Avdelningen för risk- och sårbarhetsreducerande arbete
Verksamheten för samhällets informations- och cybersäkerhet

Stöd för arbetet med regleringsbrevsuppdrag 2015

- Informationssäkerhet i RSA

Tolkning, genomförande, redovisning

MSB864 – maj 2015
ISBN 978-91-7383-577-0

Innehåll

1 Inledning 4

2 Syftet med stödet 4

3 Målgruppen för stödet 5

4 Bakgrund till stödet 5

4.1 Varför ett stöd? 5

4.2 Informationssäkerhetsuppdrag 2015 6

4.3 Närmare om MSB:s mandat 6

5 MSB:s tolkning av uppdraget 8

5.1 Behov av tolkning 8

5.2 Underlag för tolkningen 8

5.3 Identifierade syften 8

5.4 Att *beakta och analysera* informationssäkerheten 11

5.5 Vidtagna åtgärder 11

5.6 Att *redovisa* bedömningen och vidtagna åtgärder 11

6 Fokusområden i regleringsbrevsuppdraget 12

7 Förslag på genomförande 13

7.1 Fokus på samhällsviktig verksamhet och krisberedskap 13

7.2 Stöd för bedömning av informationssäkerhet inom myndigheten och i myndighetens ansvarsområde 13

7.3 Genomförande i den egna verksamheten 15

7.4 Genomförande av analys för sak- respektive geografiskt områdesansvar 16

8 Redovisning av bedömningen 18

1 Inledning

Detta stöd är tänkt att underlätta arbetet för de statliga myndigheter som på särskilt uppdrag från regeringen[1] ska bedöma och redovisa informationssäkerhet i sin risk- och sårbarhetsanalys (RSA)[2] för 2015. Stödet är även tänkt att underlätta sammanställningen av den information som myndigheterna redovisar så att det blir möjligt för mottagarna att teckna en lägesbild dels över myndigheternas interna informationssäkerhet, dels hur det ser ut i deras ansvarsområde.

I stödet beskrivs hur regeringens uppdrag rörande bedömning och redovisning av informationssäkerhet (informationssäkerhetsuppdraget 2015) kan hanteras på en generell nivå av de myndigheter som berörs. Beskrivningen baseras i grunden på hur Myndigheten för samhällsskydd och beredskap (MSB) har tolkat sitt eget informationssäkerhetsuppdrag 2015.

Stödet är helt frivilligt att använda.

Stödet beskriver:

1. tolkning,
2. genomförande, samt
3. redovisning.

MSB gör bedömningen att det särskilt är hot och risker med koppling till krisberedskap, samhällsviktig verksamhet och kontinuitetshantering som bör utgöra fokus för arbetet.

2 Syftet med stödet

Det övergripande syftet med att ge ut detta stöd är att göra det så enkelt som möjligt för regeringen att få en sammanställd lägesbild av myndigheternas redovisade resultat. Detta görs genom att presentera en metod som ska förenkla arbetet med uppdraget för myndigheterna, främst genom att anknyta till existerande processer för arbete med informationssäkerhet och RSA, samt föreslå ett enhetligt sätt för redovisning av uppdraget. Använder flera myndigheter samma metod för arbete och redovisning blir det slutliga resultatet enklare att aggregera.

[1] Uppdraget att redovisa informationssäkerheten i RSA har regeringen beslutat i myndigheternas regleringsbrev.
[2] Det vill säga de risk- och sårbarhetsanalyser som ska genomföras enligt 9 § förordningen (2006:942) om krisberedskap och höjd beredskap.

3 Målgruppen för stödet

Målgruppen är de, inom respektive berörd myndighet, som arbetar med informationssäkerhetsfrågor med koppling till myndighetens risk- och sårbarhetsanalys i detta regeringsuppdrag.

4 Bakgrund till stödet

4.1 Varför ett stöd?

Regeringen har beslutat att myndigheter som har särskilt ansvar för krisberedskap och höjd beredskap särskilt ska beakta och analysera informationssäkerhet ur olika perspektiv i sitt arbete med 2015 års RSA. Informationssäkerhetsuppdraget 2015 riktades till samtliga myndigheter som omnämns i bilagan till förordning (2006:942) om krisberedskap och höjd beredskap (KBF). I myndigheternas regleringsbrev angavs även att uppgiften skulle redovisas som en del av den sammanställning som görs i arbetet med RSA. MSB har som nämnts också fått ett informationssäkerhetsuppdrag 2015 med ovan nämnda innehåll.

Mot bakgrund av MSB:s uppgift att stödja och samordna samhällets informationssäkerhet, myndighetens arbete med RSA samt att ett antal myndigheter har uttryckt önskemål om stöd från MSB har MSB valt att ta fram ett stöd för hur arbetet med informationssäkerhetsuppdraget 2015 skulle kunna genomföras. Valet att ge ett sådant stöd har även sin grund i att Riksrevisionen vid en nyligen genomförd granskning av informationssäkerheten i den civila statsförvaltningen[3] rekommenderat att MSB bör fortsätta och även intensifiera sitt arbete med att försöka skapa en gemensam lägesbild för informationssäkerhet i statsförvaltningen. När det gäller RSA konstaterar Riksrevisionen att det finns omfattande brister vad gäller hur myndigheterna redovisar informationssäkerhet i dessa analyser. Bristerna gör att det inte går att ”ställa samman en gemensam bild av samlad förmåga att kunna motstå och hantera kriser inom informationssäkerhetsområdet”.[4]

Genom att de myndigheter som berörs av regleringsbrevsuppdraget genomför, sammanställer och redovisar uppdraget på ett förhållandevis enhetligt sätt underlättas möjligheten för mottagarna att sammanställa och analysera det aggregerade resultatet.

