2017-06-07

Expertgrupp säkerhet

Rapport med förslag till fortsatt arbete 2017 -2018

Innehåll

1. Sammanfattning och förslag

Med den digitala utvecklingen har säkerhetsfrågorna fått en allt större aktualitet och både regeringen och EU har i olika sammanhang lyft upp säkerhetsfrågorna. eSams styrgrupp beslutade i december 2016 att ge arbetsgruppen i uppdrag att inrätta en *temporär expertgrupp för säkerhetsfrågor* som ska fungera parallellt med de befintliga expertgrupperna för arkitektur och juridik. I den temporära expertgruppens uppdrag ingick att ta fram underlag för beslut i styrgruppen om gruppen ska permanentas. I uppdraget ingick även att genomföra en behovsinventering för säkerhetsfrågor som behöver hanteras i samverkan och ansvar för frågorna, identifiera nya riskområden som uppstår vid samverkan samt arbeta fram principer för styrning av säkerhet och arbetssätt vid samverkansprojekt.

Förslag
Den temporära expertgruppen för säkerhet föreslås inrättas som en permanent grupp samt kompletteras med en referensgrupp där varje medlem kan utse en representant.

Inriktningen bör vara på säkerhetsområden och säkerhetsfrågor som är centrala för digitaliseringsarbetet med fokus på sådant som behöver hanteras i samverkan mellan organisationer och som inte redan hanteras av andra specifikt ansvariga myndigheter.

Resultat av arbetet
Den temporärara expertgruppen har i *behovsinventeringen* identifierat ett antal befintliga och nya risk-/fördjupningsområden som presenteras under följande rubriker:

1. Verksamhetsinriktning och riskbedömning
2. Informationstillgångar och klassning
3. Säkerhet under hela informationslivscykeln
4. Sammanställningar av information och öppna data
5. Styrning av åtkomst i samverkan
6. Efterlevnad och uppföljning
7. Utveckling av tjänster i samverkan
8. It-försörjning och fysisk säkerhet
9. Civilt försvar och säkerhetsskydd
10. Ny teknik och nya utmaningar

Ansvarsfrågorna är beskrivna dels utifrån gällande regelverk och ansvariga myndigheter, dels i förslaget på principer där ansvarsfrågorna i samverkansprojekt tas upp i flera punkter. I förslaget på *principer* är dessa beskrivna utifrån ett livscykelperspektiv enligt följande uppställning:

- Initiala och övergripande ansvarsfrågor
- Hantering av krav och prioritering inför utveckling
- Utveckling och införande
- Hantering under tjänstens livscykel
- Avveckling av en tjänst
- Granskning och mätning

Slutsatser och förslag i denna rapport behöver vidareutvecklas och bör användas som ett underlag för det fortsatta arbetet i en permanent expertgrupp eller av andra aktörer.

2. Introduktion

2.1. Bakgrund

eSams styrgrupp beslutade i december 2016 att ge arbetsgruppen i uppdrag att inrätta en *temporär expertgrupp för säkerhetsfrågor* som ska fungera parallellt med de befintliga expertgrupperna för arkitektur och juridik. I den temporära expertgruppens uppdrag ingick att ta fram underlag för beslut i styrgruppen om gruppen ska permanentas. Underlaget skulle presenteras för arbetsgruppen i maj 2017 för beslut på nästkommande styrgruppsmöte. I uppdraget för den temporära expertgruppen ingick att:

- Genomföra en behovsinventering för att skapa en ”bruttolista” för säkerhetsfrågor som behöver hanteras i samverkan. Det ska framgå hur dagens ansvar för frågorna ser ut.
- Identifiera nya riskområden som uppstår vid samverkan för att kunna göra en bättre samverkansriskanalys.
- Arbeta fram principer för styrning av säkerhet och arbetssätt vid samverkansprojekt. Befintliga regelverk inom området ska beaktas för att kvalitetssäkra framtagandet av nya säkerhetsprinciper vid samverkan.

2.2. Syfte

När den temporära expertgruppen för säkerhetsfrågor inrättades var syftet att se till att de tjänster som levereras inom eSam håller rätt säkerhet.

2.3. Genomförande

Den temporära säkerhetsgruppen har arbetat under våren 2017 med regelbundna möten, diskussioner och avstämningar. Utöver arbetet med leverans enligt uppdraget har gruppen också diskuterat och delat återanvändbara verktyg och metoder som kan ge snabb nytta. I arbetet har underlag från befintliga regelverk och standarder använts, liksom metoder och vägledningar från e-delegationen/eSam. Gruppen har bestått av följande personer:

- Henrik Axelsson, Skatteverket
- Peter Baggesen, Polismyndigheten
- Susanne Borenberg, Naturvårdsverket
- Johnny Carlberg, eSam
- Fredrik Hasselrot, Migrationsverket
- Liisa Laukkanen, Försäkringskassan
- Ulf Ranestedt, Pensionsmyndigheten
- Ylva Söderlund, Säkerhetspolisen (adjungerad)
- Gunnar Wennerholm, Tillväxtverket (ordförande)
- Carl Önne, Myndigheten för samhällsskydd och beredskap (adjungerad)

3. Utmaningar inom säkerhetsområdet

Digitalisering - möjligheter och utmaningar

Digitaliseringen är en av de viktigaste tillväxtdrivande faktorerna i dag. Ökad global konkurrens, förändrat kundbeteende, nya affärsmodeller mm. innebär både krav och möjligheter och påverkar såväl näringsliv, offentlig sektor som samhället som helhet. Den offentliga sektorn har en viktig roll i att skapa förutsättningar för en framgångsrik utveckling, kring såväl infrastruktur, regelverk, standarder som att utnyttja it på ett effektivt sätt både internt och för externa tjänster.

Samtidigt innebär beroendet av it-lösningar att sårbarheten ökar i en omfattning som berör allt ifrån privat integritet, cyberbrott, samhällets infrastruktur till påverkan på politiska val och beslut. Användning av nya tekniker som *molntjänster, big data/aggregering av stora datamängder, Artificiell Intelligens, Internet of Things, blockkedjor* mm. innebär både nyttor och risker. Förändrat beteende hos medborgarna, sociala medier, liksom sammanblandning av privat och professionellt har också visat sig innebär nya risker.

MSB:s rapport *Informationssäkerhet – trender 2015* tar upp ett antal viktiga frågor, bland annat att informationssäkerhet allt mer blir en fråga om att skydda hela samhället och dess välstånd, komplexiteten i tjänsterna gör riskerna mer svåröverskådliga, frågor om privatlivet aktualiseras och konsekvenser av oplanerade driftavbrott riskerar att påverka samhällsviktiga funktioner. Den nationella säkerhetsstrategin från 2017 ger i avsnittet *Informations- och cybersäkerhet, digitala risker* exempel på utmaningar och antagonistiska hot som dataintrång, sabotage eller spionage, försök att påverka utgången av demokratiska val mm. I åtgärderna lyfts bland annat fram vikten av samordning och samverkan mellan myndigheter och andra aktörer och inte minst samverkan på EU-nivå.

Offentliga sektorns digitalisering och säkerhet

Regeringens strategi ”Med medborgaren i centrum” anger i sina mål för en digitalt samverkande statsförvaltning bland annat *Högre kvalitet och effektivitet i verksamheten*. Även kommuner och landsting har en liknande målbild. En viktig förutsättning för att nå detta är en god informationssäkerhet, vilket innebär att vi upprätthåller informationens krav på *konfidentialitet*, *riktighet*, *tillgänglighet* och *spårbarhet*.

Genom en god informationssäkerhet kan berörda aktörer känna tillit till varandra och varandras information, vilket är en förutsättning för att vi ska kunna utnyttja digitaliseringens möjligheter. Olika aktörer har olika förutsättningar för sin verksamhet och i sitt informationssäkerhetsarbete och därför behövs insatser för att öka möjligheterna för samordning och samverkan.

