Samlad informations- och cybersäkerhetshandlingsplan 2019–2022

Redovisning mars 2022

Myndigheten för samhällsskydd och beredskap
FRA
FMV
FÖRSVARSMAKTEN
PTS
Polisen
Säkerhetspolisen

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

Foto omslag: iStockphotos
Tryck: DanagårdLiTHO
Produktion: Advant

Publikationsnummer: MSB1875 - mars 2022
ISBN: 978-91-7927-210-4

Innehåll

Sammanfattning 6

Introduktion 8

Nationell strategi 10

Myndigheternas arbete med handlingsplanen 12

Extern samverkan 13

Uppföljning 14

Strategisk prioritering 1. Säkerställa en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet 15

Strategisk prioritering 2. Öka säkerheten i nätverk, produkter och system 16

Strategisk prioritering 3. Stärka förmågan att förebygga, upptäcka och hantera cyberattacker och andra it-incidenter 17

Strategisk prioritering 4. Öka möjligheterna att förebygga och bekämpa it-relaterad brottslighet 18

Strategisk prioritering 5. Öka kunskapen och främja kompetens-utvecklingen 18

Strategisk prioritering 6. Stärka det internationella samarbetet 19

Åtgärder 20

Strategisk prioritering 1. Säkerställa en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet 22

Målsättning 1.1. Statliga myndigheter, kommuner, regioner, företag och andra organisationer ska ha kännedom om hot och risker, ta ansvar för sin informationssäkerhet och bedriva ett systematiskt informations-säkerhetsarbete 22

Målsättning 1.3. Samverkan och informationsdelning på informations- och cybersäkerhetsområdet ska stärkas 25

Målsättning 1.4. Det ska finnas en ändamålsenlig tillsyn som skapar förut-sättningar för en ökad informations- och cybersäkerhet i samhället 26

Strategisk prioritering 2. Öka säkerheten i nätverk, produkter och system 27

Målsättning 2.1. Elektroniska kommunikationer ska vara effektiva, säkra och robusta samt tillgodose användarnas behov 27

Målsättning 2.4. Tillgången till säkra kryptosystem för it- och kommunikationslösningar ska motsvara behoven i samhället 28

Målsättning 2.5. Säkerheten i industriella informations- och styrsystem ska öka 30

Strategisk prioritering 3. Stärka förmågan att förebygga, upptäcka och hantera cyberattacker och andra it-incidenter 31

Målsättning 3.1. Förmågan att förebygga, upptäcka och hantera cyberattacker och andra it-incidenter i samhället ska förbättras 31

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 32

Strategisk prioritering 4. Öka möjligheterna att förebygga och bekämpa it-relaterad brottslighet 33

Målsättning 4.1. De brottsbekämpande myndigheterna ska ha beredskap och förmåga att bekämpa it-relaterade brott på ett effektivt och ändamålsenligt sätt 33

Målsättning 4.2. Arbetet med att förebygga it-relaterade brott ska utvecklas 34

Strategisk prioritering 5. Öka kunskapen och främja kompetensutvecklingen 35

Målsättning 5.1. Kunskapen i samhället som helhet om de mest angelägna sårbarheterna och behoven av säkerhetsåtgärder ska öka 35

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 35

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 37

Strategisk prioritering 6. Stärka det internationella samarbetet 38

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 38

Målsättning 6.2. Cybersäkerhet ska främjas inom ramen för ambitionen att värna fria flöden till stöd för innovation, konkurrenskraft och samhällsutveckling 39

Slutord 42

Bilaga 1 44

Aktuella åtgärder 45

Genomförda åtgärder 49

Avskrivna åtgärder 55

Bilaga 2 60

Sammanfattning

Sammanfattning

Denna samlade informations- och cybersäkerhetshandlingsplan (fortsättningsvis benämnd ”handlingsplanen”) 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 2022 års redovisning har ett antal åtgärder avslutats, vissa har uppdaterats och ett fåtal 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
- öka kunskapen och främja kompetensutvecklingen.

Ett flertal åtgärder i årets handlingsplan är kopplade till utvecklingen av nationellt cybersäkerhetscenter (NCSC). 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 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 sedan länge haft etablerad samverkan, inte minst 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. Enligt regeringen ska handlingsplanen bidra 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. Med anledning av att myndigheterna numera samverkar inom ramen för NCSC har SAMFI avvecklats.

Handlingsplanen redovisar en delmängd av de åtgärder som myndigheterna 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 (skr. 2016/17:213):

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 2022 års redovisning av handlingsplanen påbörjades under våren 2021 och har bedrivits i den gemensamma arbetsgrupp som myndigheterna etablerade inför den första redovisningen 2019. Myndigheterna har därför kunnat nyttja erfarenheter från tidigare år för att arbetet ska bli så effektivt som möjligt. En förändring som gjordes under året var att minska antalet fysiska möten liksom omfattningen på de externa samverkansmötena med anledning av covid-19-pandemin.

Arbetet med uppdraget att ta fram och årligen redovisa handlingsplanen har ytterligare fördjupat samarbetet mellan myndigheterna. Arbetet har tydliggjort på vilket sätt myndigheterna arbetar för att främja de strategiska prioriteringarna. En stor andel åtgärder har också bedrivits i samverkan mellan två eller flera myndigheter.

Arbetet med att ta fram och årligen redovisa handlingsplanen sker numera inom ramen för det nationella cybersäkerhetscentret (NCSC).

Den externa samverkan kopplat till uppdraget har i huvudsak skett vid två möten under hösten 2021. Upplägget på extern samverkan inför 2022 års redovisning har anpassats för att lättare kunna ta om hand idéer och synpunkter. Detta beskrivs närmare under ”Extern samverkan” nedan.

Under året har myndigheterna vidtagit vissa förberedande åtgärder inför slutredovisningen av regeringsuppdraget som avslutas i mars 2023. Det handlar exempelvis om att identifiera områden som kräver djupare analys och sammanställning av underlag.

Extern samverkan

I regeringsuppdraget framgår att myndigheterna särskilt ska samverka med Myndigheten för digital förvaltning, Integritetsskyddsmyndigheten samt tillsynsmyndigheterna för NIS-regleringen inklusive Socialstyrelsen i framtagandet av handlingsplanen. Myndigheterna bör även på ett systematiskt sätt inhämta idéer och råd och i övrigt samverka med andra relevanta statliga myndigheter, kommuner, regioner, Sveriges Kommuner och Regioner, företag och andra organisationer som kan bidra i arbetet. Samverkan med andra aktörer bidrar till att öka kunskapen om handlingsplanens åtgärder. Extern samverkan genomfördes detta år i huvudsak vid två större samverkansmöten. Vid det ena medverkade de i uppdraget utpekade myndigheterna och vid det andra representanter från näringslivet (inbjudna från MSB:s Forum för informationsdelning samt det nystartade NIS privat-offentligt samverkansforum).

