Samlad informations- och cybersäkerhetshandlingsplan 2019–2022

Redovisning mars 2020

Myndigheten för samhällsskydd och beredskap
FRA
FMV
FÖRSVARSMAKTEN
PTS
Polisen
Säkerhetspolisen

Samlad informations- och cybersäkerhetshandlingsplan för åren 2019 – 2022 – redovisning 2020

Foto omslag: Shutterstock
Tryck: DanagårdLiTHO
Produktion: Advant

Publikationsnummer: MSB1478 - mars 2020
ISBN: 978-91-7927-001-8

Innehåll

Sammanfattning

Sammanfattning

Denna samlade informations- och cybersäkerhetshandlingsplan innehåller åtgärder som Myndigheten för samhällsskydd och beredskap (MSB), Försvarets radioanstalt (FRA), Försvarets materielverk (FMV), Försvarsmakten, Post- och telestyrelsen (PTS), Polismyndigheten och Säkerhetspolisen enskilt, tillsammans eller i samverkan med andra aktörer avser att vidta för att höja informations- och cybersäkerheten i samhället. I 2020 års redovisning har ett antal åtgärder avslutats, vissa har uppdaterats och några har tillkommit. Utvalda resultat av genomförda åtgärder beskrivs i kapitlet ”Uppföljning”.

Åtgärderna i handlingsplanen ligger inom ramen för de ansvarsområden och uppdrag som myndigheterna har. Handlingsplanen ska dock inte ses som en komplett redovisning av alla de åtgärder som de olika myndigheterna avser att genomföra inom sina respektive verksamheter på informations- och cybersäkerhetsområdet.

Samtliga åtgärder i handlingsplanen ansluter till någon eller några av de sex strategiska prioriteringar som regeringen beslutat i den nationella strategin för samhällets informations- och cybersäkerhet (skr. 2016/17:213). Huvuddelen av åtgärderna syftar till att

- säkerställa en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet,
- öka säkerheten i nätverk, produkter och system samt
- stärka förmågan att förebygga, upptäcka och hantera cyberattacker och andra it-incidenter.

Av redovisningen framgår vilken myndighet som är ansvarig för respektive åtgärd, vilka som deltar i arbetet samt vad åtgärden omfattar.

Introduktion

Introduktion

I juli 2018 gav regeringen myndigheterna med ett särskilt utpekat ansvar inom informations- och cybersäkerhet, MSB, FRA, FMV, Försvarsmakten, PTS, Polismyndigheten och Säkerhetspolisen, i uppdrag att ta fram en samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022.

Myndigheterna i detta uppdrag har centrala ansvarsområden och uppdrag i arbetet med informations- och cybersäkerhet i samhället. De har också en etablerad samverkansstruktur genom Samverkansgruppen för informationssäkerhet (SAMFI). Regeringen anser att en fördjupad samverkan mellan dessa myndigheter är en förutsättning för att stärka Sveriges förmåga till skydd mot cyberattacker och andra allvarliga it-incidenter. Handlingsplanen bidrar till att ge regeringen ett bättre underlag för att kunna analysera om myndigheternas planerade åtgärder är tillräckliga för att nå målsättningarna i den nationella strategin och vilka ytterligare åtgärder regeringen behöver vidta. Enligt regeringen bör den samlade handlingsplanen syfta till att det sker en samordning avseende myndigheternas åtgärder och aktiviteter.

Handlingsplanen utgör en samlad redovisning av vilka åtgärder myndigheterna på eget initiativ planerar att vidta inom ramen för sina befintliga ansvarsområden och uppdrag för att bidra till att uppfylla de strategiska prioriteringarna i den nationella strategin. Handlingsplanen utgör inte ett styrande dokument för myndigheternas verksamhet.

Arbetet med åtgärderna i handlingsplanen ska rapporteras årligen till regeringen den 1 mars. MSB är enligt regeringsuppdraget sammanhållande för denna rapportering. Uppdraget slutredovisas den 1 mars 2023. Denna rapportering ersätter inte myndigheternas ordinarie redovisning till regeringen.

Åtgärderna genomförs inom givna ekonomiska ramar, antingen av en myndighet enskilt eller i gemensamma projekt. Löpande arbete med informations- och cybersäkerhet redovisas där det bedöms relevant. Planen ska därför inte ses som en komplett redovisning av alla de åtgärder som de olika myndigheterna avser att genomföra inom sina respektive verksamhetsområden.

Nationell strategi

I den nationella strategin för samhällets informations- och cybersäkerhet (skr. 2016/17:213) uttrycker regeringen övergripande prioriteringar vilka syftar till att utgöra en grund för Sveriges fortsatta utvecklingsarbete inom informations- och cybersäkerhetsområdet. Huvudsyftet med strategin är att bidra till att skapa långsiktiga förutsättningar för samhällets aktörer att arbeta effektivt med informations- och cybersäkerhet samt att höja medvetenheten och kunskapen i hela samhället. Vidare syftar strategin till att stödja de redan pågående insatserna som genomförs med målet att stärka samhällets informations- och cybersäkerhet. I strategin redogörs även för vad som ska skyddas och vilka hot och risker som finns.

Strategin omfattar sex strategiska prioriteringar:

1. Säkerställa en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet.
2. Öka säkerheten i nätverk, produkter och system.
3. Stärka förmågan att förebygga, upptäcka och hantera cyberattacker och andra it-incidenter.
4. Öka möjligheterna att förebygga och bekämpa it-relaterad brottslighet.
5. Öka kunskapen och främja kompetensutvecklingen.
6. Stärka det internationella samarbetet.

Strategin omfattar hela samhället, det vill säga statliga myndigheter, kommuner och regioner, företag, organisationer och privatpersoner.

Översikt över de strategiska prioriteringar och tillhörande målsättningar som anges i den nationella strategin för samhällets informations- och cybersäkerhet:

Säkerställa en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet

- Statliga myndigheter, kommuner, regioner, företag och andra organisationer ska ha kännedom om hot och risker, ta ansvar för sin informationssäkerhet och bedriva ett systematiskt informationssäkerhetsarbete.
- Det ska finnas en nationell modell till stöd för ett systematiskt informationssäkerhetsarbete.
- Samverkan och informationsdelning på informations- och cybersäkerhetsområdet ska stärkas.
- Det ska finnas en ändamålsenlig tillsyn som skapar förutsättningar för en ökad informations- och cybersäkerhet i samhället.

Öka säkerheten i nätverk, produkter och system

- Elektroniska kommunikationer ska vara effektiva, säkra och robusta samt tillgodose användarnas behov.
- Elektronisk kommunikation i Sverige ska vara tillgänglig oberoende av funktioner utanför landets gränser.
- Tillsynsmyndighetens behov av att kunna vidta adekvata åtgärder ska säkerställas.
- Tillgången till säkra kryptosystem för it- och kommunikationslösningar ska motsvara behoven i samhället.
- Säkerheten i industriella informations- och styrsystem ska öka.

Stärka förmågan att förebygga, upptäcka och hantera cyberattacker och andra it-incidenter

- Förmågan att förebygga, upptäcka och hantera cyberattacker och andra it-incidenter i samhället ska förbättras.
- Berörda aktörer ska kunna agera samordnat för att hantera cyberattacker och andra allvarliga it-incidenter.
- Det ska finnas ett utvecklat cyberförsvar för Sveriges mest skyddsvärda verksamheter med en förstärkt militär förmåga att möta och hantera angrepp från kvalificerade motståndare i cyberrymden.

Öka möjligheterna att förebygga och bekämpa it-relaterad brottslighet

- De brottsbekämpande myndigheterna ska ha beredskap och förmåga att bekämpa it-relaterade brott på ett effektivt och ändamålsenligt sätt.
- Arbetet med att förebygga it-relaterade brott ska utvecklas.

Öka kunskapen och främja kompetensutvecklingen

- Kunskapen i samhället som helhet om de mest angelägna sårbarheterna och behoven av säkerhetsåtgärder ska öka.
- Kunskapen hos enskilda användare av digital teknik om de mest angelägna sårbarheterna och behoven av säkerhetsåtgärder ska öka.
- Det ska bedrivas högre utbildning, forskning och utveckling av hög kvalitet rörande informations- och cybersäkerhet och säkerhet på it- och telekomområdet i Sverige.
- Det ska regelbundet genomföras både tvärsektoriella och tekniska informations- och cybersäkerhetsövningar i syfte att stärka Sveriges förmåga att hantera konsekvenserna av allvarliga it-incidenter.

Stärka det internationella samarbetet

- Internationella samarbeten kring cybersäkerhet ska stärkas, inom ramen för målsättningen om ett globalt, tillgängligt, öppet och robust internet som präglas av frihet och respekt för mänskliga rättigheter.
- Cybersäkerhet ska främjas inom ramen för ambitionen att värna fria flöden till stöd för innovation, konkurrenskraft och samhällsutveckling.

Myndigheternas arbete med handlingsplanen

Arbetet med 2020 års handlingsplan påbörjades under våren 2019 och har bedrivits i den gemensamma arbetsgrupp som SAMFI-myndigheterna etablerade inför arbetet med förra årets redovisning av handlingsplanen. Jämfört med förra året har gruppen riktat ett ökat fokus mot uppföljning av arbetet med åtgärderna i handlingsplanen. Myndigheterna har även som ett led i detta arbetat med att ytterligare förtydliga existerande åtgärder avseende innehåll och förväntad effekt. I årets handlingsplan redovisas uppföljningen av genomfört arbete samlat och på övergripande nivå i anslutning till respektive strategisk prioritering. Metoden kan utvecklas ytterligare för att stödja en fördjupad analys av åtgärdernas effekt på samhällets säkerhet.

I arbetet med handlingsplanen har även en utökad samverkan skett med både privata och offentliga aktörer. Syftet var både att förankra och utveckla handlingsplanen och att identifiera behov av nya åtgärder. Denna samverkan har varit värdefull och redovisas närmare i kapitlet ”Extern samverkan”. För att ytterligare utveckla myndigheternas förmåga att både identifiera och hantera behoven i samhället har SAMFI-myndigheterna i arbetet med 2020 års redovisning riktat särskilt fokus mot två åtgärder. Utvecklingen av ett nationellt cybersäkerhetscenter samt etableringen av en nationell modell för systematiskt informationssäkerhetsarbete är två exempel på plattformar för sådant samarbete och skapar förbättrad möjlighet att svara mot aktörernas behov på sikt. Arbetet med båda dessa åtgärder involverar samtliga SAMFI-myndigheter och syftar till att säkerställa att dessa myndigheters kunskap och kompetens nyttjas på ett mer samlat sätt för att stödja både privata och offentliga aktörer.

Nyheter i redovisning mars 2020

Årets redovisning av handlingsplanen innehåller flera nyheter:

- Ett nytt kapitel som tydligare beskriver den externa samverkan som skett i arbetet med 2020 års redovisning av handlingsplanen.
- Ett nytt uppföljningskapitel som sammanfattar utvalda resultat av arbetet med handlingsplanens åtgärder 2019.
- Ett antal nya åtgärder som dels utgör fortsättning på vissa avslutade åtgärder, dels möter nya behov som identifierats.
- Uppdaterade bilagor där åtgärderna sorteras och grupperas på nya sätt för att underlätta spårbarhet över tid och för ökad överskådlighet.

Extern samverkan

Extern samverkan

I regeringens uppdrag till SAMFI-myndigheterna understryks behovet av extern samverkan för att möjliggöra samordning avseende myndigheternas åtgärder och aktiviteter i handlingsplanen. Myndigheten för digital förvaltning (DIGG), Datainspektionen, tillsynsmyndigheterna av NIS-regleringen inklusive Socialstyrelsen är utpekade för samverkan i uppdraget. Samverkan med andra aktörer bidrar till att identifiera behov och förstärker genomförandet av åtgärder i handlingsplanen. I arbetet med 2020 års handlingsplan har den externa samverkan utökats.

Vid tre tillfällen genomfördes bred extern samverkan med syfte att identifiera behov av uppdatering eller tillägg samt för att förstärka samverkansmöjligheter i genomförandet av åtgärder i handlingsplanen. Ett 50-tal representanter för branschorganisationer, standardiseringsorgan, universitet och centrala myndigheter, länsstyrelser, företag samt regioner och kommuner deltog.

Vid samverkansmötena pekade aktörerna inte bara på olika behov av stöd och inriktning utan formulerade även en rad konkreta förslag på nya åtgärder. Mängden synpunkter och förslag är en indikation på ett stort engagemang kring handlingsplanen.

Ett flertal behov som lyftes, exempelvis rörande samordning av stöd och krav, utökat stöd i bedömning av hot och risker samt förebyggande av it-incidenter, förutsätter än närmare samarbete mellan SAMFI-myndigheterna.

Totalförsvarsperspektivet sågs som naturligt i handlingsplanen och kan förtydligas ytterligare, liksom forskning och utveckling samt näringslivets roll.

Ytterligare resursförstärkning hos SAMFI-myndigheterna kan bli nödvändig de kommande åren för att fullt ut kunna svara upp mot det behov som uttryckts vid extern samverkan.