Avvägningar mellan öppenhet och säkerhet

Myndigheter ställs ofta inför komplexa frågeställningar för att samtidigt hantera öppenhet i informationshantering och krav på säkerhet. För att upprätthålla öppenhet, transparens och effektivitet ställs också krav på att enkelt kunna dela data mellan myndigheter och med privatpersoner och företag, liksom att man inte ska behöva lämna samma uppgift flera gånger till myndigheter. Samtidigt kan integritetskrav innebära att samkörning av viss information och att information utnyttjas för annat ändamål än det ursprungliga kan vara tveksamt eller otillåtet. En säker och korrekt bearbetning av personuppgifter ställer därför krav på både processer och teknik och innebär ibland också att man måste avstå från andra nyttor.

Information som delas och som aggregeras

När information aggregeras och sammanställs uppkommer också nya risker. Den information som i sig själv tycks vara harmlös kan tillsammans med annan information innebära ett hot mot individens integritet eller samhällets säkerhet. Denna aspekt blir allt väsentligare i och med den ökande mängden av data i samhället och mer tillgängliggörande av öppna data. Vem som har ansvaret för den aggregerade informationen kan ofta vara oklart, men myndigheterna behöver ändå ta hänsyn till hur informationen kan komma att hanteras i senare skeden och på annat sätt än avsett.

Ansvar, regler och säkerhetsarbete i praktiken

Utmaningar kan ofta inte lösas av myndigheterna var för sig utan måste hanteras samordnat och med överenskommelser på olika nivåer och aspekter, vad gäller såväl beslutsnivå som teknik och juridik. Många av dessa utmaningar återkommer hos många myndigheter och bör lösas på ett gemensamt och generellt sätt. Övergripande regler och standarder beslutas av regering och centrala myndigheter, men det praktiska genomförande måste ske i en samverkan mellan de olika berörda myndigheterna.

Säkerhetsområdet omfattar många aspekter med flera olika författningar och myndigheter med olika ansvar. Området kan anses vara välreglerat och väl tillgodosett med ansvariga myndigheter men samtidigt finns det, som nämnts, många utmaningar både vad gäller samordning och i att faktiskt genomföra de säkerhetsåtgärder som behövs i den offentliga sektorn och i samhället i stort.

Myndigheternas säkerhetskultur och säkerhetsaspekter i utvecklingsarbete

Frågan om säkerhetskultur lyfts upp allt mer. I säkerhetspolisens årsbok 2016 beskrivs olika typer av hot mot svenska myndigheter och vilket arbete som behöver bedrivas för att åtgärda säkerhetsluckor. Det handlar bland annat om säkerhetsorganisation, säkerhetsanalyser, rutiner vid upphandlingar mm. Man konstaterar i en genomförd inventering att ju mer frekvent en myndighet hanterar generella säkerhetsfrågor i sin kärnverksamhet, desto bättre är de på säkerhetsskydd. Många myndigheter har dock brister i sitt säkerhetsarbete, bland annat vad gäller säkerhetsanalyser, som är grunden för allt säkerhetsskyddsarbete.

Eftersom it idag är en så integrerad del av all verksamhet är det viktigt att säkerhetsaspekter och skydd av information och system ingår som en naturlig del i både utvecklingsarbete och förvaltning och i det dagliga arbetet i verksamheten.

4. Uppdrag och resultat

4.1. Befintliga risker och nya riskområden

I uppdraget för den temporära expertgruppen ingick att genomföra en behovsinventering för att skapa en ”*bruttolista” för säkerhetsfrågor* som behöver hanteras i samverkan och även att identifiera *nya riskområden* som uppstår vid samverkan. För att ge ett bättre sammanhang presenteras i avsnitt 4.2 alla områden tillsammans.

Samtliga områden innehåller självfallet också i någon omfattning nya riskområden jämfört med om endast en enskild organisation hanterar informationen. Några områden som bedömdes innehålla risker av olika slag som inte tidigare uppmärksammats i tillräcklig omfattning är bland annat: *verksamhetsinriktning och riskbedömning, informationstillgångar och klassning, säkerhet under hela informationslivscykeln, sammanställningar av information och öppna data, styrning av åtkomst i samverkan, it-försörjning och fysisk säkerhet, ny teknik och nya utmaningar.*

Listan har fokus på viktiga säkerhetsområden och säkerhetsfrågor kopplat till den offentliga sektorns digitaliseringsarbete och vad som behöver hanteras i samverkan mellan organisationer. I avvägningarna har hänsyn tagits till befintliga standarder och regler och hur väl olika frågor redan kan anses omhändertagna i regler och av myndigheter. För att få en mer samlad bild av viktiga säkerhetsområden för en specifik organisation rekommenderas fördjupning i standarden SS-EN ISO/IEC 27002:2017 som tar upp följande säkerhetskategorier:

- Informationssäkerhetspolicy
- Organisation av informationssäkerhetsarbetet
- Personalsäkerhet
- Hantering av tillgångar
- Styrning av åtkomst
- Kryptering
- Fysisk och miljörelaterad säkerhet
- Driftsäkerhet
- Kommunikationssäkerhet
- Anskaffning, utveckling och underhåll av system
- Leverantörsrelationer
- Hantering av informationssäkerhetsincidenter
- Informationssäkerhetsaspekter avseende hantering av verksamhetens kontinuitet
- Efterlevnad

Den framtagna listan i avsnitt 4.2 kan ses som en komplettering och fördjupning av ovanstående, där riskområdena ses i ett större samhälleligt sammanhang och med den komplexitet som samverkan innebär.

4.2. Behovsinventering av riskområden

Den framtagna listan utgör ett underlag för bedömning av säkerhetsgruppens fortsatta arbete och inriktning. Tabellen nedan innehåller de områden som identifierades utifrån en gemensam väsentlighetsprioritering. Flera av områden har nära kopplingar och går delvis i varandra, men kan ändå ses som åtskilda utifrån vilket perspektiv man närmar sig frågan.

Prioriteringsgrunder utgjordes bland annat av hur väl området redan var hanterat av andra aktörer såsom tillsynsmyndigheter eller myndigheter med sektorsansvar. Samverkansfrågor och frågor som lätt hamnar mellan stolarna har av naturliga skäl fått en särskild fokus här. Specifika samverkansrelaterade fördjupningsområden sammanfattas i högra kolumnen. I efterföljande avsnitt ges en mer utförlig beskrivning av respektive område och fördjupningsområden.

Område	Föreslagna fördjupningsområden (”bruttolista”)
1. Verksamhetsinriktning och riskbedömning	• Säkerhetskultur och riskbedömningar • Regler, principer och intresseavvägningar • Styrning och överenskommelser i säkerhetsfrågor
2. Informationstillgångar och klassning	• Fastställande av informationsägarskap vid samverkan • Gemensam klassning och skyddsnivå • Förändring av klassningen vid informationsutbyten • Säkerhetsåtgärder utifrån olika sekretessregler i registerlagar
3. Säkerhet under hela informationslivscykeln	• Principer för ansvar under en informationslivscykel • Hantering av grunddata i utbyte mellan organisationer • Risker och skyddsvärde vid olika status
4. Sammanställningar av information och öppna data	• Avvägning mellan nytta och risk vid sammanställning • Ägarskap av aggregerad information • Öppna data
5. Styrning av åtkomst i samverkan	• Ansvar för behörighetskontroll och spårbarhet • Säkerhetsnivå för identiteter
6. Efterlevnad och uppföljning	• Ansvar för efterlevnad och uppföljning vid samverkan.
7. Utveckling av tjänster i samverkan	• Säkerhetsaktiviteter före it-utveckling • Säkerhetsaktiviteter under utveckling/införande av it-stöd
8. It-försörjning och fysisk säkerhet	• Säkerhetsaspekter vid gemensamt producerade tjänster • Fysisk säkerhet
9. Civilt försvar och säkerhetsskydd	• Risker vid ökad koncentration av samhällsviktig verksamhet • Krisberedskap, civilt försvar och digitalisering • Gemensam prioritering av samhällsviktig verksamhet • Ökat beroende av ett mindre antal privata aktörer • Säkerhetsskydd och samverkan
10. Ny teknik och nya utmaningar	• Omvärldsbevakning kring hot och risker med ny teknik • Förhållningssätt och åtgärder när ny teknik tillkommer

