Myndigheten för samhällsskydd och beredskap

Nationell handlingsplan för samhällets informationssäkerhet

Statusrapport genomförande

MSB:s kontaktpersoner:
Richard Oehme
Åke Holmgren

Publikationsnummer MSB800 – december 2014
ISBN 978-91-7383-528-2

Förord

Den nationella handlingsplanen för samhällets informationssäkerhet publicerades 2012. Myndigheten för samhällsskydd och beredskap (MSB) tog fram handlingsplanen på uppdrag av regeringen i samråd med övriga myndigheter som ingår i Samverkansgruppen för informationssäkerhet (SAMFI), det vill säga Försvarets materielverk (FMV)/Sveriges certifieringsorgan för it-säkerhet (CSEC), Försvarets radioanstalt (FRA), Försvarsmakten, Post- och telestyrelsen (PTS), samt Säkerhetspolisen/Rikskriminalpolisen.

I handlingsplanen ingår ett trettiotal åtgärdspunkter för att öka informationssäkerheten i samhället. Nyckelområden är samverkan för att motverka och hantera allvarliga it-incidenter och åtgärder för att öka medvetenheten om behovet av informationssäkerhet i samhället. Ett viktigt syfte med planen är att ge väsentliga samhällsaktörer stöd för att förbättra sin informationssäkerhet. Bland dessa finns myndigheter, landsting och kommuner men också privata aktörer.

Arbetet med handlingsplanen kommer att avslutas 2015. Under de senaste två åren har myndigheterna i SAMFI och många andra aktörer i samhället genomfört ett stort antal aktiviteter för att öka samhällets informations- och cybersäkerhet. Ett antal av de åtgärder som presenteras i planen är genomförda och för det stora flertalet åtgärder har arbetet kommit en lång väg. Inför det sista årets arbete med handlingsplanen är det dags att göra ett bokslut. I den här rapporten presenteras därför status för arbetet med handlingsplanens åtgärder.

Richard Oehme

Chef, Verksamheten för samhällets informations- och cybersäkerhet

Innehållsförteckning

Sammanfattning

Den nationella handlingsplanen för samhällets informationssäkerhet är framtagen av Myndigheten för samhällsskydd och beredskap (MSB) i samråd med övriga myndigheter som ingår i Samverkansgruppen för informationssäkerhet (SAMFI), det vill säga Försvarets materielverk (FMV)/Sveriges certifieringsorgan för it-säkerhet (CSEC), Försvarets radioanstalt (FRA), Försvarsmakten, Post- och telestyrelsen (PTS), samt Säkerhetspolisen/Rikskriminalpolisen.

Handlingsplanen publicerades 2012 och innehåller ett 30-tal åtgärder för att öka informationssäkerheten i samhället.

Alla är beroende av att informationshanteringen fungerar. Handlingsplanens breda spektrum av åtgärdsförslag är karaktäriserande för samhället idag. Exempel på åtgärder i planen är:

- Fortsätta utveckla stöd för offentliga och privata organisationers informationssäkerhetsarbete
- Utlysning av ramforskningsprogram kring informationssäkerhet
- Utreda samhällets utbildnings- och kompetensbehov inom informationssäkerhetsområdet
- Ökad samverkan för att förebygga och hantera allvarliga it-incidenter
- Planera, genomföra och utvärdera informationssäkerhetsövningar
- Förebyggande åtgärder för att öka säkerheten i de elektroniska kommunikationerna
- Utveckla ett kryptogranskningsregelverk för kommersiella produkter
- Ökad säkerhet i industriella informations- och styrsystem (SCADA)

Arbetet med handlingsplanen kommer att avslutas 2015. I den här rapporten presenteras genomförda aktiviteter till och med november 2014.

1. Inledning

Den nationella handlingsplanen för samhällets informationssäkerhet är framtagen av Myndigheten för samhällsskydd och beredskap (MSB) i samråd med övriga myndigheter som ingår i Samverkansgruppen för informationssäkerhet (SAMFI), det vill säga Försvarets materielverk (FMV)/Sveriges certifieringsorgan för it-säkerhet (CSEC), Försvarets radioanstalt (FRA), Försvarsmakten, Post- och telestyrelsen (PTS), samt Säkerhetspolisen/Rikskriminalpolisen.[1]

Handlingsplanen publicerades 2012 och sträcker sig tre år. Arbetet kommer att avslutas 2015. I den här rapporten presenteras status över genomfört arbete till och med november 2014.

[1] *Samhällets informationssäkerhet: Nationell handlingsplan 2012* (Myndigheten för samhällsskydd och beredskap), https://msb.se/RibData/Filer/pdf/26290.pdf

2. Nationell handlingsplan för samhällets informations-säkerhet

2.1 Samhällets informations- och cyber-säkerhet

Den digitala utvecklingen ger stora möjligheter att förbättra och effektivisera människors vardag och organisationers verksamhet men skapar även nya risker och utmaningar. För att ta tillvara digitaliseringens möjligheter krävs att digitaliseringen går hand i hand med arbetet med samhällets informations-säkerhet.[2] Det långsiktiga målet är att information hanteras med utgångspunkt i behoven av tillgänglighet, riktighet, konfidentialitet och spårbarhet.

Offentliga organisationer som samverkar måste känna förtroende för varandra när det gäller åtkomst till och utbyte av information. Medborgare och företag måste känna tillit till det offentligas sätt att hantera information. Bristande informationssäkerhet kan få konsekvenser i form av att verksamheten inte kan bedrivas på ett ändamålsenligt och effektivt sätt, bristande skydd för den personliga integriteten samt störningar i samhällsviktig verksamhet.

Mobilitetsutvecklingen leder till att information idag i allt högre utsträckning förflyttas inom och mellan informationssystem. Detta ställer stora krav på såväl fungerande administrativa rutiner som tekniska skyddsmekanismer.

Digitaliseringen av samhället har skapat beroenden som går över sektors-, ansvars- och nationsgränser. I dag äger och driver privata aktörer en stor andel av samhällsviktig verksamhet och kritisk infrastruktur. Privat-offentlig samverkan och internationell samverkan är en grundläggande förutsättning för att öka samhällets informationssäkerhet.

2.2 Handlingsplanen i korthet

Den nationella handlingsplanen utgår från den strategi som myndigheterna i SAMFI tidigare tog fram. Handlingsplanen utgår från fem strategiska områden (nedan) och under varje område finns ett antal åtgärdsförslag.

De fem strategiska områdena är:

1. Informationssäkerhet i verksamheter

[2] Begreppet ”informationssäkerhet” sätter fokus på informationen och ”cybersäkerhet” sätter fokus på den digitala domänen (”cyberspace”). Eftersom allt mer information idag är digital överlappar begreppen varandra. Det finns även andra begrepp som beskriver delar av området, exempelvis Nät- och informationssäkerhet (NIS) och Skydd av kritisk informationsinfrastruktur (CIIP). Begreppsanvändningen inom området är inte entydig.

2. Kompetensförsörjning
3. Informationsdelning, samverkan och respons
4. Kommunikationssäkerhet
5. Säkerheter i produkter och system.

Åtgärdsförslagen i handlingsplanen ligger inom ramen för de uppdrag som myndigheterna i SAMFI har, och de kan genomföras av en myndighet enskilt eller i gemensamma projekt. Planen ska dock inte ses som en komplett redovisning av alla de åtgärder som de olika myndigheterna kommer att genomföra inom sina respektive verksamheter.

Myndigheterna i SAMFI har särskilt angivna uppgifter avseende informationssäkerhet. För att höja samhällets informationssäkerhet krävs dock engagemang och aktiviteter på alla nivåer i samhället. En grund för handlingsplanen är därför att ta fram sätt att arbeta där fler aktörer är med och påverkar både de åtgärder som ingår i nuvarande plan och innehållet i framtidens arbete med informationssäkerhet.

Målgruppen för handlingsplanen är alla aktörer i samhället som arbetar med informationssäkerhet i sin verksamhet. För aktörer inom exempelvis transportsektorn, energisektorn, finanssektorn, samt inom vård och omsorg är det ett stöd att känna till vilken inriktning det nationella arbetet har. Handlingsplanen ger här både en grund för en aktiv dialog om mål och metoder, och en möjlighet för enskilda organisationer att samordna sitt säkerhetsarbete med det nationella säkerhetsarbetet.