Detta år anpassades upplägget på de externa samverkansmötena för att underlätta för berörda myndigheter att ta om hand de idéer och synpunkter som lämnades. Därför fokuserade agendapunkter och frågeställningar på enskilda eller grupper av åtgärder och personal som arbetar med att genomföra åtgärderna medverkade vid mötena.

Ämnesmässigt fokuserade samverkansmötena på nationell modell för cybersäkerhet, informationsdelning mellan myndigheter med särskilt ansvar för samhällets informations- och cybersäkerhet och aktörer från privat och offentlig sektor samt övningar. Diskussionerna kring dessa ämnen var konstruktiva och resultatet förvaltas vidare i linjeverksamheten i berörda myndigheter för eventuell vidare hantering.

Uppföljning

Uppföljning

Inför 2022 års redovisning av handlingsplanen har myndigheterna gjort en gemensam uppföljning av 2021 års arbete där man har sammanfattat utvalda resultat av arbetet med handlingsplanens åtgärder 2021. 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 rör endast arbetet med handlingsplanens åtgärder och inte myndigheternas övriga arbete på området.

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

Ett flertal åtgärder som myndigheterna genomfört under året har syftat till en systematisk och samlad ansats i det förebyggande arbetet med informations- och cybersäkerhet hos viktiga aktörer i samhället. Fortsatt proaktivt stöd, utökad samverkan, vägledning, utbildning och andra kunskapshöjande insatser har bidragit till säkrare informationshantering i verksamheter som omfattas av säkerhetsskyddslagen eller annan verksamhet viktig för samhällets funktion.

Utvecklat stöd för att bedriva och utvärdera ett systematiskt informationssäkerhetsarbete i alla typer av organisationer har syftat till att höja grundnivån för informationssäkerhet i hela samhället.

Åtgärder för att bidra till utveckling och efterlevnad av standarder och för att etablera säkerhetskrav på vanligt förekommande it-produkter underlättar för många olika typer av aktörer att implementera ändamålsenliga skyddsåtgärder i sin informationshantering.

MSB har under 2021 beslutat om nya föreskrifter för anmälan och identifiering av leverantörer av samhällsviktiga tjänster. Föreskrifterna är uppdaterade för att ge tydligare inriktning rörande vilka aktörer som omfattas av regleringen om informationssäkerhet för digitala och samhällsviktiga tjänster. För att stödja tillämpningen av NIS-regleringen har MSB gett fortsatt stöd till tillsynsmyndigheterna i utvecklingen av föreskrifter om säkerhetsåtgärder och i utvecklingen av effektiv och likvärdig tillsyn. Under året har MSB etablerat ett privat-offentligt samverkansforum för bransch- och intresseorganisationer vars medlemmar omfattas av NIS-regleringen. Forumet syftar till att stärka tillämpningen av NIS-regleringen genom erfarenhetsutbyte och informationsdelning. 2021 höll MSB också den första årliga NIS-konferensen som samlade över 600 deltagare.

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

Inom ramen för det nationella cybersäkerhetscentret har en förstudie genomförts rörande nationell modell för cybersäkerhet. Förstudien ska kunna ligga till grund för att påbörja ett implementeringsarbete efter beslut i det nationella cybersäkerhetscentret. I november 2021 genomfördes den första årliga cybersäkerhetskonferensen inom ramen för det nationella cybersäkerhetscentret. Konferensen vände sig till cybersäkerhetscentrets prioriterade målgrupper och samlade cirka 270 deltagare.

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

Under året har det fortsatta arbetet med åtgärderna samlat gett stöd till flera viktiga aktörer inom offentlig sektor att öka säkerheten vid kommunikation av skyddsvärd information. Det handlar om att ge stöd för ökad användning av säkra produkter och tjänster men även om utveckling av processer och utrustning för signalskydd. Försvarsmakten har, i delar tillsammans med FMV, verkat för ökad säkerhet vid utveckling och inköp av it-säkerhetsprodukter samt i nätinfrastruktur och kommunikationslösningar för säkerhetskänslig verksamhet. En process för hantering av signalskydd har arbetats fram av Försvarsmakten i samverkan med FMV, FRA och MSB vilket bidrar till att underlätta att rätt aktörer har tillgång till ändamålsenliga lösningar för signalskydd. Dessutom har utvecklingen av nya signalskyddssystem för säkert tal och meddelandetjänst för uppgifter med säkerhetsskyddsklassificeringen Begränsat Hemlig respektive Hemlig i totalförsvaret fortsatt.

Arbetet inom ramen för åtgärderna har även innefattat utredning av och genomförande av robusthetshöjande åtgärder för viktig kommunikationsinfrastruktur. PTS har fortsatt att tillsammans med teleoperatörer öka motståndskraft och uthållighet i allmänt tillgängliga elektroniska kommunikationsnät.

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

MSB fortsätter arbetet med ett regeringsuppdrag om att anskaffa och tillhandahålla tjänster för mobil datakommunikation till användare av Rakel. Uppdraget innebär att arbetet med att utveckla och etablera Rakel Generation 2 (Rakel G2) påbörjas, och ska i ett första steg ses som ett komplement till nuvarande Rakel. Arbetet utförs i samverkan med flera myndigheter och användarorganisationer. Nästa steg togs i oktober 2021 i form av uppdrag till MSB och Trafikverket att gemensamt planera och förbereda den kommande utbyggnaden av Rakel G2. Uppdraget innefattar bland annat teknisk utformning, kostnadsberäkningar, genomförandeplan och avvecklingsplan för nuvarande Rakel.

PTS har avslutat arbetet med en åtgärd som innebar att utreda möjligheten att tillgängliggöra spårbar tid och frekvens för aktörer utanför sektorn elektronisk kommunikation. Utredningen visade att det är möjligt för aktörer utanför sektorn elektronisk kommunikation att ansluta sig till tjänsten. En produkt-

specifikation är under framtagande för att tydliggöra för aktörer utanför sektorn vad som ingår i tjänsten samt kostnader för anslutning.

MSB:s vägledning för ökad säkerhet i industriella informations- och styrsystem utkommer i ny utgåva i början av 2022. Därutöver kommer även en operativt inriktad handbok om incidenthantering i industriella informations- och styrsystem att publiceras inom kort. MSB har under året publicerat ett faktablad om cyberfysiska sårbarheter i tunga fordon. Relaterat till det har MSB påbörjat arbetet med en vägledning om cybersäkerhet i tunga brandbilar med primärt syfte att stödja kommunala räddningstjänsters kravställning vid upphandling av fordon.

