Samlad informations- och cybersäkerhets-handlingsplan för åren 2019–2022

1 mars 2019

Myndigheten för samhällsskydd och beredskap
FRA
FMV
FÖRSVARSMAKTEN
PTS
Polisen
Säkerhetspolisen

Samlad informations- och cybersäkerhets-handlingsplan för åren 2019–2022

1 mars 2019

Myndigheten för samhällsskydd och beredskap (MSB)
Försvarets radioanstalt (FRA)
Försvarets materielverk (FMV)
Försvarsmakten
Post- och telestyrelsen (PTS)
Polismyndigheten
Säkerhetspolisen

Samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022 – 1 mars 2019

Myndigheten för samhällsskydd och beredskap (MSB)

Foto: Shutterstock
Produktion: Advant Produktionsbyrå
Tryck: DanagårdLiTHO

Publikationsnummer: MSB1351- mars 2019
ISBN: 978-91-7383-918-1

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. Majoriteten av åtgärderna i årets redovisning av handlingsplanen är planerade att genomföras eller påbörjas under 2019. Handlingsplanen kommer därefter att uppdateras årligen.

Åtgärderna i handlingsplanen ligger inom ramen för de ansvarsområden och uppdrag som myndigheterna har. Planen 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 77 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

Digitaliseringen är idag, så som regeringen beskriver i den nationella strategin för samhällets informations- och cybersäkerhet, ett globalt fenomen som påverkar i stort sett alla delar av vårt samhälle. Den utgör en av vår tids största förändringar och den snabba utvecklingen av informations- och kommunikationsteknologi har stor inverkan på vår framtid. Sverige ligger långt framme i teknikutvecklingen. Det medför stora möjligheter, men också risker.

Kraven på samhällets informations- och cybersäkerhet ökar i allt snabbare takt. Utvecklingen och den förändrade användningen av ny teknik och innovationer innebär att hoten blir svårare att upptäcka, att riskerna blir mer svårbedömda och att beroenden blir svårare att överskåda.

För att höja informations- och cybersäkerheten finns det ett behov av att alla berörda parter i högre grad samverkar mot gemensamma målsättningar.

Nationell strategi

I den nationella strategin för samhällets informations- och cybersäkerhet 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. Regeringen betonar att informations- och cybersäkerhet är ett ansvar för alla i samhället.

Strategin omfattar sex strategiska prioriteringar:

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

Strategin omfattar hela samhället, det vill säga myndigheter, kommuner och landsting, företag, andra organisationer och privatpersoner.

Säkerställa en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet	Öka säkerheten i nätverk, produkter och system	Stärka förmågan att förebygga, upptäcka och hantera cyber-attacker och andra it-incidenter
Statliga myndigheter, kommuner, landsting, företag och andra organisationer ska ha kännedom om hot och risker, ta ansvar för sin informationssäkerhet och bedriva ett systematisk informationssäkerhetsarbete Det ska finnas en nationell modell till stöd för ett systematiskt informations-säkerhetsarbete. Samverkan och informations-delning på informations- och cybersäkerhetsområdet ska stärkas. Det ska finnas en ändamålsenlig tillsyn som skapar förut-sättningar för en ökad informations- och cybersäkerhet i samhället.	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.	Förmågan att förebygga, upptäcka och hantera cyber-attacker 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	**Öka kunskapen och främja kompetensutvecklingen**	**Stärka det internationella samarbetet**
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.	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 sår-barheterna och behoven av säkerhetsåtgärder ska öka. Det ska bedrivas högre utbildning, forskning och ut-veckling 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.	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.

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

Handlingsplan

I juli 2018 gav regeringen myndigheterna med ett särskilt utpekat ansvar inom informations- och cybersäkerhet, Myndigheten för samhällsskydd och beredskap, Försvarets radioanstalt, Försvarets materielverk, Försvarsmakten, Post- och telestyrelsen, Polismyndigheten och Säkerhetspolisen, i uppdrag att ta fram en samlad informations- och cybersäkerhetshandlingsplan för åren 2019-2022.

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 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, och tillhörande aktiviteter, genomförs inom givna ekonomiska ramar, antingen av en myndighet enskilt eller i gemensamma projekt. Planen ska inte ses som en komplett redovisning av alla de åtgärder som de olika myndigheterna avser att genomföra inom sina respektive verksamhetsområden.