3. Status för genomförande av åtgärdsförslag

3.1 Åtgärdsförslag relaterade till informationssäkerhet i verksamheter

Utveckla ramverk för informationssäkerhet	**Åtgärd:** 1.1 **Ansvar:** MSB

Beskrivning (från handlingsplanen):

Myndigheterna i SAMFI har tillsammans med andra aktörer under de senaste åren arbetat för att fram stöd som underlättar för olika organisationer att införa ett ledningssystem för informationssäkerhet. Åtgärden omfattar att förvalta detta arbete och genomföra följande fördjupningar:

- Stöd för ledningsfunktioner att utöva sitt ansvar vad gäller informationssäkerhet, bland annat genom ett systematiskt arbete med riskanalyser och prioritering av skyddsåtgärder.
- Utveckla metoder för riskanalyser som också möjliggör värdering av informationssäkerhetsrisker i förhållande till andra typer av risker samt göra en bedömning av hur olika investeringar ger utdelning i form av bättre säkerhet.
- Utveckla den befintliga modellen för informationsklassning så att den stödjer processen från värdering av konsekvenser fram till användandet av systematiskt utformade skyddsnivåer. I detta arbete kan det även ingå att ta fram definitoner av vissa nationellt gemensamma skyddsnivåer.
- Utveckla stöd för styrningen inom upphandling av system, e-tjänster och andra produkter/tjänster som påverkar informationssäkerheten för verksamheter med stor betydelse för samhällets funktionalitet.
- Utveckla webbplatsen www.informationssäkerhet.se så att den tillhandahåller relevant information och tjänster kring informationssäkerhet för olika aktörer och därmed utgör ett centralt stöd för att utveckla och samordna samhällets informationssäkerhet.

Utbildning och medvetandehöjning som är andra viktiga delar i den administrativa informationssäkerheten behandlas i kapitel 2.

Genomfört arbete:

MSB har bedrivit ett omfattande utåtriktat arbete för att öka medvetenheten

om vikten av informationssäkerhet i olika fora. Ledningsfunktioner inom myndigheter har nåtts både genom möten i enskilda myndigheter och genom deltagande exempelvis i E-delegationens arbete, men MSB har bedömt att den viktigaste insatsen har varit att stödja de informationssäkerhetsansvariga som finns i offentliga och privata organisationer.

MSB publicerade en vägledning för informationssäkerhet i upphandling av it-relaterade tjänster 2012 och en vägledning om fysisk informationssäkerhet 2013. En vägledning för informationsklassning kommer att publiceras första kvartalet 2015. Arbetet med en vägledning för riskanalyser med inriktning på informationssäkerhet planeras att inledas 2015 men ska koordineras med MSB:s modell för riskanalys för samhällsviktig verksamhet.

Utvecklingsinsatser har gjorts både med form och innehåll på webbplatsen informationssäkerhet.se och den utvärdering av dessa förändringar som genomfördes 2013 tyder på att webbplatsen fyller en viktig funktion för främst informationssäkerhetsansvariga i olika typer av organisationer. Under 2014 inledde MSB ett samarbete med Totalförsvarets signalskyddsskola (TSS) med syftet att använda Informationssäkerhet.se för att informera om de kurser TSS erbjuder på området. På Informationssäkerhet.se kan numera både TSS kurskatalog och anmälningsblanketter för kurser laddas ned i pdf-format. Användningen av Informationssäkerhet.se har utgjort ett värdefullt stöd för TSS och kommer att fortgå tillsvidare. I oktober 2014 fick MSB motta utmärkelsen Security Award då webbplatsen Informationssäkerhet.se fick priset som ”Årets IT-säkerhetslösning 2014”.

För att ta fram stöd som underlättar för myndigheter att införa ett ledningssystem för informationssäkerhet har MSB genomfört en kartläggning av hur statliga myndigheter tillämpar MSB:s föreskrifter om statliga myndigheters informationssäkerhet (2009:10) och i övrigt arbetar med informationssäkerhet.

Mer information:

Vägledning för fysisk informationssäkerhet i it-utrymmen:

https://msb.se/sv/Produkter--tjanster/Publikationer/Publikationer-fran-MSB/Vagledning-for-fysisk-informationssakerhet-i-it-utrymmen/

Vägledning – informationssäkerhet i upphandling:

https://msb.se/sv/Produkter--tjanster/Publikationer/Publikationer-fran-MSB/Vagledning--informationssakerhet-i-upphandling/

Webbplatsen informationssäkerhet.se:

www.informationssäkerhet.se

En bild av myndigheternas informationssäkerhetsarbete 2014:

https://www.msb.se/Produkter--tjanster/Publikationer/Publikationer-fran-MSB/En-bild-av-myndigheternas-informationssakerhetsarbete-2014/

Krav på säkerhetsanalyser när säkerhetsskyddsförordningen tillämpas	**Åtgärd:** 1.2 **Ansvar:** FM och Säpo

Beskrivning (från handlingsplanen):

Samtliga myndigheter ska ges särskild information om gällande skyldighet att genomföra säkerhetsanalyser enligt säkerhetsskyddsförordningen, samt kopplingen till riskhantering med utgångspunkt i MSBFS 2009:10.

Genomfört arbete:

Säkerhetspolisen arbetar med en ny vägledning för säkerhetsanalys. I detta arbete nyttjas erfarenheter från inkomna säkerhetsanalyser och skyddsvärdesarbete.

Mer information:

Säkerhetsanalys (Säkerhetspolisen):

http://www.sakerhetspolisen.se/sakerhetsskydd/sakerhetsanalys-steg-for-steg.html

Säkerhetsskydd (Säkerhetspolisen och Försvarsmakten):

https://www.informationssakerhet.se/sv/vagledningar/Sakerhetsskydd/

Utveckla metoder för kontinuitetsplanering	**Åtgärd:** 1.3 **Ansvar:** MSB

Beskrivning (från handlingsplanen):

En analys genomförs som beskriver dels behoven av kontinuitetsplanering ur informationssäkerhetssynpunkt, dels hur området relaterar till exempelvis krisberedskap och samordning vid allvarliga it-incidenter. Därefter utarbetas förslag på generiska metoder för kontinuitetsplanering ur denna aspekt som också går att synkronisera med en organisations övergripande kontinuitetsplanering.

Genomfört arbete:

Under 2013 genomförde MSB ett större projekt i samarbete med Region Västra Götaland och Inera AB. Syftet med projektet var att öka kunskapen kring problematiken att skapa kontinuitet i informationshanteringen i komplexa beroendeförhållanden och där ett stort antal samverkar i informationshanteringen. Projektet avslutades med en rapport och ett mycket välbesökt seminarium.

MSB har även arbetat fram ett underlag för en vägledning för kontinuitetshantering med inriktning på informationssäkerhet. Ytterligare samverkan i denna fråga med andra aktörer som arbetar med kontinuitetshantering kommer att ske innan en vägledning lanseras (under 2015).

Mer information:

Rapport från kontinuitetsprojektet i Region Västra Götaland:

https://www.msb.se/RibData/Filer/pdf/27346.pdf

Stödja arbetet med säker e-förvaltning och säkra e-tjänster	**Åtgärd:** 1.4 **Ansvar:** MSB

Beskrivning (från handlingsplanen):

Ett initiativ för att stödja en säker e-förvaltning ska tas. Initiativet ska bland annat leda fram till en strategi för säker e-förvaltning samt mer specifika åtgärder som stöd för processorienterad kartläggning av information och utredning om ökad kryptografisk säkerhet för e-legitimation och elektronisk signering.

Genomfört arbete:

MSB har lett arbetet med att ta fram en strategi för informationssäkerhet i e-förvaltning som också antagits av E-delegationen och har även initierat ett arbetsutskott för informationssäkerhet i delegationen. MSB leder detta arbetsutskott som bland annat tagit fram en checklista för informationssäkerhet för e-förvaltningsprojekt och även bistått vid riskanalyser inom de projekt som redan inletts inom delegationen. En vägledning för informationssäkerhet inom e-förvaltning har påbörjats och beräknas färdigställas 2015. En vägledning för processorienterad informationskartläggning togs fram 2012 tillsammans med Riksarkivet.

MSB har under 2014 på begäran av Arbetsförmedlingen, Centrala studiestödsnämnden och Försäkringskassan genomfört en analys av informationssäkerheten hos Svensk e-legitimation. Denna analys utmynnade bland annat i rapporten ”Analys och rekommendationer avseende informationssäkerhet i Svensk e-legitimation”.

Mer information:

Strategi för informationssäkerhet i e-förvaltning:

https://msb.se/sv/Produkter--tjanster/Publikationer/Publikationer-fran-MSB/Strategi-for-informationssakerhet-i-e-forvaltning/

Vägledning: Metod för Utveckling i Samverkan – E-delegationen 2013:

http://www.edelegationen.se/Documents/Vagledningar%20mm/Metod%20f%c3%b6r%20utveckling%20i%20Samverkan%20version%201%200.pdf?epslanguage=sv

Vägledning för processorienterad informationskartläggning:

https://msb.se/sv/Produkter--tjanster/Publikationer/Publikationer-fran-MSB/Vagledning-for-processorienterad-informationskartlaggning/

Analys och rekommendationer avseende informationssäkerhet i Svensk e-legitimation:

https://www.msb.se/sv/Om-MSB/Nyheter-och-press/Nyheter/Nyheter-fran-MSB/Analys-av-informationssakerheten-i-Svensk-e-legitimation/

Utveckla stöd till särskilda verksamheter	**Åtgärd:** 1.5 **Ansvar:** MSB

Beskrivning (från handlingsplanen):

Aktiviteter ska genomföras för att öka informationssäkerheten inom vård och omsorg, kommuner samt små och medelstora företag. I detta ingår att utveckla nätverk för informationsdelning och samverkan inom respektive verksamhetsområde.

