Myndigheten för samhällsskydd och beredskap

UPPDRAGSREDOVISNING

Datum	Diarienr
2010-03-01	2010-6304

Tillgänglig och skyddad kommunikationsinfrastruktur för offentlig sektor

Svar på regeringens uppdrag till Myndigheten för samhällsskydd och beredskap

(Fö2010/701/SSK, Regeringsbeslut 12, 2010-04-14)

Förord

Regeringen gav den 14 mars 2010 Myndigheten för samhällsskydd och beredskap (MSB) i uppdrag att senast den 1 mars 2011 lämna förslag beträffande en säker digital informations- och kommunikationsinfrastruktur för myndigheter, kommuner och landsting (Fö2010/702/SSK).

MSB redovisar i denna rapport sitt förslag på hur tillgängliga och skyddade kommunikationsinfrastrukturer för offentlig sektor kan skapas.

Gemensamma kravställningar, utvecklad upphandling, utvecklad uppföljning och kompetenshöjning bidrar till kostnadseffektiva åtgärder som förutom ökad tillgänglighet och skydd bedöms kunna leda till ekonomiska besparingar i offentlig sektor.

Förslagets bärande principer är att i nära samverkan med näringslivet utveckla lösningar på gemensamma problem för att öka tillgänglighet och skydd i kommunikationsinfrastrukturerna för offentlig sektor.

Stockholm 1 mars 2011

Helena Lindberg

Generaldirektör

Richard Oehme

Chef för Enheten för samhällets informationssäkerhet

Sammanfattning

Utvecklingen inom området

Den digitala agendan för Sverige ska vara en sammanhållen strategi som syftar till att statens existerande resurser ska nyttjas bättre. Förslagen i denna rapport tar fasta på en rad av de områden som berörs i agendan. Målet är att skapa tillgängliga och skyddade kommunikationsinfrastrukturer för offentlig sektor som utgår från existerande förutsättningar i samhället. Det handlar bland annat om att nyttja befintlig infrastruktur, anpassa sig till en livskraftig marknad i snabb utveckling och ta tillvara den höga tekniska kompetens som finns inom såväl privat som offentlig sektor.

Marknaden för elektronisk kommunikation i Sverige har de senaste 20 åren utvecklats från att var helt dominerad av en aktör till att inom flera områden vara konkurrensutsatt. Skydd och tillgänglighet i operatörsnäten blir ständigt bättre, och en aktiv samverkan mellan staten och privatägda operatörer bidrar också till att skapa goda förutsättningar för hög tillgänglighet inom elektronisk kommunikation. I takt med att e-förvaltningen etableras får vissa myndigheter allt större behov av att elektroniskt förmedla stora mängder information mellan varandra. Detta ökar i sin tur kraven på tillgängliga och skyddade kommunikationsinfrastrukturer.

Hoten mot den globala, digitala informations- och kommunikationsinfrastrukturen representerar allvarliga ekonomiska och säkerhetsmässiga utmaningar för samhället. Samhällets beroende av denna infrastruktur innebär att det ytterst också finns en säkerhetspolitisk dimension.

Flera länder skapar nu övergripande strukturer för koordinering och samverkan i syfte att säkerställa kommunikationen inom den offentliga sektorn, med samhällsövergripande samverkansfunktioner och nya gemensamma lösningar. Flera länder redovisar också bedömningar om att de totala kostnaderna för den offentliga sektorns IT-behov kan minskas tack vare de vidtagna åtgärderna. Det är rimligt att anta att motsvarande effekt skulle kunna uppnås även i Sverige.

De bärande principerna i det här tillämpas i Storbritannien. Genom privat-offentlig samverkan har Public Sector Network (PSN) utvecklats – ett gemensamt koncept för den offentliga sektorn, med tydliga beskrivningar av de tjänster som ska levereras. Dessa har definierats på ett tjänsteorienterat sätt för att både teknik och struktur ska kunna anpassas till marknadens utveckling.

Om den offentliga sektorn inte agerar gemensamt finns det en uppenbar risk för att nuvarande fragmenterade arbetssättet cementeras. Resultatet kan bli småskaliga divergerande lösningar som inte stödjer varandra och som istället blir kostnadsdrivande.

Det huvudsakliga förslaget

För att utveckla och upprätthålla tillgängliga och skyddade kommunikationsinfrastrukturer för offentlig sektor krävs det en sammanhållen organisatorisk struktur som över tiden förmår tillvarata de goda förutsättningar Sverige har som ett utvecklat IT-land. Det bärande elementet i en sådan struktur är det offentligas förmåga att ställa krav – och att följa upp krav.

Genom att formulera kravprofiler för tillgänglighet och skydd i offentlig sektors kommunikationer som stöd till avtalsansvarig myndighet, såväl vid ramavtal som vid specifik upphandling tillgodoses flera till synes motstridiga krav. För det första får offentlig sektors kommunikationer en jämn och hög kvalitet. För det andra effektiviseras upphandlingsarbetet. För det tredje kommer de gemensamma kravbilderna att skapa förutsättningar för en breddad konkurrens.

För att detta ska bli verklighet behövs en funktion för samordning och inriktning som tar fram, förvaltar och över tiden vidareutvecklar krav, med möjlighet att nivåanpassa tillgänglighet och skydd. Funktionen ska ha nära samverkan med såväl offentliga organisationer som marknadens aktörer.

Flera aktörer i offentlig sektor behöver redundans i sin kommunikationsinfrastruktur, exempelvis genom flera förbindelser, över olika nät, placerade hos olika operatörer. För ett begränsat antal myndigheter med särskilda behov av kontrollerbara kommunikationer kommer det också att behövas tillgång till en statlig kontrollerbar kommunikationsinfrastruktur. För detta specifika behov kommer det att behövas en funktion för förvaltning och drift.

En sammanhållen organisatorisk struktur

Mot bakgrund av ovanstående föreslår MSB att det etableras en organisatorisk struktur bestående av två funktioner:

- en funktion för samordning och inriktning vid Myndigheten för samhällsskydd och beredskap (MSB), och
- en funktion för drift och förvaltning vid Trafikverket ICT som ansvarar för drift och förvaltning av den statliga kontrollerbara kommunikationsinfrastrukturen som avdelas för att skapa redundans hos ett begränsat antal myndigheter med särskilda behov.

Till detta kommer en nära samverkan med upphandlingsansvarig myndighet. Utgångspunkten är att denna samverkan ska säkerställa att utvecklade krav på tillgänglighet och skydd finns med i de ramavtal och partsavtal som det offentliga använder för upphandling och avrop.

För att realisera dessa funktioner föreslås att:

- MSB bör få i uppdrag att i samverkan med Trafikverket och andra berörda aktörer, utreda funktionen för samordning och inriktning (FSI) och att utveckla en plan för att implementera den. Utgångspunkten är att FSI ska bli en

funktion för samordning av verksamheten, strategisk inriktning, stöd i kravställning, upphandling och uppföljning, samt verka för kompetenshöjning.

- Trafikverket bör få i uppdrag att i samråd med MSB, och i samverkan med andra berörda aktörer, utreda funktionen för drift och förvaltning (FDF) och att utveckla en plan för att implementera den. Utgångspunkten är att FDF ska bli en funktion för drift och förvaltning av den statliga kommunikationsinfrastruktur som avdelas för att skapa redundans hos ett begränsat antal myndigheter med särskilda behov.

Specifika skyddsåtgärder

Genom att etablera ett koncept för skyddade anslutningar till Internet för offentliga organisationer skapas en möjlighet att kombinera centralt framtagna krav på skydd med de lösningar som marknaden kan erbjuda. I förslaget har detta fått benämningen Skyddad Internetanslutning (SIA).

För att realisera detta föreslås att:

- MSB bör få i uppdrag att i samråd med Trafikverket, och i samverkan med relevanta aktörer, studera och utvärdera tekniska lösningar, administrativa och juridiska förutsättningar för, samt praktiskt införande av, Skyddad Internetanslutning (SIA). Utgångspunkten är att antalet anslutningar till Internet för offentlig sektor reduceras och förses med förstärkt skydd.

Tjänsten Skyddad Internetanslutning (SIA) för offentlig sektor bör tas fram för att kunna nyttjas av de myndigheter som finns angivna i bilagan till Krisberedskapsförordningen (KBF) samt av myndigheter med synnerliga behov. Andra offentliga organisationer kan sedan, enskilt eller tillsammans med andra, med utgångspunkt från specifikationerna för SIA handla upp tjänsten av näringslivet och då få den anpassad till deras respektive behov.

Vidare föreslås att:

- Försvarsmakten (FM) bör få i uppdrag att i samråd med MSB, och i samverkan med andra berörda aktörer utveckla och godkänna ett nationellt bredbandskrypto för offentlig sektor.

Innehållsförteckning

1. Inledning

1.1 Uppdraget

Regeringen har i regeringsbeslut 12, 2010-04-14, Fö2010/701/SSK givit Myndigheten för samhällsskydd och beredskap (MSB) ett uppdrag angående samhällets informationssäkerhet:

> *Myndigheten för samhällsskydd och beredskap ska lämna förslag på hur en säker digital informations- och kommunikationsinfrastruktur för myndigheter, kommuner och landsting kan skapas. Myndigheten för samhällsskydd och beredskap genomför uppdraget i samråd med andra aktörer bl.a. de som ingår i samverkansgruppen för informationssäkerhet, SAMFI (Försvarets radioanstalt, Försvarets materielverk, Post- och telestyrelsen, Försvarsmakten och Säkerhetspolisen), Totalförsvarets forskningsinstitut, Skatteverket samt Delegationen för e-förvaltning. Myndigheten ska i detta arbete beakta befintliga infrastrukturer, även kommersiella system samt presentera alternativa lösningar med kostnadsförslag. Erfarenheter från andra länder som gjort liknande etableringar ska inhämtas. Myndigheten ska också i samråd med Försvarsmakten och Försvarets radioanstalt analysera hur befintliga eller kommande kryptosystem i detta syfte kan nyttjas för att skydda skyddsvärd eller sekretessbelagd information.*

Uppdraget återfinns i Bilaga A.

1.2 Arbetets genomförande

MSB har genomfört uppdraget i projektform med en arbetsgrupp samt en samråds- och referensgrupp. En projektledare har hållit ihop projektet i samarbete med Enheten för samhällets informationssäkerhet.

Genom samråds- och referensgruppen har ett stort antal aktörer haft möjlighet att vara delaktiga i arbetet. Dessutom har myndigheterna inom Samverkans-gruppen för informationssäkerhet (SAMFI) löpande fått information om arbetet vid ordinarie möten.

Arbetsgruppen har regelbundet konsulterat experter och hämtat material från, myndigheter, offentliga kommittéer, näringsliv och intresseorganisationer. Dessutom har arbetsgruppen besökt Bundesamt für Sicherheit in der Informationstechnik (BSI) i Tyskland samt Cabinet Office i Storbritannien.

Projektorganisationen samt samråds- och referensgruppen beskrivs närmare i Bilaga B.

1.3 Tolkning av uppdraget

Uppdraget talar om en säker digital informations- och kommunikationsinfrastruktur. Detta skapar en bred förutsättning för att angripa frågan, jämför även med diskussionerna om ett så kallat GovNet.[1]

Efter hand har det inom arbetets ram utkristalliserats att det primära i uppdraget är att fokusera på frågan om hur det kan skapas tillgängliga och skyddade kommunikationsinfrastrukturer för offentlig sektor.

Det finns flera aspekter på säkerhet kopplad till en sådan infrastruktur. Dels måste *konfidentialiteten* och *riktigheten* hos information i kommunikationsinfrastrukturen kunna upprätthållas, dels måste det säkerställas att informationen eller kommunikationen är *tillgänglig*. För att belysa detta använder rapporten uttrycket tillgänglig och skyddad kommunikationsinfrastruktur. En annan aspekt som också lyfts fram är behovet av *kostnadseffektiva* lösningar.

Målgruppen består av myndigheter, kommuner och landsting. Det koncept som föreslås i rapporten kallas därför *tillgängliga och skyddade kommunikationsinfrastrukturer för offentlig sektor*.

Myndighetsinterna lösningar behandlas inte direkt i rapporten, utgångspunkten är att ansvarsprincipen gäller. Myndigheter kan komma att påverkas i form av ackrediteringskrav. Rapporten fokuserar på att skapa gemensamma administrativa rutiner, exempelvis kravspecifikationer och uppföljning, som kan nyttjas av offentlig sektor. Rapporten fokuserar också på att i vissa avseende skapa gemensamma tekniska infrastrukturer. Det kan exempelvis handla om skyddade Internetanslutningar. Det övergripande syftet är att kunna erbjuda offentlig sektor tillgängliga och skyddade kommunikationsinfrastrukturer.

Vid prioritering av de tjänster som ska forma basen för kommunikationsinfrastrukturerna har MSB utgått från prioriterade strategiska e-förvaltningsprojekt och den utveckling som leder mot att myndigheters kommunikation med näringsliv och medborgare i allt högra grad sker baserade på e-post, webbformulär eller olika typer av filöverföring. Tjänster som telefoni och videokonferenser behandlas inte specifikt i denna rapport men kan inkluderas inom ramen för föreslaget koncept.

I rapporten behandlas inte infrastrukturer som är avskilda från det globala Internet, uppfattas som myndighetsinterna resurser, eller inte utgör en betydande komponent i kommunikation mellan myndigheter och

---

1 *Åtgärder för att förbättra samhällets samlade förmåga att förebygga och hantera IT-incidenter*. MSB:s svar på regeringens uppdrag Fö2009/2162/SSK, 2010.

näringsliv/medborgare eller en kombination av dessa. Exempel på sådan infrastruktur är Försvarsmaktens IP-nät (FMIP) och RAKEL.

Med ovanstående som utgångspunkt har uppdraget haft följande målbild:

> För att hantera existerande och framtida krav på digital kommunikation i en global miljö med komplex risk- och hotbild ska offentlig sektor erbjudas tillgängliga, skyddade och kostnadseffektiva kommunikationstjänster.

1.4 Läsanvisning

Rapporten innehåller förslag på en samlad verksamhet med ett övergripande ansvar för att vidmakthålla och utveckla tillgängliga och skyddade kommunikationsinfrastrukturer för offentlig sektor.

Rapporten är uppdelad i sex kapitel. I kapitel ett beskrivs uppdraget, MSB:s tolkning av uppdraget och arbetets genomförande. I kapitel två redogörs för de utmaningar som den digitala miljön innebär för ett arbete med att skapa tillgängliga och skyddade kommunikationsinfrastrukturer. Kapitel tre beskriver de utgångspunkter som är av grundläggande betydelse för förslaget på hur tillgängliga och skyddade kommunikationsinfrastrukturer för offentlig sektor bör skapas. I kapitel fyra förs inledningsvis ett resonemang kring olika alternativa sätt att skapa tillgängliga och skyddade kommunikationsinfrastrukturer. Kapitlet avslutas med en närmare analys av vilken väg som bör väljas. I kapitel fem presenteras rapportens förslag och här föreslår MSB hur arbetet bör drivas vidare. Avslutningsvis behandlar kapitel sex förslagets kostnader.