Myndigheternas arbete med handlingsplanen

Arbetet med handlingsplanen påbörjades under tidig höst 2018 och har i huvudsak bestått av en inventering av myndigheternas då redan planerade åtgärder. Någon ytterligare behovsanalys utöver regeringens analyser i den nationella strategin för samhällets informations- och cybersäkerhet har inte genomförts inför 2019 års redovisning.

Beredning av planen har innefattat gemensamma arbetsmöten med de involverade myndigheterna där samverkansbehov och möjligheter identifierats. Arbetet med handlingsplanen har även innefattat diskussioner och samverkan med olika aktörer i samhället. Detta har inkluderat Socialstyrelsen och tillsynsmyndigheter enligt förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-förordningen) och andra aktörer med relevans för Sveriges informations- och cybersäkerhet.

Åtgärder

Åtgärder

I kapitel 2 redovisas planerade och pågående åtgärder. Vissa åtgärder kan bidra 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 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.

Inom respektive åtgärd 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.

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

1.1.1. Proaktivt stödja de mest skyddsvärda verksamheterna

Ansvariga myndigheter: Säkerhetspolisen, FRA och Försvarsmakten

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.

När: 2019–2025

1.1.2. Utbilda bevakningsansvariga myndigheter

Ansvariga myndigheter: Försvarsmakten och MSB

Utbildning i informationssäkerhet och skyddad kommunikation. Aktiviteten är kopplad till Totalförsvarsövning 2020 (TFÖ) och alla bevakningsansvariga myndigheter samt berörda sektorer.[1] Åtgärden utförs även tillsammans med Säkerhetspolisen och Försvarshögskolan.

När: 2019

1. 15 § Förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap.

1.1.3. Utbilda privata aktörer avseende Försvarsmaktens säkerhetsskyddskrav

Ansvarig myndighet: Försvarsmakten

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.

När: 2019–2021

1.1.4. Leverera aggregerat underlag om hot och sårbarheter

Ansvariga myndigheter: Säkerhetspolisen, FRA och Försvarsmakten

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.

När: 2019 och tills vidare

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

Ansvarig myndighet: MSB

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 det verksamhetsområde som SIS TK318 arbetar inom. Åtgärden genomförs tillsammans med FMV/CSEC och berörda myndigheter och organisationer.

När: 2019

1.1.6. Ta fram stödjande material för tillämpning av ny säkerhetsskyddslag

Ansvariga myndigheter: Säkerhetspolisen och Försvarsmakten

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 bägge myndigheterna för respektive tillsynsområde. Produkterna kommer att omfatta såväl säkerhetsskydd i allmänhet som säkerhetsskyddsanalys, informationssäkerhet, personalsäkerhet, fysisk säkerhet och säkerhetsskyddade upphandlingar. Arbetet kan på sikt koordineras med utvecklingen av en nationell modell för systematiskt informationssäkerhetsarbete.

När: 2019–2022

1.1.7. Genomföra en årlig informationssäkerhetskonferens

Ansvariga myndigheter: MSB tillsammans med Försvarsmakten, FRA, Polismyndigheten, FMV, PTS och Säkerhetspolisen

Planera och genomföra årlig informationssäkerhetskonferens för kommuner, landsting, länsstyrelser och 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 samt bredda kunskapen inom området.

När: 2019–2022

1.1.8. Revidering och komplettering av MSB:s föreskrifter för statliga myndigheter

Ansvarig myndighet: MSB

Genomföra en översyn av 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). Syftet är bland annat att förtydliga krav på säkerhetsåtgärder och, där så är lämpligt, harmonisera med motsvarande krav för leverantörer av samhällsviktiga tjänster som omfattas av NIS-regleringen.

När: 2019

1.1.9. Utveckla och förvalta nationell terminologi

Ansvarig myndighet: MSB

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. Arbetet kan på sikt koordineras med utvecklingen av en nationell modell för systematiskt informationssäkerhetsarbete.

När: 2019

1.1.10. Utreda möjligheten till utökad styrning rörande informationssäkerhetsarbete för kommuner och landsting

Ansvarig myndighet: MSB

MSB ska genomföra en utredning av behovet att införa rättsliga krav på att bedriva systematiskt och riskbaserat informationssäkerhetsarbete för kommuner och landsting. 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.