Inför kommande redovisningar planeras externa samverkansmöten vid fler tillfällen och med bredare frågeställningar. Möjligheten för samhällets aktörer att bidra till behovsbilden inom området och fördjupad samverkan vid genomförandet av handlingsplanens åtgärder är av stor vikt för arbetet med handlingsplanen.

Uppföljning

Uppföljning

Inför 2020 års redovisning av handlingsplanen har SAMFI-myndigheterna gjort en gemensam uppföljning av 2019 års arbete där man har sammanfattat utvalda resultat av arbetet med handlingsplanens åtgärder 2019. I uppföljningen redovisas vad som redan åstadkommits för att möta regeringens sex strategiska prioriteringar. Oftast beskrivs målbild och förväntade resultat för de åtgärder som ryms inom respektive strategisk prioritering.

Uppföljningen presenteras för att kunna ge en överskådlig bild av vad som åstadkommits från år till år. I kommande års uppdaterade handlingsplaner avser myndigheterna att fortsätta denna gemensamma uppföljning.

Uppföljningen rör endast arbetet med handlingsplanens åtgärder och inte myndigheternas övriga arbete på området.

I 2020 års redovisning har ett flertal åtgärder uppdaterats. Det handlar om förändringar i innehåll eller tidplan.

Strategisk prioritering 1. Säkerställa en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet

Under det gångna året har myndigheterna genomfört en rad olika åtgärder som banat väg för en mer systematisk och samlad ansats i arbetet med informations- och cybersäkerhet hos viktiga aktörer i samhället. Genom riktad utbildning, etablerandet av nya samverkansforum, nya säkerhetsskyddsföreskrifter och vägledningar har insatser gjorts för att öka säkerheten i hanteringen av information – från de mest skyddsvärda till den bredare mängden information som dagligen hanteras hos olika samhällsaktörer. Inför Totalförsvarsövningen 2020 har MSB och Försvarsmakten genomfört en efterfrågad utbildning i informationssäkerhet och skyddad kommunikation för bevakningsansvariga myndigheter, vilket ska ha skapat förutsättningar för ett säkrare genomförande av övningen.

SAMFI-konferensen Informationssäkerhet för offentlig sektor arrangerades för tionde året i rad. Antal platser utökades från 600 till 750 för att möta den stora efterfrågan.

Genom att ha arbetat med standarder för både it-produkter och terminologi, och för ett ökat tillämpande av dessa, har förutsättningar för både ökad effektivitet och stärkt informationssäkerhet i hela samhället skapats.

MSB har, i samverkan med FMV, etablerat en referenslista över rekommenderade skyddsprofiler. Den är ett stöd till offentliga aktörer vid anskaffning av it-säkerhetsprodukter och ska bidra till att öka det grundläggande it-säkerhetsskyddet inom svensk statsförvaltning och samhällsviktig verksamhet. Aktörer som i sitt systematiska informationssäkerhetsarbete väljer produkter från referenslistan kan ha tilltro till it-säkerhetsprodukternas faktiska funktionalitet och att de uppfyller de krav som är ställda. Förvaltningen av referenslistan kommer att gå in i MSB:s löpande arbete för vidareutveckling av stöd inom it-säkerhet.

SAMFI-myndigheterna genomför gemensamt en förstudie om en nationell modell för systematiskt informationssäkerhetsarbete och identifierar i det arbetet de centrala delarna i en sådan modell. Den nationella modellen avser att bland annat skapa förutsättningar för ett samlat, samordnat och effektivt arbete med samhällets informationssäkerhet samt att höja lägsta nivån för informationssäkerhet.

Säkerhetspolisen och FRA har inom ramen för arbetet till skydd för särskilt skyddsvärd verksamhet börjat utveckla en gemensam lägesbild kring skyddsvärden, hot och sårbarheter.

Det fördjupade samarbetet mellan FRA, Säkerhetspolisen, Försvarsmakten och MSB som skett under 2019 är utgångspunkt för regeringens uppdrag inför inrättandet av ett nationellt cybersäkerhetscenter. Samverkan har under 2019 formaliserats i en överenskommelse. Myndigheterna har även lämnat en gemensam uppdragsredovisning till regeringen som underlag för inrättandet av ett cybersäkerhetscenter. Arbetet har skett i nära samverkan med Polismyndigheten, FMV och PTS.

Strategisk prioritering 2. Öka säkerheten i nätverk, produkter och system

Under 2019 har flera åtgärder genomförts som samlat gett flera viktiga aktörer inom framförallt offentlig sektor möjligheten att ytterligare säkra kommunikationen av skyddsvärd information internt och sinsemellan. Tilläggstjänsten Sekretess har lanserats i Rakel (ej godkänd för säkerhetsskyddsklassificerad information).

Försvarsmakten och FMV har genom kravställning på nya respektive vidareutveckling av befintliga signalskyddsystem skapat bättre förutsättningar för tillgång till behovsanpassade signalskyddssystem som håller en adekvat säkerhetsnivå med hänsyn till den kryptologiska utvecklingen. Detta förväntas resultera i bättre möjligheter till ett adekvat skydd för kommunikation av information i elektronisk form.

I samarbete med en svensk teleoperatör har FRA under året genomfört testverksamhet för att säkerställa att äldre analoga kryptofax- och kryptotelefonisystem fungerar i dagens IP-baserade telenät.

PTS har analyserat möjligheter till att öka spårbarheten i betrodda tjänster, exempelvis elektroniska underskrifter och stämplar. Analysen har diskuterats med europeiska tillsynsmyndigheter. Frågan kommer att lyftas av flera tillsynsmyndigheter i samband med den pågående översynen av eIDAS-förordningen. Det förväntade resultatet av åtgärden, på lång sikt, är ett ökat skydd i transaktioner baserade på kvalificerade certifikat.

I syfte att öka säkerheten i nätverk har PTS tillsammans med teleoperatörer tydliggjort vilka egenskaper som ur ett regionalt perspektiv bör eftersträvas för att öka motståndskraft och uthållighet i allmänt tillgängliga elektroniska kommunikationsnät.

Strategisk prioritering 3. Stärka förmågan att förebygga, upptäcka och hantera cyberattacker och andra it-incidenter

Under 2019 har Säkerhetspolisen, FRA och Försvarsmakten genom samverkan ökat de egna förmågorna att förebygga, upptäcka och hantera cyberattacker från kvalificerade hotaktörer. FRA har, i samverkan med Säkerhetspolisen, tillgängliggjort Tekniskt detekterings- och varningssystem (TDV) till fler av de mest skyddsvärda verksamheterna. Genom denna åtgärd har förmågan att förebygga, upptäcka och hantera cyberattacker mot våra mest skyddsvärda verksamheter stärkts. Försvarsmakten har dessutom med stöd av FRA utvecklat sin förmåga att genomföra såväl defensiva som offensiva operationer mot en kvalificerad motståndare i cybermiljön.

MSB har tillsammans med Försvarsmakten och Totalförsvarets forskningsinstitut (FOI) fortsatt utvecklingen av en Nationell Cyber Range (NCR) som ett led i en gemensam strategi för NCR. Arbetet leder till en modern och flexibel plattform för övning, utbildning och forskning samt tester. Den utvecklade NCR kommer att invigas under 2020.

Strategisk prioritering 4. Öka möjligheterna att förebygga och bekämpa it-relaterad brottslighet

Polismyndigheten och MSB har etablerat en process för samarbete kring incidentrapportering. Den effektiviserade informationsdelningen mellan myndigheterna leder till en snabbare hantering och ökad kvalitet – både i den proaktiva informationsdelningen till samhällsaktörer och vid inträffade incidenter. MSB verkar för att den som drabbats av en it-relaterad brottslig handling själv polisanmäler händelsen. MSB/CERT-SE stöttar Polismyndigheten i vissa utredningar. Tack vare detta samarbete kan handläggningstiden förkortas, och ett lärande och kompetensutveckling kan ske hos båda myndigheterna till gagn för samhället i stort och brottsbekämpningen specifikt.

Genom Polismyndighetens etablerande av regionala it-brottscentrum i alla sju polisregioner har det skapats större möjligheter till ökat inflöde av it-relaterade frågor från utredare, och med det en stärkt kompetensutveckling. För att öka kvaliteten i brottsutredningar där digital bevisning är en viktig del i utredningsarbetet har Åklagarmyndigheten och Polismyndigheten genomfört gemensamma kurser.

Genom informationskampanjen ”Tänk Säkert” har MSB och Polismyndigheten under 2019 nått ut med viktig information om hur individer och småföretagare kan skapa ett säkrare beteende på nätet. Kampanjen fick nationell räckvidd

och stort genomslag delvis beroende på det höga engagemanget från ett 50-tal externa aktörer från privat och offentlig sektor. I en efterföljande enkät svarade en stor andel av de som sett kampanjen att den varit intresseväckande, höjt medvetenheten och ökat kunskapen. Försvarsmaktens kampanj (som redovisas under prioritering 5) har ytterligare spridit kunskap om hur och varför information behöver skyddas hos dem som jobbar med känsliga uppgifter inom främst försvarssektorn.

Polismyndigheten har genom samarbete med finans- och transaktionsmarknaden bland annat bidragit till att banker kunnat införa krav på att person och dator måste befinna sig på samma fysiska plats vid vissa bankärenden. Detta borgar för en högre säkerhet i betalsystemet.

Strategisk prioritering 5. Öka kunskapen och främja kompetensutvecklingen

FRA har under året ökat kunskap och kompetens inom analys av hårdvarurelaterade hot och sårbarheter. Analysförmågan har redan kommit till användning inom ramen för FRA:s stödverksamhet inom teknisk it-säkerhet. Försvarsmakten har fokuserat på forskning inom bland annat AI, övervakningsfunktioner och innovation för att skapa möjlighet till tillämpbara lösningar för stärkt cybersäkerhet i både Försvarsmakten och resten av samhället.

Försvarsmakten har även genomfört en intern informationskampanj som förväntas ge ett högre säkerhetsmedvetande hos medarbetarna kring hanteringen av information och därmed bidra till att skyddsvärd information exponeras i mindre grad än tidigare. Kampanjen riktades främst till anställda inom Försvarsmakten men har också kunnat användas av andra aktörer i samhället.

FRA, Säkerhetspolisen och Försvarsmakten har kontinuerligt samverkan kring kompetensförsörjning. Bland annat har myndigheterna gemensamt genomfört rekryteringsfrämjande aktiviteter på arbetsmarknadsdagar. För att ytterligare tillföra kompetens till cyberförsvaret har Försvarsmakten börjat med det arbete som ska etablera en pliktutbildning, som på sikt inte bara kommer Försvarsmakten tillgodo utan även andra myndigheter som till exempel FRA. Inskrivning av värnpliktiga för mönstring till cybersoldatutbildning har påbörjats.

Försvarsmakten genomför forskning och teknikutveckling inom områdena cyberförsvar och informationssäkerhet (FoT Cyber) som syftar till ett stärkt cyberförsvar och att utveckla förmågor för att kunna genomföra alla typer av dator- och nätverksoperationer i cybermiljön, liksom förmågan att utveckla och upprätthålla erforderlig informations- och it-säkerhet i Försvarsmaktens tekniska metodstödsystem. Verksamheten bedrivs huvudsakligen vid FMV, FOI, FHS och KTH. Verksamheten präglas av samarbete mellan aktörerna och utpekade nationella och internationella partners.

För att intressera ungdomar för it-säkerhet och ge inblick i FRA:s övriga verksamhet har gymnasielever fått möjlighet att spendera en sommarvecka hos myndigheten. FRA har även etablerat en poddradio om cyberförsvar.

Under 2019 har ett antal övningar genomförts. Försvarsmakten har genomfört övningen SAFE Cyber 2019 som riktade sig till myndigheter med ansvar för cybersäkerhet i Sverige samt till myndigheter och företag som ansvarar för system och tjänster kopplade till Försvarsmakten. Syftet och målet med övningen var bland annat att öva riskhantering och beslutsfattande, öva hantering av incidenter samt samverkan.

Strategisk prioritering 6. Stärka det internationella samarbetet

Genom stärkt internationell samverkan under 2019 har FMV bidragit till att ta fram ett ramverk för stöd till att hantera cyberhot, sårbarheter och motåtgärder – något som kan användas av säkerhetsexperter inom både stat och näringsliv. Arbetet är ett resultat av ett samarbete inom Multinational Industrial Security Working Group (MISWG) gällande strategier för nationell cybersäkerhet, policyer för nationell industrisäkerhet och bästa praxis i detta sammanhang. Mot bakgrund av att flera av deltagarländerna i MISWG redan har motsvarande nationella modeller kan dessutom harmoniering uppnås.

MSB:s medverkan i samarbetsgruppen och nätverket för nationella Computer Security Incident Response Teams (CSIRT) inom ramen för NIS-direktivet har skapat ett strategiskt samarbete och informationsutbyte mellan medlemsländerna på cybersäkerhetsområdet. Samarbetet skapar även mervärde inom områden såsom bevakning av framväxande teknologier.