Eftersom informationssäkerhetsuppdragen 2015 är snarlika men inte helt identiska för samtliga berörda myndigheter har utformningen av stödet för hur en myndighet kan genomföra, sammanställa och redovisa uppdraget utgått

[3] Riksrevisionen, Informationssäkerheten i den civila statsförvaltningen, RiR 2014:23, 2014
[4] Riksrevisionen, Informationssäkerheten i den civila statsförvaltningen, RiR 2014:23, 2014 s 59

från tolkningarna av formuleringarna i MSB:s eget uppdrag men getts en generell utformning.

4.2 Informationssäkerhetsuppdrag 2015

I regleringsbrevet för 2015 fick som nämndes ovan samtliga myndigheter som omnämns i bilagan till KBF ett särskilt uppdrag att beakta och analysera informationssäkerhet i samband med redovisningen av RSA:er enligt 9 § KBF. De olika regleringsbrevsuppdragen är snarlikt utformade för de olika myndigheterna.

I MSB:s regleringsbrev för 2015 står följande:

"14. Myndigheten för samhällsskydd och beredskap ska i arbetet med 2015 års risk- och sårbarhetsanalyser särskilt beakta och analysera informationssäkerheten i de delar av verksamheten och i de tekniska system som är nödvändiga för att myndigheten ska kunna utföra sitt arbete. I detta arbete ska även informationssäkerheten inom myndighetens ansvarsområde beaktas och analyseras. Myndigheten ska redovisa en bedömning av informationssäkerheten samt vidtagna åtgärder. Redovisningen ska vara en del av den sammanställning som görs i arbetet med risk- och sårbarhetsanalyser enligt 9 § förordningen (2006:942) om krisberedskap och höjd beredskap."

4.3 Närmare om MSB:s mandat

MSB har enligt 11 a § i förordning (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap i uppgift att stödja och samordna arbetet med samhällets informationssäkerhet samt analysera och bedöma omvärldsutvecklingen inom området. I detta ingår bland annat att lämna råd och stöd i fråga om förebyggande arbete till andra statliga myndigheter. Myndigheten ska även rapportera till regeringen om förhållanden på informationssäkerhetsområdet som kan leda till behov av åtgärder inom olika nivåer och områden i samhället.

De myndigheter som har ett särskilt ansvar för krisberedskapen enligt 11 § KBF och de myndigheter som MSB beslutar i enskilda fall, ska lämna en redovisning baserad på RSA till Regeringskansliet och MSB. Enligt 34 § samma lag har MSB rätt att meddela de ytterligare föreskrifter som behövs för verkställigheten av 9 § KBF om RSA. Med stöd av detta mandat har MSB utfärdat föreskrifter om hur bland annat statliga myndigheter ska redovisa sina RSA, MSB:s föreskrifter och allmänna råd om statliga myndigheters risk- och sårbarhetsanalyser MSBFS 2015:3. MSB har även publicerat en vägledning för

RSA [5] och en vägledning för identifiering av samhällsviktig verksamhet och kritiska beroenden[6].

Stödet rörande informationssäkerhetsuppdraget 2015 är framtaget med stöd av MSB:s mandat inom informationssäkerhetsområdet.

[5] Vägledning för risk- och sårbarhetsanalyser, https://www.msb.se/RibData/Filer/pdf/25893.pdf
[6] Vägledning för samhällsviktig verksamhet – identifiering av samhällsviktig verksamhet och kritiska beroenden samt bedöma acceptabel avbrottstid, https://www.msb.se/RibData/Filer/pdf/27285.pdf

5 MSB:s tolkning av uppdraget

5.1 Behov av tolkning

Utformningen av informationssäkerhetsuppdraget 2015 ger, enligt MSB:s egen bedömning, visst utrymme för tolkning. Det gäller främst uppdragets omfattning. De frågor som väcks rör exempelvis hur ingående analysen ska göras och vad som ska omfattas. Frågorna aktualiseras särskilt i samband med uppgiften att redogöra för informationssäkerhet inom myndighetens ansvarsområde.

En annan aspekt som förutsätter viss tolkning är hur uppdraget ska redovisas. Enligt informationssäkerhetsuppdraget 2015 ska redovisningen vara en del av den sammanställning som görs i arbetet med risk- och sårbarhetsanalyser enligt 9 § KBF. Det framgår dock inte helt om, och i så fall hur, denna ”del” ska särskiljas från den övriga redovisningen av RSA.

5.2 Underlag för tolkningen

I följande avsnitt redovisas MSB:s tolkning av informationssäkerhetsuppdraget 2015. Tolkningen baseras i första hand på de mål och det syfte med informationssäkerhetsuppdraget 2015 som direkt kan utläsas av uppdraget[7], men stöd kan även hämtas från andra uttalanden som regeringen har gjort med anledning av uppdraget.