Genomfört arbete:

Vård och omsorg:

MSB har bedrivit ett aktivt arbete för att stödja en förbättrad informationssäkerhet i vård och omsorg. Bland annat har en strategi för informationssäkerhet för vård och omsorg tagits fram tillsammans med Socialstyrelsen och Datainspektionen. Flera andra organisationer som till exempel E-hälsomyndigheten och Västra Götalandsregionen har sedan anslutit sig till strategin och en grupp av myndigheter har arbetat med att ta fram en handlingsplan utifrån strategin.

MSB har också initierat ett antal projekt inriktade på informationssäkerhet som till exempel kring kontinuitetshantering i Västra Götalandsregionen och skydd mot obehörig åtkomst. MSB bedriver för övrigt kontinuerlig samverkan och informationsdelning med myndigheter och landsting i olika forum.

Kommuner:

MSB har löpande träffat kommunerna i olika sammanhang för att öka medvetenheten kring informationssäkerhet. MSB har också tagit fram ett antal vägledningar och annat stödmaterial specifikt för kommuner utöver det som är riktat till alla organisationer, exempelvis: ”Kommunens informationssäkerhet – en vägledning”, ”Verktygslåda för systematiskt informationssäkerhetsarbete i kommuner” och ”Att hantera överbelastningsattacker”.

MSB har tillsammans med SKL varit stödjande för upprättandet av KIS, Informationssäkerhetsnätverket Sveriges kommuner. Från starten sommaren 2011 har nätverket idag cirka 150 deltagare. MSB fortsätter att stödja nätverket med olika åtgärder, bland annat genom att hjälpa till med att arrangera nätverksträffar (två stycken per år). En särskild programgrupp etablerades under 2012 där informationssäkerhetsansvariga från de tre

största kommunerna och från tre mindre kommuner deltar tillsammans med SKL och MSB.

Under 2012 startades ett arbete med att stötta ett antal kommuner att arbeta efter metodstödet som ges på webbplatsen informationssäkerhet.se och ISO 27000-serien. Det resulterade i att Borlänge kommun och sektorn Verksamhetsstöd under våren 2013 blev den första kommunen att certifiera sig mot informationsstandarden ISO/IEC 27001.

MSB drev under 2012 och 2013, i samarbete med PTS, SKL och .SE, ett arbete för införande av säker DNS (DNSSEC) i kommuner. Kommuner kunde då via länsstyrelserna söka medel från det s.k. krishanteringsanslaget. Detta i syfte att få brister i DNS åtgärdade och signering med DNSSEC på plats. Se även åtgärd 4.3.

Vad gäller stöd till små och medelstora företag, är det långsiktiga målet att kunna erbjuda sådana företag ett värdefullt stöd för sin informationssäkerhet. Målet är att stärka såväl företagens kärnverksamhet som samhällets övergripande informationssäkerhet. MSB har under 2014 initierat ett arbete med att kartlägga branschorganisationer som riktar sig till dessa företag inom näringslivet. Arbetet kommer att intensifieras under 2015 med fokus på att utveckla en vägledning och samverkan med branschorganisationer.

Mer information:

Strategi för stärkt informationssäkerhet inom vård och omsorg:

https://msb.se/sv/Produkter--tjanster/Publikationer/Publikationer-fran-MSB/Strategi-for-starkt-informationssakerhet-inom-vard-och-omsorg/

Kommunens informationssäkerhet – en vägledning:

https://msb.se/sv/Produkter--tjanster/Publikationer/Publikationer-fran-MSB/Kommunens-informationssakerhet--en-vagledning-/

Verktygslåda för systematiskt informationssäkerhetsarbete i kommuner:

https://msb.se/sv/Produkter--tjanster/Publikationer/Publikationer-fran-MSB/Verktygslada-for-systematiskt-informationssakerhetsarbete-i-kommuner/

Att hantera överbelastningsattacker:

https://msb.se/sv/Produkter--tjanster/Publikationer/Publikationer-fran-MSB/Att-hantera-overbelastningsattacker/

Självmätning av informationssäkerhet	**Åtgärd:** 1.6 **Ansvar:** MSB

Beskrivning (från handlingsplanen):

Ta fram ett verktyg för självmätning av informationssäkerhet för myndigheter, landsting och kommuner. De olika aktörerna ska på ett säkert

sätt kunna föra in uppgifter om sin säkerhetsnivå, samt kunna jämföra sin nivå med andra, i verktyget. Det ska även vara möjligt att i verktyget sammanställa olika avidentifierade rapporter för att kunna skapa en bild av samhällets informationssäkerhet.

Genomfört arbete:

MSB driver ett utvecklingsarbete med att ta fram en applikation för självmätning av informationssäkerhet för myndigheter, landsting och kommuner. De olika aktörerna ska på ett säkert sätt kunna föra in uppgifter om sitt informationssäkerhetsarbete genom att svara på ett frågeformulär. Möjlighet ska finnas för respektive organisation att ta ut rapporter som jämför sin egen organisations informationssäkerhetsnivå över tid, mot ”Best Practice” och mot snittet, vilket kommer att bli ett mycket bra stöd för respektive organisation i det fortsatta arbetet. Det ger även MSB möjlighet att sätta in resurser på rätt ställen.

Mer information:

Kontaktperson på MSB: Lars Grundström

Förbättra skyddet av personlig integritet som en del i informationssäkerheten	**Åtgärd:** 1.7 **Ansvar:** MSB

Beskrivning (från handlingsplanen):

Utreda och förtydliga hur personlig integritet ska värnas inom informationssäkerhetsarbetet. Personlig integritet ska vara en drivande faktor vid till exempel val av skyddsnivåer och åtgärder.

Förtydliga hur balans kan skapas mellan å ena sidan personlig integritet och å andra sidan säkerhetsåtgärder som kan vara kränkande, till exempel loggning och annan övervakning.

Genomfört arbete:

MSB har på olika sätt lyft fram att integritet är en viktig del av målet för ett fungerande informationssäkerhetsarbetet liksom att informationssäkerhetsåtgärder är förutsättningen för att uppnå integritet. Tillsammans med Lunds universitet har två studier genomförts kring interitetet som grund för det fortsatta arbetet.

Mer information:

Kontaktperson MSB: Fia Ewald

Nationell terminologi för informationssäkerhet	**Åtgärd:** 1.8 **Ansvar:** FMV/CSEC

Beskrivning (från handlingsplanen):

Att i samarbete med relevanta specialister, SIS/TK 318 Informationssäkerhet och SIS förlag AB ta fram en reviderad version av SIS HB 550 Terminologi för informationssäkerhet, samt säkerställa att det finns en långsiktig förvaltning av terminologin.

Genomfört arbete:

SIS TK318 har genomfört följande:

- Efter beslut om ny publiceringsform överfört materialet till mall och format för SIS Teknisk Rapport
- Slutfört grundläggande uppdatering av terminologi för informationssäkerhet, rensat ut förlegade termer och begrepp och kompletterat med nya termer och definitioner
- Genomfört avstämning med ämnesexperter för flertalet delar i rapporten
- Genomfört en intern remiss av rapporten till organisationerna i SIS/TK 318 Informationssäkerhet.
- SIS har tilldelat särskilda medel för slutförande av arbetet innefattande redaktör för slutredigering, terminologigranskning av TNC och administrativt stöd.

MSB har genomfört följande:

Under 2014 genomförs två förstudier av förutsättningar och möjligheter till myndighetssamordning av terminologi och fackspråk på informations-säkerhetsområdet. Dels genomförs en bred förstudie av källor, metoder och organisationsformer för utveckling och underhåll av termer och fackspråk av relevans för berörda branscher, sektorer och myndigheter. Målet är förslag till utvecklings- och förvaltningsstrategier av en termdatabas i regi av myndigheter. Dels genomförs en fördjupad studie av källor, korpus och begreppsanalys som underlag för myndighetssamordning av fackspråk.

Mer information:

Kontaktperson på FMV/CSEC: Dag Ströman

MSB:s förstudie kommer att resultera i en rapport som, i första hand, kommer att presenteras för SAMFI. Kontaktperson MSB: Tom Andersson

3.2 Åtgärdsförslag relaterade till kompetensförsörjning

Utreda samhällets utbildnings- och kompetensbehov inom informationssäkerhetsområdet	**Åtgärd:** 2.1 **Ansvar:** MSB

Beskrivning (från handlingsplanen):

Utreda samhällets behov av kompetens inom informationssäkerhetsområdet i ett femårigt perspektiv.

FRA, PTS och MSB samarbetar med Försvarshögskolan (FHS) om utveckling av utbildningen CIAO under 2012.