Polismyndighetens resurs hos Europol etablerades under början av 2019. Detta har ökat inflödet av ärenden till Polismyndigheten och bidragit till att hjälpa andra länder med information från Sverige i sina pågående ärenden. Sammantaget har åtgärden gett en bättre möjlighet att bekämpa gränsöverskridande cyberrelaterad brottslighet.

Åtgärder

Åtgärder

I kapitlet redovisas planerade och pågående åtgärder. Vissa åtgärder bidrar till arbetet inom flera strategiska prioriteringar eller målsättningar i den nationella strategin för samhällets informations- och cybersäkerhet. I handlingsplanen redovisas dock åtgärderna under den strategiska prioritering och tillhörande målsättning som åtgärden tydligast knyter an till. Åtgärderna under respektive målsättning är redovisade utan inbördes prioritetsordning. För att bevara spårbarheten i handlingsplanen behåller pågående åtgärder sin ursprungliga numrering trots att vissa åtgärder avslutats 2019 och inte längre finns med i detta kapitel. Åtgärder som avslutats återfinns i bilaga 1.

För varje åtgärd i handlingsplanen förtydligas vilken, eller vilka, SAMFI-myndigheter som är ansvariga för genomförandet. Den ansvariga myndigheten samverkar i flera fall med andra myndigheter eller organisationer.

I genomförandet av åtgärderna kan samverkan med andra aktörer ske på olika sätt och exempelvis syfta till inhämtning av synpunkter eller underlag. Deltagande i samverkan sker alltid utifrån tillgängliga resurser. Genomförandet av de olika åtgärderna sker genomgående med hänsyn tagen till respektive myndighets ansvarsområde. Ambitionen är att arbetet med de olika åtgärderna så långt möjligt ska kännetecknas av transparens mellan SAMFI-myndigheterna.

För att öka läsbarhet har nya och uppdaterade åtgärder i kapitlet markerats med märkningen Ny åtgärd respektive Uppdaterad. Samma märkning finns i bilaga 1.

betyder ansvarig myndighet.
betyder period för åtgärdens genomförande.
betyder åtgärdens unika nummer i handlingsplanen.

Strategisk prioritering 1. Säkerställa en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet

Målsättning 1.1. Statliga myndigheter, kommuner, landsting, företag och andra organisationer ska ha kännedom om hot och risker, ta ansvar för sin informationssäkerhet och bedriva ett systematiskt informationssäkerhetsarbete

Proaktivt stödja de mest skyddsvärda verksamheterna

Omfattande och systematiskt proaktivt stöd till de mest skyddsvärda verksamheterna, till exempel rådgivning, utbildning, övning, it-säkerhetsanalyser och tillsyn. Åtgärden genomförs i enlighet med redovisningen av regeringsuppdrag om utvecklingen av arbetet till skydd för särskilt skyddsvärd verksamhet (Fö2017/00535/SUND) samt redovisning av motsvarande uppdrag ställt till Försvarsmakten i myndighetens regleringsbrev för 2018.

Säkerhetspolisen, FRA och Försvarsmakten
2019–2025
1.1.1.

Utbilda privata aktörer avseende Försvarsmaktens säkerhetsskyddskrav

Försvarsmakten har påbörjat kontraktsskrivande av beredskapsavtal med näringslivet. I detta ingår säkerhetsskyddad upphandling med säkerhetsskyddsavtal (SUA) och kravställning samt utbildning inom säkerhetsskyddsområdet så att dessa kan vara en leverantör till Försvarsmakten.

Några utbildningar har genomförts. Försvarsmakten utbildar parallellt med nya avtal.

Försvarsmakten
2019–2021
1.1.3.

Leverera aggregerat underlag om hot och sårbarheter Uppdaterad

Systematiskt delge aggregerad information om hot och sårbarheter till beslutsfattare på olika nivåer, till exempel föreskrivande myndigheter. Detta möjliggör att information av känslig karaktär kan anpassas för att komma till nytta inom ett bredare nationellt cybersäkerhetsarbete. Åtgärden genomförs i enlighet med redovisningen av regeringsuppdrag till Säkerhetspolisen och FRA om utvecklingen av arbetet till skydd för särskilt skyddsvärd verksamhet (Fö2017/00535/SUND) samt redovisning av motsvarande uppdrag ställt till Försvarsmakten i myndighetens regleringsbrev för 2018.

Säkerhetspolisen, FRA och Försvarsmakten
2019–2025
1.1.4.

Ta fram en handlingsplan för myndigheters deltagande i standardiseringsarbete inom ramen för SIS TK318 Uppdaterad

MSB ska ta fram och förankra en treårig handlingsplan för ett strategiskt och långsiktigt arbete med standardisering avseende systematiskt och riskbaserat informationssäkerhetsarbete. Det nationella engagemanget för nationellt och internationellt arbete med standardisering inklusive förmågan att nyttja resultaten från standardiseringsarbetet inom informations- och cybersäkerhetsområdet behöver stärkas. Handlingsplanen ska fokusera på myndigheters deltagande och det verksamhetsområde som SIS TK318 arbetar inom. Åtgärden genomförs tillsammans med FMV/CSEC och berörda myndigheter och organisationer.

MSB
2020–2021
1.1.5.

Ta fram stödjande material för tillämpning av ny säkerhetsskyddslag Uppdaterad

Säkerhetspolisen och Försvarsmakten tar fram nya och uppdaterade vägledningar respektive handböcker, utbildningsmaterial med mera för att stödja dem som ska tillämpa den nya säkerhetsskyddslagen och nya föreskrifter om säkerhetsskydd. Materialet tas fram koordinerat av de båda myndigheterna för respektive tillsynsområde. Produkterna kommer att omfatta såväl säkerhetsskydd i allmänhet som säkerhetsskyddsanalys, informationssäkerhet, personalsäkerhet, fysisk säkerhet och säkerhetsskyddade upphandlingar.

Säkerhetspolisen och Försvarsmakten
2019–2021
1.1.6.

Genomföra en årlig informationssäkerhetskonferens Uppdaterad

Planera och genomföra årlig informationssäkerhetskonferens för kommuner, regioner och statliga myndigheter där deltagarna utbyter erfarenhet och får kunskap inom informationssäkerhetsområdet.

Målet med konferensen är att bidra till att stärka offentlig sektors informationssäkerhet genom att belysa viktiga frågor inom området. MSB leder arbetet med konferensen.

MSB, FRA, FMV, Försvarsmakten, PTS, Polismyndigheten och Säkerhetspolisen
2019–2022
1.1.7.

Revidering och komplettering av MSB:s föreskrifter för statliga myndigheter Uppdaterad

Se över och komplettera MSB:s föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet (MSBFS 2016:1) och om statliga myndigheters rapportering av it-incidenter (MSBFS 2016:2). Arbetet innebär att föreskrifterna som ställer krav på att statliga myndigheter bedriver ett systematiskt och riskbaserat informationssäkerhetsarbete ses över samt kompletteras med helt nya föreskrifter om grundläggande krav på it-säkerhetsåtgärder och tillhörande vägledning.

Föreskrifterna om it-incidentrapportering ses också över och tydliggörs för att underlätta myndigheternas it-incidentrapportering. Där det är lämpligt kommer kraven i föreskrifterna att harmoniseras med motsvarande krav i NIS-regleringen. Översynen bidrar till en ökad systematik i myndigheternas informationssäkerhetsarbete och mer enhetliga bedömningar.

MSB
2019–2020
1.1.8.

Utveckla och förvalta nationell terminologi Uppdaterad

En process för utveckling och förvaltning av nationell terminologi ska tas fram. Termbanken ska innehålla begrepp för fackområdet informations- och cybersäkerhet. I arbetet ska ingå en kartläggning av olika tekniska lösningar för tillhandahållande av termer. Processen för utveckling och förvaltning bör ske i bred remiss till relevanta privata och offentliga aktörer. Termbanken ska vara allmänt tillgänglig och avgiftsfri.

MSB
2020–2021
1.1.9.

Utveckla MSB:s metodstöd för systematiskt informationssäkerhetsarbete Uppdaterad

MSB utvecklar metodstödet för systematiskt informationssäkerhetsarbete med berörda aktörer inom följande prioriterade områden: metoder för att klassa information, riskanalys, incidenthantering, kontinuitet med hänsyn taget till totalförsvarsaspekter, samt organisationers styrning och ledning.

MSB
2020
1.1.11.

Utforma vägledning för grundläggande it-säkerhetsåtgärder

Uppdaterad

Ta fram en vägledning om grundläggande it-säkerhetsåtgärder som kan användas av alla typer av organisationer. Utifrån denna grundnivå kan en organisation genom riskbedömning och analyser av rättsliga krav och verksamhetsbehov avgöra om de vidtagna it-säkerhetsåtgärderna är tillräckliga eller behöver förstärkas ytterligare. It-säkerhetsåtgärderna är av särskild vikt för de organisationer vars verksamhet är av betydelse för samhällets funktionalitet.

MSB
2019–2020
1.1.12.

Stödja aktörernas arbete att utveckla robusta fysiska förutsättningar för verksamhet och ledning Ny åtgärd

MSB ska ta fram en övergripande strategisk inriktning för ledningsplatsstrukturen i syfte att kunna prioritera åtgärder som stärker de civila aktörernas förmåga till ledning och aktörsgemensam samverkan i vardagen och vid höjd beredskap.

Utifrån denna inriktning stödjer MSB aktörer med robusthetshöjande åtgärder för ordinarie verksamhet och ledning samt med planering, uppbyggnad och utveckling av alternativa och skyddade ledningsplatser. I detta ingår att stödja i utvecklingen av ledningssystem och säkerställa tillgång till säkra och robusta kommunikationer som grund för ledningsförmågan.

MSB
2020 – 2022
1.1.14.

Genomföra en årlig konferens om säkra kommunikationer Ny åtgärd

MSB ska genomföra en årlig konferens för användarkretsen av Rakel, SGSI och Webbaserat Informationssystem (WIS) där deltagarna får information och utbyter erfarenheter, och därmed får ökad kunskap om säkra kommunikationer. Målet med konferensen är att stärka aktörernas förmåga för effektiv och säker samverkan.

MSB
2020–2023
1.1.15.

Ta fram en struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen Ny åtgärd

MSB ska ta fram en struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen. Uppföljningsstrukturen kommer utgöra en viktig komponent i arbetet att säkerställa en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet. Åtgärden följer av ett regeringsuppdrag (Ju2019/03058/SSK, Ju2019/02421/SSK) som ska genomföras i löpande dialog med Sveriges Kommuner och Regioner (SKR) i de delar som berör kommuner och regioner samt vid behov i samverkan med Myndigheten för digital förvaltning (DIGG) och andra relevanta myndigheter.

MSB
2019–2021
1.1.16.

Målsättning 1.2. Det ska finnas en nationell modell till stöd för ett systematiskt informationssäkerhetsarbete

Genomföra en förstudie till nationell modell för systematiskt informationssäkerhetsarbete Uppdaterad

SAMFI-myndigheterna kommer att genomföra en förstudie kring hur en nationell modell för systematiskt informationssäkerhetsarbete konkret kan utvecklas. Förstudien ska beskriva syftet med en nationell modell samt genomföra en intressentanalys. Förstudien ska även beskriva hur arbetet med en sådan modell

kan bedrivas så att alla intressenter kan delta och bidra på adekvat nivå, hur beslut fattas, vilka delar en modell bör innehålla och i vilken ordning delarna kan utvecklas. Förstudien ska identifiera behov av och ta fram förslag på eventuella nya åtgärder i uppföljningen av den nationella handlingsplanen. MSB har en samordnande roll i arbetet.

MSB, FRA, FMV, Försvarsmakten, PTS, Polismyndigheten och Säkerhetspolisen
2019–2020
1.2.1.

Målsättning 1.3. Samverkan och informationsdelning på informations- och cybersäkerhetsområdet ska stärkas

Sprida kunskap och erfarenheter om arbetet med informationsvärdering till andra myndigheter och organisationer

Försvarsmakten avser att stödja andra myndigheter och organisationer med värdering och klassificering av informationsmängder i tekniska system. Detta ska syfta till att förbättra metoder och arbetssätt för värdering av information och ska genomföras genom kunskaps- och erfarenhetsdelning. Aktiviteter baseras på förfrågan från andra myndigheter och organisationer.

Försvarsmakten
2019–2022
1.3.1.

Höja kunskapen avseende informationssäkerhet inom Försvarsmaktens tillsynsområde för säkerhetsskydd

Informationsspridning avseende informationssäkerhet exempelvis Försvarsmaktens krav på godkända säkerhetsfunktioner (KSF) och godkända it-säkerhetsprodukter, genom till exempel träffar med säkerhetsskyddschefer på myndigheter som Försvarsmakten har tillsyn över.

Försvarsmakten
2019–2022
1.3.2.