När: 2019–2020

1.1.11. Utveckla MSB:s metodstöd för systematiskt informationssäkerhetsarbete

Ansvarig myndighet: MSB

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

Arbetet kan på sikt koordineras med utvecklingen av en nationell modell för systematiskt informationssäkerhetsarbete.

När: 2019–2020

1.1.12. Ta fram koncept för grundläggande säkerhetsåtgärder för informationssäkerhet

Ansvarig myndighet: MSB

Ta fram koncept för grundläggande säkerhetsåtgärder som ska vara tillämpbara för alla typer av organisationer. I konceptet ska även krav på riskanalys ingå.

Säkerhetsåtgärderna är av särskild vikt för de organisationer vars verksamhet är av betydelse för samhällets funktionalitet.

Arbetet kan på sikt koordineras med utvecklingen av en nationell modell för systematiskt informationssäkerhetsarbete.

När: 2019–2020

1.1.13. Etablera och förvalta en referenslista för it-säkerhetsprodukter

Ansvariga myndigheter: MSB i samverkan med FMV

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.

När: 2019 och tills vidare

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

1.2.1. Genomföra en förstudie till nationell modell för systematiskt informationssäkerhetsarbete

Ansvariga myndigheter: MSB, Försvarsmakten, FRA, Polismyndigheten, FMV, PTS och Säkerhetspolisen

SAMFI-myndigheterna och andra relevanta aktörer 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 arbete 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

bereda eventuellt nya åtgärder i uppföljningen av den nationella handlingsplanen som redovisas senast den 1 mars 2020. MSB har en samordnande roll i arbetet.

När: 2019

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

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

Ansvarig myndighet: Försvarsmakten

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.

När: 2019–2022

1.3.2. Höja kunskapen avseende informationssäkerhet inom Försvarsmaktens tillsynsområde för säkerhetsskydd

Ansvarig myndighet: Försvarsmakten

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.

När: 2019–2022

1.3.3. Etablera samverkansmöjligheter för NIS-aktörer

Ansvarig myndighet: MSB

Åtgärden syftar till att etablera ett koncept för MSB, NIS-tillsynsmyndigheterna och Socialstyrelsen att nå ut till leverantörer av samhällsviktiga och digitala tjänster samt att skapa förbättrade förutsättningar för berörda leverantörer att utbyta erfarenheter med andra inom respektive sektor. MSB avser att tillhandahålla information och stöd rörande systematiskt informationssäkerhetsarbete, informera om incidentrapportering samt arbetet med koppling till EU. Tillsynsmyndigheterna och Socialstyrelsen kan tillhandahålla information om tillsyn och andra frågor kopplade till respektive sektor. I arbetet med åtgärden ingår att ta fram förslag på hur ett sådant koncept kan utformas med externt stöd samt hur finansiering ska lösas. Åtgärden utförs tillsammans med NIS-tillsynsmyndigheterna och Socialstyrelsen.

När: 2019 och tills vidare

1.3.4. Fördjupa samarbetet mellan FRA, Säkerhetspolisen, Försvarsmakten och MSB

Ansvariga myndigheter: 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 myn-

dighets ansvarsområde. Sedan årsskiftet arbetar en särskild arbetsgrupp med dessa frågor. Myndigheterna avser att återkomma till regeringen under 2019 med förslag på aktiviteter.

När: 2019

1.3.5. Utveckla säkerhetskrav för specifika it-produkter

Ansvariga myndigheter: FMV i samverkan med MSB

FMV/CSEC ska i samverkan med MSB medverka i europeiska[1] och internationella[2] 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.

När: 2019 och tills vidare

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

Ansvarig myndighet: Försvarsmakten

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.

När: 2019 – 2022

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

1.4.1. Fortsätta utveckling av föreskrifter för säkerhetsskydd

Ansvariga myndigheter: Säkerhetspolisen och Försvarsmakten

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.

När: 2019–2022

1.4.2. Stödja och samordna utveckling av NIS-föreskrifter rörande säkerhetsåtgärder

Ansvarig myndighet: MSB

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.