Genomfört arbete:

Under 2014 genomförs en fördjupad forskarstudie av kompetensförsörjning med inriktning på samtidens och framtidens kompetensbehov på informationssäkerhetsområdet inom samhällsviktiga verksamheter. Genom workshops med ämnesexperter på myndigheter, företag och andra organisationer kartläggs drivkrafter i tillgång och efterfrågan på kompetens samt organisationers strategier och metoder för kompetensförsörjning. Målet med fördjupningsstudien är att lägga förslag till metod för en nationell kompetensanalys. Uppdraget genomförs av en forskargrupp under ledning av forskare vid Högskolan i Skövde.

Kursen Chief Information Assurance Officer (CIAO) har givits av Försvarshögskolan (FHS) under ett antal år, ursprungligen som ett samarbete med amerikanska National Defense University (NDU). Under 2013-2014 har ett utvecklingsarbete bedrivits i samverkan med PTS, FRA och MSB. Kurskonceptet har modifierats för att passa såväl svenska som europeiska krav. FHS genomförde den första svenska kursen 2013. Totalt har 50 elever med viktiga positioner inom området genomfört kursen 2013-14.

Mer information:

Kontaktperson MSB: Fia Ewald

Utbildningen Chief Information Assurance Officer (CIAO):

http://www.fhs.se/sv/utbildning/uppdragsutbildningar/informationssakerhet/ciao-utbildning/bakgrund/

Öka medvetandet om informationssäkerhet i samhället	**Åtgärd:** 2.2 **Ansvar:** MSB

Beskrivning (från handlingsplanen):

Ta fram och genomföra ett program för att höja medvetenheten kring informationssäkerhet i samhället.

Genomfört arbete:

MSB har genomfört två så kallade nollmätningar om medvetenhet om informationssäkerhet, dels utbildningssektorn och dels i övrig kommunal verksamhet. Underlaget har använts i arbetet med att sprida de kunskapsprodukter som MSB och andra myndigheter har inom området, bland andra DISA (Datorstödd informationssäkerhetsutbildning för användare) och Informationssäkerhetsskolan ISA (informationssäkerhet för grundskoleelever). För ISA har också tagits fram stödmaterial för lärare och det har även skett ett samarbete med Surfa lugnt. Ett femtiotal organisationer har slutit avtal för att regelmässigt använda DISA och för närvarande pågår ett utvecklingsarbete för att ytterligare förbättra DISA. En vidareutveckling av DISA riktad mot vård och omsorg har också inletts under 2014 genom att skapa ett kunskapsunderlag om vilka risker som är mest relevanta i vårdmiljön

För att öka en allmänhetens medvetenhet om risker och säkerhet genomfördes under 2013 och 2014 kampanjer i Sverige som en del av den Europeiska informationssäkerhetsmånaden (ECSM). Dessutom har det under 2014 gjorts en behovsanalys av medvetandehöjande insatser inför 2015. MSB har också beslutat om att mer systematiskt arbeta med kunskapsförsörjning och säkerhetskultur vilket har lett till bland annat ett par studier kring kompetens och kunskapsförsörjning samt ett antal seminarier i dessa frågor. Därutöver pågår utvecklings- och forskningsinsatser, till exempel utvecklingsarbete av mätverktyg för riskmedvetenhet och ett femårigt forskningsprogram om säkerhetskultur.

Myndigheterna i SAMFI har årligen genomfört en konferens om informationssäkerhet för offentlig sektor med över 500 deltagare från statliga myndigheter, kommuner och landsting. Konferensen är värdefull för att sprida kunskap om systematiskt informationssäkerhetsarbete men också viktig för erfarenhetsutbyte deltagarna emellan.

Mer information:

Kontaktperson för medvetandehöjning, kompetens och säkerhetskultur hos MSB: Tom Andersson

Europeiska informationssäkerhetsmånaden (ECSM) i Sverige:

http://www.dinsakerhet.se/Informationssakerhet/

European Cyber Security Month (ECSM), information från Enisa:

http://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/european-cyber-security-month-advocacy-campaign

Datorstödd informationssäkerhetsutbildning för användare (DISA):

https://www.msb.se/Forebyggande/Informationssakerhet/Stod-inom-informationssakerhet/DISA--utbildning-informationssakerhet/

Informationssäkerhetsskolan (ISA):

https://www.msb.se/sv/Forebyggande/Informationssakerhet/Stod-inom-informationssakerhet/ISA---for-arskurs-4-och-5/

Att undervisa om informationssäkerhet:

https://www.msb.se/RibData/Filer/pdf/26345.pdf

Utlysning av ramforskningsprogram kring informationssäkerhet	**Åtgärd:** 2.3 **Ansvar:** MSB

Beskrivning (från handlingsplanen):

Utveckla ramforskningsprogram kring informationssäkerhet och ökad samverkan kring informationssäkerhetsforskning och utveckling i samhället. Ett första steg är att genomföra en utlysning av forskningsmedel inom informationssäkerhetsområdet under 2012.

Genomfört arbete:

MSB beviljade forskningsmedel till programmet Security Culture and Information Technology (SECURIT) 2012 (se nedan) och för närvarande pågår arbetet med en forskningsutlysning inom området industriella informations- och styrsystem. SECURIT planeras pågå till och med juni 2017 och forskningssatsningen inom området industriella informations- och styrsystem ska löpa under fem års tid med start senast juni 2015.

MSB har tagit fram en forskningsstrategi för åren 2014-2018. Den är ett ramverk och en inriktning för MSB-finansierad forskning under perioden. Informationssäkerhet ingår som ett av fem forskningsområden.

För att öka samverkan kring informationssäkerhetsforskning och utveckling i samhället stödjer MSB sedan 2009 det svenska nätverket för doktorander inom it-säkerhet (SWITS).

Mer om SECURIT:

Forskningsprogrammet SECURIT finansieras av MSB och koordineras av Totalförsvarets forskningsinstitut (FOI). Forskningen genomförs gemensamt av Chalmers, Göteborgs universitet, FOI, KTH och Örebro universitet i samarbete med Linköpings universitet.

SECURIT har som mål att förbättra organisationers informationssäkerhet och däri ligger att ha en god säkerhetskultur eftersom det är en viktig förutsättning för informationssäkerheten. För att uppnå målen studerar SECURIT:

- Egenskaper hos individer och organisationer som är relevanta för informationssäkerheten
- Effekter av åtgärder som syftar till att förbättra informationssäkerheten genom att påverka individer och organisationer

Exempel på vad forskningen inom SECURIT syftar till att besvara för typ av frågor är bland annat:

- Vilka faktorer påverkar framgång och acceptans för förändringar med avsikt att förbättra organisationers informationssäkerhet?
- Hur och varför formas säkerhetkultur olika i olika organisationer?
- Hur kommuniceras och tolkas säkerhetskultur med avsikt att hantera organisationers informationssäkerhet?
- Hur kan attityd hos ledning och medarbetare påverka säkerhetskultur och säkerhetsklimat i organisationer?

Mer information:

Forskningsprogrammet SECURIT:

http://www.foi.se/sv/Var-kunskap/Informationssakerhet-och-Kommunikation/Informationssakerhet/Projekt/SECURIT/

MSB:s forskningsutlysning om industriella informations- och styrsystem:

https://www.msb.se/sv/Om-MSB/Forskning/Utlysningar/Pagaende-utlysningar/Utlysning-industriella-styrsystem-steg-1/

MSB:s arbete med forskning för ett säkrare samhälle:

https://www.msb.se/forskning

Informationsinsats om signalskydd	**Åtgärd:** 2.4 **Ansvar:** FM, MSB och FRA

Beskrivning (från handlingsplanen):

Ta fram ett informationsunderlag om signalskydd och sprida detta till myndigheter, kommuner och landsting.

Genomfört arbete:

Försvarsmakten har tillsammans med FRA och MSB under 2014 arbetat med

medvetandehöjande insatser kring signalskydd och har inom ramen för detta arbete tagit fram en informationskampanj för signalskydd. Informationskampanjen har primärt utformats för att öka medvetenheten om, och visa på vinsten med, signalskydd i olika verksamheter. Ett ytterligare mål med kampanjen har varit att få tillstånd en attityd- och beteendeförändring hos de målgrupper som berörs av informationskampanjen..
Mer information: Informationskampanj för signalskydd: www.infirmationssäkerhet.se/signalskydd Kontaktperson MSB: Ronny Janse

3.3 Åtgärdsförslag relaterade till informationsdelning, samverkan och respons

Ökad samverkan för att förebygga och hantera allvarliga it-incidenter	**Åtgärd:** 3.1 **Ansvar:** SAMFI
Beskrivning (från handlingsplanen): Fortsatt arbete med nationell samverkan inom informationssäkerhets-området, inom ramen för gällande ansvar och roller. Fortsatt utveckling av en nationell samverkansfunktion för informationssäkerhet. Fortsatt arbete mellan säkerhets- och underrättelsetjänsterna för att ytterligare stärka förmågan att hantera allvarliga antagonistiska it-angrepp. Fastställa den nationella hanterandeplanen för allvarliga it-incidenter efter övning och revidering.	
Genomfört arbete: Myndigheterna i SAMFI har fortsatt arbete med nationell samverkan inom informationssäkerhetsområdet inom ramen för gällande ansvar och roller. Basen för den generella samverkan har varit regelbundna möte i SAMFI, cirka sex halvdagsmöten per år, samt olika mer praktiska arbetsgrupper under SAMFI. När det gäller att förebygga och hantera allvarliga it-incidenter har övningen NISÖ 2012 planerats, genomförts och utvärderats (se åtgärd 3.5) samt att samverkan genomförts kring tekniska förmågeuppbyggande övningar. Samverkan har även genomförts mellan olika myndigheter i SAMFI vid inträffade it-relaterade händelser.	