Regeringen har i första hand beskrivit informationssäkerhetsuppdraget 2015 och syftet med att besluta om ett sådant uppdrag i en skrivelse som publicerades i mars 2015[8]. Den skrivelsen togs fram som ett svar på den granskningsrapport som Riksrevisionen hade lämnat till riksdagen i november 2014 rörande informationssäkerheten i den civila statsförvaltningen[9]. I Riksrevisionens rapport ges en fördjupad bild av de behov och problembilder som omhändertas i regeringens skrivelse och därför ingår även Riksrevisionens rapport som en bakgrund i tolkningsunderlaget. Dessutom anser MSB att regeringens urval av myndigheter som har fått informationssäkerhetsuppdraget 2015 bör utgöra ett underlag vid tolkningen. Ett annat är det faktum att regeringen valt att arbetet med och redovisningen av informationssäkerhetsuppdraget 2015 ska ske inom ramen för RSA.

5.3 Identifierade syften

Det är särskilt två syften som MSB efter analys av underlagen som nämns i föregående avsnitt, och då särskilt regeringens skrivelse, har bedömt som centrala för hur arbetet med informationssäkerhetsuppdraget 2015 kan genomföras.

---

[7] Se avsnit 4.2.
[8] Skr 2014/15:84 Riksrevisionens rapport om informationssäkerhet i den civila statsförvaltningen, 2015.
[9] Riksrevisionen, Informationssäkerheten i den civila statsförvaltningen, RiR 2014:23, 2014

Regeringen önskar få en *förbättrad lägesbild på informationssäkerhetsområdet*. Det kan sägas vara det första och övergripande syftet med informationssäkerhetsuppdraget 2015 som också får direkt betydelse för tolkningen av uppdraget. Det andra, kompletterande syftet, att fokus inom informationssäkerhetsområdet bör riktas mot dess betydelse för krisberedskap och ”*samhällets beredskap och robusthet mot allvarliga it-incidenter*”.

I informationssäkerhetsuppdraget 2015 nämner även regeringen att ett syfte är att *höja medvetenheten om vikten av informationssäkerhet*. Enligt MSB:s mening kan en sådan höjd medvetenhet uppnås på flera sätt och är mindre beroende av hur själva arbetet med informationssäkerhetsuppdraget 2015 utformas i detalj. Arbetet med lägesbild bidrar i hög grad till höjd medvetenhet.

I sin granskningsrapport från förra året pekade Riksrevisionen på att RSA-redovisningen uppvisade omfattande brister när det gällde informationssäkerhet[10] samt att det med stöd av RSA ”*i sin nuvarande utformning*” inte gick att ”*ge en nationell, sammantagen bild av myndigheternas förmåga att hantera och motstå kriser på informationssäkerhetsområdet*”[11].

I sin skrivelse, med anledning av Riksrevisionens rapport, slår regeringen fast att en stärkt krisberedskap är en prioriterad fråga och målet är att minska riskerna för och konsekvenserna av allvarliga händelser och kriser i samhället. Genom informationssäkerhetsuppdraget 2015 kommer enligt skrivelsen både regeringens och myndigheternas kunskap på området att förbättras:

”I syfte att höja medvetenheten om vikten av informationssäkerhet och för att skapa en bild av läget hos berörda myndigheter har regeringen i respektive myndighets regleringsbrev för 2015 beslutat att myndigheter som har ett särskilt ansvar för krisberedskap och höjd beredskap särskilt ska redovisa sitt arbete med informationssäkerhet.”[12]

Avslutningsvis konstaterar regeringen i skrivelsen att flera åtgärder på informationssäkerhetsområdet, bland annat informationssäkerhetsuppdraget 2015, har vidtagits ”*i syfte att förbättra samhällets beredskap och robusthet mot allvarliga it-incidenter*” samt att regeringen ”*avser att även fortsättningsvis prioritera arbetet*”.[13]

Av skrivningen framgår att regleringsbrevsuppdraget har som syfte att höja medvetenheten om vikten av informationssäkerhet samt bidra till en lägesbild.

---

[10] Riksrevisonen, *Informationssäkerheten i den civila statsförvaltningen*, RiR 2014:23, 2014 s 77
[11] Riksrevisionen *Informationssäkerheten i den civila statsförvaltningen*, RiR 2014:23, 2014 s 47
[12] Skr 2014/15:84 *Riksrevisionens rapport om informationssäkerhet i den civila statsförvaltningen*, 2015, s 14.
[13] Skr 2014/15:84 *Riksrevisionens rapport om informationssäkerhet i den civila statsförvaltningen*, 2015 s 15

Detta utgör den huvudsakliga grunden för MSB:s tolkning av det första och övergripande syftet med regleringsbrevsuppdraget.

När det gäller det kompletterande syftet, det vill säga vilka aspekter som ska tas upp särskilt vid denna lägesbild på informationssäkerhetsområdet, kan följande noteras. Regeringen har i sin skrivelse och med referenser till Riksrevisionens rapport på flera sätt satt in informationssäkerheten i en kontext med koppling till krisberedskap och behovet av att förbättra samhällets beredskap och robusthet mot allvarliga it-incidenter. Denna koppling förstärks enligt MSB:s uppfattning även av valet att rikta informationssäkerhetsuppdraget 2015 om informationssäkerhet till de myndigheter som har ett särskilt ansvar för krisberedskap och höjd beredskap samt tydliggjort att uppdraget ska redovisas som en del av ”den sammanställning som görs i arbetet med risk- och sårbarhetsanalyser” enligt 9 § KBF.