När: 2019–2020

1. http://www.sogis.org
2. http://www.commoncriteriaportal.org

1.4.3. Ta fram stöd för och utveckla samordnad tillsyn inom NIS

Ansvarig myndighet: MSB

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.

När: 2019

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

2.1.1. Ta fram stöd för anskaffning av robust elektronisk kommunikation

Ansvarig myndighet: PTS

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.

När: 2019–2020

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

Ansvarig myndighet: PTS

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.

När: 2019–2022

2.1.3. Utreda möjligheten att öka spårbarheten i betrodda tjänster

Ansvarig myndighet: PTS

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.

När: 2019 och tills vidare

2.1.4. Utveckling och anskaffning av it-säkerhetsprodukter

Ansvariga myndigheter: Försvarsmakten och FMV

Utveckling och 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. Exempelvis torde stora delar av leverantörsledet kunna och vilja nyttja granskade och godkända produkter när de hanterar myndigheternas skyddsvärden.

När: 2019 och tills vidare

2.1.5. Etablera nya säkra och robusta kommunikationer för aktörer med särskilda säkerhetsskyddsbehov

Ansvarig myndighet: Försvarsmakten

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

När: 2019–2022

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

Ansvarig myndighet: MSB

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 nivån Begränsat Hemlig i SGSI, kryptering i Rakel och etablering av kompletterande datatjänster till Rakel. Dessa tjänster kan aktörer, efter lämplighetsbedömning, välja att nyttja ifall det saknas egna tekniska förutsättningar för att dela känslig och säkerhetsskyddsklassificerad information.

När: 2019–2022

2.1.7. Etablera en federationstjänst för SGSI-anslutna aktörer

Ansvarig myndighet: MSB

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.

När: 2019

2.1.8. Följa och bidra till utvecklingen av säker kommunikation för andra organisationer

Ansvarig myndighet: Försvarsmakten

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.

När: 2019–2022

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

2.2.1. Utreda elektronisk kommunikations oberoende av funktioner utomlands

Ansvarig myndighet: PTS

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).

När: 2019–2020

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

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

Ansvarig myndighet: PTS

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.

När: 2019–2022

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

Ansvarig myndighet: PTS

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 en PTP-anslutning till tjänsten.

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.

När: 2019–2020

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

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

Ansvariga myndigheter: FMV, FRA, Försvarsmakten och MSB

Med utgångspunkt i Informationssäkerhetsutredningen NISU 2014 bilaga 4 (SOU 2015:23), utarbetas 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.

När: 2019

2.4.2. Fortsatt utveckling av signalskyddssystem

Ansvariga myndigheter: Försvarsmakten och FMV

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

När: 2019 och tills vidare

2.4.3. Ta fram process för hantering av signalskydd

Ansvariga myndigheter: Försvarsmakten i samverkan med FMV, FRA och MSB

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).

När: 2019

2.4.4. Införa krypterat mobilt tal och textmeddelandefunktion på nivån Begränsat Hemlig

Ansvarig myndighet: Försvarsmakten

Försvarsmakten ska införa krypterat mobilt tal och textmeddelandefunktion på nivån Begränsat Hemlig. Det finns ett stort och ökande behov att utbyta säker-

hetsskyddsklassificerade 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.

När: 2019

2.4.5. Införa säkert tal på nivån Hemlig i totalförsvaret

Ansvariga myndigheter: Försvarsmakten i samverkan med FMV, MSB och FRA

Försvarsmakten, i samverkan med FMV, MSB och FRA, ska införa säkert tal på nivån Hemlig i totalförsvaret. Behovet av säkert tal är mycket stort i totalförsvaret och ökande. Dagens system ska fasas ut. Därför ska ett nytt system införas. Detta utgörs av en krypterande mobiltelefon med nyckelserver för enklare nyckelhantering.

När: 2020

2.4.6. Utveckla och införa säkert meddelandekrypto på nivån Hemlig i totalförsvaret

Ansvariga myndigheter: Försvarsmakten i samverkan med FMV, MSB och FRA

Försvarsmakten i samverkan med FMV, MSB och FRA ska utveckla och införa säkert meddelandekrypto på nivån 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.

När: 2019 - 2022

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

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

Ansvarig myndighet: MSB

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.