MSB har även verkat för att nyttjandet av skyddade sattelittjänster för tid, takt och position får ökat nyttjande inom samhällsviktig verksamhet. MSB har via regleringsbreven 2020–2021 i uppdrag (1104/2011/EU) att vara behörig myndighet (så kallad Competent PRS Authority eller CPA) för den offentligt reglerade satellitnavigeringstjänsten Galileo PRS som är en GNSS-tjänst (Global Navigation Satellite System) avsedd för myndighetsbruk och ackrediterade användare som har behov av hög robusthet och tillgänglighet. Att vara CPA innebär ett samordnande ansvar för nationella aktiviteter relaterade till tjänsten Galileo PRS. Under 2021 intensifierade MSB arbetet med att bygga upp och utveckla en svensk PRS-mottagare i syfte att tillgängliggöra PRS-tjänsten i Sverige för myndigheter och andra aktörer som ansvarar för samhällsviktig verksamhet och kritisk infrastruktur.

En teknisk lösning som möjliggör informationsdelning med hjälp av Webbaserat Informationssystem (WIS) över SGSI är anskaffad och etablerad av MSB. Enligt plan driftsätts den fullt ut under 2022.

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

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

MSB och Försvarsmakten har fortsatt att utveckla den nationella cyber rangen (CRATE) hos Totalförsvarets forskningsinstitut i Linköping där aktörer som driver samhällsviktig verksamhet kan genomföra praktiska övningar för att stärka den egna förmågan. Under 2021 har flera styrdokument för CRATE beslutats som stödjer det myndighetsgemensamma arbetet. En sektors- och scenarioanpassning av CRATE har genomförts för övning och utbildning inom energi med hjälp av det simulerade elnätet RICS-el. Övningar har genomförts och övningsmoduler har lagts online. Fortsatt har utveckling skett i enlighet med strategin för CRATE med tekniklyft i form av visualisering av övningsmiljöer och förbättringar hos verktygen för definition och styrning av övningar.

MSB publicerade under året en webbkurs om elektromagnetiska hot. Kursens mål är att höja medvetenheten om hotbilden, ge viss kunskap om kompensatoriska åtgärder, samt ge en introduktion till hur man kan göra en risk- och sårbarhetsanalys. Även incidenthantering och incidentrapportering berörs i kursen.

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

Genom Polismyndighetens 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.

Polismyndighetens samarbete med finans- och transaktionsmarknaden har fortsatt i syfte att öka säkerheten i betalsystemen och minska risken för it-brott kopplade till transaktionssystemen.

Internationellt har Polismyndigheten deltagit i uppbyggnaden av ett europeiskt brottsförebyggande nätverk mot cyberkriminalitet och initierat ett nordiskt samarbete för att förebygga cyberbrott genom att bland annat dela erfarenheter från genomförda informationskampanjer.

Strategisk prioritering 5. Öka kunskapen och främja kompetensutvecklingen

Under året har även Försvarsmaktens interna informationskampanj för högre säkerhetsmedvetande hos medarbetarna i hanteringen av information fortsatt. Kampanjen väntas 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 dialog kring kompetensförsörjning.

Under 2021 har den första omgången av Försvarsmaktens cybersoldater ryckt ut. Under första halvan av 2021 har den andra omgången genomfört utökade urvalstester och påbörjat sin värnpliktsutbildning. Försvarsmakten har dessutom etablerat en utbildningsfunktion med inriktning cyber vid Ledningsstridsskolan.

FRA har under året ökat kunskap och kompetens inom analys av hårdvarurelaterade hot och sårbarheter.

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 genomför vidare 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 FOI, FMV, FHS

och CDIS. Verksamheten präglas av samarbete mellan aktörerna och utpekade nationella och internationella partners.

Resultaten från CDIS ger bland annat Försvarsmakten tillgång till utbildningar i forskningens framkant som stöd för Försvarsmaktens kompetensförsörjning och kompetensutveckling.

Försvarsmakten har genomfört övningen SAFE Cyber 2021. SAFE Cyber 2021 hade marint tema, och riktade sig till personal från myndigheter, företag och organisationer med ansvar för system och tjänster med koppling till Försvarsmaktens marina verksamhet. Övningen var webbaserad. MSB:s arbete med att förbereda övningen NISÖ 2021 har fortsatt under året i samverkan med Försvarsmakten, Säkerhetspolisen, PTS och Polismyndigheten.

Under året har MSB genomfört utbildningsinsatser för såväl kommuner och regioner som statliga myndigheter. Utbildningarna har genomförts både som lärarledda och webbaserade utbildningar riktade till olika roller. En kurs särskilt anpassad för myndighetschefer är under utveckling och en pilotomgång har genomförts under året.

MSB har under året avslutat ett regeringsuppdrag (Ju2019/03057/SSK) om riktade utbildningsinsatser på informationssäkerhetsområdet till offentlig sektor. Arbetet med informationssäkerhet i offentlig sektor behöver alltjämt stärkas och fler behöver utbildas. Genom utbildning finns god möjlighet att höja kompetensen inom organisationer. Utvärderingarna påvisar ökad kunskap för kursdeltagarna.

MSB har genomfört en förstudie rörande kompetensförsörjning inom informations- och cybersäkerhetsområdet för samhället. Efterfrågan på kompetenser på informations- och cybersäkerhetsområdet är hög. Förstudien syftade till att kartlägga behov och föreslå åtgärder för att utöka tillgången på kompetent och erfaren arbetskraft.

Strategisk prioritering 6. Stärka det internationella samarbetet

MSB har i egenskap av nationell kontaktpunkt för NIS-direktivet deltagit i det europeiska NIS-nätverket för CSIRT-enheter samt NIS Cooperation Forum och flera av dess undergrupper. Myndigheten har inlett ett utvecklingsarbete för att stärka NIS-regleringens tillämpning och efterlevnad i Sverige.

Antal ärenden till Polismyndighetens resurs hos Europol har varit fortsatt högt under 2021. Samarbetet innebär även att Sveriges arbete med att stötta andra länder i pågående ärenden ökar.

FMV/CSEC har medverkat i flera internationella standardiseringsorgan och forum för att utveckla och förbättra standarder för kravställning och evaluering av it-säkerhet och kryptografi. Under året har myndigheten bland annat bidragit till ISO/SC27 där ISO15408 (”Common Criteria”) genomgår en uppdatering. FMV/CSEC deltar även i EU/ENISAS arbetsgrupper för att ta fram en certifieringordning inom ramen för cybersäkerhetsakten för certifiering av it-produkter.

FMV har även fortsatt deltagit i Multinational Industrial Security Working Group (MISWG) gällande strategier för nationell cybersäkerhet, policyer för nationell industrisäkerhet och bästa praxis i detta sammanhang.

