Digital Operational Resilience Act		(x)
Cybersäkerhetsakten+ – Certifiering av ”hanterade cybersäkerhetstjänster”	[x]	
Färdskrivarförordningen	(x)	(x)
Maskinförordningen		x
RED – Radioutrustningsdirektivet		(x)
Elnätskodex		(x)

Som framgår av tabellen ovan är det fråga om många rättsakter där flertalet har tämligen stränga cybersäkerhetskrav (jämför även bilaga 3).

EU-rättsakterna med relevans för CSA-certifiering som beskrivs mer i detalj i bilaga 3 omfattar:

- EU-regleringar där CSA-certifiering krävs eller utgör presumtion för uppfyllnad av cybersäkerhetskraven.
- Vem eller vad som omfattas av regleringen.
- Typ av cybersäkerhetskrav med relevans för cybersäkerhetsakten.
- Vilka svenska myndigheter som har (eller kan antas ha/få) ansvar för det svenska genomförandet (tillsyn, föreskriftsrätt, m.m.).
- Om certifiering *måste användas* (krav) eller om certifiering anges *användbart eller önskvärt* som presumtion för kravuppfyllelse. Olika typsituationer för sådan presumtion beskrivs i bilaga 2.
- Om EU-kommissionen ges möjlighet i EU-rättsakten att anta (eller har antagit) delegerade akter eller genomförandeakter om certifiering.

[15] Även där inte CSA-certifiering nämns som ett sätt att påvisa efterlevnad av cybersäkerhetskrav (och rättsläget därför är mer osäkert) utgår vi ifrån att dessa certifikat i vissa situationer ändå kan användas på detta sätt, se bilaga 2.

- De fall där vi identifierat att det finns svensk eller annan medlemsstats reglering med krav på certifiering.

7.4 NIS2-direktivet

Syfte och omfattning:

NIS2-direktivet[16] ersätter det tidigare NIS-direktivet från 2016.

NIS2-direktivet skärper kraven för verksamhetsutövare jämfört med det tidigare NIS-direktivet. Kraven gäller för såväl offentliga som privata verksamhetsutövare samt större delen av offentlig sektor som sådan. Verksamhetsutövaren ska vidta tekniska, driftsrelaterade och organisatoriska riskhanteringsåtgärder (vilket i nuvarande lagstiftning benämns som säkerhetsåtgärder), för att skydda nätverks- och informationssystem och systemens fysiska miljö mot incidenter. Åtgärderna ska utgå från ett allriskperspektiv och en riskanalys och vara proportionella i förhållande till risken. De ska utvärderas och särskilt innefatta en rad saker som listas i direktivet.

Det finns två viktiga skillnader mellan gällande lagstiftning och det nya direktivet. Den första är att NIS2-direktivet omfattar betydligt fler aktörer och sektorer. Den andra viktiga skillnaden är att kraven kommer att gälla för hela verksamheten, inte bara för samhällsviktiga och digitala tjänster.

För privata verksamhetsutövare gäller som huvudregel ett storlekskrav med innebörd att verksamheten måste sysselsätta minst 50 personer eller ha en årsomsättning som överstiger 10 miljoner euro för att omfattas av lagen.

Certifieringskoppling:

EU-kommissionen kan anta delegerade akter där de kan ange vilka kategorier av väsentliga eller viktiga entiteter som ska vara skyldiga att använda vissa certifierade IKT-produkter, -tjänster och -processer eller erhålla ett CSA-certifikat.

Medlemsstat får ålägga NIS-entiteter att använda certifierade IKT-produkter, -tjänster och -processer, varvid CSA-certifikatet ger en presumtion om att cybersäkerhetskraven i direktivet är uppfyllda.

Vid utmätning av vissa sanktioner skall i förmildrande riktning ska beaktas om verksamhetsutövaren har följt godkända uppförandekoder eller godkända certifieringsmekanismer.

7.5 CER-direktivet – Critical Entities Resilience Directive

Syfte och omfattning:

[16] EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet).

CER-direktivet[17] syftar till att minska sårbarheter och stärka den fysiska motståndskraften hos samhällsviktig verksamhet (i direktivet benämnda kritiska entiteter) inom EU för att säkerställa ett oavbrutet tillhandahållande av tjänster som är väsentliga för ekonomin och samhället som helhet samt öka motståndskraften hos den samhällsviktiga verksamhet som tillhandahåller dessa tjänster.

Certifieringskoppling:

CER-direktivet refererar inte till CSA-certifiering direkt, på t.ex. det sätt som NIS2-direktivet gör. Men de säkerhetskrav som ställs i CER kan förväntas motsvara de i NIS2-direktivet eller även annars tangera säkerhetskrav som kommer ställas i de CSA-baserade certifieringsordningarna. Till exempel ställs det i CER-direktivet krav på fysiskt skydd vilket det också finns i EUCC:s krav på leverantören att fysiskt skydda utvecklingsmiljön, designdokumentation och den känsliga programkoden. Givet att ett certifikat utgivet i enlighet med någon av certifieringsordningarna i CSA presumerar efterlevnad i den del certifikatet täcker krav ställda i CER, kan certifieringsordningarna därför komma att ha stor betydelse även för CER. Detta vare sig certifikat används frivilligt, krävs vid upphandlingar eller införs som generellt krav via nationell lagstiftning. Där det sist nämnda i så fall är en inriktning som sker på nationell nivå.

7.6 Cyberresiliensakten – Cyber Resilience Act (CRA)

Syfte och omfattning:

Syftet med CRA[18] är att skapa förutsättningar för utvecklingen av säkra produkter med digitala element genom att säkerställa att hårdvaru- och programvaruprodukter har färre sårbarheter när de släpps ut på marknaden och att tillverkarna tar säkerheten på allvar under produktens hela livscykel. Det ska även skapas förutsättningar för att användarna ska kunna ta hänsyn till cybersäkerheten när de väljer och använder produkter med digitala element.

Certifieringskoppling:

CRA medför omfattande krav på berörda aktörer, i synnerhet de som tillhandahåller, producerar, distribuerar eller använder s.k. högriskprodukter med it-funktionalitet. Detta inkluderar krav på riskhantering, dokumentation, transparens, informations- och cybersäkerhet, kvalitetskontrollsystem, ackreditering av certifieringsorgan, standardisering, CE-märkning, och därtill en kraftfull tillsyn med koordinerade s.k. ”sweeps”, där funna brister kan leda till höga sanktioner samt förbud mot att sätta produkten på marknaden.

Regelefterlevnad uppvisas genom en så kallad konformitetsbedömning av krav. Produkter med digitala inslag som har certifierats under en europeisk cybersäkerhetscertifieringsordning ska antas vara i överensstämmelse med de

[17] EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG.

[18] Färdigförhandlad men inte slutligt antagen. Senast publicerade utkast: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_17000_2023_INIT.

väsentliga kraven i förslaget. EU-kommissionen kan genom delegerade akter kräva certifiering och därvid bestämma assuransnivåer och göra riskbedömningar, framför allt i beaktande av produkternas användning i NIS2-verksamhetsutövarnas system. EU-kommissionen ska, när det är applicerbart, specificera om ett CSA-certifikat ger tillverkaren undantag från skyldigheterna att genomföra en konformitetsbedömning genom anmälda organ.

Tillsyn samt myndigheter och andra berörda verksamhetsutövare:

I första hand gäller den generella uppräkningen av myndigheter och andra berörda verksamhetsutövare i avsnitt 7.2 som har en roll inom tillsyn. Dessutom ska nationella myndigheter utföra marknadsövervakning och tillsyn inom medlemsstatens territorium.

7.7 Förordningen om artificiell intelligens – AI Act

Syfte och omfattning:

AI-förordningen[19] riktar sig till alla tillhandahållare, tillverkare, distributörer (och i viss mån användare) av AI-system (informationssystem som använder AI-algoritmer). Syftet med förslaget till förordning är bl.a. att harmonisera regler för AI inom EU och att säkerställa att AI-system som placeras och används på den inre marknaden är säkra. AI-förordningens förslag innebär bl.a. förbud mot vissa former av ”högrisk-AI” och omfattande krav på berörda aktörer, i synnerhet om de tillhandahåller, producerar, distribuerar eller använder högrisk-AI-system. Kraven inkluderar bl.a. krav på riskhantering, ”data governance”, dokumentation, informations- och cybersäkerhet (allrisk), kvalitetskontrollsystem, ekosystem av certifieringsorganisationer (”notified bodies”), standardisering samt CE-märkning.

Certifieringskoppling:

AI-system med hög risk som har CSA-certifierats, (eller för vilka en CSA-försäkran om överensstämmelse har utfärdats vid assuransnivån Grundläggande), ska förutsättas överensstämma med cybersäkerhetskrav som anges i artikel 15 i AI-förordningen, förutsatt att cybersäkerhetscertifikatet eller försäkran om överensstämmelse eller delar därav omfattar dessa krav. Enisa har Q4 2023 startat en tematisk grupp som tittar på vilka områden som har mogna standarder att certifiera emot.

Tillsyn samt myndigheter och andra berörda verksamhetsutövare:

Den generella uppräkningen av myndigheter och andra berörda verksamhetsutövare i avsnitt 7.2 omfattar de som har en roll inom tillsyn. Dessutom innehåller AI-akten bestämmelser om marknadskontroll och rapporteringsskyldigheter för tillhandahållare när det gäller utredning av AI-relaterade incidenter och tekniska problem. Akten anger också vilken typ av information som tillhandahållare av AI-system ska hålla och kunna delge behöriga myndigheter, vilken information som

[19] Färdigförhandlad men inte slutligt antagen. Senast publicerade utkast: https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf

myndigheter får och ska inhämta, relationen mellan behöriga myndigheter och kommissionen.

7.8 Förordning om elektronisk ID (EIDAS2)

Syfte och omfattning:

eIDAS2-förordningen[20] innebär att alla EU-länder ska kunna erbjuda medborgare och företag digitala plånböcker som kan kopplas till deras nationella digitala identitet med bevis på andra personliga attribut (t.ex. körkort, utbildningsbevis och bankkonton). E-identitetsplånböckerna ska tillhandahållas av offentliga myndigheter eller privata enheter godkända av offentlig myndighet. EU-förhandlingen kring förslaget pågår. EU-kommissionen har startat arbetsgrupper för att diskutera vilka specifika krav som skall ställas på e-plånboken och hur plånboken kan certifierias, inklusive vilka skyddsprofiler (Protection Profiles) som behövs för det, jämför. avsnitt 6.16.2.

Certifieringskoppling:

En ändring som tillkommit under EU-förhandlingen av förslaget är att europeiska e-identitetsplånböcker *ska* CSA-certifieras. Enligt det ursprungliga förslaget utgjorde CSA-certifiering endast en presumtion för uppfyllnad av cybersäkerhetskrav. Man kan förmodligen anta att en tvingande CSA-certifiering innebär att man vid tillsynen inte skall ifrågasätta ett CSA-certifikat.

EU-kommissionen ska genom genomförandeakter upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för certifiering av de europeiska e-identitetsplånböckerna. EU-kommissionen får anta delegerade akter för särskilda kriterier som skall uppfyllas av certifierinsorgan under CSA. Så länge som CSA-ordningar för cybersäkerhetscertifiering inte eller endast delvis omfattar de relevanta cybersäkerhetskraven för e-identitetsplånböcker ska medlemsstaterna för dessa krav inrätta nationella certifieringssystem i enlighet med de krav som fastställs i genomförandeakter från EU-kommissionen.

Tillsyn samt myndigheter och andra berörda verksamhetsutövare:

När de föreslagna ändringarna i eIDAS2-förordningen träder i kraft, innebär det också att en rad nya krav måste mötas. Sverige måste bl.a. exempelvis inrätta ett bedömningsorgan som har till uppdrag att certifiera e-legitimationslösningar som uppnår tillitsnivåerna i förordningen. De europeiska e-identitetsplånböckernas överenstämmelse med cybersäkerhetskraven certifieras av ackrediterade offentliga eller privata organ som utses av medlemsstaterna.

7.9 DORA-förordningen – Digital Operational Resilience Act

Syfte och omfattning:

[20] Antagen men ej publicerad i EUR-Lex. Antagen version: https://data.consilium.europa.eu/doc/document/PE-68-2023-INIT/en/pdf.

DORA-förordningens[21] syfte är att bidra med en ökad digital operativ motståndskraft inom EU:s finanssektor och dess kritiska IKT- (informations- och kommunikationsrelaterade) tjänster. DORA kommer till exempel att gälla för organisationer som tillhandahåller: revisionstjänster, försäkringstjänster, bank- och finanstjänster, kryptotjänster, värdepapperstjänster samt för tredjepartsleverantörer av IKT-tjänster.

Certifieringskoppling:

För att genomföra tillsynsverksamheten får den ledande tillsynsmyndigheten ta hänsyn till relevanta tredjepartscertifieringar och interna eller externa IKT-revisionsrapporter som den kritiska tredjepartsleverantören av IKT-tjänster har gjort tillgängliga. EU-kommissionen ges befogenhet att komplettera denna förordning genom att anta tekniska standarder för tillsyn. Motsvarande gäller för penetrationstestning och penetrationstestare inom området.

7.10 Dataförvaltningsförordningen

Syfte och omfattning:

Enligt dataförvaltningsförordningen[22] ska deltagare i dataområden som erbjuder data eller datatjänster till andra deltagare uppfylla väsentliga krav för att underlätta interoperabiliteten mellan data, datadelningsmekanismer och datadelningstjänster samt mellan gemensamma europeiska dataområden.

Certifieringskoppling:

För att förhindra olaglig statlig åtkomst till icke-personuppgifter av myndigheter i tredjeländer bör leverantörer av databehandlingstjänster som omfattas av denna förordning, däribland molntjänster och edgetjänster, vidta alla rimliga åtgärder för att förhindra åtkomst till system där icke-personuppgifter lagras, inbegripet, när så är lämpligt, genom kryptering av data, frekventa revisioner, verifierad anslutning till relevanta certifieringssystem för säkerhetsförsäkran och ändring av företagspolicyer. EU-kommissionen ges befogenhet att anta delegerade akter som ytterligare specificerar de väsentliga kraven rörande interoperabilitet.

7.11 Cybersäkerhetsaktens utvidgning till förvaltade säkerhetstjänster

Syfte och omfattning:

Cybersolidaritetsakten syftar till att stödja en gradvis uppbyggnad av en gemensam cyberreserv på EU-nivå med leverantörer av förvaltade säkerhetstjänster, , redo att

[21] EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011.

[22] EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2023/2854 av den 13 december 2023 om harmoniserade regler för skälig åtkomst till och användning av data och om ändring av förordning (EU) 2017/2394 och direktiv (EU) 2020/1828 (dataförordningen).

ingripa på medlemsstaternas begäran vid omfattande antagonistiska cyberincidenter. I detta syfte föreslås parallellt attcybersäkerhetsakten[23] utvidgas till att inbegripa dessa förvaltade säkerhetstjänster.

Certifieringskoppling:

Certifieringen av förvaltade säkerhetstjänster kan bli relevant för alla EU-rättsakter som refererar till CSA-certifiering, särskilt NIS2- och CER-direktiven.

7.12 Färdskrivarförordningen

Syfte och omfattning:

Alla fordon som omfattas av reglerna om kör- och vilotider inom EU ska vara utrustade med färdskrivare, enligt Europaparlamentets och Rådets förordning (EU) nr 165/2014. I färdskrivaren, som ska vara typgodkänd, registreras bland annat förarnas kör- och vilotider. Med hjälp av uppgifterna som registrerats i färdskrivaren kan förare, företag och kontrollmyndigheter kontrollera att reglerna följts.

Certifieringskoppling:

Säkerhetscertifikat bör utfärdas av ett certifieringsorgan som erkänts av förvaltningskommittén inom ramen för det avtal om ömsesidigt erkännande av certifikat för evaluering av it-säkerhet (Mutual Recognition Agreement of Information Technology Security Evaluation Certificates) som ingåtts av gruppen av höga tjänstemän på informationssäkerhetsområdet (SOG-IS). CSA-ordningen för EUCC (IKT-produkter evalueras/certifieras mot Common Criteria) är färdigförhandlad och täcker färdskrivare. Trots att EUCC är klar är det omdiskuterat om/hur detta kan ersätta nuvarande system med ömsesidigt godkännande inom SOG-IS som också baserar sig på evaluering/certifiering mot Common Criteria.

EU-kommissionen ges befogenhet att anta delegerade akter för vissa saker men inte rörande den kategori av produkter där man refererar till CSA-certifiering.

7.13 Maskinförordningen

Syfte och omfattning:

I maskinförordningen[24] fastställs hälso- och säkerhetskrav för konstruktion och tillverkning av maskiner, relaterade produkter och delvis fullbordade maskiner för att möjliggöra tillhandahållande på marknaden eller ibruktagande av dem, samtidigt som en hög nivå säkerställs i fråga om skydd av människors, särskilt konsumenters och yrkesmässiga användares, hälsa och säkerhet.

---

[23] Antagen men ej publicerad i EUR-Lex. Antagen version: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_8024_2024_INIT&qid=1714079047470.

[24] Regulation (EU) No 165/2014 of the European Parliament and of the Council of 4 February 2014 on tachographs in road transport, repealing Council Regulation (EEC) No 3821/85 on recording equipment in road transport and amending Regulation (EC) No 561/2006 of the European Parliament and of the Council on the harmonisation of certain social legislation relating to road transport.

Certifieringskoppling:

Maskiner och relaterade produkter som har certifierats eller för vilka en försäkran om överensstämmelse har utfärdats enligt en CSA-ordning ska förutsättas överensstämma med de grundläggande hälso- och säkerhetskraven i förordningen i den mån dessa krav omfattas av cybersäkerhetscertifikatet eller försäkran om överensstämmelse eller delar av dem. Genom att upprätta EU-försäkran om överensstämmelse tar tillverkaren ansvar för att maskinen eller den relaterade produkten uppfyller kraven i denna förordning.

7.14 Radioutrustningsdirektivet

Syfte och omfattning:

Produkter med radiokomponenter (radioutrustning) regleras av radioutrustningsdirektivet[25]. Det ställs i RED många krav på radioutrustningen, varav en del handlar om att den, grovt förenklat, ska fungera som kommunikationsutrustning, vilket vi i denna rapport därmed menar är en typ av cybersäkerhetskrav.

Certifieringskoppling:

Det finns i dagens RED ingen direkt koppling till cybersäkerhetsakten. Regleringen är av karaktären New Legislative Framework (NLF) och kopplar därmed inte till certifieringar, varken generellt eller till cybersäkerhetsakten. Jämför. emellertid kommentar om koppling mellan NLF och CSA-certifiering i exempel 2 c) i bilaga 2.

7.15 Elnätskodex

Syfte och omfattning:

EU-kommissionens delegerade akt om cybersäkerhetsaspekter av gränsöverskridande elflöden (här kallad ”Elnätskodex)[26] innehåller regler för elförsörjningen i EU (”nätföreskrifter”) för att åtgärda it-säkerhetsaspekter avseende elflöden över gränserna. Det ska bidra till att elsystemet i EU blir mer resilient och säkert. De allmänna bestämmelser om säkerhet i nätverks- och informationssystem som fastställs i direktiv (EU) 2022/2555 (NIS 2-direktivet) kompletteras av denna elnätskodex.

Certifieringskoppling:

Berörda EU-samarbetsorgan (där svenska myndigheter kan delta) ska säkerställa att rekommendationerna för upphandling av cybersäkerhet är förenliga med och tar

[25] Europaparlamentets och rådets direktiv 2014/53/EU av den 16 april 2014 om harmonisering av medlemsstaternas lagstiftning om tillhandahållande på marknaden av radioutrustning och om upphävande av direktiv 1999/5/EG.

[26] KOMMISSIONENS DELEGERADE FÖRORDNING (EU) …/…av den 11.3.2024 om komplettering av Europaparlamentets och rådets förordning (EU) 2019/943 genom inrättandet av en nätföreskrift om sektorsspecifika regler för cybersäkerhetsaspekter av gränsöverskridande elflöden.

hänsyn till de senast tillgängliga europeiska ordningarna för cybersäkerhetscertifiering som är relevanta för IKT-produkten, IKT-tjänsten eller IKT-processen.

De avancerade cybersäkerhetskontrollerna i leveranskedjan ska omfatta kontroller av verksamhetsutövare med kritisk påverkan för att under upphandling kontrollera att IKT-produkter, -tjänster och -processer som kommer att användas som tillgångar med kritisk inverkan uppfyller cybersäkerhetsspecifikationerna. IKT-produkten, IKT-tjänsten eller IKT-processen ska verifieras antingen genom en europeisk ordning för cybersäkerhetscertifiering eller genom verifieringsverksamhet som väljs ut och organiseras av verksamhetsutövare.

De icke-bindande rekommendationer för upphandling av cybersäkerhet som utarbetas genom förordningen får innehålla sektorsspecifik vägledning om användningen av certifieringsordningar, när ett lämpligt system finns tillgängligt för en typ av IKT-produkt, IKT-tjänst eller IKT-process som används av verksamhetsutövaremed kritisk påverkan, utan att det påverkar ramen för inrättandet av CSA-ordningar. Ansvariga för överföringssystem ska, med bistånd av EU-samarbetsorganen på området, ha ett nära samarbete med Enisa när det gäller att tillhandahålla den sektorsspecifika vägledning som ingår i icke-bindande rekommendationer om cybersäkerhetsupphandling

7.16 Allmän dataskyddsförordning – GDPR/DSF

Syfte och omfattning:

I GDPR[27] fastställs bestämmelser om skydd för fysiska personer med avseende på behandlingen av personuppgifter och om det fria flödet av personuppgifter samt rätten till skydd av personuppgifter. Enligt GDPR ska personuppgifter bl.a. behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder för att skydda integritet och konfidentialitet hos persondata.

Certifieringskoppling:

I cybersäkerhetsakten stipuleras att den inte ska påverka tillämpningen av unionsrätt som innehåller särskilda bestämmelser om certifiering av IKT-produkter, -tjänster och -processer, t.ex. GDPR. Det certifieringsramverk som regleras i GDPR har alltså ingen direkt koppling till CSA-certifiering. Man bör dock kunna utgå ifrån att tillsynsmyndigheter i sin tillsyn av cybersäkerhetsskyddsåtgärder reglerade i enlighet med GDPR även kan beakta certifikat utgivna under en CSA-ordning, om detta certifikat täcker de krav vars efterlevnad är föremål för tillsyn enligt GDPR.

[27] Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (den allmänna dataskyddsförordningen. Jfr. art. 1.1 st. 2 i GDPR och ss. 12-13 i Prop. 2020/21:186.

8 Nationell reglering med relevans för uppdraget

Försvarets materielverks bedömning:

Såväl EU-rätt, nationelltgenomförande av EU-rätt samt annan nationell rätt påverkar verksamhetsutövare (privata och offentliga) såväl som sektorsmyndigheter som genom t.ex. tillsyn, föreskrifter och samordning som också påverkar verksamhetsutövarna.

Vid genomförandet av uppdraget har det inte funnits förutsättningar att göra någon fullständig kartläggning av berörda privata och offentliga verksamhetsutövare som kan vara intressenter i certifieringar enligt cybersäkerhetsakten.

Inom NIS2-direktivets genomförande har 11 tillsynsmyndigheter inom 18 sektorer identifierats, med drygt 4.200 tillsynsobjekt/verksamhetsutövare. Antalet bedöms dock vara större, särskilt för t.ex. Läkemedelsverket som hanterar en rad aktörer (till exempel ca 7.500 aktörer inom läkemedelsområdet). För övrig reglering inom ramen för de EU-regleringar som presenterats i denna rapport tillkommer fem myndigheter där antalet tillsynsobjekt inte analyserats.

Säkerhetspolisen och Försvarsmakten är myndigheter med ansvar för föreskrifter, tillsyn och samordning inom säkerhetsskydd. Utöver det bedriver ett antal tillsynsmyndigheter tillsyn avseende säkerhetsskydd över en rad myndigheter och enskilda verksamhetsutövare kopplat till olika sektorer. T.ex. bedriver Säkerhetspolisen tillsyn över åtminstone 120 myndigheter som spänner över vitt skilda områden, från de brottslighetshanterande myndigheterna till de stora samhällsviktiga myndigheterna (undantaget försvarsmyndigheter) som t.ex. Skatteverket, Försäkringskassan, Myndigheten för samhällsskydd och beredskap samt de olika infrastrukturrelaterade myndigheterna m.m. Försvarsmakten bedriver tillsyn över alla försvarsrelaterade myndigheter. Affärsverket Svenska Kraftnät, Transportstyrelsen och Post- och telestyrelsen m.fl. myndigheter bedriver tillsyn över enskilda verksamhetsutövare inom respektive infrastrukturområden (till stor del jämförbart med den föreslagna cybersäkerhetslagens sektorstäckning). Alla tillsynsmyndigheter ska ha överblick över sina tillsynsobjekt, t.ex. har Post- och telestyrelsen 12 tillsynsobjekt.

Beredskapsmyndigheterna ansvarar, enligt förordning (2022:524) om statliga myndigheters beredskap, för att egna informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt. Myndigheten för samhällsskydd och beredskap får meddela ytterligare föreskrifter om sådana säkerhetskrav. Beredskapsmyndigheterna är de 21 länsstyrelserna och ytterligare 39 uppräknade centrala myndigheter. Det rör sig således om totalt 59 viktiga samhällsfunktioner, exklusive försvarsmyndigheterna som inte anges som särskilda beredskapsmyndigheter. Fördelningen av beredskapssektorer och sektorsansvariga myndigheter tangerar till stor del den föreslagna cybersäkerhetslagens sektorer och sektorsmyndigheter.

Eftersom CSA-certifiering kan vara relevant inom alla dessa sektorer, inklusive försvarssektorn, som ett medel för verksamhetsutövare att visa att man uppfyller stipulerade (ofta omfattande) cybersäkerhetskrav, och att certifiering i närtid kan bli tvingande, är det flera myndigheter och privata verksamhetsutövare som bör bevaka

och försöka påverka när certifiering bör användas och, om certifiering blir obligatoriskt, påverka innehållet i certifieringskraven. Det är sektorerna och dess tillhörande myndigheter som kan och därmed bör ha huvudansvar för detta.

8.1 Svensk reglering och ansvarsfördelning för EU-rättens genomförande

Som vi sett i kapitel 7 finns det en rad EU-rättsakter med cybersäkerhetskrav inom olika områden. Dessa cybersäkerhetskrav är antingen direkt tillämpliga genom EU-förordning eller ska om det är fråga om ett EU-direktiv överföras till svensk lagstiftning. Dessa EU-rättsakter ställer krav på att det ska finnas olika typer av nationella myndigheter för genomförandet och att dessa ska ha vissa uppgifter och befogenheter. Det är dock svensk lagstiftning som pekar ut vilka svenska myndigheter som ska ha dessa uppgifter och befogenheterna och därvid reglerar t.ex. detaljerna kring tillsynsbefogenheter samt ger myndigheterna ifråga t.ex. föreskriftsrätt där det anses behövas för det nationella genomförandet.

Utöver att Försvarets materielverk generellt är nationell genomförande- och tillsynsmyndighet för certifieringsramverket (se kapitel 9) är det många nationella myndigheter som är ansvariga för tillsynen av uppfyllande av cybersäkerhetskraven som sådana inom sina sektorer. Vilka myndigheter det rör sig om kommer att beskrivas summariskt per EU-rättsakt i detta kapitel. Ibland kommer detta bara ange vad EU-rättsakten eller förslaget till akt kräver för typ av myndighet eller organ, ibland anges den i Sverige utsedda myndigheten, ibland ett antagande rörande vilka myndigheter som kan komma att bli utsedda för respektive reglering. En mer utförlig beskrivning ges i bilaga 3. För till exempel det svenska genomförandet av det nya NIS-direktivet, NIS2[28], föreslås i SOU 2024:18 Nya regler om cybersäkerhet att en rad myndigheter ska ha detta ansvar, även för NIS2:s tillkommande sektorer, medan Myndigheten för samhällsskydd och beredskap fortsatt föreslås som samordnande myndighet för regleringens genomförande.

Se vidare nedan en tabell över de EU-rättsakterna som är beskrivna i denna rapport (kolumn 1), kopplade till de typer av nationella sektorsmyndigheter som på ett eller annat sätt har getts eller föreslås få ansvar för det nationella genomförandet av respektive akt (kolumn 2). I kolumn 2 anges också för NIS-direktivet vilka sektorer det är fråga om och antalet befintliga (enligt befintliga NIS-direktivet) eller prognostiserade [enligt utredningen för NIS2-direktivet] tillsynsobjekt.

EU-rättsakt	**Sektorsmyndigheter (tillsyn/föreskrifter/m.m.)** Befintliga tillsynsobjekt inom (parentes) Prognostiserade tillsynsobjekt inom [hakparentes]

[28] Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet)

NIS2, Nät- och infromationssäkerhets-direktivet	**Statens energimyndighet (249) [598]**: energi **Transportstyrelsen (130) [750]:** transporter/tillverkning (del av) **Finansinspektionen (12):** för bank/finansmarknadsinfrastruktur **Inspektionen för vård och omsorg (240) [819]:** hälso- och sjukvårdssektorn (del av), **Läkemedelsverket:** hälso- och sjukvårdssektorn (del av)/tillverkning (del av) **Livsmedelsverket (94) [525–675]** dricksvatten/avloppsvatten/livsmedel **Post- och telestyrelsen (60) [1100]** digital infrastruktur/digitala leverantörer/IKT-tjänster/post- och budtjänster/rymden **Läkemedelsverket** hälso- och sjukvårdssektorn (ej vårdgivare) /medicintekniska produkter **Länsstyrelserna i Stockholms [180], Skåne, Västra Götalands [110] och Norrbottens län:** Offentlig förvaltning/avfallshantering/forskning/kemikalier (del av)/ lärosäten med examenstillstånd **MSB:** riskhanteringsåtgärder/systematiskt och riskbaserat informationssäkerhetsarbete för offentlig förvaltning och lärosäten med examenstillstånd **[49]** om.
CER-direktivet - Critical Entities Resilience Directive	Troligen relevanta **NIS2-myndighet(er)**.
CRA - Cyberresiliensakten	Utredning pågår.
AI-akten - Akten om artificiell intelligens	Utredning pågår.
eID – Bl.a. certifiering av e-plånböcker	Utredning pågår: Troligen **DIGG** för e-leg och e-identitetsplånboken och **PTS** för övriga ”betrodda tjänster” (dvs. ung. som idag).
DORA - Digital Operational Resilience Act	**Finansinspektionen**
CSA+ - Certifiering av ”hanterade cybersäkerhetstjänster”	Nyss färdigförhandlad: Troligen **FMV** och **Swedac** för motsvarande roller som för CSA-ramverket i övrigt.
Färdskrivarförordningen	**FMV**: Certifikat från CSEC.
Maskinförordningen	Ny förordning. Utredning pågår. Troligen **Arbetsmiljöverket** (som idag).
RED – Radioutrustnings-direktivet	**PTS**
Elnätskodex	Ny förordning. Troligen **Energimyndigheten** (eftersom reglerna kompletterar NIS2-direktivet).