När: 2019–2021

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

Ansvarig myndighet: MSB

MSB ska främja nyttjandet av skyddade satellittjänster för tid, takt och position för samhällskritiska funktioner. Tid, takt och position är kritiska faktorer för många funktioner i vårt samhälle. Vid bortfall av GNSS (Global Navigation Satellite System, till exempel GPS) kan många system och tjänster inte längre fungera normalt. Exempel på system som kan drabbas av störningar i tjänster som tillhandahåller tid, takt och position är styrsystem för vattenrening, tekniska system som används inom jordbruket, drift av elnät och kommunikationssystem.

Utryckningsfordon från polis, brandkår och ambulans får via GNSS snabbare och exaktare uppgifter om destination och vägval. Förutom för bilar så är GNSS idag ett viktigt hjälpmedel för flygplan, tåg och fartyg. Yrkestrafiken använder sedan lång tid tillbaka satellitnavigering som hjälp för att hitta mottagare av gods och för att följa var fordonen befinner sig.

I framtiden kommer GNSS även vara viktigt för trådlösa applikationer inom smarta städer, så som självkörande fordon. Det finns idag en tydlig hotbild mot GNSS i form av störning och vilseledning. Galileo PRS är en Europeisk GNSS-tjänst avsedd för auktoriserade användare som har behov av hög robusthet mot störning och vilseledning, samt hög tillgänglighet. Det finns därför stora fördelar med att arbeta för att kritiska funktioner i samhället som idag använder olika GNSS-tjänster och är i fortsatt behov av mobila lösningar ska gå över till den krypterade tjänsten Galileo PRS. 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.

När: 2019–2022

2.5.3. Genomföra en nationell satsning på ökad säkerhet i cyber-fysiska system

Ansvarig myndighet: MSB

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 samverkans-strukturer 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).

När: 2019–2020

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.

3.1.1. Öka incidenthanteringsförmågan avseende kvalificerade hotaktörer

Ansvariga myndigheter: Säkerhetspolisen, FRA och Försvarsmakten

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 åtgärd i enlighet med redovisning av uppdrag ställt till Försvarsmakten i myndighetens regleringsbrev för 2018.

När: 2019–2025

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

Ansvarig myndighet: MSB

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.

När: 2019–2022

3.1.3. Etablera ett sensorsystem för NIS-leverantörer

Ansvarig myndighet: MSB

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.

När: 2019–2022

3.1.4. Fortsätta utvecklingen av nationell Cyber Range

Ansvarig myndighet: MSB

MSB fortsätter tillsammans med berörda aktörer 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.

När: 2019–2020

3.1.5. Skapa förutsättningar för samverkan inom ramen för MSB:s CSIRT-verksamhet

Ansvarig myndighet: MSB

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.

När: 2019–2020

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

3.2.1. Utreda möjligheten att delge operativ information och incidentinformation säkert mellan SAMFI-myndigheterna

Ansvariga myndigheter: MSB, FRA, Säkerhetspolisen, Försvarsmakten, PTS, FMV och Polismyndigheten

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.

När: 2019–2020

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

Ansvariga myndigheter: Säkerhetspolisen, Försvarsmakten och FRA

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 det 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.

När: 2019 och tills vidare

3.2.3. Etablera ett samarbetsforum för olika myndigheters incidenthanteringsfunktioner

Ansvarig myndighet: MSB tillsammans med Polismyndigheten

MSB tillsammans med Polismyndigheteten etablerar ett samarbetsforum för informationsutbyte om statistik och aktuella händelser inom myndigheters incidenthanteringsfunktioner.

När: 2019 och tills vidare

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.

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

Ansvarig myndighet: Försvarsmakten

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

När: 2019–2022

3.3.2. Tillhandahålla TDV till de mest skyddsvärda verksamheterna

Ansvariga myndigheter: FRA i samverkan med Säkerhetspolisen och Försvarsmakten

FRA bedriver i samverkan med Säkerhetspolisen och Försvarsmakten 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.

När: 2019 tills vidare

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

Ansvariga myndigheter: Försvarsmakten med stöd av FRA

Försvarsmakten med stöd av FRA förstärker förmågan att genomföra defensiva och offensiva operationer mot en kvalificerad motståndare i cybermiljön. Uppdraget har ställts i regleringsbrev till Försvarsmakten och FRA. Förslag på åtgärder har dialogiserats med Försvarsdepartementet inom bland annat budgetunderlag 19.