När samhällets förmåga att upprätthålla beredskap och robusthet uttryckligen nämns gör MSB tolkningen att särskild uppmärksamhet bör riktas mot de mest centrala funktionerna i samhället – det vill säga samhällsviktig verksamhet. Samhällsviktig verksamhet är även en viktig del myndigheternas arbete med RSA och omnämns uttryckligen i 9 § KBF. Enligt de verkställighetsföreskrifter som MSB har utfärdat rörande tillämpningen av 9 § KBF ska statliga myndigheter med ett geografiskt områdesansvar redovisa samhällsviktig verksamhet av regional betydelse, medan statliga myndigheter med ett sakområde ska redovisa samhällsviktig verksamhet av nationell betydelse.[14] Eftersom arbetet med informationssäkerhetsuppdraget 2015 har en utpekad koppling till myndigheternas arbete med och redovisning av RSA bör fokus riktas mot den samhällsviktiga verksamhet som omfattas av RSA.[15]

Ett arbete som ska ge samhällsviktig verksamhet beredskap och robusthet mot allvarliga it-incidenter behöver omfatta kontinuitetshantering. Kontinuitetshantering bidrar till ett mindre sårbart samhälle och är en metod för att skapa en förmåga att kunna fortsätta att bedriva sin verksamhet på en acceptabel nivå, oavsett vilken typ av störning som organisationen utsätts för.

Detta sammantaget gör att MSB uppfattar att arbetet med informationssäkerhetsuppdraget 2015 bör behandla informationssäkerhet med koppling till krisberedskap och där särskilt rikta fokus mot förmågan till kontinuitetshantering i samhällsviktig verksamhet.

[14] 5 § Myndigheten för samhällsskydd och beredskaps föreskrifter1 om statliga myndigheters risk- och sårbarhetsanalyser, MSBFS 2015:3

[15] I de allmänna råden till MSBFS 2015:3 tydliggörs ytterligare vilken samhällsviktig verksamhet som ska redovisas.

5.4 Att beakta och analysera informationssäkerheten

Enligt informationssäkerhetsuppdraget 2015 får myndigheterna i uppgift att i arbetet med 2015 års RSA ”särskilt beakta och analysera” informationssäkerheten. Syftet med RSA är enligt 9 § KBF att stärka myndigheternas egna respektive samhällets krisberedskap och detta ska bland annat ske genom att myndigheterna årligen analyserar om det finns sådan sårbarhet eller sådana hot och risker inom myndighetens ansvarsområde som synnerligen allvarligt kan försämra förmågan till verksamhet inom området.

Eftersom informationssäkerhetsuppdraget 2015 ska redovisas som en del av myndighetens RSA gör MSB därför tolkningen att bedömningen av informationssäkerheten bör särskilt röra de aspekter som redovisas i RSA. Det vill säga identifierade och analyserade hot, risker, sårbarheter, kritiska beroenden och åtgärder med koppling till krisberedskap och samhällsviktig verksamhet. Allt i enlighet med den övriga redovisningen av resultaten från RSA så som den regleras i MSBFS 2015:3. Dispositionen som anvisas i nämnda föreskrifter, är enligt MSBS:s uppfattning, ett lämpligt stöd eftersom det är centralt att beakta exempelvis sårbarheter, hot och risker vid bedömningen av informationssäkerhet.

MSB vill betona att även om MSB gör tolkningen att arbetet med informationssäkerhetsuppdraget 2015 särskilt bör fokusera på informationssäkerhet som ett stöd för myndighetens och samhällets krisberedskap, och då särskilt i form av kontinuitetshanteringen hos samhällsviktig verksamhet, inte på något sätt utesluter att även andra aspekter av informationssäkerhet analyseras.

5.5 Vidtagna åtgärder

Enligt informationssäkerhetsuppdraget 2015 ska inte bara en bedömning av informationssäkerheten redovisas utan även vidtagna åtgärder. Vad vidtagna åtgärder innebär kan tolkas på olika sätt. Med tanke på att regeringen önskar en lägesbild över samhället gör MSB bedömningen att det här är av större betydelse att få en bild av hur myndigheternas har valt att arbeta med sin interna informationssäkerhet, eller i sitt ansvarsområde, på en mer övergripande nivå än att fokusera på enstaka säkerhetsåtgärder. Som några exempel på relevanta frågor för den övergripande nivån kan i så fall nämnas: Finns förutsättningarna för ett systematiskt arbete på plats? Är ansvar och roller utpekade? Har resurser avsatts för informationssäkerhetsarbetet?

5.6 Att redovisa bedömningen och vidtagna åtgärder

Redovisningen av myndighetens bedömning av informationssäkerheten samt vidtagna åtgärder ska enligt informationssäkerhetsuppdraget 2015 uttryckligen vara en del av den sammanställning som görs i arbetet med RSA.[16] Det innebär

[16] Formuleringen är hämtad från MSB:s regleringsbrev 2015

enligt MSB:s uppfattning att redovisningen behöver följa dispositionen som föreskrivs i 5 respektive 6 §§ i MSBFS 2015:3.

Regeringens uttalade målsättning att informationssäkerhetsuppdraget 2015 ska bidra till förbättrad lägesbild och ökad medvetenhet om informationssäkerhet, behöver enligt MSB också beaktas i samband med redovisningen av uppdraget. För att underlätta arbetet med att nå denna målsättning är det av vikt att det är så enkelt som möjligt att sammanställa och aggregera informationen. Även Riksrevisionens analys av bristerna på området och rekommendationerna till MSB stödjer denna tolkning. I praktiken innebär det att det är värdefullt om:

1. så många myndigheter som möjligt utför regleringsbrevsuppdraget på ett metodmässigt likartat sätt, samt att
2. redovisningen av regleringsbrevsuppdraget på ett enkelt sätt kan samlas in från RSA för att därefter sammanställas och analyseras.