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 och inte längre finns med i detta kapitel. Åtgärder som avslutats återfinns under ”Genomförda åtgärder” i bilaga 1.

För varje åtgärd i handlingsplanen anges vilken, eller vilka, 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 myndigheterna.

I 2022 års redovisning har ett flertal åtgärder uppdaterats. Det handlar om förändringar i innehåll eller tidplan.

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, regioner, 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 Uppdaterad

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 och tills vidare
1.1.3.

Leverera aggregerat underlag om hot och sårbarheter

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 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 föreskrifter om säkerhetsskydd. Materialet tas fram koordinerat av de båda myndigheterna. Produkterna kommer att omfatta såväl grunderna för säkerhetsskydd som säkerhetsskyddsanalys, informationssäkerhet, personalsäkerhet, fysisk säkerhet och skyldighet när en annan aktör kan få tillgång till säkerhetskänslig verksamhet.

Säkerhetspolisen och Försvarsmakten
2019 och tills vidare
1.1.6.

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
2020–2022
1.1.9.

Utveckla MSB:s metodstöd för systematiskt informationssäkerhetsarbete

Uppdaterad

MSB utvecklar metodstödet för systematiskt informationssäkerhetsarbete med berörda aktörer inom prioriterade områden med fokus på riskhantering.

MSB
2022
1.1.11.

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

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

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.

Regelbunden uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen Ny åtgärd

Inom ramen för MSB:s regeringsuppdrag att skapa en struktur för uppföljning av det systematiska informationssäkerhetsarbetet i offentlig förvaltning har MSB tagit fram ett uppföljningsverktyg, som visar i vilken utsträckning en organisation bedriver ett systematiskt informationssäkerhetsarbete. Verktyget, Infosäkkollen, stödjer uppföljning och förbättring av systematiskt informationssäkerhetsarbete i kommuner, regioner och statliga myndigheter och kommer att skickas ut vartannat år. Verktyget genererar automatiskt en nivåbedömning och hänvisningar till hur organisationen kan komma vidare i arbetet. Efter inrapportering till MSB får organisationen återkoppling om hur resultatet förhåller sig till andra, liknande organisationer. MSB kommer att redovisa en samlad bedömning om nivån på det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen till regeringen. Dessutom ska resultatet användas för att utveckla MSB:s stöd och vidareutveckla Infosäkkollen. I vidareutvecklingen ingår att se över möjligheterna att utöka Infosäkkollen till fler områden respektive erbjuda verktyget till fler aktörer.

MSB
2022 och tills vidare
1.1.19.

Ta fram stödjande material för säkerhetsåtgärder i informationssystem

Ny åtgärd

MSB tar fram vägledning och filmer till stöd för statliga myndigheter i deras tillämpning av MSB:s föreskrifter om säkerhetsåtgärder i informationssystem (MSBFS 2020:7). Vägledning och filmer kommer att utformas så att de även kan stödja kommuner, regioner, företag och andra organisationer i deras it-säkerhetsarbete och på så sätt bidra till att höja samhällets informations- och cybersäkerhet. I vägledningen kommer det finnas rekommendationer om exempelvis ansvarsfördelning, omvärldsbevakning, nätverkssegmentering, behörighetshantering, kryptering, loggning och ändringshantering. Filmerna är tänkta att ytterligare tillgängliggöra och sprida vägledningens innehåll till fler målgrupper.

MSB
2022
1.1.20.

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 Uppdaterad

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 och tills vidare
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. Bland annat har en årlig konferens och ett privat-offentligt samverkansforum etablerats som båda riktar sig till företrädare för NIS-leverantörer. Delar av arbetet medfinansieras av EU:s fond för ett sammanlänkat Europa.

MSB
2019–2022
1.3.3.

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.

Etablera nationell samverkan inom nationellt cybersäkerhetscenter

Ny åtgärd

Det nationella cybersäkerhetscentret ska etablera sig som en nationell plattform för privat-offentlig samverkan på cybersäkerhetsområdet. Förberedelser har gjorts för att skapa förutsättningar för denna samverkan. I uppstartsfasen ingår att sätta strukturer och att identifiera prioriterade aktörer för samverkan. På längre sikt kommer omfattning av samverkan och målgrupper att utökas.

FRA, Försvarsmakten, MSB, och Säkerhetspolisen i nära samverkan med Polismyndigheten, FMV och PTS

2021 och tills vidare

1.3.8.

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

Uppdaterad

Säkerhetspolisen och Försvarsmakten kommer att vidareutveckla bland annat föreskrifter om säkerhetsskydd för respektive tillsynsområde, med anledning av ny säkerhetsskyddsförordning (SFS 2021:955).

Säkerhetspolisen och Försvarsmakten

2019 och tills vidare

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

2019–2023

1.4.2.

Vidareutveckla stödet för samordnad tillsyn inom NIS

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.

Inrättande av nationell myndighet för cybersäkerhetscertifiering Ny åtgärd

FMV utgör från och med den 28 juni 2021 nationell myndighet för cybersäkerhetscertifiering och har för ändamålet etablerat Inspektionen för cybersäkerhetscertifiering med ansvar att genomföra de uppgifter som följer av EU:s cybersäkerhetsakt samt lag och förordning med kompletterande bestämmelser till EU:s cybersäkerhetsakt. Inom uppgiften ingår bland annat omvärldsbevakning av frågor som rör cybersäkerhet och cybersäkerhetscertifiering av IKT-produkter, IKT-tjänster och IKT-processer, samverkan med nationella och internationella aktörer på området och tillsynsansvar över efterlevnaden av det europeiska ramverket för cybersäkerhetscertifiering.

FMV
2022 och tills vidare
1.4.5.

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 Uppdaterad

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 därefter i labbmiljö och/eller i ett pilotprojekt där möjligheten att implementera regionalt autonoma nät prövas i en geografiskt avgränsad del av landet.

PTS
2019–2022
2.1.2.

Utveckling och anskaffning av it-säkerhetsprodukter

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

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.

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.

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 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
2022
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.

Införa krypterat mobilt tal och textmeddelandefunktion för säkerhetsskyddsklassen Begränsat Hemlig

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
2020–2023
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
2019–2024
2.4.6.

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

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 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, operativa, 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, operativ ICS förmåga och threat hunting 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
2019–2022
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.

Fortsätta utvecklingen av nationell Cyber Range

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

MSB tillsammans med Försvarsmakten
2019–2022
3.1.4.