I bilagorna finns ytterligare bakgrundsmaterial.

Bilaga A: Regeringsuppdraget
Bilaga B: Uppdragets organisation
Bilaga C: Förkortningar och begrepp
Bilaga D: Myndigheter som är utpekade i bilagan till KBF
Bilaga E: Infrastruktur i Sverige

2. Utgångspunkter och utmaningar

2.1 En utvecklad e-förvaltning ställer krav

Sedan något decennium är det grundläggande för svenska myndigheter att kunna skapa och utbyta digital information i allt större omfattning. Kännetecknande för den digitala utvecklingen är att förändringarna sker i en stegvis upptrappning från lokala lösningar till mer gemensamma lösningar. För den svenska e-förvaltningen blir det allt mer tydligt att lokala lösningar inte är tillräckliga vare sig för funktion eller för säkerhet.

Varje myndighet ska enligt lag och förordning eftersträva hög effektivitet och god hushållning av statens medel i sin verksamhet. Enligt myndighetsförordningen ska myndigheten också utveckla verksamheten och verka för att genom samarbete med myndigheter och andra ta till vara de fördelar som kan vinnas för enskilda samt för staten som helhet. Omvärldens förändringar skapar dessutom ett starkt tryck på statsförvaltningen och med den stora effektiviseringskrav.[2]

E-delegationen verkar för att ta fram underlag för gemensamma lösningar där en väsentlig utgångspunkt är att se statlig förvaltning som en helhet. Efter hand som e-förvaltningen slår igenom kommer vissa myndigheter att behöva elektroniskt förmedla stora mängder känslig information sinsemellan. Detta ställer inte bara krav på konfidentialitet och sekretess, utan även krav på tillgänglighet och riktighet.[3]

Hela offentliga sektorn är en del av e-förvaltningen men behoven skiljer sig mellan offentliga aktörer. För centrala myndigheter finns likheter, men också skillnader allt utifrån myndigheternas olika verksamheter och uppgifter. På regional och lokal nivå finns breda kontaktytor mot medborgarna och exempelvis till privata vård- och omsorgsföretag, som arbetar på landstingens och kommunernas uppdrag. Nationell e-hälsa, det vill säga de tjänster och system som finns för hantering av patientinformation, utgör också exempel på en av kravställarna för en tillgänglig och skyddad kommunikationslösning.

E-delegationens arbete sätter fokus på kommunikationsfrågorna och föreslår att elektroniskt informationsutbyte mellan myndigheter ska baseras på standardiserad meddelandehantering. Delegationen konstaterar att organisationer inom offentlig sektor har olika uppfattning om vad en e-tjänst är och vad teknisk samverkansförmåga innebär. Det har resulterat i olika

2 *IT inom statlig förvaltning – har myndigheterna på ett rimligt sätt prövat om outsourcing bidrar till ökad effektivitet?* RiR 2011:4, Riksrevisionen, 2011.

3 *Strategi för myndigheternas arbete med e-förvaltning.* Betänkande av E-delegationen , SOU 2009:86.

lösningar som i sin tur medför svårigheter att integrera e-tjänster och lösningar.

Enligt delegationen bör offentlig sektor se till att olika arkitekturer kan samverka utan krav på större investeringar i en gemensam arkitektur. Interaktion mellan oberoende parter kräver tydlig ansvarsfördelning och val av kommunikationssätt. För att säkerställa att ett informationsutbyte sker på ett standardiserat och teknikoberoende sätt föreslår delegationen att informationsöverföring mellan myndigheter ska baseras på standardiserad meddelandehantering.[4] Myndigheterna behöver en grundläggande infrastruktur där utgångspunkten är att samverkan ska kunna ske mellan oberoende enheter.

Interaktion mellan oberoende parter kräver tydlig ansvarsfördelning och val av kommunikationssätt. Delegationen pekar även på behovet av att se till statens samlade nytta, det vill säga. Att offentliga aktörer bör anlägga ett koncern-gemensamt perspektiv när de koordinerar och följer upp arbetet med gemensamma administrativa stöd.[5]

Regeringens intentioner med e-delegationens arbete förutsätter till stora delar ett mer *samordnat synsätt* i offentlig sektor, vilket framgår av delegationens betänkande. Synsättet är på många sätt tillämpbart och i flera fall en förut-sättning för att skapa tillgängliga och skyddade kommunikationsinfra-strukturer. Synsättet ligger också till grund för flera av rapportens förslag.

2.2 Den över tiden föränderliga hot- och riskbilden

Samhället har på senare år blivit alltmer IT-beroende – ett beroende som i dag omfattar alla samhällssektorer. IT-incidenter kan i dag hota kritisk infra-struktur, samhällsviktiga verksamheter och ytterst Sveriges säkerhet. Samhället behöver därför lägga resurser på att förebygga och hantera IT-incidenter på ett helt annat sätt än tidigare.

Den digitala informations- och kommunikationsinfrastrukturen är föränderlig när det gäller teknik, organisation, metoder och kompetens. Det ställer särskilda krav på säkerhet och nationell IT-incidenthanteringsförmåga. Hoten, riskerna och sårbarheten ökar, men förmågan att hantera dessa ökar inte i samma takt. De flesta IT-incidenter är inte ett resultat av brottsligt uppsåt, utan uppstår på grund av bristande kompetens, misstag, felaktig användar-dokumentation eller liknande. En del incidenter beror på tekniska samman-brott och naturhändelser. Men de antagonistiska hoten går inte att bortse ifrån; informationssystem utsätts regelbundet för angrepp.

---

4 *Strategi för myndigheternas arbete med e-förvaltning*. SOU 2009:86. Sid. 68f

5 *Strategi för myndigheternas arbete med e-förvaltning*. SOU 2009:86. Sid. 81

En växande krets av statliga och icke-statliga aktörer – till exempel främmande underrättelsetjänster, kriminella grupper och terroristgrupper – har skaffat sig förmåga att komma över, stjäla, förändra och förstöra information. Aktörerna riktar sitt intresse mot hela skalan av tänkbara mål: från enskilda medborgare och affärsverksamheter till kritisk infrastruktur och samhällsviktig verksamhet. Hoten mot den globala digitala informations- och kommunikationsinfrastrukturen tillhör de allvarligaste ekonomiska och säkerhetsmässiga utmaningar som samhället står inför i dag. [6]

Ur ett samhällsövergripande perspektiv handlar det om att värna stabiliteten hos en mängd samhällsfunktioner som är beroende av fungerande IT-stöd. Det finns emellertid vissa samhällsområden där stabilitet är extra viktigt. Till dem hör den elektroniska kommunikationsinfrastrukturen, eftersom den utgör en förutsättning för att olika myndigheter och andra aktörer ska kunna kommunicera sinsemellan. Dessaska också kunna tillhandahålla vissa grundläggande samhällstjänster även under störda förhållanden.

2.3 Den digitala marknaden

2.3.1 Konkurrens och beroenden

Konkurrensen i kombination med teknikutvecklingen har lett till ett brett tjänsteutbud och lägre priser. Ytterligare en följd är att operatörerna rationaliserar och minimerar sina investerings- och driftkostnader. Dessa sänks inte sällan på bekostnad av tillförlitlighet, uthållighet och säkerhet.[7] I det stora utbudet finns således skillnader på kvalitet, säkerhet och tillgänglighet, skillnader som inte alltid är tydliga för kunderna. Lagstiftaren skärpte 2005 kraven på säkerhet genom att införa en regel i lagen (2003:389) om elektronisk kommunikation. Regeln innebär att den som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster ska se till att verksamheten uppfyller rimliga krav på god funktion och teknisk säkerhet samt på uthållighet och tillgänglighet vid extraordinära händelser i fredstid.[8]

Det är få operatörer i dag som ensamma har egen teknisk kompetens och egna resurser för att driva elektronisk kommunikation i alla led. Flera leverantörer är specialiserade på en viss typ av verksamhet, vilket skapar beroenden både till andra operatörer och till underleverantörer. Olika operatörer har olika förutsättningar att uppnå god funktion och teknisk säkerhet. Det påverkar i sin tur operatörernas förmåga att identifiera och hantera olika typer av felsituationer. Av användarna krävs inte bara insikt i hur det egna behovet av tillgänglighet

6 *Åtgärder för att förbättra samhällets samlade förmåga att förebygga och hantera IT-incidenter*. MSB:s svar på regeringens uppdrag Fö2009/2162/SSK, 2010.

7 *Klarar vi krisen? Samhällets krisberedskapsförmåga 2007*. KBM:s temaserie 2008: 2, Krisberedskapsmyndigheten (KBM).

8 6a § 5 kap lag (2003:389) om elektronisk kommunikation

och skydd ser ut, utan även god kunskap om marknaden och de olika operatörernas förmåga att uppfylla identifierade behov.

2.3.2 Kommunikationsarkitektur

All användning av elektroniska tjänster och elektronisk kommunikation bygger på en kommunikationsarkitektur. Kommunikationsarkitekturen kan betraktas som en värdekedja med olika nivåer. Varje nivå har olika aktörer med olika roller. I vissa fall har en och samma aktör ansvar för flera nivåer i värdekedjan. De olika aktörernas och tjänsteleverantörernas relationer till varandra varierar. I de flesta fall finns inga kopplingar alls, men i vissa fall råder avtalsförhållanden, till exempel vid hyra av ledning eller transmissionskapacitet. Varje tjänsteleverantör har för de olika tjänsterna olika tekniska lösningar och teknisk utrustning. Varken nätägare, transmissionsleverantörer eller Internetoperatörer (på de lägre nivåerna i värdekedjan) har någon möjlighet till insyn i eller kontroll över vad som sker på tjänstenivån.

För att arkitekturen ska bli robust måste varje lager utformas så att risken för problem minimeras inom respektive lager. Riskerna måste naturligtvis vägas mot kostnaderna för att göra just den delen i arkitekturen robust.

2.4 Offentlig sektor som kravställare

En ökad medvetenhet om informationens värde och krav på skydd finns i samhället i stort och hos de myndigheter som utgör en del av e-förvaltningen. Säkerhet har identifierats som en förutsättning både för att lyckas med de krav som finns från statsmakten och medborgare på att utveckla en e-förvaltning men också för att nå de fördelar som e-tjänster kan innebära för den enskilda myndigheten. En fungerande säkerhet är en av förutsättningarna för förbättrad service och för effektivare förvaltning med möjlighet till ekonomisk rationalisering. För de statliga myndigheterna gäller också MSB:s föreskrift om att följa informationssäkerhetsstandarden ISO 27001, vilket även många landsting och kommuner gör på frivillig basis.

Om den offentliga sektorn ska kunna tillgodogöra sig de fördelar som marknaden erbjuder, måste den kunna kravställa och upphandla på ett adekvat sätt. Skydds- och tillgänglighetsaspekter måste få en central roll i kravställningen såväl vid ramavtalsupphandling som vid enskilda aktörers upphandlingar. Den offentliga sektorn kan här utveckla sin potential som kravställare genom att utforma sina krav så att de på ett mer direkt sätt kan nyttjas av fler offentliga aktörer. Det som inledningsvis kan upplevas som en extra kostnad kan på sikt visa sig vara kostnadseffektivt såväl för enskilda myndigheter som för samhället. Avbrott i vissa myndigheters system kan få oanade säkerhets- och kostnadseffekter såväl för samhället som för enskilda medborgare. Hur stora dessa effekter blir är svårt att uppskatta i förväg då omfattningen beror på störningarnas art och på vem som blir utsatt för störningarna.

Det är centralt att bägge parter, såväl leverantör som användare, är överens om vilken vara eller tjänst som utbjudits och vad som regleras i det upprättade avtalet. Ett ökat utbud innebär att riskerna för missförstånd ökar, exempelvis rörande tjänstens utlovade kvalitet. Men ett ökat utbud har också fördelar. Mångfalden av operatörer gör att det finns möjlighet för myndigheterna att sprida riskerna genom att använda fler operatörer. På så sätt kan ökad tillgänglighet och redundans byggas upp.

Det faktum att alltmer av den kritiska infrastrukturen i huvudsak är privatägd påverkar statens möjligheter att reglera informationssäkerhetsnivå och tillgänglighet i operatörernas infrastrukturer.

Det stora och ständigt ökande beroendet av kommunikationsinfrastruktur har också kopplingar till säkerhetsskydd. Infrastrukturen är idag global. Att vara beroende av operatörer, många gånger med system placerade utanför landets gränser, kräver särskilda överväganden. Utvecklingen mot outsourcing och molntjänster bör särskilt uppmärksammas.

Svenska myndigheter riskerar i en sådan situation att få en sämre kontroll över samhällsviktig verksamhet och samhällsviktiga system. Rättslig reglering kan i vissa fall även utgöra hinder för vissa lösningar.[9]

Säkerhetsskyddslagstiftningen är tillämplig om verksamheten är av betydelse för rikets säkerhet eller om den behöver särskilt skydd mot terrorism. Det är väsentligt att vissa verksamheter köper tjänster av en operatör som långsiktigt kan uppfylla kraven på att anläggningar och funktioner av betydelse ska finnas i Sverige. Det gäller

- verksamheter som behöver tillgänglig skyddad elektronisk kommunikation ur ett krishanteringsperspektiv
- verksamheter som är av betydelse för rikets säkerhet
- verksamheter som behöver skydd mot terrorism.

2.5 Några internationella erfarenheter

Under de senaste åren har många nationer arbetat alltmer aktivt med informationssäkerhet. Allt fler länder skapar övergripande strukturer för koordinering och samverkan samt samlar omfattande kompetenser och resurser. Ett antal länder har till exempel skapat nya centrala samhälls-övergripande samverkansfunktioner för att koordinera den nationella hanteringen av IT-incidenter och i viss mån koordinera tillgänglig och skyddad kommunikation. Andra länder står i begrepp att bygga upp sådana funktioner.

9 Se exempelvis Bokföringslag (1999:1078)

Flera nationella strategier betonar att det behövs ökad privat-offentlig samverkan, nationella kampanjer för att öka medvetande på alla nivåer i samhället och en tydlig säkerhetskultur. Andra teman som återkommer är behovet av mer internationell samverkan och informationsdelning, kompetenshöjning, samt ett tydligt nationellt ledarskap.