Som framgår av tabellen ovan är det fråga om många rättsakter (flertalet med tämligen stränga cybersäkerhetskrav), väldigt många sektorer, väldigt många sektorsmyndigheter (med många, svåra och resurs- och kompetenskrävande uppgifter) samt väldigt många aktörer och tillsynsobjekt. Det gör sammantaget att det är väldigt svårt för respektive sektorsmyndighet att ha överblick och själva förstå hur deras cybersäkerhetsarbete, inklusive certifiering, bör bedrivas på ett nationellt harmoniserat sätt.

8.1.1 Försvarets materielverks uppgifter och ansvar vs myndigheter och verksamhetsutövare

Föreskrivande myndighet, om den fått det delegerat till sig via lag och förordning, ansvarar för att ge ut de föreskrifter som kan anses nödvändiga för att genomföra EU-rättsakten för den egna sektorn. Den föreskrivande myndigheten bör själv förstå vilket värde ett certifikat har och när det kan vara motiverat att via föreskrift kräva eller rekommendera certifiering (såvida detta inte redan är EU-reglerat).

Utsedd tillsynsmyndighet ansvarar för att se till att EU-rättsaktens cybersäkerhetskrav (och eventuella tillkommande nationellt föreskrivna cybersäkerhetskrav) efterlevs. Tillsynsmyndigheten måste därmed själv förstå vilket värde ett certifikat innebär vid bedömningen av om sektorns cybersäkerhetskrav är uppfyllda.

Det kan samtidigt noteras att det är en stor utmaning för varje sektorsmyndighet att på egen hand behärska alla kompetensområden som rör cybersäkerhet, inklusive kompetens att bedöma värdet av de olika certifieringsordningarna.

8.1.2 Ansvarsprincipen, närhetsprincipen och likhetsprincipen

En viktig del i svensk krishantering är vad som brukar kallas de tre grundprinciperna:

- **Ansvarsprincipen:** Den som har ansvar för en verksamhet under normala förhållanden ska ha det också under en krissituation. Det betyder t.ex. att det är den vanliga sjukvården som har hand om vården även vid en kris, att kommunerna sköter skola och äldreomsorg och så vidare.
- **Närhetsprincipen:** En kris ska hanteras där den inträffar och av dem som är närmast berörda och ansvariga. Det är t.ex. alltså i första hand den drabbade kommunen och den aktuella regionen som leder och arbetar med insatsen. Först om de lokala resurserna inte räcker till blir det aktuellt med statliga insatser.
- **Likhetsprincipen:** Under en kris ska verksamheten fungera på liknande sätt som vid normala förhållanden – så långt det är möjligt. Verksamheten ska också, om det är möjligt, skötas på samma plats som under normala förhållanden.

De tre ansvarsprinciperna stödjer rådande sektorsbaserade ansvarsfördelning kring arbetet med cybersäkerhet genom att:

- **Ansvarsprincipen:** Beredskapsmyndigheternas ansvar rörande cybersäkerhetsarbete som förberedelser för cybersäkerhetsrelaterade krislägen är till stora delar överlappande i och med att dessa myndigheter alltid enligt beredskapsförordningen har ett ansvar för säkerheten i egna informationssystem. Kunskaper och resurser som byggs upp i den egna delen kan nyttiggöras även för

andra. I de många och viktiga fall dessa myndigheter också utgör sektorsmyndighet med ansvar för cybersäkerhet eller säkerhetsskydd förstärks dessa synergieffekter ytterligare. Att i normalläget lägga ansvaret för cybersäkerhet på andra än de som ska agera i kris skulle därmed förmodligen försämra förmågan att hantera en cyberrelaterad kris. Detta talar för att de myndigheter som har olika typer av ansvar för cybersäkerhet idag skall behålla sitt ansvar. Men, detta arbete skulle dock kunna förstärkas av en central stödfunktion så att ett systematiserat och mindre fragmenterat cybersäkerhetsarbete med god överblick, nationellt, globalt och inom EU, kan bedrivas av hela statsförvaltningen. En sådan stödfunktion skulle även kunna ge goda synergieffekter, t.ex. kring gemensamma regler och råd, erfarenhets- och kunskapsöverföring samt expertisutbyte utan att ansvar från de myndigheter som har det idag.

- **Närhetsprincipen:** De synergieffekter som uppnås genom att ansvaret enligt ansvarsprincipen är fördelat på samma sätt vid normalläge som vid kris gör sig på liknande sätt gällande även rörande närhetsprincipen. Cybersäkerhetsfrågor är tekniska frågor som kräver teknisk kompetens för att lösa. De som hanterar ett system eller reglerar en sektor i normalläge har bättre förutsättningar än någon annan att göra det i krisläge, och det arbete man ändå måste lägga ned i förberedelser för cybersäkerhetsrelaterade kriser har man nytta av även i arbetet med cybersäkerhet i normalläget. Det är långt ifrån givet att högre beslutsnivåer skulle ha bättre teknisk kompetens i själva den tekniska problemlösningen, både vad det gäller förebyggande och återställande förmåga. Endast när andra överväganden behövs finns det anledning att lyfta frågan till högre beslutsnivåer.
- **Likhetsprincipen:** De synergieffekter som uppnås genom att ansvaret enligt ansvarsprincipen är fördelat på samma sätt vid normalläge som vid kris gör sig på liknande sätt gällande rörande likhetsprincipen. Cybersäkerhetsfrågor är tekniska frågor som kräver teknisk kompetens för att lösa. De som hanterar ett system eller reglerar en sektor i normalläge har bättre förutsättningar än någon annan att göra det i krisläge, och det arbete man ändå måste lägga ned i förberedelser för cybersäkerhetsrelaterade kriser har man nytta av även i arbetet med cybersäkerhet i normalläget. Men en gemensam förståelse kan underlätta samverkan vid en kris samt även att en stödfunktion kan användas.

8.2 NIS2-direktivet

NIS2-direktivet[29] har ersatt det tidigare NIS-direktivet från 2016. I SOU 2024:18 Nya regler om cybersäkerhet (presenterad för regeringen den 5 mars 2024) föreslås att NIS2-direktivet i huvudsak införlivas genom en ny lag, cybersäkerhetslagen, och att den tidigare NIS-lagen upphävs.

Det finns två viktiga skillnader mellan gällande lagstiftning och det nya förslaget till cybersäkerhetsreglering. Den första är att cybersäkerhetslagen föreslås omfatta betydligt fler aktörer, eftersom antalet sektorer utökas från 7 till 18. Den andra

[29] EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet).

viktiga skillnaden är att kraven kommer att gälla för hela verksamheten inte bara för samhällsviktiga och digitala tjänster.

Tillsyn samt myndigheter och andra berörda verksamhetsutövare:

Se för det första den generella uppräkningen av myndigheter och andra berörda verksamhetsutövare i avsnitt 7.2.

Medlemsstaterna ska utse behöriga myndigheter med ansvar för att övervaka tillämpningen av direktivet på nationell nivå. I direktivet fastställs även en ram för samarbete både på nationell nivå och mellan medlemsstaterna, vilket ska ske bl.a. genom en särskilt inrättad samarbetsgrupp. Nedan anges den föreslagna myndighetsorganisationen för genomförandet av NIS2.

Tillsynsmyndigheter med tillhörande sektorer enligt NIS2-utredningen:

- **Statens energimyndighet** ska vara tillsynsmyndighet för sektorn energi,
- **Transportstyrelsen** för sektorerna transporter och del av sektorn tillverkning,
- **Finansinspektionen** för sektorerna bankverksamhet och finansmarknadsinfrastruktur,
- **Inspektionen för vård och omsorg** för del av hälso- och sjukvårdssektorn,
- **Läkemedelsverket** för del av hälso- och sjukvårdssektorn och del av sektorn tillverkning, **Livsmedelsverket** för sektorerna dricksvatten, avloppsvatten och produktion, bearbetning och distribution av livsmedel, **Post- och telestyrelsen** för sektorerna digital infrastruktur, digitala leverantörer, förvaltning av IKT-tjänster, post- och budtjänster och sektorn rymden,
- **Länsstyrelserna i Stockholms, Skåne, Västra Götalands och Norrbottens län** för sektorerna offentlig förvaltning, avfallshantering, forskning, del av sektorn tillverkning och tillverkning, produktion och distribution av kemikalier samt lärosäten med examenstillstånd.
- **Myndigheten för samhällsskydd och beredskap** ska även fortsättningsvis leda ett samarbetsforum där tillsynsmyndigheterna ingår. Syftet med forumet ska vara att underlätta samordning och åstadkomma en effektiv och likvärdig tillsyn. Myndigheten för samhällsskydd och beredskap får i föreskrifter ange vilka verksamhetsutövare som omfattas av lagen om cybersäkerhet och om verksamhetsutövaren är väsentlig. För sektorn offentlig förvaltning och lärosäten med examenstillstånd får Myndigheten för samhällsskydd och beredskap i stället för länsstyrelserna i 8 § meddela föreskrifter om riskhanteringsåtgärder, systematiskt och riskbaserat informationssäkerhetsarbete.

Myndigheten för samhällsskydd och beredskap ska leda ett samarbetsforum där tillsynsmyndigheterna ingår. Syftet med forumet ska vara att underlätta samordning och åstadkomma en effektiv och likvärdig tillsyn.

Myndigheten för samhällsskydd och beredskap får, efter samråd med tillsynsmyndigheterna, meddela föreskrifter om vilka verksamhetsutövare som omfattas av cybersäkerhetlagen och om verksamhetsutövaren är väsentlig. Myndigheten för samhällsskydd och beredskap får också meddela föreskrifter om anmälningsskyldighet för verksamhetsutövarna.

Tillsynsmyndigheterna får, efter samråd med Myndigheten för samhällsskydd och beredskap, meddela föreskrifter om bl.a. riskhanteringsåtgärder och systematiskt och riskbaserat informationssäkerhetsarbete. För sektorn offentlig förvaltning och lärosäten med examenstillstånd får Myndigheten för samhällsskydd och beredskap i stället för de berörda länsstyrelserna meddela föreskrifter om bl.a. riskhanteringsåtgärder, systematiskt och riskbaserat informationssäkerhetsarbete.

Den myndighet som har tillsynsansvar och/eller föreskriftsrätt inom en sektor har typiskt sett bäst kunskaper om sektorn (och den privata marknad som därmed eventuellt är aktuell) i fråga och därmed bäst förutsättningar att veta vilken tillsyn som är möjlig, lämplig och effektiv. Det är också tillsynsmyndigheterna som bäst kan bedöma vilka föreskrifter som är lämpliga (effektiva men proportionerliga) inom sin sektor och dess marknad. Därför bör sektorsmyndigheterna (på relevant nivå) representera sin sektor vid utformningen av EU-regleringen på området. Detta avser typiskt sätt att bistå regeringen vid EU-förhandlingar i rådet eller att inom kommittéväsendet bistå regeringen eller själva representera Sverige vid framtagandet av delegerad eller genomförande lagstiftning.

Cybersäkerhetslagen (föreslagen genomförandelag för NIS2-direktivet) föreslås gälla i begränsad utsträckning för offentliga verksamhetsutövare som bedriver säkerhetskänslig verksamhet eller brottsbekämpning, men där den delen inte utgör en väsentlig andel. Motsvarande kommer att gälla för enskilda verksamhetsutövare som bedriver annan verksamhet tillsammans med säkerhetskänslig verksamhet eller brottsbekämpning. För den säkerhetskänsliga delen av verksamheten eller den delen av verksamheten som avser brottsbekämpning kommer det endast att gälla en anmälnings- och uppgiftsskyldighet.

Enligt utredningens förslag undantas säkerhetskänslig verksamhet från hela eller delar av cybersäkerhetslagens tillämpningsområde. Verksamhetsutövaren behöver inte heller lämna säkerhetsskyddsklassificerade uppgifter till tillsynsmyndigheten. Cybersäkerhetslagen gäller dock för övrig verksamhet som verksamhetsutövaren bedriver. Detta innebär att en tillsynsmyndighet kan bedriva tillsyn hos en verksamhetsutövare som även bedriver säkerhetskänslig verksamhet. Gränsdragningen rörande vad som utgör säkerhetskänslig verksamhet kan därmed bli avgörande för vilka delar av verksamheten som tillsynsmyndigheten kan bedriva tillsyn. För flera tillsynsområden kommer det att vara samma tillsynsmyndighet som bedriver tillsyn enligt säkerhetsskyddsregleringen och NIS2-regleringen. För några sektorer och verksamhetsutövare kommer det dock att vara olika tillsynsmyndigheter. Det finns därmed ett behov av samarbete mellan tillsynsmyndigheten för säkerhetsskyddslagen och tillsynsmyndigheten för cybersäkerhetslagen i de fall en verksamhetsutövare bedriver säkerhetskänslig verksamhet.

Varje medlemsstat ska utse eller inrätta en eller flera CSIRT-enheter (Computer Security Incident Response Team) och utse eller inrätta en eller flera myndigheter med ansvar för hanteringen av storskaliga cybersäkerhetsincidenter och kriser (cyberkrishanteringsmyndigheter). NIS2-utredningen föreslår att Myndigheten för samhällsskydd och beredskap ska vara Sveriges CSIRT-enhet och ”cyberkrishanteringsmyndighet”.

8.3 CER-direktivet – Critical Entities Resilience Directive

Tillsyn samt myndigheter och andra berörda verksamhetsutövare:

Enligt CER-direktivet ska nationella myndigheter ska utföra marknadsövervakning och tillsyn inom medlemsstatens territorium.

Utifrån relationen till certifiering, främst certifiering i enlighet med en CSA-ordning; de som främst berörs av CER-direktivet är:

- (Se för det första den generella uppräkningen av myndigheter och andra berörda verksamhetsutövare i avsnitt 7.2.)
- Utredningsdirektiven till den s.k. NIS2-utredningen (som också omfattar CER-entiteterna) utgår i princip ifrån att tillsynsmyndigheterna för NIS-sektorerna skall vara desamma för de motsvarande kritiska entiteterna enligt CER-direktivet. Både NIS2-direktivet och CER-direktivet innehåller bestämmelser om förhållandet till sektorsspecifika unionsrättsakter. Exempelvis följer det av CER-direktivet att berörda bestämmelser i det direktivet inte ska vara tillämpliga om det i en sektorsspecifik unionsrättsakt ställs åtminstone likvärdiga krav på att kritiska entiteter ska vidta åtgärder för att stärka sin motståndskraft. En sektorsspecifik unionsrättsakt som pekas ut särskilt i båda direktiven är Dora-förordningen.[30] I CER-direktivet framhålls dock även att behörig myndighet för sektorerna bankverksamhet och finansmarknadsinfrastruktur i princip ska vara den behöriga myndigheten enligt Dora-förordningen.

8.4 Cyberresiliensakten – Cyber Resilience Act (CRA)

Tillsyn samt myndigheter och andra berörda verksamhetsutövare:

Se för det första den generella uppräkningen av myndigheter och andra berörda verksamhetsutövare i avsnitt 7.2.

Dessutom ska nationella myndigheter utföra marknadsövervakning och tillsyn inom medlemsstatens territorium. Cyberresiliensakten är dock nyligen antagen och svensk myndighetsorganisation är inte bestämd ännu.

8.5 AI-förordningen – AI Act

Tillsyn samt myndigheter och andra berörda verksamhetsutövare:

Se för det första den generella uppräkningen av myndigheter och andra berörda verksamhetsutövare i avsnitt 7.2.

Regeringen har tillsatt en kommitté – en AI-kommission[31] – som bl.a. ska:

[30] Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 20 (23) 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 (Dora-förordningen).

[31] Dir. 2023:164

- identifiera behov av och lämna förslag som främjar en konkurrenskraftig, säker och etisk AI-utveckling och AI-användning i Sverige,
- analysera och föreslå hur Sverige proaktivt kan bidra till utformningen av internationella policyer och regelverk inom AI-området, i synnerhet genom EU, i syfte att främja en konkurrenskraftig, säker och etisk AI.

AI-kommissionen har dock inget uppdrag att föreslå myndighetsorganisation med tillhörande tillsynsansvar, föreskriftsrätt, m.m., kring genomförandet av AI-akten.

8.6 eIDAS2-förordningen

Tillsyn samt myndigheter och andra berörda verksamhetsutövare:

Se för det första den generella uppräkningen av myndigheter och andra berörda verksamhetsutövare i avsnitt 7.2.

Resultatet av utredningen om genomförandet av EIDAS2-förordningen är inte publicerat, därmed inte heller fördelningen av ansvar och befogenheter för svenska myndigheter för genomförandet. Bedömningen är dock att Myndigheten för digital förvaltning (DIGG) utses som för e-leg och e-identitetsplånboken och Post- och telestyrelsen för övriga ”betrodda tjänster” som tillsynsmyndigheter, (dvs. ungefär som idag).

8.7 DORA-förordningen – Digital Operational Resilience Act

Tillsyn samt myndigheter och andra berörda verksamhetsutövare:

Enligt DORA-förordningen ska behöriga myndigheter säkerställa efterlevnaden av förordningen i enlighet med de befogenheter som myndigheten tilldelats i de EU-rättsakter som anger behörig myndighet för de finansiella entiteterna. De behöriga myndigheterna ska även ha alla tillsyns-, utrednings- och sanktionsbefogenheter som krävs för att de ska kunna fullgöra sina skyldigheter enligt förordningen.

Se den generella uppräkningen av myndigheter och andra berörda verksamhetsutövare i avsnitt 7.2, och att här är Finansinspektionen tillsynsmyndighet. Enligt utredningsdirektiv till NIS2/CER-utredningen ska där lagstiftningarna överlappar de tillsynsmyndigheter som har ansvar för DORA även ha ansvaret för CER-tillsynen.

8.8 Cybersäkerhetsaktens utvidgning till förvaltade säkerhetstjänster

Tillsyn samt myndigheter och andra berörda verksamhetsutövare:

Se för det första den generella uppräkningen av myndigheter och andra berörda verksamhetsutövare i avsnitt 7.2.

Notera att särskilt avseende Försvarets materielverk och Swedac gäller samma förhållanden som för cybersäkerhetsakten i övrigt. Mest relevanta myndigheter i övrigt torde vara tillsynsmyndigheterna för NIS2- och CER-direktiven.

8.9 Färdskrivarförordningen

Tillsyn samt myndigheter och andra berörda verksamhetsutövare:

Se för det första den generella uppräkningen av myndigheter och andra berörda verksamhetsutövare i avsnitt 7.2.

Notera att Försvarets materielverk/CSEC är certifieringsorgan för färdskrivare. Transportstyrelsen är behörig myndighet och ska i övrigt fullgöra de uppgifter som ankommer på Sverige i fråga om typgodkännande av färdskrivarkort. Swedac är behörig myndighet för ackrediteringar rörande färdskrivare.

8.10 Maskinförordningen

Tillsyn samt myndigheter och andra berörda verksamhetsutövare:

Se för det första den generella uppräkningen av myndigheter och andra berörda verksamhetsutövare i avsnitt 7.2.

Arbetsmiljöverket var marknadskontrollmyndighet för maskindirektivet och kan därmed förväntas bli det även rörande den nya förordningen som ersätter direktivet.

8.11 Radioutrustningsdirektivet

Tillsyn samt myndigheter och andra berörda verksamhetsutövare:

Se för det första den generella uppräkningen av myndigheter och andra berörda verksamhetsutövare i avsnitt 7.2.

I Sverige har RED genomförts genom radioutrustningslagen, radioutrustningsförordningen och Post- och telestyrelsens föreskrifter. Post- och telestyrelsen är marknadskontrollmyndighet och utövar marknadskontroll över att produkter fungerar som kommunikationsutrustning, vilket vi tolkat som en typ av cybersäkerhetskrav.

8.12 Elnätskodex

Tillsyn samt myndigheter och andra berörda verksamhetsutövare:

Se för det första den generella uppräkningen av myndigheter och andra berörda verksamhetsutövare i avsnitt 7.2.

Svensk myndighet är inte explicit utsedd men ansvarig myndighet kan antas bli Energimyndigheten eftersom reglerna utgör ett komplement till NIS2-direktivets regler om cybersäkerhet inom energiförsörjningen.

8.13 Dataförvaltningsförordningen

Tillsyn samt myndigheter och andra berörda verksamhetsutövare:

Varje medlemsstat ska utse behöriga organ för att hjälpa offentliga aktörer som ska dela skyddade data. Hjälpen kan bestå i att ge tekniskt stöd för att tillhandahålla säker behandlingsmiljö, vägledning för lagring och strukturering av data, tekniskt stöd för

pseudonymisering m.m. Dataförvaltningsförordningen är dock nyligen antagen. Svensk myndighetsorganisation är inte bestämd ännu.

8.14 Allmän dataskyddsförordning – GDPR/DSF

Tillsyn samt myndigheter och andra berörda verksamhetsutövare:

Se för det första den generella uppräkningen av myndigheter och andra berörda verksamhetsutövare i avsnitt 7.2. Tillsynsmyndighet på området är Integritetsskyddsmyndigheten (IMY).

8.15 Säkerhetsskyddslagen

Syfte och omfattning (avseende säkerhetsskydd)

Ett av Säkerhetspolisens verksamhetsområden är säkerhetsskydd. Säkerhetsskydd handlar om att skydda den information och de verksamheter som är av betydelse för Sveriges säkerhet mot spionerі, sabotage, terroristbrott och vissa andra hot. Området handlar även om att skydda verksamhet som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd. Om vissa myndigheter och företag i Sverige utsätts för antagonistiska handlingar kan det orsaka allvarliga konsekvenser för Sveriges säkerhet. Det kan till exempel handla om verksamheter inom rättsväsendet, energi- eller vattenförsörjningen, telekommunikationer eller transportsektorn. Dessa verksamheter kan i sitt uppdrag behöva hantera uppgifter som är av betydelse för Sveriges säkerhet. Om dessa uppgifter röjs, förstörs eller ändras kan det inverka på Sveriges säkerhet. Det är därför verksamheter som behöver ett särskilt skydd, säkerhetsskydd.

Säkerhetskänslig verksamhet

Säkerhetskänslig verksamhet är sådan verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd. Uttrycket Sveriges säkerhet tar sikte på sådant som är av grundläggande betydelse för Sverige, som försvaret, det demokratiska statsskicket, rättsväsendet och samhällsviktig verksamhet som är av betydelse ur ett nationellt perspektiv.

Med internationellt åtagande om säkerhetsskydd avses att Sverige förbundit sig att skydda något åt en annan stat eller mellanfolklig organisation, till exempel luftfartsskydd eller uppgifter som utbytts inom militära samarbeten eller samarbeten mot terrorism.

Den som till någon del bedriver säkerhetskänslig verksamhet har grundläggande skyldigheter att utreda behovet av säkerhetsskydd, planera och vidta säkerhetsskyddsåtgärder samt kontrollera det egna säkerhetsskyddet.

Säkerhetsskyddsklassificerade uppgifter

Med säkerhetsskyddsklassificerade uppgifter avses uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen, eller som skulle ha omfattats av den lagen om den varit tillämplig i den aktuella verksamheten.

Det innebär att även enskilda verksamhetsutövare, som i regel inte omfattas av offentlighets- och sekretesslagen, ska skydda sådana uppgifter. Detta följer den inom säkerhetsskydd fundamentala principen att nivån av skydd ska vara detsamma oavsett var, hur eller av vem som verksamheten bedrivs.

Vilka bedriver säkerhetskänslig verksamhet?

Även enskilda verksamhetsutövare (”utövare av säkerhetskänslig verksamhet), som i regel inte omfattas av offentlighets- och sekretesslagen, ska skydda sådana uppgifter. Detta följer av den inom säkerhetsskydd fundamentala principen att nivån av skydd ska vara densamma oavsett var, hur eller av vem som verksamheten bedrivs. Varje verksamhetsutövares har själv ansvaret för att bedöma om den bedriver säkerhetskänslig verksamhet.

Det finns ingen förteckning, tillståndsprövningsprocess eller liknande som tydligt pekar ut vilka som bedriver säkerhetskänslig verksamhet. Det är istället, i likhet med vad som gäller inom många andra lagreglerade områden, varje verksamhetsutövares ansvar att hålla sig informerad, göra bedömningar och bedriva sin verksamhet enligt de författningar som gäller på säkerhetsskyddsområdet. Det är alltså verksamhetsutövaren själv som ansvarar för att bedöma om den bedriver säkerhetskänslig verksamhet enligt 1 kap. 1 § säkerhetsskyddslagen.

Säkerhetskrav för informationssystem för säkerhetskänslig verksamhetSäkerhetsförordningen stipulerar vissa särskilda säkerhetskrav för informationssystem som används i säkerhetskänslig verksamhet. En verksamhetsutövare som ansvarar för ett informationssystem som ska användas i säkerhetskänslig verksamhet ska bl.a. vidta lämpliga skyddsåtgärder för att kunna upptäcka, försvåra och hantera skadlig inverkan på informationssystemet samt obehörig avlyssning av, åtkomst till och användning av informationssystemet, samt också se till att spårbarhet finns för händelser som är av betydelse för säkerheten i systemet.

Tillsyn

Säkerhetspolisen och övriga tillsynsmyndigheter inom säkerhetsskyddsregleringen bedriver tillsyn för att säkerställa att verksamhetsutövarna efterlever säkerhetsskyddslagens krav. Säkerhetspolisen är tillsammans med Försvarsmakten samordningsmyndigheter för tillsyn och samråd. Samordningsmyndigheterna har till uppgift att i samverkan följa upp, utvärdera och utveckla arbetet med tillsyn och samråd. I fråga om samråd så innebär det att ta fram och tillhandhålla metodstöd för tillsyn och samråd, förmedla relevant hotinformation till tillsynsmyndigheterna, samt leda ett samarbetsforum där tillsynsmyndigheterna ingår, i syfte att underlätta samordning och åstadkomma en effektiv och likvärdig tillsyn.

Tillsynsmyndigheter kan besluta om ingripande i form av ett föreläggande, föreläggande med vite och sanktionsavgift. Myndigheterna har enligt säkerhetsskyddslagen vissa undersökningsbefogenheter för att genomföra sitt uppdrag.

Tillsynsmyndigheterna ska ha en aktuell förteckning över sina tillsynsobjekt. I skrivande stund finns inte information om antalet tillsynsobjekt på varje område men

t.ex. har Post- och telestyrelsen 12 tillsynsobjekt. Säkerhetspolisen bedriver tillsyn över åtminstone 120 myndigheter som spänner över vitt skilda områden, från de brottslighetshanterande myndigheterna till de stora samhällsviktiga myndigheterna (undantaget försvarsmyndigheter) som t.ex. Skatteverket, Försäkringskassan, myndigheterna som bedriver tillyn enligt NIS-lagen m.m. Försvarsmakten genom MUST bedriver tillsyn över alla myndigheter under Försvarsdepartementet, t.ex. Fortifikationsverket, Försvarshögskolan, Försvarets materielverk och Myndigheten för samhällsskydd och beredskap. Affärsverket Svenska Kraftnät. Transportstyrelsen och Post- och telestyrelsen bedriver tillsyn över enskilda verksamhetsutövare inom respektive infrastrukturområden. Försvarets materielverk, Finansinspektionen, Statens energimyndighet och Strålsäkerhetsmyndigheten bedriver tillsyn över enskilda verksamhetsutövare inom sina respektive områden. Länsstyrelserna i Stockholms, Skåne, Västra Götalands och Norrbottens län bedriver tillsyn över kommuner och regioner inom respektive län samt statliga myndigheter och enskilda verksamhetsutövare med säte i respektive län, om de inte hör till någon annan tillsynsmyndighets tillsynsområde. I bilaga 4 ges en mer komplett förteckning över tillsynsmyndigheterna och vilka myndigheter och typer av enskilda verksamhetsutövare med säkerhetskänslig verksamhet respektive tillsynsmyndighet bedriver tillsyn över.

Föreskriftsrätt, råd och vägledning

Säkerhetspolisen får meddela föreskrifter om säkerhetsskyddsanalys, anmälnings- och rapporteringsskyldighet, säkerhetsskyddsåtgärder, säkerhetsskyddsklassificering och säkerhetsskyddsavtal samt verkställigheten av säkerhetsskyddslagen. Innan föreskrifter meddelas ska Säkerhetspolisen ge Försvarsmakten tillfälle att yttra sig. Denna föreskriftsrätt gäller inte i de fall som Försvarsmakten, Försvarets materielverk eller Regeringskansliet har föreskriftsrätt enligt säkerhetsskyddsförordningen.

Säkerhetspolisen och Försvarsmakten ska på begäran lämna råd om säkerhetsskydd till Regeringskansliet, riksdagen och dess myndigheter och till Justitiekanslern. Säkerhetspolisen och Försvarsmakten ska informera varandra när råd har lämnats.

Försvarsmakten får meddela föreskrifter om:

1. kryptografiska funktioner som är avsedda för skydd av säkerhetskänslig verksamhet,
2. säkerhetsskyddsanalys, anmälnings- och rapporteringsskyldighet, säkerhetsskyddsåtgärder, säkerhetsskyddsklassificering och säkerhetsskyddsavtal enligt säkerhetsskyddslagen (2018:585) och denna förordning inom sitt och Försvarets materielverks tillsynsområde, och
3. verkställigheten av säkerhetsskyddslagen inom sitt och Försvarets materielverks tillsynsområde med undantag för föreskrifter om förfarandet vid registerkontroll.

Denna föreskriftsrätt gäller inte i de fall som Regeringskansliet eller Försvarets materielverk har föreskriftsrätt enligt förordningen. Innan föreskrifter meddelas ska

Försvarsmakten ge Säkerhetspolisen tillfälle att yttra sig. Detsamma gäller innan föreskrifter meddelas enligt 3 kap. 6 § första stycket, 7 och 10 §§ i förordningen.