MSB har fortsatt att utveckla den nationella operativa samverkansfunktion för informations- och cybersäkerhet (NOS) och myndighetens operativa uppdrag (inklusive CERT-SE). I detta ingår både samverkansprocesser och tekniskstöd. Under 2015 kommer ett samlat operativt koncept för att förebygga och hantera it-incidenter att implementeras.

Säkerhetspolisen, Försvarsmakten/Must och FRA påbörjades i december 2012 samarbetet Nationell samverkan till skydd mot allvarliga IT-hot (NSIT). NSIT analyserar och bedömer hot och sårbarheter samt skyddsåtgärder när det gäller allvarliga eller kvalificerade it-hot mot de mest skyddsvärda nationella intressena. Syftet är att utveckla samverkan för att försvåra för en kvalificerad angripare att komma åt eller skada svenska skyddsvärda civila och militära resurser. MSB är sedan 2014 observatör i NSIT.

Den nationella hanterandeplanen, vilken MSB tog fram som ett regeringsuppdrag vilket redovisades i mars 2011, övades i NISÖ 2012 och har uppdaterats. För närvarande pågår ett arbete med att införliva erfarenheter från internationella cybersäkerhetsövningar. En uppdaterad hanterandeplan kommer att fastställas under 2015.

Mer information:

SAMFI:

https://www.msb.se/sv/Forebyggande/Informationssakerhet/Informationssakerhet-i-samhallet/Samverkansgruppen-SAMFI/

MSB:s uppdrag när det gäller att förebygga och hantera it-incidenter:

https://www.msb.se/sv/Forebyggande/Informationssakerhet/IT-incidenterCERT-SE/

Information om NSIT:

http://www.fra.se/snabblankar/nyheterochpress/nyhetsarkiv/nyheter/sapomustochfrainyttsamarbeteforattstarkadennationellasakerheten.197.html

Hantering av allvarliga it-incidenter:

https://www.msb.se/sv/Forebyggande/Informationssakerhet/Informationssakerhet-i-samhallet/Hanterandeplan-IT-incidenter/

It-incidentrapportering	**Åtgärd:** 3.2 **Ansvar:** MSB

Beskrivning (från handlingsplanen):

Genomföra en fördjupad analys av obligatorisk it-incidentrapportering för, primärt, statliga myndigheter.

Genomfört arbete:

MSB har på regeringens uppdrag tagit fram ett förslag på ett system för it-incidentrapportering som ska vara obligatoriskt för statliga myndigheter och

frivilligt för övriga organisationer. I rapporten till regeringen konstaterar MSB att en viktig del i arbetet med samhällets informationssäkerhet är en systematisk, bred och samlad rapportering av it-incidenter. Syftet med ett nationellt system för it-incidentrapportering är att öka samhällets förmåga att förebygga, motstå, återhämta och lära av it-incidenter och it-relaterade kriser.

Frågan om ett eventuellt införande av obligatorisk it-incidentrapportering bereds av Regeringskansliet och har varit vilande med hänvisning till ett eventuellt kommande krav från EU på att införa ett sådant system.

Efter det att regeringsuppdraget ovan redovisades (december 2012) har MSB fortsatt att arbeta med att utveckla den frivilliga it-incidentrapporteringen, bl a har en prototyp till ett incidentrapporteringsverktyg tagits fram. Syftet är att slutföra arbetet med detta incidentrapporteringsverktyg under 2015.

Mer information:

Information om regeringsuppdrag till MSB rörande it-incidentrapportering:

https://www.msb.se/Om-MSB/Nyheter-och-press/Nyheter/Nyhetsarkiv/Nyhetsarkiv-2012/MSB-foreslar-system-for-it-incidentrapportering-for-att-stodja-samhallets-informationssakerhet-/

Tekniska detekterings- och varningssystem	**Åtgärd:** 3.3 **Ansvar:** FRA och övr. SAMFI

Beskrivning (från handlingsplanen):

Arbetet med tekniska detekterings- och varningssystem fortsätter inom ramen för ordinarie verksamhet hos myndigheterna i SAMFI och andra aktörer.

Ett särskilt behov är att utveckla system som på ett säkert sätt kan tillvarata och hantera information från säkerhets- och underrättelsetjänsterna.

Genomfört arbete:

Arbetet med att på olika sätt detektera och varna för it-incidenter har fortsatt inom ramen för ordinarie verksamhet hos myndigheterna i SAMFI. MSB/CERT-SE har exempelvis utvecklat ett system för att, via huvudsakligen publika datakällor, samla in data över infekterade datorer i Sverige och filtrera ut de som tillhör myndigheter, kommuner, landsting och andra samhällsviktiga organisationer. Systemet varnar även organisationerna.

I enlighet med det regeringsuppdrag som FRA fick i november 2011 har myndigheten tagit fram en pilotversion av TDV som har testats hos en annan myndighet (regeringsuppdraget redovisades i december 2012). TDV är tänkt som ett förstärkt skydd för de mest skyddsvärda funktionerna i samhället och utgör ett komplement till grundläggande informationssäkerhetsåtgärder. Systemet upptäcker olika former av it-angrepp, till exempel i form av skadlig

kod. Det som är avgörande för systemets funktion är de kvalificerade detekteringsverktyg och signaturer som används för att upptäcka it-angreppen. Dessa bygger på kunskap från FRA:s uppdrag både på informationssäkerhets- och signalspaningsområdet. Idag pågår försöksverksamhet. Verksamheten har visat att systemet fungerar genom att avancerad skadlig kod som sannolikt härrör sig från kvalificerade angripare har upptäckts.

Mer information:

System för att identifiera infekterade datorer och varna organisationer (MSB/CERT-SE):

https://www.cert.se/megamap/

Information om TDV och regeringsuppdrag till FRA:
http://www.fra.se/verksamhet/informationssakerhet/regeringsuppdragtillfra.121.html

Nationell samverkan kring arbetet med informationssäkerhet i EU	**Åtgärd:** 3.4 **Ansvar:** SAMFI

Beskrivning (från handlingsplanen):

Ett aktivt deltagande i det informationssäkerhetsarbete som sker inom ramen för EU och en ökad nationell samverkan kring EU:s arbete med informationssäkerhet.

Genomfört arbete:

Myndigheterna i SAMFI har inom ramen för sin ordinarie verksamhet deltagit i ett stort antal aktiviteter som rör EU:s arbete med informations- och cybersäkerhet.

I februari 2013 lanserade EU en cybersäkerhetsstrategi och samtidigt med denna ett utkast till ett direktiv om nät- och informationssäkerhet (NIS). Myndigheterna i SAMFI har på olika sätt stöttat Regeringskansliet i de förhandlingar som pågår om NIS-direktivet. Som del av cybersäkerhets-strategin lanserade EU-kommissionen även den så kallade NIS-plattformen i juni 2013. Plattformen är en privat-offentlig samverkan för att ta fram ramverk (identifiera rekommendationer) kring NIS. PTS och MSB deltar i NIS-plattformens arbete.

EU-kommissionen driver även forumet EFMS (European Forum for Member States on public policies for security and resilience in the context of Critical Information Infrastructure Protection (CIIP)) sedan 2009. Forumet behandlar idag informations- och cybersäkerhet ur ett brett perspektiv och PTS och MSB deltar regelbundet i möten.

Samarbetet inom EU omfattar även it-brott och i januari 2013 invigde EU-kommissionen European Cybercrime Centre (EC3). Rikskriminalpolisen

driver ett projekt för att införa ett it-brottscentrum i den nya Polismyndigheten. Detta centrum blir bland annat kontaktpunkt till EC3.

Avslutningsvis så har den europeiska nätsäkerhetsmyndigheten Enisa under de senaste åren arangerat ett mycket stort antal aktiviteter och driver ett antal arbetsprocesser och forum. Ämnesmässigt rör det sig om exempelvis it-incidenthantering (stöd till CERT-funktioner och samverkan kring it-incidenthantering), skydd av kritisk informationsinfrastruktur (säkerhet i industriella styrsystem, cyberövningar, tekniska säkerhetsfrågor etc.), dataskydd och eID, samt riskhantering (hot och risker, ramverk för risk- och kontinuitetshantering, etc). Myndigheterna i SAMFI har i olika omfattning deltagit i Enisas arbete. I Sverige har PTS ett huvudansvar för Enisa-samordning och informationsspridning. Detta sker genom en så kallad ”National Liasion Officer” (NLO).