Storbritannien skapade för 15 år sedan sitt första nätverk med skyddade Internetanslutningar. Det omfattade då en liten del av den statliga centrala administrationen. Nätverkslösningarna har därefter successivt utvecklats. Myndigheterna driver nu nya projekt för att omvandla några få stora nät till ett flertal mindre nät. Det nya projektet bedöms ge omfattande kostnadsreduceringar för offentlig sektor.

Tyskland gjorde omfattande investeringar i nätverk med skyddade Internetanslutningar för federala myndigheter 2006–2008. Nu inleds nästa steg, en utveckling av konceptet Netze des Bundes, med syfte att skapa en gemensam infrastruktur för den federala administrationen.

Storbritannien och Tyskland bedömer att det finns ett stort hot mot IT-infrastrukturen, och antalet attacker och faktiska intrång belägger detta. Trots skyddsåtgärderna räknar bägge länderna med intrång i sina skyddade nät. Därför satsar de också resurser på tekniska kontrollsystem för att upptäcka intrång och för att följa aktiviteten i nätverken. Som en följd av det upplevda hotet har bägge länderna strikta regler för trådlösa anslutningar för de centrala myndigheterna med auktorisation och kryptering (VPN). En grundläggande strategi i båda länderna är att minska antalet anslutningspunkter till Internet och att öka kapaciteten och skyddet i de kvarvarande.

I Tyskland har Deutsche Telekom en särställning som leverantör. I Storbritannien drivs nätverken av några få operatörer som myndigheterna anser vara kontrollerbara och säkerhetsmässigt acceptabla. Det nya brittiska projektet syftar till lösningar där flera operatörer som uppfyller specificerade krav inbjuds som leverantörer till något av de skyddade näten. Det främjar konkurrensen för leverantörer till de offentliga nätverken.

Arbetsgruppen har också studerat dokumentation om strategier för cybersäkerhet från Australien och Kanada. Grundsynen på hot och risker liknar den i Tyskland och Storbritannien. Dokumenten betonar vikten av tålighet (resilience) och skydd. Hoten anses vara allvarliga och växande. Antalet anslutningspunkter mot Internet kommer att reduceras. I Australien anges att antalet anslutningspunkter i den federala administrationen ska reduceras från 100 till 10. Dessa anslutningar ska placeras hos tio utvalda myndigheter som får ytterligare resurser för att skydda dem. En bieffekt är att de totala kostnaderna därmed bedöms kunna minska.

I Finland har staten skapat en gemensam kommunikationslösning för statsförvaltningen (VY-verkko). Genom nätverket kan anslutna myndigheter kommunicera med varandra och med omvärlden genom en central kopplingsfunktion. Statens mål med VY-verkko är bland annat att minska statens totala

kostnader för IKT-lösningar, höja servicenivån för användarna samt att öka skyddet för myndigheternas kommunikation. Myndigheter har kunnat ansluta sig till nätverket från och med hösten 2010. Målet är att merparten av statsförvaltningen ska vara ansluten till och med 2014.

3. Vägval

3.1 Tillgänglighet och skydd

3.1.1 En tillgänglig och skyddad infrastruktur i normalläge och kris

Samhällsutvecklingen har på några decennier gjort IT-systemen till en naturlig och nödvändig del av vår vardag. Men utvecklingen har även medfört nya hot och risker. Informationssäkerheten måste hålla jämna steg med IT-utvecklingen för att fördelarna med IT ska kunna nyttjas till sin fulla potential.

I det svenska samhället behövs det administrativa och tekniska infrastrukturer för informationsdelning och respons i vid mening – där samtliga aktörer av betydelse för samhällets kritiska informationsinfrastrukturer finns representerade. Infrastrukturerna ska fungera under normala förhållanden, men ska också innefatta en organisation som kan fungera som stöd under allvarliga störningar och kriser. Stödorganisationer och infrastrukturer måste självfallet ha hög informationssäkerhet, så att de inte slås ut vid allvarliga störningar. För att bli kostnadseffektiva och för att på bästa sätt ta vara på befintlig kompetens och organisation bör infrastrukturerna bygga på nuvarande strukturer.

En övergång från normalläge till krisläge ska inte innebära stora förändringar vad gäller aktörer och arbetssätt, eftersom det försvårar och fördröjer arbetet i en redan pressad situation. En infrastruktur som specifikt är till för krishantering skapar en situation där omställningen från normal verksamhet till krishantering blir så stor att det allvarligt påverkar verksamheten. En sådan lösning bör därför undvikas. Infrastrukturerna måste även kunna vara flexibla och erbjuda olika nivåer av tillgänglighet och skydd som svarar mot de olika aktörernas behov.

3.1.2 Robusthet och tillgänglighet

I takt med att samhället blir alltmer beroende av modern teknik, minskar toleransen för avbrott och andra störningar. Efter hand som *e-förvaltningen* etableras får vissa myndigheter dessutom allt större behov av att elektroniskt förmedla stora mängder information sinsemellan. Detta ökar kraven på tillgängliga och skyddade kommunikationsinfrastrukturer samt förändrade administrativa rutiner. Samtidigt blir utbudet av elektronisk kommunikation alltmer omfattande.

Det finns olika incitament för att öka tillgängligheten i elektronisk kommunikation. Operatörerna investerar i dag i tillgänglighet av kommersiella skäl. Det är kundernas krav och kundernas vilja att betala som styr dessa investeringar. Utöver operatörernas investeringar har staten, genom PTS, under många år investerat för att göra de publika näten mer robusta, samt i olika samverkansprojekt. Exempel på åtgärder är fysiskt skyddade knutpunkter, fysiskt redundanta förbindelser, reservelverk, transportabla mobilbasstationer, system

för robust och spårbar tid, informationssystem vid driftstörningar, informationssystem för att reducera antalet avgrävningar med mera.

Att åstadkomma robusthet genom upphandling har visat sig vara ett effektivt sätt för staten att nå resultat i en konkurrensutsatt marknad. Denna privat-offentliga samverkan har skapat en god grund att bygga vidare på. Arbetet med framtida tillgängliga och skyddade kommunikationsinfrastrukturer bör kunna bidra till att vidareutveckla arbetet med robusthet och tillgänglighet.

3.1.3 Anslutning till Internet

Anslutningsformen till näten är en viktig förutsättning för tillgänglighet. Här kan användarna dra nytta av mångfalden av operatörer – Om offentlig sektor nyttjar resurser från flera operatörer ökar möjligheterna att förbättra tillgängligheten genom upphandling. Men samtidigt ökar också riskerna för att något blir fel. Olika operatörer har olika förutsättningar att uppnå god funktion och teknisk säkerhet, vilket i sin tur kräver goda kunskaper vid upphandling. Myndigheter, kommuner och landsting måste låta resultatet av risk- och sårbarhetsanalyser få genomslag när de upphandlar IKT-lösningar.

Skyddet för myndigheter, kommuner och landsting varierar utifrån respektive aktörs investeringar. Vissa aktörer har satsat omfattande resurser på att skapa skyddade Internetanslutningar – andra har inte dessa resurser. Det innebär att det i offentlig sektor finns många olika lösningar för val av Internetleverantör och för den rent tekniska anslutningen till Internet. Antalet anslutningar till offentlig sektor uppskattas till mer än 600.

Det finns skäl att anta att skyddet kan förbättras om antalet anslutningar reduceras. Strävan bör därför vara att reducera antalet anslutningar samt att optimera skyddet av de kvarvarande anslutningarna.

3.1.4 Skyddad kommunikation

All digital kommunikation är i grunden osäker. Normalt överförs information över näten i klartext. Det är en flexibel lösning, som samtidigt gör det möjligt att till exempel avlyssna kommunikation, sända information i andras namn samt förvanska information. En metod för att skydda information är att använda kryptering. En säker nätkommunikation kräver flera olika sorters kryptografiska funktioner på flera olika nivåer. Kryptografiska funktioner kan användas för att uppnå konfidentialitet. Genom att endast den som har tillgång till ett visst kryptosystem har möjlighet att tyda eller förändra den information som skyddas av systemet. I många fall används kryptografiska funktioner enbart för att skapa elektroniska signaturer och för att identifiera komponenter och användare på ett säkert sätt. Genom elektroniska signaturer kan en avsändare av elektronisk information säkert identifieras och det går inte att

förvanska information utan att detta upptäcks. När det finns elektroniska signaturer kan en avsändare inte förneka en transaktion eller en handling.[10]

I en skyddad kommunikationsinfrastruktur är det viktigt att det finns möjlighet att använda nationellt godkända kryptosystem om kraven på skydd motiverar detta. Den som vill vara säker på att en kryptografisk funktion eller ett krypto-system fungerar på avsett sätt måste granska dessa. I de fall en kommersiell kryptolösning ska användas måste granskaren ha kompetens för denna uppgift samt förtroende från uppdragsgivaren. De svenska myndigheter som har kvalificerad kunskap och kompetens inom kryptoområdet är Försvarsmakten och Försvarets radioanstalt. Försvarsmakten har i uppgift att säkerhetsgranska kryptosystem för att därefter ge dem ett nationellt godkännande.

Det kryptosystem som för de flesta är mest lämpat som grundskydd i skyddad kommunikationsinfrastruktur är VPN-krypto (Virtual Private Network). Med hjälp av detta kan säkra privata förbindelser skapas över ett publikt nätverk som Internet. Förbindelserna krypteras över logiska anslutningar, eller virtuella kretsar, mellan värdar (noder) i ett större nätverk – informationen ”tunnlas” genom det logiska nätet.

Arbetet med en tillgänglig och skyddad kommunikationsinfrastruktur bör därför innefatta utveckling av ett nationellt godkänt kryptosystem.

3.1.5 Utbildning och administrativa rutiner

För att kommunikationen ska vara tillgänglig och skyddad måste personalen vara rätt utbildad och ständigt uppdaterad på området informations- och kommunikationsteknologi, IKT. Personalen måste kunna konfigurera hårdvara och mjukvara i anslutningen till Internet. Utbildningsnivån varierar stort, även inom offentlig sektor, vilket kan leda till brister i hanteringen av utrustning och i tillämpningen av den tekniska utvecklingen.

Utöver behovet av en tillgänglig och skyddad kommunikationsinfrastruktur krävs väl fungerande administrativa rutiner. Rutinerna bör vara anpassade för de olika myndigheternas behov.

Alla aktörer i offentlig sektor behöver inte ha samma höga krav vad gäller tillgänglighet och skydd. Vidare behöver inte alla aktörer ha tillgång till alla funktioner i infrastrukturerna. Med en sådan uppdelning kan staten undvika omfattande och kostnadskrävande lösningar.

3.2 Resursanvändning

De kommunikationsbehov som finns mellan myndigheter, kommuner och landsting, till vardags och i krissituationer, påverkas av en snabb, global teknisk och verksamhetsmässig utveckling. Kommunikationsbehoven påverkas

10 *Bredband för tillväxt i hela landet*. Betänkande från IT-infrastrukturutredningen, SOU 1999:85.

även av att kommunikationen med medborgare och näringsliv ändrar karaktär. Såväl hotbild som krav på servicenivå förändras över tiden och det måste hela tiden finnas en balans mellan tillgänglighet och skydd. I rapporten beaktas såväl statliga som kommersiella resurser och kombinerar dessa för att finna kostnadseffektiva lösningar.

I Sverige finns förutsättningar för att skapa tillgängliga och skyddade kommunikationsinfrastrukturer som även fungerar under störningar. I det svenska samhället finns redan många av de nödvändiga kompetenser och resurser som behövs för att skapa ett system som kan möta detta behov och som är hållbart över tiden. Stora delar av resurserna finns tillgängliga i näringslivet medan andra delar återfinns i den offentliga sektorn. De samlade resurserna behöver dock kompletteras, i viss mån samordnas och delvis omorganiseras för att de ska bli ändamålsenliga, tillgängliga och rätt dimensionerade.

Regeringens digitala agenda pekar på att det bör gå att nyttja statens resurser bättre genom en sammanhållen strategi. Den digitala agendan ska vara ett komplement till pågående insatser. Den ska samordna åtgärder inom IT-området som till exempel säkerhet, infrastruktur, kompetensförsörjning, tillit, tillgänglighet, användbarhet, standarder, entreprenörskap och innovation.

Att inte agera gemensamt inom offentlig sektor leder till att nuvarande fragmenterade arbetssätt cementeras. Riskerna blir svåra att överblicka. Småskaliga lösningar blir divergerande och kostnadsdrivande vilket inte ligger i linje med den digitala agendan som syftar till en effektiv användning av offentliga IT-resurser.

För att undvika angrepp och för att se till att kommunikationen fungerar under kriser kan flera myndigheter behöva skydda informationen om sina kommunikationsinfrastrukturer. Om sådan information blir tillgänglig för obehöriga kan det allvarligt försvåra krishanteringsarbetet.

Staten äger i dag i viss fysisk kommunikationsinfrastruktur, en resurs som fullt ut går att kontrollera. Den har identifierats som strategisk för vissa myndigheters verksamhet.

3.3 Rättsliga frågor

3.3.1 Inledning

Arbetet med att skapa en skyddad och tillgänglig kommunikationsinfrastruktur för offentlig sektor aktualiserar en rad juridiska överväganden. Dessa är kopplade till informationshanteringen inom infrastrukturen, men även till det rättsliga ramverk som ska stödja offentlig sektors användning av informationshanteringen.

3.3.2 Informationshantering

När det gäller informationshantering bör lagar som personuppgiftslagen (1998:204) samt offentlighet- och sekretesslagen (2009:400) särskilt beaktas. Tillgängliga och skyddade kommunikationsinfrastrukturer kan exempelvis innebära att offentlig sektor får tillgång till gemensamma lösningar när det gäller skydd av typen brandväggar, loggningsfunktioner och liknande. I anslutning till att sådana lösningar utformas bör rättsliga frågor diskuteras, som hur personuppgiftsansvaret ser ut för informationen som hanteras i det gemensamma skyddet och vem som bör hantera frågor om utlämnande av uppgifter. Även andra regelverk bör analyseras närmare, exempelvis lag (2003:389) om elektronisk kommunikation.

Tillgängliga och skyddade kommunikationsinfrastrukturer kan också innebära att det blir enklare att uppfylla de krav som redan idag ställs på informationshantering och informationsutbyte i offentlig sektor.
Säkerhetsskyddslagstiftningen syftar till att skydda verksamheter av betydelse för rikets säkerhet och samt ge skydd mot terrorism.[11] Det är väsentligt att sådana verksamheter har tillgång till en infrastruktur som kontrolleras av en operatör som långsiktigt kan uppfylla kraven på att anläggningar och funktioner av betydelse ska finnas i Sverige.