6 Fokusområden i regleringsbrevsuppdraget

I regleringsuppdraget omnämns ett antal fokusområden som myndigheten, med ovan nämnda ingångsvärden, särskilt ska beakta och analysera. Vilka fokusområden som omnämns skiljer sig delvis åt mellan olika myndigheter. Flera myndigheter har dock, precis som MSB, fått i uppdrag att beakta och analysera informationssäkerheten:

- i de delar av *verksamheten* som är nödvändiga för att myndigheten ska kunna utföra sitt arbete,
- i de *tekniska system* som är nödvändiga för att myndigheten ska kunna utföra sitt arbete, samt
- inom *myndighetens ansvarsområde*.

Med hänsyn till att en bedömning av att den egna verksamhetens informationssäkerhet är så nära sammankopplad med informationssäkerheten i de tekniska system som är nödvändiga för att myndigheten ska kunna utföra sitt arbete ser MSB fördelar med att göra en gemensam bedömning av dessa två punkter. De skulle kunna sägas motsvara myndighetens interna informationssäkerhet. Bedömningen av informationssäkerheten inom myndighetens ansvarsområde skulle istället kunna beskrivas som en bedömning av det externa förhållandet, det vill säga genomförande av uppdraget avseende myndighetens sak- eller geografiska områdesansvar.

7 Förslag på genomförande

7.1 Fokus på samhällsviktig verksamhet och krisberedskap

Detta kapitel utgör ett stöd för den enskilda myndigheten att genomföra uppdraget i sin egen verksamhet och för sitt sakområdes- respektive geografiska områdesansvar. Enligt MSB:s tolkning av informationssäkerhetsuppdraget 2015 bör analysen koncentreras till samhällsviktig verksamhet och krisberedskap.

I 2 § MSBFS 2015:3 definierar MSB begreppet *samhällsviktig verksamhet* på följande sätt:

”Med samhällsviktig verksamhet avses en verksamhet som uppfyller minst ett av följande villkor:

- *Ett bortfall av, eller en svår störning i verksamheten som ensamt eller tillsammans med motsvarande händelser i andra verksamheter på kort tid kan leda till att en allvarlig kris inträffar i samhället.*
- *Verksamheten är nödvändig eller mycket väsentlig för att en redan inträffad kris i samhället ska kunna hanteras så att skadeverkningarna blir så små som möjligt.”*

Vid en analys av *krisberedskap* ska enligt 9 § KBF en myndighet analysera om det finns *”sådan sårbarhet eller sådana hot och risker inom myndighetens ansvarsområde som synnerligen allvarligt kan försämra förmågan till verksamhet inom området”* och då särskilt beakta:

1. *situationer som uppstår hastigt, oväntat och utan förvarning, eller en situation där det finns ett hot eller en risk att ett sådant läge kan komma att uppstå,*
2. *situationer som kräver brådskande beslut och samverkan med andra aktörer,*
3. *att de mest nödvändiga funktionerna kan upprätthållas i samhällsviktig verksamhet, och*
4. *förmågan att hantera mycket allvarliga situationer inom myndighetens ansvarsområde.*

7.2 Stöd för bedömning av informationssäkerhet inom myndigheten och i myndighetens ansvarsområde

För att förenkla uppdragets genomförande föreslår MSB att det sker i två steg: först för den egna verksamheten och därefter för det sak- respektive geografiska områdesansvar som myndigheten har. Samma stöd för bedömningar kan dock användas i båda fallen.

För att kunna göra den bedömning av informationssäkerhet som regeringens uppdrag innebär måste en koppling göras mellan verksamhet och informationshantering. Detta görs lämpligen genom en processorienterad informationskartläggning av de verksamhetsprocesser som utpekats som samhällviktiga. Stöd för att genomföra kartläggningen finns i MSB:s vägledning.

Att göra denna kartläggning av informationshantering är av central betydelse för att kunna identifiera verksamhetens beroende av information. Informationskartläggningen gör det möjligt att identifiera de olika typer av bärare som till exempel telefoni, it-system, molntjänster och kommunikation använder för att hantera informationen. En sammanställning kan göras av de resurser i form av information och tekniska lösningar som är kritiska för att kunna upprätthålla verksamheten på rimlig nivå. I detta sammanhang bör två saker noteras:

- Med rimlig nivå avses inte enbart tillgänglighet. Även krav på riktighet, spårbarhet och konfidentialitet i informationshanteringen, för att verksamheten ska kunna upprätthållas med tillräcklig kvalitet, ska analyseras.
- Kritiska beroenden kan finnas till särskilda resurser. I de fall där kontinuitetsåtgärder som reservrutiner införts för att reducera negativa konsekvenser av dessa beroenden, bör detta noteras.

Kartläggningen kan sedan användas för att genomföra en riskanalys ur informationssäkerhetssynpunkt. Observera att analysen ska genomföras med inriktning på konskevenser för verksamheten och i förlängningen på nationell nivå om olika typer av risker realiseras. Ett annat viktigt förhållningssätt är att hot och risker av olika karaktär analyseras, inte endast antagonistiska hot riktade mot it-system.