Etablera samverkansmöjligheter för NIS-aktörer Uppdaterad

MSB, NIS-tillsynsmyndigheterna och Socialstyrelsen etablerar en nationell mötesplats för leverantörer av samhällsviktiga och digitala tjänster. Den syftar till att höja kunskapen om NIS-regleringen och att skapa förutsättningar för NIS-leverantörer att utbyta erfarenheter med andra inom sin sektor. MSB kommer att tillhandahålla information och stöd om systematiskt informationssäkerhetsarbete, om incidentrapportering samt om arbetet med koppling till EU. NIS-tillsynsmyndigheterna och Socialstyrelsen kommer att tillhandahålla information om tillsyn och andra frågor kopplade till respektive sektor.

MSB
2019–2022
1.3.3.

Utveckla säkerhetskrav för specifika it-produkter

FMV/CSEC ska i samverkan med MSB medverka i europeiska och internationella arbetsgrupper i syfte att utarbeta detaljerade krav på it-säkerhet och evalueringsmetodik för specifika typer av it-produkter av intresse för Sverige, till exempel USB-minnen och databashanterare.

FMV i samverkan med MSB
2019 och tills vidare
1.3.5.

Utöka samverkan med andra myndigheter, internationella partners och civila företag inom försvarssektorn avseende lägesbild och incidenthanteringsförmåga

Försvarsmakten avser att utöka samverkan med andra myndigheter, internationella partners och civila företag inom försvarssektorn. Syftet är att förbättra lägesbilden och förmågan att hantera incidenter hos myndigheter och företag inom försvarssektorn som levererar tjänster och materiel till Försvarsmakten. Åtgärden riktar sig även mot internationella partners som Försvarsmakten har samarbetsavtal med.

Försvarsmakten
2019–2022
1.3.6.

Förbereda etablerandet av ett nationellt cybersäkerhetscenter

Ny åtgärd

FRA, Försvarsmakten, MSB, Säkerhetspolisen, Polismyndigheten, FMV och PTS förbereder etablerandet av ett nationellt cybersäkerhetscenter. Arbetet sker i form av ett gemensamt etableringsprojekt. Cybersäkerhetscentret ska stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot mot Sverige. Centret ska även ge ett utvecklat och samordnat stöd till olika aktörer i privat och offentlig sektor om hur de kan skydda sig mot cyberattacker. Verksamheten i centret kommer att utvecklas stegvis de kommande åren.

MSB, FRA, FMV, Försvarsmakten, PTS, Polismyndigheten och Säkerhetspolisen
2020
1.3.7.

Målsättning 1.4. Det ska finnas en ändamålsenlig tillsyn som skapar förutsättningar för en ökad informations- och cybersäkerhet i samhället

Fortsätta utveckling av föreskrifter för säkerhetsskydd

Säkerhetspolisen och Försvarsmakten kommer att vidareutveckla bland annat föreskrifter om säkerhetsskydd för respektive tillsynsområde, med anledning av bland annat betänkandet från utredningen om vissa säkerhetskyddsfrågor, Kompletteringar till den nya säkerhetsskyddslagen (SOU 2018:82).

Säkerhetspolisen och Försvarsmakten
2019–2022
1.4.1.

Stödja och samordna utveckling av NIS-föreskrifter rörande säkerhetsåtgärder Uppdaterad

Inom ramen för existerande NIS-samverkan etableras en arbetsgrupp med syfte att dela erfarenheter och stödja NIS-tillsynsmyndigheternas och Socialstyrelsens arbete med föreskrifter om säkerhetsåtgärder. Arbetet kan bidra till ökad tydlighet för aktörer som träffas av NIS-regleringen genom samordnad planering och utformning.

MSB
2019–2020
1.4.2.

Vidareutveckla stödet för samordnad tillsyn inom NIS Ny åtgärd

Inom ramen för existerande NIS-samverkan samordna tillsynsmyndigheterna i en arbetsgrupp för att skapa förutsättningar för effektiv och likvärdig tillsyn. Samordningen syftar till att skapa gemensamma förhållningssätt och möjlighet att harmonisera bedömningar vid tillsyn inom olika sektorer.

MSB
2020–2022
1.4.4.

Strategisk prioritering 2. Öka säkerheten i nätverk, produkter och system

Målsättning 2.1. Elektroniska kommunikationer ska vara effektiva, säkra och robusta samt tillgodose användarnas behov

Genomföra projekt för att minska beroendet av centrala funktioner i elektroniska kommunikationsnät och -tjänster

PTS genomför ett projekt som syftar till att minska beroendet av centrala funktioner i elektroniska kommunikationsnät och -tjänster. Projektet inleds med en analys som genomförs tillsammans med teleoperatörer i syfte att bedöma möjligheterna till att minska beroendet till centrala funktioner. Erfarenheter från analysen tillämpas i ett pilotprojekt där möjligheten att implementera regionalt autonoma nät prövas i en geografiskt avgränsad del av landet. Åtgärden tar utgångspunkt i slutrapporten från projekt Särimner.

PTS
2019–2022
2.1.2.

Utveckling och anskaffning av it-säkerhetsprodukter Uppdaterad

Utveckling, anskaffning och säkerhetsgranskning av generella it-säkerhetsprodukter i första hand för Försvarsmaktens behov men med möjlig vidare användning av andra myndigheter som kan dra nytta av den granskning som genomförs.

Försvarsmakten och FMV
2019 och tills vidare
2.1.4.

Etablera nya säkra och robusta kommunikationer för aktörer med särskilda säkerhetsskyddsbehov

Försvarsmakten vidareutvecklar möjligheten till säker och robust kommunikation för aktörer inom försvarssektorn och aktörer inom totalförsvaret med särskilda säkerhetsskyddsbehov.

Försvarsmakten
2019–2022
2.1.5.

Etablera nya säkra och robusta kommunikationstjänster för aktörer inom allmän ordning, säkerhet, hälsa och försvar Uppdaterad

MSB tillhandahåller nya säkra och robusta kommunikationstjänster för aktörer inom totalförsvaret och utvecklar förmågan att dela känslig och säkerhetsskyddsklassificerad information. Åtgärden innebär bland annat att realisera tjänster så som krypterad videokonferens till säkerhetsskyddsklassen Begränsat Hemlig i SGSI, förstärkt skydd för kommunikationen i Rakel genom införande av ytterligare kryptering (ej godkänd för säkerhetsskyddsklassificerad information) och etablering av kompletterande datatjänster till Rakel.

MSB
2019–2022
2.1.6.

Etablera en federationstjänst för SGSI-anslutna aktörer Uppdaterad

MSB ska tillsammans med berörda aktörer etablera och förvalta en federationstjänst i Swedish Government Secure Intranet (SGSI). Genom att etablera och förvalta en federationstjänst skapas en central funktion mellan de SGSI-anslutna myndigheterna. Med en central federationstjänst skapas möjligheter att, med hjälp av kryptering, öka skyddet på informationen när den ska delas mellan olika aktörer vilket ökar förmågan till säkrare informationsdelning.

MSB
2020
2.1.7.

Följa och bidra till utvecklingen av säker kommunikation för andra organisationer

Försvarsmakten ska bidra med erfarenheter avseende realisering av säkra systemlösningar i det strategiska arbetet med vidareutveckling av exempelvis nätinfrastrukturer, kommunikationslösningar med mera inom ramen för totalförsvaret.

Försvarsmakten
2019–2022
2.1.8.

Etablera WIS över SGSI Ny åtgärd

MSB ska ta fram, etablera och förvalta en lösning som möjliggör att informationsdelning med hjälp av Webbaserat informationssystem (WIS) kan göras över SGSI. Detta säkerställer skyddad och internetoberoende informationsdelning mellan aktörer som använder WIS och är anslutna till SGSI.

MSB
2020–2021
2.1.9.

Målsättning 2.2. Elektronisk kommunikation i Sverige ska vara tillgänglig oberoende av funktioner utanför landets gränser

Utreda elektronisk kommunikations oberoende av funktioner utomlands

PTS utreder dels vad det innebär konceptuellt med ”elektronisk kommunikation oberoende av funktioner utomlands”, dels i vilken grad elektronisk kommunikation idag fungerar oberoende av funktioner utomlands.

Utredningen kommer analysera i vilken mån operatörer av särskild betydelse för det allmänna kan leverera elektroniska kommunikationstjänster oberoende av funktioner utomlands samt kartlägga eventuella beroenden som omöjliggör detta i dagsläget. Utredningen kan ligga till grund för förändringar av Post- och telestyrelsens föreskrifter om fredstida planering för totalförsvarets behov av telekommunikation (PTSFS 1995:1).

PTS
2019–2020
2.2.1.

Målsättning 2.3. Tillsynsmyndighetens behov av att kunna vidta adekvata åtgärder ska säkerställas

Utreda möjligheten att besluta om specifika säkerhetsåtgärder hos aktörer i sektorn elektronisk kommunikation

PTS utreder möjligheten att fatta beslut om åtgärder som syftar till att ålägga operatörer att skyndsamt vidta säkerhetsåtgärder för att möta specifika sårbarheter i operatörernas nät och eller tjänster.

PTS
2019–2022
2.3.1.

Utreda möjligheten att tillgängliggöra spårbar tid och frekvens för aktörer utanför sektorn elektronisk kommunikation

PTS utreder möjligheten att tillgängliggöra spårbar tid och frekvens för aktörer utanför sektorn elektronisk kommunikation. Sedan 2015 upprätthåller PTS ett nationellt system för produktion och distribution av spårbar tid och frekvens inom sektorn för elektronisk kommunikation. Syftet med systemet är att bidra

med robusthet och redundans samt att minska beroendet av GNSS (Global Navigation Satellite System) för tid- och frekvens synkronisering inom sektorn. Aktörer från andra sektorer, däribland från finanssektorn och energisektorn, har i olika sammanhang uttryckt intresse för att ansluta sig till tjänsten med Precision Time Protocol.

För samhället skulle tillgängliggörande gentemot fler aktörer vara positivt ur ett beredskapsperspektiv. För att aktörer utanför sektorn elektronisk kommunikation ska kunna ansluta sig behöver dock vissa ytterligare utredningar företas.

PTS
2019–2020
2.3.2.

Målsättning 2.4. Tillgången till säkra kryptosystem för it- och kommunikationslösningar ska motsvara behoven i samhället

Utarbeta ett preciserat förslag till nationell strategi och åtgärdsplan för säkra kryptografiska funktioner Uppdaterad

Med utgångspunkt i Informationssäkerhetsutredningen NISU 2014 bilaga 4 (SOU 2015:23), utarbetar FMV med stöd av FRA, Försvarsmakten och MSB ett förslag till en nationell strategi och åtgärdsplan för hantering och överföring av information i elektroniska kommunikationsnät och it-system med hjälp av kryptering även för den information som inte faller in under signalskyddstjänstens mandat. Strategin ska omfatta övergripande mål för samhällets informationssäkerhetsarbete relaterat till kryptografi, och hur Sverige ska upprätthålla säkerhet och integritet i samhällsviktig it-infrastruktur med hjälp av kryptografiska funktioner.

Resultatet ska utgöra en rapport med ett preciserat förslag till nationell strategi och åtgärdsplan för kryptografiska funktioner, efter samråd med Försvarsmakten, FRA och MSB. Förslaget ska innehålla en kostnadsredovisning och kunna ligga till grund för konkret uppgiftsställning till berörda myndigheter.

FMV med stöd av FRA, Försvarsmakten och MSB
2020
2.4.1.

Fortsatt utveckling av signalskyddssystem

Försvarsmakten kravställer nya såväl som vidareutvecklade signalskyddssystem som upphandlas av FMV. Försvarsmakten genomför granskning och godkännande av de produkter som levereras.

Försvarsmakten och FMV
2019 och tills vidare
2.4.2.

Ta fram process för hantering av signalskydd Uppdaterad

Myndigheterna med ansvar för olika delar av signalskyddet kommer att ta fram och uppdatera processer som kan hantera bland annat beslut om tilldelning och distribution av signalskyddsmaterial till de aktörer som omfattas av den nya säkerhetsskyddslagen. Processerna ska säkerställa att rätt aktörer får tillgång till signalskydd. Den nya säkerhetsskyddslagen kommer att innebära att ytterligare aktörer, både myndigheter och enskilda, omfattas av krav på användning av kryptosystem som är godkända av Försvarsmakten, för skydd av säkerhetsskyddsklassificerade uppgifter (signalskydd).

Försvarsmakten i samverkan med FMV, FRA och MSB
2019–2020
2.4.3.

Införa krypterat mobilt tal och textmeddelandefunktion för säkerhetsskyddsklassen Begränsat Hemlig Uppdaterad

Försvarsmakten ska införa krypterat mobilt tal och textmeddelandefunktion för säkerhetsskyddsklassen Begränsat Hemlig. Det finns ett stort och ökande behov att utbyta säkerhetsskyddsklassificerade meddelanden inom Försvarsmakten och totalförsvaret. Telefonen ska stödja samverkansbehov för myndighetsledningen, högre chefer och deras primära kontaktytor internt och externt. Telefonen är också ämnad för funktionsexperter och operativa behov. Med telefonen finns ett stort utbud av applikationer som gör det möjligt att ersätta en vanlig tjänstemobiltelefon.