4.2.1. Verksamhetsinriktning och säkerhetskultur

Här avses främst hur olika verksamhetsinriktning kan innebära utmaningar för informationssäkerheten vid samverkan. Olika organisationer har olika *säkerhetskulturer* utifrån sitt uppdrag, verksamhet, ansvarsområde och risksituation. Detta märks exempelvis på olika krav avseende konfidentialitet respektive tillgänglighet, där konsekvenserna av en brist kan variera stort. Detta leder till att skillnader mellan myndigheternas:

- bedömningsgrund för risker och åtgärder (olika riskaversion)
- vana och förmåga att se risker flera led framåt i en process
- rutiner för utbildning, riskhantering och åtgärder
- prioritering av effektivitetsmål respektive säkerhetsmål
- definitioner och användning av begrepp
- organisation och inriktning på säkerhetsarbetet.

Förslag på fördjupningsområden

- **Säkerhetskultur och riskbedömningar**
  Riskbedömningar och informationsklassningar blir rimligen olika för exempelvis myndigheter inom rättsväsendet, den sociala sektorn och handels- och tillväxtfrämjande myndigheter. Vissa verksamheter har fokus på *tillgänglighet* och andra på *konfidentialitet*. Skilda traditioner och synsätt inom olika myndighetssektorer kan innebära olika inriktning på säkerhetsfrågorna och i de fall myndigheter behöver dela information måste det garanteras att detta sker på ett säkert sätt. En ökad trafik och exponering av personuppgifter kan också innebära risker för id-kapningar och bedrägerier. Kriminella aktörer väljer rimligen att gå mot den i sammanhanget svagaste länken. Därför är det intressant att undersöka lämpliga metoder för att tydliggöra dessa aspekter.
- **Regler, principer och intresseavvägningar**
  Varje myndighet är ansvarig för sin riskbedömning och åtgärder för sin egen informationssäkerhet och för detta finns lämpliga metoder och vägledningar framtagna. Vid samverkan och informationsutbyte mellan myndigheter och andra aktörer behövs dock ytterligare metoder och tydliggöranden som samlad informationsanalys, informationsklassning och riskbedömning, informationsutbytesöverenskommelser, begrepps- och informationsutbytesbeskrivningar, klargörande av primär källa etc. Här ingår också metoder för att hantera intresseavvägningar mellan exempelvis tillgänglighet, effektivitet och konfidentialitet.
- **Styrning och överenskommelser i säkerhetsfrågor**
  Oavsett om det finns överenskommelser mellan myndigheter och metoder för att hantera skilda säkerhetskulturer så har myndigheter inga sanktionsmöjligheter mot varandra vid intressekonflikter, utan kan vid incidenter eller kris välja att prioritera egen verksamhet. På längre sikt kan det också ske glidningar i prioriteringar. Följden kan bli att tjänster och funktioner som kräver att flera myndigheter tillhandahåller information eller infrastruktur för gemensamma initiativ kan komma att förhindras vid incidenter. I överenskommelser mellan myndigheter behöver man därför också ta höjd för hantering av olika typer av hot och incidenter. Övergripande ansvar och styrning där många olika slags aktörer, som stat, kommun, landsting och privata företag är inblandade behöver också klargöras.

4.2.2. Informationstillgångar och klassning

För att uppfylla ambitionen med *digitalt först* behövs digitala lösningar för informationsutbyte mellan statliga och andra aktörer, vilket i sin tur kräver samsyn i skyddsnivå på informationen. Informationsklassning behövs för att säkerställa att informationen har lämplig skyddsnivå utifrån dess betydelse för såväl organisationens verksamhet, den enskilda individen som samhället i stort. Klassningen samt legala krav utgör grunden för fastställande av säkerhetsåtgärder för informationen. Det finns flera utmaningar när det gäller hantering och klassning av informationstillgångar i samverkan, men en överenskommen modell för klassning är en framgångsfaktor för att hitta rätt nivå på informationssäkerhetskraven.

Förslag på fördjupningsområden

- **Fastställande av informationsägarskap vid samverkan**
  Informationsägarskap i samverkansarbetet behöver definieras och fastställas utifrån flera aspekter, bland annat för att styra säkerhetskrav på informationsmängder som delas med annan part. Det är också nödvändigt med en samlad överblick över hur informationen flödar mellan olika aktörer och vilka förändringar som sker under informationslivscykeln.

- **Gemensam klassning och skyddsnivå**
  Olika organisationer kan ibland klassa samma information olika och även ha olika skyddsnivåer för samma informationsmängd. Går det att skapa en gemensam informationsklassning och gemensam skyddsnivå?
- **Förändring av klassningen vid informationsutbyten**
  Skyddsbehovet för olika informationsmängder kan förändras när de kombineras med annan information i gemensamma tjänster. Hur bör man hantera det faktum att enskilda informationsmängder kan ha lågt skyddsvärde, men en samlad informationsmängd har högt skyddsvärde?
- **Säkerhetsåtgärder utifrån olika lagkrav**
  Krav på säkerhetsåtgärder kan ibland variera i exempelvis vägledningar från olika tillsynsmyndigheter för likartade informationsmängder. Hur kan samverkande myndigheter hantera detta?

4.2.3. Säkerhet under hela informationslivscykeln

Informationstillgångar behöver säkras och skyddas under hela informationens livscykel. När organisationer samverkar i livshändelser och processer uppstår nya hot och risker, eftersom information successivt kan förädlas och få ett förändrat innehåll under livscykeln, både i sig själv och i sitt samband med annan information. Vidare skiljer sig definitioner och skyddsnivåer ofta åt mellan olika organisationer. Det behövs därför vägledning och metoder för ansvar och hantering av information i organisationsöverskridande processer under hela informationens livscykel.

Förslag på fördjupningsområden

- **Principer för ansvar under en informationslivscykel**
  Både information i sig och dess metadata förändras under en process. För information som hanteras i samverkan i flera organisationer behövs metoder för att tydliggöra ansvar, begreppsdefinitioner och säkra spårbarhet under hela informationens livscykel.
- **Hantering av grunddata i utbyte mellan organisationer**
  Definitioner av och regler kring grunddata är en viktig fråga vid utveckling av digitala tjänster, där också säkerhetsaspekterna vid utbyte av data mellan olika organisationer behöver lyftas upp tillsammans med arkitekturfrågorna.
- **Risker och skyddsvärde vid olika status**
  Under en livscykel för ett informationsobjekt kan klassning av informationen skilja sig mellan olika organisationer. Skyddsvärdet kan också förändras under livscykeln utifrån informationens status, exempelvis om det är ett utkast, som kan ha högt skyddsvärde, eller om handlingen blivit upprättad och därmed allmän handling med lågt skyddsvärde (givet att inte sekretess föreligger).

4.2.4. Sammanställningar av information och öppna data

Digitaliseringen och ny teknik innebär omfattande möjligheter till nya sammanställningar av information. Detta ger förutsättningar för nya tjänster, tillväxt i ekonomin och högre välfärd. Bättre sammanställningar av information innebär bättre möjligheter för myndigheter att arbeta effektivt och att säkra både rättigheter och skyldigheter för privatpersoner och företag.