När: 2019–2022

3.3.4. Utveckla en militär Cyber Range

Ansvarig myndighet: Försvarsmakten

Försvarsmakten har påbörjat en etablering av 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.

När: 2019–2020

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.

4.1.1. Stärka samarbete vid incidentrapportering rörande brottslig verksamhet

Ansvariga myndigheter: Polismyndigheten tillsammans med MSB

Polismyndigheten etablerar tillsammans med MSB en process för samarbete kring incidentrapportering i syfte att öka lagföring och förstärka möjligheten till att brottsförebygga.

När: 2019

4.1.2. Etablera regionala it-brottscentrum

Ansvarig myndighet: Polismyndigheten

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.

När: 2019–2022

4.1.3. Samarbeta med brottsbekämpande myndigheter

Ansvarig myndighet: Polismyndigheten

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

När: 2019–2022

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

4.2.1. Använda europeiska resurser för brottsförebyggande kampanjer

Ansvariga myndigheter: Polismyndigheten tillsammans med MSB

Polismyndigheten tillsammans med MSB fördjupar samarbete 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).

När: 2019–2022

4.2.2. Delta i samarbete med finans- och transaktionsmarknaderna

Ansvarig myndighet: Polismyndigheten

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

När: 2019–2022

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.

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

Ansvarig myndighet: MSB

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.

När: 2019–2020

5.1.2. Vidareutveckla analysförmåga av hårdvara

Ansvarig myndighet: FRA

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

När: 2019 tills vidare

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

5.2.1. Genomföra en riktad informationskampanj för att höja säkerhetsmedvetandet

Ansvarig myndighet: Försvarsmakten

Försvarsmakten genomför en informationskampanj riktad främst mot verksamma i alla delar av Försvarsmakten och sekundärt mot andra försvarsmyndigheter. Kampanjen innebär ett nytt sätt att nå ut till målgruppen. Den är tänkt att innehålla både intresseväckande film och djupare information. Syftet med kampanjen är att höja säkerhetsmedvetandet hos enskilda medarbetare genom att peka både på beteenden som innebär risker, möjliga konsekvenser av bristande säkerhet och hur man kan minska dessa risker. Kampanjen kan komma att följas upp med fler kampanjer av liknande typ.

När: 2019–2022

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.

5.3.1. Utveckla förutsättningar för kompetensförsörjning

Ansvariga myndigheter: FRA, Säkerhetspolisen och Försvarsmakten

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.

När: 2019–2025

5.3.2. Etablera en modell för kompetensutveckling

Ansvariga myndigheter: Försvarsmakten tillsammans med FRA och Säkerhetspolisen

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.

När: 2019–2022

5.3.3. Stärka och vidareutveckla forskning och teknikutveckling inom cyberförsvarsområdet

Ansvarig myndighet: Försvarsmakten

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 med flera stödjer i forskningen.

När: 2019 och tills vidare

5.3.4. Etablera anpassad uttagning och rekrytering mot cyberinriktningen

Ansvariga myndigheter: Försvarsmakten tillsammans med FRA

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

När: 2019–2022

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

Ansvarig myndighet: MSB

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.

Arbetet bör koordineras med redan pågående aktiviteter som genomförs av andra aktörer. Åtgärden genomförs tillsammans med relevanta aktörer i samhället.

När: 2019–2020

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.

5.4.1. Genomföra delmoment i TFÖ 2020

Ansvariga myndigheter: Försvarsmakten tillsammans med MSB

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.

När: 2019–2020

5.4.2. Genomföra NISÖ 2021

Ansvarig myndighet: MSB

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. Detta för att stärka samhällets samlade förmåga att hantera it-relaterade samhällsstörningar där aktörerna snabbt behöver samordna sig för att kunna vidta relevanta åtgärder.

När: 2019–2021

5.4.3. Genomföra återkommande samövningar med cybersäkerhetsmyndigheter gällande hantering av it-incidenter

Ansvarig myndighet: MSB

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

När: 2019–2020

5.4.4. Genomföra årlig informations- och cybersäkerhetsövning SAFE Cyber

Ansvariga myndigheter: Försvarsmakten i samverkan med FRA, MSB och Säkerhetspolisen

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.