3.3.3 Ett rättsligt ramverk

En skyddad och tillgänglig kommunikationsinfrastruktur förutsätter i många delar att det finns ett rättsligt ramverk som stöd för aktörerna. Även om detta ramverk bygger på och utnyttjar befintlig rättslig struktur kan det finnas områden där författningsändringar eller författningstillägg blir nödvändiga.

Även andra rättsliga frågor bör utredas närmare. Hur avtal med operatörer och leverantörer utformas är av stor betydelse för att tillgängliga och skyddade kommunikationsinfrastrukturer ska kunna erbjuda den funktionalitet som beskrivs här. Vidare är det centralt att närmare utreda formerna för uppföljning och stöd till de anslutna offentliga aktörerna. Detta påverkar bland annat formerna för abonnemangen och tillgången till kryptolösningar för skyddsvärd information.

11 Säkerhetsskyddslag (1996:627)

4. Alternativa lösningar

4.1 Målbild och särskilda krav

Målbilden för uppdraget är att offentlig sektor ska kunna erbjudas tillgängliga, skyddade och kostnadseffektiva kommunikationstjänster. Den föreslagna lösningen ska kunna hantera existerande och framtida krav i en global miljö med komplex risk- och hotbild. Mot bakgrund av de diskussioner som förts i kapitel 2 och 3, och målbilden, betonas att lösning

- ska vara kostnadseffektiv
- måste vara flexibel för att kunna hantera en snabb teknisk utveckling på global nivå
- ska utnyttja existerande infrastrukturer så långt som det är möjligt och ta tillvara den samlade kompetens som finns i samhället
- ska kunna erbjuda olika nivåer av tillgänglighet och skydd som svarar mot de olika aktörernas behov
- ska säkerställa en ändamålsenlig administrativ styrning och ett långsiktigt åtagande
- ska kunna erbjuda tillgängliga och skyddade kommunikationsinfrastrukturer som fungerar både under kris och normaltillstånd
- ska garantera ett långsiktigt och ändamålsenligt arbete med tillgänglighet och skydd
- för vissa myndigheter ska kunna erbjuda tjänster som nyttjar en statligt kontrollerbar infrastruktur med hög säkerhetsnivå
- ska bygga på ett ramverk som även hanterar de rättsliga aspekterna.

4.2 Alternativa lösningar

I detta avsnitt presenteras tre alternativa lösningar för att skapa tillgängliga och skyddade kommunikationsinfrastrukturer för offentlig sektor. Under arbetet har, som nämnts ovan, ett brett spektrum av aktuella och framtida behov beaktats. Internationella och nationella erfarenheter har även analyserats. Följande alternativ har analyserats i arbetet med uppdraget:

1. Det första alternativet är att av en kommersiell operatör upphandla ett fysiskt och logiskt nät för myndigheter, kommuner och landsting.
2. Det andra alternativet är att nyttja statliga resurser, samt komplettera med upphandling från näringslivet, för att skapa ett fysiskt och logiskt nät för myndigheter, kommuner och landsting.

3. Det tredje alternativet är att gemensamt utveckla och sprida kompetens för kravställning och upphandling, samt att nyttja resurser från offentlig sektor och näringsliv på ett koordinerat sätt.

De olika förslagen skiljer sig främst vad gäller antalet aktörer samt i vilken utsträckning privata respektive statliga infrastrukturer används. Upphandling är ett viktigt instrument i samtliga alternativ.

4.3 Analys av de olika alternativen

Några grundfrågor är särskilt viktiga vid analysen av de olika alternativen och måste besvaras. För det första är det centralt att kraven på tillgänglighet och skydd kan uppfyllas samt erbjudas till anslutna aktörer på ett flexibelt sätt. Efter hand som e-förvaltningen etableras får vissa myndigheter allt större behov av att elektroniskt förmedla stora mängder information sinsemellan. Detta ökar kraven på tillgängliga och skyddade kommunikationsinfrastrukturer samt ändamålsenliga administrativa rutiner.

Frågan om hur kommunikationsinfrastrukturerna hanteras i normalläge respektive krissituation är kopplad till både tillgänglighet och skydd. En lösning som innebär att omställningen i infrastrukturen från normal verksamhet till krishantering blir så stor att det allvarligt påverkar verksamheten bör undvikas. En övergång från normalläge till krisläge ska inte medföra stora förändringar för aktörer och arbetssätt, eftersom det försvårar och fördröjer krishanteringen.

Samtliga tre alternativ torde kunna garantera tillräcklig tillgänglighet och skydd, både i normalläge och vid kris. Detta är i hög grad beroende på hur styrmedlen nyttjas. En förutsättning för samtliga alternativ är en förståelse för risk- och hotbild samt tekniska och administrativa möjligheter. Till detta måste läggas en god förmåga att omvandla denna förståelse till upphandlingskrav.

Säkerhetsskyddslagstiftningen gäller sådan verksamhet som är av betydelse för rikets säkerhet eller som särskilt behöver skyddas mot terrorism.[12] Det är väsentligt att sådana verksamheter har tillgång till en infrastruktur som kontrolleras av en operatör som långsiktigt kan uppfylla kraven på att anläggningar och funktioner av betydelse ska finnas i Sverige. I praktiken handlar det om sådan infrastruktur som staten kontrollerar. Vid en analys av de olika alternativen visar det sig att alternativ ett uppvisar brister vad gäller de direkta möjligheterna att säkerställa kraven kopplade till säkerhetsskyddet eftersom det går ut på att upphandla ett fysiskt och logiskt nät av en kommersiell aktör. Den del av infrastrukturen som staten tillhandahåller blir härigenom inte tillgänglig. De båda andra alternativen, alternativ 2 och 3,

12 1 § Säkerhetsskyddslagen (1996:627)

innebär inte några sådana begränsningar utan är därför lämpligare vid beaktandet av säkerhetsskyddsaspekter.

De kommunikationsbehov som finns mellan myndigheter, kommuner och landsting, till vardags och i krissituationer påverkas av en snabb global utveckling – både tekniskt och verksamhetsmässigt. Kommunikationsbehoven påverkas även av att kommunikationen med medborgare och näringsliv ändrar karaktär. Såväl risk- och hotbild som krav på servicenivå förändras över tiden.

Att tillhandahålla service i hela värdekedjan klarar enbart några av de dominerande operatörerna med egna nät. Mindre operatörer får svårt att vara med och erbjuda sina tjänster. Det saknas en fullt utvecklad marknad inom detta område och det finns risk att genomförda upphandlingar cementeras till nackdel för den offentliga sektorn och för hela marknaden. Att använda tjänsteutbudet i vidare mening vidgar däremot marknaden till en mer utvecklad konkurrens. Det gynnar såväl offentlig sektor som marknaden i sin helhet.

Kostnadsaspekterna är centrala och här är ett ökat samarbete mellan de offentliga aktörerna önskvärt, något som även är uttryckt i den digitala agendan. Detta har också betonats i samband med utvecklingen inom e-förvaltningsområdet. Att inte agera gemensamt inom offentlig sektor leder till att nuvarande fragmenterade arbetssätt cementeras. Riskerna blir svåra att överblicka. Småskaliga lösningar blir divergerande och kostnadsdrivande vilket inte ligger i linje med den digitala agendan som syftar till en effektiv användning av offentliga IT-resurser.

Det är centralt att det valda alternativet ger goda möjligheter att hantera den tekniska utvecklingen på ett ändamålsenligt sätt och att så långt som möjligt främja en väl fungerande konkurrens. I det fall en betydande del av användarna, som den offentliga sektorn utgör, låses till en eller ett fåtal kommersiella aktörer som i alternativ 1 hämmas konkurrens och utveckling – detta leder i längden till fördyringar som drabbar såväl offentlig sektor som övriga delar i samhället. Alternativet skapar heller inte möjlighet för offentlig sektor att vara pådrivande i utvecklingen. En liknande effekt uppnås också med alternativ 2 där offentlig sektor låses till en statlig aktör som tar på sig ett stort ansvar för verksamheten och dess utveckling. Behovet av en flexibel och utvecklingsbar kravbild synes därför bäst uppfyllas av det tredje alternativet där ett av målen är att gemensamt utveckla och sprida kompetens för kravställning och egen upphandling på en marknad med fungerande konkurrens. Stödet till offentlig sektor är inte i form av en färdig lösning utan istället stöd med koordinerad kravställning för egen upphandling.

Sammantaget ger analysen att alternativ 3 är den mest lämpliga väg att gå när det gäller att skapa tillgängliga och skyddade kommunikationsinfrastrukturer för offentlig sektor. Alternativet förutsätter dock att en rad frågor klargörs, bland annat kopplade till administrativa funktioner, ansvar, säkerhetsfrågor och styrmedel.

I kapitel 5 presenteras rapportens förslag. Där ges en närmare beskrivning för hur den lösnings som valts bör införas.

5. Förslag

5.1 Sammanfattande förslag och bärande principer

För att utveckla och upprätthålla tillgängliga och skyddade kommunikationsinfrastrukturer för offentlig sektor krävs det en sammanhållen organisatorisk struktur som över tiden förmår tillvarata de goda förutsättningar Sverige har som ett utvecklat IT-land. Det bärande elementet i en sådan struktur är det offentligas förmåga att ställa krav – och att följa upp krav.

Genom att formulera kravprofiler för tillgänglighet och skydd i offentlig sektors kommunikationer som stöd till upphandlingsansvarig myndighet tillgodoses flera till synes motstridiga krav. För det första får offentlig sektors kommunikationer en jämn och hög kvalitet. För det andra effektiviseras upphandlingsarbetet. För det tredje kommer den enhetliga kravbilden att skapa förutsättningar för en breddad konkurrens.

För att detta ska bli verklighet behövs en funktion för samordning och inriktning som tar fram, förvaltar och över tiden vidareutvecklar krav, med möjlighet att nivåanpassa tillgänglighet och skydd. Funktionen ska ha nära samverkan med såväl offentliga organisationer som marknadens aktörer.

Flera aktörer i offentlig sektor behöver redundans i sin kommunikationsinfrastruktur, exempelvis genom flera förbindelser, över olika nät, placerade hos olika operatörer. För ett begränsat antal myndigheter med särskilda behov av kontrollerbara kommunikationer kommer det också att behövas tillgång till en statlig kontrollerbar kommunikationsinfrastruktur. För detta behov kommer det att behövas en funktion för förvaltning och drift.

En sammanhållen organisatorisk struktur

Mot bakgrund av ovanstående föreslår MSB att det etableras en organisatorisk struktur bestående av två funktioner:

- en funktion för samordning och inriktning vid Myndigheten för samhällsskydd och beredskap (MSB), och
- en funktion för drift och förvaltning vid Trafikverket ICT som ansvarar för drift och förvaltning av den statliga kontrollerbara kommunikationsinfrastrukturen som avdelas för att skapa redundans hos ett begränsat antal myndigheter med särskilda behov.

Till detta kommer en nära samverkan med upphandlingsansvarig myndighet. Utgångspunkten är att denna samverkan ska säkerställa att utvecklade krav på tillgänglighet och skydd finns med i de ramavtal och partsavtal som det offentliga använder för upphandling och avrop.

För att realisera dessa funktioner föreslås att:

- MSB bör få i uppdrag att i samverkan med Trafikverket och andra berörda aktörer, utreda funktionen för samordning och inriktning (FSI) och att utveckla en plan för att implementera den. Utgångspunkten är att FSI ska bli en funktion för samordning av verksamheten, strategisk inriktning, stöd i kravställning, upphandling och uppföljning, samt verka för kompetenshöjning.

- Trafikverket bör få i uppdrag att i samråd med MSB, och i samverkan med andra berörda aktörer, utreda funktionen för drift och förvaltning (FDF) och att utveckla en plan för att implementera den. Utgångspunkten är att FDF ska bli en funktion för drift och förvaltning av den statliga kommunikationsinfrastruktur som avdelas för att skapa redundans hos ett begränsat antal myndigheter med särskilda behov.

Specifika skyddsåtgärder

Genom att etablera ett koncept för skyddade anslutningar till Internet för offentliga organisationer skapas en möjlighet att kombinera centralt framtagna krav på skydd med de lösningar som marknaden kan erbjuda. I förslaget har detta fått benämningen Skyddad Internetanslutning (SIA).

För att realisera detta föreslås att:

- MSB bör få i uppdrag att i samråd med Trafikverket, och i samverkan med relevanta aktörer, studera och utvärdera tekniska lösningar, administrativa och juridiska förutsättningar för, samt praktiskt införande av, Skyddad Internetanslutning (SIA). Utgångspunkten är att antalet anslutningar till Internet för offentlig sektor reduceras och förses med förstärkt skydd.

Tjänsten Skyddad Internetanslutning (SIA) för offentlig sektor bör tas fram för att kunna nyttjas av de myndigheter som finns angivna i bilagan till Krisberedskapsförordningen (KBF) samt av myndigheter med synnerliga behov. Andra offentliga organisationer kan sedan gå samman och med utgångspunkt från specifikationerna för SIA handla upp tjänsten av näringslivet och då få den anpassad till deras respektive behov.

Vidare föreslås att:

- Försvarsmakten (FM) bör få i uppdrag att i samråd med MSB, och i samverkan med andra berörda aktörer utveckla och godkänna ett nationellt bredbandskrypto för offentlig sektor.

5.1.1 Tillgängliga och skyddade kommunikationsinfrastrukturer för offentlig sektor

Tillgängliga och skyddade kommunikationsinfrastrukturer för offentlig sektor bör dra nytta av de goda förutsättningar Sverige har som ett utvecklat IT-land. Några av dessa förutsättningar är en utbyggd befintlig infrastruktur, en konkurrensmarknad stadd i snabb utveckling och en generellt hög teknisk kompetensnivå inom både den privata som offentliga sektorn.

Det mest effektiva sättet att utveckla tillgängliga och skyddade kommunikationsinfrastrukturer för den offentliga sektorn är att ge de offentliga aktörerna möjligheten att nyttja de resurser som finns på ett väl koordinerat sätt. Det gäller både resurser inom den offentliga sektorn och sådana resurser som finns att upphandla från näringslivet. Grunden i förslaget är därför en utvecklad upphandling med tydliga krav på kostnadseffektivitet, tillgänglighet och skydd. Därmed kan det mer konkreta, offentliga åtagandet koncentreras till några få specifika områden där staten behöver ha tydligare kontroll över verksamheten, samt till funktioner som samhället behöver men som marknaden inte kan erbjuda. Vid sidan av detta kan staten även behöva skapa och stödja olika former av samverkan och vid behov ta på sig rollen att vara samordnande.

De åtgärder som beskrivs väntas att bli mest effektiva om den offentliga sektorn samverkar internt och med näringslivet kring koordinerade lösningar på gemensamma problem. En kombination av resurser från offentlig och privat sektor ger bäst förutsättningar för kostnadseffektiva, tillgängliga och skyddade kommunikationsinfrastrukturer – både idag och imorgon.