Polis, försvar och andra myndigheter kan också på ett tidigare stadium identifiera och avvärja hot genom denna teknik. Samtidigt innebär informationssammanställningar också ett hot mot den personliga integriteten, något som den kommande dataskyddsförordningen, GDPR, ska styra och som innebär stora krav på organisationer i deras uppgiftsbehandling. Sammanställningar av information kan påverka skyddsvärdet av informationen, där enskilt öppen information i en sammanställning tillsammans med annan information kan få ett högre skyddsvärde.

Förslag på fördjupningsområden

- **Avvägning mellan nytta och risk vid sammanställning**
  Det behövs vägledningar för hur myndigheter ska göra bedömningar och avvägningar i fråga om sammanställningar av information. Nyttoeffekterna kan å ena sidan vara mycket stora, men risker, liksom juridiska aspekter kan också bli omfattande. Olika aspekter och regleringar kring sekretess samt personuppguppgifter behöver klargöras, främst utifrån ansvaret för sammanställningar av information
- **Ägarskap av aggregerad information**
  Vilket ansvar har de enskilda dataleverantörerna och vilket ansvar har den som sammanställer informationen? Det kan vara svårt att på ett generellt sätt ange vem som ansvarar för aggregerad information och även om det krävs bedömningar i varje specifikt fall behövs det vägledning i hur man skall hantera frågan.
- **Öppna data**
  Genom öppna data kan stora informationsmängder tillgängliggöras, vilka i sig bedöms inte vara känsliga, men som tillsammans med information från andra källor, såväl från offentlig som privat sektor kan innebära säkerhetsrisker eller hot mot den personliga integriteteten. Metoder för att analysera detta, liksom juridiska frågor behöver tas upp i ett fortsatt arbete.

4.2.5. Styrning av åtkomst i samverkan

Den som tillhandahåller en tjänst måste säkerställa att de som ska få åtkomst till information är de som de utger sig för att vara, att de endast ges åtkomst till den information de är behöriga till, att de endast kan utföra de operationer de har rätt att utföra samt att utförda operationer loggas och kan härledas till den som utfört operationen. Vid samverkan blir åtkomsthantering mer komplex, bland annat för att olika organisationer kan göra olika bedömningar av informationens skyddsvärde samt att ansvar för den samlade informationsmängden kan vara oklart.

Förslag på fördjupningsområden

- **Ansvar för behörighetskontroll och spårbarhet**
  Det finns behov av vägledning om ansvar för identiteter, behörighetskontroll, grundbehörigheter och spårbarhet i olika skeden och hur det kan realiseras genom avtal/överenskommelser.
- **Säkerhetsnivå för identiteter**
  Det finns behov av likvärdig hantering av säkerhetsnivå på identiteter mellan myndigheter och mot konsumenter, bland annat beroende på att prioritering och kunskapsnivå kan skilja sig åt mellan olika aktörer. Det finns en risk att för mycket eller för lite information tillgängliggörs om myndigheter inte kommer överens vad som är rätt tillitsnivå för identiteter.

4.2.6. Efterlevnad och uppföljning

Grunderna för efterlevnad är att säkerställa att uppsatta regelverk är korrekt och ändamålsenligt uppsatta, att de har avsedd verkan samt att de följs av ansvariga aktörer. Uppföljning av efterlevnad kan ske löpande genom övervakning eller genom granskning och kan exempelvis utföras av interna eller externa granskningar/revisioner eller tillsynsmyndigheter. Graden av granskning kan även variera. I vissa fall granskas enbart utformningen/designen av kontrollerna i sig medan man i vissa fall även granskar den faktiska efterlevnaden.

Förslag på fördjupningsområden

- **Ansvar för efterlevnad och uppföljning vid samverkan**
  Ansvar behöver tydliggöras för att uppföljning av åtgärder genomförs. Eventuella begränsningar i insynsmöjligheter mellan aktörer behöver klargöras, liksom hur brister i efterlevnad hanteras. Här kan också mätmetoder för efterlevnad och uppföljning skilja sig åt mellan olika organisationer utifrån deras inriktning och säkerhetskultur.

4.2.7. Utveckling av tjänster i samverkan

Ansvar för säkerhetsfrågor i samband med tjänsteutveckling ligger i dag hos de enskilda aktörerna. Vid samverkan kompliceras ansvarsfrågan och här finns ett behov av att vidareutveckla metoder och rutiner vid samverkansprojekt.

Förslag på fördjupningsområden

- **Säkerhetsaktiviteter före utveckling av en lösning**
  - Praktiska säkerhetsstöd för samarbetsprojekt kring exempelvis riskanalysmetod, dokumentationsansvar, kravhantering mm.
  - Styrning av ansvar vid samverkansprojekt för att få beslut och rätt kompetens tillgänglig vid rätt tillfälle. Det är viktigt att beslutsordningen är klar och tydlig.
  - Avstämning mot de säkerhetskrav som ställs samt vilken flexibilitet som finns för att hantera nya krav under tjänstens livscykel.
- **Säkerhetsaktiviteter under utveckling/införande av en lösning**
  - Kravnedbrytning till leveranser där administrativa och tekniska skydd beskrivs för att svara upp mot skyddsbehovet.
  - Risk- och sårbarhetsanalys med åtgärder.
  - Systemutveckling med verifikationssteg, säkerhetsgranskningar och ackreditering.
  - Uppföljning och åtgärder så att skyddsnivån hålls tillräcklig över livscykeln.
  - Val av metoder och deras konsekvenser för utvecklingstakt och leverans.

4.2.8. It-försörjning och fysisk säkerhet

I området it-försörjning och fysisk säkerhet ingår dels frågor som är gemensamma för myndigheter, som risker med ensidigt beroende vid outsourcing, molnlösningar, centrala respektive decentraliserade lösningar etc. I samverkan kan också avtalsfrågor kring drift bli komplexa om externa leverantörer används. Frågan om molntjänster har tagits upp ibland annat Pensionsmyndighetens utredning *”Molntjänster i staten”* och Statens servicecenters utredning ”*En gemensam statlig molntjänst för myndigheternas it-drift*”. Här kan en komplettering kring säkerhetsområdet vara intressant.

Förslag på fördjupningsområden

- **Säkerhetsaspekter vid gemensamt producerade tjänster**
  Intressanta frågor att behandla ur ett samverkansperspektiv är bland annat:
  - Central eller decentraliserad infrastruktur
  - Gemensamma lösningar, kritiska beroenden till externa aktörer
  - Avtalshantering vid outsourcing och molntjänster
  - Robusta system och robust verksamhet på kort och lång sikt
  - Incidenthantering
  - Kontinuitetsplanering
- **Fysisk säkerhet**
  Behov av gemensamma grundkrav för fysisk säkerhet vid it-driftställen. Finns det särskilda krav och aspekter kring fysisk säkerhet i lokaler och andra utrymmen i samband med tjänster och information i samverkan, exempelvis kring tillträdeskontroll och försörjningssystem?

4.2.9. Civilt försvar och säkerhetsskydd

I december 2015 beslutade regeringen om återupptagen totalförsvarsplanering. Med totalförsvar avses den verksamhet som behövs för att förbereda Sverige för krig, vilket består av militärt och civilt försvar. Civilt försvar är den verksamhet som ansvariga aktörer genomför i syfte att göra det möjligt för samhället att hantera situationer då beredskapen höjs och syftar till skydd av befolkningen, säkerställande av samhällsviktiga funktioner samt övriga samhällets stöd till Försvarsmakten. Verksamheten ska bedrivas av statliga myndigheter, kommuner, landsting, privata företag och frivilligorganisationer.

Planeringen av civilt försvar ska utgå från aktörernas krisberedskapsarbete. Krisberedskap definieras som förmågan att före, under och efter en kris förebygga, motstå och hantera krissituationer. Vid större kriser finns särskilda regelverk med krav på upprättande av nödvändiga funktioner för att säkerställa samhällsviktig verksamhet.