Regeringskansliet får meddela föreskrifter om bl.a. säkerhetsskyddsanalys, anmälnings- och rapporteringsskyldighet, säkerhetsskyddsåtgärder, säkerhetsskyddsklassificering och säkerhetsskyddsavtal enligt säkerhetsskyddslagen och säkerhetsskyddsförordningen samt verkställigheten av säkerhetsskyddslagen i övrigt för Regeringskansliet, utlandsmyndigheterna och sådana kommittéer och särskilda utredare som avses i kommittéförordningen.

En tillsynsmyndighet som utövar tillsyn över enskilda verksamhetsutövare får inom sitt tillsynsområde meddela föreskrifter som kompletterar föreskrifter från Säkerhetspolisen, Försvarsmakten och Försvarets materielverk. Innan en tillsynsmyndighet meddelar sådana föreskrifter ska myndigheten samråda med Säkerhetspolisen och Försvarsmakten.

Tillsynsmyndigheterna ska inom sina respektive tillsynsområden ge vägledning om säkerhetsskydd.

8.16 Krisberedskapsförordningen

Förordningen om statliga myndigheters beredskap föreskriver att varje myndighet ansvarar för att egna informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt. I ansvaret ingår att myndigheten särskilt ska beakta behovet av säkra ledningssystem. Myndigheten för samhällsskydd och beredskap får meddela ytterligare föreskrifter om sådana säkerhetskrav för informationshanteringssystem. Myndigheten ska därvid beakta nationell och internationell standard för informationssäkerhet.

Beredskapsmyndigheterna är de 21 länsstyrelserna och följande 39 centrala myndigheter:

- Arbetsförmedlingen
- Bolagsverket
- Domstolsverket
- E-hälsomyndigheten
- Energimarknadsinspektionen
- Finansinspektionen
- Folkhälsomyndigheten
- Försäkringskassan
- Kriminalvården
- Kustbevakningen
- Lantmäteriet
- Livsmedelsverket
- Luftfartsverket
- Läkemedelsverket
- Migrationsverket
- Polismyndigheten
- Post- och telestyrelsen
- Riksgäldskontoret
- Sjöfartsverket
- Skatteverket
- Socialstyrelsen
- Statens energimyndighet
- Statens jordbruksverk
- Statens servicecenter
- Statens skolverk
- Statens veterinärmedicinska anstalt
- Strålsäkerhetsmyndigheten
- Svenska kraftnät
- Sveriges meteorologiska och hydrologiska institut

- Myndigheten för digital förvaltning
- Myndigheten för psykologiskt försvar
- Myndigheten för samhällsskydd och beredskap
- Naturvårdsverket
- Pensionsmyndigheten
- Säkerhetspolisen
- Trafikverket
- Transportstyrelsen
- Tullverket
- Åklagarmyndigheten
-

Myndigheten för samhällsskydd och beredskap har tillsammans med aktörerna i beredskapssystemet identifierat 59 viktiga samhällsfunktioner. Drygt 40 av de viktiga samhällsfunktionerna har sin huvudsakliga hemvist i en beredskapssektor eller hos en beredskapsmyndighet. Beredskapsplanering ska ske för alla viktiga samhällsfunktioner. I utvecklingen av beredskapssystemet kan ytterligare myndigheter och sektorer komma att integreras. MSB har 2023 publicerat Lista med viktiga samhällsfunktioner - Utgångspunkt för att stärka samhällets beredskap. Där beskrivs viktiga samhällsfunktioner med respektive utan huvudsaklig hemvist i en beredskapssektor, inklusive för olika områden en uppdelning mellan sektorsansvarig myndighet och övriga myndigheter inom den sektorn.

Beredskapssektorer och sektorsansvariga myndigheter:

- Hälsa, vård och omsorg: Socialstyrelsen
- Livsmedelsförsörjning och dricksvatten: Livsmedelsverket
- Ordning och säkerhet: Polismyndigheten
- Räddningstjänst och skydd av civilbefolkningen: Myndigheten för samhällsskydd och beredskap
- Transporter: Trafikverket
- Ekonomisk säkerhet: Försäkringskassan
- Elektroniska kommunikationer och post: Post- och telestyrelsen
- Energiförsörjningen: Energimyndigheten
- Finansiella tjänster: Finansinspektionen
- Försörjning av grunddata: Skatteverket

9 Försvarets materielverks uppgifter och ansvar

Försvarets materielverks bedömning:

Försvarets materielverks uppgift, enligt cybersäkerhetsakten och svensk reglering, är bl.a. att, i samarbete med andra berörda sektorsmyndigheter, övervaka och kontrollera efterlevnaden av bestämmelserna i CSA-ordningar och samt att övervaka att certifierade IKT-produkter-, tjänster- respektive processer överensstämmer med kraven i beslutade ordningar.

Ett CSA-certifikat garanterar inte säkerheten, utan utgör ett intyg om att de stipulerade kontrollerna gjorts och att de gjorts på stipulerat sätt. Försvarets materielverk kan hålla certifikatinnehavare ansvariga för att produkten, tjänsten eller processen motsvarar de krav och kontroller som det specifika certifikatet representerar. Försvarets materielverk kan även hålla certifieringsorgan ansvarigt för om de kontroller som åligger dem att göra inte blivit genomförda enligt certifieringsordningens regelverk.

Försvarets materielverk ska inom ramen för sina resurser samarbeta med andra nationella myndigheter för cybersäkerhetscertifiering eller andra myndigheter, bland annat genom att utbyta information om IKT-produkter, -tjänster och -processer som eventuellt avviker från kraven.

Föregående avsnitt visar att utveckling av certifieringsregelverk förutsätter omfattande kompetens rörande it i allmänhet, cybersäkerhet, principer för teknisk kontroll och relevanta standarder. Till det kommer behov av att på olika sätt analysera och förstå nationella behov av cybersäkerhet, dvs. behoven hos de olika sektorsmyndigheter och verksamhetsutövare (offentliga och privata) inom ramen för vars och ens rättsliga ansvar och behov.

9.1 Cybersäkerhetsakten om nationell myndighet för cybersäkerhetscertifiering

I cybersäkerhetsakten anges i artikel 58 att varje medlemsstat ska utse en eller flera nationella myndigheter för cybersäkerhetscertifiering på sitt territorium eller, efter överenskommelse med en annan medlemsstat, utse en eller flera nationella myndigheter för cybersäkerhetscertifiering som är etablerade i den andra medlemsstaten som ansvariga för tillsynsuppgifterna i den utseende medlemsstaten. Sverige har endast utsett en sådan myndighet för vårt eget territorium, den svenska nationella myndigheten för cybersäkerhetscertifiering (eng; ”National Cybersecurity Certification Authority” – NCCA), dvs. Inspektionen för Cybersäkerhetscertifiering (ICC) vid Försvarets materielverk.

Medlemsstaterna ska vidare säkerställa att NCCA:erna har tillräckliga resurser för att kunna utöva sina befogenheter och kunna utföra sina uppgifter på ett effektivt och ändamålsenligt sätt. En NCCA ska bl.a.:

- övervaka och kontrollera efterlevnaden av bestämmelserna i europeiska ordningar för cybersäkerhetscertifiering,

- övervaka att IKT-produkters, IKT-tjänsters och IKT-processers överensstämmelse med kraven i de europeiska cybersäkerhetscertifikat som utfärdats inom deras respektive territorier, i samarbete med andra berörda marknadsövervakningsmyndigheter (numera ”marknadskontrollmyndigheter” [32]),
- kontrollera att tillverkare eller leverantörer av IKT-produkter, IKT-tjänster eller IKT-processer som är etablerade inom deras respektive territorier fullgör sina skyldigheter,
- aktivt bistå och stödja de nationella ackrediteringsorganen med övervakning och kontroll av verksamhet som bedrivs av organen för bedömning av överensstämmelse,
- i tillämpliga fall utfärda bemyndiganden för organ för bedömning av överensstämmelse och begränsa, tillfälligt upphäva eller återkalla befintliga bemyndiganden om organen inte uppfyller kraven i cybersäkerhetsakten,
- behandla klagomål från fysiska eller juridiska personer avseende europeiska cybersäkerhetscertifikat
- lämna en årlig sammanfattande rapport om den verksamhet som bedrivits,
- samarbeta med andra nationella myndigheter för cybersäkerhetscertifiering eller andra myndigheter, bl.a. genom att utbyta information om IKT-produkter, -tjänster och -processer som eventuellt avviker från kraven i cybersäkerhetsakten eller från kraven i särskilda europeiska ordningar för cybersäkerhetscertifiering, och
- övervaka relevant utveckling på området cybersäkerhetscertifiering.

En NCCA ska enligt cybersäkerhetsakten övervaka och kontrollera efterlevnaden av bestämmelserna i europeiska ordningar för cybersäkerhetscertifiering, för övervakning av IKT-produkters, IKT-tjänsters och IKT-processers överensstämmelse med kraven i de europeiska cybersäkerhetscertifikat som utfärdats inom deras respektive territorier. Denna övervakning och kontroll skall ske i samarbete med andra berörda ”marknadskontrollmyndigheter” eller andra nationella myndigheter[33]. En rimlig tolkning är att det senare avser alla nationella myndigheter med befogenheter och ansvar avseende genomförande av EU-lagstiftning innebärande cybersäkerhetskrav, även annan än den rörande marknadskontroll, t.ex. sektorsmyndigheterna inom NIS2, vare sig dessa även utgör marknadskontrollmyndigheter eller inte. Syftet är övervakning och informationsutbyte med sikte på kontroll och tillsyn av efterlevnad av respektive EU-rättsakts cybersäkerhetskrav.

NCCA ges i artikel 58 vissa minimibefogenheter för att kunna fullgöra tillsyn över efterlevnaden av det europeiska ramverket för cybersäkerhetscertifiering. De ska åtminstone ha befogenheter att:

[32] CSA art. 58.7.a. Sedan CSA:s tillkomst har reglerna om marknadsövervakning i Förordning (EG) nr 765/2008 ersatts av regler om marknadskontroll i Förordning (EU) 2019/1020 av den 20 juni 2019 om marknadskontroll […]. Därmed har begreppet övervakningsmyndigheter ersatts av marknadskontrollmyndigheter.

[33] CSA art. recit 102 och 58.7.h CSA

a) begära att organ för bedömning av överensstämmelse, innehavare av ett europeiskt cybersäkerhetscertifikat och utfärdare en EU-försäkran om överensstämmelse ska lägga fram alla uppgifter som myndigheten behöver för att kunna fullgöra sin uppgift,
b) genomföra undersökningar, i form av kontroller, av organ för bedömning av överensstämmelse, innehavare av ett europeiskt cybersäkerhetscertifikat och utfärdare av en EU-försäkran om överensstämmelse med certifieringsreglerna,
c) vidta lämpliga åtgärder, i enlighet med nationell rätt, för att säkerställa att organ för bedömning av överensstämmelse, innehavare av europeiska cybersäkerhetscertifikat och utfärdare av en EU-försäkran om överensstämmelse uppfyller kraven i cybersäkerhetsakten eller CSA-ordning,
d) få tillgång till alla lokaler hos organ för bedömning av överensstämmelse eller innehavare av ett europeiskt cybersäkerhetscertifikat i syfte att genomföra utredningar i enlighet med unionsrätten eller medlemsstaternas processrätt,
e) i enlighet med nationell rätt, återkalla europeiska cybersäkerhetscertifikat som utfärdats av NCCA:n eller europeiska cybersäkerhetscertifikat som utfärdats av bemyndigat organ för bedömning av överensstämmelse, om sådana certifikat inte uppfyller kraven i cybersäkerhetsakten eller en CSA-ordning,
f) utdöma sanktioner i enlighet med nationell rätt och kräva att överträdelser av skyldigheterna i denna förordning omedelbart upphör.

NCCA ska samverka med EU-kommissionen, Enisa och andra medlemsstater inom ramen för den europeiska gruppen för cybersäkerhetscertifiering (ECCG).

9.2 Svensk lagstiftning om myndighet för genomförande av cybersäkerhetsakten

Enligt förordning (2021:555) med kompletterande bestämmelser till EU:s cybersäkerhetsakt är Försvarets materielverk dels svensk NCCA, dvs. nationell myndighet för cybersäkerhetscertifiering enligt lagen (2021:553) med kompletterande bestämmelser till EU:s cybersäkerhetsakt, dels nationell representant i den europeiska gruppen för cybersäkerhetscertifiering (ECCG). Vid Försvarets materielverk finns också ett ackrediterat organ för bedömning av överensstämmelse.

Försvarets materielverks tillsynsbefogenheter i form av NCCA följer av lag (2021:553) med kompletterande bestämmelser till EU:s cybersäkerhetsakt (jfr avsnitt 9.1) och innefattar följande:

- Vid tillsyn över att denna lag och föreskrifter som har meddelats i anslutning till lagen följs har NCCA:n de befogenheter som anges i artikel 58.8 i cybersäkerhetsakten.
- NCCA:n får besluta de förelägganden som behövs för tillsynen och för att cybersäkerhetsakten, genomförandeakter som har meddelats med stöd av cybersäkerhetsakten, denna lag och föreskrifter som har meddelats i anslutning till lagen ska följas. Ett beslut om föreläggande får förenas med vite och sanktionsavgifter för parter som inte uppfyller kraven i en certifieringsordning. Sanktionsavgiften kan högst vara 15Msek.

- NCCA:n får begära handräckning av Kronofogdemyndigheten för att få tillträde till andra lokaler än bostäder, och där genomföra utredningar i enlighet med artikel 58.8 d i cybersäkerhetsakten.
- Vid handräckning tillämpas bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet, avhysning eller avlägsnande. Om NCCA:n begär det, ska Kronofogdemyndigheten inte i förväg underrätta den som utredningen ska genomföras hos.
- NCCA:n får besluta att återkalla ett europeiskt cybersäkerhetscertifikat som har utfärdats av myndigheten eller av ett organ för bedömning av överensstämmelse i enlighet med cybersäkerhetsakten, om certifikatet inte uppfyller kraven i cybersäkerhetsakten eller en CSA-ordning.

10 Näringslivets behov och medverkan

Försvarets materielverks bedömning:

Näringslivet behöver ges möjlighet att påverka utformningen av säkerhetskraven samt regler för kontroll och certifiering vid utveckling av certifieringsordningar. Detta är centralt för att svenska företag inte ska drabbas av olika typer av utlåsningseffekter och för att främja företagens möjlighet att uppfylla kraven och därmed lättare få tillgång till den inre marknaden.

Överlappande, multipla krav från olika sektorsmyndigheter och upphandlande myndigheter orsakade av olika EU- eller nationella regleringar som avser samma typ av produkt eller tjänst ökar näringslivets kostnader väsentligt och minskar dess konkurrenskraft. Det är samtidigt svårt för en enskild sektorsmyndighet eller upphandlande myndighet att själv identifiera behovet av samordning eller att leda arbetet med att öka samordning och minska fragmenteringen av reglering, vägledningar och standarder.

Digitaliseringens försörjningskedjor är till hög grad globala avseende både hård- och mjukvara. EU-specifika standarder refererade i certifieringsordningar riskerar att öka företagens kostnader och minskar deras konkurrenskraft och leveransförmåga på den globala marknaden.

Det är av vikt att certifieringsordningarna och relaterade standarder utformas så att företagen på egen hand tidigt kan genomföra de kontroller och tester som senare ska genomföras i samband med en certifiering. Om så inte är fallet kommer det vara mycket svårt för företagen att etablera effektiv och konkurrenskraftig produktion med korta leveranstider som motsvarar kraven redan när certifieringsprocessen inleds.

I de fall standarder refererade i certifieringsordningar utvecklats av organisationer som är öppna eller är föremål för EU-kommissionens öppna samråd, kan näringslivet verka på egen hand för att tillvarata sina intressen. Eftersom viktiga steg vid utveckling av en certifieringsordning och relaterad standard inte alltid är öppna och tillgängliga för näringslivet, kan det vara motiverat att svenska myndigheter dels verkar för ökad öppenhet, dels får i uppdrag att så långt det är möjligt bevaka näringslivets behov.

10.1 Behovet av öppen standard

Näringslivet behöver tillträde och möjlighet att påverka utformningen av de funktionella kraven, säkerhetskraven och reglerna för kontroll och certifiering. Detta är centralt för att svenska företag inte ska drabbas av olika typer av utlåsningseffekter och för att främja företagens möjlighet att uppfylla kraven och därmed få tillgång till den inre marknaden, företrädelsevis oavsett storlek på företag.

Som beskrivits i avsnitt 3 ”Standardisering” bör standarder och regler för kontroll och certifiering utvecklas av öppna standardiseringsorgan i enlighet med WTO-TBT:s principer, eller annars av defactostandardiseringsorgan där svenska för företag har tillträde och möjlighet att påverka.

Vilka standarder och tekniska specifikationer som refereras i en certifieringsordning bestäms huvudsakligen inom ramen för Enisas arbete att på EU-kommissionens uppdrag utarbeta ett förslag till certifieringsordning. Därmed har Försvarets materielverk här en viktig uppgift att verka för att EU:s certifieringsordningar (och

annan EU-reglering) baseras på krav utvecklade av sådana organisationer. I samband med att EU-kommissionen överväger att göra certifiering obligatoriskt via annan EU-rätt, så blir det även väsentligt för berörda sektorsmyndigheter att bevaka och agera på detta behov.

10.2 Undvik fragmentering av krav och standarder

Överlappande, multipla krav från olika sektorsmyndigheter, upphandlande myndigheter eller via olika EU- eller nationella regleringar som avser samma typ av produkt eller tjänst kan öka näringslivets kostnader väsentligt och minskar dess konkurrenskraft. Denna typ av kravfragmentering kan allvarligt försvåra för små- och medelstora företag och motverka innovation.

Det är därmed motiverat att upphandlande myndigheter, nationella regleringar och EU-regleringar som avser samma produkt eller tjänst samordnar sina rättsliga eller andra krav till att när så är möjligt omfattas av samma standarder och certifieringsordningar. Detta gäller även andra krav, t.ex. som rör NIS2, säkerhetskänslig verksamhet, Nato, etc.

Samtidigt är det svårt för en enskild sektorsmyndighet eller upphandlande verksamhetsutövare att själv identifiera behovet av samordning eller att leda initiativ för att öka sådan samordning.

Av samma anledning är det angeläget att global standard främjas för de företag som verkar på en internationell marknad. EU-specifika krav (standarder) ökar företagens kostnader och minskar deras konkurrenskraft och leveransförmåga på den internationella marknaden. I begränsad omfattning inom säkerhetsområdet kan dock EU-specifika standarder vara motiverade. Principiellt bör EU-specifik standard undvikas utom där det av säkerhetsmässiga eller andra skäl är väl motiverat med en regional standard.

10.3 Förutsägbara och repeterbara kriterier för krav

För att näringslivet ska kunna vara effektivt behöver de själva kunna avgöra kravuppfyllnad, dvs. själva kunna förstå om de motsvarar certifieringskrav på en specifik produkt eller tjänst. Därmed är det av vikt att certifieringsordningarna och relaterad standard utformas så att företagen på egen hand ”i förväg” kan genomföra de kontroller och tester som senare ska genomföras i samband med en certifiering.

Detta är nödvändigt för att näringslivet ska själv veta om de motsvarar kraven, innan produkten/tjänsten prövas i en certifiering. Om så inte är fallet kommer det vara mycket svårt för företagen att etablera effektiv och konkurrenskraftig produktion med korta leveranstider som motsvarar kraven när certifieringsprocessen inleds.

Detta ställer i sin tur krav på kvalitet och tydlighet på både funktionella standarder och standarder som ligger till grund för kontroll/certifiering. Krav ska utformas så att leverantörer på egen hand med god förutsägbarhet ska kunna avgöra om en produkt/tjänst motsvarar ställda krav. Detta behov av förutsägbarhet efterfrågas även inom det säkerhetskänsliga området som omfattas av säkerhetsskyddslagen.

10.4 Krav utformade så att de inte utgör en onödig barriär för små och medelstora företag.

Olika mer eller mindre omfattande regleringar kan leda till höga kostnader för näringslivet. Detta gäller i hög grad även för cybersäkerhetsaktens olika certifieringsordningar. Stora företag har lättare att bära kostnaden för att analysera vad de juridiska och tekniska kraven innebär och för att genomföra de faktiska certifieringarna. Sådana kostnader kan utgöra hinder för små- och medelstora företag. Vidare kan även frivilliga certifieringssystem få en i praktiken reglerande effekt, då större företag som söker denna typ av kvalitetsmärke för kraven vidare till sina, oftast mycket mindre underleverantörer. Därmed är det angeläget att kraven som är utformade för frivillig certifiering är tydliga och innebär en balans mellan säkerhetsegenskaperna och kostnaderna för kontrollerna.

Det är väsentligt för näringslivet att certifieringsordningar och därtill relaterade standarder utformas så att de inte utgör en onödig barriär för små och medelstora företag. I de fall standarder refererade i certifieringsordningar utvecklats av organisationer som är öppna, så kan näringslivet därmed själv ansvara för sitt deltagande och verka för att kraven är rimliga och i balans med kostnaderna.

Eftersom alla stegen vid utveckling av en certifieringsordning och refererade standarder och tekniska specifikationer inte inom ramen för t.ex. öppen standardisering ger tillträde för t.ex. näringslivet (se avsnitt 6, ”Utveckling av certifieringsordningar och möjligheter till påverkan”) blir det därmed motiverat att svenska myndigheter dels verkar för ökad öppenhet, dels för fram svenska behov i de fall arbetet inte sker i former som är öppna för näringsliv eller akademin.

Försvarets materielverk som är svensk representant i EU-kommissionens och Enisas arbetsgrupper kan av denna anledning behöva stöd i arbetet att förstå näringslivets behov och intressen, för att sedan proaktivt verka för att ta tillvara svenska intressen inom de arbetsgrupper som etablerats av EU-kommissionen och Enisa. I de fall annan EU-rätt refererar till cybersäkerhetscertifiering, kan även berörda sektorsmyndigheter ha möjlighet att påverka utvecklingen.

10.5 Konsekvent och objektiv tillämpning av certifieringsordningar inom EU

Ett EU-certifikat har samma juridiska värde oavsett i vilken medlemsstat certifikatet är utfärdat. Om kvaliteten varierar stort avseende de certifieringar som genomförs i olika medlemsstater, så missgynnar det vissa företag på bekostnad av andra. Det kan snabbt leda till att det land som tillhandahåller ”billigast” certifikat tvingar alla leverantörer att söka sådana certifikat. Detta skulle vara till direkt men för cybersäkerheten på europisk nivå. Det är därmed ett stort behov för näringslivet att kvaliteten på de certifieringar som genomförs är jämn mellan alla medlemsstater inom EU. Hellre en jämn nivå som omfattar färre, men väl reglerade kontroller, än funktionsrika granskningar baserade på långtgående subjektiva bedömningar och som öppnar för inkonsekvent tillämpning inom EU.

EU:s certifieringsordningar bör prioritera utveckling av standarder och regler som leder till lika bedömning mellan medlemsstaterna. För att säkerställa att cybersäkerhetsaktens certifieringsordningar utvecklas på detta sätt, bör Försvarets materielverk och berörda sektorsmyndigheter verka för att utvärdera om de certifieringar som genomförs kan betraktas som likvärdiga, samt att de krav som inarbetas i certifieringsordningarna är utformade så att de förväntas främja en jämn bedömning.

10.6 Eftersträva ömsesidigt erkännande av cybersäkerhetscertifieringar med andra marknader

Digitaliseringens försörjningskedjor är globala. De företag som levererar produkter, system och tjänster verkar ofta på en global marknad. De måste efterleva flera olika regleringar och krav på certifieringar. Om ett certifikat inte erkänns mellan olika marknader innebär detta att företagen behöver genomföra certifiering av dessa produkter och tjänster flera gånger, även i de fall då de underliggande standarderna är desamma. För företagen kan en sådan brist på tillit mellan olika marknader vara mycket kostnadsdrivande.

För att undvika kostsamma multipla granskningar av samma egenskaper hos produkter och tjänster är det av vikt att EU:s certifieringar harmoniseras med regleringar och certifieringsordningar som är etablerade i andra marknader.

11 Utgångspunkter, analys och förslag

Försvarets materielverks bedömning:

Det är en rad faktorer som påverkar hur nationella behov i fråga om cybersäkerhet kan identifieras och omsättas till säkerhetskrav som Sverige bör framhålla i arbetet med att utveckla certifieringsordningar inom EU:s cybersäkerhetsakt.

Det finns ett drygt tiotal EU-regleringar som refererar till cybercertifiering som ett sätt att visa uppfyllnad av krav på cybersäkerhetsegenskaper.

Genom både sådan EU-rätt och tillkommande nationell rätt, inklusive säkerhetsskyddslagstiftningen, styrs ansvar för cybersäkerhet genom ett stort antal sektorsmyndigheter och ett ännu mycket större antal verksamhetsutövare (offentliga såväl som privata).

Verksamhetsutövare ansvarar för att bedöma egna risker och vilka säkerhetsåtgärder som ska införas. Verksamhetsutövare behöver även tillämpa en genomtänkt, sammansatt strategi för vilka kontroller som ska genomföras av t.ex. ledningsystem för informationssäkerhet, nätverks- och informationssystem, systemarkitektur och med ingående komponenter, driftövervakning och anlitade tjänster.

Det är en stor utmaning för både den stora gruppen sektorsmyndigheter och det ännu större antalet verksamhetsutövare att var och en etablera och upprätthålla nödvändig kompetens inom informations- och kommunikationsteknik (IKT), cybersäkerhet, risker för sårbarheter och attacker, effektiva säkerhetsåtgärder, effektiva kontrollmetoder och certifiering, samt förmåga att påverka relevanta standarder och certifieringsordningar.

Försvarets materielverks förslag:

En samlad nationell kompetens- och stödfunktion bör etableras inom staten. Denna ska ha en stark nationell förmåga för analys, samordning, proaktiv och tidig påverkan på utvecklingen av standarder och certifieringsordningar, samt ska kunna stödja sektorsmyndigheter och verksamhetsutövare inom cybersäkerhetsområdet.

Försvarets materielverk föreslår ingen förändring av sektorsmyndigheters och verksamhetsutövares ansvar enligt EU-rätt eller nationell rätt. Den föreslagna funktionen ska utgöra ett stöd till sektorsmyndigheter och verksamhetsutövare, som självständigt fortsatt bär ansvar för sina respektive uppdrag och verksamheter. Det är sektorsmyndigheters och verksamhetsutövares rättsliga ansvar och de behov som följer av detta som ska inrikta stödfunktionens verksamhet.

Stödfunktionen ska i samråd med sektorsmyndigheter utarbeta rekommenderade lösningar för säkerhetsbehov som finns inom en eller flera sektorer, samt i övrigt utgöra ett expertstöd till sektorsmyndigheter och verksamhetsutövare angående effektiva, genomförbara och kostnadseffektiva lösningar som kan adressera respektive sektors behov, avseende bl.a. produkter, arkitektur, drift, tjänster, underhåll, övervakning och kontrollmetoder (inkl. certifiering) samt därtill relaterade standarder. Stödfunktionen ska samverka med sektorsmyndigheterna och tillsammans med dessa bevaka eller proaktivt delta i eller påverka utvecklingen i relevanta standardiseringsorgan och certifieringsordningar.

Inom specifika teknik- eller sakområden, t.ex. kryptering, frågor som rör reglerad avlyssning (eng: ”legal intercept”) eller områden där en enskild sektorsmyndighet är tongivande kan enskilda myndigheter få i uppdrag att samverka med stödfunktionen samt representera svenska intressen i relevanta organisationer, t.ex. standardiseringsorgan.

I det fall det beslutas att en s.k. Nationell modell för cybersäkerhet med tillhörande cybersäkerhetsnorm etableras, bör den kunna utgöra ett betydande stöd till både sektorsmyndigheter och verksamhetsutövare och tillhandahålla information om certifierade produkter, tjänster och processer och deras säkerhetsnivåer.

Försvarets materielverk förordar att stödfunktionen organiseras inom en redan existerande myndighet, eller inom en ny myndighet för cybersäkerhet, om en sådan etableras i enlighet med Försvarsberedningens förslag. De närmare formerna för stödfunktionens ansvar och uppgifter i relation till sektorsmyndigheterna bör närmare utredas.

Stödfunktionen föreslås vara anslagsfinansierad för sin huvuduppgift. Verksamheten föreslås utöver det kunna finansieras med avgifter för eventuellt tillhandahållet stöd till sektorsmyndigheter och verksamhetsutövare.

11.1 Sammanfattning av uppdraget och dess bakgrund

För uppdraget ska anges att informations- och cybersäkerheten generellt i samhället såväl som säkerhetskänslig verksamhet ofta är beroende av säkerhetsegenskaper hos kommersiella produkter och tjänster som skulle kunna verifieras inom det europeiska ramverket för cybersäkerhetscertifiering. Av denna anledning bör risk-, hot- och sårbarhetsanalyser för såväl samhället i allmänhet som för de säkerhetskänsliga verksamheterna ingå i det analysarbete som sedan kan omsättas till säkerhetskrav som Sverige bör framhålla i arbetet med att utarbeta certifieringsordningar.

Uppdraget syftar till att utveckla proaktiva arbetssätt i förhållande till nationella intressen och förhandlingspositioner inom det alltmer betydelsefulla området cybersäkerhet.

Regeringen bedömmer att det är viktigt att myndigheter med ansvar för både hot-, sårbarhets- och riskanalyser för samhället i allmänhet såväl som myndigheter med ansvar för säkerhetskänslig verksamhet bidrar till cybersäkerhetsarbetet.

Mot bakgrund av att näringslivet både använder och producerar certifierade produkter är det viktigt ett en dialog förs med dem under uppdragets genomförande.

Försvarets materielverk ska inom ramen för uppdraget analysera och lämna förslag på hur nationella behov i fråga om cybersäkerhet kan identifieras och omsättas till säkerhetskrav som Sverige bör framhålla i arbetet med att utveckla certifieringsordningar inom EU:s cybersäkerhetsakt.