Förslaget får bäst effekt då det genomförs i sin helhet. En samordnad verksamhet, ett gemensamt förhållningssätt för offentlig sektor samt en förmåga att operativt driva vissa funktioner medverkar till en stabil grundnivå, såväl i det dagliga arbetet som vid svåra störningar. Förslaget skapar tillgängliga och skyddade kommunikationsinfrastrukturer som fungerar under normala förhållanden och under påfrestningar. Det innefattar även en organisation som kan fungera som stöd under allvarliga störningar och kriser. Förslaget innebär att myndigheters, kommuners och landstings arbetssätt inte förändras i en övergång från normalläge till krisläge. De föreslagna åtgärderna kan tvärtom underlätta arbetet i pressade situationer.

Syftet med tillgänglighetsåtgärderna är att skapa en mer robust informationshantering vid samhällets normaltillstånd och vid allvarliga störningar och kriser. Om säkerheten fungerar bra till vardags betyder det ofta att verksamheten är förberedd på allvarligare händelser.[13]

Viktigt är att förslaget tillvaratar och utvecklar den kompetens och organisation som redan finns, samt drar nytta av nuvarande offentliga och privata tekniska strukturer. Förslaget erbjuder därvidlag ett kostnadseffektivt och koordinerat arbetssätt för att skapa tillgängliga och skyddade kommunikationsinfrastrukturer, där alla aktörer inte behöver vidta samma åtgärder parallellt.

Förslaget innehåller vidare komponenter för att förstärka det förebyggande arbetet, förmågan till respons, samt förmågan till återställning och uppföljning. Den organisationsform som rapporten föreslår syftar till att stödja myndigheternas, kommunernas och landstingens primära uppdrag.

13 *Strategi för samhällets informationssäkerhet 2010–2015*. MSB, 2010.

Fullt utbyggda bör skyddade och tillgängliga kommunikationsinfrastrukturer för offentlig sektor kunna omfatta samtliga myndigheter, kommuner och landsting. Införandet bör dock ske successivt. Det är en uppfattning som också delas av utländska myndighetsrepresentanter i de länder projektgruppen besökt.

De myndigheter som särskilt pekas ut i bilagan till Krisberedskapsförordningen har en särskild roll i krishanteringssystemet och behöver kunna samverka även under ansträngda förhållanden. Dessa myndigheter har ett utvecklat säkerhetsmedvetande och arbetar systematiskt med informationssäkerhet. MSB bedömer att det ur flera aspekter är lämpligast att börja implementera en tillgänglig och skyddad kommunikationsinfrastruktur i samverkan med, och hos, dessa myndigheter samt myndigheter med synnerliga behov. Detta ger goda förutsättningar för att snabbt introducera lösningar såsom Skyddad Internetanslutning (SIA). Erfarenheterna från dessa myndigheter kommer att vara värdefulla i det fortsatta arbetet.

Den centrala delen av förslaget är att stärka det offentliga kravställandet och ge den offentliga sektorn bättre möjlighet att få tillgång till marknadens resurser och utveckling. Omvänt får marknadens aktörer möjlighet att anpassa tjänsteutbudet till en mer koordinerad kravbild från offentlig sektor. Det är inte bara den offentliga sektorn, utan hela marknaden, som får ökade förutsättningar för tillgänglighet och skydd på affärsmässiga grunder och under konkurrens.

5.1.2 Rättsliga aspekter

De rättsliga aspekterna som aktualiseras av förslaget (avsnitt 3.3) måste, utredas närmare i samband med utredningen av de föreslagna funktionerna. Syftet bör i första hand vara att identifiera sådana förhållanden och krav som har eller kan ha direkt inverkan på den närmare utformningen av de mer praktiska inslagen i förslaget. Det kan exempelvis handla om hanteringen av loggуppgifter, eller behovet av att upprätta personuppgiftsbiträdesavtal, i samband med att ett koncept för Skyddad Internetanslutning (SIA) tas fram.

För att den offentliga sektorn fullt ut ska kunna utnyttja fördelarna med tillgängliga och skyddade kommunikationsinfrastrukturer är det önskvärt att en så stor del av sektorn som möjligt tar tillvara de möjligheter som ges och upphandlar tjänster för ökad tillgänglighet och skydd. En grundförutsättning för att hela den offentliga sektorn ska kunna delta aktivt är att den organisatoriska strukturen, och de tjänster som erbjuds, skapar ett förtroende. Rättsliga ramverk är här ett verktyg och det är viktigt att de utformas på ett ändamålsenligt sätt.

Exempelvis är det centralt att de olika funktionernas har tydliga uppgifter och ett tydligt ansvar. MSB bör få huvudansvaret för att ta fram ett förslag på hur rättsliga ramverk kan utformas, med hänsyn till myndighetens föreslagna inriktande och samordnande ansvar. Trafikverket bör få ansvar för att närmare utreda de rättsliga frågorna kring funktionen FDF. För att underlätta koppling

till övriga delar av det rättsliga ramverket bör detta arbete ske i samråd med MSB.

Tillgängliga och skyddade kommunikationsinfrastrukturer för offentlig sektor bygger till stora delar på upphandling av olika tjänster. Upphandlingsansvarig myndighet bör därför erbjudas ett ändamålsenligt stöd. Här har föreslagits att MSB, i rollen som ansvarig för FSI, ges ett utpekat ansvar för att erbjuda sådant stöd. Formerna för hur stödet bör utformas måste dock utredas närmare i samverkan med upphandlingsansvarig myndighet.

Etableringen av FDF är beroende av den föreslagna omorganisationen inom Trafikverket ICT[14]. Det kan därför behövas en interimistisk verksamhet för drift för delar av infrastrukturen.

5.2 Beskrivning av förslaget i detalj

5.2.1 Föreslag till struktur och organisation

Mot bakgrund av ovanstående föreslår MSB att det etableras en organisatorisk struktur bestående av två funktioner:

- en funktion för samordning och inriktning vid Myndigheten för samhällsskydd och beredskap (MSB), och
- en funktion för drift och förvaltning vid Trafikverket ICT som ansvarar för drift och förvaltning av den statliga kontrollerbara kommunikationsinfrastrukturen som avdelas för att skapa redundans hos ett begränsat antal myndigheter med särskilda behov.

Till detta kommer en nära samverkan med upphandlingsansvarig myndighet. Utgångspunkten är att denna samverkan ska säkerställa att utvecklade krav på tillgänglighet och skydd finns med i de ramavtal och partsavtal som det offentliga använder för upphandling och avrop.

För att realisera dessa funktioner föreslås att:

- MSB bör få i uppdrag att i samverkan med Trafikverket och andra berörda aktörer, utreda funktionen för samordning och inriktning (FSI) och att utveckla en plan för att implementera den. Utgångspunkten är att FSI ska bli en funktion för samordning av verksamheten, strategisk inriktning, stöd i kravställning, upphandling och uppföljning, samt verka för kompetenshöjning.

14 *Trafikverket ICT*. Betänkande av Utredningen om Trafikverket ICT, SOU 2010:82.

- Trafikverket bör få i uppdrag att i samråd med MSB, och i samverkan med andra berörda aktörer, utreda funktionen för drift och förvaltning (FDF) och att utveckla en plan för att implementera den. Utgångspunkten är att FDF ska bli en funktion för drift och förvaltning av den statliga kommunikations-infrastruktur som avdelas för att skapa redundans hos ett begränsat antal myndigheter med särskilda behov.

Med ett etablerande av FDF vid Trafikverket, och närmare bestämt vid *Trafikverket-ICT*, nyttjas den redan etablerade rikstäckande kommunikations-infrastrukturen som staten byggt upp[15]. En sådan etablering innebär att det skapas en nödvändig kontroll över den kommunikationsinfrastruktur som är tänkt att skapa redundans hos de myndigheter som är angivna i bilagan till Krisberedskapsförordningen (KBF) samt till myndigheter med synnerliga behov.

5.2.1.1 Funktionen för samordning och inriktning (FSI)

Funktionen för samordning och inriktning (FSI) bör ha i uppgift att utveckla den strategiska inriktningen av arbetet med en tillgänglig och skyddad kommunikationsinfrastruktur för offentlig sektor. I detta kan ingå att svara för utveckling av föreskrifter, råd och anvisningar, uppföljning, stöd vid upphandling, kravställning mot leverantörer, och att verka för kompetens-höjning.

För att underlätta etableringen av FSI bör funktionen placeras hos en myndighet vars verksamhet redan inrymmer förutsättningar för att etablera och stödja den verksamhet som FSI ska bedriva. Utgångspunkten i detta är först och främst att det primära mandatet för myndigheten inte får komma i konflikt med den uppgift som FSI ska utföra. Detta utesluter sannolikt sektorsansvariga myndigheter. Ett annat viktigt kriterium är en helhetssyn på samhällets behov av tillgänglig och skyddad kommunikation inom olika sektorer. Myndigheten bör också ha förmåga att samla in den information som krävs för att få en rättvis bild av behoven. Ytterligare ett viktigt område är att myndigheten är van vid att kravställa och hantera frågor kring storskaliga kommunikationssystem. Slutligen är det viktigt att myndigheten är van vid och har förmågan att kravställa och hantera frågor kring skydd av information.

MSB har idag ansvar för frågor om skydd mot olyckor, krisberedskap och civilt försvar. Ansvaret avser åtgärder före, under och efter en olycka eller kris. Myndigheten ska utveckla och stödja samhällets beredskap, vara pådrivande i arbetet med förebyggande och sårbarhetsreducerade åtgärder, arbeta med samordning mellan berörda aktörer, bidra med att minska konsekvenserna av olyckor och kriser, följa upp och utvärdera samt se till att utbildning och övning kommer tillstånd inom myndighetens ansvarsområde. I detta arbete ingår

15 http://www.trafikverket.se/ICT/

bland annat att identifiera och analysera sådana sårbarheter, hot och risker som kan anses vara särskilt allvarliga och se till att ledningsmetoder, stödsystem och materiel för krishantering utvecklas och tillhandahålls. MSB ska även stödja och samordna arbetet med samhällets informationssäkerhet samt svara för att Sverige har en nationell funktion med uppgift att stödja samhället i arbetet med att förebygga och hantera IT-incidenter. Myndigheten har även föreskriftsrätt för statliga myndigheter på informationssäkerhets-området.

Till detta kommer myndighetens uppgifter vid olyckor och kriser. Myndigheten ska se till att berörda aktörer vid en kris får tillfälle att samordna kris-hanteringsåtgärderna och samordna information till allmänhet och medier. MSB ska också hjälpa aktörerna att effektivt använda samhällets samlade resurser och samordna stödet till centrala, regionala och lokala organ i frågan om information och lägesbilder. Utöver detta finns sedan ett antal uppgifter inom uppföljning, utvärdering och lärande samt inom forskning och utveckling.[16] Myndigheten hanterar sedan tidigare ett antal system såsom Rakel, WIS, SGSI med flera.

Vid en sammantagen bedömning finner MSB att huvuddelen av uppgifterna som FSI förväntas ha inryms i myndighetens nuvarande instruktion. Därför bör Funktionen för samordning och inriktning placeras hos MSB.

FSI måste bedriva sin verksamhet i nära samverkan med Funktionen för drift och förvaltning (FDF) och upphandlingsansvarig myndighet. Både FSI och FDF måste ha en nära samverkan med offentlig sektor och näringslivet. Det är synnerligen viktigt att hitta arbetsformer som garanterar berörda aktörer insyn i och inflytande över FSI:s verksamhet. FSI bör upprätta en användargrupp bestående av centrala myndigheter, länsstyrelser, kommuner och landsting. Gruppens erfarenheter bör utgöra ingångsvärden i utvecklingen av kommunikationsinfrastrukturen. FSI bör även upprätta samverkansgrupper med representanter för näringslivet.

5.2.1.2 Funktion för drift och förvaltning (FDF)

Funktionen för drift och förvaltning (FDF) bör ha i uppgift att svara för drift och förvaltning av den statliga kommunikationsinfrastruktur som avdelas för att skapa redundans hos ett begränsat antal myndigheter med särskilda behov.

Den bedömning som görs här är att en kommunikationsinfrastruktur som staten själv kontrollerar är en strategisk resurs, och en nödvändig komponent i skyddade och tillgängliga kommunikationsinfrastrukturer för offentlig sektor. En sådan kommunikationsinfrastruktur är en förutsättning för att det, oberoende av omvärldshändelser, ska gå att upprätthålla en tillgänglig, skyddad och fullt kontrollerbar redundant kommunikationsinfrastruktur för de

16 Se vidare förordning (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap

myndigheter som finns utpekade i bilagan till Krisberedskapsförordningen (KBF) samt för myndigheter med synnerliga behov. Den redundanta skyddade kommunikationsinfrastrukturen avseende fibernät ska ha resurser som är skilda från operatörens övriga verksamhet. Fibernätinfrastrukturen bör erbjudas myndigheter som finns angivna i KBF samt myndigheter med synnerliga behov. FDF bör ha förmåga att komplettera de egna tillgångarna med externa resurser. Det är viktigt att betona att det förslag som diskuteras här innebär att den huvudsakliga kapaciteten till offentlig sektor även i fortsättningen kommer att levereras av näringslivet.

MSB bedömer att Trafikverkets nät är det enda offentligt ägda alternativ som tillräckligt väl uppfyller kraven för att kunna leverera redundans till de särskilt utpekade myndigheterna (med reservation för vissa kompletteringsbehov). Trafikverkets nät är riksomfattande och bedöms vara det nät som har minst behov av att hyra in resurser från andra operatörer för att kunna skapa den redundans som diskuteras här (se även Bilaga E). MSB anser därför att FDF bör placeras hos Trafikverket.

I betänkandet av Utredningen om Trafikverket ICT[17] föreslår utredaren att den del av Trafikverket ICT:s verksamhet som går ut på att tillhandahålla kapacitet i Trafikverkets fiberoptiska kabel (nät och drift inklusive master) samt transportnära informationstekniska tjänster överförs till ett affärsdrivande verk. Detsamma gäller för den kanalisation som finns längs vissa vägar. Vidare föreslår utredaren att staten tillsätter en utredning med uppdrag att analysera och ge förslag på hur de statliga fibernät som i dag ägs av affärsverket Svenska Kraftnät, Trafikverket och Teracom AB ska samordnas till stöd för regeringens bredbandsstrategi.

Utredarens förslag, det vill säga att överföra Trafikverket ICT till ett affärsdrivande verk och vidare utreda hur Svenska Kraftnät, Trafikverket och Teracom AB ska kunna samordna sina fibernät till stöd för regeringens bredbandsstrategi, stämmer väl överens med vårt förslag på att etablera en funktion för drift och förvaltning. FDF bör, om betänkandets förslag går igenom, bli en del av det föreslagna affärsverket.