Med säkerhetsskydd avses skydd mot spionerі, sabotage och andra brott som kan hota rikets säkerhet. Det inkluderar även skydd i andra fall av uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) och som rör rikets säkerhet, samt skydd mot terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott (terrorism), även om brotten inte hotar rikets säkerhet. Lag (2009:464.

Förslag på fördjupningsområden

- **Risker vid ökad koncentration av samhällsviktig verksamhet**
  Hur hanteras det faktum att det kan bli en ökad koncentration av samhällsviktig verksamhet (”många ägg läggs i samma korg”)? Gemensamma lösningar kan ofta medföra robusthetshöjande fördelar samtidigt som de även kan medföra en koncentrering av kritiska beroenden och även skapa en ökad attraktivitet för angrepp (exempelvis genom cyberattacker från resursstarka angripare). Koncentrationsaspekter kan exempelvis röra sig om teknik, bemanning och geografisk placering.
- **Krisberedskap, civilt försvar och digitalisering**
  Säkerställs planeringen av reservalternativ i det pågående digitaliseringsarbetet? Kommer exempelvis manuella reservrutiner, personalkapacitet och kompetens även att säkerställas på lång sikt vid en minskning av bemanningen? Planerar respektive samverkansaktör för möjligheten att upprätthålla solitära lösningar i händelse av kris, höjd beredskap eller krig?

- **Gemensam prioritering av samhällsviktig verksamhet**
  Finns det förutsättningar för att hantera gemensamma prioriteringar av samhällsviktig verksamhet vid större avbrott i gemensamma tjänster? Kan motsvarande prioriteringar genomföras vid höjd beredskap eller krig? Påverkas samverkan av det faktum att alla aktörer inte är bevakningsansvariga myndigheter?
- **Ökat beroende av ett mindre antal externa aktörer**
  Hur hanteras beroendet av externa aktörer kopplat till gemensamma lösningar då fler samverkansparter kan bli starkt beroende av ett fåtal privata aktörer? Hur ska prioritering ske mellan olika samhällskritiska verksamheter hos privata aktörer vid händelse av kris? Hur påverkas geografisk landsplacering av exempelvis molntjänster i händelse av höjd beredskap eller krig i Sverige. Hur påverkas det av höjd beredskap eller krig i det land som tjänsten är placerad?
- **Säkerhetsskydd och samverkan**
  Hur påverkar aggregeringen av aktörernas information och tjänster Sveriges säkerhet och behovet av säkerhetsskydd? Information om gemensamma lösningar kan öka känslighetsgraden kopplat till exempelvis sabotage, brottslighet och kartläggning. Finns det exempelvis förutsättningar för att hantera detta på ett tillfredsställande sätt i form av gemensamma sekretessbedömningar, skyddsåtgärder, ansvar, avtal och överenskommelser? Hur ser förutsättningarna ut för att dela eventuella hemliga uppgifter? Hur hanteras risker kopplat till utlämningsärenden eller kartläggning av nyckelpersoner?

4.2.10. Ny teknik och nya utmaningar

Även om digitalisering och nya tekniska möjligheter har diskuterats under flera år, är konsekvenserna för säkerheten fortfarande oklara. Det gäller exempelvis områden som *Big data*, där organisationer kan samla och analysera stora informationsmängder från olika källor, *Internet of things*, där sensorer kan fånga information som kan användas på olika sätt, *Artificiell intelligens*, där informationen automatiskt analyseras av datorer för att hitta mönster och dra slutsatser som kanske inte tidigare var möjliga. ”*Spionen lägger pussel - behåll din bit*” stod det på affischerna under andra världskriget. Många av de nya tekniska lösningarna utgår från att man delar med sig av sin information, där man med ny teknik kan lägga allt större pussel - vilket kan leda till både nytta och hot på samma gång.

Förslag på fördjupningsområden

- **Omvärldsbevakning kring hot och risker med ny teknik**
  Tänkbara områden i dag att analysera kan exempelvis handla om sensorstyrd utrustning, bilar, medicinsk utrustning, robotar i hemsjukvården, som i sig kan innebära fysiska risker för användare eller risk för övervakning, hackning mm. Om ett år kan kartan se annorlunda ut. Utgångspunkten för analysen ska vara hur det påverkar gemensamma tjänster eller säkerhetsåtgärder.
- **Förhållningssätt och åtgärder när ny teknik tillkommer**
  Myndigheter intar ofta en avvaktande hållning när ny teknik lanseras och lagstiftningen hänger ofta inte med i utvecklingen, vilket också kan ses som ett uttryck av säkerhetstänkande. Samtidigt bör man inom offentlig sektor kunna inta ett förhållningssätt där riskanalyser genomförs återkommande, eftersom nya risker och hot snabbt kan dyka upp och behöva värderas och hanteras. Vidare kan man också med ny teknik och nya lösningar hantera hot från annan ny teknik, exempelvis med hjälp av *blockkedjor*, lösningar för *eget utrymme* etc.

4.3. Ansvarsförhållanden

Det finns omfattande regelverk, standarder, utpekat myndighetsansvar för säkerhetsfrågor och säkerhetsåtgärder. Trots detta uppstår ofta i den praktiska hanteringen frågor om hur ansvaret ser ut vad gäller exempelvis övergripande ansvar för komplexa lösningar, ansvar för sammanställningar av information eller för säkerhetsåtgärder som omfattar både verksamhet och teknik. Rent principiellt åligger det respektive informationsägare/-leverantör att ta ansvar för sina informationstillgångar, men det sammanhållande ansvaret vid samverkan mellan myndigheter är ibland inte fullt tydligt.

Statliga myndigheter med särskilda uppgifter eller uppdrag inom informationssäkerhets- och cybersäkerhetsområdet ingår i samverkansgruppen för informationssäkerhet (SAMFI). Deltagarna är Myndigheten för samhällsskydd och beredskap (MSB), Post- och telestyrelsen (PTS), Försvarets radioanstalt (FRA), Säkerhetspolisen (SÄPO), Polismyndigheten, Försvarets materielverk (FMV) och Försvarsmakten. Detta beskrivs närmare i det så kallade *NISU-betänkandet*, som ger en bred översikt över reglering och det formella ansvaret i dag.

Inom områdena Krisberedskap, Totalförsvarsplanering och Säkerhetsskydd har följande aktörer ett särskilt ansvar:

- Myndigheten för samhällsskydd och beredskap (MSB)
- Försvarsmakten
- Militära underrättelse- och säkerhetstjänsten (MUST)
- Säkerhetspolisen
- Polisen
- Affärsverket svenska kraftnät
- Transportstyrelsen
- Post- och Telestyrelsen (PTS)
- Bevakningsansvariga myndigheter enligt förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap.
- Länsstyrelser.

Se närmare i avsnitt *6. Referenser och förslag på vidare läsning*, där aktuell reglering framgår, liksom annat underlag.

MSB och övriga myndigheter i SAMFI samt Datainspektionen och Riksarkivet är viktiga stödjande och styrande myndigheter för andra organisationer. MSB bedriver ett omfattande arbete med att informera om informationssäkerhet och har också föreskriftsrätt inom området. Det metodstöd som ska ses som hjälp att kunna följa och implementera standarden SS-EN ISO/IEC 27002:2017 uppdateras för närvarande och beräknas vara klart 2017. Informationsklassningsmodellen planeras bli uppdaterad inom en snar framtid inklusive rekommendationer om säkerhetsåtgärder och skyddsnivåer. Ansvaret för utveckling inom myndigheter finns idag beskrivet i MSB:s föreskrift för systematiskt informationssäkerhetsarbete, MSBFS 2016:1.

Ansvar för säkerhetsaspekter vid utveckling inom kommun och landsting finns hos respektive organisation. SKL och Inera har tagit fram material där ett antal relevanta moment har beskrivits. MSB:s metodstöd i systematiskt informationssäkerhetsarbete kan också utnyttjas av kommuner och landsting genom de generella vägledningar som tagits fram.