Överenskommelse om användning och hantering inom totalförsvaret utarbetas av Försvarsmakten tillsammans med MSB.

Systemet bör vidareutvecklas för en bredare användning inom totalförsvaret.

Försvarsmakten
2019 och tills vidare
2.4.4.

Införa säkert tal för säkerhetsskyddsklassen Hemlig i totalförsvaret Uppdaterad

Försvarsmakten, i samverkan med FMV, MSB och FRA, ska införa säkert tal för säkerhetsskyddsklassen Hemlig i totalförsvaret. Behovet av säkert tal är mycket stort i totalförsvaret och ökande. Nuvarande system är gamla och stödjer inte dagens förbindelser varför behovet av en modern ersättare är mycket stort. Det nya systemet utgörs av en krypterande mobiltelefon med nyckelserver för enklare nyckelhantering.

Försvarsmakten i samverkan med FMV, MSB och FRA
2020–2022
2.4.5.

Utveckla och införa säkert meddelandekrypto för säkerhetsskyddsklassen Hemlig i totalförsvaret

Försvarsmakten, i samverkan med FMV, MSB och FRA, ska utveckla och införa säkert meddelandekrypto för säkerhetsskyddsklassen Hemlig i totalförsvaret. Det finns ett stort och ökande behov inom totalförsvaret att kunna utbyta säkerhetsskyddsklassificerade meddelanden mellan aktörer som inte har tillgång till ihopkopplade system för säkerhetskyddsklassificerade uppgifter. De system som används i dag (kryfax och krypto-PC) ska fasas ut. Därför ska ett nytt system för att lösa behovet tas fram och införas.

Försvarsmakten i samverkan med FMV, MSB och FRA
2019–2022
2.4.6.

Målsättning 2.5. Säkerheten i industriella informations- och styrsystem ska öka

Tillhandahålla expertis och medvetandehöjande material om it-säkerhet vid uppbyggnaden av nya intelligenta transportsystem

Arbeta med medvetandehöjande insatser och stärka det förebyggande arbetet rörande it-säkerhet under uppbyggnaden av de nya intelligenta transportsystemen. Arbetet genomförs tillsammans med FOI och andra ansvariga instanser.

MSB
2019–2021
2.5.1.

Främja nyttjandet av skyddade satellittjänster för tid, takt och position för samhällskritiska funktioner Uppdaterad

Tid, takt och position är kritiska faktorer för många funktioner i vårt samhälle. Vid bortfall av GNSS kan många system och tjänster inte längre fungera normalt. Samtidigt finns en tydlig hotbild mot GNSS i form av både störning av signalen och mer intelligenta attacker som exempelvis vilseledning. MSB ska därför främja nyttjandet av den offentligt reglerade tjänsten Galileo Public Regulated Service (PRS) till fördel för kritiska samhällsfunktioner som är i behov av mobila lösningar för tid, takt och position. För fasta installationer som är kritiskt beroende av exakt tid och/eller frekvens bör arbetet samordnas med PTS tjänst för korrekt och spårbar tid och frekvens.

MSB
2019–2022
2.5.2.

Genomföra en nationell satsning på ökad säkerhet i cyberfysiska system

MSB ska tillsammans med berörda aktörer genomföra en nationell satsning som inkluderar tekniska, förebyggande, förmågehöjande och koordinerande aktiviteter i syfte att öka säkerheten i industriella informations- och styrsystem och sakernas internet (IoT). Dessa aktiviteter ska resultera i utvecklandet och tillhandahållandet av utbildningar, vägledningar, tekniska verktyg, stärka

befintliga samverkansstrukturer samt tillhandahålla stöd för kompetensförsörjning. Det övergripande syftet är att stärka samhällets samlade förmåga att förebygga och hantera såväl brister och felaktigheter som it-angrepp i sådan samhällsfunktionalitet som är beroende av industriella informations- och styrsystem (ICS).

MSB
2019–2020
2.5.3.

Strategisk prioritering 3. Stärka förmågan att förebygga, upptäcka och hantera cyberattacker och andra it-incidenter

Målsättning 3.1. Förmågan att förebygga, upptäcka och hantera cyberattacker och andra it-incidenter i samhället ska förbättras

Öka incidenthanteringsförmågan avseende kvalificerade hotaktörer

Säkerhetspolisen, FRA och Försvarsmakten utvecklar förmågan att upptäcka cyberangrepp eller försök till angrepp av kvalificerade hotaktörer samt stödjer de mest skyddsvärda verksamheterna med incidenthantering vid sådana angrepp och angreppsförsök. Åtgärden genomförs i enlighet med redovisning av regeringsuppdrag om utvecklingen av arbetet till skydd för särskilt skyddsvärd verksamhet (Fö2017/00535/SUND). Försvarsmakten genomför liknande åtgärder i enlighet med redovisning av uppdrag ställt till Försvarsmakten i myndighetens regleringsbrev för 2018.

Säkerhetspolisen, FRA och Försvarsmakten
2019–2025
3.1.1.

Tillhandahålla medvetandehöjande material om att minska störningskänsligheten vid användandet av trådlös kommunikation i industriella informations- och styrsystem som används i samhällsviktig verksamhet

MSB tillhandahåller medvetandehöjande material om att minska störningskänsligheten vid användandet av trådlös kommunikation i industriella informations- och styrsystem som används i samhällsviktig verksamhet. Med den omfattande digitaliseringen och teknikutvecklingen blir samhället allt mer beroende av olika trådlösa kommunikationstekniker. Det kan exempelvis röra sig om styrning och kontroll av olika industriella informations- och styrsystem via wifi. I användandet av trådlös kommunikation finns det utöver olika traditionella it-hot även en elektromagnetisk hotdimension. Åtgärden syftar till att arbeta kunskapshöjande kring elektromagnetiska hot och vikten av att minska störningskänsligheten i industriella informations- och styrsystem samt öka förmågan att detektera störningsincidenter.

MSB
2019–2022
3.1.2.

Etablera ett sensorsystem för NIS-leverantörer

MSB ska genom CERT-SE erbjuda leverantörer av samhällsviktiga och digitala tjänster (NIS-leverantörer) möjlighet att ansluta sig till ett sensorsystem. Sensorsystemet ger de anslutna aktörerna en utökad förmåga att upptäcka och skydda sig mot allvarligare it-angrepp. Genom en förbättrad lägesbild och informationsdelning, bidrar sensorsystemet även till en ökad förmåga i samhället att förebygga och hantera it-angrepp. Systemet ska utgöra ett komplement till kommersiella produkter och vara utformat med hög nivå av säkerhet och integritetsskydd.

MSB
2019–2022
3.1.3.

Fortsätta utvecklingen av nationell Cyber Range

MSB fortsätter tillsammans med Försvarsmakten och Totalförsvarets forskningsinstitut (FOI) att utveckla en nationell Cyber Range (övningsmiljö). För att säkra svensk kritisk informationsinfrastruktur och samhällsviktiga it-system krävs praktiskt inriktad övning. Åtgärden syftar till att utveckla en nationell Cyber Range för utbildning, träning och övning i informations- och cybersäkerhet inom ICS.

MSB
2019–2020
3.1.4.

Målsättning 3.2. Berörda aktörer ska kunna agera samordnat för att hantera cyberattacker och andra allvarliga it-incidenter

Arbeta inom NSIT för att öka förmågan att möta komplexa och allvarliga it-hot

Nationell samverkan till skydd mot allvarliga it-hot (NSIT) är en samverkan mellan Säkerhetspolisen, Försvarsmakten och FRA. NSIT analyserar och bedömer hot och sårbarheter när det gäller allvarliga eller kvalificerade it-angrepp mot de mest skyddsvärda nationella intressena. NSIT utvecklar samverkan och genomför aktiviteter syftande till att försvåra för en kvalificerad angripare att komma åt eller skada skyddsvärda civila eller militära resurser.

Säkerhetspolisen, Försvarsmakten och FRA
2019 och tills vidare
3.2.2.

Målsättning 3.3. Det ska finnas ett utvecklat cyberförsvar för Sveriges mest skyddsvärda verksamheter med en förstärkt militär förmåga att möta och hantera angrepp från kvalificerade motståndare i cyberrymden

Leverera militärstrategiska lägesbilder rörande statusen i Försvarsmaktens informations- och ledningsstödsystem, hot och risker

Försvarsmakten levererar militärstrategisk lägesbild veckovis och presenterar för sin myndighetsledning. Lägesbilden kan vid behov användas för hela försvarssektorn, till exempel inom ramen för NSIT.

Försvarsmakten
2019–2022
3.3.1.

Tillhandahålla TDV till de mest skyddsvärda verksamheterna

Uppdaterad

FRA bedriver i samverkan med Säkerhetspolisen fortsatt utveckling av Tekniskt detekterings- och varningssystem (TDV) samt utplacering hos de mest skyddsvärda verksamheterna. Åtgärden genomförs i enlighet med redovisning av regeringsuppdrag om utvecklingen av arbetet till skydd för särskilt skyddsvärd verksamhet (Fö2017/00535/SUND) samt regleringsbrevet för budgetåret 2019 avseende Försvarets radioanstalt.

FRA i samverkan med Säkerhetspolisen
2019 och tills vidare
3.3.2.

Förstärka förmågan att genomföra defensiva och offensiva operationer mot en kvalificerad motståndare i cybermiljön Uppdaterad

Försvarsmakten förstärker förmågan att genomföra defensiva och offensiva operationer mot en kvalificerad motståndare i cybermiljön. FRA stödjer Försvarsmakten att genomföra aktiva operationer i cybermiljön för ett förstärkt cyberförsvar.

Uppdraget har ställts i regleringsbrev till Försvarsmakten och FRA. Förslag på åtgärder har dialogiserats med Försvarsdepartementet inom bland annat budgetunderlag 19.

Försvarsmakten med stöd av FRA
2019–2022
3.3.3.

Utveckla en militär Cyber Range

Försvarsmakten etablerar en militär Cyber Range för att förstärka Försvarsmaktens möjligheter att bedriva utbildning, träning och övningar i cyberförsvar. Utöver det skapas även möjligheter till att kunna evaluera både förmåga och teknik inom cyberområdet.

Försvarsmakten
2019–2020
3.3.4.

Strategisk prioritering 4. Öka möjligheterna att förebygga och bekämpa it-relaterad brottslighet

Målsättning 4.1. De brottsbekämpande myndigheterna ska ha beredskap och förmåga att bekämpa it-relaterade brott på ett effektivt och ändamålsenligt sätt

Etablera regionala it-brottscentrum

Polismyndigheten bygger upp regionala it-brottscentrum i polisens sju regioner för att öka förmågan att utreda och beivra it-relaterade brott samt höja kvaliteten i det brottsförebyggande arbetet inom området.

Polismyndigheten
2019–2022
4.1.2.

Samarbeta med brottsbekämpande myndigheter

Polismyndigheten fördjupar samarbetet med andra brottsbekämpande myndigheter bland annat genom regelbundna möten och gemensamt deltagande på utbildningar för att öka förmågan att bekämpa it-relaterade brott.

Polismyndigheten
2019–2022
4.1.3.

Målsättning 4.2. Arbetet med att förebygga it-relaterade brott ska utvecklas

Använda europeiska resurser för brottsförebyggande kampanjer

Uppdaterad

Polismyndigheten fördjupar samarbetet med Europol avseende brottsförebyggande arbete genom att öka användningen av det material och de aktiviteter som Europol erbjuder, bland annat under European Cyber Security Month (ECSM).

Polismyndigheten
2020–2022
4.2.1.

Delta i samarbete med finans- och transaktionsmarknaderna

Polismyndigheten deltar i samarbete med finans- och transaktionsmarknaderna i arbetet för säkrare betalningar och för att minska it-relaterade brott via transaktionssystemen.

Polismyndigheten
2019–2022
4.2.2.

Uppbyggande av europeiskt nätverk för förebyggande av cyberbrott

Ny åtgärd

För att bromsa ökningen av cyberbrott ska Polismyndigheten delta i uppbyggnaden av ett europeiskt brottsförebyggande nätverk gällande cyberkriminalitet.

Polismyndigheten
2020–2022
4.2.3.

Nordiskt preventionsarbete gällande cyberbrott

Ny åtgärd

Polismyndigheten initierar ett preventionsarbete inom norden gällande cyberbrott. Samarbetet innebär att ta del av varandras informationskampanjer samt erfarenhetsutbyte kring olika sätt att förhindra cyberbrott.

Polismyndigheten
2020
4.2.4.

Strategisk prioritering 5. Öka kunskapen och främja kompetensutvecklingen

Målsättning 5.1. Kunskapen i samhället som helhet om de mest angelägna sårbarheterna och behoven av säkerhetsåtgärder ska öka

Etablera ett strategiskt arbetssätt för bevakning och värdering av samhällets förmåga inom informations- och cybersäkerhetsområdet

MSB etablerar processer och strukturer för att upprätthålla en aktuell bild över samhällets förmåga inom informations- och cybersäkerhet. I detta ingår långsiktig planering för genomförande av kartläggningar samt regelbunden uppföljning av informationssäkerheten hos aktörer av vikt för samhällsviktig verksamhet samt förmåga avseende strategisk och operativ omvärldsbevakning. Åtgärden utförs tillsammans med myndigheter som utövar tillsyn samt genomför kartläggningar och utredningar med bäring på informations- och cybersäkerhetsområdet.