Utveckla nationellt cybersäkerhetscenter Uppdaterad

FRA, Försvarsmakten, MSB, och Säkerhetspolisen, i nära samverkan med Polismyndigheten, FMV och PTS, etablerar det nationella cybersäkerhetscentret (NCSC) i enlighet med regeringsuppdrag (Fö2019/01330). Cybersäkerhetscentret ska stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot. Centret, som inrättades av regeringen december 2020, kommer stegvis att byggas upp fram till 2025. I etableringsfasen kommer myndigheterna bland annat att leverera anpassade lägesbilder och samordnat stöd vid större cyberangrepp samt etablera former för nationell samverkan på cybersäkerhetsområdet. Inom ramen för cybersäkerhetscentret arrangerar myndigheterna en årlig cybersäkerhetskonferens och ger stöd till cybersäkerhetstävlingen Cyber Challenge.

FRA, Försvarsmakten, MSB, och Säkerhetspolisen i nära samverkan med Polismyndigheten, FMV och PTS

2021–2025

3.1.6.

Samordna incidenthantering inom nationellt cybersäkerhetscenter

Ny åtgärd

Inom ramen för det nationella cybersäkerhetscentret ska myndigheterna bygga upp gemensam förmåga att samordna arbetet vid större cybersäkerhetsincidenter. Centret ska underlätta samverkan mellan myndigheterna och på så vis ska myndigheterna snabbare och effektivare kunna hantera och förbygga större it-incidenter. Initialt består arbetet i att ta fram strukturer för arbetet och strukturer för att kunna identifiera vilka incidenter som ska samordnas inom centret.

FRA, Försvarsmakten, MSB, och Säkerhetspolisen i nära samverkan med Polismyndigheten, FMV och PTS

2021 och tills vidare

3.1.7.

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 ledningssystem, 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 det nationella cybersäkerhetscentret.

Försvarsmakten

2019–2022

3.3.1.

Tillhandahålla TDV till de mest skyddsvärda verksamheterna

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 2021 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

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.

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

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

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

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

Polismyndigheten utvecklar ett nordiskt samarbete gällande prevention av cyberbrott. Samarbetet innebär att ta del av varandras informationskampanjer samt erfarenhetsutbyte kring olika sätt att förhindra cyberbrott.

Polismyndigheten
2020–2022
4.2.4.

Delta i brottsförebyggande samarbete med Stöldskyddsföreningen

Uppdaterad

Polismyndigheten deltar i ett brottsförebyggande samarbete med Stöldskyddsföreningen och ett flertal andra aktörer i syfte att skydda allmänheten samt små och medelstora företag. I detta samarbete ingår bland annat Säkerhetskollen.se för varningar till allmänheten om pågående bedrägeritrender, samt ett kunskapscenter ihop med MSB och flera andra myndigheter i syfte att skapa medvetenhetshöjande kampanjer, en helpdesk med mera.

Polismyndigheten och MSB
2021 och tills vidare
4.2.6.

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

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.

Leverera anpassade lägesbilder inom nationellt cybersäkerhetscenter

Ny åtgärd

Inom ramen för det nationella cybersäkerhetscentret ska myndigheterna leverera anpassade lägesbilder. Initialt handlar det om att identifiera vilka behov som finns i samhället och vad som inte kan tillgodoses av redan existerande arbete i myndigheterna. Lägesbilderna kommer kunna vända sig till både offentlig och privat sektor.

FRA, Försvarsmakten, MSB, och Säkerhetspolisen i nära samverkan med Polismyndigheten, FMV och PTS

2021 och tills vidare

5.1.3.

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

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

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.

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

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.

MSB
2020–2022
5.3.6.

Etablera nationellt samordningscenter för cybersäkerhet (NSC)

Ny åtgärd

I syfte att främja svensk forskning och innovation på cybersäkerhetsområdet har MSB fått i uppdrag att etablera ett nationellt samordningscenter för cybersäkerhetsforskning och innovation (NSC). NSC ska främja svenska ansökningar till cybersäkerhetsutlysningar inom EU-programmen Horizon Europe och Digital Europe samt stödja det europeiska kompetenscentret för cybersäkerhet gällande exempelvis utformning av nya EU-program för forskning och innovation på cybersäkerhetsområdet. Det ska även bygga upp och samordna en svensk ”kompetensgemenskap” som består av både behovsägare och utförare inom forskning och innovation på området. Etableringen sker på uppdrag av regeringen (Ju2021/03097).

MSB
2021–2022
5.3.7.

Kartlägga behovet av kompetensförsörjning inom säkerhetsskyddsområdet

Ny åtgärd

Försvarsmakten och Säkerhetspolisen ska kartlägga behovet av kompetensförsörjning inom säkerhetsskyddsområdet och föreslå åtgärder som underlättar kompetensförsörjningen på kort och lång sikt. Uppdraget ska i relevanta delar genomföras i dialog med Affärsverket svenska kraftnät, Finansinspektionen, Försvarets materielverk, Länsstyrelsen i Stockholms län, Länsstyrelsen i Skåne län, Länsstyrelsen i Västra Götalands län, Länsstyrelsen i Norrbottens län, Post- och telestyrelsen, Statens energimyndighet, Strålsäkerhetsmyndigheten och Transportstyrelsen.

Försvarsmakten och Säkerhetspolisen
2021–2022
5.3.8.

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 NISÖ 2021

Uppdaterad

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 i samverkan med Försvarsmakten, Säkerhetspolisen, PTS och Polismyndigheten
2019–2022
5.4.2.

Genomföra återkommande samövningar med cybersäkerhets-myndigheter 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
2020–2022
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 Uppdaterad

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 och tills vidare
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

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

Polismyndigheten
2020–2022
6.1.4.

Etablera en cybersäkerhetsgrupp inom ITS Ny åtgärd

PTS etablerar en cybersäkerhetsgrupp inom standardiseringsorganet Svenska Informations- och Telekommunikationsstandardiseringen, ITS. Denna etablering möjliggör att ett aktivt informationsutbyte bedrivs med svenska företag och myndigheter som är aktiva i internationell standardisering inom det aktuella området.

PTS
2021–2022
6.1.5.

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

FMV deltar 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 för cybersäkerhet.

FMV
2019 och tills vidare
6.2.1.

Bevaka och bidra till NIS-direktivets fortsatta implementering och utveckling Uppdaterad

Den europeiska NIS-regleringens krav syftar till att öka nivån på informations- och cybersäkerhet inom ett stort antal viktiga samhällstjänster. Som nationell kontaktpunkt för NIS-direktivet och nationell CSIRT-enhet, deltar MSB i EU:s strategiska samarbetsgrupp för NIS-frågor (NIS Cooperation Group) och nätverket för EU:s CERT-funktioner (CSIRT Network). Under 2022 arbetar EU:s strategiska samarbetsgrupp bland annat med revidering av NIS-regleringen, utveckling av nya arbetsgrupper, samt gemensamma metoder för storskaliga incidenter.