Behovet av att även kunna certifiera produkter, tjänster och processer i partnerländer utanför EU, särskilt USA, ska beaktas. I uppdraget ingår att lämna förslag på vilka myndigheter som bör ges till uppgift att bidra till arbetet med behovsanalysen samt hur näringslivet kan beredas möjlighet att delta i arbetet.

Försvarets materielverk ska även som del av uppdraget analysera och lämna förslag på hur information om certifierade produkter, tjänster och processer och deras

säkerhetsnivåer kan tillgängliggöras för myndigheter och andra verksamhetsutövare (offentliga såväl som privata).

11.2 Utgångspunkter

Uppdraget att analysera och lämna förslag på hur nationella behov i fråga om cybersäkerhet kan identifieras och omsättas till säkerhetskrav som Sverige bör framhålla i arbetet med att utveckla certifieringsordningar inom EU:s cybersäkerhetsakt (CSA) är komplicerat. Det är en rad faktorer som påverkar hur en sådan lösning kan utformas. I detta avsnitt redovisas ett antal av de utgångspunkter som beaktats.

Nätverks- och informationssystem som används allmänt i samhället, även inom säkerhetskänslig verksamhet, baseras generellt på kommersiella produkter och tjänster som är konstruerade utifrån komplex informations- och kommunikationsteknik. De olika teknikområdena ger förutsättningar för såväl systemens funktionella egenskaper som deras säkerhetsegenskaper. Exempel på sådana förutsättningar/teknikområden redovisas i avsnitt 2 ”Informations- och kommunikationsteknik”. Att på ett adekvat sätt kunna göra risk-, hot- och sårbarhetsanalyser för nätverks- och informationsystem förutsätter därför en djup kompetens inom samtliga dessa teknikområden, hur de samverkar och hur de påverkar de cybersäkerhetsrisker som detta medför.

De krav som etableras i den informations- och kommunikationsteknik som allmänt utgör grunden för nätverks- och informationssystem och även cybersäkerhetsaktens certifieringsordningar baseras till övervägande del på referenser till krav som anges in olika standarder och andra tekniska specifikationer utvecklade av formaliserade standardiseringsorgan eller andra de facto-standardiseringsorgan.

En närmare beskrivning av dessa organisationer och de standarder som utvecklas redovisas i avsnitt 3 ”Standardisering” samt i ”

Bilaga 5 – Exempel på standardiseringsorgan och de facto-standardiseringsorgan inom cyberområdet".

Arbete med standardisering omfattar förmågan att se brister i befintliga standarder och kompetensen att veta hur standarderna kan förbättras. Med den snabba teknikutvecklingen samt ständigt nya typer av sårbarheter och attackvägar, kan det snabbt uppstå behov av nya standarder. I många fall är standarder utvecklade för att adressera (oftast) omfattande funktionella krav. Att verifiera att implementation av sådana omfattande krav t.ex. via certifiering är säker kan många gånger visa sig vara mycket svårt eller rent av praktiskt omöjligt. Utmaningarna med att kunna verifiera korrekt funktion och frånvaro av sårbarheter kan därför behöva mer eller mindre direkt styra och begränsa förutsättningarna för hur systemens funktioner utformas och de därtill tillhörande standarderna. Förmågan att göra sådan analys kräver en mångfacetterad kombination av kompetens och förmåga att identifiera strategier som kan möta sektorsmyndigheters och verksamhetsutövares behov av cybersäkerhet och sedan föra fram konkreta förslag inom standardiseringarbetet på internationell nivå.

Att omsätta nationella behov till säkerhetskrav inom EU-arbetet handlar om svensk påverkan på de standarder som refereras till i certifieringsordningarna och därmed ett behov av svensk medverkan i de organisationer som utvecklar dessa standarder. För de allra flesta tillämpningar är det ett stort antal sådana organisationer inom vilka bevakning och påverkan är och kan bli än mer nödvändig. Detta för att Sverige ska kunna adressera sina behov både ur säkerhetssynpunkt och konkrrensförmåga .

Framgångsrikt arbete med cybersäkerhet förutsätter att det finns en god kännedom om tillämpningen för det specifika nätverks- och informationsystemet, verksamhetens mål och hur cybersäkerhetsrisker kan samverka med verksamhetens övriga hot och risker. Det förutsätter även en god kännedom om den egna verksamheten och it-mognaden hos verksamhetens användare av IT-systemen. En närmare beskrivning av cybersäkerhetsområdet återfinns i avsnitt 4 "Cybersäkerhet". Där framgår att det krävs mycket god kompetens om de tekniska systemens funktioner och egenskaper för att kunna bedöma vilka risker som kan föreligga och för att kunna avgöra vilken kombination av ekonomiskt och verksamhetsmässigt effektiva åtgärder som bör vidtas.

Effektivt arbete med cybersäkerhet förutsätter även kunskap om vilka kontroll- och verifieringsmetoder som är lämpliga, samt förståelse för när och hur certifiering enligt cybersäkerhetsakten är en lämplig metod samt att kompletterande krav och kontroller utöver de certifierade behöver genomföras av den egna organisationen eller dess leverantörer. Sådana aspekter redovisas i avsnitt 5 "Cybersäkerhetscertifiering".

Ett cybersäkerhetscertifikat som utfärdas av en behörig organisation utgör ett intyg om att kontroller av krav eller egenskaper på en produkt, tjänst eller process har prövats i enlighet med en överenskommen metod, av en organisation som bedömts vara kompetent att genomföra dessa kontroller. Vare sig certifikatinnehavaren (leverantören) eller certifieringsorganet kan hållas ansvarigt för att en certifierad produkt eller tjänst är lämplig för ett givet ändamål i ett nätverks- eller

informationssystem. Om en produkt eller tjänst är lämplig i en given situation kan i huvudsak enbart verksamhetsutövaren ansvara för.

Avsnitt 6 ”EU:s cybersäkerhetsakt och dess certifieringsordningar” beskriver närmare det europeiska ramverket för cybersäkerhetscertifiering. Där redovisas även de tre certifieringsordningarna som är under utveckling samt tillhörande standarder i bilagorna 5, 6 och 7. I avsnittet beskrivs även processen för utveckling av en certifieringsordning och som på olika sätt kan medge möjlighet för insyn och påverkan av svenska intressenter.

Det finns ett drygt tiotal EU-regleringar (etablerade eller under utveckling) som refererar till cybersäkerhetscertifiering som ett sätt att visa uppfyllnad av respektive reglerings krav på cybersäkerhetsegenskaper. En CSA-certifiering kan således på nationell få påverkan inom alla sektorer som omfattas av eller på annat sätt är beroende av dessa EU-regleringar. Avsnitt 7 ”EU-reglering med referenser till cybersäkerhetscertifiering” beskriver närmare exempel på sådana EU-regleringar och dessas kopplingar till cybersäkerhetscertifiering. Det kan även noteras att cybersäkerhetsakten ger enskilda medlemsstater möjlighet att reglera krav genom att göra certifiering enligt akten obligatorisk på nationell nivå, vilket kan få väsentlig påverkan på förutsättningarna för marknadstillträde inom vissa sektorer i enskilda medlemsstater, även om ingen tvingande reglering antagits på EU-nivå.

Såväl EU-rätt, nationellt genomförande av EU-rätt samt annan nationell rätt påverkar direkt många olika typer av verksamhetsutövare (offentliga såväl som privata). Detta inklusive s.k. sektorsmyndigheter som genom tillsyn, marknadskontroll, föreskrifter och samordning på olika sätt påverkar förutsättningarna för sådana verksamhetsutövare. Avsnitt 8 ”Nationell reglering med relevans för uppdraget” ger exempel på sådan nationell reglering.

Säkerhetspolisen och Försvarsmakten är myndigheter med ansvar för föreskrifter, tillsyn och samordning inom säkerhetsskydd.

Beredskapsmyndigheterna ansvarar, enligt förordning (2022:524) om statliga myndigheters beredskap, för att egna informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt.

Eftersom CSA-certifieringar kan vara relevanta inom alla dessa sektorer , inklusive försvarssektorn, dels som ett medel för det egna säkerhetsarbetet, dels som ett medel för verksamhetsutövare att visa att man uppfyller stipulerade (ofta omfattande) cybersäkerhetskrav, och därtill att certifieringar i närtid kan bli tvingande, är det flera sektorsmyndigheter och verksamhetsutövare som bör ha kompetens att både bedöma om och när certifiering är lämpligt, vad relevanta certifieringar representerar samt bevaka och påverka certifieringsordningarnas innehåll.

Avsnitt 9 ”Försvarets materielverk:s uppgifter och ansvar” förklarar Försvarets materielverkets uppgift, enligt cybersäkerhetsakten och svensk reglering. Det innebär bl.a. att övervaka och kontrollera efterlevnaden av bestämmelserna i certifieringsordningarna och därmed övervaka att certifierade IKT-produkter-, tjänster- respektive processer överensstämmer med kraven i de beslutade

certifieringsordningar. Detta ska göras i samarbete med berörda sektorsmyndigheter. Det anges även att ett CSA-certifikat inte garanterar cybersäkerheten, utan utgör ett intyg om att de stipulerade kontrollerna av kraven genomförts, att de gjorts på stipulerat sätt och av utsett organ. Försvarets materielverk kan hålla certifikatinnehavare ansvariga för att produkten, tjänsten eller processen motsvarar de krav och kontroller som det specifika certifikatet representerar. Försvarets materielverk kan även hålla certifieringsorgan ansvarigt för om de kontroller som åligger dem att göra inte blivit genomförda enligt certifieringsordningens regelverk.

Enskilda verksamhetsutövare inom näringslivet ska efterleva lagar och regler etablerade inom EU-rätten såväl som nationellt och som är tillämpbara för den egna verksamheten.

Näringslivet har även en mycket central roll som leverantör och tillhandahållare av produkter och tjänster. Avsnitt 10 ”Näringslivets behov och medverkan” ger en överblick över de behov och förutsättningar som kan anses vara centrala för näringslivet i sin roll som tillhandahållare av produkter och tjänster som kan bli föremål för cybersäkerhetscertifiering.

Dessa olika avsnitt visar att ändamålsenlig utveckling av certifieringsregelverk förutsätter omfattande kompetens, med nödvändig bredd och djup rörande IKT i allmänhet, cybersäkerhet, principer för teknisk kontroll och relevanta standarder. Till det kommer behov av att på olika sätt analysera och förstå nationella behov av cybersäkerhet, dvs. behoven hos de olika offentliga och privata verksamhetsutövare som beskrivs i föregående avsnitt som skulle kunna vara eller är användare av certifikaten.

Varje organisation har unika säkerhetsbehov baserade på hur produkten eller tjänsten används i det enskilda fallet, organisationens riskprofil, affärsmodell, regleringskrav och andra faktorer. En produkt eller tjänst som är certifierad kan vara lämplig i en kontext men olämplig i en annan, beroende på de specifika säkerhetsriskerna och kraven i den miljön. Att förstå de underliggande kontrollerna som genomförs vid en certifiering och deras relevans för den egna organisationens säkerhetsbehov är avgörande för att effektivt använda cybersäkerhetscertifikat som en del av ett riskbaserat cybersäkerhetsarbete.

Användare av certifikaten måste förstå vilka säkerhetskontroller och standarder certifieringen baseras på och hur dessa relaterar till de egna säkerhetskraven, kunna utvärdera hur väl certifieringens omfattning och de testade säkerhetsaspekterna överensstämmer med de egna riskerna och säkerhetsbehoven. De måste också använda certifieringen som en del av en större säkerhetsstrategi och vid behov implementera ytterligare säkerhetsåtgärder och kontroller för att adressera områden och egna risker som inte täcks av certifieringen.

11.3 Försvarets materielverks analys och bedömning

Genom både EU-rätt och nationell rätt, inklusive säkerhetsskyddslagstiftningen, regleras olika former av uppgifter, ansvar och befogenheter för cybersäkerhet hos ett

stort antal sektorsmyndigheter och ett ännu mycket större antal verksamhetsutövare (offentliga såväl som privata).[34]

Enskilda verksamhetsutövare behöver därmed ansvara för att bedöma egna risker och därmed vilka säkerhetsåtgärder som behöver vidtas. Verksamhetsutövare behöver tillämpa en genomtänkt och sammansatt strategi för vilka cybersäkerhetsrelaterade kontroller som ska genomföras av systemarkitektur med ingående komponenter, använda tjänster och personalens kompetens. Certifiering av produkter, tjänster eller processer enligt någon av cybersäkerhetsaktens (CSA) ordningar kan vara verktyg i den processen men certifiering fråntar inte verksamhetsutövaren ansvaret för att känna till det egna systemets alla olika delar eller vilka kontroller som bör genomföras. Det åligger verksamhetsutövaren att förstå de underliggande kontrollerna som genomförs vid en certifiering och deras relevans för den egna organisationens säkerhetsbehov.

Ett CSA-certifikat garanterar inte säkerheten, utan utgör ett intyg om att de stipulerade kontrollerna gjorts och att de gjorts på stipulerat sätt av därtill utsett organ, och kan på så sätt underlätta verksamhetsutövarens riskbedömning.

Försvarets materielverks uppgift, enligt cybersäkerhetsakten och svensk reglering är bl.a. att övervaka och kontrollera efterlevnaden av bestämmelserna i certifieringsordningarna och därmed övervaka att certifierade IKT-produkter-, tjänster- respektive processer överensstämmer med kraven i certifieringsordningarn krav. Detta ska göras i samarbete med andra berörda marknadsövervakningsmyndigheter.

Det är en stor utmaning för både den stora gruppen sektorsmyndigheter och det ännu större antalet verksamhetsutövare att var och en etablera och upprätthålla all den kompetens inom it, cybersäkerhet, attackvägar och effektiva säkerhetsåtgärder, standarder och de olika kontrollmetoder som man direkt eller indirekt är beroende av eller själv behöver tillämpa, för vilka en certifiering kan utgöra en komponent att bedöma utifrån sitt ansvar.

Rådande kompetensbrist förstärker utmaningarna för enskilda sektorsmyndigheter och verksamhetsutövare att själva etablera erfoderlig kompetens för både det egna cybersäkerhetsarbetet och för förmågan att aktivt medverka vid utveckling av standarder och/eller certifieringsordningar. Det är en mycket omfattande uppgift för enskilda myndigheter och andra verksamhetsutövare att ha tillräcklig kompetens och resurser för att bevaka och aktivt medverka i alla de olika standardiseringsorgan (inklusive de facto-standardiseringsorgan) och/eller certifieringsordningar som är av relevans för den egna verksamheten.

För svenskt vidkommande så finns det uppenbara risker för divergens i påverkan samt förmåga att påverka genom att kompetens och expertis inom cybersäkerhet inte är tydligt samordnat och organiserat.

P.g.a. cybersäkerhetsområdets komplexitet, utmaningen med tillgång till tillräcklig kompetens hos enskilda myndigheter och verksamhetsutövare, samt värdet av

[34] Begreppen tillsy

samordning mellan olika sektorer i samhället, finns ett behov av ökat centralt stöd avseende kunskap om IKT-teknik, cybersäkerhet, existerande standarders för- och nackdelar ur säkerhetshänseende, hur dessa interagerar säkerhets- och kostnadsmässigt, kunskap om olika attacktekniker och angripare, kunskap om vilka kombinationer av åtgärder som kan motverka attacker och/eller dessas konsekvenser på ett ekonomiskt effektivt sätt. Samtidig ska det betonas att sektorsmyndigheternas och de enskilda verksamhetsutövarnas ansvar är reglerad och är fördelad på en mycket stor mängd olika sektorsmyndigheter och verksamhetsutövare.

Det finns därmed ett behov av att skapa en samordnad förmåga att identifiera principer för säkerhetsåtgärder och tillhörande genomförbara kontrollstrategier som kan uppfylla nationell- och EU-reglering på ett ekonomiskt, tidsmässigt och effektivt sätt. En sådan funktion kan utgöra en samlad kompetens omfattande det enormt omfattande och komplexa området IKT, cybersäkerhet, principer för teknisk kontroll, certifiering och standardisering som redovisats i denna rapport. En sådan funktion kan ges nödvändiga resurser för att behärska dessa områden och kan även ges resurser att ge stöd till sektorsmyndigheter när de utövar sin roll, samt till verksamhetsutövare till stöd för cybersäkerhet i egna nätverks- och informationssystem. Det kan också ge stöd om och när certifiering enligt cybersäkerhetsakten är en effektiv metod för kontroll och när andra alternativ är att föredra.

En nationell stödfunktion med samlad kompetens, tillgänglig för såväl sektorsmyndigheter och verksamhetsutövare, förväntas leda till effektivisering av statens och samhällets resurser inom cybersäkerhetsområdet. Samtidigt bör en sådan funktion etableras med försiktighet så att den inte ”kanibaliserar” på den kompetens som idag finns, och som fortsatt behöver finnas, hos myndigheterna. Det blir viktigt att långsiktigt bygga upp den föreslagna stödfunktionen med ny kompetent personal så långt det är möjligt.

Med tillräckliga resurser kan en sådan funktion även bidra till att även identifiera olika sektorsmyndigheters och verksamhetsutövares behov av cybersäkerhet och i samverkan med dessa proaktivt medverka till att påverka innehållet i certifieringskraven i ordningarna eller de standarder som ordningarna bygger på.

11.4 Förslag – En samlad nationell kompetens- och stödfunktion för cybersäkerhet

En samlad nationell kompetens- och stödfunktion för cybersäkerhet bör etableras inom staten. Denna stödfunktion ska ge stärkt nationell förmåga för analys, samordning, proaktiv påverkan inom standardisering och certifieringordningar, och ska kunna stödja sektorsmyndigheter och verksamhetsutövare (offentliga såväl som privata) inom cybersäkerhetsområdet.

Sektorsmyndigheter och/eller verksamhetsutövares ansvar enligt EU-rätt och/eller nationell rätt föreslås kvarstå oförändrad. Den föreslagna funktionen utgör ett stöd till sektorsmyndigheter och verksamhetsutövare, som självständigt fortsatt bär ansvar

för sina respektive uppdrag och verksamheter. Det är sektorsmyndigheters och verksamhetsutövares behov och tolkning av sina respektive rättsliga ansvar som ska inrikta stödfunktionens verksamhet.

Stödfunktionen föreslås ha till uppgift att etablera god kännedom om vanligt förekommande användningsområden för nätverks- och informationssystem och vilka de rättsliga förutsättningarna för cybersäkerhetsarbete är.

Stödfunktionen bör ha god kännedom om vilka hot och sårbarheter som finns och vilka åtgärder som kan vidtas för att minska risken för en incident och/eller dess konsekvenser.

Stödfunktionen föreslås etablera kunskap och erfarenhet av de olika kategorier av standarder som är relevanta och ligger till grund för dagens it- och kommunikationssystem, förstå hur de samverkar säkerhetsmässigt och vad det innebär för cyberrisker i allmänhet.

Stödfunktionen förslås ha till uppgift att strategiskt, långsiktigt och kontinuerligt bevaka hur förändringar, t.ex. beträffande hotbild och utveckling av teknik och standarder etc., kan påverka cybersäkerheten.

Stödfunktionen föreslås få till uppgift att i samråd med sektorsmyndigheter utarbeta rekommenderade lösningar för säkerhetsbehov som delas av flera sektorer, samt i övrigt utgöra ett expertstöd till sektorsmyndigheter och verksamhetsutövare angående effektiva, genomförbara och kostnadseffektiva lösningar som kan adressera respektive sektors behov, avseende bl.a. arkitektur, produkter, drift, underhåll, övervakning och kontrollmetoder (inkl. certifiering), samt därtill relaterade standarder.

Stödfunktionen föreslås ha till uppgift att i samverkan med sektorsmyndigheterna bevaka och/eller påverka utvecklingen i relevanta standardiseringsorgan.

Stödfunktionen föreslås ha till uppgift att samordna sektorsmyndigheters och verksamhetsutövande myndigheters arbete inom standardiseringsorganen, samt upptäckta och hantera målkonflikter mellan myndigheter vid utveckling av certifieringsordningar och/eller standarder.

Inom specifika teknik- eller sakområden (t.ex. kryptering, frågor som rör reglerad avlyssning eller områden där en enskild sektorsmyndighet är tongivande) kan enskild myndighet få i uppdrag att samverka med stödfunktionen samt representera svenska intressen i relevanta organ, t.ex. standardiseringsorgan.

Stödfunktionen föreslås särskilt samverka med myndigheter med ansvar för föreskrifts- och tillsynsarbete inom säkerhetsskyddslagens område i syfte att allmänt inrikta stödfunktionens arbete, inklusive frågor som rör EU:s certifieringsordningar och relaterade standarder. Dessa myndigheter föreslås bl.a. bidra med stöd i bedömning om när det av säkerhetsmässiga skäl kan vara motiverat att utveckla EU-regionala standarder som refereras i en certifieringsordning i stället för globala standarder.

Stödfunktionen föreslås ha till uppgift att verka för ökad ensning inom ramen för sektorsmyndigheternas tillämpning av respektive rättsordning och därmed tillgodose

verksamhetsutövares behov av samordnat stöd och regler för att minska splittringen avseende t.ex. reglering, vägledningar och standarder.

Stödfunktionen föreslås ha till uppgift att i samverkan med sektorsmyndigheter och verksamhetsutövare etablera kunskap om vilka kontroll- och verifieringsmetoder som är lämpliga, förståelse för när och hur certifiering enligt cybersäkerhetsakten är en lämplig metod, samt när andra alternativ är att föredra.

Stödfunktionen föreslås ha till uppgift att i samverkan med sektorsmyndigheter och verksamhetsutövare utvärdera certifieringsordningarnas effektivitet i både Sverige och övriga medlemsstater.

Stödfunktionen föreslås ha till uppgift att i samverkan med sektorsmyndigheter och verksamhetsutövare inom EU verka för att certifiering enbart används där så är lämpligt och där tillhörande standarder är tillräckligt tydliga för enhetlig tillämpning, samt i samverkan med sektorsmyndigheter verka mot ineffektiva åtgärder i certifieringsordningar och relaterade standarder.

Stödfunktionen föreslås ha till uppgift att samverka med myndigheter med uppgifter och ansvar för Sveriges medlemskap i Nato, i syfte att verka för samordning, och när så är lämpligt ensning, mellan Natos regelverk för cybersäkerhet och certifiering, samt motsvarande inom EU och på nationell nivå.

Stödfunktionen föreslås ha i uppdrag att samverka med näringslivet för att identifiera dess behov i relation till de certifieringsordningar (och relaterade standarder) som utvecklas.

Försvarets materielverk, som är Sveriges representant i EU-kommissionens och Enisas arbetsgrupper, ska samverka med Stödfunktionen i syfte att identifiera sektorsmyndigheters, verksamhetsutövares och näringslivets behov och föra fram dessa.

I de fall EU-rätt refererar till cybersäkerhetscertifiering bör berörda sektorsmyndigheter i samverkan med Stödfunktionen arbeta för att tillvarata näringslivets behov.

Stödfunktionen föreslås ha till uppgift att ge stöd till Försvarets materielverk inom ramen för dess uppdrag att representera Sverige i EU-kommissionen och Enisas olika arbetsgrupper vid utveckling och utvärdering av certifieringsordningar och därtill relaterade standarder.

Stödfunktionen föreslås vara anslagsfinansierad för sin huvuduppgift. Verksamhet föreslås utöver det kunna finansieras med avgifter för eventuellt tillhandahållet stöd till sektorsmyndigheter och verksamhetsutövare.

Stödfunktionen bör ges tillräckliga resurser för att kunna etablera och upprätthålla bred och djup kompetens inom cyberområdet, effektivt samverka med sektorsmyndigheterna, tillsammans med sektorsmyndigheterna samt delta och proaktivt påverka i relevanta organisationer och grupper vid utveckling av standarder, tekniska specifikationer och/eller certifieringsordningar.

Stödfunktionen föreslås ges till uppgift att årligen rapportera till regeringen med en bedömning av till hur arbetet med att identifiera nationella behov av cybersäkerhet,

utvecklingen av stöd till sektorsmyndigheter och verksamhetsutövare, samt resultatet av påverkansarbete på relevanta standarder och certifieringsarbete.

11.5 Hur nationella behov i fråga om cybersäkerhet kan identifieras – motivering till förslaget

Olika organisationer och intressenter har olika ansvar, uppgifter och behov inom cybersäkerhetsområdet.

Sektorsmyndigheter (föreskrivande, tillsyns- och samordnande myndigheter) kan ha behov av att ange mer eller mindre detaljerade krav eller vägledningar som motsvarar lagstiftningens intentioner, t.ex. krav- och kontrollmekanismer som kan utgöra stöd för dessa myndigheters föreskrifts- och tillsynsarbete inom cyberområdet, eller t.ex. samråd kring driftsättning av nätverks- och informationssystem, utkontraktering eller upphandling.

Verksamhetsutövare (offentliga såväl som privata) behöver stöd för att etablera säkerhet i enlighet med eget ansvar, hotbild, reglering och tillgängliga resurser samt vid upphandling och utkontraktering.

Näringslivet behöver (som producent/leverantör) reglering som inte onödigt hindrar innovation, skapar utestängning från marknaden eller bidrar till fragmentering av reglering, vägledningar och standarder (nationellt eller internationellt). Näringslivet behöver möjlighet att påverka regleringar och tillhörande krav på funktion och teknisk kontroll.

Vad som därmed kan anses sägas vara nationella behov grundas därmed i de många olika intressenternas konkreta behov, bedömningar och riskhanteringsbeslut som sektorsmyndigheter och verksamhetsutövare har att ansvara för inom ramen för vars och ens ansvar, uppgifter och förutsättningar.

Utmaningarna med cybersäkerhetsområdets komplexitet, bristen på kompetens hos sektorsmyndigheter och verksamhetsutövare och svårigheterna för enskilda organisationer att bevaka och påverka alla relevanta standarder och certifieringsordningar, pekar på att det finns ett gemensamt behov av ökat centralt stöd avseende kunskap om IKT-teknik, cybersäkerhet, existerande standarders för- och nackdelar ur säkerhetshänseende, hur dessa interagerar säkerhets- och kostnadsmässigt, kunskap om olika attacktekniker och angripare, kunskap om vilka kombinationer av åtgärder som kan motverka attacker och/eller dessas konsekvenser på ett ekonomiskt effektivt sätt. Vidare behöver regleringar och standarder inom cybersäkerhet vara harmoniserade så att svenska aktörer för IKT-produkter och IKT-tjänster inte missgynnas.

Den nationella stödfunktion för cybersäkerhet som föreslås enligt föregående avsnitt kan i samråd med sektorsmyndigheter utarbeta rekommenderade lösningar för säkerhetsbehov som delas av flera sektorer, samt i övrigt utgöra ett expertstöd till sektorsmyndighet och enskilda verksamhetsutövare angående effektiva, genomförbara och kostnadseffektiva lösningar som kan adressera respektive organisations behov, avseende bl.a. arkitektur, produkter, drift, underhåll,

övervakning och kontrollmetoder (inkl. certifiering), samt därtill relaterade standarder.

Stödfunktionen kan etablera och upprätthålla kompetens inom IKT och cybersäkerhet, samt effektivt samverka med sektorsmyndigheterna och tillsammans med dessa bevaka eller proaktivt delta i eller påverka utvecklingen i relevanta standardiseringsorgan och/eller certifieringsordningar.

11.6 Myndigheter som bör bidra till arbetet med behovsanalys – motivering till förslaget

Det finns ett drygt tiotal EU-regleringar (etablerade eller under utveckling, se kapitel 7 och bilaga 3) som refererar till cybercertifiering som ett sätt att visa uppfyllnad av respektive reglerings krav på cybersäkerhetsegenskaper. Cybersäkerhetscertifiering kan således på nationell nivå få påverkan inom alla sektorer som omfattas av eller på annat sätt är beroende av dessa EU-regleringar.

Säkerhetspolisen och Försvarsmakten är myndigheter med ansvar för föreskrifter, tillsyn och samordning inom säkerhetsskydd. Utöver det bedriver ett antal tillsynsmyndigheter tillsyn avseende säkerhetsskydd över en rad myndigheter och enskilda verksamhetsutövare (offentliga såväl som privata) kopplat till olika sektorer. Beredskapsmyndigheterna ansvarar, enligt förordning (2022:524) om statliga myndigheters beredskap, för att egna informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt.

Eftersom cybersäkerhetscertifiering kan vara relevant inom alla dessa EU-reglerade sektorer , och inom försvarssektorn, dels som ett medel för det egna säkerhetsarbetet, dels som ett medel för verksamhetsutövare att visa att man uppfyller stipulerade (ofta omfattande) cybersäkerhetskrav, och att certifiering i närtid kan bli tvingande, är det många sektorsmyndigheter och verksamhetsutövare som behöver ha kompetens att påverka både om och när certifiering är lämpligt samt bevaka och påverka certifieringsordningarnas innehåll.

Det framstår som väl motiverat att de myndigheter som är ansvariga för genomförande av EU-regleringar som hänvisar till certifiering samverkar och ges stöd i syfte att tillse att dessa lättare kan bedöma när certifiering är lämpligt, och likaledes verka för alternativa mekanismer inom EU-rätten när andra kontrollmekanismer är mer lämpliga. I de fall certifiering beslutats bli ett krav på EU-nivå, behöver de olika sektorsmyndigheterna stöd för att samlat kunna verka för att certifieringsordningar och de tillhörande standarderna har en säkerhetshöjande effekt som är rimlig i förhållande till kostnaden för certifiering.

För att säkerställa samordning mellan myndigheterna föreslås att sektorsmyndigheter ges i uppdrag samordna sitt deltagande vid utveckling av standarder och/eller certifieringsordningar med stödfunktionen.

11.7 Proaktiv påverkan på certifieringsordningarna och standarder – motivering till förslaget

Cybersäkerhetsakten beskriver ett ramverk genom vilket certifieringsordningar för cybersäkerhet kan utvecklas i samverkan mellan bland annat EU-kommissionen, medlemsstaterna, Enisa och näringslivet. Vid utarbetandet av förslag till certifieringsordningar ska Enisa samråda med alla berörda intressenter genom en formell, öppen, transparent och inkluderande samrådsprocess. Enisa ska ha ett nära samarbete med medlemsstaternas NCCA-myndigheter. Baserat på Enisas förslag utarbetar EU-kommissionen därefter ett utkast till genomförandeakt. Genom ett kommittéförfarande och förhandlingar med medlemsstaterna når slutligen genomförandetakten sitt slutliga innehåll efter omröstning av medlemsstaterna i genomförandekommittén.