Vid riskanalysen kan även sårbarheter framkomma. Dessa sårbarheter kan exempelvis bestå av kompetensbrist, bristande kontinuitetsplanering, för starkt beroende till enskild leverantör såväl som tekniska brister.

I uppdraget ingår även att rapportera om de åtgärder som vidtagits för att hantera risker och sårbarhet. MSB har, som tidigare nämnts, tolkat detta som det systematiska informationssäkerhetsarbete som myndigheter ska bedriva. För myndighetens interna arbete kan den inrapportering som skedde i samband med MSB:s enkät om informationssäkerhet i myndigheterna 2014 användas som underlag[17].

[17] Resultatet av enkäten redovisades i rapporten En bild av myndigheternas informationssäkerhetsarbete 2014, https://www.msb.se/RibData/Filer/pdf/27428.pdf

7.3 Genomförande i den egna verksamheten

Den analys som ska genomföras är enbart inriktad på informationssäkerhet och denna aspekt ska analyseras inom ramen för arbetet med den generella RSA som myndigheten är skyldig att genomföra enligt MSBFS 2015:3. Det finns också en föreskrift som gäller myndigheters arbete med informationssäkerhet, MSBFS 2009:10. I den senare föreskriften ställs krav på att myndigheten bland annat utifrån RSA och inträffade incidenter ska avgöra hur risker hanteras, samt besluta om åtgärder för myndighetens informationssäkerhet. Myndigheter förutsätts därmed ha en metod för att göra riskanalyser som går att hantera i ett informationssäkerhetsperspektiv som tillämpas systematiskt.

Som nämndes i avsnitt 5.3 ska, enligt 6 § MSBFS 2015:3, länsstyrelser redovisa samhällsviktig verksamhet av regional betydelse. Enligt 5 § i MSBSFS 2015:3 ska statliga myndigheter med ansvar för ett sakområde däremot redovisa samhällsviktig verksamhet av nationell betydelse.

Rekommendationen är att myndigheten vid sitt genomförande av uppdraget sammanställer underlaget utifrån det resultat som framkommit då myndigheten uppfyllt kraven i de två föreskrifterna.

Det innebär i korthet att de samhällsviktiga verksamheter inom en myndighet som identifierats i samband med generella RSA-arbetet nu analyseras ur en informationssäkerhetssynpunkt. Eftersom kontinuitetshantering ses som en förutsättning för krisberedskapen i detta sammanhang har denna fråga särskild betydelse när risker analyseras. Konkret innebär det att:

- Sammanställ de verksamheter som bedömts som samhällsviktiga inom myndigheten under RSA-arbetet.
- Bland de verksamheter som anses som samhällviktiga är det endast de som är av nationell alternativt regional[18] betydelse som ska bedömas. Kontrollera om det genomförts riskanalyser ur ett informationssäkerhetsperspektiv med inriktning på dessa nationellt/regionalt samhällsviktiga verksamheter under det senaste året.
- Om riskanalyser är genomförda och dokumenterade använd dessa som underlag. Säkerställ att riskanalyserna även omfattar samtliga väsentliga tekniska system som stödjer informationshanteringen i den nationellt/regionalt samhällsviktiga verksamheten.
- Om riskanalyser saknas genomför då sådana med den metod som generellt tillämpas inom myndigheten.
- Om beslutad metod saknas använd då en enkel metod som bygger på att risker bedöms utifrån konsekvens och sannolikhet.

[18] Gäller endast länsstyrelser.

- Säkerställ att risker kopplade till bristande kontinuitetshantering identifierats och analyserats.

7.4 Genomförande av analys för sak- respektive geografiskt områdesansvar

Denna del av uppdraget är sannolikt mer krävande för myndigheten. Det är därför lämpligt att skapa ett formellt projekt kring detta för att säkerställa en tydlig planering och att det finns tillräckligt med resurser för att genomföra det.

Kommunikation

Eftersom det är nödvändigt att engagera flera personer inom myndigheten inklusive ledningen, är det lämpligt att skapa en kommunikationsplan för att gå igenom hur kommunikation bör ske samt i detta arbete även ta fram en tidsplan.

Materialinsamling

I denna del som ligger utanför myndighetens egen verksamhet är ett rimligt första steg att samla in ett underlag från de aktörer som står för nationellt alternativt regionalt[19] samhällviktig verksamhet inom myndighetens ansvarsområde. Främst är det aktörernas riskanalyser av sin nationellt samhällsviktiga verksamhet som är av intresse, men det kan även vara annan typ av dokumentation som beskriver de hot aktörerna själva ser för sin verksamhet. I den mån myndigheten själv har sammanställt hot och risker mot verksamhet av den typ som avses här inom det egna sak- respektive geografiska ansvarsområdet, bör detta användas som underlag. Även uppgifter om vidtagna säkerhetsåtgärder av aktörerna bör inhämtas där så är möjligt. I vissa fall kanske intervjuer och andra sätt att samla information kan vara nödvändiga för att förstå hotbilden hos de olika aktörerna eller för att få rätt kontext till frågeställningarna.

Exempelvis genomför MSB i samverkan med SKL en enkätundersökning av kommuners informationssäkerhet och har även kartlagt styrningen av informationssäkerhet inom vården.[20]

Analys av insamlat material

Det material som har samlats in sammanställs och analyseras så att det på ett lämpligt sätt framgår:

- Vad aktörerna själva bedömt som samhällsviktig verksamhet och i de fall där detta inte definierats, analysera vad som kan vara det.