MSB

2019 och tills vidare

6.2.2.

Slutord

Slutord

Myndigheterna har nu arbetat med regeringsuppdraget om att ta fram och årligen redovisa den samlade informations- och cybersäkerhetshandlingsplanen under snart fyra år. 2022 års redovisning är den fjärde inom ramen för uppdraget. I handlingsplanen har det varit möjligt att följa de åtgärder myndigheterna har vidtagit för att bidra till målen i den nationella strategin för samhällets informations- och cybersäkerhet (skr. 2016/17:213) på ett strukturerat och spårbart sätt.

Under kommande år kommer myndigheterna att förbereda slutrapporten av uppdraget som lämnas till Regeringskansliet 1 mars 2023. Rapporten kommer att spänna över hela uppdragstiden och försöka belysa om arbetet lett till de effekter som regeringen avsåg med uppdraget.

Sedan uppdraget ställdes till myndigheterna har mycket hänt i omvärlden. Hotbilden mot samhällets informations- och cybersäkerhet kvarstår och har på många områden förändrats och ökat. För att möta cyberhoten inrättade regeringen det nationella cybersäkerhetscentret 2020. I centret ingår samtliga av de myndigheter som har i uppdrag att ta fram och redovisa denna handlingsplan. Eftersom både SAMFI-strukturen och NSIT avvecklats med anledning av att cybersäkerhetscentret inrättades, övergick myndigheternas samverkan kring handlingsplanen till detta nya sammanhang.

Cybersäkerhetscentret utgör en långsiktig plattform för myndighetssamverkan och gemensamt arbete som kan bidra till ett samordnat myndighetsagerande för att stärka Sveriges cybersäkerhet även efter det att detta uppdrag avslutas.

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		22
1.1.3.	Utbilda privata aktörer avseende Försvarsmaktens säkerhetsskyddskrav	Försvarsmakten	Uppdaterad, tidplan	22
1.1.4.	Leverera aggregerat underlag om hot och sårbarheter	Säkerhetspolisen, FRA och Försvarsmakten		22
1.1.6.	Ta fram stödjande material för tillämpning av ny säkerhetsskyddslag	Säkerhetspolisen och Försvarsmakten	Uppdaterad, tidplan och innehåll	23
1.1.9.	Utveckla och förvalta nationell terminologi	MSB	Uppdaterad, tidplan	23
1.1.11.	Utveckla MSB:s metodstöd för systematiskt informationssäkerhetsarbete	MSB	Uppdaterad, tidplan och innehåll	23
1.1.14.	Stödja aktörernas arbete att utveckla robusta fysiska förutsättningar för verksamhet och ledning	MSB		23
1.1.15.	Genomföra en årlig konferens om säkra kommunikationer	MSB		24
1.1.19.	Regelbunden uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen	MSB	Ny åtgärd	24
1.1.20.	Ta fram stödjande material för säkerhetsåtgärder i informationssystem	MSB	Ny åtgärd	24
1.3.1.	Sprida kunskap och erfarenheter om arbetet med informationsvärdering till andra myndigheter och organisationer	Försvarsmakten		25
1.3.2.	Höja kunskapen avseende informationssäkerhet inom Försvarsmaktens tillsynsområde för säkerhetsskydd	Försvarsmakten	Uppdaterad, tidplan	25

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

#	Åtgärd	Ansvarig myndighet	Status	Sida
1.3.3.	Etablera samverkansmöjligheter för NIS-aktörer	MSB	Uppdaterad, innehåll	25
1.3.6.	Utöka samverkan med andra myndigheter, internationella partners och civila företag inom försvarssektorn avseende lägesbild och incidenthanteringsförmåga	Försvarsmakten		25
1.3.8.	Etablera nationell samverkan inom nationellt cybersäkerhetscenter	FRA, Försvarsmakten, MSB, och Säkerhetspolisen i nära samverkan med Polismyndigheten, FMV och PTS	Ny åtgärd	26
1.4.1.	Fortsätta utveckling av föreskrifter för säkerhetsskydd	Säkerhetspolisen och Försvarsmakten	Uppdaterad, tidplan och innehåll	26
1.4.2.	Stödja och samordna utveckling av NIS-föreskrifter rörande säkerhetsåtgärder	MSB	Uppdaterad, tidplan	26
1.4.4.	Vidareutveckla stödet för samordnad tillsyn inom NIS	MSB		26
1.4.5.	Inrättande av nationell myndighet för cybersäkerhetscertifiering	FMV	Ny åtgärd	27

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

#	Åtgärd	Ansvarig myndighet	Status	Sida
2.1.2.	Genomföra projekt för att minska beroendet av centrala funktioner i elektroniska kommunikationsnät och -tjänster	PTS	Uppdaterad, innehåll	27
2.1.4.	Utveckling och anskaffning av it-säkerhetsprodukter	Försvarsmakten och FMV		27
2.1.5.	Etablera nya säkra och robusta kommunikationer för aktörer med särskilda säkerhetsskyddsbehov	Försvarsmakten		27
2.1.6.	Etablera nya säkra och robusta kommunikationstjänster för aktörer inom allmän ordning, säkerhet, hälsa och försvar	MSB		28
2.1.8.	Följa och bidra till utvecklingen av säker kommunikation för andra organisationer	Försvarsmakten		28
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, tidplan	28
2.4.2.	Fortsatt utveckling av signalskyddssystem	Försvarsmakten och FMV		29
2.4.4.	Införa krypterat mobilt tal och textmeddelandefunktion för säkerhetsskyddsklassen Begränsat Hemlig	Försvarsmakten		29

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

#	Åtgärd	Ansvarig myndighet	Status	Sida
2.4.5.	Införa säkert tal för säkerhetsskydds-klassen Hemlig i totalförsvaret	Försvarsmakten i samverkan med FMV, MSB och FRA	Uppdaterad, tidplan	29
2.4.6.	Utveckla och införa säkert meddelande-krypto för säkerhetsskyddsklassen Hemlig i totalförsvaret	Försvarsmakten i samverkan med FMV, MSB och FRA		30
2.5.2.	Främja nyttjandet av skyddade satellittjänster för tid, takt och position för samhällskritiska funktioner	MSB		30
2.5.3.	Genomföra en nationell satsning på ökad säkerhet i cyberfysiska system	MSB		30