För att kunna påverka utvecklingen av dessa certifieringsordningar måste svenska myndigheter, branschorganisationer och företag delta inom olika forum och grupper inom ramen för EU-kommissionen och Enisas arbetsprocess, samt inom alla de olika organ som utvecklar de standarder och tekniska specifikationer som refereras i certifieringsordningarna eller annars är av betydelse för dessa. Exempel på sådana organ och standarder framgår av bilaga 6, 7, 8 och 10.

Det råder brist på kompetens och den är svår och dyr att rekrytera, vilket förstärker utmaningarna för sektorsmyndigheters och verksamhetsutövares (offentliga såväl som privata) förmåga att aktivt medverka vid utveckling av standarder och/eller certifieringsordningar.

Stödfunktionen kan etablera kunskap om vilka kontroll- och verifieringsmetoder som är lämpliga, samt förståelse för när och hur certifiering enligt cybersäkerhetsakten är en lämplig metod samt vilka kompletterande krav och kontroller som kan behöva genomföras av verksamhetsutövare.

Stödfunktionen kan ha till uppgift att i samverkan med sektorsmyndigheterna bevaka och/eller påverka utvecklingen i relevanta standarder och certifieringsordningar.

Stödfunktionen kan ha till uppgift att samordna sektorsmyndigheters och verksamhetsutövande myndigheters arbete inom standardiseringsorganen, samt upptäckta och hantera målkonflikter mellan myndigheter.

11.8 Stöd till myndigheter och verksamhetsutövare – motivering till förslaget

Som framgår av tidigare avsnitt föreslås etablerande av en stödfunktion som kan etablera en nationell samlad förmåga för att definiera principer för cybersäkerhetsåtgärder och tillhörande genomförbara kontrollstrategier som kan uppfylla nationell- och EU-reglering på ett ekonomiskt, tidsmässigt och effektivt sätt. Den föreslagna funktionen föreslås ges i uppdrag att etablera en samlad kompetens inom det väldigt omfattande och komplexa området IKT, cybersäkerhet, principer för teknisk kontroll, certifiering och standardisering. Funktionen föreslås även ges resurser som kan ge stöd till sektorsmyndigheter och verksamhetsutövare (offentliga

såväl som privata) när de utövar sitt ansvar för cybersäkerhet i egna nätverks- och informationssystem i allmänhet, samt stöd att bedöma när certifiering enligt cybersäkerhetsakten är en effektiv metod för kontroll och när andra alternativ är att föredra.

Stödfunktionen kan i samråd med sektorsmyndigheter utarbeta rekommenderade lösningar för att adressera säkerhetsbehov som delas av flera sektorer, samt i övrigt utgöra expertstöd till sektorsmyndigheter angående effektiva, genomförbara och kostnadseffektiva lösningar som kan adressera respektive sektors behov, avseende bl.a. arkitektur, produkter, drift, underhåll, övervakning och kontrollmetoder (inkl. certifiering), samt därtill relaterade standarder.

Av regeringens ”Nationell strategi för samhällets informations- och cybersäkerhet” från 2017 framgår att i dagsläget bedriver de olika aktörerna i samhället sitt informationssäkerhetsarbete på delvis olika sätt, utifrån olika förutsättningar och behov, baserat på flera olika regelverk och delvis olika uppfattningar om hot och risker. Inom ramen för Samverkansgruppen för informationssäkerhet (SAMFI) och senare Nationellt cybersäkerhetscenter gjordes förstudier för att närmare beskriva dels arbetsprocesserna för ett samordnat stöd och kravställning, dels utformningen av ett sådant stöd. Enligt förstudien föreslås att den nationella modellen för cybersäkerhet innehåller:

- en nationell cybersäkerhetsnorm
- en struktur med arbetsprocesser för utveckling och förvaltning av cybersäkerhetsnormen.

Enligt förstudien kan cybersäkerhetsnormen underlätta och effektivisera organisationers arbete med cybersäkerhet. Normen är tänkt att skapa förutsättningar för att stärka samhällets robusthet i cyberdomänen bl.a. genom att:

- information av samma värde får ett likvärdigt skydd oavsett var i samhället informationen hanteras
- näringslivet kan ges en enhetlig och effektiv styrning vid upphandling och utkontraktering av it-system och tjänster oavsett vilken myndighet eller annan offentlig organisation som upphandlar, utkontrakterar eller samverkar med näringslivet
- skapa förutsättningar för minskad fragmentering och ökad enhetlighet av krav och stöd på området, samt att myndigheterna genom normen strävar efter att ta fram gemensamma publikationer där så är möjligt
- förenkla för organisationer att omhänderta både rättsliga och andra krav på cybersäkerhet

Cybersäkerhetsnormen har föreslagits bl.a. ha följande innehåll:

- Övergripande beskrivning av och stöd för hur användarna ska tillämpa cybersäkerhetsnormen.
- Gemensam terminologi och taxonomi.

- Processer och metoder för att kategorisera system och välja säkerhetsåtgärder med stöd av en klassningsmodell för cybersäkerhetsnormen som kopplar skyddsnivåer med tillhörande säkerhetsåtgärder.
- Skyddsnivåer bestående av konkreta krav på säkerhetsåtgärder, inklusive bakomliggande skäl för valet av respektive åtgärder, exempelvis rättsliga eller sektorsspecifika krav.
- Processer och metoder för utvärdering av säkerhetsåtgärder, godkännande av informationssystem samt kontinuerlig övervakning av cybersäkerheten i syfte att säkerställa att säkerhetsåtgärder över tid har avsedd effekt.

Cybersäkerhetsnormen ska stödja organisationers cybersäkerhetssäkerhetsarbete och bland annat beakta standarder inom cybersäkerhetsområdet så länge svenska behov kan mötas. Samtliga dokument som ingår i normen ska utgöra en sammanhållande och praktiskt användbar helhet utan sinsemellan motsägande krav eller andra inkonsekvenser.

I det fall det beslutas att en sådan s.k. Nationell modell för cybersäkerhet med tillhörande cybersäkerhetsnorm etableras, bör den kunna utgöra ett betydande stöd till både sektorsmyndigheter och verksamhetsutövare och innehålla information om certifierade produkter, tjänster och processer och deras säkerhetsnivåer.

11.9 Samverkan med partnerländer utanför EU

11.9.1 Inledning

Uppdraget innefattar att behovet av att kunna certifiera produkter, tjänster och processer även i partnerländer utanför EU, särskilt USA, beaktas.

Som tidigare noterats är digitaliseringens försörjningskedjor globala. De företag som levererar produkter, system och tjänster verkar ofta på en global marknad. De ska efterleva standarder, olika regionala eller nationella regleringar och ibland krav på certifieringar. Om inte certifikat erkänns mellan olika marknader innebär detta att företagen behöver genomföra certifiering av sådana produkter och tjänster flera gånger, även i de fall då de underliggande standarderna är desamma. För företagen kan en sådan brist på tillit mellan olika marknader vara mycket kostnadsdrivande.

Av samma anledning är det angeläget att globala standarder främjas för de företag som verkar på någon internationell marknad. EU-specifika krav och, regionala standarder, kan öka företagens kostnader och minska deras konkurrenskraft och leveransförmåga på den internationella marknaden. I begränsad omfattning inom säkerhetsområdet kan dock EU-specifika standarder vara motiverade. Principiellt bör EU-specifika standarder undvikas utom där det av säkerhetsmässiga eller andra skäl är väl motiverat med regionala standarder.

Cybersäkerhet är nära knutet till nationella säkerhetsintressen. Många länder kan vara ovilliga att anta internationella standarder som de anser kan kompromettera deras nationella säkerhet eller suveränitet. Risken för cyberangrepp måste ses som en del av den nationella säkerheten. Det rapporteras i stort sett dagligen om cyberangrepp som syftar till spionerі eller sabotage och där statsaktörer eller till sådana associerade organisationer ligger bakom. Det kan finnas stora svårigheter att samverka i

internationell standardisering och i en öppna standardiseringsorgan där representanter från andra länder med skilda värderingar och/eller intressen än de i den egna säkerhetspolitiska/ekonomiska intressesfären.

Detta illustreras inte minst av diskussioner kring regler som föreslagits ska ingå i cybersäkerhetsaktens certifieringsordning för cybersäkerhet i molntjänster, regler som ledde till frågor inte minst från USA eftersom de föreslagna reglerna ansågs bl.a. vara marknadsbegränsande för amerikanska molntjänstleverantörer[35].

11.9.2 Cybersäkerhetsakten och relation till tredjeländer

Cybersäkerhetsakten (CSA) anger att det behövs ett tätare internationellt samarbete för att förbättra cybersäkerhetsstandarder, bland annat genom att fastställa gemensamma beteendenormer och anta uppförandekoder, använda internationella standarder utbyta information, och på så vis främja dels snabbare internationellt samarbete som svar på nätverks- och informationssäkerhetsproblem och dels främja en gemensam global syn på sådana problem för en ökad cybersäkerhet.

Cybersäkerhetsakten anger att för att ytterligare underlätta handeln och erkänna att IKT-leveranskedjorna är globala får avtal om ömsesidigt erkännande av europeiska cybersäkerhetscertifikat ingås av unionen i enlighet med artikel 218 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget).

EU-kommissionen får med beaktande av rådgivningen från Enisa och den europeiska gruppen för cybersäkerhetscertifiering rekommendera att relevanta förhandlingar inleds. Varje europeisk ordning för cybersäkerhetscertifiering bör föreskriva särskilda villkor för sådana avtal om ömsesidigt erkännande med tredjeländer.

EU-kommissionen kan utvärdera hur Enisa möjligen skulle kunna stödja bedömningen av om IKT-produkter, -tjänster och -processer som förs in från tredjeländer är förenliga med unionsreglerna.

Enisa ska tillhandahålla rådgivning och stöd till EU-kommissionen i frågor som rör avtal om ömsesidigt erkännande av cybersäkerhetscertifikat med tredjeländer i samarbete med Europeiska gruppen för cybersäkerhetscertifiering. Det anges även att Enisas styrelse ska anta en strategi för förbindelserna med tredjeländer och internationella organisationer i de frågor som Enisa har behörighet för.

Cybersäkerhetsakten anger även att certifieringsordningar antagna enligt akten kan innehålla villkor för ömsesidigt erkännande av certifieringsordningar med tredjeländer.

[35] Big Tech cries foul over EU cloud-security label – POLITICO (https://www.politico.eu/article/tech-sector-foul-eu-cloud-security-label/)

11.9.3 Särskild dialog mellan EU-kommissionen och USA

Det pågår f.n. en dialog om samverkan på cybersäkerhetsområdet mellan EU-kommissionen och USA.[36]

I möte i början av januari 2024 mellan Kommissionär Thierry Breton, och Alejandro N. Mayorkas, United States Secretary of Homeland Security, diskuterades bl.a. ”EU-USA Joint Cyber Safe Products Action Plan”. Denna plan var ett resultat från toppmötet mellan EU och USA i oktober 2023, som beskriver stegen för ytterligare samarbete mellan kommissionen och relevanta amerikanska tillsynsmyndigheter för att bereda grunden för att om möjligt etablera ömsesidigt erkännande av cybersäkerhet avseende ”sakernas internet ” (Internet of Things). Handlingsplanen bygger på Cyber Resilience Act och det föreslagna amerikanska cybersäkerhetsmärkningsprogrammet Cyber Trust Mark Act.

11.9.4 Försvarets materielverks bedömning

Frågan om behovet av att även kunna certifiera produkter, tjänster och processer i partnerländer utanför EU, särskilt USA, är av både handelspolitisk och säkerhetspolitisk natur.

Sverige kan inom ramen för EU-samarbetet verka för att svenska intressen adresseras, inklusive Sveriges möjlighet att samverka med USA kring cybersäkerhetscertifieringar och relaterade standarder.

För att minska risken för onödiga tekniska handelshinder och kravfragmentering för näringslivet kan Sverige verka för att globala standarder utvecklas och används. I de fall det finns behov av regionala standarder bör myndigheter med ett särskilt ansvar för säkerhetsskyddslagstiftningen medverka för att bedöma behovet av sådana regionala standarder.

[36] EU and United States enhance cooperation on cybersecurity | Shaping Europe’s digital future (europa.eu) (https://digital-strategy.ec.europa.eu/en/news/eu-and-united-states-enhance-cooperation-cybersecurity)

Bilagor

Bilaga 1 – Uppdraget

Regeringen

Regeringsbeslut **I:1**

2023-05-11
Fö2021/00796 (delvis)

Försvarsdepartementet

Försvarets materielverk
115 88 Stockholm

Uppdrag till Försvarets materielverk om att föreslå hur nationella behov kan tillgodoses vid framtagandet av certifieringsordningar enligt EU:s cybersäkerhetsakt

Regeringens beslut

Försvarets materielverk ges i uppdrag att analysera och lämna förslag på hur nationella behov i fråga om cybersäkerhet kan identifieras och omsättas till säkerhetskrav som Sverige bör framhålla i arbetet med att utveckla certifieringsordningar inom EU:s cybersäkerhetsakt. Behovet av att även kunna certifiera produkter, tjänster och processer i partnerländer utanför EU, särskilt USA, ska beaktas. I uppdraget ingår att lämna förslag på vilka myndigheter som bör ges i uppgift att bidra till arbetet med behovsanalysen samt hur näringslivet kan beredas möjlighet att delta i arbetet.

Försvarets materielverk ska även analysera och lämna förslag på hur information om certifierade produkter, tjänster och processer och deras säkerhetsnivåer kan tillgängliggöras för myndigheter och andra verksamhetsutövare.

Försvarets materielverk ska i genomförandet av uppdraget samverka med Försvarsmakten och Säkerhetspolisen och vid behov med Försvarets radioanstalt, Myndigheten för samhällsskydd och beredskap, Polismyndigheten, Post- och telestyrelsen och andra berörda myndigheter samt föra dialog med näringslivet.

Uppdraget ska redovisas skriftligt till Regeringskansliet (Försvarsdepartementet) senast den 30 april 2024.

Telefonväxel: 08-405 10 00
Fax: 08-723 11 89
Webb: www.regeringen.se

Postadress: 103 33 Stockholm
Besöksadress: Jakobsgatan 9
E-post: fo.registrator@regeringskansliet.se

Skälen för regeringens beslut

Försvarets materielverk är nationell myndighet för cybersäkerhetscertifiering enligt EU:s cybersäkerhetsakt. Inom ramen för den uppgiften representerar myndigheten Sverige i Europeiska gruppen för cybersäkerhetscertifiering som deltar i arbetet med utarbetande av certifieringsordningar.

Informations- och cybersäkerheten generellt i samhället såväl som säkerhetskänslig verksamhet är ofta beroende av säkerhetsegenskaper hos kommersiella produkter och tjänster som skulle kunna verifieras inom det europeiska ramverket för cybersäkerhetscertifiering. Av denna anledning bör risk-, hot- och sårbarhetsanalyser för såväl samhället i allmänhet som de säkerhetskänsliga verksamheterna ingå i det analysarbete som sedan kan omsättas till säkerhetskrav som Sverige bör framhålla i arbetet med att utarbeta certifieringsordningar. Uppdraget syftar således till att utveckla proaktiva arbetssätt i förhållande till nationella intressen och förhandlingspositioner inom ett alltmer betydelsefullt område för cybersäkerhetsarbetet. Regeringen bedömer att det är av vikt att myndigheter med ansvar för både hot-, sårbarhets- och riskanalyser för samhället i allmänhet såväl som myndigheter med ansvar för säkerhetskänslig verksamhet bidrar till det arbetet. Mot bakgrund av att näringslivet både är en konsument och producent av certifierade produkter är det av vikt ett en dialog förs med dessa under uppdragets genomförande.

Regeringen bedömer även att det är av vikt att utveckla arbetssätt för informationsspridning om certifierade produkter, tjänster och processer. Detta i syfte att svenska myndigheter och andra verksamhetsutövare ska kunna tillgodogöra sig hur certifiering kan användas som en del i respektive organisations arbete med cybersäkerhet.

På regeringens vägnar

Pål Jonson

Anders Jörnesten

Kopia till

Statsrådsberedningen/NSR
Justitiedepartementet/L4, PO
Utrikesdepartementet/SP
Finansdepartementet/DIS
Klimat- och näringslivsdepartementet/EIN
Försvarets radioanstalt
Försvarsmakten
Myndigheten för samhällsskydd och beredskap
Polismyndigheten
Post- och telestyrelsen
Säkerhetspolisen

Bilaga 2 – Presumtion om uppfyllnad av cybersäkerhetskrav

Följande typsituationer och möjliga/lämpliga förhållningssätt har identifierats rörande presumtion om uppfyllnad av cybersäkerhetskrav:

Typsituation	Möjliga/lämpliga förhållningssätt
1) Unionsrätt refererar tydligt till cybersäkerhetsakten och dess certifiering.	En CSA-certifiering presumeras visa överensstämmelse med rättsakten ifråga när föremålen för certifiering och tillsyn är (i princip) desamma och har granskats utifrån (i princip) samma säkerhets- och evalueringskrav, jfr. avsnitt 7.1. Man bör dock notera att en aldrig så stark presumtion, vilket det är fråga om här, ”bara” är en presumtion. En tillsynsmyndighet kan ha information som gör att presumtionen behöver brytas. Myndigheten torde dock i dessa fall ha starka beviskrav för att så är fallet.
2) Unionsrätt refererar till ”certifiering” utan referens till CSA:	---
a) CSA-certifiering är underförstått .	Se 1), förutsatt att man kan visa med tillräcklig säkerhet att CSA-certifiering är underförstått.
b) CSA-certifiering är INTE underförstått.	En CSA-certifiering presumeras visa överensstämmelse med kraven i rättsakten ifråga när föremålen för certifiering och tillsyn är (i princip) desamma och har granskats utifrån (i princip) samma säkerhets- och evalueringskrav. Att vid tillsyn använda befintliga certifieringar och uppfyllnad av standarder som bevis för överensstämmelse mot säkerhetskrav är vedertaget. Det som hänt på senare tid är att EU-lagstiftning mer uttryckligt, ofta i själva lagstiftningstexten, pekar mot certifieringar, t.ex. CSA-certifieringar.
c) NLF-baserad reglering av cybersäkerhets- och evalueringskrav	En CSA-certifiering presumeras visa överensstämmelse med kraven i rättsakten ifråga när föremålen för certifiering och tillsyn är (i princip) desamma och har granskats utifrån (i princip) samma säkerhets- och evalueringskrav. Att vid tillsyn använda befintliga certifieringar och uppfyllnad av standarder som bevis för överensstämmelse mot säkerhetskrav är vedertaget.
3) CSA gör uttryckliga undantag från sitt tillämpningsområde:	

a) Art. 1.1 CSA: GDPR	Där det finns certifikat i enlighet med andra certifieringsordningar än cybersäkerhetsakten torde dessa vara mer frekventa och användningsbara vid tillsynen. Men CSA-certifieringar kan ju också ha ett bevisvärde, jfr 2b) ovan. Vad som här kan uppstå är att det kan finnas flera certifieringar för (i princip) samma sak. Om alla dessa certifieringar kommit till (i princip) samma resultat är situationen relativt okomplicerad. Om de dock skiljer sig måste tillsynsmyndigheten avgöra saken utan att ha en förhållandevis stark presumtion att göra sin bedömning utifrån.
b) Art 1.2 CSA: ” […] medlemsstaternas befogenheter i fråga om verksamhet som berör allmän säkerhet, försvar, nationell säkerhet och statens verksamhet på straffrättens område.”	Principerna ovan (1-3a) torde gälla även här, låt vara att eventuella certifieringar inom de undantagna områdena utgör nationella certifieringsordningar inom områden utanför EU:s kompetens. En tillkommande komplikation för tillsynsmyndigheterna är att gränsen för EU-respektive nationell kompetens inom dessa områden inte alltid är glasklar. Till det kommer att det kan förutses att it-produkter/tjänster/processer/system för dessa ändamål ofta kommer att upphandlas med (åtminstone viss) förlitan på certifieringar som baserar sig på certifieringsordningar baserade på EU-rätt med den inre marknadend funktion (alltså inte nationell säkerhet etc.) som rättslig grund för EU-lagstiftningen.

Bilaga 3 – EU-rättsakter med certifieringsreferenser

Nedan tabell sammanställer:

- EU-reglering där certifiering enligt cybersäkerhetsakten krävs eller kan utgöra presumtion för uppfyllnad av kraven i regleringen.
- Vem eller vad som omfattas av regleringen.
- Typ av cybersäkerhetskrav med relevans för cybersäkerhetsakten.
- Vilka svenska myndigheter som har (eller kan antas ha/få) ansvar för det svenska genomförandet (tillsyn, föreskriftsrätt, m.m.).
- Om certifiering *måste* användas (krav) eller om certifiering *kan* användas som presumtion för kravuppfyllelse.
- Om EU-kommissionen (KOM) möjlighet i EU-rättsakten att anta (eller antagit) delegerade eller genomförande akter om certifiering.
- Om det finns svensk eller annan MS-reglering med krav på certifiering.

EU-reglering	Vem/vad omfattas av regleringen	Typ av cybersäkerhetskrav med relevans för cybersäkerhetsakten	Svenska myndigheter med ansvar	Certifiering krävs eller anges som presumtion för kravuppfyllelse	KOM-mandat rörande certifieringskrav	SE eller annan MS reglering	Ytterligare kommentarer
NIS2 (antagen)	Energi, transporter (och del av sektorns tillverkning), bankverksamhet och finansmarknads-infrastruktur, del av hälso- och sjukvårdssektorn (och del av sektorns tillverkning), sektorerna dricksvatten, avloppsvatten och produktion, bearbetning och	Lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverks- och informationssystem som de använder för sin verksamhet eller för att tillhandahålla sina tjänster och för att förhindra eller minimera	Statens energimyndighet Transport-styrelsen Finans-inspektionen Inspektionen för vård och omsorg Läkemedelsverket Livsmedelsverket Post- och telestyrelsen Länsstyrelserna i Stockholms, Skåne, Västra Götalands och Norrbottens län MSB	CSA-certifikat ger presumtion om överensstämmelse med cyberkraven i NIS2 KOM kan anta delegerad akt där de kan ange vilka kategorier av väsentliga eller viktiga entiteter som ska vara skyldiga att använda vissa certifierade IKT-produkter, IKT-tjänster och IKT-processer eller erhålla ett CSA- certifikat.	24.1. För att visa att vissa krav enligt artikel 21 [Riskhanteringsåtgärder för cybersäkerhet] är uppfyllda får MS ålägga väsentliga och viktiga entiteter att använda särskilda IKT-produkter, IKT-tjänster och IKT-processer, som har utvecklats av den väsentliga eller viktiga entiteten eller upphandlats från tredje parter, som är	NIS2-utredningen inte lämnat förslag i denna del, hänvisar till KOM:s kommande delegerade akter. MS kan föreskriva att CSA certifikat ger presumtion om överensstäm melse med	Kan ev. förväntas att dels KOM reglerar mot CSA, dels några MS, vilket i praktiken får en inriktande effekt för hela marknaden. EU:s sekundärrätt och/eller andra MS reglering med krav mot CSA-cert kan innebära att

	distribution av livsmedel, sektorerna digital infrastruktur, digitala leverantörer, förvaltning av IKT-tjänster, post- och budtjänster och sektorn rymden, offentlig förvaltning, avfallshantering, forskning, del av sektorn tillverkning och tillverkning, produktion och distribution av kemikalier samt lärosäten med examenstillstånd. Verksamhetsutövarna ska tillhandahålla tillsynsmyndigheten den information som behövs för tillsynen.	incidenters påverkan på mottagarna av deras tjänster och på andra tjänster	Tillsynsmyndigheten ska utöva tillsyn över att cybersäkerhetslagen och föreskrifter som meddelats i anslutning till lagen följs. Tillsynsmyndigheten får om det finns särskilda skäl ålägga en verksamhetsutövare att på egen bekostnad låta ett oberoende organ utföra en riktad säkerhetsrevision och att redovisa resultatet för tillsynsmyndigheten. Tillsynsmyndigheten får också låta genomföra säkerhetsskanningar hos verksamhetsutövare som omfattas av cybersäkerhetslagen.		certifierade enligt europeiska ordningar för cybersäkerhetscertifiering som antagits i enlighet med artikel 49 i förordning (EU) 2019/88. 2. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 38 för att komplettera detta direktiv genom att ange vilka kategorier av väsentliga eller viktiga entiteter som ska vara skyldiga att använda vissa certifierade IKT-produkter, IKT-tjänster och IKT-processer eller erhålla ett certifikat enligt en europeisk ordning för cybersäkerhetscertifiering som har antagits enligt CSA. I fall där det inte finns en lämplig europeisk ordning för cybersäkerhetscertifiering med avseende	cyberkraven i NIS2	CSA-cert blir dominerande faktor för cyberkrav (ink krypto) vilket kan påverka förutsättningarna för både SE:s tillämpning av NIS2 samt hur de produkter/tjänster utformas som används inom säkerhetskänslig verksamhet.

					på tillämpningen av punkt 2 i denna artikel kan kommissionen, efter samråd med samarbetsgruppen och europeiska gruppen för cybersäkerhetscertifiering, begära att Enisa utarbetar ett förslag till certifieringsordning enligt CSA.		
CER (antagen)	Samhällsviktig verksamhet, här kallat ”kritiska entiteter” som tillhandahåller samhällsviktiga tjänster inom sektorerna energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, dricksvatten, avloppsvatten, digital infrastruktur, offentlig förvaltning, rymden samt produktion, bearbetning och	CER-direktivet refererar inte till CSA-certifiering direkt, på t.ex. det sätt som NIS2D gör. Men de säkerhetskrav som ställs i CER kan förväntas motsvara de i NIS-direktivet eller även annars tangera säkerhetskrav som kommer ställas i de CSA-baserade certifieringsordningarna.	[NIS2 utredning pågår] Enligt utredningsdirektiven till den s.k. NIS2-utredningen (som också omfattar CER-entiteterna) i princip utgå ifrån att tillsynsmyndigheterna för NIS-sektorerna skall vara desamma för de motsvarande kritiska entiteterna enligt CER-direktivet.	CSA certifikat ger troligen presumtion om överensstämmelse med cyberkraven i CER. MS kan troligen föreskriva att CSA certifikat ger presumtion om överensstämmelse med cyberkraven i NIS2.	Delegerade akter med ref till EUCC, EUCS och/eller EU5G förväntas i framtiden?		

	distribution av livsmedel.						
CRA (förhandl. pågår)	Ekonomiska operatörer, vilket i huvudsak är tillverkare, importörer och distributörer, ska följa de cybersäkerhetskrav förordningen anger för alla produkter med digitala inslag för att de ska kunna göras tillgängliga på den inre marknaden.	Kraven innebär att tillverkare ska ta cybersäkerhet i beaktande i designen och utvecklingen av produkter med digitala inslag. Därtill ska tillverkare granska säkerhetsaspekter under utvecklingsprocessen, ha transparens gentemot konsumenter gällande cybersäkerhetsaspekter samt försäkra säkerhetssupport och uppdateringar på ett proportionerligt sätt under produktens livscykel.	Medlemsstater ska upprätta eller utse en anmälande myndighet som ska ansvara för utförandet av de nödvändiga processerna för bedömning och notifiering av organ för bedömning av överensstämmelse och dessa aktörers kontroll. Nationella tillsynsmyndigheter ska utföra marknadsövervakning och tillsyn inom medlemsstatens territorium. Förslaget kommer att medföra kostnader och nya uppgifter för myndigheter på nationell och EU-nivå som föreslås få ansvar att granska, bedriva tillsyn och upprätthålla de	Regelefterlevnad uppvisas genom en konformitetsbedömning. Produkter med digitala inslag som har certifierats under en europeisk cybersäkerhetscertifieringsordning ska antas vara i överensstämmelse med de väsentliga kraven i förslaget. KOM ska, när det är applicerbart, specificera om ett CSA-certifikat ger tillverkaren undantag från skyldigheterna att genomföra en konformitetsbedömning genom anmälda organ.	EU-förhandlingen pågår. Delegerade akter med ref till EUCC, EUCS och/eller EU5G förväntas i framtiden?	EU-förhandlingen pågår.	Se NIS ovan.

			krav som ställs i förordningen.				
AI (färdigförhandlad men ej formellt antagen)	Baserat på riskbedömning för olika risktyper av AI: -tillhandahållare av AI-system som används på den inre marknaden oavsett om tillhandahållaren är etablerad inom EU eller inte, -de som använder AI-system som finns inom EU, och -användare och tillhandahållare av AI-system där det som genereras av AI-systemet används inom EU oavsett om tillhandahållaren eller användaren är etablerad eller befinner sig inom EU eller i tredjeland.	Förbättra styrning och effektiv tillämpning av befintliga lagar om säkerhetskrav som är tillämpliga på AI och underlätta utvecklingen av en inre marknad för lagliga, säkra och pålitliga AI-system och förhindra fragmentering. Regleringen innebär ett juridiskt batteri för att hantera riskerna som AI-system innebär, och att ingripa om AI inte (längre) gör det den är avsedd att göra eller om riktigheten inte upprätthålls.	Akten innehåller bestämmelser om marknadskontroll och rapporteringsskyldigheter för tillhandahållare när det gäller utredning av AI-relaterade incidenter och tekniska problem. Det anges vilken typ av information som tillhandahållare av AI-system ska hålla och kunna delge behöriga myndigheter, vilken information som myndigheter får och ska inhämta, relationen mellan behöriga myndigheter och kommissionen. Regler om regelefterlevnad och åtgärder som krävs för att uppfylla förordningens krav tas upp.	AI-system med hög risk som har CSA-certifierats, eller för vilka en CSA-försäkran om överensstämmelse har utfärdats, ska förutsättas överensstämma med cybersäkerhetskrav som anges i artikel 15 i AI-förordningen, förutsatt att cybersäkerhetscertifikatet eller försäkran om överensstämmelse eller delar därav omfattar dessa krav.	EU-förhandlingen pågår. Delegerade akter med ref till EUCC, EUCS och/eller EU5G förväntas i framtiden? Det spekuleras också i en separat CSA-ordning för AI. Enisa har Q4 2023 startat en tematisk grupp som tittar på vilka områden som har mogna standarder att certifiera emot.		