[19] Gäller endast länsstyrelser.
[20] https://www.msb.se/sv/Om-MSB/Nyheter-och-press/Nyheter/Nytt-informationssakerhet/En-bild-av-kommunernas-informationssakerhetsarbete-2015/ och https://www.msb.se/sv/Om-MSB/Nyheter-och-press/Nyheter/Nyheter-fran-MSB/Kartlaggning-visar-pa-risker-och-brister-i-vardens-informationshantering/

- Vilken samhällsviktig verksamhet som är av nationell respektive regional betydelse.
- Informationssäkerhetsaspekter avseende tillgänglighet, riktighet, konfidentialitet och spårbarhet.
- Om det finns enskilda risker eller sårbarheter som återkommer hos flera aktörer.
- Där så är möjligt analysera beroendeförhållanden mellan exempelvis olika aktörer.
- En sammanställning av de åtgärder som vidtagits av aktörer inom ansvarsområdet för att förbättra säkerheten.

Därefter kan en sammanställning av ett antal hot mot samhällsviktig verksamhet göras av projektledaren.

Riskanalys

Riskanalys bör genomföras med deltagande från myndighetens ledning eftersom områdesansvaret är en central del i myndighetens uppdrag. En workshop där projektledare, ledningen, informationssäkerhetsansvarig och beredskapsansvarig deltar är en lämplig form för att genomföra riskanalysen.

Projektledaren leder analysen med stöd av myndighetens metod för riskanalys, eller om sådan saknas med annan enkel metod som bygger på att risker bedöms utifrån konsekvens och sannolikhet. Därefter föreslås följande aktiviteter:

- Projektledaren presenterar de hot som tagits fram ur analysen av aktörernas underlag och en bedömning görs hur den generella risken för varje hot ser ut.
- Workshopen tar ställning till om det finns ytterligare hot som inte framkommit i den tidigare punkten och analyserar i så fall dessa.
- En gemensam analys av eventuella kritiska beroenden som framkommit vid sammanställningen av aktörernas egna riskanalyser och annat underlag.
- Säkerställande av att risker kopplade till bristande kontinuitetshantering identifierats och analyserats.
- En gemensam bedömning av vidtagna säkerhetsåtgärder hos aktörer inom ansvarsområdet.

8 Redovisning av bedömningen

Resultaten av analyserna för myndighetens verksamhet och ansvarsområde ska enligt informationssäkerhetsuppdraget 2015 redovisas inom ramen för RSA. Det redovisade resultatet kan innehålla uppgifter av känslig karaktär och behöver hanteras med lämplig säkerhetsnivå. I 18 kap. 13 § offentlighets- och sekretesslagen (OSL) ges också möjlighet att skydda uppgifter i upprättade RSA. Sekretessen gäller endast om det kan antas att det allmännas möjligheter att förebygga eller hantera fredstida kriser skulle motverkas om uppgiften röjs.[21] När det gäller uppgifter som rör myndighetens bedömning av den egna informationssäkerheten och informationssäkerheten i ansvarsområdet kan sådana uppgifter dessutom komma att aktualisera sekretess till skydd för säkerhets- och bevakningsåtgärder enligt 18:8 OSL. Även andra sekretessbestämmelser kan bli aktuella.

Mot bakgrund av regeringens anvisning att uppdraget ska redovisas i RSA gör MSB tolkningen att redovisningen därför behöver följa den disposition som är föreskriven i MSBFS 2015:3. Dispositionen innehåller dock en del punkter som inte är direkt tillämpliga vid redovisningen alternativt behöver tolkas. Det handlar främst om punkten 6 i vilken den generella krisberedskapen ska redovisas, något som enligt MSB:s uppfattning faller utanför informationssäkerhetsuppdraget 2015, samt punkten 8 där en redovisning av informationssäkerhetsuppdraget 2015 får ta sikte på ”vidtagna åtgärder” istället.

Som framgår av bland annat KBF, föreskrifterna på området, MSBFS 2015:3, och MSB:s vägledning för RSA[22] innebär RSA ett förhållandevis omfattande arbete där en mängd olika typer av information ska samlas in, analyseras och redovisas. Eftersom det huvudsakliga syftet med RSA är att ge en sammanhållen bild av respektive myndighets bedömning av olika sårbarheter och risker har MSB sett det som värdefullt att myndigheterna redovisar sin RSA på ett sammanhållet sätt och i enlighet med anvisad disposition – det vill säga inte gör någon särredovisning av olika aspekter.

I detta fall finns det dock som nämnts även andra ingångsvärden som behöver beaktas. Redovisningen av informationssäkerheten för de berörda myndigheterna sker här inom ramen för ett särskilt regleringsbrevsuppdrag för 2015. Genomförandet och redovisningen av uppdraget ska enligt regeringen uttryckligen bidra till att ”skapa en bild av läget hos berörda myndigheter”. För att uppnå syftet med informationssäkerhetsuppdraget 2015 bör regleringsbrevsinformationen på något sätt särskiljas för att underlätta arbetet med att sammanställa redovisningen till en gemensam lägesbild.