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

#	Åtgärd	Ansvarig myndighet	Status	Sida
3.1.1.	Öka incidenthanteringsförmågan avseende kvalificerade hotaktörer	Säkerhetspolisen, FRA och Försvarsmakten		31
3.1.2.	Tillhandahålla medvetandehöjande material om att minska störnings-känsligheten vid användandet av trådlös kommunikation i industriella informations- och styrsystem som används i samhällsviktig verksamhet	MSB		31
3.1.4.	Fortsätta utvecklingen av nationell Cyber Range	MSB tillsammans med Försvarsmakten		31
3.1.6.	Utveckla nationellt cybersäkerhetscenter	FRA, Försvarsmakten, MSB, och Säkerhets-polisen i nära samverkan med Polismyndigheten, FMV och PTS	Uppdaterad, innehåll	32
3.1.7.	Samordna incidenthantering inom nationellt cybersäkerhetscenter	FRA, Försvarsmakten, MSB, och Säkerhets-polisen i nära samver-kan med Polismyndig-heten, FMV och PTS	Ny åtgärd	32
3.3.1.	Leverera militärstrategiska lägesbilder rörande statusen i Försvarsmaktens informations- och ledningsstödsystem, hot och risker	Försvarsmakten		32
3.3.2.	Tillhandahålla TDV till de mest skyddsvärda verksamheterna	FRA i samverkan med Säkerhetspolisen		33
3.3.3.	Förstärka förmågan att genomföra defensiva och offensiva operationer mot en kvalificerad motståndare i cybermiljön	Försvarsmakten med stöd av FRA		33

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

#	Åtgärd	Ansvarig myndighet	Status	Sida
4.1.3.	Samarbeta med brottsbekämpande myndigheter	Polismyndigheten		33
4.2.1.	Använda europeiska resurser för brottsförebyggande kampanjer	Polismyndigheten		34
4.2.2.	Delta i samarbete med finans- och transaktionsmarknaderna	Polismyndigheten		34
4.2.3.	Uppbyggande av europeiskt nätverk för förebyggande av cyberbrott	Polismyndigheten		34
4.2.4.	Nordiskt preventionsarbete gällande cyberbrott	Polismyndigheten		34
4.2.6.	Delta i brottsförebyggande samarbete med Stöldskyddsföreningen	Polismyndigheten och MSB	Uppdaterad, tidplan och innehåll	34

Strategisk prioritering 5. Öka kunskapen och främja kompetensutvecklingen

#	Åtgärd	Ansvarig myndighet	Status	Sida
5.1.2.	Vidareutveckla analysförmåga av hårdvara	FRA		35
5.1.3.	Leverera anpassade lägesbilder inom nationellt cybersäkerhetscenter	FRA, Försvarsmakten, MSB, och Säkerhetspolisen i nära samverkan med Polismyndigheten, FMV och PTS	Ny åtgärd	35
5.3.1.	Utveckla förutsättningar för kompetensförsörjning	FRA, Säkerhetspolisen och Försvarsmakten		35
5.3.2.	Etablera en modell för kompetensutveckling	Försvarsmakten tillsammans med FRA och Säkerhetspolisen		36
5.3.3.	Stärka och vidareutveckla forskning och teknikutveckling inom cyberförsvarsområdet	Försvarsmakten		36
5.3.4.	Etablera anpassad uttagning och rekrytering mot cyberinriktningen	Försvarsmakten och FRA		36
5.3.6.	Finansiera forskning för att möta framtidens utmaningar på informations- och cybersäkerhetsområdet	MSB	Uppdaterad, innehåll	36
5.3.7.	Etablera nationellt samordningscenter för cybersäkerhet (NSC)	MSB	Ny åtgärd	37
5.3.8.	Kartlägga behovet av kompetensförsörjning inom säkerhetsskyddsområdet	Försvarsmakten och Säkerhetspolisen	Ny åtgärd	37
5.4.2.	Genomföra NISÖ 2021	MSB i samverkan med Försvarsmakten, Säkerhetspolisen, PTS och Polismyndigheten	Uppdaterad, tidplan	37

Strategisk prioritering 5. Öka kunskapen och främja kompetensutvecklingen

#	Åtgärd	Ansvarig myndighet	Status	Sida
5.4.3.	Genomföra återkommande samövningar med cybersäkerhetsmyndigheter gällande hantering av it-incidenter	MSB	Uppdaterad, tidplan	38
5.4.4.	Genomföra årlig informations- och cybersäkerhetsövning SAFE Cyber	Försvarsmakten i samverkan med FRA, MSB och Säkerhetspolisen		38

Strategisk prioritering 6. Stärka det internationella samarbetet

#	Åtgärd	Ansvarig myndighet	Status	Sida
6.1.1.	Arbeta för internationell harmonisering av regler och krav för informationssäkerhet	Försvarsmakten	Uppdaterad, tidplan	38
6.1.3.	Utveckla och förbättra standarder och metodik för krav och kontroll av cybersäkerhet i it-produkter	FMV		39
6.1.4.	Resurs vid Europol	Polismyndigheten		39
6.1.5.	Etablera en cybersäkerhetsgrupp inom ITS	PTS	Ny åtgärd	39
6.2.1.	Delta i internationellt samarbetsforum för industrisäkerhet	FMV		39
6.2.2.	Bevaka och bidra till NIS-direktivets fortsatta implementering och utveckling	MSB	Uppdaterad, innehåll	40

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
1.1.8.	**Revidering och komplettering av MSB:s föreskrifter för statliga myndigheter** 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	2020

#	Åtgärd	Ansvarig myndighet	Klar
1.1.12.	**Utforma vägledning för grundläggande it-säkerhetsåtgärder** 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	2020
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
1.1.16.	**Ta fram en struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen** MSB utvecklar en struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen (Ju2019/03058/SSK, Ju2019/02421/SSK). Uppföljningen kommer att ske med stöd av en modell som innehåller en bred uppsättning frågor om det systematiska informationssäkerhetsarbetet hos respektive organisation. Modellen genererar automatiskt en nivåbedömning och hänvisningar till hur organisationen kan komma vidare i arbetet. Efter inrapportering till MSB får organisationen även återkoppling om hur resultatet förhåller sig till andra, liknande organisationer. MSB kommer att redovisa en samlad bedömning om nivån på det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen till regeringen. Dessutom ska resultatet användas för att utveckla MSB:s stöd och vidareutveckla uppföljningsstrukturen. Uppföljningen är tänkt att ske vartannat år. Uppdraget genomförs 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	2021