När: 2019–2022

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.

6.1.1. Arbeta för internationell harmonisering av regler och krav för informationssäkerhet

Ansvarig myndighet: Försvarsmakten

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 ITTF (Implementation Tempest Task-Force), olika grupper inom kryptoområdet och inom till exempel FMN-samarbetet (Federated Mission Networking). 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.

När: 2019–2022

6.1.2. Etablera en resurs vid Europol

Ansvarig myndighet: Polismyndigheten

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.

När: 2019

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

Ansvarig myndighet: FMV

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.

När: 2019 och tills vidare

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

6.2.1. Delta i internationellt samarbetsforum för industrisäkerhet

Ansvarig myndighet: FMV

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 av cybersäkerhet mot inhemsk industri. Kunskaperna kommer att bidra till uppbyggnaden av den svenska industrisäkerhetsmyndigheten (DSA) samt ge underlag som bidrar till arbetet med nationell modell till stöd för ett systematiskt informationssäkerhetsarbete.

När: 2019

6.2.2. Fortsätta delta i samarbetsgruppen och CSIRT-nätverket inom ramen för NIS-direktivets genomförande och tillämpning

Ansvarig myndighet: MSB

MSB ska fortsätta delta i samarbetsgruppen och CSIRT-nätverket inom ramen för NIS-direktivets genomförande och tillämpning. Som nationell kontaktpunkt och nationell CSIRT-enhet deltar MSB i EU-samarbetet för att harmonisera genomförandet av NIS-direktivet övergripande i NIS Cooperation Group, samt samarbeta gällande incidenthantering i CSIRTs Network.

När: 2019 och tills vidare

Uppföljning och fortsatt arbete

Uppföljning och fortsatt arbete

För att förverkliga regeringens målsättningar på informations- och cybersäkerhetsområdet har de strategiska prioriteringar som formulerats i den nationella strategin för samhällets informations- och cybersäkerhet omsatts till konkreta åtgärder. Arbetet med åtgärderna kommer att följas upp. I kommande redovisningar av den samlade informations- och cybersäkerhetshandlingsplanen avser även myndigheterna att tillsammans analysera vilka ytterligare åtgärder som krävs för att uppfylla målsättningarna i strategin utifrån behoven i samhället.

Det fortsatta arbetet med handlingsplanen kommer att inledas snarast efter att 2019 års redovisning har lämnats till regeringen. Arbetet kommer att bedrivas inom ramen för den gemensamma arbetsgruppen som etablerats av SAMFI-myndigheterna i syfte att genomföra uppdraget. Genom att inleda arbetet tidigt på året ökar möjligheterna till resurssättning, samordning och samplanering.

Under 2019 kommer en metod för förvaltning och uppföljning att tas fram. Syftet är att skapa förutsättningar för att följa upp genomförandet av åtgärderna som beskrivs i handlingsplanen. Metoden bör omfatta de arbetsprocesser som behövs för uppföljning, analys och utformning av kompletterande aktiviteter för att säkerställa förväntat resultat.

Arbetet med uppföljning kommer att ske i samverkan med berörda aktörer. Detta inkluderar bland annat Myndigheten för digital förvaltning, Datainspektionen, Socialstyrelsen och tillsynsmyndigheter inom ramen för NIS-regleringen, Sveriges Kommuner och Landsting (SKL), företag och andra organisationer.

Slutord

Slutord

Arbetet med 2019 års redovisning av en samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022 har utgjort en samverkansplattform som enligt myndigheternas uppfattning bidragit till ökad samordning av myndigheternas åtgärder och aktiviteter. Även om planering och resurssättning av de åtgärder som nu ingår i handlingsplanen i stora delar redan hade genomförts när handlingsplansarbetet inleddes har samordning av det kommande arbetet med vissa åtgärder och aktiviteter kunnat ske. Detta gäller samordning i form av ett utökat informationsutbyte mellan myndigheter som genomför åtgärder med angränsande syfte, upplägg eller målgrupp. För några få åtgärder har det funnits möjlighet till mer omfattande samordning. Myndigheterna har exempelvis enats om att lägga in en åtgärd i handlingsplanen om att gemensamt genomföra en förstudie om en nationell modell till stöd för systematiskt informationssäkerhetsarbete. Myndigheterna bedömer att förutsättningarna för ytterligare samordning av åtgärder och aktiviteter under åren 2020–2022 kommer att kunna öka under det fortsatta arbetet med handlingsplanen.