eIDAS2 (antagen 240326)	Utfärdare (och användare) av europeiska e-identitetsplånböcker.	Europeiska e-identitetsplånböcker ska göra det möjligt för användaren att (a) på ett säkert sätt begära och erhålla, lagra, välja, kombinera och dela – på ett sätt som är transparent och spårbart för användaren – nödvändiga identifieringsdata och elektroniska intyg på attribut för fysiska personer, för autentisering online och offline i samband med onlineanvändning av offentliga och privata tjänster, och (b) skriva under med hjälp av kvalificerade elektroniska underskrifter. E-identitetsplånböckerna ska [bland mycket annat] i	Utredning pågår: Troligen utses som tillsynsmyndigheter DIGG för e-leg och e-identitetsplånboken och PTS för övriga ”betrodda tjänster” (dvs. ung. som idag). Om de föreslagna ändringarna i eID-förordningen träder i kraft, innebär det att en rad nya krav måste mötas. Sverige måste bl.a. exempelvis inrätta ett bedömningsorgan som har till uppdrag att certifiera e-legitimationslösningar som uppnår tillitsnivåerna i förordningen. De europeiska e-identitetsplånböckernas överenstämmelse med cybersäkerhetskraven certifieras av ackrediterade	De europeiska e-identitetsplånböckernas överensstämmelse med standarder och tekniska specifikationer ***ska certifieras*** av organ för bedömning av överensstämmelse utsedda av MS och i enlighet med en CSA-ordning [Enligt det ursprungliga förslaget utgjorde CSA-certifiering endast en presumtion för cyberkravuppfyllnad. Man kan förmodligen anta att en tvingande CSA-certifiering innebär att man vid tillsynen inte skall ifrågasätta ett CSA-certifikat.]	Så länge som CSA-ordningar för cybersäkerhetscertifiering inte eller endast delvis omfattar de relevanta cybersäkerhetskraven för e-identitsplånböcker ska medlemsstaterna för dessa krav inrätta nationella certifieringssystem i enlighet med de krav som fastställs i genomförandeakter från KOM. EU-kommissionen ska genom genomförandeakter upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för certifiering av de europeiska e-identitetsplånböckerna. KOM får anta delegerade akter för särskilda kriterier	Utredning pågår. Se kolumnen innan om en skyldighet som kan uppstå om att anta nationella certifieringsordningar för eID (med säkerhetskrav beslutade av KOM).	Cybersäkerhetsakten har redan kriterier för CAB:ar men här ges alltså KOM möjligheten att besluta om fler kriterier.

		synnerhet uppfylla krav vad gäller tillitsnivån ”hög”, i synnerhet när den tillämpas på kraven för styrkande och kontroll av identitet, och förvaltning och autentisering av medel för elektronisk identifiering,	offentliga eller privata organ som utses av medlemsstaterna.		som skall uppfyllas av CSA-CAB:ar.		
DORA	Säkerhet i nätverks- och informationssystem som stöder finansiella entiteters affärsprocesser. 1. […] förordning tillämplig på följande entiteter: a) Kreditinstitut. b) Betalningsinstitut, inbegripet sådana betalningsinstitut som är undantagna enligt direktiv (EU) 2015/2366. c) Leverantörer av kontoinformationstjänster. d) Institut för elektroniska	**a)** Krav som är tillämpliga på finansiella entiteter i fråga om **i)** riskhantering inom informations- och kommunikationsteknik (IKT) **ii)** rapportering av allvarliga IKT-relaterade incidenter och underrättande om, på frivillig grund, betydande cyberhot till de behöriga myndigheterna, **iii)** rapportering av allvarliga betalningsrelaterade operativa	Åtminstone Finansinspektionen. Enligt utredningsdirektiv till NIS2/CER-utredningen skall där lagstiftningarna överlappar de tillsynsmyndigheter som har ansvar för DORA även ha ansvaret för CER-tillsynen.	För att genomföra tillsynsverksamheten får den ledande tillsynsmyndigheten ta hänsyn till relevanta tredjepartscertifieringar och interna eller externa IKT-revisionsrapporter som den kritiska tredjepartsleverantören av IKT-tjänster har gjort tillgängliga. Enligt DORA-förordningen ska de behöriga myndigheterna säkerställa efterlevnaden av förordningen i enlighet med de befogenheter som	EU-kommissionenges befogenhet att komplettera denna förordning genom att anta tekniska standarder för tillsyn. Motsvarande gäller för penetrationstestning och penetrationstestare inom området.	De europeiska tillsynsmyndigheterna ska, genom den gemensamma kommittén och i samråd med Europeiska unionens cybersäkerhetsbyrå (Enisa), utarbeta gemensamma förslag till tekniska standarder för tillsyn. Motsvarande gäller för penetrationsteststning och	Referenser till cybersäkerhetsakten avser främst vissa definitioner. Men det finns alltså en allmän referens till tredjepartscertifieringar, vilket det är fråga om i cybersäkerhetsakten på assuransnivåerna ”betydande” och ”hög”. Och CSA-ordningarna kommer ju direkt eller indirekt täcka väldigt mycket

	pengar, inbegripet sådana institut för elektroniska pengar som är undantagna enligt direktiv 2009/110/EG. e) Värdepappersföretag. f) Leverantörer av kryptotillgångstjänster, auktoriserade enligt en Europaparlamentets och rådets förordning om marknader för kryptotillgångar och om ändring av förordningarna (EU) nr 1093/2010 och (EU) nr 1095/2010 och direktiven 2013/36/EU och (EU) 2019/1937 (förordningen om kryptotillgångar) och emittenter av tillgångsanknutna token. g) Värdepapperscentraler. h) Centrala motparter. i) Handelsplatser. j) Transaktionsregist	incidenter eller säkerhetsincidenter till de behöriga myndigheterna av de finansiella entiteter som avses i artikel 2.1 a–d, **iv)** testning av digital operativ motståndskraft, **v)** utbyte av information och underrättelser i samband med cyberhot och cybersårbarheter, **vi)** åtgärder för en sund hantering av tredjepartsrelaterad IKT-risk. DORA är *lex specialis* i förhållande till cyberkrav i NIS2.		myndigheten tilldelats i de EU-rättsakter som anger behörig myndighet för de finansiella entiteterna (artikel 46). I svensk rätt regleras Finansinspektionens tillsyns- och utredningsbefogenheter i finansiella entiteters rörelselagstiftning och lagar som kompletterar olika EU-förordningar på finansmarknadsområdet. Enligt DORA-förordningen ska de behöriga myndigheterna även ha alla tillsyns-, utrednings- och sanktionsbefogenheter som krävs för att de ska kunna fullgöra sina skyldigheter enligt förordningen. I förordningen anges uttryckligen de utredningsbefogenheter som den behöriga myndigheten		penetrationstestare inom området.	som även ”finansiella entiteter” kommer använda (”IKT-produkter”, ”CRA-produkter, moln, 5G, AI, förvaltade säkerhetstjänster, etc.).

	er. k) Förvaltare av alternativa investeringsfonder. l) Förvaltningsbolag. m) Leverantörer av datarapporteringstjänster. n) Försäkrings- och återförsäkringsföretag. o) Försäkringsförmedlare, återförsäkringsförmedlare och försäkringsförmedlare som bedriver förmedling som sidoverksamhet. p) Tjänstepensionsinstitut. q) Kreditvärderingsinstitut. r) Administratörer av kritiska referensvärden. s) Leverantörer av gräsrotsfinansieringstjänster. t) Värdepapperiseringsregister. u) Tredjepartsleverantörer av IKT-tjänster			som minst ska ha (artikel 50.2).			

	DORA är *lex specialis* i förhållande till organisationer inom den finansiella sektorn och NIS2, och i viss mån till CER.						
Cyber Solidarity Act, Se detaljer nedan rörande CSA+	För att stödja inrättandet av EU-cybersäkerhetsreserven skulle kommissionen kunna överväga att begära att Enisa utarbetar ett förslag till certifieringssystem för sökande i enlighet med förordning (EU) 2019/881 för **förvaltade säkerhetstjänster** på de områden som omfattas av cyberkrismekanismen.			När ett EU-certifieringssystem för hanterade säkerhetstjänster enligt cybersäkerhetsakten införts SKA leverantören vara certifierad i enlighet med det systemet.			
CSA+ (Förhandl. klar)	(Tillhandahållare av) förvaltade/hanterade säkerhetstjänster enligt KOM:s förslag:	En europeisk ordning för cybersäkerhetscertifiering för hanterade säkerhetstjänster ska vara utformat för att, i tillämpliga fall, uppnå	Samma som övriga CSA-ordningar: FMV/ICC (tillsynsmyndighet, inklusive bemyndigande (som eventuellt kan bli fallet	Innebär en utvidgning av cybersäkerhetsakten till förvaltade/hanterade säkerhetstjänster.	Enligt nuvarande CSA kan KOM be Enisa om förslag till CSA-ordning. Baserat på det presenterar KOM ett förslag till ordning (genomförandeföror	Förmodligen i enlighet med nu gällande nationella CSA-genomförande: Lag och förordning på	Under förhandlingen Av CSA+ gång har definitionen av ”förvaltade säkerhetstjänster” ändrats och ligger nu nära

	Tjänst som består i att utföra, eller tillhandahålla stöd för, verksamhet som rör hantering av cybersäkerhetsrisker, inbegripet incidenthantering, penetrationstester, säkerhetsrevisioner och konsulttjänster	åtminstone följande säkerhetsmålsättningar: a) Att säkerställa att de hanterade säkerhetstjänsterna tillhandahålls med den kompetens, sakkunskap och erfarenhet som krävs, inbegripet att den personal som ansvarar för att tillhandahålla dessa tjänster har en mycket hög nivå av teknisk kunskap och kompetens på det specifika området, tillräcklig och lämplig erfarenhet och största möjliga yrkesintegritet. b) Att säkerställa att leverantören har lämpliga interna förfaranden för att säkerställa att de hanterade säkerhetstjänsterna alltid tillhandahålls med en mycket hög nivå av kvalitet.	utöver SWEDAC-ackreditering) av certifieringsorgan. Förmodligen i enlighet med dagens nationella CSA-genomförande: FMV stödjer Fö i förhandlingarna. Vem som skall utföra certifiering är ett senare beslut.		dning) som förhandlas med MS i kommitté-förfarande. FMV/ICC deltar i framtagandet av Enisas förslag och stöttar sedan Fö i kommitté-förhandlingen.	området. Ingen diskussion ännu om utvidgningen av cybersäkerhet sakten triggar uppdatering av lag/förordning. När en CSA-ordning antas måste nationella certifieringsordningar med samma tillämpningsområde upphöra.	motsvarande begrepp i NIS2-direktivet.

		c) Att skydda data som är föremål för åtkomst, behandling, lagring eller överföring i samband med tillhandahållandet av hanterade säkerhetstjänster mot åtkomst, lagring, utlämnande, förstöring eller annan behandling, som sker oavsiktligt eller otillåtet, eller förlust eller ändring eller brist på tillgänglighet. d) Att säkerställa att tillgängligheten och tillgången avseende data, tjänster och funktioner återställs i rätt tid vid en fysisk eller teknisk incident. e) Att säkerställa att behöriga personer, program eller maskiner kan få åtkomst endast till de data, tjänster eller funktioner					

		som omfattas av deras åtkomsträttigheter. f) Att registrera och möjliggöra bedömning av vilka data, tjänster eller funktioner som någon haft åtkomst till, som använts eller på andra sätt behandlats, vid vilken tidpunkt och av vem. g) Att säkerställa att de IKT-produkter, IKT-tjänster och IKT-processer [och hårdvara] som används vid tillhandahållandet av de hanterade säkerhetstjänsterna är säkra i sitt grundutförande och är säkra genom sin konstruktion, inte innehåller några kända sårbarheter och inbegriper de senaste säkerhetsuppdateringarna.”					

European Cybersecurity Competence Centre	Kompetenscentrumet. Främja cybersäkerhetsresiliens, anammande av bästa praxis för cybersäkerhet, principen om inbyggd säkerhet och **säkerhetscertifiering** av digitala produkter och tjänster, på ett sätt som kompletterar andra offentliga enheters insatser.			Kompetenscentrumet och nätverket bör också stödja standardiseringen och ibruktagandet av cybersäkerhetsprodukter, cybersäkerhetstjänster och cybersäkerhetsprodukter och samtidigt, när så är möjligt, **främja** genomförandet av den europeiska ramen för cybersäkerhetscertifiering, inrättad genom förordning (EU) 2019/881.			
Dataförvaltnings-förordningen (Antagen)	Deltagare i dataområden som erbjuder data eller datatjänster till andra deltagare ska uppfylla väsentliga krav för att underlätta interoperabiliteten mellan data, datadelningsmekanismer och datadelningstjänster samt mellan gemensamma europeiska dataområden.	För att förhindra olaglig statlig åtkomst till icke-personuppgifter av myndigheter i tredjeländer bör leverantörer av databehandlingstjänster som omfattas av denna förordning, däribland molntjänster och edgetjänster, vidta alla rimliga åtgärder för att förhindra åtkomst till system där		För att förhindra olaglig statlig åtkomst till icke-personuppgifter av myndigheter i tredjeländer bör leverantörer av databehandlingstjänster som omfattas av denna förordning, däribland molntjänster och edgetjänster, vidta alla rimliga åtgärder för att förhindra	EU-kommissionen ges befogenhet att anta delegerade akter som ytterligare specificerar de väsentliga kraven rörande interoperabilitet.		CSA-ordningarnas certifikat kan eventuellt utgöra sådana ”certifieringssystem för säkerhetsförsäkran”. [Interoperabilitet är en fråga om cybersäkerhet eftersom bristande interoperabilitet påverkar tillgänglighet

		icke-personuppgifter lagras, inbegripet, när så är lämpligt, genom kryptering av data, frekventa revisioner, verifierad anslutning till relevanta certifieringssystem för säkerhetsförsäkran och ändring av företagspolicyer. Deltagare i dataområden som erbjuder data eller datatjänster till andra deltagare ska uppfylla följande väsentliga krav för att underlätta interoperabiliteten mellan data, datadelningsmekanismer och datadelningstjänster samt mellan gemensamma europeiska dataområden.		åtkomst till system där icke-personuppgifter lagras, inbegripet, när så är lämpligt, genom kryptering av data, frekventa revisioner, verifierad anslutning till relevanta certifieringssystem för säkerhetsförsäkran och ändring av företagspolicyer.			till information.]
Färdskrivar-förordningen (Antagen)	Färdskrivare	Typgodkännande krävs.	FMV/CSEC är certifieringsorgan för färdskrivare.	Säkerhetscertifikat bör utfärdas av ett certifieringsorgan som	CSA-ordningen för EUCC (IKT-produkter		Om KOM menar att EUCC gör

			Transportstyrelsen är behörig myndighet och ska i övrigt fullgöra de uppgifter som ankommer på Sverige i fråga om typgodkännande av färdskrivarkort. Swedac är behörig myndighet för ackrediteringar rörande färdskrivare.	erkänts av förvaltningskommittén inom ramen för det avtal om ömsesidigt erkännande av certifikat för evaluering av it-säkerhet (Mutual Recognition Agreement of Information Technology Security Evaluation Certificates) som ingåtts av gruppen av höga tjänstemän på informationssäkerhetsområdet.	evalueras/certifieras mot Common Criteria) är färdigförhandlad och täcker färdskrivare. Trots att EUCC är klar är det omdiskuterat om/hur detta kan ersätta nuvarande system med ömsesidigt godkännande inom SOG-IS (gruppen av höga tjänstemän på informationssäkerhetsområdet).		SOG-IS-certifiering olaglig där tillämpningsområdena överlappar borde de ganska snart göra en översyn av EU-reglerna om färdskrivare… inte känt om detta arbete påbörjats.
Maskin-förordningen (Antagen)	I denna förordning fastställs hälso- och säkerhetskrav för konstruktion och tillverkning av maskiner, relaterade produkter och delvis fullbordade maskiner för att möjliggöra tillhandahållande på marknaden eller ibruktagande av dem, samtidigt som en hög nivå säkerställs i fråga om skydd av	Denna förordning är [med vissa specificerade undantag] tillämplig på Maskiner och följande relaterade produkter: a) Utbytbar utrustning. b) Säkerhetskomponenter. c) Lyftredskap. d) Kedjor, kättingar, linor och vävband. e) Avtagbara mekaniska kraftöverföringsanordningar. Denna	Arbetsmiljöverket var marknadskontroll myndighet för maskindirektivet och kan förmodligen förväntas bli det även rörande den nya förordningen som ersätter direktivet.	Maskiner och relaterade produkter som har certifierats eller för vilka en försäkran om överensstämmelse har utfärdats enligt en CSA-ordning ska förutsättas överensstämma med de grundläggande hälso- och säkerhetskraven i förordningen i den mån dessa krav omfattas av cybersäkerhetscertifikatet eller försäkran	EU-kommissionen ges befogenhet att anta delegerade akter för vissa saker men inte rörande den kategori av produkter där man refererar till CSA-certifiering.		

	människors, särskilt konsumenters och yrkesmässiga användares, hälsa och säkerhet […]	förordning gäller även delvis fullbordade maskiner.		om överensstämmelse eller delar av dem. Genom att upprätta EU-försäkran om överensstämmelse tar tillverkaren ansvar för att maskinen eller den relaterade produkten uppfyller kraven i denna förordning.			
Radioutrustnings direktivet 2014/53/EU (RED)	Produkter med radiokomponenter	Det ställs i RED många krav på radioutrustningen, varav en del handlar om att den, grovt förenklat, ska fungera som kommunikationsutrustning, vilket vi i denna rapport därmed menar är en typ av cybersäkerhetskrav.	Post- och telestyrelsen är marknadskontrollmyndighet och utövar marknadskontroll enligt RED (förordning (EU) 2019/1020 över att produkter överensstämmer med kraven i Europaparlamentets och rådets direktiv 2014/53/EU av den 16 april 2014 om harmonisering av medlemsstaternas lagstiftning om tillhandahållande på marknaden av radioutrustning och om upphävande av direktiv				

			1999/5/EG, med undantag för produkternas egenskaper när det gäller elsäkerhet.				
Network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows Delegerad förordning - C(2024)1383	Regler för elförsörjningen i EU (”nätföreskrifter”) för att åtgärda it-säkerhetsaspekter avseende elflöden över gränserna. Det ska bidra till att elsystemet i EU blir mer resilient och säkert.	It is based on the powers that the European Parliament and the Council conferred on the Commission in the Regulation (EU) 2019/9434 (Electricity Regulation) to develop sector-specific rules (‘network code’) that address the cybersecurity aspects of cross-border electricity flows. This includes rules on common minimum requirements, planning, monitoring, reporting and crisis management	Svensk myndighet inte explicit utsedd men ansvarig myndighet kan antas bli/vara Energimyndigheten eftersom reglerna är ett komplement till NIS2-direktivet. Art. 35.4 Berörda EU-samarbetsorgan (där Svenska myndigheter kan delta)”shall ensure that the sets of cybersecurity procurement recommendations: […] (b) are compatible with and take in account the most recent available European cybersecurity certification schemes relevant	Article 33.4: The advanced cybersecurity controls in the **supply chain** shall include controls for critical-impact entities to verify, during procurement, that ICT products, ICT services and ICT processes that will be used as critical-impact assets satisfy the cybersecurity specifications. The ICT product, ICT service or ICT process shall be verified either through a European cybersecurity certification scheme referred to in Article 31 or through verification activities selected and organized by the entity. Article 36 Guidance on use of European	[T]he general rules on the security of network and information systems laid down in Directive (EU) 2022/2555 (NIS 2 Directive) are complemented by [this] network code.		

			to the ICT product, ICT service, or ICT process.	cybersecurity certification schemes for procurement of ICT products, ICT services and ICT processes 1. The non-binding cybersecurity procurement recommendations developed pursuant to Article 35 may include sector-specific guidance on the use of European cybersecurity certification schemes, whenever a suitable scheme is available for a type of ICT product, ICT service or ICT process used by critical-impact entities, without prejudice to the framework for the establishment of European cybersecurity certification schemes pursuant to Article 46 of Regulation (EU) 2019/881. 2. The TSOs, with the assistance of the ENTSO for Electricity, and in			

				cooperation with the EU DSO entity shall closely cooperate with ENISA in providing the sector specific guidance included in non-binding cybersecurity procurement recommendations pursuant to paragraph 1.			

Bilaga 4 – Tillsynsmyndigheter och deras tillsynsområden

Enligt säkerhetsskyddsförordningen (2021:955) är följande myndigheter tillsynsmyndigheter och för angivna tillsynsområden:

Säkerhetspolisen	• Domstolarna som inte hör till Försvarsdepartementet • Domstolsverket • Domarnämnden • Åklagarmyndigheten • Polismyndigheten • Ekobrottsmyndigheten • Kriminalvården • Kustbevakningen • Tullverket • Skatteverket • Försäkringskassan • Pensionsmyndigheten • Statens servicecenter • Riksgäldskontoret • Riksarkivet • Finansinspektionen • Statens fastighetsverk • Inspektionen för strategiska produkter • Myndigheten för samhällsskydd och beredskap • Lantmäteriet • Post- och telestyrelsen • Transport-styrelsen • Affärsverket svenska kraftnät • Strålsäkerhetsmyndigheten • Statens energimyndighet • Livsmedelsverket • Luftfartsverket • Sjöfartsverket • Trafikverket • Folkhälsomyndigheten • Socialstyrelsen • Statens jordbruksverk • Statens veterinärmedicinska anstalt • E-hälsomyndigheten • Läkemedelsverket • Migrationsverket

	• Länsstyrelserna • Säkerhets- och integritetsskyddsnämnden
Försvarsmakten	• Fortifikationsverket • Försvarshögskolan • Övriga myndigheter som hör till Försvarsdepartementet
Affärsverket Svenska Kraftnät	• Enskilda verksamhetsutövare inom områdena elförsörjning och dammanläggningar, med undantag för kärnteknisk verksamhet
Transportstyrelsen	• Enskilda verksamhetsutövare inom områdena: • Vägtrafik • Sjöfart • Spårbunden trafik • Civil luftfart • Flygtrafiktjänster för civil luftfart • Flygtrafikledningstjänst för militär luftfart
Post- och telestyrelsen	• Enskilda verksamhetsutövare inom områdena elektronisk kommunikation och posttjänst
Försvarets materielverk	• Enskilda verksamhetsutövare inom området försvarsmateriel
Finansinspektionen	• Enskilda verksamhetsutövare inom området finansiella företag samt för motsvarande utländska företag som är etablerade i Sverige
Statens energimyndighet	• Enskilda verksamhetsutövare inom områdena fjärrvärme-, naturgas-, olje- och drivmedelsförsörjning
Strålsäkerhetsmyndigheten	• Enskilda verksamhetsutövare inom området kärnteknisk verksamhet
Länsstyrelsen i Stockholms län	• Kommuner och regioner som hör till Stockholms, Uppsala, Södermanlands, Västmanlands, Värmlands, Gotlands, Örebro, Dalarnas eller Gävleborgs län • Statliga myndigheter, utom Säkerhetspolisen och Justitiekanslern, och enskilda verksamhetsutövare som har sitt säte i något av dessa län, om de inte hör till någon annan tillsynsmyndighets tillsynsområde
Länsstyrelsen i Skåne län	• Kommuner och regioner som hör till Kronobergs, Blekinge, Kalmar eller Skåne län • Statliga myndigheter och enskilda verksamhetsutövare som har sitt säte i något av dessa län, om de inte hör till någon annan tillsynsmyndighets tillsynsområde
Länsstyrelsen i Västra Götalands län	• Kommuner och regioner som hör till Hallands, Jönköpings, Västra Götalands eller Östergötlands län

	• Statliga myndigheter och enskilda verksamhetsutövare som har sitt säte i något av dessa län, om de inte hör till någon annan tillsynsmyndighets tillsynsområde
Länsstyrelsen i Norrbottens län	• Kommuner och regioner som hör till Västernorrlands, Jämtlands, Västerbottens eller Norrbottens län • Statliga myndigheter och enskilda verksamhetsutövare som har sitt säte i något av dessa län, om de inte hör till någon annan tillsynsmyndighets tillsynsområde

Bilaga 5 – Exempel på standardiseringsorgan och de facto-standardiseringsorgan inom cyberområdet

Inom området för it-teknik och cybersäkerhet finns det flera ledande standardiseringsorgan (formella enligt WTO-TBT eller de facto) som spelar en avgörande roll för att fastställa globalt erkända standarder och bästa praxis. Dessa organisationer bidrar till att säkerställa säkerheten, pålitligheten och interoperabiliteten för informationssystem och nätverk.

Svenska standardiseringsorgan (enligt EU:S 1025/2012 och WTO-TBT):

SIS (Swedish Institute for Standards) - SIS är en ideell förening och utsedd att vara Sveriges representant i CEN och ISO. Den tekniska kommittén TK318

SEK Svensk Elstandard – SEK ansvarar för standardisering inom det elektrotekniska området i Sverige.

ITS (Informationsteknik Standardiseringen) – är främst engagerade i telekommunikationsstandarder.

Standardsorgan Etablerade inom EU (enligt EU:S 1025/2012 och WTO-TBT):

CEN (European Committee for Standardization) – CEN är en av de tre europeiskt erkända standardiseringsorgan och utvecklar frivilliga standarder som syftar till att stödja harmonisering inom den europeiska marknaden, vilket underlättar handel mellan länderna. Deras arbete täcker ett brett spektrum av sektorer förutom elektroteknik och telekommunikation, som hanteras av deras systerorganisationer CENELEC och ETSI.

CENELEC (European Committee for Electrotechnical Standardization) - CENELEC är ansvarigt för standardisering inom det elektrotekniska området i Europa. De arbetar för att harmonisera elektrotekniska standarder på den europeiska marknaden, vilket underlättar handel och bidrar till att säkerställa säkerhet och kompatibilitet för elektriska och elektroniska produkter och tjänster.

ETSI (European Telecommunications Standards Institute) – ETSI är en oberoende, ideell organisation som utvecklar standarder inom informations- och kommunikationsteknik (IKT), inklusive fasta, mobil, radio, konvergerade, broadcast och internet-teknologier i Europa. ETSI är känt för sin roll i utvecklingen av globalt viktiga standarder som GSM, 3G, 4G och 5G.

Internationella standardiseringsorgan (enligt EU:S 1025/2012 och WTO-TBT):

ISO (International Organization for Standardization) – ISO utvecklar och publicerar internationella standarder för en bred uppsättning industriområden, inklusive it-säkerhet och informationssäkerhetsledningssystem (t.ex., ISO/IEC 27000-serien).

IEC (International Electrotechnical Commission) – I samarbete med ISO, arbetar IEC med standardisering inom det elektrotekniska fältet, inklusive elektronisk utrustning och system för it och cybersäkerhet.

ITU (International Telecommunication Union) – En FN-organisation som utvecklar tekniska standarder (ITU-T rekommendationer) för telekommunikationsnät och tjänster, inklusive aspekter av cybersäkerhet och dataskydd.

IEEE (Institute of Electrical and Electronics Engineers) – IEEE är en av de ledande organisationerna för utveckling av standarder för elektronik-, el- och it-industrin, inklusive nätverkssäkerhet och dataskydd.

Andra de facto-standardiseringsorgan:

IETF (Internet Engineering Task Force) - IETF utvecklar och främjar frivilliga internet-standarder, speciellt inom områdena Internetprotokoll, arkitektur och säkerhet.

NIST (National Institute of Standards and Technology) – En amerikansk federal myndighet som utvecklar och främjar teknik, mätstandarder och cybersäkerhetsstandarder och riktlinjer för att skydda informationssystem.

ETSI (European Telecommunications Standards Institute) – ETSI producerar globalt tillämpliga standarder för informations- och kommunikationsteknik (IKT), inklusive fasta, mobil, radio, konvergerade, broadcast och internetteknologier.

OWASP (Open Web Application Security Project) – En ideell organisation som arbetar för att förbättra programvarusäkerheten genom att utveckla kostnadsfria och öppet tillgängliga artiklar, metoder, dokumentation, verktyg och tekniker.

SANS Institute – Även om det primärt är känt för utbildning och certifiering, utvecklar SANS Institute även säkerhetspolicyer och riktlinjer som är vida respekterade inom it-säkerhetsgemenskapen.

Cloud Security Alliance (CSA) – CSA främjar bästa praxis för att säkerställa en säker molnutveckling och drift, och publicerar forskning och standarder för att hjälpa till att säkra molntjänster.

ANSI (American National Standards Institute) – Koordinerar USA:s standarder och riktlinjer, inklusive de för it och cybersäkerhet.

W3C (World Wide Web Consortium) – Utvecklar webbstandarder för att säkerställa webbens långsiktiga tillväxt.

ISACA (Information Systems Audit and Control Association) – Erbjuder it-professionella kunskap och bästa praxis för riskbedömning och styrning.

(ISC)² (International Information System Security Certification Consortium) – Specialiserar sig på utbildning och certifieringar för personer som jobbar med cybersäkerhet.

GSMA (Global System for Mobile Communications Association) – Representerar intressena för mobiloperatörer världen över och utvecklar standarder för mobila ekosystem.

CCRA, eller "Common Criteria Recognition Arrangement", är ett internationellt avtal och samarbete mellan länder som erkänner och accepterar resultatet av varandras säkerhetsevalueringar av it-produkter och system. Detta avtal bygger på "Common Criteria for Information Technology Security Evaluation" (CC), en internationell standard (ISO/IEC 15408) för bedömning av säkerheten och tillförlitligheten i it-produkter och system.

SOGIS-MRA, är ett ömsesidigt erkännandeavtal som omfattar europeiska länder. Det fokuserar på säkerhetsevaluering och certifiering av it-produkter och skyddssystem enligt den gemensamma kriteriestandarden (Common Criteria). Målet med SOGIS-MRA är att främja ömsesidigt erkännande av säkerhetscertifieringar mellan deltagande länder.

MITRE är en amerikansk ideell organisation som driver forsknings- och utvecklingscentrum finansierade av den federala regeringen. MITRE är kanske mest känt för sitt arbete med att utveckla och underhålla CVE (Common Vulnerabilities and Exposures) -databasen, en offentligt tillgänglig katalog över säkerhetsbrister och sårbarheter i programvara och hårdvara, samt för ramverket MITRE ATT&CK®, en globalt tillgänglig kunskapsbas av motståndares taktiker och tekniker baserat på verkliga observationer.