Verksamheten vid FDF måste bedrivas i nära samverkan med Funktionen för samordning och inriktning (FSI) samt med operatörer och leverantörer. Både FSI och FDF måste ha en nära samverkan med offentlig sektor och med näringslivet. FDF bör inrätta en användargrupp. Gruppens erfarenheter bör utgöra ingångsvärden i utvecklingen av kommunikationsinfrastrukturen. FDF bör även upprätta en samverkansgrupp med representanter för näringslivet.

17 *Trafikverket ICT*. Betänkande av Utredningen om Trafikverket ICT, SOU 2010:82.

5.2.1.3 Tillsammans skapar FSI och FDF ökad tillgänglighet och ökat skydd över tiden

Redundans för fysiska och logiska anslutningar

Mångfalden av operatörer medför nya möjligheter att skapa tillgängliga och skyddade kommunikationsinfrastrukturer för offentlig sektor.

Risk- och sårbarhetsanalyser bör vara viktiga utgångspunkter då myndigheter, kommuner och landsting tar fram sina behov avseende tillgänglighet till, och skydd av, elektroniska kommunikationer. Om verksamheten behöver en hög grad av tillgänglighet bör såväl fysisk som logisk anslutning till kommunikationsinfrastruktur vara redundant, samt vara försedd med lastdelningsfunktion.

MSB bedömer att myndigheter som finns utpekade i bilagan till KBF, samt myndigheter med synnerliga behov, bör ha fler fysiska och logiska förbindelser. Något som flera av dessa myndigheter redan har i dagsläget. I syfte att öka tillgängligheten bör FDF erbjuda dessa myndigheter abonnemang för att nyttja den del av den statligt kontrollerade kommunikationsinfrastruktur som avdelats för att skapa redundans.

Både FSI och FDF bör systematiskt stödja offentliga aktörer i arbetet med ökad tillgänglighet och ökat skydd utifrån gällande föreskrifter, råd och anvisningar.

En utvecklad offentlig upphandling

Den offentliga sektorn är en betydande beställare som genom stor upphandlingsvolym har förutsättningar att ställa krav och genom avtal påverka såväl normer och priser som tillgänglighet och skydd. En sådan påverkan gynnar samtliga aktörer inom den offentliga sektorn och på sikt även medborgare och näringsliv.

E-delegationen pekar på vikten av att hela den offentliga sektorn nyttjar det som en enskild myndighet har gjort bra. E-delegationen pekar också på betydelsen av att utveckla fler former av ”koncerntänkande” med gemensam planering av stödprocesser, där varje aktör fokuserar på sina kärnprocesser. Ett sådant arbetssätt minskar resursåtgången eftersom de offentliga aktörerna kan lära av varandra och undvika onödiga misstag. Ett centraliserat förhållningsätt i upphandlingsprocesserna gör att tillgängligheten och skyddet ökar och att resurserna kan nyttjas mer effektivt.

Också Riksrevisionens granskning avseende IT och outsourcing konstaterar att det är ”stora skillnader mellan olika myndigheters kompetens att bedöma frågor om IT och outsourcing. Det finns därför ett behov av bättre vägledningar

och erfarenhetsutbyte, så att myndigheterna inte alltid behöver börja från början när dessa frågor prövas”. [18]

Även om myndigheter, kommuner och landsting har tillgång till bra ramavtal och anvisningar från centralt håll, kan det vara svårt för att göra en adekvat upphandling för den egna verksamheten. Inte sällan får tillgänglighets- och skyddsfrågor stå tillbaka för kortsiktiga ekonomiska överväganden. Därför är det i detta sammanhang viktigt att betona att myndigheter, kommuner och landsting i sina risk- och sårbarhetsanalyser ska beakta informationssäkerhet.[19]

Att den offentliga sektorn utvecklar sin upphandling med ökad riskspridning gör att fler operatörer kan erbjuda sektorn sina tjänster. Det i sin tur utvecklar konkurrensen och driver på säkerhetsarbetet hos dessa aktörer. På så sätt skapas en situation där hela marknaden drar nytta av utvecklade krav-ställningar och upphandlingsrutiner.

Mot bakgrund av ovanstående, bör FSI utveckla ett nära samarbete upp-handlingsansvarig myndighet.

De offentliga aktörerna har varierande resurser för upphandling. En viktig del i arbetet med att skapa tillgängliga och skyddade kommunikationsinfra-strukturer är att erbjuda proaktivt stöd till myndigheter, kommuner och landsting som upphandlar dessa tjänster. Stöd från centralt håll bidrar till att på ett kostnadseffektivt sätt förbättra tillgängligheten till, och skydd av, kommunikationsinfrastrukturer för offentlig sektor.

Två viktiga delar i en utvecklad upphandling för offentlig sektor är krav-ställning och uppföljning.

Ökad samverkan och samordning i ramavtalsupphandlingar förbättrar den offentliga sektorns förmåga att utveckla kravspecifikationer och ramavtal. Detta skapar en förmåga hos den offentliga sektorn att agera som en mer kompetent beställare. Det utvecklar även leverantörernas kompetens och deras förståelse för den offentliga sektorns behov.

Det kan i särskilda fall vara befogat med krav så att kommunikationen mellan offentliga aktörer, och kommunikationen mellan offentliga aktörer och med-borgarna, sker i system som finns inom landets gränser. Erfarenheter från Storbritannien visar att sådant arbete är omfattande och att det bör ske i nära samverkan med leverantörerna. Erfarenheterna visar också att när väl kraven är utformade och beskrivs på ett tydligt sätt är det lättare att forma avtal som går att följa upp.

---

18 *IT inom statlig förvaltning – har myndigheterna på ett rimligt sätt prövat om outsourcing bidrar till ökad effektivitet?* RiR 2011:4, Riksrevisionen, 2011.

19 Krav på förmågebedömning av informationssäkerhet regleras i bilagorna till MSBFS 2010:6 och 2010:7.

Tillgänglighets- och skyddskrav kan dock vara kostnadsdrivande. Kravställaren har därigenom också ett ansvar för att kraven på skydd och tillgänglighet är balanserade. Utgångspunkten för detta är många gånger ett systematiskt arbete med risk- och sårbarhetsanalyser samt ett system för klassificering av information. Här ger ledningssystem för informationssäkerhet en god grund.[20]

Det är av central betydelse att avtalen ger användarna rätt till opartisk uppföljning. Kontinuerlig uppföljning, tekniska kontroller, säkerhetsrevisioner och intrångsanalyser skapar förutsättningar för en bild av hur kraven uppfylls. Uppföljning skapar en mer kvalificerad dialog mellan offentlig sektor och leverantörer. Det bidrar till att insatserna för tillgänglighet och skydd blir kostnadseffektiva.

FSI, och även till viss del FDF, kommer efter hand att få en bild av den offentliga sektorns behov av skyddad och tillgänglig kommunikations-infrastruktur. De två funktionerna kommer, på ett sätt som inte varit möjligt tidigare, att få en bra översikt över vilka åtgärder staten kan behöva komplettera med för att öka tillgängligheten för samhällsviktig verksamhet i de publika näten. Ett nära samarbete med myndigheter, kommuner, landsting och med näringslivet skapar goda möjligheter att vidareutveckla den privat-offentlig samverkan.

Ytterligare ett steg i upphandlingskedjan är att vidareutveckla riktlinjer för tillgänglig elektronisk kommunikation för samhällsviktig verksamhets behov i de publika näten. Denna fråga bör närmare belysas i det uppdrag MSB föreslås få avseende FSI. Det är också viktigt att följa upp nätens robusthet och tillgänglighet.

FSI ska stödja ramavtalsansvariga myndigheter vid ramavtalsupphandlingar, stödja användarna vid deras respektive upphandlingar samt utveckla statens tillgänglighets- och skyddsarbete för kommunikationsinfrastrukturer. Funktionen skapar därmed goda grunder för att uppnå tillgängliga och skyddade kommunikationsinfrastrukturer för den offentliga sektorn – något som också gynnar medborgare och näringsliv.

Kompetensutveckling av IT-personal i offentlig sektor

Tillgängliga och skyddade kommunikationsinfrastrukturer kräver att IT-personalen i den offentliga sektorn har en hög kompetens. Det är en förutsättning för att exempelvis rätt kunna konfigurera den utrustning hos myndigheter, kommuner och landsting som är ansluten till Internet.

Både FSI och FDF bör på olika sätt verka för en hög kompetensnivå hos IT-personal i offentlig sektor, exempelvis genom användargrupper och samverkan med privata utbildningsaktörer. En kontinuerlig och koordinerad kompetens-

20 Råd och rekommendationer finns på www.informationssäkerhet.se

utveckling skapar kontaktnät som bygger upp det förtroende som krävs för samverkan vid oväntade händelser.

5.2.2 Föreslag till specifika skyddsåtgärder

Genom att etablera ett koncept för skyddade anslutningar till Internet för offentliga organisationer skapas en möjlighet att kombinera centralt framtagna krav på skydd med de lösningar som marknaden kan erbjuda. I förslaget har detta fått benämningen Skyddad Internetanslutning (SIA).

För att realisera detta föreslås att:

- MSB bör få i uppdrag att i samråd med Trafikverket, och i samverkan med relevanta aktörer, studera och utvärdera tekniska lösningar, administrativa och juridiska förutsättningar för, samt praktiskt införande av, Skyddad Internetanslutning (SIA). Utgångspunkten är att antalet anslutningar till Internet för offentlig sektor reduceras och förses med förstärkt skydd.

Tjänsten Skyddad Internetanslutning (SIA) för offentlig sektor bör tas fram för att kunna nyttjas av de myndigheter som finns angivna i bilagan till Krisberedskapsförordningen (KBF) samt av myndigheter med synnerliga behov. Andra offentliga organisationer kan sedan gå samman och med utgångspunkt från specifikationerna för SIA handla upp tjänsten av näringslivet och då få den anpassad till deras respektive behov.

Vidare föreslås att:

- Försvarsmakten (FM) bör få i uppdrag att i samråd med MSB, och i samverkan med andra berörda aktörer utveckla och godkänna ett nationellt bredbandskrypto för offentlig sektor.

5.2.3.1 Skyddad Internetanslutning (SIA)

Den offentliga sektorn kan öka sitt skydd genom att minska antalet logiska anslutningar till Internet och genom att ge kvarvarande anslutningar förstärkta skyddsmekanismer enligt gemensamt framtagna specifikationer. I ett flertal länder har offentlig förvaltning etablerat gemensamma förmedlingsnoder mot Internet, det vill säga att de har minskat antalet logiska anslutningar till Internet. De har därmed kommit långt i arbetet med centraliserat skydd för sina kommunikationsinfrastrukturer.

Genom att etablera ett koncept för skyddade anslutningar till Internet för offentliga organisationer, fortsättningsvis benämnd Skyddad Internetanslutning (SIA), skapas en möjlighet att kombinera centralt framtagna krav på tillgänglighet och skydd med de lösningar som marknaden kan erbjuda. SIA skapar också nya möjligheter att etablera gemensamma funktioner och tjänster.

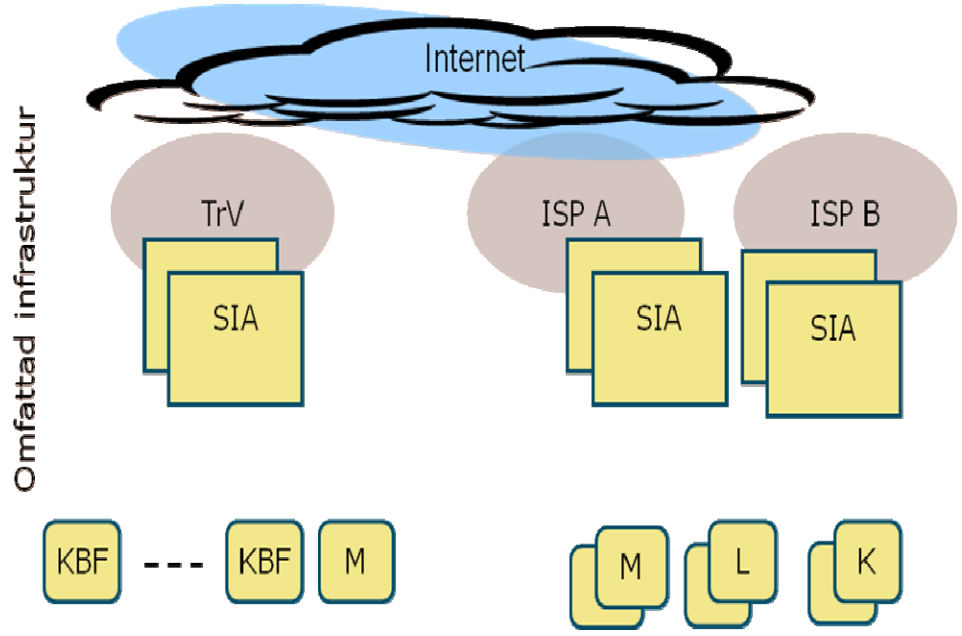
SIA är en nätverksknutpunkt. Inåt, mot de medverkande organisationerna, finns krypterade, redundanta, fasta förbindelser som ansluter utgången från en

medverkande organisations system med ingången i SIA. Utåt, mot Internet, finns redundanta högkapacitetsanslutningar mot Internetleverantörer (ISP:er).

När SIA införs skapas en skyddad miljö för de organisationer som ligger innanför SIA. Det skapar även ett skydd mellan de anslutna organisationerna. Intrång i en organisations IT-system påverkar inte skyddet hos andra organisationer som är anslutna till en specifik SIA. Däremot kan den skyddade zon som etableras innanför SIA påverkas, därför är det också rimligt att ställa krav på organisationer som önskar ansluta sig. Ett arbete med att formulera dessa krav bör inledas parallellt med utvecklingen av SIA. Organisationer som önskar ansluta sig till en SIA bör ackrediteras enligt de överenskomna kraven.

SIA möjliggör även insynsskyddad kommunikation mellan deltagande organisationer. Det försvårar exempelvis kartläggning av enskilda myndigheter och ger möjligheten att prioritera trafik. Dessa möjligheter kan skapas oberoende av logisk Internetanslutning.

SIA syftar inte till att förändra ansvarsprincipen. De medverkande organisationerna har fortfarande ansvar för sitt eget skydd, men får genom SIA ett kvalificerat stöd i detta arbete.