#	Åtgärd	Ansvarig myndighet	Klar
1.1.17.	**Se över föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster** I enlighet med förordningen om informationssäkerhet för leverantörer av samhällsviktiga och digitala tjänster, genomför MSB en översyn av gällande föreskrifter för anmälan och identifiering av verksamheter som berörs av Kasseersättningen. Arbetet kommer att ske i nära samarbete med NIS-tillsynsmyndigheterna och Socialstyrelsen och syftar till att identifiera behov av att förtydliga eller justera kriterierna för vilka verksamheter som berörs av NIS-regleringen i egenskap av leverantörer av samhällsviktiga tjänster.	MSB	2021
1.2.1.	**Genomföra en förstudie till nationell modell för cybersäkerhet** En förstudie genomförs inom ramen för det nationella cybersäkerhetscentret isyfte att centret ska driva det fortsatta arbetet med den nationella modellen.	MSB, FRA, FMV, Försvarsmakten, PTS, Polismyndigheten och Säkerhetspolisen	2021
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
1.3.5.	**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	2020
1.3.7.	**Förbereda etablerandet av ett nationellt cybersäkerhetscenter** 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
1.4.3.	**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

#	Åtgärd	Ansvarig myndighet	Klar
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
2.1.9.	**Etablera WIS över SGSI** 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	2021
2.3.1.	**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 skynd-samt vidta säkerhetsåtgärder för att möta specifika sårbarheter i operatörernas nät och eller tjänster.	PTS	2020
2.3.2.	**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. Regeringen beslutade 2020 att ge PTS ”Uppdrag att utreda förutsättningarna för att tillgängliggöra det nationella systemet för spårbar tid och frekvens för relevanta aktörer” (dnr I2020/01811/D). Uppdraget ska slutredovisas senast den 15 januari 2021. Utredningen visade att det är möjligt för aktörer utanför sektorn elektronisk kommunikation att ansluta sig till tjänsten. En produktspecifikation är under framtagande för att tydliggöra för aktörer utanför sektorn vad som ingår i tjänsten samt kostnader för anslutning.	PTS	2021

#	Åtgärd	Ansvarig myndighet	Klar
2.4.3.	**Ta fram process för hantering av signalskydd** 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 signal- skydd. 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	2020
2.5.1.	**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	2021
3.3.4.	**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	2020
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
4.1.2	**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	2020
5.2.1.	**Genomföra en riktad informationskampanj för att höja säkerhetsmedvetandet** 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	2020

#	Åtgärd	Ansvarig myndighet	Klar
5.2.2.	**Genomföra riktade utbildningsinsatser på informationssäkerhetsområdet till offentlig sektor** 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	2021
5.2.3.	**Nationell kampanj ”Tänk säkert”** 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
5.3.5.	**Genomföra en förstudie rörande kompetensförsörjning inom informations- och cybersäkerhetsområdet för samhället** 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	2021
5.4.1.	**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	2021
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
1.1.5.	**Genomföra en förstudie i syfte att öka myndigheters deltagande i standardiseringsarbete inom ramen för SIS TK318** MSB ska genomföra en förstudie i syfte att belysa myndigheters betydelse för ett strategiskt och långsiktigt arbete med standardisering avseende systematiskt och riskbaserat informations- och cybersäkerhetsarbete, det område som SIS TK318 arbetar med. Det nationella engagemanget för nationellt, europeiskt och internationellt arbete med standardisering inklusive förmågan att nyttja resultaten från standardiseringsarbetet inom informations- och cybersäkerhetsområdet behöver stärkas. Förstudien ska fokusera på myndigheters deltagande och det verksamhetsområde som SIS TK318 arbetar inom. Förstudien ska inhämta synpunkter från och förankras hos berörda myndigheter och organisationer. Åtgärden avskrivs då MSB bedömer att de resursmässiga förutsättningarna i relation till annan prioriterad verksamhet saknas. MSB fortsätter att verka för ökat deltagande i standardiseringsarbete på området informations- och cybersäkerhet inom ramen för det löpande arbetet i TK318.	MSB	2021
1.1.7.	**Genomföra en årlig informationssäkerhetskonferens** 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. Motsvarande konferens genomförs inom ramen för det nationella cybersäkerhetscentret.	MSB, FRA, FMV, Försvarsmakten, PTS, Polismyndigheten och Säkerhetspolisen	2020
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

#	Åtgärd	Ansvarig myndighet	Avskriven
1.1.18.	**Genomföra en årlig cybersäkerhetskonferens** Planera och genomföra årlig cybersäkerhetskonferens för det nationella cybersäkerhetscentrets målgrupper. Målet för konferensen är att stärka Sveriges cybersäkerhet genom att belysa de frågor och områden som cybersäkerhetscentret hanterar, såsom aktuella hot, sårbarheter och skyddsåtgärder. Åtgärden omfattas av verksamheten som beskrivs i åtgärd 3.1.6.	MSB, FRA, FMV, Försvarsmakten, PTS, Polismyndigheten och Säkerhetspolisen	2021
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. PTS avvaktar med åtgärden efter omprioritering av verksamheter.	PTS	2019
2.1.7.	**Etablera en federationstjänst för SGSI-anslutna aktörer** 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. Identifierade behov av omprioriteringar i förvaltningen och utvecklingen relaterat till SGSI gör att åtgärden avskrivs i handlingsplanen.	MSB	2020

#	Åtgärd	Ansvarig myndighet	Avskriven
2.2.1.	**Utreda elektronisk kommunikations oberoende av funktioner utomlands** PTS fortsätter att utreda frågan och ser behov av djupare analyser i samråd med andra myndigheter, exempelvis Säkerhetspolisen och Regeringskansliet. 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 avvaktar med åtgärden som behöver utredas bredare och djupare. Ett sådant samarbete kommer att behöva göras i samråd med andra myndigheter.	PTS	2021
3.1.3.	**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. Då etableringen av ett sensorsystem för NIS-leverantörer med önskad funktionalitet bedöms kräva förändrade juridiska förutsättningar, pausas arbetet som beskrivs i åtgärden efter genomförd teknisk förstudie och rättslig analys.	MSB	2021
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

#	Åtgärd	Ansvarig myndighet	Avskriven
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
3.2.2.	**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. Den typ av samverkan som har bedrivits inom NSIT kommer fortsättningsvis att bedrivas inom ramen för det nationella cybersäkerhetscentret.	Säkerhetspolisen, Försvarsmakten och FRA	2020
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
4.2.5.	**Delta i samarbete med Internetstiftelsen för att öka den enskildes säkerhet på nätet** Polismyndigheten deltar i samarbetet ”Nätsäker” med Internetstiftelsen och andra aktörer för att minska den enskildes risker på nätet. Samarbetet har avslutats.	Polismyndigheten	2021

#	Åtgärd	Ansvarig myndighet	Avskriven
5.1.1.	**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. Åtgärden uppgår i arbetet med regeringsuppdraget att ta fram en struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen (Ju2019/03058/SSK, Ju2019/02421/SSK).	MSB	2020

Bilaga 2:

Uppdrag om en samlad informations- och cyber-säkerhetshandlingsplan 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 MSB1875 - mars 2022 ISBN 978-91-7927-210-4