Mer information:

EU:s arbete med informations- och cybersäkerhet:

http://ec.europa.eu/digital-agenda/en/cybersecurity

European Cybercrime Centre (EC3):

https://www.europol.europa.eu/ec3

Europeiska unionens byrå för nät- och informationssäkerhet (Enisa):

http://www.enisa.europa.eu/

Planera, genomföra och utvärdera informationssäkerhetsövningar	**Åtgärd:** 3.5 **Ansvar:** MSB, PTS och FM

Beskrivning (från handlingsplanen):

Planera, genomföra och utvärdera den nationella informationssäkerhets-övningen NISÖ 2012 och en teknisk informationssäkerhetsövning under 2013, samt kommande övningar.

Delta aktivt i det arbete som sker med informationssäkerhetsövningar inom EU och Nato/PFP.

Genomfört arbete:

Den 28-29 november 2012 genomförde MSB den nationella informations-säkerhetsövningen NISÖ 2012. Övningen syftade till att stärka samhällets samlade förmåga till krishantering, och specifikt möjligheten till att hantera större it-relaterade kriser genom en utvecklad förmåga till samarbete. Övningen var av nationell karaktär men med ett visst nordisk deltagande (ett separat spår för nordiska nationella CERT-funktioner). Likt dess föregångare (NISÖ 2010) fokuserade scenariot i övningen på informationssäkerhet där samhällsviktig verksamhet, inom energi, telekom och transportsektorn

utsätts för påfrestningar. I övningen ingick såväl centrala myndigheter som privata företag inom utpekade sektorer. Lärdomar från övningen presenterades i en erfarenhetsrapport. Arbetet med att utveckla övningsserien NISÖ pågår för närvarande.

MSB har i samverkan med övriga myndigheter i SAMFI arbetat med att utveckla förmågan att hantera it-incidenter genom tekniska informations- och cybersäkerhetsövningar. I september 2012 gav MSB ut en handbok som syftar till att vara en hjälp vid planering, genomförande och återkoppling av tekniska informations- och cybersäkerhetsövningar. Underlaget till handboken utarbetades ursprungligen av Försvarshögskolan. Arbetet med tekniska informations- och cybersäkerhetsövningar fortsätter och involverar även samverkan mellan de nordiska nationella CERT-funktionerna.

Sverige har deltagit i övningarna Cyber Europe 2012 respektive 2014. Övningarna har organiserats av den europeiska nätsäkerhetsmyndigheten Enisa tillsammans med EU:s och EFTA:s medlemsländer. MSB har varit samordnande myndighet för Sveriges deltagande och planeringen av övningarna. I övningen 2012 deltog Bankföreningen (representerandes affärsbankerna i Sverige), MSB, PTS, Riksbanken, Riksgälden och Swedbank. Övningen Cyber Europe 2014 genomförs som en serie av delövningar och avslutas under första kvartalet 2015.

Den 17-21 november 2014 deltog Sverige i övningen Nato Cyber Coalition 2014. I den årligen återkommande multinationella cybersäkerhetsövningen, deltar militära respektive nationella CERT-organisationer och cybercenter. Syftet är att öva sig på att hantera tekniska och operativa cyberincidenter. I år deltog totalt 31 länder inklusive fem partnerländer. Sverige har deltagit i övningen sedan 2011, främst genom Försvarsmakten, men i år deltog både Försvarsmakten och MSB med egna team bestående av cirka tio deltagare vardera. Under övningen befann sig de svenska deltagarna i Sverige och kopplade upp sig mot Natos övningsmiljö.

Mer information:

NISÖ 2012 – erfarenhetsrapport:

https://www.msb.se/RibData/Filer/pdf/27066.pdf

Handbok – Tekniska informations- och cybersäkerhetsövningar:

https://www.msb.se/sv/Forebyggande/Informationssakerhet/Stod-inom-informationssakerhet/-Handbok---Tekniska-informations--och-cybersakerhetsovningar/

Cyber Europe 2014:

https://www.msb.se/sv/Om-MSB/Nyheter-och-press/Nyheter/Nytt-informationssakerhet/30-oktober-deltog-Sverige-i-ovningen-Cyber-Europe-2014/

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe

Nato Cyber Coalition 2014: http://www.nato.int/cps/en/natohq/news_114902.htm?selectedLocale=en

3.4 Åtgärdsförslag relaterade till kommunikationssäkerhet

Förebyggande åtgärder för att öka säkerheten i de elektroniska kommunikationerna	**Åtgärd:** 4.1 **Ansvar:** PTS
Beskrivning (från handlingsplanen): Följande förebyggande åtgärder vad avser fysiska och logiska hot, utbildningar och informationssystem, ska vidtas för att öka driftsäkerheten i elektronisk kommunikation: • Kartläggningar av sårbarheter i stödsystem och nätdelar hos operatörer inom sektorn för elektronisk kommunikation genomföras. • Funktionskontroller på skyddade anläggningar inom sektorn för elektronisk kommunikation genomförs. • Tillträdesskydd vid anläggningar för elektronisk kommunikation stärks. • En nationell krisledningsövning (Telö) för aktörer inom sektorn för elektronisk kommunikation planeras, genomförs och utvärderas. • Det nationella systemet för robust och spårbar tid vidareutvecklas. • Informationssystemen Ledningskollen, Gemensam lägesuppfattning (GLU) och Driftinformation för operatörer (DIO) vidareutvecklas. • Särskilda utbildningsinsatser inom området driftsäkerhet i stadsnät genomförs. • En pilotstudie av samhällsviktiga verksamheters behov av elektronisk kommunikation genomförs.	
Genomfört arbete: Kartläggningen av sårbarheter är slutförd och åtgärder är vidtagna. Funktionskontrollerna på skyddade anläggningar är pågående, analys och prioritering av åtgärdsbehov pågår. Förstärkning av tillträdesskydd slutförs under 2014. En nationell krisledningsövning hölls under 2013 och en slutrapport har publicerats. Förstudier inför Telö 2015 har påbörjats. Det nationella systemet för robust och spårbar tid beräknas vara etablerat under 2015. Informationssystemen Ledningskollen, GLU och DIO är överlämnade till	

förvaltningsråd.

Särskilda utbildningsinsatser inom området driftsäkerhet i stadsnät genomfördes under 2012, 96 stadsnät deltog under 49 utbildningstillfällen. Pilotstudien av samhällsviktiga verksamheters behov av elektronisk kommunikation genomfördes och avrapporterades under 2012.

Mer information:

Telö 13:

http://www.pts.se/upload/Rapporter/Tele/2014/telo-13-pts-fortsatta-arbete-pts-er-2014_14.pdf

Ledningskollen:

http://www.pts.se/upload/Ovrigt/Om-PTS/infomaterial/Ledningskollen-folder-130704.pdf

Gemensam lägesuppfattning (GLU):

http://www.pts.se/upload/Faktablad/SE/2013/Faktablad-GLU-20130301.pdf

Driftinformation för operatörer (DIO):

http://www.pts.se/upload/Faktablad/SE/2013/faktablad-driftinformation-mellan-operatorer-dio-pts-f-2013_3-%202014.pdf

Åtgärder för att följa upp säkerheten i sektorn elektronisk kommunikation	**Åtgärd:** 4.2 **Ansvar:** PTS

Beskrivning (från handlingsplanen):

Viktiga åtgärder som ska vidtas för att öka säkerheten i elektronisk kommunikation är:

- En kontinuerlig vidareutveckling av rutiner för daglig bevakning av driftstörningar och hantering av incidentrapporter.
- En analys av tillsynsmetodik genomförs då nya mandat och verktyg har tillkommit.
- En planlagd tillsyn av driftsäkerheten vid den svenska toppdomänen .SE genomförs.
- Allmänna råd ersätts med föreskrifter om driftsäkerhet.
- Föreskrift om säkerhetsskydd för elektronisk kommunikation tas fram.

Genomfört arbete:

Nya rutiner för daglig bevakning av driftstörningar och hantering av incidentrapporter togs fram under 2013. Samma år genomfördes en analys av tillsynsmetodiken. Den planlagda tillsynen av driftsäkerheten vid den

svenska toppdomänen .SE genomfördes även denna under 2013.

Framtagningen av föreskrifter om driftsäkerhet är pågående och beräknas slutförd under 2015. En förstudie har påbörjats om föreskrifter om säkerhetsskydd för elektronisk kommunikation. Ett förslag till föreskrifter kommer inte att tas fram innan utredningen *En modern säkerhetsskyddslag* har lämnat sitt slutbetänkande (Dir. 2011:94).