MSB
2019–2020
5.1.1.

Vidareutveckla analysförmåga av hårdvara

FRA vidareutvecklar förmågan att analysera hårdvarurelaterade hot och sårbarheter. Förmågeutvecklingen sker dels genom uppbyggnad av ett hårdvarulaboratorium, dels genom kompetens- och personalförstärkning på området.

FRA
2019 och tills vidare
5.1.2.

Målsättning 5.2. Kunskapen hos enskilda användare av digital teknik om de mest angelägna sårbarheterna och behoven av säkerhetsåtgärder ska öka

Genomföra en riktad informationskampanj för att höja säkerhetsmedvetandet Uppdaterad

Försvarsmakten lanserade i maj 2019 en kommunikationskampanj främst riktad mot verksamma i alla delar av Försvarsmakten och sekundärt mot andra myndigheter, främst försvarsmyndigheter. Även andra externa målgrupper (till exempel kommuner och privatpersoner) har nåtts av kampanjen. Kampanjupplägget skiljer sig från tidigare kampanjer med liknande syfte och är således ett nytt sätt att nå ut till målgrupperna.

En bärande del har varit att jobba med korta informationsfilmer som spridits via sociala medier liksom Försvarsmaktens webbplats, där fördjupad information återfinns. Syftet med kampanjen är att höja säkerhetsmedvetandet hos enskilda medarbetare genom att öka kunskapen om underrättelsehotet samt peka på beteenden som innebär risker, möjliga konsekvenser av bristande säkerhet och hur man kan minska dessa risker. Kampanjen pågår under 2019, men även under 2020 då den även kommer att kompletteras med andra säkerhetsaspekter.

Försvarsmakten
2019 och tills vidare
5.2.1.

Genomföra riktade utbildningsinsatser på informationssäkerhetsområdet till offentlig sektor Ny åtgärd

MSB ska genomföra riktade utbildningsinsatser på informationssäkerhetsområdet till offentlig sektor och även vid behov utveckla stöd till mindre myndigheter.

Åtgärden är en del av ett regeringsuppdrag (Ju2019/03057/SSK) som ska genomföras i samverkan med Myndigheten för digital förvaltning (DIGG) och Sveriges Kommuner och Regioner (SKR) och vid behov länsstyrelserna.

MSB
2019–2021
5.2.2.

Nationell kampanj ”Tänk säkert” Ny åtgärd

Genomföra en nationell kampanj för att få individer och företagare att vidta åtgärder för att skydda sin viktigaste information. Kampanjen äger rum under den europeiska informationssäkerhetsmånaden (ECSM) i oktober.

MSB tillsammans med Polismyndigheten
2020
5.2.3.

Målsättning 5.3. Det ska bedrivas högre utbildning, forskning och utveckling av hög kvalitet rörande informations- och cybersäkerhet och säkerhet på it- och telekomområdet i Sverige

Utveckla förutsättningar för kompetensförsörjning

FRA, Säkerhetspolisen och Försvarsmakten behöver utveckla förutsättningar till kompetensförsörjning för att nå målbilden i redovisningen av regeringsuppdrag om utvecklingen av arbetet till skydd för särskilt skyddsvärd verksamhet (Fö2017/00535/SUND) samt enligt redovisningen av motsvarande uppdrag till Försvarsmakten i myndighetens regleringsbrev för 2018. På sikt bör arbetet involvera fler verksamheter (till exempel SAMFI-myndigheterna) och verka för nationell kompetensförsörjning på cybersäkerhetsområdet.

FRA, Säkerhetspolisen och Försvarsmakten
2019–2025
5.3.1.

Etablera en modell för kompetensutveckling

Försvarsmakten tillsammans med FRA och Säkerhetspolisen etablerar en sammanhängande modell för kompetensutveckling och flöden inom Försvarsmakten och mellan Försvarsmakten och FRA samt Säkerhetspolisen. Åtgärden utförs dessutom med andra aktörer inom området, både nationellt och internationellt.

Försvarsmakten tillsammans med FRA och Säkerhetspolisen
2019–2022
5.3.2.

Stärka och vidareutveckla forskning och teknikutveckling inom cyberförsvarsområdet Uppdaterad

Försvarsmakten stärker och vidareutvecklar forskning och teknikutveckling inom cyberförsvarsområdet. Syftet är att öka kunskapen om och säkerställa tillgång till metoder och teknik i forskningens framkant. Resultaten ska kunna omsättas i tillämpningar som bland annat bidrar till förmågan att genomföra operationer i cyberrymden. Totalförsvarets forskningsinstitut (FOI), Försvarshögskolan (FHS), Kungliga Tekniska Högskolan (KTH) med flera stödjer i forskningen.

Försvarsmakten
2019 och tills vidare
5.3.3.

Etablera anpassad uttagning och rekrytering mot cyberinriktningen

Uppdaterad

Försvarsmakten utvecklar ett koncept för pliktutbildning samt struktur för vidareutbildning inom cyberförsvarsområdet och genomför en kompetensbehovsinventering. Ett exempel på åtgärd är cybersoldatutbildning. Även FRA utreder möjligheten att genomföra cybersoldatutbildning. Åtgärden utförs även tillsammans med andra aktörer inom området, både nationellt och internationellt.

Försvarsmakten och FRA
2019–2022
5.3.4.

Genomföra en förstudie rörande kompetensförsörjning inom informations- och cybersäkerhetsområdet för samhället

Uppdaterad

MSB avser att analysera möjligheterna att stödja utvecklingen av kompetensförsörjning inom informations- och cybersäkerhetsområdet. MSB ska även lägga förslag på åtgärder i form av styrning och stöd som detta skulle förutsätta inom olika typer av utbildningar så som yrkesutbildningar, vidareutbildningar, högskola och gymnasium.

MSB
2020
5.3.5.

Finansiera forskning för att möta framtidens utmaningar på informations- och cybersäkerhetsområdet

Ny åtgärd

MSB finansierar forskning om informations- och cybersäkerhetsutmaningar som följer av digitaliseringen samt lösningar för att möta dem. Myndigheten bevakar samhällsutvecklingen och utvecklar sina metoder för att utforma nya utlysningar utifrån de unika informationsflöden som myndigheten har. Forskningen spänner över tekniska, samhällsvetenskapliga, organisatoriska och strategiska frågor. Genom samarbete med internationella partners kan resurser samlas för att uppnå kritisk massa och synergier. Under 2020–2021 inleds stöd till forskning inom framtidens autonoma och automatiserade cybersäkerhet.

MSB
2020–2022
5.3.6.

Målsättning 5.4. Det ska regelbundet genomföras både tvärsektoriella och tekniska informations- och cybersäkerhetsövningar i syfte att stärka Sveriges förmåga att hantera konsekvenserna av allvarliga it-incidenter

Genomföra delmoment i TFÖ 2020

Försvarsmakten planerar, genomför och utvärderar delmoment i Totalförsvarsövning 2020 (TFÖ 2020) tillsammans med MSB. I de olika aktiviteterna i övningen ingår som övningsmoment att kunna överföra säkerhetsskyddsklassificerad information.

Försvarsmakten tillsammans med MSB
2019–2020
5.4.1.

Genomföra NISÖ 2021

MSB genomför Nationell informationssäkerhetsövning 2021 (NISÖ) i samverkan med Försvarsmakten, Säkerhetspolisen, PTS och Polismyndigheten. Förra övningen genomfördes 2018. Syftet med NISÖ är att ge privata och offentliga aktörer möjlighet att öva tillsammans. Övningen syftar till att stärka samhällets samlade förmåga att hantera it-relaterade samhällsstörningar där aktörerna snabbt behöver samordna sig för att kunna vidta relevanta åtgärder.

MSB
2019–2021
5.4.2.

Genomföra återkommande samövningar med cybersäkerhetsmyndigheter gällande hantering av it-incidenter Uppdaterad

MSB genomför återkommande samövningar med svenska och europeiska cybersäkerhetsmyndigheter gällande hantering av it-incidenter. Syftet med övningarna är att utveckla den gemensamma förmågan att hantera it-incidenter.

MSB
2020–2021
5.4.3.

Genomföra årlig informations- och cybersäkerhetsövning SAFE Cyber

Försvarsmakten genomför i samverkan med FRA, MSB och Säkerhetspolisen en årlig informations- och cybersäkerhetsövning kallad SAFE Cyber. Övningen omfattar samverkan med syfte att säkerställa viktiga funktioner i händelse av dator- och nätverksoperationer riktade mot Sverige. Fokus för övningen är it-säkerhet inklusive risk- och incidenthantering, hotbild, lägesbild, rapportering, ledning, koordinering och beslutsfattande. Övningen riktar sig till personal från myndigheter med ansvar för cyberförsvaret av Sverige samt myndigheter och företag med ansvar för system och tjänster med koppling till Försvarsmakten. Upplägg och tema för årliga övningstillfällen varierar och anpassas till omvärldsutvecklingen.

Försvarsmakten i samverkan med FRA, MSB och Säkerhetspolisen
2019–2022
5.4.4.

Strategisk prioritering 6. Stärka det internationella samarbetet

Målsättning 6.1. Internationella samarbeten kring cybersäkerhet ska stärkas, inom ramen för målsättningen om ett globalt, tillgängligt, öppet och robust internet som präglas av frihet och respekt för mänskliga rättigheter

Arbeta för internationell harmonisering av regler och krav för informationssäkerhet

Försvarsmakten arbetar för internationell harmonisering av regler och krav för informationssäkerhet. Detta görs genom samverkan för att dela och utveckla kunskap inom olika områden och för att harmonisera bestämmelser och informationssäkerhetsåtgärder. Arbetet bedrivs exempelvis inom Implementation Tempest Task Force (ITTF), olika grupper inom kryptoområdet och inom till exempel samarbetet Federated Mission Networking (FMN). FMN är ett koncept för att skapa gemensamma nätverk för att stödja multinationella insatser. Säkerhetssamverkan inom detta ramverk är därför av stor betydelse för skydd av Sveriges bidrag i sådana insatser.

Försvarsmakten
2019–2022
6.1.1.

Utveckla och förbättra standarder och metodik för krav och kontroll av cybersäkerhet i it-produkter

FMV/CSEC ska medverka i svenska och internationella standardiseringsorgan och forum för att utveckla och förbättra standarder för kravställning och evaluering av it-säkerhet och kryptografi.

FMV
2019 och tills vidare
6.1.3.

Resurs vid Europol Ny åtgärd

Polismyndigheten har en resurs på Joint Cybercrime Action Taskforce (J-CAT) hos Europol i Haag för att förstärka samarbetet med andra länder och myndigheter i arbetet med att utreda cyberbrott.

Polismyndigheten
2020–2022
6.1.4.

Målsättning 6.2. Cybersäkerhet ska främjas inom ramen för ambitionen att värna fria flöden till stöd för innovation, konkurrenskraft och samhällsutveckling

Delta i internationellt samarbetsforum för industrisäkerhet Uppdaterad

FMV deltar sedan tidigare aktivt i det internationella samarbetsforumet Multinational Industrial Security Working Group (MISWG). Inom MISWG finns ett antal arbetsgrupper inom olika områden. Genom att delta i MISWG Ad Hoc Working Group (AHWG) 7 on Cyber Security inhämtas kunskap om hur andra länders industrisäkerhetsmyndigheter arbetar med kravställning inom cybersäkerhetsområdet gentemot industrin. Kunskaperna kommer att bidra till uppbyggnaden av FMV som nationell industrisäkerhetsmyndighet (Designated Security Authority) samt ge underlag som bidrar till arbetet med nationell modell till stöd för ett systematiskt informationssäkerhetsarbete.

FMV
2019–2020
6.2.1.

Bevaka och bidra till NIS-direktivets utveckling Uppdaterad

NIS-regleringens krav bidrar till att öka nivån på informations- och cybersäkerhet i ett stort antal viktiga samhällstjänster. Som nationell kontaktpunkt för NIS-direktivet och nationell CSIRT-enhet, deltar MSB i NIS Cooperation Group och CSIRT's Network för att bevaka och bidra till utveckling av NIS-direktivets utveckling i EU

MSB
2019 och tills vidare
6.2.2.

Slutord

Slutord

Arbetet med 2020 års redovisning av en samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022 har bidragit till ökad samordning av myndigheternas åtgärder och aktiviteter. Myndigheterna har byggt vidare på erfarenheter från arbetet med förra årets handlingsplan och har beaktat hur planen nyttjats av samhällets aktörer. Arbetet med att utveckla handlingsplanens åtgärder vad gäller tydlighet och uppföljning kommer att fortsätta även nästa år.

Etablerandet av ett nationellt cybersäkerhetscenter och en nationell modell för systematiskt informationssäkerhetsarbete bedöms inte bara kunna utveckla samhällets informations- och cybersäkerhet. Som samverkansplattformar kan de samla och samordna arbetet med många av åtgärderna, något som kan komma att påverka utformningen av nästa års handlingsplan.