Momentet ***hur*** utveckling ska ske i praktiken åligger, som nämnts, respektive organisation. I följande avsnitt beskrivs förslag på principer för styrning av säkerhet vid samverkansprojekt, som kan tjäna som underlag för att förtydliga det konkreta ansvaret i en utvecklingsinsats.

4.4. Principer för styrning av säkerhet vid samverkansprojekt

4.4.1. Inledning

I styrningen av de deltagande myndigheternas gemensamma informationssäkerhet i projekt och i förvaltningsfas behövs en tydlig struktur för ansvar, befogenheter och uppföljning. *Vägledning för digital samverkan* samt *principer för digital samverkan* är viktiga utgångspunkter, där principerna S1-S4 särskilt berör säkerhet:

1. Bedriv ett riskbaserat informationssäkerhetsarbete
2. Skydda den personliga integriteten
3. Beakta informationens skyddsvärde i hela kedjan
4. Analysera rättsliga förutsättningar

I en särskild bilaga till vägledningen, *Roller och överenskommelser* framgår viktiga roller i utvecklingsarbetet utifrån lednings-, konsument- och producentperspektivet. Dessa kommer att ha sina respektive ansvar också för säkerhetsfrågorna under planering, utveckling, drift och avveckling. Exempel på sådana roller är *Samverkansansvarig* (som kan vara livshändelseansvarig), *Nyttorealiseringsansvarig, Samverkansprocessägare, Begreppsägare för utbytesinformation, Färdledare, Behovsansvarig, Införandeansvarig, Utvecklingsansvarig, Informationsägare*. I principerna nedan tas enbart några av dessa roller upp.

Metod för utveckling i samverkan är en ytterligare lämplig utgångspunkt för att beskriva principer under tjänstens livscykel, där dock vissa kompletteringar kan behövas, bland annat kring informationens livscykel samt aspekter kring avveckling.

I följande avsnitt föreslås ett antal principer för styrning av säkerhet vid samverkansprojekt. Principerna behöver vidareutvecklas ytterligare och samordnas och presenteras tillsammans med andra principer kring digital samverkan.

4.4.2. Förslag på principer

Initiala och övergripande ansvarsfrågor

- Ansvar inom gemensamma insatser fastställs genom överenskommelser mellan deltagande organisationer där varje myndighet ansvarar för sin information. Inför en ny gemensam insats utses en färdledare, som är ansvarig för övergripande och gemensamma informationssäkerhetsfrågor. I överenskommelserna ska framgå hur man hanterar olika riskacceptans i val av lösning och i drift så att det är tydligt hur beslut fattas.
- Där det finns flera sammanhängande tjänster och information i en livshändelse ska livshändelseansvarig myndighet säkra att åtgärder vidtas för att styra och samordna den samlade informationssäkerheten.
- Redan i ett tidigt skede i en insats bör en myndighet utses som ansvarig för övergripande informationssäkerhetsfrågor efter införandet av tjänsten. Ansvaret dokumenteras i en förvaltningsöverenskommelse.

- I ett tidigt skede i insatsen görs en samlad riskbedömning där både riskbedömningar utifrån de deltagande myndigheternas riskbedömningar och risker med aggregerad information och gemensamma tjänster analyseras. I de fall risksammanställningen som sådan blir komplex bör en sammanställning av myndighetsspecifika samt övergripande krav på åtgärder utnyttjas för att säkerhetskrav i hela kedjan kan tillgodoses
- Det ska finnas former för hur dokumentation ska upprättas, hur den bevaras, hur avtal/överenskommelser ska se ut, samt rekommendationer för vem som har ansvar för dokumentationen. Vidare ska det finnas överenskomna former för utbyte av riskanalyser och informationsklassning samt krav på informationssäkerhetsåtgärder vid utbytet, där särskilt sekretessaspekter beaktas.

Hantering av krav och prioritering inför utveckling

- Färdledande myndighet ansvarar för det sammanhållna kravarbetet beträffande informationssäkerhet samtidigt som varje deltagande myndighet bidrar med sina krav. Kravarbetet ska göras utifrån sammanhållna informationsklassningar och analyser.
- Färdledande myndighet samordnar övergripande krav och prioritering av åtgärder utifrån kraven, även om dessa på något sätt divergerar. Det ska finnas former för hur kraven dokumenteras, dels under projektet men även i fortsatt förvaltning.

Utveckling och införande

- Färdledande myndighet är ansvarig för samordningen av informationssäkerhetsarbetet i samband med utvecklingsarbete.
- Krav och prioritering från informationssäkerhetsperspektivet samlas och bildar en del av underlaget för utveckling av tjänsten. De sammanhållna kraven bildar grunden och ska vara dokumenterade och uppföljningsbara.
- Vid utveckling och införande ska samtliga identifierbara risker beaktas i sammanhållna analyser, exempelvis projektrisker och verksamhetsrisker. Verksamhetsriskerna ska vara analyserade, dokumenterade och omhändertagna innan driftsättning. Verksamhetsrisker dokumenteras på ett sådant sätt att de kan följas upp och vid behov senare kan bli en fråga för förvaltningen av tjänsten.
- Tekniska säkerhetstester genomförs i anslutning till driftsättningen och utvärderas innan lösningen görs tillgänglig för användarna.

Hantering under tjänstens livscykel

- Skyddsvärdet ska alltid utgå från dokumenterade analyser och informationsklassning. Värdet hos den enskilda informationsmängden kan förändras genom livscykeln och måste säkerställas under hela livscykeln genom återkommande analyser.
- För att skyddsvärdet ska kunna säkerställas under hela kedjan eller livscykeln och att informationen inte kommer i orätta händer, förvanskas eller förstörs, måste korrekt klassning göras av informationen. Utifrån informationsklassningen ska säkerhetsåtgärder vidtas och dokumentation finnas tillgänglig för uppföljning
- Det ska finnas ett dokumenterat ägarskap av informationen och vem som är ”master” samt dokumenterade former för att identifiera/märka information, och definiera operativa rutiner kring exempelvis incidenthantering och rapportering.

- Dokumentationen av informationsklassning, handlingsplaner och underlag för förvaltning hanteras enligt överenskommen form. Beträffande bevarande av handlingsplaner och övrig dokumentation måste särskilt sekretessaspekter tas i med i planeringen för bevarandet.
- Långsiktig samverkan mellan drift och förvaltning ska säkerställas över gränssnitten mellan de deltagande myndigheterna.

Avveckling av en tjänst

- Redan under planeringen av en gemensam tjänst bör också den framtida avvecklingen planeras, så den kan genomföras på ett säkert sätt. Färdledaren ansvarar för den övergripande nivån, där frågor kring avställning, arkivering, konvertering etc. hanteras, liksom att den initiala riskanalysen också tar upp avvecklingsfrågan. Respektive informationsägare är sedan ansvarig för sina informationsmängder.
- För genomförandet av avvecklingen av en gemensam tjänst ska det framgå i överenskommelsen mellan organisationerna vem som är ansvarig för gemensamma informationssäkerhetsfrågor så att dessa hanteras under avvecklingen.