Mer information:

Information om driftsäkerhet från PTS:

http://www.pts.se/sv/Bransch/Internet/God-funktion-och-teknisk-sakerhet/

Särskild satsning på införande av DNSSEC	**Åtgärd:** 4.3 **Ansvar:** MSB och PTS

Beskrivning (från handlingsplanen):

Följa upp insatserna som gjordes under 2011 och fortsätta arbetet med att införa DNSSEC för återstående domäner inom offentlig sektor.

Genomfört arbete:

PTS, MSB, Sveriges kommuner och landsting, samt .SE har samverkat kring DNSSEC. Under åren 2012-2014 så har MSB genomfört riktade insatser för att nå ut till kommuner genom länsstyrelserna med bakgrund i deras geografiska områdesansvar och uppmanat till införande av DNSSEC. Under denna period har Länsstyrelserna beviljats medel från anslag 2:4 krisberedskap och cirka 200 kommuner har därigenom kunnat införa DNSSEC.

Bakgrund:

DNS översätter de adresser som dagligen används (exempelvis www.en-kommun.se) till IP-adresser. Utan DNS skulle användare vara hänvisade till att använda IP-adresser, vilket skulle vara mycket svårhanterligt. DNS är därmed en grundläggande förutsättning för att den information och de tjänster som görs tillgängliga på nätet verkligen är nåbara för användarna.

En tidigare genomförd granskning av hur DNS är konfigurerat inom kommuner har visat att det finns utrymme för förbättringar, vilket även framgår av de årliga rapporter som.SE publicerar i serien ”Hälsoläget”. Det förekommer i många fall brister som består av rena fel i förhållande till de specifikationer som gäller för DNS. Detta kan orsaka att berörda servrar i DNS inte fungerar korrekt och exempelvis levererar felaktiga svar, inaktuella svar eller inte svarar alls. Som ett tillägg till DNS har en standard utvecklats som fått beteckningen DNSSEC (DNS Security Extensions). Med DNSSEC säkras domännamnssystemet från missbruk genom att svaren på DNS-uppslagningar signeras kryptografiskt. Detta möjliggör upptäckt av falska

eller manipulerade svar, så att det kan säkerställas att svaren verkligen kommer från rätt källa. Detta är grundförutsättningar för att skapa tilltro till informationen och tjänster på publika webbplatser samt användning av e-post.
Mer information: Vägledning för införande av DNSSEC (från .SE): https://www.informationssakerhet.se/sv/vagledningar/DNSSEC/ Kontaktperson MSB: Ronny Janse

Krypto för skyddsvärda uppgifter	**Åtgärd:** 4.4 **Ansvar:** FM, MSB och FRA
Beskrivning (från handlingsplanen): Föreslå lösningar på ekonomiska och juridiska aspekter vid införande av Krypto för skyddsvärda uppgifter (KSU).	
Genomfört arbete: FM har tillsammans med FRA och MSB utrett uppgiften och tagit fram ett förslag som remissats till ett landsting, en myndighet och en leverantör. Slutrapport är under färdigställande.	
Mer information: Kontaktperson Försvarsmakten: Pia Gruvö	

Utveckla Swedish Government Secure Intranet (SGSI)	**Åtgärd:** 4.5 **Ansvar:** MSB
Beskrivning (från handlingsplanen): Vidmakthålla och i vissa avseenden utveckla säkerhetsarbetet i SGSI. Utveckla tjänster i nätet som efterfrågas av användarna.	
Genomfört arbete: Under 2013 har det genomförts en behovsinventering av tjänster i SGSI som myndigheter efterfrågar och för flera av de identifierade behoven har det under 2014 genomförts pilotprojekt. Bland annat har det genomförts projekt för skyddad internet-access samt projekt för mobila lösningar med syfte att över SGSI få åtkomst till myndighetsintern information via mobila enheter, samt möjlighet till skyddat tal mellan de anslutna myndigheterna.	

Bakgrund:

Swedish Government Secure Intranet (SGSI) är ett kommunikationsnätverk som ger säker kommunikation mellan myndigheter i Sverige och i Europa. SGSI är skilt från internet och trafiken är krypterad, samt att SGSI är utformat för att klara höga krav på tillgänglighet och driftsäkerhet.

Myndigheter som vill kommunicera med EU-administrationen eller med en annan medlemsstat genom sTESTA (secure Trans European Services for Telematics between Administrations, vilket är ett säkert nät mellan EU:s medlemsstater och EU:s olika organ) måste vara anslutna till SGSI. SGSI är Sveriges enda nätverk med koppling till sTESTA och uppfyller EU-rådets och Kommissionens föreskrifter för hantering av information.

Inom Sverige använder myndigheter SGSI som ett säkert nätverk för utbyte av känslig information och minskar därmed risker kopplat till att skicka information över internet. SGSI används bland annat för att få åtkomst till olika databaser hos de olika anslutna myndigheterna och så finns en tjänst för videkonferens inom SGSI.

Mer information:

Swedish Government Secure Intranet (SGSI):

https://www.msb.se/sv/Produkter--tjanster/SGSI---Swedish-Government-Secure-Intranet-/

Kontaktperson MSB: Roger Forsberg

Tillgängliga och skyddade kommunikations-infrastrukturer för offentlig sektor	**Åtgärd:** 4.6 **Ansvar:** SAMFI

Beskrivning (från handlingsplanen):

Fortsatt arbete med tillgängliga och skyddade kommunikations-infrastrukturer för offentlig sektor.

Genomfört arbete:

Frågan om tillgängliga och skyddade kommunikationsinfrastrukturer för offentlig sektor bereds i Regeringskansliet. MSB redovisade ett regeringsuppdrag i frågan i mars 2011 och har sedan dess fortsatt arbeta med myndighetens befintliga externa kommunikationstjänster för samverkan och ledning, bl a SGSI (ovan) samt Rakelsystemet.

Bakgrund:

MSB fick 2010 i uppdrag av regeringen att lämna förslag på en säker digital informations- och kommunikationsinfrastruktur för myndigheter, kommuner och landsting. I mars 2011 lämnade MSB sitt förslag på hur en tillgänglig och skyddad kommunikationsinfrastruktur för offentlig sektor skulle kunna skapas. Förslaget går i stort ut på att skapa en sammanhållande organisatorisk

struktur med uppdrag att samordna, inrikta, ansvara för drift och förvalta. Vissa delar av infrastrukturen ska enligt MSB:s förslag tillhandahållas genom staten och andra genom näringslivet.
Mer information: Tillgänglig och skyddad kommunikationsinfrastruktur for offentlig sektor: https://www.msb.se/Upload/Nyheter_press/Tillganglig_och_skyddad_kommunikationsinfrastruktur_for_offentlig_sektor.pdf Rakelsystemet: https://www.msb.se/sv/Produkter--tjanster/Rakel/Om-Rakel/Vad-ar-Rakel/

3.5 Åtgärdsförslag relaterade till säkerheter i produkter och system

Utveckla ett kryptogranskningsregelverk för kommersiella produkter	**Åtgärd:** 5.1 **Ansvar:** FMV/CSEC, FM och MSB
Beskrivning (från handlingsplanen): Utveckla ett kryptogranskningsregelverk inom FMV/CSEC certifieringsordning. Ta fram uppgifter och dokumentation, exempelvis protokoll, som kan användas inom ramen för KSU-godkännande från försvarsmakten. Licensiera evalueringsföretag att genomföra kryptogranskning enligt de av FMV/CSEC utvecklade, och av Försvarsmakten godkända, kryptoregelverket.	
Genomfört arbete: FMV/CSEC har i samverkan med Försvarsmakten utvecklat en preliminär granskningsprocess för kryptografiska funktioner i samband med Common Criteria-evaluering av produkter, Cryptographic Validation Program (CVP). CVP är avsett att vara ett underlag för KSU-godkännande av MUST. Granskningsprocessen introducerar följande moment i en CC-certifiering: • Kryptoterminologi • Krav på kryptokompetens hos granskarna. • Krav på hur krypto specificeras. • Krav på beskrivning av kryptonycklars livscykel i IT-produkter. • Krav på granskning av kryptofunktioner. • Krav på sårbarhetsanalys.	

- Krav på penetrationstestning.
- Modell för specificering av slumptalsgeneratorer.

En åtgärdslista med förslag på ytterligare utveckling av CVP finns framtagen.

Dessa underlag kommer delges övriga SAMFI-myndigheter för information och diskussion. FMV/CSEC i samverkan med Försvarsmakten beslutar sedan om fortsatt arbete.

Mer information:

Kontaktperson FMV/CSEC: Dag Ströman

Kontaktperson MSB: Ronny Janse

Dokument från FMV/CSEC:

- Missiv CVP, FMV dnr 14FMV10129-3:1
- Cryptographic Validation Program (CVP), FMV dnr 14FMV10129-1:1
- Restlista CVP, FMV10129-2:1

Ökad användning av CC-evaluerade produkter	**Åtgärd:** 5.2 **Ansvar:** MSB, FMV/CSEC och FM

Beskrivning (från handlingsplanen):

Utveckla och certifiera skyddsprofiler. Ta fram föreskrift från MSB med krav på it-produkters säkerhetsegenskaper, baserade på kraven i certifierade skyddsprofiler. Ta fram råd och anvisningar för hur verksamheter kan använda produkter som certifieras för att uppnå god informationssäkerhet.