TrV – Trafikverket

ISP – Internet Service Provider

KBF – Myndigheter enligt bilagan till förordningen (2006:942) om krisberedskap och höjd beredskap

M – Myndighet

L - Landsting/region

K – Kommun

Figur 1. Principen för Skyddad Internetanslutning (SIA)

Tanken är inte att samtliga offentliga organisationer ska ansluta sig till en och samma SIA. Här finns stora möjligheter att utveckla SIA utifrån grundläggande krav på tillgänglighet, skydd och behov av tjänster. Konceptet SIA bygger på att det offentliga tar fram kravspecifikationer och att vissa, eller samtliga, tjänster levereras av marknaden. Offentliga organisationer kan därigenom gå samman och handla upp tjänsten av näringslivet, utifrån specifikationerna för SIA.

Några av de funktioner som skulle kunna ingå i en SIA är brandväggar, överbelastningsskydd, intrångsdetektering (IDS), viruskontroller, spamfiltrering, loggfunktioner, redundans, tunnlingsteknik, trafikfiltrering, routing samt domännamnsservrar (DNS/DNSsec). Skyddet i SIA bygger lämpligen på kommersiella system som kompletteras med kunskaper som finns hos expertmyndigheter inom informationssäkerhetsområdet.

Ett första steg i arbetet med att introducera SIA är en studie för att ta fram ett koncept (en pilot). Studien bör exempelvis omfatta en definition av generisk arkitektur, tekniska lösningar, administrativa och juridiska förutsättningar, paketering av tjänster i abonnemangsformer, test- och pilotverksamhet samt införandeplan. Det är viktigt att aktörer från den offentliga sektorn och näringslivet deltar i studien för att skapa förtroende för det koncept som tas fram.

Skyddade Internetanslutningar bör sedan introduceras successivt i den offentliga sektorn – dels som en tjänst för särskilt utvalda aktörer, dels i form av specifikationer som kan användas i upphandling.

Tjänsten SIA för offentlig sektor bör tas fram för att kunna nyttjas av de myndigheter som finns angivna i bilagan till Krisberedskapsförordningen (KBF) samt av myndigheter med synnerliga behov. För dessa myndigheter skulle tjänsten kunna levereras som ett abonnemang från Funktionen för drift och förvaltning (FDF). Det finns samordningsvinster mellan SIA och det förslag till nationellt IT-intrångsdetekterings- och varningssystem (TDV) som diskuteras i MSB:s svar på regeringens uppdrag om ett tekniskt detekterings- och varningssystem[21] och den Nationella operativa samverkansfunktionen för informationssäkerhet (NOS) som MSB inrättar. När det gäller SIA för de myndigheter som pekas ut ovan är CERT-SE och NOS det naturliga valet för att hantera skyddsmekanismerna.

SIA bör sedan etableras vidare genom upphandling utifrån de centralt framtagna specifikationerna. Här kan med fördel skyddsmekanismer upphandlas som tjänst av privata företag – så kallade managed security services providers – utifrån de etablerade specifikationerna och egna tillkommande behov.

---

21 Fö2010/702/SSK, Regeringsbeslut 13, 2010-04-14.

5.3.2.2 Ett nationellt bredbandskrypto för offentlig sektor

Det finns idag inget nationellt godkänt kryptosystem för att skydda skyddsvärda uppgifter som inte rör rikets säkerhet. Det finns dock VPN-krypton som är nationellt godkända för att skydda information som klassats ”Hemlig/Restricted” samt ”Hemlig”.

Det finns behov av att anpassa det VPN-krypto som i dag finns för nivån ”Hemlig/Restricted” till att skydda skyddsvärda uppgifter som inte rör rikets säkerhet så att det går att använda som grundskydd vid myndigheters anslutning till SIA. För att ett kryptosystem ska ge det skydd som eftersträvas måste säkra rutiner för användning av systemet utvecklas med hänsyn taget till den skyddsnivå som ska gälla för SIA. Dessutom krävs ett kryptosystem som kan hantera en hög bandbredd för att kunna uppfylla vissa organisationers behov av hög trafikkapacitet vid anslutning till SIA.

Sammanfattningsvis behövs ett nationellt godkänt bredbandskrypto för offentlig sektor. Det handlar alltså om ett kryptosystem som kan hantera skyddsvärda uppgifter som inte rör rikets säkerhet och som har en kapacitet på upp till 10 Gbit per sekund. Försvarsmakten i samråd med MSB, och i samverkan med andra berörda aktörer, bör därför ges i uppdrag att utveckla och godkänna ett sådant krypto.

Om det behövs starkare skydd än krypto för hantering av skyddsvärda uppgifter, måste respektive informationsägare ansvara för att säkra informationen med hjälp av lämpligt kryptosystem så att systemet uppfyller de ställda säkerhetskraven.

6. Kostnader

6.1 Gemensamma insatser skapar rationaliseringar och effektiviseringar

En bärande princip för rapportens förslag är att gemensamma insatser kan öka tillgängligheten till, och skydd av, offentlig sektors kommunikationsinfrastruktur. Detta innebär en betydande potential för både rationalisering och effektivisering.

För att åskådliggöra de kostnader som rapportens förslag innebär behöver kostnaderna för det föreslagna arbetssätet, och de tekniska lösningarna, sättas i relation till de kostnader som offentlig sektor har för sin kommunikationsinfrastruktur i dag.

MSB:s uppfattning är att förslaget med stor sannolikhet kommer att reducera kostnaderna för den offentliga sektorns kommunikation över Internet och enskilda aktörers säkerhetsarbete. Antagandet stöds av de internationella erfarenheter som inhämtats i arbetet med rapporten.

Under arbetets gång har det visat sig vara svårt att få fram uppgifter för att i detalj kunna identifiera kostnaden för nuvarande lösningar i Sverige. Kostnaderna redovisas uppdelade på olika sätt hos olika aktörer. En generell bild är alltså svår att få fram. Flera myndigheter har problem med att redovisa sina IT-kostnader på total nivå, och ännu fler har svårigheter att redovisa sina IT-kostnader på olika delområden.[22]

För att få en uppfattning om den besparingsvolym som förslagen kan innebära används uppskattningar hämtade från Storbritannien och det omfattande utredningsarbete som har gjorts där. MSB:s förslag bygger i stort på samma bärande principer som tillämpas i Storbritannien. Där har, som nämnts ovan, ett gemensamt koncept för den offentliga sektorn arbetas fram inom olika projekt tillsammans med näringslivet, med tydliga beskrivningar av de tjänster som ska levereras. Konceptet Public Sector Network (PSN) har definierats på ett tjänsteorienterat sätt för att kunna anpassas till marknadens utveckling både avseende teknik och struktur.

I arbetet med att definiera konceptet PSN i Storbritannien har en besparingspotential på cirka 20 % kalkylerats fram.[23] Vidare uppskattas de fysiska och logiska tjänsterna från ”fixed data network services” utgöra ca 13 % av den totala IKT-kostnaden.

---

22 *IT inom statlig förvaltning – har myndigheterna på ett rimligt sätt prövat om outsourcing bidrar till ökad effektivitet?* RiR 2011:4, Riksrevisionen, 2011.

23 *Public Sector Network. Outline Business Case* (Version 2.8). Cabinet Office (http://www.cabinetoffice.gov.uk/resource-library/public-sector-network).

Offentlig sektor i Sverige skiljer sig i sin struktur från offentlig sektor i Storbritannien, men den bedömning som görs här är att de uppskattningar som redovisas inom ramen för PSN kan tillämpas på svenska förhållanden eftersom stora delar av PSN överensstämmer med MSB:s förslag.

Den svenska offentliga sektorns kostnader för IKT uppskattas till cirka 40 miljarder årligen.[24] Hur stor del av den totala kostnaden som går till kommunikationsinfrastrukturen finns inte definierad. MSB uppskattar, utifrån den statistik som myndigheten har haft tillgång till, att den delen uppgår till 15-20 %.

Sammanfattningsvis ser MSB möjligheter till betydande effektivisering och rationaliseringspotential, med utgångspunkt från antagandena ovan.

6.2 Kostnader för att genomföra förslag

De bedömda kostnaderna för att genomföra rapportens förslag redovisas nedan utifrån de huvudsakliga förslagen i föregående kapitel. Den indirekta effekten av en fungerande kommunikationsinfrastruktur är dock inte medräknade här.

Utred förutsättningarna för att etablera funktionen för samordning och inriktning (FSI)

MSB bedömer att förslaget att utreda FSI kan genomföras inom myndighetens ordinarie ram.

Om FSI sedan etableras, uppskattas ett initialt behov (första och andra året) av 10 personår för att inrätta verksamheten och genomföra inledande uppdrag. Efter detta uppskattas den fortsatta förvaltningen av FSI uppgå till 10 personår. Till detta kommer uppskattade kostnader på 25–35 miljoner per år för att upphandla expertis från näringslivet när det gäller exempelvis teknisk utveckling, insatser för kompetenshöjning och uppföljning.

Utred förutsättningarna för att etablera funktionen för drift och förvaltning (FDF)

MSB bedömer att förslaget att utreda FDF bör kunna genomföras inom Trafikverkets ordinarie ram.

Om FDF sedan etableras, uppskattas ett initialt behov (första och andra året) av 5 personår för att inrätta verksamheten och genomföra föreslagna uppdrag. Efter detta uppskattas den fortsatta förvaltningen av FDF uppgå till 5–7 personår. Kostnaderna för FDF, samt kostnaderna för de aktörer som använder FDF:s infrastruktur, bör i stor utsträckning kunna finansieras genom abonnemang.

---

24 *IT-sourcing i offentlig sektor*. Institutet för informationsteknologi, 2010.

När det gäller offentlig sektors kostnad för ökad tillgänglighet, utgörs denna främst av en förmodad ökad andel redundanta fysiska förbindelser. Hur dessa kostnader fördelar sig beror på hur offentliga aktörer har etablerat sina anslutningar i dag. Huvuddelen av de myndigheter som föreslås kunna använda FDF har redan nu redundanta anslutningar. Därför torde endast begränsade kostnader uppstå. En inventering och översyn av dessa myndigheters anslutningar bör ingå i de inledande studierna angående FDF. När det gäller övriga aktörer i offentlig sektor, måste respektive aktör själv avgöra behovet av tillgänglighet utifrån genomförda risk och sårbarhetsanalyser.

Utveckla konceptet skyddad Internetanslutning (SIA) samt etablera en SIA som kan nyttjas av de myndigheter som pekas ut i bilagan till KBF och myndigheter med synnerliga behov

Att utveckla ett koncept för och att etablera en skyddad Internetanslutning (SIA) och kommunikationen mellan användarna bakom SIA kräver en omfattande utrednings- och testverksamhet. Ett sådant arbete är komplext, eftersom resultatet kommer att bestämma ramverket för tillgänglighet och skydd i offentlig sektors kommunikationsinfrastruktur för en lång tid framåt. Utredningsarbetet och testverksamheten ska ta fram tekniska lösningar och grundläggande arkitektur, och dessutom innehålla omfattande test- och pilotverksamhet. De organisatoriska och juridiska förutsättningarna behöver också utredas. Slutligen bör arbetet omfatta att praktiskt etablera en SIA för de myndigheter som pekas ut i bilagan till KBF samt att ta fram en implementeringsplan för konceptet SIA i offentlig sektor.

För att nå framgång krävs att myndigheter, kommuner och landsting deltar. Därutöver behöver expertis upphandlas från näringslivet. MSB uppskattar att studier och implementering av SIA enligt ovan kan genomföras efter beslut inom 1,5–2 år och till en kostnad av cirka 30 miljoner kronor, utöver kostnader för FSI. Av dessa kostnader utgör cirka 10–15 % kostnader för teknik, alltså hård- och mjukvara. Resterande kostnader är upphandlad kompetens och verksamhet från i huvudsak näringslivsaktörer.

Utveckla och godkänn ett nationellt bredbandskrypto

Kostnaderna för att utveckla och godkänna ett nationellt bredbandskrypto belastar i huvudsak Försvarsmakten. Kryptot ska kunna hantera skyddsvärda uppgifter som inte rör rikets säkerhet och klara en kapacitet på upp till 10 Gbit per sekund.

Kostnaden för förslaget bör kunna inrymmas i Försvarsmaktens ordinarie ram. Detta under förutsättning att arbetet kan ingå i Försvarsmaktens reguljära arbete med att utveckla kryptosystem för offentlig sektors behov.

Myndigheten för
samhällsskydd och beredskap

UPPDRAGSREDOVISNING

Datum	Diarienr
2011-03-01	2010-6304

Bilaga A: Regeringsuppdraget

'10 04/19 15:49 FAX 46 8 204483 FÖ DEP CIV E TET 020

REGERINGEN

Försvarsdepartementet

Regeringsbeslut 12

2010-04-14 Fö2010/701/SSK

Myndigheten för samhällsskydd och beredskap
651 81 KARLSTAD

Uppdrag till Myndigheten för samhällsskydd och beredskap angående samhällets informationssäkerhet

Regeringens beslut

1. Myndigheten för samhällsskydd och beredskap ska lämna förslag på hur en säker digital informations- och kommunikationsinfrastruktur för myndigheter, kommuner och landsting kan skapas. Myndigheten för samhällsskydd och beredskap ska genomföra uppdraget i samråd med andra berörda aktörer bl.a. de som ingår i samverkansgruppen för informationssäkerhet, SAMFI (Försvarets radioanstalt, Försvarets materielverk, Post- och telestyrelsen, Försvarsmakten och Säkerhetspolisen), Totalförsvarets forskningsinstitut, Skatteverket samt Delegationen för e-förvaltning. Myndigheten ska i detta arbete beakta befintlig infrastruktur, även kommersiella system, samt presentera alternativa lösningar med kostnadsförslag. Erfarenheter från andra länder som gjort liknande etableringar ska inhämtas. Myndigheten ska också i samråd med Försvarsmakten och Försvarets radioanstalt analysera hur befintliga eller kommande kryptosystem i detta syfte kan nyttjas för att skydda skyddsvärd eller sekretessbelagd information.

2. Myndigheten för samhällsskydd och beredskap ska ta fram en nationell plan som klargör hur allvarliga IT-incidenter ska hanteras samt skapa tekniska kompetensnätverk av experter som kan stödja samhället vid allvarliga IT-incidenter för att skapa en ökad förmåga till respons. Myndigheten för samhällsskydd och beredskap ska genomföra uppdraget i samråd med de myndigheter som ingår i samverkansgruppen för informationssäkerhet, SAMFI.

3. Myndigheten för samhällsskydd och beredskap ska utreda hur ett system för obligatorisk IT-incidentrapportering för statliga myndigheter kan utformas.