Ett antal behov av ytterligare åtgärder har lyfts av privata och offentliga aktörer inom ramen för den samverkan som skett för handlingsplansarbetet. I vissa fall har dessa behov kunnat omhändertas redan i årets redovisning alternativt bedöms kunna komma att omhändertas inom ramen för arbetet med cybersäkerhetscentret och nationell modell. Andra bedöms, på grund av begränsade resurser eller mandat, inte kunna fullt ut hanteras på ett ändamålsenligt sätt inom ramen för arbetet med handlingsplanen.

Arbetet med nästa års redovisning av handlingsplanen kommer att inledas snarast efter att 2020 års redovisning har lämnats till regeringen. Arbetet kommer fortsätta att bedrivas inom ramen för den gemensamma arbetsgruppen som etablerats av SAMFI-myndigheterna. Genom att inleda arbetet och extern samverkan tidigt på året ökar möjligheterna till resurssättning, samordning och samplanering.

Bilaga 1:

Förteckning över åtgärder

Förteckning över åtgärder

Aktuella åtgärder

Bilagan innehåller en överskådlig lista på samtliga åtgärder i handlingsplanen. Åtgärder som avslutats återfinns i avsnittet ”Genomförda åtgärder” nedan. Åtgärder som inte längre är relevanta att genomföra återfinns under avsnittet ”Avskrivna åtgärder” nedan.

Strategisk prioritering 1. Säkerställa en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet

#	Åtgärd	Ansvarig myndighet	Status	Sida
1.1.1.	Proaktivt stödja de mest skyddsvärda verksamheterna	Säkerhetspolisen, FRA och Försvarsmakten		24
1.1.3.	Utbilda privata aktörer avseende Försvarsmaktens säkerhetsskyddskrav	Försvarsmakten		24
1.1.4.	Leverera aggregerat underlag om hot och sårbarheter	Säkerhetspolisen, FRA och Försvarsmakten	Uppdaterad	24
1.1.5.	Ta fram en handlingsplan för myndigheters deltagande i standardiseringsarbete inom ramen för SIS TK318	MSB	Uppdaterad	25
1.1.6.	Ta fram stödjande material för tillämpning av ny säkerhetsskyddslag	Säkerhetspolisen och Försvarsmakten	Uppdaterad	25
1.1.7.	Genomföra en årlig informationssäkerhetskonferens	MSB, FRA, FMV, Försvarsmakten, PTS, Polismyndigheten och Säkerhetspolisen	Uppdaterad	25
1.1.8.	Revidering och komplettering av MSB:s föreskrifter för statliga myndigheter	MSB	Uppdaterad	25
1.1.9.	Utveckla och förvalta nationell terminologi	MSB	Uppdaterad	26
1.1.11.	Utveckla MSB:s metodstöd för systematiskt informationssäkerhetsarbete	MSB	Uppdaterad	26
1.1.12.	Utforma vägledning för grundläggande it-säkerhetsåtgärder	MSB	Uppdaterad	26
1.1.14.	Stödja aktörernas arbete att utveckla robusta fysiska förutsättningar för verksamhet och ledning	MSB	Ny åtgärd	27
1.1.15.	Genomföra en årlig konferens om säkra kommunikationer	MSB	Ny åtgärd	27

Strategisk prioritering 1. Säkerställa en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet

#	Åtgärd	Ansvarig myndighet	Status	Sida
1.1.16.	Ta fram en struktur för uppföljning av det systematiska informationssäkerhets-arbetet i den offentliga förvaltningen	MSB	Ny åtgärd	27
1.2.1.	Genomföra en förstudie till nationell modell för systematiskt informations-säkerhetsarbete	MSB, FRA, FMV, Försvarsmakten, PTS, Polismyndigheten och Säkerhetspolisen	Uppdaterad	27
1.3.1.	Sprida kunskap och erfarenheter om arbetet med informationsvärdering till andra myndigheter och organisationer	Försvarsmakten		28
1.3.2.	Höja kunskapen avseende informa-tionssäkerhet inom Försvarsmaktens tillsynsområde för säkerhetsskydd	Försvarsmakten		28
1.3.3.	Etablera samverkansmöjligheter för NIS-aktörer	MSB	Uppdaterad	28
1.3.5.	Utveckla säkerhetskrav för specifika it-produkter	FMV i samverkan med MSB		29
1.3.6.	Utöka samverkan med andra myndig-heter, internationella partners och civila företag inom försvarssektorn avseende lägesbild och incidenthanteringsförmåga	Försvarsmakten		29
1.3.7.	Förbereda etablerandet av ett nationellt cybersäkerhetscenter	MSB, FRA, FMV, Försvarsmakten, PTS, Polismyndigheten och Säkerhetspolisen	Ny åtgärd	29
1.4.1.	Fortsätta utveckling av föreskrifter för säkerhetsskydd	Säkerhetspolisen och Försvarsmakten		29
1.4.2.	Stödja och samordna utveckling av NIS-föreskrifter rörande säkerhets-åtgärder	MSB	Uppdaterad	30
1.4.4.	Vidareutveckla stödet för samordnad tillsyn inom NIS	MSB	Ny åtgärd	30

Strategisk prioritering 2. Öka säkerheten i nätverk, produkter och system

#	Åtgärd	Ansvarig myndighet	Status	Sida
2.1.2.	Genomföra projekt för att minska bero-endet av centrala funktioner i elektro-niska kommunikationsnät och -tjänster	PTS		30
2.1.4.	Utveckling och anskaffning av it-säker-hetsprodukter	Försvarsmakten och FMV	Uppdaterad	30
2.1.5.	Etablera nya säkra och robusta kom-munikationer för aktörer med särskilda säkerhetsskyddsbehov	Försvarsmakten		31
2.1.6.	Etablera nya säkra och robusta kommunikationstjänster för aktörer inom allmän ordning, säkerhet, hälsa och försvar	MSB	Uppdaterad	31

Strategisk prioritering 2. Öka säkerheten i nätverk, produkter och system

#	Åtgärd	Ansvarig myndighet	Status	Sida
2.1.7.	Etablera en federationstjänst för SGSI-anslutna aktörer	MSB	Uppdaterad	31
2.1.8.	Följa och bidra till utvecklingen av säker kommunikation för andra organisationer	Försvarsmakten		31
2.1.9.	Etablera WIS över SGSI	MSB	Ny åtgärd	32
2.2.1.	Utreda elektronisk kommunikations oberoende av funktioner utomlands	PTS		32
2.3.1.	Utreda möjligheten att besluta om specifika säkerhetsåtgärder hos aktörer i sektorn elektronisk kommunikation	PTS		32
2.3.2.	Utreda möjligheten att tillgängliggöra spårbar tid och frekvens för aktörer utanför sektorn elektronisk kommunikation	PTS		32
2.4.1.	Utarbeta ett preciserat förslag till nationell strategi och åtgärdsplan för säkra kryptografiska funktioner	FMV med stöd av FRA, Försvarsmakten och MSB	Uppdaterad	33
2.4.2.	Fortsatt utveckling av signalskyddssystem	Försvarsmakten och FMV		33
2.4.3.	Ta fram process för hantering av signalskydd	Försvarsmakten i samverkan med FMV, FRA och MSB	Uppdaterad	34
2.4.4.	Införa krypterat mobilt tal och textmeddelandefunktion för säkerhetsskyddsklassen Begränsat Hemlig	Försvarsmakten	Uppdaterad	34
2.4.5.	Införa säkert tal för säkerhetsskyddsklassen Hemlig i totalförsvaret	Försvarsmakten i samverkan med FMV, MSB och FRA	Uppdaterad	34
2.4.6.	Utveckla och införa säkert meddelandekrypto för säkerhetsskyddsklassen Hemlig i totalförsvaret	Försvarsmakten i samverkan med FMV, MSB och FRA		35
2.5.1.	Tillhandahålla expertis och medvetandehöjande material om it-säkerhet vid uppbyggnaden av nya intelligenta transportsystem	MSB		35
2.5.2.	Främja nyttjandet av skyddade satellittjänster för tid, takt och position för samhällskritiska funktioner	MSB	Uppdaterad	35
2.5.3.	Genomföra en nationell satsning på ökad säkerhet i cyberfysiska system	MSB		35

Strategisk prioritering 3. Stärka förmågan att förebygga, upptäcka och hantera cyberattacker och andra it-incidenter

Strategisk prioritering 4. Öka möjligheterna att förebygga och bekämpa it-relaterad brottslighet

#	Åtgärd	Ansvarig myndighet	Status	Sida
4.1.2.	Etablera regionala it-brottscentrum	Polismyndigheten		39
4.1.3.	Samarbeta med brottsbekämpande myndigheter	Polismyndigheten		39
4.2.1.	Använda europeiska resurser för brottsförebyggande kampanjer	Polismyndigheten	Uppdaterad	39
4.2.2.	Delta i samarbete med finans- och transaktionsmarknaderna	Polismyndigheten		39
4.2.3.	Uppbyggande av europeiskt nätverk för förebyggande av cyberbrott	Polismyndigheten	Ny åtgärd	40
4.2.4.	Nordiskt preventionsarbete gällande cyberbrott	Polismyndigheten	Ny åtgärd	40

Strategisk prioritering 5. Öka kunskapen och främja kompetensutvecklingen

#	Åtgärd	Ansvarig myndighet	Status	Sida
5.1.1.	Etablera ett strategiskt arbetssätt för bevakning och värdering av samhällets förmåga inom informations- och cybersäkerhetsområdet	MSB		40
5.1.2.	Vidareutveckla analysförmåga av hårdvara	FRA		40
5.2.1.	Genomföra en riktad informationskampanj för att höja säkerhetsmedvetandet	Försvarsmakten	Uppdaterad	41
5.2.2.	Genomföra riktade utbildningsinsatser på informationssäkerhetsområdet till offentlig sektor	MSB	Ny åtgärd	41
5.2.3.	Nationell kampanj ”Tänk säkert”	MSB tillsammans med Polismyndigheten	Ny åtgärd	41
5.3.1.	Utveckla förutsättningar för kompetensförsörjning	FRA, Säkerhetspolisen och Försvarsmakten		42
5.3.2.	Etablera en modell för kompetensutveckling	Försvarsmakten tillsammans med FRA och Säkerhetspolisen		42
5.3.3.	Stärka och vidareutveckla forskning och teknikutveckling inom cyberförsvarsområdet	Försvarsmakten	Uppdaterad	42
5.3.4.	Etablera anpassad uttagning och rekrytering mot cyberinriktningen	Försvarsmakten och FRA	Uppdaterad	43
5.3.5.	Genomföra en förstudie rörande kompetensförsörjning inom informations- och cybersäkerhetsområdet för samhället	MSB	Uppdaterad	43
5.3.6.	Finansiera forskning för att möta framtidens utmaningar på informations- och cybersäkerhetsområdet	MSB	Ny åtgärd	43

Strategisk prioritering 5. Öka kunskapen och främja kompetensutvecklingen

Strategisk prioritering 6. Stärka det internationella samarbetet

Genomförda åtgärder

#	Åtgärd	Ansvarig myndighet	Klar
1.1.2.	**Utbilda bevakningsansvariga myndigheter** Utbildning i informationssäkerhet och skyddad kommunikation. Aktiviteten är kopplad till Totalförsvarsövning 2020 (TFÖ) och alla bevakningsansvariga myndigheter samt berörda sektorer är inblandade. Åtgärden utförs även tillsammans med Säkerhetspolisen och Försvarshögskolan.	Försvarsmakten och MSB	2019
1.1.13.	**Etablera och förvalta en referenslista för it-säkerhetsprodukter** MSB ska etablera och förvalta en referenslista över rekommenderade skyddsprofiler (eng. protection profiles) samt it-säkerhetsprodukter som tredjepartsgranskats enligt den internationella standarden Common Criteria, ISO 15408. Vidare ska det finnas en förteckning över rekommenderade kryptofunktioner. Listan ska fungera som ett stöd till organisationer vid anskaffning av it-säkerhetsprodukter som används inom svensk statsförvaltning och inom samhällsviktiga verksamheter i Sverige.	MSB i samverkan med FMV	2019
1.3.4.	**Fördjupa samarbetet mellan FRA, Säkerhetspolisen, Försvarsmakten och MSB** FRA, Säkerhetspolisen, Försvarsmakten och MSB avser att fördjupa sitt samarbete på informations- och cybersäkerhetsområdet. I detta ingår förmågebehov, organisatoriska aspekter och privat-offentlig samverkan inom respektive myndighets ansvarsområde. Sedan årsskiftet arbetar en särskild arbetsgrupp med dessa frågor. Myndigheterna avser att återkomma till regeringen under 2019 med förslag på aktiviteter.	FRA, Säkerhetspolisen, Försvarsmakten och MSB	2019
1.4.3.	**Ta fram stöd för och utveckla samordnad tillsyn inom NIS** Inom ramen för existerande NIS-samverkan etableras en arbetsgrupp för att ge stöd och skapa förutsättningar för effektiv och likvärdig tillsyn. Samordningen syftar till att skapa gemensamma riktlinjer och möjlighet att harmonisera bedömningar vid tillsyn inom olika sektorer.	MSB	2019