Genomfört arbete:

FMV/CSEC, MSB och Försvarsmakten har arbetat tillsammans med de andra myndigheterna i SAMFI kring kravställning av it-säkerhetsprodukter baserat på standarden Common Criteria. Common Criteria Recognition arrangement (CCRA) reformererades under 2014 vilket ändrade processen för hur kravställningar produceras och hur aktörer ska jobba med standarden. Inom ramen för arbetet i SAMFI:s arbetsgrupper har löpande anpassningar skett mot det nya CCRA och kravställning på it-produkter med hänsyn till den nya utvecklingen. SAMFI, genom MSB, har deltagit i tre International Technical Communities (iTC) för kravställning på USB-stickor, brandväggar samt full-disk-kryptering. Den förändrade CCRA-processen har inneburit att MSB:s arbete med att ta fram en föreskrift på området har försenats och en föreskrift tidigast kommer att kunna träda i kraft 2016.

Bakgrund:

Common Criteria (CC) är en internationellt erkänd standard med standardbeteckningen ISO/IEC IS 15408. CC är ett ramverk som används vid kravställning och utvärdering av produkters it-säkerhet. CC används för opartisk granskning av it-säkerhet. Standarden erkänns internationellt av världens ledande länder inom it-säkerhet. CC utvecklades i nära samarbete mellan flera länders säkerhetsmyndigheter och anses vara obligatoriskt för it-produkter i kritiska infrastrukturer i flera länder. CC tillämpas inom flera olika samhällssektorer, exempelvis försvar, finans, sjukvård, transport och kommunikation. Den huvudsakliga utvecklingen av standarden sker inom den internationella organisationen Common Criteria Recognition arrangement (CCRA).

Mer information:

Information om Common Critieria:

http://www.commoncriteriaportal.org/

Information om säkra it-produkter:

https://www.informationssakerhet.se/sv/regelverk/Sakra-IT-produkter/

Kontaktperson FMV/CSEC: Dag Ströman

Kontaktperson MSB: Ronny Janse

Nationellt evalueringslaboratorium	**Åtgärd:** 5.3 **Ansvar:** FMV/CSEC, FM och FRA

Beskrivning (från handlingsplanen):

Analysera förutsättningarna för ett nationellt evalueringslaboratorium med nödvändig kompetens och utrustning för att analysera fysiska attacker mot information i datorutrustning.

Genomfört arbete:

FMV/CSEC har gjort en analys vilken redovisats i en preliminär rapport. Rapporten innehåller en analys av förutsättningarna för ett nationellt evalueringslaboratorium som besitter nödvändig kompetens och har rätt utrustning för att analysera fysiska attacker mot information i dator-utrustning. Rapporten ger en fördjupad bakgrund till de säkerhetsområden som ett nationellt hårdvarulaboratorium kan hantera. Rapporten beskriver också vilka resurser (i form av miljöparametrar, lokaler, utrustning, personal och utbildning) som ett sådant laboratorium måste ha till sitt förfogande. Rapporten visar på olika möjliga vägar att bygga upp dessa resurser samt beskriver vilka nationella och internationella resurser som skulle kunna

användas för att bygga upp de resurser som behövs.

Rapport är baserad på litteraturstudier, studiebesök, arbetsmöten och diskussioner med Försvarsmakten och FRA.

Studiebesök har utförts på ett laboratorium i Storbritannien som utför evaluering av hårdvaruprodukter inom ramen för SOGIS MRA.

FMV/CSEC har i samverkan med FRA och Försvarsmakten även besökt Ångström Microstructure Laboratory vid Uppsala universitet.

Rapporten omfattar bl a:

- Exempel på scenario där fysiska attacker genomförs
- Exempel på hur attacker genomförs.
- Exempel på olika former av skydd mot fysiska attacker.
- Verktyg som används för att genomföra attacker
- Internationellt arbete inom området
- Samverkan inom Europa för att certifiera produkter, SOGIS-MRA
- Krav på en certifieringsordning för hårdvaruevaluering
- Krav Evalueringslaboratorium, inklusive personal, utrustning, utbildning, lokaler, datorutrustning och nätverk
- Möjlig väg för att etablera en certifieringsordning för hårdvaruevaluering

Arbete med rapporten pågår fortfarande och den kommer att färdigställas under första kvartalet 2015.

Mer information:

Preliminär rapport från FMV/CSEC:

- Missiv - Nationellt evalueringslaboratorium, 14FMV10139-2:1
- Rapport, Nationellt evalueringslaboratorium, 14FMV10139-1:1
- Restlista - Nationellt evalueringslaboratorium, 14FMV10139-3:1

Rapporten färdigställs under 2015.

Kontaktperson FMV/CSEC: Dag Ströman

Ökad säkerhet i industriella informations- och styrsystem (SCADA)	**Åtgärd:** 5.4 **Ansvar:** MSB

Beskrivning (från handlingsplanen):

Fortsätta att genomföra det program för ökad säkerhet i industriella

informations- och styrsystem (SCADA) som initierades av MSB 2010 och kommer att löpa till slutet av 2012. Programmet utgör en samordnad nationell, tvärsektoriell, satsning vilket möjliggör ett effektiv resursutnyttjande och ökar förutsättningarna för att tillvarata de satsningar som görs inom olika sektorer av ansvariga myndigheter. Särskilt viktiga områden är informationssäkerhet i elförsörjningen och i transportsystem.

Planera, genomföra och utvärdera ett program för ökad säkerhet i industriella informations- och styrsystem 2013-15.

Genomfört arbete:

MSB driver ett program för att öka den nationella förmågan att förebygga och hantera it-relaterade hot mot industriella informations- och styrsystem i samhällsviktiga verksamheter och i kritisk infrastruktur. Programmet har som mål att utveckla privat-offentlig samverkan, att utöka den tekniska kompetensen i frågorna, sprida information och praktiskt stödja användare av informations- och styrsystem för att öka säkerheten.

En central del i programmet är samarbetet mellan Totalförsvarets forskningsinstitut (FOI) i Linköping och MSB för att bygga upp en plattform för att öka den tekniska förmågan i samhället. Samarbetet bedrivs i dag under namnet NCS3 (Nationellt centrum för säkerhet i samhällsviktiga styrsystem) och verksamheten genomför bland annat praktiska utbildningar och övningar, utvecklar utbildnings- och övningskoncept, utför tekniska studier och utvecklar demonstratorer. Under 2012-14 har den tekniska och pedagogiska miljön vid NCS3 utvecklats och förbättrats. Nya utbildnings- och övningskoncept har tagits fram och riktade kurser för operatörer inom bland annat elproduktion, transport och kärnkraft har genomförts. En kurs för de nordiska nationella CERT-funktionerna har utveckats och genomförs i december 2014. Vidare har ett antal tekniska studier genomförts och ett tekniskt samarbetsprojekt mellan Idaho National Lab och FOI genomförs för närvarande.

Arbetet i programmet rör även medvetandehöjning, samverkan och informationsdelning. I detta ingår att ta fram praktiskt stöd för att öka säkerheten i industriella informations- och styrsystem. Exempelvis har en ny version (3:e utgåvan) av vägledningen om säkerhet i industriella informations- och styrsystem givits ut på såväl svenska som engelska. Vägledningen har i dag fått en mycket bred spridning både nationellt och internationellt och MSB samverkar även internationellt kring ramverk och good practice. För närvarande sker ett arbete för att ta fram en e-utbildning baserad på vägledningen. Programmet har även genomfört ett antal studier utanför NCS3, bl a rörande GNSS och säkerhet i inbyggda system. Det nationella privat-offentliga informationsdelningsforumet FIDI-SCADA fortsätter att vara en central komponent i programmet och möten genomförs regelbundet i forumet. Det internationella samarbetet har utvecklats inom området och programmet deltar i ett flertal forum och samarbetsprocesser, både inom EU och internationellt.

Programmet omfattar inte renodlad forskning och utveckling, men en viktig

del av arbetet är att verka för att öka forskningen inom området. MSB genomför för närvarande en forskningsutlysning inom området (Åtgärd 2.3) och programmet deltar aktivt i inriktnings- och utlysningsarbetet.
Mer information: MSB:s program för säkerhet i industriella informations- och styrsystem: https://www.msb.se/scada Nationellt centrum för säkerhet i samhällsviktiga styrsystem (NCS3): http://www.foi.se/sv/Var-kunskap/Informationssakerhet-och-Kommunikation/NCS3/

4. Fortsatt arbete

Arbetet med att genomföra de åtgärdsförslag som presenteras i den nationella handlingsplanen kommer att avslutas 2015. I samband med detta kommer en sammanfattande rapport av genomfört arbetet att presenteras.

Myndigheten för samhällsskydd och beredskap
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ.nr MSB800 – december 2014 ISBN 978-91-7383-528-2