Granskning och mätning

- Säkerhetsåtgärderna i livscykelns olika delar ska verifieras genom dokumenterade kontrollåtgärder i form av exempelvis revisioner av dokumentation och vidtagna åtgärder, exempelvis återkommande kodgranskning, systemtester i form av penetrationstester mm.
- Beträffande åtgärder är uppföljning/kontroll avgörande och därför ska en överenskommen granskningsplan finnas utifrån informationsklassning och kravbild. Granskningarna dokumenteras och fynden rapporteras i form av handlingsplan med uppföljningsbara åtgärder. Handlingsplanen ska säkerställas under förvaltningsfasen genom kontinuerlig uppföljning.
- Fastställda kontrollpunkter ska finnas för att säkerställa att analyser genomförs och att resultatet är relevant i form av kontrollkriterier och nyckeltal.
- Det ska finnas former för hur granskning och mätning rapporteras till den ansvariga myndigheten och för hur återkoppling sker

5. Behov av en permanent expertgrupp för säkerhet

5.1. Överväganden och förslag

Säkerhetsfrågorna har fått en allt större aktualitet de senaste åren. Beroendet till digitala lösningar är större, tidigare hot har blivit mer komplexa och det har tillkommit nya hot och risker som kräver annorlunda säkerhetsåtgärder än tidigare. Både regeringen och EU har lyft upp säkerhetsfrågorna och det finns redan i dag både reglering och ansvariga myndigheter inom området.

Det krävs samtidigt åtgärder för att tillse att det praktiska säkerhetsarbetet inom myndigheterna sker på ett ändamålsenligt sätt och där gemensamma lösningar har god säkerhet genom hela kedjan. Detta är ett arbete som ska ske på respektive myndighet samtidigt som det behövs en övergripande samordning och styrning av säkerhetsarbetet.

För detta ändamål föreslås att eSams expertgrupp för säkerhet permanentas samt kompletteras med en referensgrupp där varje medlem kan utse en representant.

5.2. Expertgruppens syfte och inriktning

Syftet med expertgruppen för säkerhetsfrågor är att bidra till att tjänster som levereras av eSams medlemsorganisationer håller rätt avvägd säkerhet. Expertgruppen bör driva säkerhetsfrågor som är centrala för digitaliseringsarbetet med fokus på sådant som behöver hanteras i samverkan mellan organisationer och som inte hanteras av andra specifikt ansvariga myndigheter.

Regeringen och myndigheter med särskilda uppgifter inom området informationssäkerhet (SAMFI) driver informationssäkerhetsarbetet på central och strategisk nivå. En del i detta är MSB:s föreskrifter inom området. Expertgruppens inriktning och roll bör, utifrån detta och de iakttagelser som framgår i rapporten, främst vara att hantera gemensamma frågor och samverkansfrågor som rör myndigheternas praktiska säkerhetsarbete. I praktiken, men inte formellt, blir det också en normerande roll. Gruppen bör vara en producerande funktion, som samtidigt inte ersätter det arbete som redan sker i befintliga organisationer och nätverk. Viktiga uppgifter bör vara att:

- Leverera stöd, underlag och analyser för att förenkla för medlemsmyndigheterna inom området säkerhet och säkra att säkerhetsfrågorna är med i ett tidigt skede i prioriterade insatser.
- Ta fram och förvalta vägledningar och principer, ge stöd inom informationssäkerhet på en generell nivå samt inom valda fokusområden. Bidra till erfarenhetsutbyte.
- Analysera och ta fram förslag på åtgärder vid nya direktiv eller lagförslag.
- Bidra med expertkompetens i specifika frågor och i uppdrag inom eSam.
- Främja återanvändning av metoder och verktyg.

5.3. Organisation och arbetssätt

Expertgruppen för säkerhet bör lämpligen ha samma uppbyggnad och arbetssätt som expertgrupperna för arkitektur och juridik, dvs:

- En mindre grupp som arbetar löpande med säkerhetsfrågorna och som också kan ha adjungerade medlemmar utanför eSams medlemsmyndigheter.
- En större referensgrupp med deltagare från alla medlemsmyndigheter.

Expertgruppen samverkar nära med expertgrupperna för arkitektur och juridik och vid behov med andra organisationer. Det är viktigt att expertgruppen är tydlig med sin inriktning så att det inte uppstår överlappningar eller risk för att frågor hamnar mellan stolarna.

5.4. Förslag på fortsatt arbete

Viktiga initiala arbetsområden för en permanent expertgrupp för säkerhet bör vara:

- Initiera arbete inom de fördjupningsområden som tagits upp, bland annat frågor kring säkerhetskultur och riskbedömningar, informationsklassning och skyddsnivå, ansvar under en informationslivscykel, sammanställningar av information mm. I detta ligger också frågor som redan lyfts inom eSam, som grunddata, öppna data och informationsutbyte. Även de föreslagna principerna behöver vidareutvecklas.
- Gör en översiktlig kartläggning av medlemsorganisationernas nuvarande säkerhetsarbete och inriktning.
- Inventera lämpliga metoder och verktyg som kan återanvändas, exempelvis checklistor, uppföljningsmetoder, riktlinjer, risk- och sårbarhetsanalyser, kontinuitetsplaner, granskningar, vägledningar etc. De kan med fördel publiceras på informationssakerhet.se där MSB planerar att lägga upp en kunskapsbank får återanvändning.

Insatserna behöver prioriteras och planeras så att ambitionsnivån är i fas med tillgängliga resurser. eSams verksamhetsplan och prioriterade områden plan är en utgångspunkt, där också samordning och avstämning behöver ske med andra viktiga aktörer inom området.

6. Referenser och förslag på vidare läsning

Digitalisering, strategier och vägledningar

- För ett hållbart digitaliserat Sverige – en digitaliseringsstrategi (N2017/03643/D) (http://www.regeringen.se/49adea/contentassets/5429e024be6847fc907b786ab954228f/digitaliseringsstrategin_slutlig_170518-2.pdf)
- Med medborgaren i centrum, Regeringens strategi för en digitalt samverkande statsförvaltning (http://www.regeringen.se/informationsmaterial/2012/12/n2012.37/)
- Metod för utveckling i samverkan, e-delegationen (http://www.esamverka.se/stod-och-vagledning/vagledningar/metod-for-utveckling-i-samverkan.html)
- Vägledning för digital samverkan, e-delegationen (http://www.esamverka.se/stod-och-vagledning/vagledningar/digital-samverkan.html)
- Vägledande principer för digital samverkan, e-delegationen (http://www.esamverka.se/stod-och-vagledning/vagledningar/digital-samverkan.html)
- Utredningen om effektiv styrning av nationella digitala tjänster (SOU 2017:23) (http://www.sou.gov.se/n-201601-utredningen-om-effektiv-styrning-av-nationella-digitala-tjanster-i-en-samverkande-forvaltning/)
- eIDAS - Utländska e-legitimationer i svenska digitala tjänster, E-legitimationsnämnden (http://www.elegnamnden.se/eidas.4.361dc8c15312eff6fdf6ef.html)
- Outsourcing – en vägledning om sekretess och persondataskydd, eSam (http://www.esamverka.se/stod-och-vagledning/vagledningar/outsourcing---en-vagledning-om-sekretess-och-persondataskydd.html)
- Molntjänster i staten – En ny generation av outsourcing, Pensionsmyndigheten (https://www.pensionsmyndigheten.se/nyheter-och-press/pressrum/pensionsmyndigheten-svenska-myndigheter-borgora-sig-molnberedda)
- En gemensam statlig molntjänst för myndigheternas it-drift, Statens servicecenter (http://www.statenssc.se/OmOss/Documents/Delrapport%20-%20En%20gemensam%20statlig%20molntj%C3%A4nst%20f%C3%B6r%20myndigheternas%20it-drift_2017-02-07.pdf)