CIS (Center for Internet Security) – Fokuserar på att förbättra cybersäkerhetsposturen för offentliga och privata sektorentiteter.

FIRST (Forum of Incident Response and Security Teams) – Främjar samarbete mellan incidentrespons- och säkerhetsteam.

PCI SSC (Payment Card Industry Security Standards Council) – Utvecklar och främjar säkerhetsstandarder för kreditkortsindustrin.

3GPP (3rd Generation Partnership Project) – Utvecklar protokoll för mobiltelekommunikation.

OASIS (Organization for the Advancement of Structured Information Standards) Ett globalt konsortium som arbetar med utvecklingen och antagandet av öppna, offentliga sektor- och branschspecifika e-standarder.

FIDO Alliance (Fast IDentity Online) - Arbetar för att minska världens överberoende av lösenord genom att standardisera stark autentisering.

ENISA (European Union Agency for Cybersecurity) – Stärker cybersäkerheten inom EU och samarbetar med medlemsländerna samt privata sektorn.

APWG (Anti-Phishing Working Group) – Fokuserar på globalt svar på cyberbrottslighet riktat mot konsumenter.

Internet Society (ISOC) – Stöder och främjar utvecklingen av internet som en global teknisk infrastruktur.

Trusted Computing Group (TCG) – Utvecklar och främjar öppna standarder och specifikationer för säker datalagring, –överföring och -användning.

ICANN (Internet Corporation for Assigned Names and Numbers) – Samordnar tilldelningen av unika internetidentifierare.

CENELEC (European Committee for Electrotechnical Standardization) – Ansvarar för standardisering inom det elektrotekniska området i Europa.

ISO/IEC JTC 1 (Joint Technical Committee 1) – Ett samarbete mellan ISO och IEC som fokuserar på standarder för informationsteknologi.

CEPT (European Conference of Postal and Telecommunications Administrations) – Främjar samarbete mellan europeiska post- och telekommunikationsorganisationer, inklusive cybersäkerhetsfrågor.

Bilaga 6 – EUCC: Standardiseringsorgan och standarder

Typ	Förklaring
Global	Tar fram standarder som är tänkta att fungera globalt via nationellt deltagande (SDO där man beslutat landsvis)
Regional	Tar fram standarder som är tänkta att fungera regionalt via nationellt deltagande (SDO där man beslutat landsvis)
Nationell	Tar fram standarder som är tänkta att fungera för en nation (SDO inom det landets mandat)
Expertgrupp	Tar fram standarder som är tänkta att fungera inom ett visst ”teknik” område utan koppling till geografi, så kallade ”de facto”

Typ av Organisation	Standardiserings organ/De Facto	Arbetsgrupper (WG) /Tekniska kommittéer (TC)	Vad gör de?	Varför är de relevanta?	Exempel på standarder, certifieringsordningar, dokument och andra publikationer	Deltagande från FMV
Expertgrupp	CCRA – iTC (de facto)	1. Application Software 2. Biometrics Security 3. Database management systems	iTC (international Technical Community) skriver cPP:er (Collaborative Protection Profiles) vilka är säkerhetskravställn	iTC:erna skriver cPP:er.	Protection Profiles och Collaborative Protection Profiles: PP-Module for Client Virtualization Version 1.1 PP-Module for File Encryption Version 1.0	Följs och stöds av FMV/CSEC

		4. Dedicated Security Component 5. Full Disk Encryption 6. Hardcopy Devices 7. Network Fundamentals and Firewalls 8. USB portable storage devices	ing för en viss typ av produkt.		PP-Module for File Encryption Enterprise Management Version 1.0 Protection Profile for General Purpose Operating Systems Version 4.3 Network Device cPP Hardcopy Device cPP Firewall PP-Configuration	
Expertgrupp	CCRA (de facto)	CCDB (Common Criteria Development Board) ES CCMB (Common Criteria Maintenance board)	Gemensam överenskommelse mellan medlemsländer för att öka säkerheten i teknologiska informations- och kommunikationsmedel genom säkra funktionella krav och assuranskrav. CCDB leder arbetet CCMB utför arbetet	Ger ut supporting documents som underlag för harmoniserade tolkningar inom CCRA.	CCRA versionen av CC och CEM Supporting documents: • CCDB-2015-01-004 Full Drive Encryption: Encryption Engine • Rationale for Smart cards and similar devices • CCDB-2007-11-001 Site Certification CCDB-2015-01-001 Evaluation Activities for Network Device cPP	FMV/CSEC är medlemmar och deltar i möten.

Expertgrupp	GlobalPlatform (de facto)		Konsensus-driven standardiseringsorganisation för tekniska standarder.	Utvecklar standarder för SE (Secure Elements) och IoT (Internet of Things)	Standarder: Secure Element Configuration for Authentication Devices v1.0 Protection Profile: Secure Element Protection Profile v1.0	
Expertgrupp	MITRE		Globalt utvecklings- och forskningscentrum som utvecklar tekniker för global cybersäkerhet, utveckling av standarder och relaterade aktiviteter.	Ger ut CVE-katalog, CWE, CVSS m.fl. Dessa listar, kategoriserar och bedömer allvarlighetsgrad hos kända sårbarheter och svagheter för cybersäkerhet inom it-produkter som är viktiga att ha i åtanke vid utveckling, evaluering och certifiering av it-produkter	CVE – Identifierar, definierar och katalogiserar kända cybersäkerhets-sårbarheter. CWE – Ett kategorisystem för sårbarheter och svagheter i både hård- och mjukvara. CVSS – System för att bedöma hur allvarliga säkerhetssårbarheter i datorsystem.	
Expertgrupp	OWASP		En ideell stiftelse som arbetar för att öka säkerheten i programvara.	Erbjuder artiklar, dokument och metoder angående säkerhet i mjukvara, IoT och	OWASP Top Ten: Ett dokument som belyser viktiga säkerhetsrisker inom webbapplikationer där deltagare från hela världen delar med sig av sin expertkunskap. Syftet är att OWASP Top	

				webbapplikationer som är viktiga att ha i åtanke vid utveckling, evaluering, testning och certifiering.	Ten ska kunna användas som en rekommendation för utvecklingen av säkra applikationer och för regelbunden testning av applikationens säkerhet.	
Expertgrupp	SAFECode		En global ideell organisation där tekniska experter och företagsledare tillsammans delar insikter och idéer för att skapa, förbättra och förespråka skalbar och effektiva säkerhetsmjukvaru program. Medlemmar • Microsoft • Siemens • Dell Technologies • Oracle • Security Compass m.fl.	Erbjuder en plattform för utbyte av idéer och insikter i syfte att andra ska dra lärdom av andras arbete inom utvecklings-området. Tar fram och publicerar dokument inom cybersäkerhets-certifiering och mjukvarusäkerhet samt erbjuder gratis träning inom mjukvarusäkerhet.	Dokument: SAFECode Perspective on Cybersecurity Certification Principles for Software Assurance Assessment	

Global	CASCO (SDO)		CASCO är en del av ISO som fokuserar på certifieringsprocessen så att den kan användas globalt. CASCO har flera arbetsgrupper som är öppna för medlemmar i ISO och IEC.	Hur man certifierar så att det gäller globalt är viktigt om man vill agera med certifikat på en global marknad.	ISO/IEC 17025 General requirements for the competence of testing and calibration laboratories ISO/IEC 17065 Conformity assessment – Requirements for bodies certifying products, processes and services	
Global	IEEE (SDO)	Industry Connections Security group • Anti-Malware Support Services Working Group • Encrypted Traffic Inspection Working Group • Malware Metadata Exchange Format Working Group	Internationell standardiseringsorganisation som utvecklar och ger ut standarder inom teknikområdet.		Standarder: IEEE 1686-2022 Standard for Intelligent Electronic Devices Cybersecurity IEEE 1363-2000 Standard Specifications for Public-Key Cryptography IEEE 2600-2008 Standard for Information Technology: Hardcopy Device and System Security IEEE 2600.1-2009 Standard for Protection Profile in Operational Environment A IEEE 802.11 Standards for connections in wireless networking	

		• Malware Working Group				
Global	IETF (de facto)		Standardiseringsorgan som utvecklar specifikationer för nya tekniska standarder för Internet.	Snabbutvecklar standarder av olika slag till internet och kryptografi. Hanterar viktiga standarder för till exempel TCP, TLS, SSH och IPsec	Standarder: RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile – Hantering av publika kryptonycklars certifikat RFC 793 Transmission Control Protocol – Dataöverföringsprotokoll som används för huvuddelen av all kommunikation över Internet. RFC 8446 The Transport Layer Security (TLS) Protocol Version 1.3 – Säker kommunikation mellan datorsystem RFC 4251 The Secure Shell (SSH) Protocol Architecture – Protokoll för säker anslutning över internet eller lokalt nätverk RFC 4301 Security Architecture for the Internet Protocol (IPsec) – Datasäkerhetsteknologier för virtuella private nätverk	
Global	ISO/IEC (SDO)	ISO/IEC JTC 1 Information	ISO är en privat internationell standardiseringsorganisation som	Tar fram standarder för bl.a. evaluering,	Standarder:	Bevakas av FMV/CSEC genom SIS

		Technology – Subcommittes: • ISO/IEC JTC 1/SC6 Telecommunications and information exchange between systems • ISO/IEC JTC 1/SC7 Software and systems engineering • ISO/IEC JTC 1/SC27 Information security, cybersecurity and privacy protection ○ WG2 Cryptography and Security Mechanisms	utvecklar och ger ut internationella standarder. IEC utvecklar och ger ut internationella standarder inom elektroteknik och elektronik. De båda är globala organisationer som arbetar inom ISO i JTC 1. (Joint Technical Committee.)	testning och krav för certifieringsorgan.	ISO/IEC 15408 Information Security, cybersecurity and privacy protection – Evaluation criteria for IT security ISO/IEC 17025 General requirements for the competence of testing and calibration laboratories ISO/IEC 17065 Conformity assessment – Requirements for bodies certifying products, processes and services	Bevakas av FMV/ICC

		○ WG3 Security evaluation, testing and specification				
Global	ITU (SDO)		FN:s organ för information och kommunikations-teknologi. Utvecklar standarder för att nätverk och teknologi ska fungera tillsammans och erbjuder en stor plattform för informationsutbyte mellan medlemmar.	X.509-certifikat används allmänt för identifiering till exempel i webbtrafik. X501-kataloger används i lightversionen LDAP.	Standarder: X.509 Certifikat X.501 Katalog	
Global	TCG (de facto)		Utvecklar, definierar och promotar öppna, neutrala och globala standarder	Utvecklar standarder för TPM vilken handlar om säkra kryptoprocesser genom	Standarder: Trusted Platform Module Library Specification 2.0 – Internationell standard för säkra kryptoprocesser	

			inom teknikindustrin.	hårdvarubaserat skydd.		
Nationell	BSI (de facto)		Tysklands nationella organ för cybersäkerhet	Skriver egna regelverk och tolkningar som används av andra länder.	Standarder: AIS 31 Functionality Classes and Evaluation methodology for physical random number generators AIS 42 Guidelines for Developer Documentation according to Common Criteria AIS 46 Minimum Requirements for Evaluating Side-Channel Attack Resistance of Elliptic Curve Implementations	Bevakas av FMV/CSEC genom SOGIS och CCRA.
Nationell	NIST (de facto)		Ett av USA:s nationella standardiseringsorgan.	Utvecklar standarder för It-säkerhet, särskilt kryptografi. Är ett bibliotek som ofta används.	Standarder: NIST SP-800-38A Recommendation for Block Cipher Modes of Operation: Methods and Techniques FIPS 197 Advanced Encryption Standard	Bevakas av FMV/CSEC
Nationell	SIS (SDO)	TK 318 • AG11 Ledningssystem för informationssäkerhet	En svensk ideell förening som arbetar tillsammans med ISO och CEN för att ta fram internationella	Arbetar för att ta fram internationellt harmoniserade standarder inom ISO och CEN standarder som vid antagande blir även svenska	Standarder: SS-ISO/IEC 15408–1:2022 Informationssäkerhet, cybersäkerhet och integritetsskydd - Utvärderingskriterier för It-säkerhet - Del 1: Introduktion och generell modell	FMV/CSEC är medlemmar, får info och är aktiva från och till. FMV/ICC är medlemmar och

		• AG21 Kryptografi • AG31 Kravställning och verifiering	standarder. TK 318 arbetar med att delta i nationellt och internationellt standardiseringsarbete för informationssäkerhet, cybersäkerhet och integritetsskydd. Inom ISO och CEN har varje medlemsland motsvarande.	standarder (SS). För till exempel utvärderingskriterier för IT-säkerhet och säkerhetskrav för kryptomoduler. Men även Certifierings krav och vägledning för certifiering av organisationer inom informations- och cyber säkerhet. Kan om så krävs ta fram och ge ut unika svenska standarder (SS).	SS-EN ISO/IEC 19790:2020 Informationsteknik - Säkerhetstekniker - Säkerhetskrav för kryptomoduler	arbetar aktivt i olika tekniska kommittéer.
Nationell	NIAP		Amerikanskt certifieringsorgan för cybersäkerhet.	Drivande i utveckling av CC, CEM samt certifieringsregelverk inom CCRA.	PP-Module for Client Virtualization Version 1.1 PP-Module for File Encryption Version 1.0 PP-Module for File Encryption Enterprise Management Version 1.0 Protection Profile for General Purpose Operating Systems Version 4.3	

Regional	CEN/CENELEC (SDO)	CEN/CLC/JTC 13 – Cybersecurity and Data protection	Utvecklar och ger ut europeiska standarder och tekniska dokument inom en lång rad av olika områden.	JTC 13 utvecklar standarder för cybersäkerhet och dataskydd.	Standarder: CEN ISO/IEC/TS 27006-2:2022 Requirements for bodies providing audit and certification of information security management systems - Part 2: Privacy information management systems EN ISO/IEC 15408-1:2023 Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 1: Introduction and general model EN ISO/IEC 15408-2:2023 Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 2: Security functional components EN ISO/IEC 15408-3:2023 Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 3: Security assurance components EN ISO/IEC 15408-4:2023 Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 4: Framework for the specification of evaluation methods and activities	Bevakas av FMV/ICC

					EN ISO/IEC 18045:2023 Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Methodology for IT security evaluation	
Regional	ECCG	ECCG EUCC Subgroup ECCG Crypto subgroup	EU:s officiella grupp för cybersäkerhetscertifiering.	Övervakar och styr utvecklingen av certifieringsordningar inom cybersäkerhetsakten.		Deltagande via FMV/CSEC i både huvudgrupp och undergrupper för maintenance och krypto. Bevakas av FMV/ICC
Regional	Enisa		EU:s nätverks- och informationssäkerhetsbyrå. Arbetar för att säkerställa en hög nivå av cybersäkerhet i Europa	Tar fram och ger ut ”State of the Art”-dokument och andra standarder. ”State of the Art” innebär att de innehåller den bästa och senaste informationen inom ett område eller angående en produkt.	Här är en lista över ”State-of-the-art” dokument som ska tillämpas inom EUCC. Om de inte tillämpas ske detta meddelas till EU-kommissionen tillsammans med angivande av orsak. • State-of-the-art document - application of attack potential to hardware devices with security boxes • State-of-the-art document - accreditation of ITSEFs for the EUCC scheme	Deltagande I det direkta standardiseringsarbetet är begränsat till en utsedd grupp av Enisa. Sverige kan påverka via kommenterar från FMV/ICC. FMV/CSEC är mycket aktiva inom Cyber Security-arbetet med daglig kontakt.

					• State-of-the-art document accreditation of ITSEFs for the EUCC scheme • State-of-the-art document - application of attack potential to smartcards and similar devices • State-of-the-art document - certification of "open" smart card products • State-of-the-art document - Composite product evaluation for Smart Cards and similar devices • State-of-the-art document - minimum ITSEF requirements for security evaluations of smart cards and similar devices • State-of-the-art document - Minimum ITSEF requirements for security evaluations of Hardware devices with security boxes (HDWSB) • State-of-the-art document - minimum site security requirements • State-of-the-art document - Security Architecture requirements (ADV_ARC) for smart cards and similar devices	

					extended to Secure Sub Systems in socs • State of the art document - evaluation of ALC documentation & site audits of development and production environments • State of the art document - ALC Re-use Methodology • State of the art document - Re-use of Evaluation Results • State of the art document - performing testing Det finns även ytterligare dokument som är till stöd för underhållet av EUCC, eller som senare kan komma att föreslås bli ”state-of-the-art”-dokument: • Proposed maintenance organisation for the EUCC scheme • EUCC accreditation requirements for CB activities • Guidance on vulnerability handling in certified solutions SOG-IS crypto evaluation scheme agreed cryptographic mechanisms	

Regional	ETSI (SDO)	Partnerships • 3GPP • oneM2M Technical Committees • CYBER – Cybersecurity Technical Committee • ESI – Electronic Signatures and Infrastructures • LI – Lawful Interception technical committee • MTS-SIG – Methods for Testing and Specification Security Special Interest Group • NFV – Network Functions Virtualizations	Utvecklar och ger ut standarder för informations- och kommunikationsteknologi.	Utvecklar standarder och Protection Profiles på teknisk detaljnivå i Europa.	Protection Profiles: ETSI TS 103 732 CYBER; Consumer Mobile Device Protection Profile ETSI TS 102 556 Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Protection Profile	

		• NTECH – Network Technologies • SAGE – Security Algorithms Group of Experts • SAI – Securing Artificial Intelligence • SCP – Smart Card Platform				
Regional	SOGIS	JIWG (Joint Interpretations Working group) • JHAS (JIL Hardware-related Attacks Subgroup) • JEDS (JIWG Embedded Devices Subgroup) • ISCI WG1 (International Smartcard Certification	Överenskommelse mellan medlemsländer inom EU eller EFTA för arbete och utveckling av standarder SOGIS har arbetsgrupper som jobbar direkt under the Maintenance Committee (MC) med rekommendatione	Utveckling av regelverk för certifiering och evaluering, särskilt för smarta kort och security boxes.	Supporting documents: SOGIS Crypto Evaluation Scheme – Agreed cryptographic mechanisms SOGIS Harmonised Cryptographic Evaluation Procedures	FMV/CSEC är medlemmar och deltar i deras möten. Bevakas av FMV/ICC

		Initiative – Working Group 1) SOGIS Crypto WG	r för kryptografi som kan certifieras inom SOGIS.			

Bilaga 7 – EUCS: Standardiseringsorgan och standarder

Typ av Organisation	Standardiserings organ/De Facto	Arbetsgrupper (WG) / Tekniska kommittéer (TC)	Vad gör de?	Varför är de relevanta?	Exempel på standarder, certifieringsordningar, dokument och andra publikationer.	Deltagande från FMV
Expertgrupp	OWASP		En ideell stiftelse som arbetar för att öka säkerheten i programvara.	Erbjuder artiklar, dokument och metoder angående säkerhet i mjukvara, IoT och webbapplikationer som är viktiga att ha i åtanke vid utveckling, evaluering, testning och certifiering.	Dokument: OWASP Cloud-Native Application Security Top 10 – Listar 10 viktiga dokument som tar upp viktiga aspekter att ha i åtanke vid utveckling och användning av Cloud-applikationer.	
Global	IETF (de facto)		Standardiseringsorgan som utvecklar specifikationer för nya tekniska standarder för Internet.	Snabbutvecklar standarder av olika slag till internet och kryptografi. Hanterar viktiga standarder för till exempel TCP, TLS, SSH och IPsec	Standarder: RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile – Hantering av publika kryptonycklars certifikat RFC 793 Transmission Control Protocol – Dataöverföringsprotokoll som används för huvuddelen av all kommunikation över Internet.	

					RFC 8446 The Transport Layer Security (TLS) Protocol Version 1.3 – Säker kommunikation mellan datorsystem RFC 4251 The Secure Shell (SSH) Protocol Architecture – Protokoll för säker anslutning över internet eller lokalt nätverk RFC 4301 Security Architecture for the Internet Protocol (IPsec) – Datasäkerhetsteknologier för virtuella private nätverk	
Global	ISO/IEC (SDO)	ISO/IEC JTC 1 Information Technology – Subcommittees: • ISO/IEC JTC 1/SC 38 Cloud computing and distributed platforms	ISO är en privat internationell standardiseringsorganisation som utvecklar och ger ut internationella standarder. IEC utvecklar och ger ut internationella standarder inom elektroteknik och elektronik.	Tar fram standarder för bl.a. evaluering, testning och krav för certifieringsorgan.	Standarder: ISO/IEC 22123-1:2023 Information technology; Cloud computing – Part 1: Vocabolary ISO/IEC 19944-1:2020 Cloud computing and distributed platforms — Data flow, data categories and data use ISO/IEC TS 23167:2020 Information technology, Cloud computing, Common technologies and techniques	Bevakas av FMV/ICC
Nationell	CIS (de facto)	Center for Internet Security	US baserad organisation som publicerar olika	Ta fram listor och metoder för olika	Standarder:	

			listor mest inriktat på USA men används även internationellt.	säkerhetslösningar samt rapporter.	CIS Critical Security Controls - Prioritized & simplified best practices CIS Hardened Images® -Virtual images hardened to CIS Benchmarks on cloud service provider marketplaces	
Regional	CEN/CENELEC (SDO)	CEN/CLC/JTC 13 – Cybersecurity and Data protection • WG 2 Cybersecurity Management Systems • WG 3 Security Evaluation and Assessment	Utvecklar och ger ut europeiska standarder och tekniska dokument inom en lång rad av olika områden.	JTC 13 utvecklar standarder för cybersäkerhet och dataskydd. WG 2 arbetar utvecklar TS 18026 och WG 3 utvecklar krav för kommande standard för ackreditering av CAB (Conformity Assessment Body) som ska evaluera och certifiera molntjänster.	Standarder: CEN/TS 18026:2024 Three-level approach for a set of cybersecurity requirements for cloud services – Tekniska krav som stödjer de tre assuransnivåerna i CSA.	Bevakas av FMV/ICC
Regional	ETSI (SDO)	Partnerships • 3GPP • oneM2M Technical Committees • CYBER – Cybersecurity	Utvecklar och ger ut standarder för informations- och kommunikationsteknologi.	Utvecklar standarder och Protection Profiles på teknisk detaljnivå i Europa.	ETSI TS 103 458 – Application of Attribute Based Encryption (ABE) for PII and personal data protection on IoT devices, WLAN, cloud and mobile services - High level requirements	

		Technical Committee • ESI – Electronic Signatures and Infrastructures • LI – Lawful Interception technical committee • MTS-SIG – Methods for Testing and Specification Security Special Interest Group • NFV – Network Functions Virtualisation • NTECH – Network Technologies • SAGE – Security Algorithms Group of Experts				

		• SAI – Securing Artificial Intelligence SCP – Smart Card Platform				

Bilaga 8 – EU5G: Standardiseringsorgan och standarder

Nedan beskriver exempel på standardiseringsorganisationer och standarder som är av relevans för certifiering av eUICC inom EU5G. eUICC,Embedded Universal Integrated Circuit Card, är en teknisk lösning (IKT-produkt) där en användare kan ladda ner en eller flera abonnemang från olika operatörer över internet. Jfr. avsnitt 6.16.2.

Typ av Organisation	Standardiserings organ/De Facto	Arbetsgrupper (WG) / Tekniska kommittéer (TC)	Vad gör de?	Varför är de relevanta?	Exempel på standarder, certifieringsordningar, dokument och andra publikationer.	Deltagande från FMV
Expertgrupp	GlobalPlatform (de facto)		Konsensus-driven standardiseringsorganisation för tekniska standarder.	Utvecklar standarder för SE (Secure Elements) och IoT (Internet of Things)	Standarder: Secure Element Configuration for Authentication Devices v1.0 GPC_SPE_174 | Secure Element Protection Profile v1.0	
Expertgrupp	OWASP		En ideell stiftelse som arbetar för att öka säkerheten i programvara.	Erbjuder artiklar, dokument och metoder angående säkerhet i mobil-applikationer som är bra att arbeta utefter vid utveckling och testning av mobil-applikationer.	Dokument: OWASP Mobile Application Security Verification Standard – Definierar en säkerhetsstandard för mobil-applikationer. OWASP Mobile Application Security Testing Guide – Erbjuder en test-guide för tillverkare som täcker processer, tekniker och verktyg för säkerhetstest av mobil-applikationer.	

Expertgrupp	Europeiska EU-kommissionen	NIS-samarbetsgruppen	Samarbetsgrupp för MS, Kom, och Enisa för områden under NIS regleringen. EU5G kommer ursprungligen från NIS samarbetsgruppen s arbete och hänvisar till 5G-verktygslådan. En viktig grupp som påverkar mycket av det som görs inom EU och 5G/Telecom cybersäkerhet. Relevant för eUICC, SAS och NESAS delar av EU5G	Utvecklar rekommendationer och vägledningar	Cybersäkerhet i 5G (Kommissionens rekommendation av den 26 mars 2019 om cybersäkerhet i 5G-nätverk3/2019) (EU-verktygslådan för 5G-säkerhet) är en uppsättning robusta och omfattande åtgärder för en EU-samordnad strategi för säkra 5G-nätverk. Cybersäkerhet i 5G-nät: EU-rapport om säkerheten i Open RAN. EU:s medlemsstater med stöd av Europeiska kommissionen och EU:s cybersäkerhetsbyrå Enisas rapport om cybersäkerhet i öppna radioaccessnät (Open RAN)	Expertgrupp
Global	GSMA (de facto)	Partnerships 3GPP	Global organisation för mobil kommunikation. Utbyter	Utvecklar standarder för funktionalitet inom mobiltelefoni och eSIM.	SGP.21 Architecture Specification – Definierar arkitektur och tekniska krav för distanshantering av eSIM	

			information, utvecklar standarder och tekniker för cybersäkerhet inom mobil teknologi.		SGP.22 RSP Technical Specification – Teknisk specifikation av distanshantering av eSIM SGP.31 eSIM IoT Architecture and Requirements – Definierar arkitektur och tekniska krav för distanshantering av eSIM för IoT-enheter med begränsat nätverk och/eller användargränssnitt SGP.01 Embedded SIM Remote Provisioning Architecture – Definierar ett gemensamt globalt arkiteturramverk för att möjliggöra distanshantering och hantering av eUICC i maskin-till-maskin-enheter. SGP.02 Remote Provisioning Achitecture for Embedded UICC Technical Specification – Teknisk specifikation av arkitekturen för distanshantering av eUICC	
Global	IETF (de facto)		Standardiseringsorgan som utvecklar specifikationer för nya tekniska standarder för Internet.	Snabbutvecklar standarder av olika slag till internet och kryptografi. Hanterar viktiga standarder för till exempel TCP, TLS, SSH och IPsec	Standarder: RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile – Hantering av publika kryptonycklars certifikat RFC 793 Transmission Control Protocol – Dataöverföringsprotokoll	

					som används för huvuddelen av all kommunikation över Internet. RFC 8446 The Transport Layer Security (TLS) Protocol Version 1.3 – Säker kommunikation mellan datorsystem RFC 4251 The Secure Shell (SSH) Protocol Architecture – Protokoll för säker anslutning över internet eller lokalt nätverk RFC 4301 Security Architecture for the Internet Protocol (IPsec) – Datasäkerhetsteknologier för virtuella private nätverk	
Nationell	BSI (de facto)		Tysklands nationella organ för cybersäkerhet	Har gett ut ett antal Protection Profiles som relaterar till eUICC	Standarder: BSI-CC-PP-0084-2014 - Security IC Platform Protection Profile with Augmentation Packages Version 1.0 BSI-CC-PP-0099-V2-2020 - Java Card System – Open Configuration Protection Profile Version 3.1 BSI-CC-PP-0100-2018 – Embedded UICC for Consumer Devices Protection Profile Version 1.0 BSI-CC-PP- 0104-2019 Cryptographic Service Provider (CSP) Version 0.9.8	

Regional	Enisa	EU:s nätverks- och informationssäkerhetsbyrå. Arbetar för att säkerställa en hög nivå av cybersäkerhet i Europa	Samlar statistik, gör analysrapporter, vägledningar och rekommendationer. Faciliterar samarbete mellan EU, MS och industrin.	Har inflytande på EU-lag-förslag.	ENISA Threat Landscape. En årlig rapport om statusen för cybersäkerhetshoten. Den identifierar de främsta hoten, viktiga trender som observerats med avseende på hot, hotaktörer och attacktekniker, samt analys av effekter och motivation. Den beskriver också relevanta begränsningsåtgärder. 5G Security Controls Matrix. En omfattande och dynamisk matris av säkerhetskontroller och bästa praxis för 5G-nätverk, för att stödja de nationella myndigheterna i EU:s medlemsstater med att implementera de tekniska åtgärderna i EU:s 5G Cybersecurity Toolbox.	Deltagande I det direkta standardiseringsarbetet är begränsat till en utsedd grupp av Enisa. Sverige kan påverka via kommenterar från FMV/ICC. FMV/CSEC är mycket aktiva inom Cyber Security-arbetet med daglig kontakt.

Nedan beskriver exempel på standardiseringsorganisationer och standarder som är av relevans för certifiering av GSMA SAS-processer, jfr. avsnitt 6.16.3.

Typ av Organisation	Standardiserings organ/De Facto	Arbetsgrupper (WG) / Tekniska kommittéer (TC)	Vad gör de?	Varför är de relevanta?	Exempel på standarder, certifieringsordningar, dokument och andra publikationer.	Deltagande från FMV

Global	GSMA (de facto)	Partnerships • 3GPP	Global organisation för mobil kommunikation. Utbyter information, utvecklar standarder och tekniker för cybersäkerhet inom mobil teknologi.	Utvecklar ett certifierings ordning för utvecklare/tillhandahållare av eUICC och av eUICC-användare och deras abonnemang.	FS.18 Security Accreditation Scheme Consolidated Security Requirements and Guidelines Version 11.0 SAS for UICC Production (SAS-UP) Scope definitions Version 2.1 SAS for Subscription Management (SAS-SM) Scope Definitions FS.50 – Security Assurance Specification Development Requirements FS.04 SAS-UP Standard 9.2 FS.05 SAS-UP Methodology 10.1 SAS-UP Costs Guidance 6.0 FS.08 SAS SM Standard 4.0 FS.09 SAS SM Methodology 9.0 SAS-SM Costs Guidance 9.1 SAS-SM Guidelines for use of Cloud Services 1.5	

					GSMA SAS Remote Audit and Certification Policy v4.1 FS.05C19 SAS-UP Covid-19 Methodology Variations v1.1	

Nedan beskriver exempel på standardiseringsorganisationer och standarder som är av relevans för certifiering av GSMA NESAS,certifiering av utvecklingsprocess och komponenter i 5G-system. Jfr. avsnitt 6.16.4.