2.1.3.	**Utreda möjligheten att öka spårbarheten i betrodda tjänster** PTS utreder möjligheten att öka spårbarheten i betrodda tjänster. Det finns ett behov av att utreda möjligheten till ökad spårbarhet mellan bakomliggande utrustning för generering av kryptografiska nycklar och de tjänster som tillhandahålls på den inre marknaden. Syftet med åtgärden är att öka tilliten till systemet genom att tillföra ett ökat skydd för enskilda länder och förlitande part i en transaktion baserad på ett kvalificerat certifikat. PTS kommer att arbeta för att det inom EU tas fram kompletterande regler på områden där en bristande harmonisering på den inre marknaden för kvalificerade betrodda tjänster leder till ett minskat förtroende till tjänsterna.	PTS	2019
4.1.1.	**Stärka samarbete vid incidentrapportering rörande brottslig verksamhet** Polismyndigheten etablerar tillsammans med MSB en process för samarbete kring incidentrapportering i syfte att öka lagföring och förstärka möjligheten till att brottsförebygga.	Polismyndigheten tillsammans med MSB	2019
6.1.2.	**Etablera en resurs vid Europol** Polismyndigheten anställer en resurs som placeras på Joint Cybercrime Action Taskforce (J-CAT) hos Europol i Haag för att underlätta samarbetet med andra länder och myndigheter i arbetet med att utreda brott.	Polismyndigheten	2019

Avskrivna åtgärder

#	Åtgärd	Ansvarig myndighet	Avskriven
1.1.10.	**Utreda möjligheten till utökad styrning rörande informationssäkerhetsarbete för kommuner och landsting** MSB ska genomföra en utredning av behovet att införa rättsliga krav på att bedriva systematiskt och riskbaserat informationssäkerhetsarbete för kommuner och regioner. De rättsliga kraven ska komplettera redan existerande NIS-reglering. Utredningen bör, utöver krav på systematiskt och riskbaserat informationssäkerhetsarbete, även analysera behov av att införa krav på incidentrapportering samt tillsyn. Utredningen ska kunna svara på vilken styrning som krävs för att förbättra informationssäkerhetsarbetet i kommuner och landsting och utförs med stöd av referensgrupp inkluderat kommuner, landsting och länsstyrelser. Åtgärden genomförs med berörda aktörer. MSB avvaktar genomförandet av regeringsuppdraget att ta fram en struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen (Ju2019/03058/SSK, Ju2019/02421/SSK) för att bedöma fortsatt behov av reglering av kommuner och regioner.	MSB	2019
2.1.1.	**Ta fram stöd för anskaffning av robust elektronisk kommunikation** PTS tar fram stöd för anskaffning av robust elektronisk kommunikation. Robustheten i elektronisk kommunikation påverkas av flera faktorer. En faktor är användarnas anskaffning av kommunikationsnät och kommunikationstjänster. Det finns behov av stöd till företag, myndigheter och andra organisationer som på olika sätt är beroende av robust elektronisk kommunikation i sin verksamhet, avseende hur de kan anskaffa robust elektronisk kommunikation. Stödet ska förenkla för verksamheter att värdera den egna verksamhetens behov av säker elektronisk kommunikation, omsätta dessa behov till krav inför en anskaffning samt stöd för att följa upp kraven under avtalstiden. Åtgärden uppgår i arbetet med det framtida nationella cybersäkerhetscentret.	PTS	2019
3.1.5.	**Skapa förutsättningar för samverkan inom ramen för MSB:s CSIRT-verksamhet** Åtgärden syftar till att underlätta samverkan och vid behov samordning av åtgärder inom ramen för CSIRT-verksamheten (Computer Security Incident Response Team) och MSB/CERT-SE:s uppgifter att stödja samhället i arbetet med att förebygga och hantera it-incidenter. I arbetet ska både behoven av tillgång till arbetsplatser och skyddade möteslokaler omhändertas. Åtgärden uppgår i arbetet med det framtida nationella cybersäkerhetscentret.	MSB	2019

3.2.1.	**Utreda möjligheten att säkert delge operativ information och incidentinformation säkert mellan SAMFI-myndigheterna** SAMFI-myndigheterna ska utreda möjligheten att delge information på ett säkert sätt i syfte att underlätta samverkan mellan berörda myndigheter. Det kan till exempel omfatta information om it-relaterade hot i syfte att förbättra respektive myndighets incidenthantering och säkerhetskravställning. Åtgärden uppgår i arbetet med det framtida nationella cybersäkerhetscentret.	MSB, FRA, Säkerhetspolisen, Försvarsmakten, PTS, FMV och Polismyndigheten	2019
3.2.3.	**Etablera ett samarbetsforum för olika myndigheters incidenthanteringsfunktioner** MSB tillsammans med Polismyndigheteten etablerar ett samarbetsforum för informationsutbyte om statistik och aktuella händelser inom myndigheters incidenthanteringsfunktioner. Åtgärden uppgår i ordinarie linjeverksamhet inom ramen för samverkansavtalet mellan de båda myndigheterna.	MSB tillsammans med Polismyndigheten	2019

Bilaga 2:

Uppdrag om en samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022

Regeringen

Regeringsbeslut **I:9**

2018-07-12
Ju2018/03737/SSK

Justitiedepartementet

Uppdrag om en samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022

Regeringens beslut

Regeringen uppdrar åt Myndigheten för samhällsskydd och beredskap, Försvarets radioanstalt, Försvarets materielverk, Försvarsmakten, Post- och telestyrelsen, Polismyndigheten och Säkerhetspolisen att ta fram en samlad handlingsplan för dessa myndigheters arbete utifrån målen i Nationell strategi för samhällets informations- och cybersäkerhet (skr. 2016/17:213). Handlingsplanen ska omfatta åren 2019–2022. Myndigheten för samhällsskydd och beredskap ska vara sammanhållande för arbetet med handlingsplanen.

Av handlingsplanen ska framgå planerade åtgärder som myndigheterna enskilt eller i samverkan med andra aktörer avser att vidta för att höja informations- och cybersäkerheten i samhället. Den samlade handlingsplanen bör syfta till att bidra till att det sker en samordning avseende myndigheternas åtgärder och aktiviteter.

I framtagandet av handlingsplanen ska myndigheterna särskilt samverka med den eller de myndigheter som utövar tillsyn med stöd av den kommande lagen om informationssäkerhet för samhällsviktiga och digitala tjänster samt Datainspektionen och Myndigheten för digital förvaltning (från den 1 september 2018). Myndigheterna bör även på ett systematiskt sätt inhämta idéer och råd och i övrigt samverka med andra relevanta statliga myndigheter, kommuner, landsting, Sveriges Kommuner och Landsting, företag och andra organisationer som kan bidra i arbetet. Handlingsplanen kan även omfatta planerade åtgärder inom ramen för internationella samarbeten.

Myndigheten för samhällsskydd och beredskap ska vara sammanhållande för en redovisning av den samlade handlingsplanen senast den 1 mars 2019 till Regeringskansliet (Justitiedepartementet, Försvarsdepartementet och Näringsdepartementet).

Myndigheten för samhällsskydd och beredskap ska även vara sammanhållande för en årlig redovisning av dessa myndigheters arbete med att genomföra handlingsplanen. Den första redovisningen ska lämnas den 1 mars 2020 till Regeringskansliet (Justitiedepartementet, Försvarsdepartementet och Näringsdepartementet) och därefter den 1 mars varje år fram till att uppdraget slutredovisas den 1 mars 2023. I samband med de årliga redovisningarna bör myndigheterna vid behov uppdatera handlingsplanen så att den ger en rättvisande bild av myndigheternas huvudsakliga aktiviteter.

En utgångspunkt för uppdragets genomförande är att de aktiviteter och åtgärder som myndigheterna redovisar i handlingsplanen ska rymmas inom givna ekonomiska ramar.

Skälen för regeringens beslut

Regeringen har vidtagit en rad åtgärder för att stärka informations- och cybersäkerheten i samhället. I det fortsatta arbetet ser regeringen ett behov av en samlad redovisning av vilka åtgärder de sju myndigheterna på eget initiativ planerar att vidta för att höja informations- och cybersäkerheten i samhället inom ramen för sina befintliga ansvarsområden de kommande åren. Med en samlad handlingsplan kommer regeringens styrning av de sju myndigheterna för att genomföra strategin bli mer ändamålsenlig. Uppdraget bidrar till att ge regeringen ett bättre underlag för att kunna analysera om myndigheternas planerade åtgärder är tillräckliga för att nå målsättningarna i strategin och vilka ytterligare åtgärder regeringen behöver vidta.

Utöver detta uppdrag om en samlad handlingsplan avser regeringen att återkomma med specifika uppdrag som myndigheterna ska utföra i samverkan. Ett prioriterat uppdrag är ett uppdrag om framtagandet av en nationell modell för systematiskt informationssäkerhetsarbete som utgör en av målsättningarna i den nationella strategin för samhällets informations- och cybersäkerhet. Den nationella modellen syftar till att utgöra en gemensam plattform för det systematiska informationssäkerhetsarbetet genom att

samordna och samla regelverk, metoder, verktyg, utbildningar med mera på ett lättillgängligt sätt.

Regeringens strategi ger uttryck för regeringens övergripande prioriteringar och målsättningar och syftar till att utgöra en plattform för Sveriges fortsatta utvecklingsarbete. Ingen aktör kan ensam lösa utmaningarna på detta område. När flera aktörer arbetar mot samma mål är det särskilt viktigt med samverkan och en gemensam riktning. Tillsammans med strategin bidrar den samlade handlingsplanen till en sådan riktning och risken minskar för till exempel överlappande arbete eller att centrala behov inte tillgodoses.

Försvarsberedningen har i sin rapport Motståndskraft, Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025 (Ds 2017:66) betonat vikten av ett kontinuerligt och systematiskt arbete med informations- och cybersäkerhet för en trovärdig totalförsvarsförmåga. För att öka förmågan inom totalförsvaret är det enligt Försvarsberedningen centralt att bygga vidare på arbetet inom krisberedskapen och de strukturer för samhällets informations- och cybersäkerhet som redan är etablerade.

Myndigheterna i detta uppdrag har centrala ansvarsområden i arbetet för en god informations-och cybersäkerhet i samhället. De har också en etablerad samverkansstruktur genom Samverkansgruppen för informationssäkerhet (SAMFI). Regeringen anser att en fördjupad samverkan mellan dessa myndigheter är en förutsättning för att stärka vår förmåga att skydda oss mot cyberattacker och andra allvarliga it-incidenter.

För ett effektivt genomförande av strategin krävs att myndigheterna i detta uppdrag i så stor utsträckning som möjligt samordnar sitt arbete. Myndigheterna ska därför i sin egen planering och prioritering av verksamheten när så är relevant för myndigheten beakta arbetet med handlingsplanen för att ta tillvara effektivitets- och kvalitetsnyttor i arbetet med hela samhällets informations- och cybersäkerhet. I uppdraget ingår även att löpande hålla regeringen informerad om hur arbetet med handlingsplanen fortskrider.

Avgränsningar i uppdraget

Löpande arbete med informations- och cybersäkerhet i den egna organisationen ska i enlighet med ansvarsprincipen bedrivas kontinuerligt och självständigt. Den typen av åtgärder ska inte ingå i handlingsplanen.

Varje myndighet ska även bedöma om, och i så fall i vilken omfattning, planerade åtgärder ska delges inom ramen för den samlade handlingsplanen med anledning av att informationen bedöms hemlig eller omfattas av sekretess.

På regeringens vägnar

Morgan Johansson

Emelie Juter

Likalydande original till

Myndigheten för samhällsskydd och beredskap
Försvarets radioanstalt
Försvarets materielverk
Försvarsmakten
Post- och telestyrelsen
Polismyndigheten
Säkerhetspolisen

Kopia till

Datainspektionen
Transportstyrelsen
Statens energimyndighet
Finansinspektionen
Inspektionen för vård och omsorg
Livsmedelsverket
Sveriges Kommuner och Landsting
Vetenskapsrådet
Arbetsmarknadsdepartementet/A
Finansdepartementet/BA, DF, SFÖ, K, FPM
Försvarsdepartementet/SUND, MFI, MFU
Justitiedepartementet/L4, L6, KRIM, Å, PO, KH
Kulturdepartementet/MF
Miljödepartementet/STM
Näringsdepartementet/D, IFK, FÖF, SUBT, BT, TIF, SUN
Socialdepartementet/FS, SF
Utbildningsdepartementet/F
Utrikesdepartementet/ES, HI, SÄK

Ett samarbete mellan:

Myndigheten för samhällsskydd och beredskap

FÖRSVARSMAKTEN

651 81 Karlstad Tel 0771-240 240 **www.msb.se**
Publ.nr MSB1478 - mars 2020 ISBN 978-91-7927-001-8