---

[21] Tillämpningen av sekretessbestämmelsen beskrivs närmare i MSB, Vägledning för risk och sårbarhetsanalyser, 2011, s 20f

[22] MSB, Vägledning för risk- och sårbarhetsanalyser, 2011 https://www.msb.se/sv/Produkter--tjanster/Publikationer/Publikationer-fran-MSB/Vagledning-for-Risk--och-sarbarhetsanalyser/

Enligt MSB:s mening kan detta enklast ske genom att under respektive rubrik i dispositionen redovisa informationssäkerhetsaspekterna under en särskild underrubrik, exempelvis ”Informationssäkerhetsuppdraget 2015”. Med hänsyn till uppgifternas känslighet kan även en bilaga som omfattas av sekretess bli aktuell.

Här följer en genomgång av hur informationssäkerhetsfrågorna kan kopplas till respektive punkt i RSA-redovisningen. I ett flertal av punkterna bör den interna respektive externa rapporteringen särskiljas. Rubrikerna är hämtade från MSBFS 2015:3:

1. ”Beskrivning av myndigheten och dess ansvarsområde”.

   [Någon särskild redovisning av informationssäkerhetsuppdraget 2015 behövs inte här]

2. ”Beskrivning av arbetsprocess och metod”.

   Informationssäkerhetsuppdraget 2015

   [Här redovisas arbetsprocessen och metoden som myndigheten har följt när det gäller arbetet med informationssäkerhetsuppdraget 2015. Beskrivningen är central för att kunna jämföra resultat mellan olika myndigheter. Här bör exempelvis underlag, involverade aktörer, avgränsning, arbetsprocesser, metodval och bedömningsskalor redovisas.]

3. ”Identifierad samhällsviktig verksamhet inom myndighetens ansvarsområde som är av nationell betydelse” för myndigheter med ett sakområdesansvar respektive ”Identifierad samhällsviktig verksamhet inom det geografiska området som är av regional betydelse” för länsstyrelser.

   [Någon särskild redovisning av regleringsbrevsuppdraget behövs inte här.]

4. ”Identifierade kritiska beroenden för den identifierade samhällsviktiga verksamheten”.

   Informationssäkerhetsuppdraget 2015

   [Denna punkt bör redovisas så att det interna respektive externa ansvaret hålls åtskilt i rapporteringen. Här redovisas en översikt över identifierade kritiska beroenden och en övergripande bedömning av dessa ur ett kontinuitetsperspektiv. Bedömningen bör även innefatta en gradering av de kritiska beroendena. Hur graderingen har utförts bör framgå av redovisningen. Om det i den externa analysen framkommer att vissa kritiska beroenden finns hos flera aktörer och därför kan

ses som mer generella bör detta särskilt noteras i den övergripande bedömningen.]

5. ”Identifierade och analyserade hot och risker för myndigheten och dess ansvarsområde” för myndigheter med ett sakområdesansvar respektive ” Identifierade och analyserade hot och risker för länsstyrelsen och länets geografiska område”.

   Informationssäkerhetsuppdraget 2015

   [Denna punkt bör redovisas så att det interna respektive externa ansvaret hålls åtskilt i rapporteringen. Här redovisas en översikt över identifierade hot och risker samt en övergripande bedömning av dessa. Bedömningen bör även innefatta en gradering av identifierade hot och risker. Hur graderingen har utförts bör framgå av redovisningen. Om det i den externa analysen framkommer att vissa hot och risker riktas mot flera aktörer och därför kan ses som mer generella bör detta särskilt noteras i den övergripande bedömningen.]

6. ”Bedömning av myndighetens generella krisberedskap enligt indikatorer som framgår av bilaga”.

   [Se bilaga till MSBFS 2015:3 under rubrik Informationssäkerhet.]

7. ”Beskrivning av identifierade sårbarheter och brister i krisberedskap inom myndigheten och dess ansvarsområde” för myndigheter med ett sakområdesansvar, respektive ”Beskrivning av identifierade sårbarheter och brister i krisberedskap inom länsstyrelsen och dess geografiska område” för länsstyrelser.

   Informationssäkerhetsuppdraget 2015

   [Denna punkt bör redovisas så att det interna respektive externa ansvaret hålls åtskilt i rapporteringen. Här redovisas en översikt över identifierade sårbarheter samt en övergripande bedömning av dessa. Bedömningen bör även innefatta en gradering av identifierade sårbarheter och brister. Hur graderingen har utförts bör framgå av redovisningen. Om det i den externa analysen framkommer att vissa sårbarheter och brister finns hos flera aktörer och därför kan ses som mer generella, bör detta särskilt noteras i den övergripande bedömningen.]

8. ”Genomförda, pågående och planerade åtgärder sedan föregående RSA-rapportering”**.**

Informationssäkerhetsuppdraget 2015

[Denna punkt bör redovisas så att det interna respektive externa ansvaret hålls åtskilt i rapporteringen. Här redovisas de åtgärder som vidtagits inom myndighetens verksamhet och ansvarsområde för att hantera risker och minska sårbarheter. Redovisningen behöver enbart omfatta vidtagna åtgärder av betydelse för informationssäkerhetsuppdraget 2015. Hur vidtagna åtgärder kan tolkas framgår av avsnitt 5.5.

Om det i den externa analysen framkommer att vissa åtgärder har vidtagits av flera aktörer och därför kan ses som mer generella, bör detta särskilt noteras i den övergripande bedömningen.”]

9. ”Behov av ytterligare åtgärder med anledning av risk- och sårbarhetsanalysens resultat.”

Informationssäkerhetsuppdraget 2015

[Här redovisas en översikt över identifierade behov av ytterligare åtgärder inom myndighetens verksamhet och ansvarsområde samt en övergripande bedömning av dessa.]