Säkerhet och trendanalyser

- Nationell säkerhetsstrategi, Regeringen 2017 (http://www.regeringen.se/informationsmaterial/2017/01/nationell-sakerhetsstrategi/)
- Informationssäkerhet - trender 2015, MSB (https://www.msb.se/sv/Produkter--tjanster/Publikationer/Publikationer-fran-MSB/Informationssakerhet---trender-2015/)
- Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten (SOU 2015:23), NISU 2014 (”NISU-betänkandet”) (http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2015/03/sou-201523/)
- Informationssäkerhet för samhällsviktiga och digitala tjänster (SOU 2017:36), betänkande av Utredningen om genomförande av NIS-direktivet (http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2017/05/sou-201736/)
- Säkerhetspolisens årsbok 2016 (http://www.sakerhetspolisen.se/publikationer/rapporter-amnesvis/om-sakerhetspolisen/sakerhetspolisens-2016.html)
- Årsrapport 2016, FRA (http://www.fra.se/snabblankar/nyheterochpress/publicerat.115.html)
- Helårsbedömning 2017, Nationellt centrum för terrorbedömning (NCT). (http://www.sakerhetspolisen.se/download/18.1beef5fc14cb83963e73383/1484663040490/NCT_Helarsbedomning_2017.pdf)
- Myndigheter i samverkan mot den organiserade brottsligheten 2016 (https://polisen.se/Aktuellt/Rapporter-och-publikationer/Organiserad-brottslighet/Publicerat-Organiserad-brottslighet/Myndigheter-i-samverkan-mot-den-organiserade-brottsligheten-2016/)

Integritetsskydd

- Personuppgiftslagen, Datainspektionen (http://www.datainspektionen.se/fragor-och-svar/personuppgiftslagen/)
- Dataskyddsförordningen (GDPR), Datainspektionen (http://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/)
- Dataskydd, EU-kommissionen (http://ec.europa.eu/justice/data-protection/index_en.htm)
- Ny dataskyddslag, Kompletterande bestämmelser till EU:s dataskyddsförordning (SOU 2017:39), betänkande av Dataskyddsutredningen (http://www.regeringen.se/49a184/contentassets/e98119b4c08d4d60a0a2d0878990d5ec/ny-dataskyddslag-sou-201739)

Totalförsvarsplanering och civilt försvar

- Regeringen beslutar om återupptagen totalförsvarsplanering (http://www.regeringen.se/pressmeddelanden/2015/12/regeringen-beslutar-om-aterupptagen-totalforsvarsplanering/)
- Regeringen höjer ambitionen i arbetet med att stärka totalförsvaret (http://www.regeringen.se/pressmeddelanden/2017/05/regeringen-hojer-ambitionen-i-arbetet-med-att-starka-totalforsvaret/)
- Planeringsanvisningar för det civila försvaret, Regeringen (http://www.regeringen.se/4aeb92/globalassets/regeringen/dokument/justitiedepartementet/beslut-civilt-forsvar-planeringsanvisningar.pdf)
- Sverige kommer att möta utmaningarna - Gemensamma grunder (grundsyn) för en sammanhängande planering för totalförsvaret (FM2016-13584:3 / MSB2016-25), Försvarsmakten och MSB (https://www.msb.se/Upload/Insats_och_beredskap/160610%20FM2016_13584_3%20Rapport%20MSB%20och%20FM.pdf)
- Hotbildsunderlag i utvecklingen av civilt försvar (FOI Memo 5089), FOI (https://www.foi.se/download/18.2bc30cfb157f5e989c3201a/1477565924431/Hotbildsunderlag+i+utvecklingen+av+civilt+f%C3%B6rsvar.pdf)

Lagar och förordningar (urval)

- Tryckfrihetsförordning (1949:105) (https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/tryckfrihetsforordning-1949105_sfs-1949-105)
- Offentlighets- och sekretesslag (2009:400) (http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/offentlighets--och-sekretesslag-2009400_sfs-2009-400)
- Förvaltningslag (1986:223) (http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forvaltningslag-1986223_sfs-1986-223)
- Personuppgiftslag (1998:204) (http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/personuppgiftslag-1998204_sfs-1998-204)
- Arkivlag (1990:782) (http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/arkivlag-1990782_sfs-1990-782)
- Lag (2003:389) om elektronisk kommunikation (http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2003389-om-elektronisk-kommunikation_sfs-2003-389)
- Lag (1998:112) om ansvar för elektroniska anslagstavlor (https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-1998112-om-ansvar-for-elektroniska_sfs-1998-112)
- Förordningen (1995:1300) om statliga myndigheters riskhantering (https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-19951300-om-statliga-myndigheters_sfs-1995-1300)
- Säkerhetsskyddslag (1996:627) (https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/sakerhetsskyddslag-1996627_sfs-1996-627)
- Säkerhetsskyddsförordning 1996:633 (http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/sakerhetsskyddsforordning-1996633_sfs-1996-633)

- Lag (1992:1403) om totalförsvar och höjd beredskap (https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-19921403-om-totalforsvar-och-hojd_sfs-1992-1403)
- Lag (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap (http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2006544-om-kommuners-och-landstings_sfs-2006-544)
- Förordning (2006:637) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap (http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-2006637-om-kommuners-och-landstings_sfs-2006-637)
- Förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap (http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-20151052-om-krisberedskap-och_sfs-2015-1052)
- Förordning (2015:1053) om totalförsvar och höjd beredskap (http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-20151053-om-totalforsvar-och-hojd_sfs-2015-1053)
- Arkivförordning (1991:446) (http://rkrattsbaser.gov.se/sfst/adv?fritext=arkivf%C3%B6rordning&sbet=&rub=&org=&upph=false)

Föreskrifter och allmänna råd från MSB och Riksarkivet

- MSBFS 2016:1 föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet (https://www.msb.se/sv/Om-MSB/Lag-och-ratt/Gallande-regler/Krisberedskap-och-informationssakerhet/MSBFS-20161/)
- MSBFS 2016:2 föreskrifter och allmänna råd om statliga myndigheters rapportering av it-incidenter (https://www.msb.se/sv/Om-MSB/Lag-och-ratt/Gallande-regler/Krisberedskap-och-informationssakerhet/MSBFS-20162/)
- MSBFS 2016:7 föreskrifter och allmänna råd om statliga myndigheters risk- och sårbarhetsanalyser (https://www.msb.se/sv/Om-MSB/Lag-och-ratt/Gallande-regler/Krisberedskap-och-informationssakerhet/MSBFS-20167/)
- MSBFS 2015:5 föreskrifter och allmänna råd om kommuners risk- och sårbarhetsanalyser (https://www.msb.se/sv/Om-MSB/Lag-och-ratt/Gallande-regler/Krisberedskap-och-informationssakerhet/MSBFS-20155/)
- MSBFS 2015:4 föreskrifter och allmänna råd om landstings risk- och sårbarhetsanalyser (https://www.msb.se/sv/Om-MSB/Lag-och-ratt/Gallande-regler/Krisberedskap-och-informationssakerhet/MSBFS-20154/)
- MSBFS 2009:11 föreskrifter om civila myndigheters kryptoberedskap (https://www.msb.se/sv/Om-MSB/Lag-och-ratt/Gallande-regler/Krisberedskap-och-informationssakerhet/MSBFS-200911/)
- Riksarkivets föreskrifter om elektroniska handlingar, RA-FS 2009:1-2 (https://riksarkivet.se/rafs?item=105 och https://riksarkivet.se/rafs?item=106)
- Riksarkivets föreskrifter om verksamhetsbaserad arkivredovisning (beskrivning över informationstillgångarna) (https://riksarkivet.se/rafs?item=104)
- Vägledning för processbaserad informationskartläggning (https://riksarkivet.se/Media/pdf-filer/V%C3%A4gledning%20f%C3%B6r%20processorienterad%20informationskartl%C3%A4ggning.pdf)
- Redovisa verksamhetsinformation, (https://riksarkivet.se/Media/pdf-filer/V%C3%A4gledningSkrift.pdf)
- Vägledning för fysisk informationssäkerhet i it-utrymmen (https://riksarkivet.se/Media/pdf-filer/doi-t/Vagledning_IT-utrymmen.pdf)

Metodstöd och standarder

- informationssakerhet.se, MSB (https://www.informationssakerhet.se, https://www.informationssakerhet.se/metodstod-for-lis/)
- ISO/IEC 27001:2014 och ISO/IEC 27002:2014, SIS (http://www.sis.se/tema/ISO27000/)