Typ av Organisation	Standardiserings organ/De facto	Arbetsgrupper (WG) / Tekniska kommittéer (TC)	Vad gör de?	Varför är de relevanta?	Exempel på standarder, certifieringsordningar, dokument och andra publikationer.	Deltagande från FMV
Expertgrupp	3GPP	Organisatoriska partners • ARIB • ATIS • CCSA • ETSI • TSDSI • TTA • TTC	The 3rd Generation Partnership Project (3GPP) är en central organisation som förenar sju organisationer för att tillsammans producera rapporter och specifikationer	Tar fram tekniska specifikationer och globala standarder för utvecklingsprocesser och komponenter i 5G-system och annan mobilkommunikation .	Tekniska Specifikationer; TS 33.116 Security Assurance Specification (SCAS) for the MME network product class TS 33.117 Catalogue of general security assurance requirements TS 33.216 Security Assurance Specification (SCAS) for the evolved Node B (eNB) network product class	

			som definierar 3GPP teknologier.		TS 33.250 Security assurance specification for the PGW network product class TS 33.326 Security Assurance Specification (SCAS) for the Network Slice-Specific Authentication and Authorization Function (NSSAAF) network product class TS 33.511 Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class TS 33.512 5G Security Assurance Specification (SCAS); Access and Mobility management Function (AMF) TS 33.513 5G Security Assurance Specification (SCAS); User Plane Function (UPF) TS 33.514 5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) network product class TS 33.515 5G Security Assurance Specification (SCAS) for the Session Management Function (SMF) network product class	

					TS 33.516 5G Security Assurance Specification (SCAS) for the Authentication Server Function (AUSF) network product class TS 33.517 5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) network product class TS 33.518 5G Security Assurance Specification (SCAS) for the Network Repository Function (NRF) network product class TS 33.519 5G Security Assurance Specification (SCAS) for the Network Exposure Function (NEF) network product class TS 33.521 5G Security Assurance Specification (SCAS); Network Data Analytics Function (NWDAF) TS 33.522 5G Security Assurance Specification (SCAS); Service Communication Proxy (SCP) TS 33.523 5G Security Assurance Specification (SCAS); Split gNB product classes	

					TS 33.526 Security assurance specification for the Management Function (MnF) TS 33.527 Security Assurance Specification (SCAS) for 3GPP virtualized network products Specifikationerna ovan utvecklas kontinuerligt, varvid flera olika versioner av var och en av dessa är tillämpade samtidigt. Därmed är antalet faktiska varianter av ovan specifikationer som används många gånger fler än antalet i ovan lista.	
Global	GSMA (de facto)	Partnerships 3GPP	Global organisation för mobil kommunikation. Utbyter information, utvecklar standarder och tekniker för cybersäkerhet inom mobil teknologi.	Utvecklar vägledningar och rekommendationer av och för mobiloperatörer och har mycket inflytande på metoder för drift av mobilnät. Utvecklar standarder för funktionalitet inom mobiltelefoni. Driver IMEI-databasen.	FS.13 – NESAS Overview - Få en överblick över NESAS. FS.14 NESAS Security Test Laboratory Accreditation – Krav för ackreditering FS.15 NESAS Development and Lifecycle Assessment Methodology – Revisionsbedömning för nätverksutrustningsleverantörers processer. FS.16 NESAS Development and Lifecycle Security Requirements – Säkerhetskrav för	FMV/CSEC bevakar NESAS via EU.

					nätverksutrustningsleverantörers processer. FS.46 NESAS Audit Guidelines – Hur man förbereder och genomför en revision. FS.47 NESAS Product and Evidence Evaluation Methodology – Detaljer om hur produkt- och bevisvärderingen fungerar. FS.50 Security Assurance Specification Development Requirements – Krav på struktur och innehåll för att skapa säkerhetsspecifikationer	
Global	IEEE (SDO)		Internationell standardiseringsorganisation som utvecklar och ger ut standarder inom teknikområdet.	Genom möjligheten att få åtkomst till 4G/5G-mobilnätet genom WiFi-access.	IEEE 802.11 Standards for connections in wireless networking.	
Nationell	BSI (de facto)		Tysklands nationella organ för cybersäkerhet	Utvecklar och äger certifieringsordning för 5G-tillverkare.	NESAS-CCS-GI certification-scheme – Certifierings ordning för 5G-tillverkare	Bevakas av FMV/CSEC genom SOGIS och CCRA.

Regional	ETSI (SDO)	Partnerships • 3GPP • oneM2M Technical Committees • CYBER – Cybersecurity Technical Committee • ESI – Electronic Signatures and Infrastructures • LI – Lawful Interception technical committee • MTS-SIG – Methods for Testing and Specification Security Special Interest Group • NFV – Network Functions Virtualisation	Utvecklar och ger ut standarder för informations- och kommunikationsteknologi.	Utvecklar standarder på teknisk detaljnivå i Europa.	ETSI TS 129 060 Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface ETSI TS 123 502 5G; Procedures for the 5G System (3GPP TS 23.502 version 15.2.0 Release 15) ETSI EN 301 893 5 GHz RLAN; Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU ETSI TS 123 501 5G; System Architecture for the 5G System (3GPP TS 23.501 version 15.2.0 Release 15)	

		• NTECH – Network Technologies • SAGE – Security Algorithms Group of Experts • SAI – Securing Artificial Intelligence SCP – Smart Card Platform				

Referenser

GSMA | eSIM Consumer and IoT Specifications - eSIM

GSMA | Security Accreditation Scheme (SAS) - Security

BSI - Federal Office for Information Security (bund.de)

OWASP Mobile Application Security

GlobalPlatform Specifications Archive - GlobalPlatform

Download ETSI ICT Standards for free

3GPP Portal > Home

Common Criteria : CC Portal (commoncriteriaportal.org)

MITRE ATT&CK®IETF | Internet Engineering Task Force
ISO - International Organization for Standardization

ISO - ISO committee for conformity assessment (CASCO)

Home - SAFECode

ITU: Committed to connecting the world

Welcome To Trusted Computing Group | Trusted Computing Group

NIAP: NIAP Home Page (niap-ccevs.org)

National Institute of Standards and Technology (nist.gov)

Svenska institutet för standarder, SIS - Svenska institutet för standarder, SIS

CEN-CENELEC - CEN-CENELEC (cencenelec.eu)

The European Consumer Consultative Group (ECCG) - European Commission (europa.eu)

ENISA (europa.eu)
SOG-IS - Home (sogis.eu)

Bilaga 9 – Jämförelse med Storbritanniens nationella cybersäkerhetscenter

Tanken på att etablera en samlad nationell kompetens- och stödfunktionen för cybersäkerhet enligt vad som föreslås i denna rapport är inte unik.

Storbritanniens cybersäkerhetscenter (UK NCSC) är ett exempel på en nationell kompetens- och stödfunktion för cybersäkerhet, som har till uppgift att etablera expertis inom IKT, cybersäkerhet och principer för teknisk kontroll och ge stöd till sektorsmyndigheter och verksamhetsutövare.

Som en del av verksamheten finns en särskild enhet som fokuserar på bevakning och proaktiv påverkan på relevanta standarder.

UK NCSC har fler än 1000 anställda.

Nedan följer en kort beskrivning (engelska) om verksamheten:

> The NCSC's mission:
>
> The National Cyber Security Centre (NCSC) is part of the Government Communications Headquarters (GCHQ) and its statutory powers and functions are those of GCHQ.
>
> GCHQ is a central government department which was put on a statutory footing by the Intelligence Services Act 1994, which also sets out: GCHQ's functions; the purposes for which those functions may be exercised; and the Director of GCHQ's statutory responsibilities.
>
> A statutory function of GCHQ, set out at section 3(1)(b) of ISA, and relevant to the work of the NCSC is to "provide advice and assistance about…cryptography and other matters relating to the protection of information and other material, to the armed forces of the Crown to Her Majesty's Government in the United Kingdom or to a Northern Ireland Department or, in such cases as it considers appropriate, to other organisations or persons, or to the general public, in the United Kingdom or elsewhere".
>
> The NCSC is the UK's technical authority for tackling cyber threats and works to defend the UK from cyber risks, deter our adversaries and develop our cyber security capability, consistent with delivering the National Cyber Strategy. The NCSC's activities include providing advice and assistance on cyber security to help address systemic vulnerabilities, and helping organisations increase the cyber resilience of their networks. The NCSC website provides more information about its work. The NCSC cannot single-handedly change cyber security cultures 2 and practices across the UK and therefore works in partnership with many others to achieve improvements.

Källa:

https://ico.org.uk/media/about-the-ico/mou/4027247/ncsc-mou-20230912.pdf

https://www.legislation.gov.uk/ukpga/1994/13/section/3#commentary-key-3d851e70601ca61396e4960978010120

Bilaga 10 – Exempel på internationella Skyddprofiler enligt Common Criteria

Vid tillämpning av standarden ISO/IEC 15408 (”Common Criteria”) är det vanligt förekommande att definiera funktionella krav och krav på kontroll via s.k. skyddsprofiler (eng: ”Protection Profiles”). Sådana kan betraktas som standarder eller tekniska specifikationer för specifika typer produkter och användningsfall.

Vid certifiering enligt Common Criteria (t.ex. inom ramen för EUCC) kan leverantören göra anspråk på att en produkt uppfyller krav angivna i en specifik skyddsprofil. I dessa fall styrs certifieringskraven helt av de krav som anges i den refererade skyddsprofilen. Skyddsprofiler utgör ofta komplicerade och omfattande tekniska specifikationer som anger krav på säkerhetsfunktioner och hur dessa ska granskas. Varje skyddsprofil är utformad för att adressera specifika användningsfall och de säkerhetsproblem som produkten ska adressera.

Nedan tabell listar exempel på sådana skyddsprofiler, vem som förvaltar skyddsprofilen (”äger”) och produkter som certifierats enligt respektive skyddsprofil de senaste två åren.

Skyddsprofil (protection profile - PP)	Kategori	Förvaltare av skyddsprofilen	Certifierad produkt
ANSSI-CC-PP-2021/01 Calypso Basic Protection Profile 11-11-2021	ICs, Smart Cards and Smart Card-Related Devices and Systems	Internet of Trust Calypso Networks Association	• Infineon SLM10TLD002Y design step A12 with CALYPSO™ move software
ANSSI-CC-PP-2021/02 PC Client Specific TPM Protection Profile 30-11-2021	ICs, Smart Cards and Smart Card-Related Devices and Systems	Trusted Computing Group (TCG)	• OPTIGATM Trusted Platform Module SLB9672_2.0 v15 • OPTIGATM Trusted Platform Module SLB9672_2.0 v16 SLB9673_2.0 v26
BSI-CC-PP-0032-V2-2015-MA-01 Common Criteria Protection Profile Electronic Health Card Terminal	ICs, Smart Cards and Smart Card-Related Devices and Systems	Federal Office for Information Security (BSI)	• CHERRY eHealth Terminal ST-1506, AFxZ FW 3.0.0, HW 4.0.0 • ORGA 6141 online Version 3.8.2:1.2.0

(eHCT), Version 3.6 17-09-2015			
BSI-CC-PP-0035-2007 Security IC Platform Protection Profile Version 1.0 23-08-2007	ICs, Smart Cards and Smart Card-Related Devices and Systems	Atmel Secure Products Infineon Technologies AG NXP Semiconductors Germany GmbH Renesas Technology Europe Ltd. STMicroelectronics	• Infineon Security Controller M7893 B11 with optional RSA2048 v2.03.008, SHA-2 V1.01, Toolbox v2.03.008 and with specific IC dedicated software (firmware)
BSI-CC-PP-0055-110 Machine Readable Travel Document with "ICAO Application", Basic Access Control, Version 1.10 25-03-2009	ICs, Smart Cards and Smart Card-Related Devices and Systems	Oberthur Technologies	• CardOS V6.0 ID R1.0 (BAC) • ChipDoc v3.1 on JCOP 4 P71 in ICAO BAC configuration (v2) • MaskTech ePP Applet on Secora ID S v1.1 • Veridos ePass Applet on Sm@rtCafé Expert 8.0 C1, Version 1.0 • TnD v5.1 on ID-One Cosmo J V2 (BAC Configuration) • eTravel Essential 1.2 – BAC and AA activated (release '0300') • eTravel 2.5.A BAC on MultiApp V5.0.A (version 2.5.A.0) • ACOS-IDv2.1 eMRTD (A) BAC Configuration(Version 2.1 eMRTD (A))

BSI-CC-PP-0056-2009 Machine Readable Travel Document with "ICAO Application" Extended Access Control, Version 1.10 07-05-2009	ICs, Smart Cards and Smart Card-Related Devices and Systems	Federal Office for Information Security (BSI)	• TnD v5.1 on ID-One Cosmo J V2 (EAC Configuration) • eTravel Essential 1.2 – BAC, EAC and AA activated (release '0300') • eTravel 2.5.A EAC on SAC on MultiApp V5.0.A (version 2.5.A.0.0) • eTravel 2.5.A EAC on BAC on MultiApp V5.0.A (version 2.5.A.0.0) • eTravel 2.5.A BAC on MultiApp V5.0.A (version 2.5.A.0.0) • Digital Identity 1.0.A PACE, EAC on MultiApp V5.0.A (version 1.0.A) • ChipDoc v3.1 on JCOP 4 P71 in ICAO EAC (1&2) with PACE configuration (v2) • Veridos ePass Applet on Sm@rtCafé Expert 8.0 C1, Version 1.0 • TnD v5.1 on ID-One Cosmo J V2 (PACE/EAC1/Polymorphic eMRTD/LDS2 configuration) • eTravel Essential 1.2 – PACE, EAC and AA activated (release '0300') • eTravel 2.5.A EAC on SAC on MultiApp V5.0.A(version 2.5.A.0.0) • eTravel 2.5.A EAC on BAC on MultiApp V5.0.A (version 2.5.A.0.0) • Digital Identity 1.0.A PACE, EAC on MultiApp V5.0.A(version 1.0.A) • ACOS-IDv2.1 SSCD (A) CL-TC-Comm (Version 2.1 SSCD (A))

BSI-CC-PP-0059-2009 Protection profiles for secure signature creation device - Part 2: Device with key generation 11-12-2009	ICs, Smart Cards and Smart Card-Related Devices and Systems	CEN/ISSS	• ACOS-IDv2.0 SSCD (A) CL-TC-Comm (v2.0 SSCD (A)) • ACOS-IDv2.0 SSCD (A) CB-Comm (v2.0 SSCD (A)) • ID-One Cosmo v9.1 embedding VITALE application version 2.1.4 • ChipDoc v3.1 on JCOP 4 P71 in SSCD configuration (v2) • MaskTech eSign Applet on Secora ID S v1.1 • BelPIC V1.8 on MultiApp V5.0 Platform • ACOS-IDv2.1 SSCD (A) CL-TC-Comm (Version 2.1 SSCD (A)) • ACOS-IDv2.1 SSCD (A) CB-Comm (Version 2.1 SSCD (A))
BSI-CC-PP-0068-V2-2011 Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE_PP), Version 1.0 02-11-2011	ICs, Smart Cards and Smart Card-Related Devices and Systems	Federal Office for Information Security (BSI)	• ChipDoc v3.1 on JCOP 4 P71 in ICAO EAC (1&2) with PACE configuration (v2) • MaskTech ePP Applet on Secora ID S v1.1 • Veridos ePass Applet on Sm@rtCafé Expert 8.0 C1, Version 1.0 • eTravel Essential 1.2 – PACE, EAC and AA activated (release '0300') • ACOS-IDv2.1 SSCD (A) CL-TC-Comm (Version 2.1 SSCD (A)) • DNIe version 4.0
BSI-CC-PP-0070-2011 Digital Tachograph - Smart Card (Tachograph Card), Version 1.02 30-11-2011	ICs, Smart Cards and Smart Card-Related Devices and Systems	Federal Office for Information Security (BSI)	• Tachograph G1, G2V1, G2V2 on IFX_CCI_000039h version 2.2.1.M • Idemia IDeal Drive DT V3.1 on Cosmo V9.1

BSI-CC-PP-0071-2012 Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted channel to certificate generation application 12-12-2012	ICs, Smart Cards and Smart Card-Related Devices and Systems	CEN/ISSS	• ACOS-IDv2.0 SSCD (A) CL-TC-Comm (v2.0 SSCD (A)) • ACOS-IDv2.0 SSCD (A) CB-Comm (v2.0 SSCD (A)) • ID-One Cosmo v9.1 embedding VITALE application version 2.1.4 • ChipDoc v3.1 on JCOP 4 P71 in SSCD configuration (v2) • MaskTech eSign Applet on Secora ID S v1.1 • ACOS-IDv2.1 SSCD (A) CL-TC-Comm (Version 2.1 SSCD (A)) • ACOS-IDv2.1 SSCD (A) CB-Comm (Version 2.1 SSCD (A))
BSI-CC-PP-0072-2012 Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted channel to signature creation application 12-12-2012	ICs, Smart Cards and Smart Card-Related Devices and Systems	CEN/ISSS	• ACOS-IDv2.0 SSCD (A) CL-TC-Comm (v2.0 SSCD (A)) • ID-One Cosmo v9.1 embedding VITALE application version 2.1.4 • ChipDoc v3.1 on JCOP 4 P71 in SSCD configuration (v2) • MaskTech eSign Applet on Secora ID S v1.1 • BelPIC V1.8 on MultiApp V5.0 Platform • ACOS-IDv2.1 SSCD (A) CL-TC-Comm (Version 2.1 SSCD (A))

BSI-CC-PP-0075-2012 Protection profiles for secure signature creation device - Part 3: Device with key import 27-09-2012	ICs, Smart Cards and Smart Card-Related Devices and Systems	CEN/ISSS	• ACOS-IDv2.0 SSCD (A) CL-TC-Comm (v2.0 SSCD (A)) • ACOS-IDv2.0 SSCD (A) CB-Comm (v2.0 SSCD (A)) • ID-One Cosmo v9.1 embedding VITALE application version 2.1.4 • ChipDoc v3.1 on JCOP 4 P71 in SSCD configuration (v2) • MaskTech eSign Applet on Secora ID S v1.1 • ACOS-IDv2.1 SSCD (A) CL-TC-Comm (Version 2.1 SSCD (A)) • ACOS-IDv2.1 SSCD (A) CB-Comm (Version 2.1 SSCD (A))
BSI-CC-PP-0076-2013 Protection profiles for secure signature creation device - Part 6: Extension for device with key import and trusted channel to signature creation application 16-04-2013	ICs, Smart Cards and Smart Card-Related Devices and Systems	CEN/ISSS	• ACOS-IDv2.0 SSCD (A) CL-TC-Comm (v2.0 SSCD (A)) • ID-One Cosmo v9.1 embedding VITALE application version 2.1.4 • ChipDoc v3.1 on JCOP 4 P71 in SSCD configuration (v2) • MaskTech eSign Applet on Secora ID S v1.1 • ACOS-IDv2.1 SSCD (A) CL-TC-Comm (Version 2.1 SSCD (A))
BSI-CC-PP-0084-2014 Security IC Platform Protection Profile with Augmentation Packages Version 1.0 19-02-2014	ICs, Smart Cards and Smart Card-Related Devices and Systems	Inside Secure Infineon Technologies AG NXP Semiconductors Germany GmbH STMicroelectronics EUROSMART	• Samsung STRONGV2P0 of S5E9840 with Specific IC Dedicated Software revision 1.1 • NXP SN300 Series - Secure Element SN300_SE B1.1 J9 • NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3) • S3FT9FA (S3FT9FA_20220430) • NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1) • Samsung S3FV9QM/S3FV9QK 32-bit RISC Microcontroller for Smart Card with

			optional Secure RSA/ECC/SHA Libraries including specific IC Dedicated Software (Référence : S3FV9QM_20220504, Version 3) • S3NSEN4/S3NSEN3 with Bootloader & system API v1.1, DTRNG FRO M libraries v2.2, v3.3 & PTG.1 DTRNG FROM library v1.4 (Revision 1) • S3NSN4V 32-bit RISC Microcontroller for Smart Card including specific IC Dedicated software (Référence S3NSN4V_20220407) • S3FV9RR/S3FV9RQ/S3FV9RP/S3FV9RK 32-bit RISC Microcontroller for Smart Card with optional AE1 Secure Libraries including specific IC Dedicated software (Référence: S3FV9RR_20220407) • Google H1D3 Secure Microcontroller with Crypto Library v1.2.10 • STMicroelectronics ST33K1M5C and ST33K1M5T B01 • STMicroelectronics ST33K1M5A and ST33K1M5M B01 • STARCOS 3.7 COS GKV C3 • NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4) • S3D384C/ S3D352C/ S3D300C/ S3D264C/ S3D232C/ S3K384C Microcontroller • NXP JCOP 7.0 on SN300 Secure Element, JCOP 7.0 R1.62.0.1 • Secure Element S3B512C/SC3512C (32-bit RISC Microcontroller) with optional ATP1 Secure Library and Fingerprint Library including specific IC Dedicated software • NXP Secure Smart Card Controller P6022y VB* including IC Dedicated Software
BSI-CC-PP-0086-2015 Electronic	ICs, Smart Cards and Smart Card-	Federal Office for Information Security (BSI)	• DNIe version 4.0

Document implementing Extended Access Control Version 2 defined in BSI TR-03110 (EAC2-PP), Version 1.01 13-07-2015	Related Devices and Systems		
BSI-CC-PP-0091-2017 Digital Tachograph - Tachograph Card (TC PP) Version 1.0 19-05-2017	ICs, Smart Cards and Smart Card-Related Devices and Systems	European Commission - Joint Research Centre	• Tachograph G1, G2V1, G2V2 on IFX_CCI_000039h version 2.2.1.M • Idemia IDeal Drive DT V3.1 on Cosmo V9.1 • STMicroelectronics J-TACHOG2V2 v.1.0.2
BSI-CC-PP-0097-V2-2020 Protection Profile 1: Network Connector Requirements, Version 1.6.4 17-06-2020	ICs, Smart Cards and Smart Card-Related Devices and Systems	Federal Office for Information Security (BSI)	• RISE Konnektor V5.0
BSI-CC-PP-0098-V2-2021 Protection Profile 2: Connector Requirements, Version 1.5.9 03-05-2021	ICs, Smart Cards and Smart Card-Related Devices and Systems	Federal Office for Information Security (BSI)	• RISE Konnektor V5.0

BSI-CC-PP-0099-2017 Java Card Protection Profile - Open Configuration, Version 3.0.5 21-12-2017	ICs, Smart Cards and Smart Card-Related Devices and Systems	Oracle Corporation	• NXP JCOP 4.5 P71 • Infineon SECORA™ ID S v1.1 (SLJ52GxxyyyzS) • NXP JCOP6.x on SN200.C04 Secure Element • NXP JCOP 4 P71 • Infineon SECORA™ ID X v1.1 (SLJ52GxAyyyzX) • NXP JCOP 4 SE050M
BSI-CC-PP-0099-V2-2020 - Java Card System – Open Configuration Protection Profile Version 3.106-05-2020	ICs, Smart Cards and Smart Card-Related Devices and Systems	Oracle Corporation	• MultiApp V5.0.A Javacard Platform • Plateforme Java Card MultiApp GP-SE (version 5.0) • NXP JCOP 7.0 with eUICC extension on SN300 Secure Element, JCOP 7.0 R1.64.0.2 • Veridos/Giesecke+Devrient MS Sm@rtCafé® Expert 8.0 C1 • Giesecke+Devrient MS Sm@rtCafé® Expert 8.0 C1 • NXP JCOP on SN100.C25 Secure Element • MultiApp V5.0 Java Card Virtual Machine • NXP JCOP 7.0 on SN300 Secure Element, JCOP 7.0 R1.62.0.1 • Idemia IDeal Drive DT V3.1 on Cosmo V9.1 • Plateforme Java Card MultiApp V5.0.A - version 5.0.A • NXP JCOP 6.2 on SN220 Secure Element, R1.01.1, R1.02.1, R1.02.1-1, R2.01.1 • NXP JCOP 4.x on P73N2M0B0.2C2/2C6 Secure Element
BSI-CC-PP-0100-2018 Embedded UICC for Consumer Devices Protection	ICs, Smart Cards and Smart Card-Related Devices and Systems	GSMA	• NXP JCOP 7.0 with eUICC extension on SN300 Secure Element, JCOP 7.0 R1.64.0.2

Profile Version 1.0 05-06-2018			
BSI-CC-PP-0104-2019 Common Criteria Protection Profile Cryptographic Service Provider 28-02-2019	ICs, Smart Cards and Smart Card-Related Devices and Systems	Federal Office for Information Security (BSI)	• Thales TESS v3.0 CSP on S3NSN4V • cryptovision CSP – Java Card applet providing Cryptographic Service Provider version 2.0
BSI-CC-PP-0117-2022 Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile, Version 1.5 01-03-2022	ICs, Smart Cards and Smart Card-Related Devices and Systems	EUROSMART	• Arm Integrated Secure Element CryptoIsland-300P, version 1.0
collaborative Protection Profile for Full Drive Encryption - Encryption Engine, Version 2.0 09-09-2016	Boundary Protection Devices and Systems | Data Protection	The Full Drive Encryption International Technical Community	• Galleon Embedded Computing XSR and G1 Hardware Encryption Layer • Galleon Embedded Computing XSR and G1 Software Encryption Layer
collaborative Protection Profile for Full Drive Encryption Authorization Acquisition, Version 2.0	Boundary Protection Devices and Systems | Data Protection	The Full Drive Encryption International Technical Community	• Galleon Embedded Computing XSR and G1 Hardware Encryption Layer • Galleon Embedded Computing XSR and G1 Software Encryption Layer

01-02-2019			
collaborative Protection Profile for Network Devices, v2.2e 23-03-2020	Boundary Protection Devices and Systems	The Network Device International Technical Community (NDiTC)	• FortiGate/FortiOS Version 6.2.7
Common Criteria Protection Profile for Application Firmware of Secure Smartcard Reader for Electronic Identity Verification System 01-08-2017	ICs, Smart Cards and Smart Card-Related Devices and Systems	TÜBİTAK BİLGEM	• VERA Type-II SSR Application Firmware v1.5.2
EN 419211-2 Protection profiles for secure signature creation device - Part 2: Device with key generation 01-11-2013	ICs, Smart Cards and Smart Card-Related Devices and Systems	CEN/ISSS	• JSIGN4 Security Target Lite • IDentity Applet v3.4-p2/QSCD on NXP JCOP 4 P71

EN 419211-4 Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted channel to certificate generation application 27-11-2013	ICs, Smart Cards and Smart Card-Related Devices and Systems	CEN/ISSS	• JSIGN4 Security Target Lite • IDentity Applet v3.4-p2/QSCD on NXP JCOP 4 P71
EN 419211-5 Protection profiles for secure signature creation device - Part 5: Extension for device with key generation and trusted channel to signature creation application 04-12-2013	ICs, Smart Cards and Smart Card-Related Devices and Systems	CEN/ISSS	• JSIGN4 Security Target Lite
KECS-PP-0820-2017 Korean National Protection Profile for Database Encryption V1.0 18-08-2017	Boundary Protection Devices and Systems | Data Protection	National Security Research Institute (NSR) Telecommunications Technology Association (TTA)	• CubeOne V3.0

KECS-PP-0820a-2017 Korean National Protection Profile for Database Encryption V1.1 11-12-2019	Boundary Protection Devices and Systems | Data Protection	National Security Research Institute (NSR) Telecommunications Technology Association (TTA)	• Spiceware DBE v2.0 • PrivacyDB V2.1 • Echelon V3.5 • D'Amo v5.0
KECS-PP-0821-2017 Korean National Protection Profile for Electronic Document Encryption V1.0 18-08-2017	Boundary Protection Devices and Systems | Data Protection	National Security Research Institute (NSR) Telecommunications Technology Association (TTA)	• HDS v1.0 • Document Security V6.0
KECS-PP-0821a-2017 Korean National Protection Profile for Electronic Document Encryption V1.1 11-12-2019	Boundary Protection Devices and Systems | Data Protection	National Security Research Institute (NSR) Telecommunications Technology Association (TTA)	• FED 5 SP1 • ubCUBE v3.7
KECS-PP-0822a-2017 Korean National Protection Profile for Single Sign On 11-12-2019	**Access Control Devices and Systems**	National Security Research Institute (NSR) Telecommunications Technology Association (TTA)	• Pass-Ni SSO v5.0 • INISAFE Nexess V4.3 • TouchEn Wiseaccess v1.4 • KSignAccess V4.1 • SafeIdentity v5.1 • Bandi SSO v7.0 • Magic SSO V4.0

pp_esm_ac_v2.1 Standard Protection Profile for Enterprise Security Management Access Control 24-10-2013	**Access Control Devices and Systems**	NIAP ESM Technical Community	• Oracle Access Management 12c • Oracle Access Management 12c • Illumio Adaptive Security Platform
PP-Configuration for Network Devices, Intrusion Prevention Systems (IPS), Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, v1.0 08-12-2020	Boundary Protection Devices and Systems	National Information Assurance Partnership (NIAP)	• FortiGate/FortiOS Version 6.2.7
PP-Module for Intrusion Prevention Systems, v1.0 05-11-2021	Boundary Protection Devices and Systems	National Information Assurance Partnership (NIAP)	• FortiGate/FortiOS Version 6.2.7
PP-Module for Stateful Traffic Filter Firewalls, v1.4e 07-01-2020	Boundary Protection Devices and Systems	National Information Assurance Partnership (NIAP)	• FortiGate/FortiOS Version 6.2.7
PP-Module for Virtual Private Network (VPN) Gateways, v1.1 07-01-2020	Boundary Protection Devices and Systems	National Information Assurance Partnership (NIAP)	• FortiGate/FortiOS Version 6.2.7

Secure Element Protection Profile v1.0 GPC_SPE_174 18-03-2021	ICs, Smart Cards and Smart Card-Related Devices and Systems	GlobalPlatform	• Plateforme Java Card MultiApp GP-SE (version 5.0) • Thales TESS v3.0 Platform