Även om en behovsanalys inte har ingått i årets arbete med handlingsplanen, har behov av vissa framtida åtgärder identifierats. I vissa fall har dessa behov kunnat omhändertas redan i årets redovisning. Det finns dock ett antal mer omfattande områden som myndigheterna bedömt vara av stor betydelse för arbetet med att stärka informations- och cybersäkerheten i samhället, men som inte fullt ut hanteras i form av åtgärder i denna redovisning av handlingsplanen. Anledningarna till detta kan vara bristande resurser eller mandat. I vissa fall bedöms arbetet underlättas om det sker inom ramen för ett regeringsuppdrag.

BILAGA 1

Förteckning över åtgärder

Bilaga 1. Förteckning över åtgärder

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

#	Åtgärd	Ansvarig myndighet	Sida
3.1.1	Öka incidenthanteringsförmågan avseende kvalificerade hotaktörer	Säkerhetspolisen, FRA och Försvarsmakten	26
3.1.2	Tillhandahålla medvetandehöjande material om att minska störningskänsligheten vid användandet av trådlös kommunikation i industriella informations- och styrsystem som används i samhällsviktig verksamhet	MSB	27
3.1.3	Etablera ett sensorsystem för NIS-leverantörer	MSB	27
3.1.4	Fortsätta utvecklingen av nationell Cyber Range	MSB	27
3.1.5	Skapa förutsättningar för samverkan inom ramen för MSB:s CSIRT-verksamhet	MSB	27
3.2.1	Möjlighet att delge operativ information och incidentinformation säkert mellan SAMFI-myndigheterna	MSB, FRA, Säkerhetspolisen, Försvarsmakten, PTS, FMV och Polismyndigheten	28
3.2.2	Arbeta inom NSIT för att öka förmågan att möta komplexa och allvarliga it-hot	Säkerhetspolisen, Försvarsmakten och FRA	28
3.2.3	Etablera ett samarbetsforum för olika myndigheters incidenthanteringsfunktioner	MSB tillsammans med Polismyndigheten	28
3.3.1	Leverera militärstrategiska lägesbilder rörande statusen i Försvarsmaktens informations- och ledningsstödsystem, hot och risker	Försvarsmakten	28
3.3.2	Tillhandahålla TDV till de mest skyddsvärda verksamheterna	FRA i samverkan med Säkerhetspolisen och Försvarsmakten	28
3.3.3	Förstärka förmågan att genomföra defensiva och offensiva operationer mot en kvalificerad motståndare i cybermiljön	Försvarsmakten med stöd av FRA	29
3.3.4	Utveckla en militär Cyber Range	Försvarsmakten	29

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

#	Åtgärd	Ansvarig myndighet	Sida
4.1.1	Stärka samarbete vid incidentrapportering rörande brottslig verksamhet	Polismyndigheten tillsammans med MSB	29
4.1.2	Etablera regionala it-brottscentrum	Polismyndigheten	29
4.1.3	Samarbeta med brottsbekämpande myndigheter	Polismyndigheten	30
4.2.1	Använda europeiska resurser för brottsförebyggande kampanjer	Polismyndigheten tillsammans med MSB	30
4.2.2	Delta i samarbete med finans- och transaktionsmarknaderna	Polismyndigheten	30

5. Öka kunskapen och främja kompetensutvecklingen

6. Stärka det internationella samarbetet

BILAGA 2

Uppdrag om en samlad informations- och cybersäkerhets-handlingsplan 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.

Telefonväxel: 08-405 10 00
Fax: 08-20 27 34
Webb: www.regeringen.se

Postadress: 103 33 Stockholm
Besöksadress: Rosenbad 4
E-post: ju.registrator@regeringskansliet.se

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

Myndigheten för samhällsskydd och beredskap (MSB)
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ.nr MSB1351- mars 2019 ISBN 978-91-7383-918-1