Postadress 103 33 Stockholm
Besöksadress Jakobsgatan 9
Telefonväxel 08-405 10 00
Telefax 08-723 11 89
E-post: registrator@defence.ministry.se

4. Myndigheten för samhällsskydd och beredskap ska, liksom tidigare Krisberedskapsmyndigheten, kontinuerligt analysera och bedöma omvärldsutvecklingen avseende hot, sårbarheter och risker inom informationssäkerhetsområdet samt konsekvenser för viktiga funktioner i samhället. Den samlade bedömningen ska tas fram i samverkan med berörda aktörer i samhället. Detta ska ses som ett komplement till den löpande rapportering och lägesbedömning som försvarsunderrättelse-myndigheterna och Säkerhetspolisen lämnar till regeringen inom ramen för sina respektive uppdrag.

5. Myndigheten för samhällsskydd och beredskap ska ha möjlighet att utifrån analyser av förmågebedömningar, genomförda risk- och sårbarhetsanalyser samt bedömningar av beroendeförhållanden föreslå enskilda myndigheter att anlita Försvarets radioanstalt för IT-säkerhetsanalyser. Detta ska ske i samråd med tillsynsmyndigheterna enligt säkerhetsskyddsförordningen (1996:633). Efter genomförda analyser ska Myndigheten för samhällsskydd och beredskap informera tillsynsmyndigheterna om påträffade förhållanden av betydelser för dessa myndigheters förebyggande och brottsbekämpande arbete.

Myndigheten för samhällsskydd och beredskap ska redovisa bedömda kostnader samt lämna förslag till finansiering. Myndigheten för samhällsskydd och beredskap ska hålla Regeringskansliet (Försvarsdepartementet) fortlöpande informerat under uppdragets genomförande.

Uppdragen ska redovisas senast 1 mars 2011 till Regeringskansliet (Försvarsdepartementet).

Ärendet

Att myndigheterna och andra offentliga aktörer kan kommunicera på ett säkert sätt är en förutsättning för god nationell informationssäkerhet och möjligheten att hantera allvarliga IT-incidenter eller andra allvarliga störningar. I det svenska samhället behövs en administrativ och teknisk infrastruktur vid kriser och olyckor för informationsdelning och respons i vid mening, där samtliga aktörer av betydelse för samhällets kritiska informationsinfrastruktur finns representerade. Infrastrukturen ska fungera under normala förhållanden men ska också innefatta en organisation och struktur som kan fungera som stöd under allvarliga störningar och kriser. En sådan stödorganisation och infrastruktur behöver ha en hög informationssäkerhet för att inte slås ut vid allvarliga störningar. För att bli kostnadseffektiv och för att på bästa sätt ta vara på befintlig kompetens och organisation ska det övervägas att låta infrastrukturen bygga på nuvarande teknisk struktur. En övergång från normalläge till krisläge ska inte innebära stora förändringar vad gäller aktörer och arbetssätt, eftersom det bedöms försvåra och fördröja arbetet.

En nationellt digital informations- och kommunikationsinfrastruktur består sannolikt inte av ett enskilt fysiskt nät utan av flera olika nät, där det finns en gemensam logisk tjänst, för säkert informationsutbyte med hög tillgänglighet som kan nyttjas av myndigheter och andra offentliga aktörer.

Myndigheten för samhällsskydd och beredskap har på regeringens uppdrag redovisat en rapport Åtgärder för att förbättra samhällets samlade förmåga att förebygga och hantera IT-incidenter (Fö2009/2162/SSK). Enligt rapporten är den rapportering av IT-incidenter som idag sker på frivillig basis otillräcklig för att kunna bidra till en löpande aktuell lägesbild av tillståndet vid samhällsviktig verksamhet och kritisk infrastruktur. Regeringen anger i budgetpropositionen för 2010 (prop. 2009/10:1, bet 2009/10:FöU1, rskr. 2009/10:104) att rapportering av IT-incidenter som utgör hot mot eller medför allvarliga konsekvenser för samhällsviktig verksamhet och kritisk infrastruktur behöver förbättras.

Hot mot verksamheter och tillgångar kan antingen vara antagonistiska eller oavsiktliga som exempelvis naturolyckor och tekniska fel. Sårbarheter, som fallerande skydd och bristande rutiner, bidrar till att hot realiseras. Regeringen ser därför ett behov av att ha en aktuell och relevant uppfattning om hot, sårbarheter och risker på samt trender och tendenser på informationssäkerhetsområdet.

På regeringens vägnar

Sten Tolgfors

Linda Ericson

Kopia till

Statsrådsberedningen/SAM
Justitiedepartementet/PO
Justitiedepartementet/Gransk
Justitiedepartementet/L4
Utrikesdepartementet/FIM
Finansdepartementet/BA
Finansdepartementet/SF
Finansdepartementet/SKA
Näringsdepartementet/ITP
Rikspolisstyrelsen

Säkerhetspolisen
Försvarsmakten
Försvarets materielverk
Försvarets radioanstalt
Totalförsvarets forskningsinstitut
Skatteverket
Post och telestyrelsen
Sveriges kommuner och landsting
Delegationen för e-förvaltning

Bilaga B: Uppdragets organisation

Styrning

Richard Oehme, chef för Enheten för samhällets informationssäkerhet, ROS-ISÄK, vid MSB

Projektgrupp

Representant	Organisation	Uppgift
Jonny Nilsson	PTS	Projektledare
Anders Wik	Fd. FRA	Sakkunnig
Arne Jonsson	MSB	Sakkunnig
Håkan Simonsson	SAAB Group	Sekreterare

Följande personer vid Enheten för samhällets informationssäkerhet har även medverkat i arbetet med att författa denna rapport: Helena Andersson, Dr. Åke J. Holmgren, Svante Nygren och Richard Oehme.

Samrådsgrupp i enlighet med regeringens uppdrag

Organisation	Representant
SÄPO*	Henrik Christiansson
FMV*	Ola Winberg
FRA*	Cecilia Laurén Stefan Karlsson
PTS*	Ove Landberg
FOI	Christian Jönsson
e-delegationen	Anneli Hagdal t.o.m 2010-12-31 Peter Krantz fr.o.m 2011-01-01
Skatteverket	Teijo Mattila

* Myndigheter som ingår i Samverkansgruppen för informationssäkerhet, SAMFI

Myndigheterna i samverkansgruppen för informationssäkerhet (SAMFI) har fortlöpande delgivits information om uppdraget vid reguljära möten.

Referensgrupp

En referensgrupp bildats med de myndigheter som ingår i samrådsgruppen kompletterade med för uppdraget relevanta organisationer.

Organisation	**Representant**
Försvarsmakten	Rickard Stridh Kim Hakkarainen Pia Gruvö
SÄPO	Henrik Christiansson
FMV	Ola Winberg
FRA	Stefan Karlsson Cecilia Laurén
PTS	Ove Landberg
FOI	Christian Jönsson
e-delegationen	Anneli Hagdal t.o.m 2010-12-31 Peter Krantz fr.o.m 2011-01-01
Skatteverket	Teijo Mattila
Trafikverket	Ola Barthel
Svenska kraftnät	Alireza Hafezi
Länsstyrelsen i Västra Götalands län	Mats Lilienberg Göran Svensson
Landstinget i Östergötland	Lars-Åke Pettersson
Karlskrona kommun	Anders Danielsson

Referensgruppen har samlats vid tre tillfällen.

Bilaga C: Förkortningar och begrepp

CERT (Computer Emergency Response Team) – Funktion för incidenthantering.

CERT-SE – Den svenska nationella CERT-funktionen vid MSB

Clean pipe - Benämningen på ett kommersiellt nätverksbaserat koncept för skyddad anslutning till Internet.

DNS – Domän Namn System, ett system för att förenkla adressering av datorer på IP-nätverk som till exempel Internet

E-delegationen– en expertgrupp som Sveriges regering inrättat för att leda och samordna arbetet med målet att förenkla för medborgare och företag att utöva sina rättigheter och fullgöra sina skyldigheter samt ta del av förvaltningens service.

FDF (Funktion för drift och förvaltning) – I denna rapport förslag på funktion för drift och förvaltning av den statligt kontrollerbara kommunikationsinfrastrukturen

FOI – totalförsvarets forskningsinstitut

FM – Försvarsmakten

FMV – Försvarets materielverk

FRA – Försvarets radioanstalt

FSI (Funktion för strategisk inriktning) –I denna rapport förslag till funktion för bl.a. samordning och inriktning samt upphandlingsstöd

GovNet (Governmental Network) – En gemensam, skyddad informations- och kommunikationsinfrastruktur för myndigheter eller för offentlig sektor.

ICT – Information and Communication Technology, jämför med IKT

IKT – Informations och Kommunikations Teknologi, det svenska begreppet för ICT.

ISP – Internet Service Provider, en teleperatör som tillhandahåller Internetkoppling till en privatkund eller en organisation

KBF – Krisberedskapsförordningen: förordning (2006:942) om krisberedskap och höjd beredskap

MSB – Myndigheten för samhällsskydd och beredskap

NOS (Nationell operativa samverkansfunktionen för informationssäkerhet) – en samverkansform som inrättats av MSB. NOS

syftar till att skapa en förbättrad förmåga i samhället att hantera allvarliga IT-incidenter.

PTS – Post- och telestyrelsen

Rakel – Gemensamt radiokommunikationssystem för organisationer i samhället som arbetar med allmän ordning, säkerhet eller hälsa.

RPS – Rikspolisstyrelsen

RSA – Risk- och sårbarhetsanalys

SAMFI (Samverkansgruppen för informationssäkerhet) – Gruppen består av Försvarets materielverk, Försvarets radioanstalt, Försvarsmakten, MSB, Post- och telestyrelsen, Rikspolisstyrelsen samt Säkerhetspolisen.

SGSI (Swedish Government Secure Intranet) – Nättjänst som inte är beroende av Internet och till vilken svenska myndigheter kan ansluta sig och kommunicera med varandra samt med EU:s institutioner och organ.

SIA (Skyddad Internetanslutning) - I denna rapport ett koncept för skyddad anslutning till Internet för offentlig verksamhet

Sitic (Sveriges incidentcentrum) – Den svenska CERT-funktionen. Drivs av MSB från 1 januari 2011 under namnet CERT-SE.

Skydd – Effekt av handlingar, rutiner och tekniska arrangemang som syftar till att minska sårbarheten

SvK – Svenska kraftnät

Säkra kryptografiska funktioner – Kryptosystem som är nationellt godkända för att skydda både hemliga och skyddsvärda uppgifter. Kryptolösningar finns hos samtliga i kapitel 3 utpekade myndigheter för att skydda samtal, faxöverföring, datafiler, videokonferens eller hela nätverk.

Säpo – Säkerhetspolisen

Tillgänglighet – Skyddsmål där informationstillgångar skall kunna utnyttjas i förväntad utsträckning och inom önskad tid

TrV – Trafikverket

TrV ICT – Trafikverket, organisatorisk enhet vid Trafikverket inom området Informations- och kommunikations teknologin, Information and Communication Technology,

VPN – Virtuellt Privat Nät, en teknik som används för att skapa säkra förbindelser, så kallade *tunnlar*, mellan två punkter i ett osäkert datanätverk (såsom Internet).

VY-verkko – En gemensam skyddad kommunikationslösning för finska statsförvaltningen

WIS (Webbaserat informationssystem) – Ett nationellt webbaserat informationssystem som används för informationsdelning mellan aktörerna i det svenska krishanteringssystemet före, under och efter en kris.

Bilaga D: Myndigheter som är utpekade i bilagan till KBF

UTPEKADE MYNDIGHETER ENLIGT 11 § KBF	
Samverkansområden	***Myndigheter med särskilda uppgifter inom samverkansområdena***
Teknisk infrastruktur	Affärsverket svenska kraftnät
	Elsäkerhetsverket
	Myndigheten för samhällsskydd och beredskap
	Post- och telestyrelsen
	Statens energimyndighet
	Livsmedelsverket
Transporter	Sjöfartsverket
	Statens energimyndighet
	Trafikverket
	Transportstyrelsen
Farliga ämnen	Kustbevakningen
	Livsmedelsverket
	Myndigheten för samhällsskydd och beredskap
	Rikspolisstyrelsen
	Smittskyddsinstitutet
	Socialstyrelsen
	Statens jordbruksverk
	Statens veterinärmedicinska anstalt
	Strålsäkerhetsmyndigheten
	Tullverket
Ekonomisk säkerhet	Finansinspektionen
	Försäkringskassan
	Pensionsmyndigheten
	Riksgäldskontoret
	Skatteverket
Geografiskt områdesansvar	Länsstyrelserna
	Myndigheten för samhällsskydd och beredskap
Skydd, undsättning och vård	Kustbevakningen
	Myndigheten för samhällsskydd och beredskap
	Rikspolisstyrelsen
	Sjöfartsverket
	Socialstyrelsen
	Transportstyrelsen
	Tullverket

I samverkansområdena deltar fler myndigheter än de som av regeringen har ett särskilt utpekat ansvar enligt krisberedskapsförordningen (för närvarande Försvarsmakten, FRA, Fortifikationsverket, Lantmäteriet, SMHI och FOI).

Bilaga E: Infrastruktur i Sverige

I denna bilaga beskrivs hur de etablerade kommunikationsinfrastrukturer i Sverige, med dess aktörer, ser ut.

Kommersiell infrastruktur

Internetoperatören (Internet Service Provider, ISP) erbjuder en uppsättning tjänster i enlighet med ett avtal som upprättats mellan operatören och slutanvändaren. Kommersiellt ansvarar operatören för tjänstens utformning och kvalitet gentemot användaren.

För att realisera tjänsten tillförsäkrar sig operatören en teknisk infrastruktur antingen genom egna investeringar i utrustning och organisation eller genom att i sin tur upprätta avtal med leverantörer för hela eller delar av den tekniska infrastrukturen. Det finns i Sverige idag flera hundra operatörer med varierande grad av egen ägd infrastruktur. Det finns också en omfattande del av branschen som helt eller i huvudsak erbjuder delar av infrastrukturen till de operatörer som efter vidareförädling säljer tjänsterna till slutanvändarna.

De lägre nivåerna i infrastrukturens hierarki, till exempel kanalisation för kablar med fiber eller koppar, radio och transmissionssystem som används för Internettrafik, nyttjas i de flesta fall även för trafik för andra tillämpningar som fast och mobil telefoni. De flesta ISP:er använder idag, helt eller delvis, underleverantörer för att realisera denna den av infrastrukturen.

Ytterligare en typ av aktör är företag som specialiserar sig på att etablera specifika datormiljöer där operatörer kan samlokalisera. Detta blir allt vanligare då man eftersträvar stordriftsfördelar för att minska kostnaderna.

Statlig infrastruktur

Det finns flera statliga ägare av infrastruktur i Sverige vilka presenteras kort nedan.

Trafikverket ICT

Trafikverket ICT levererar nätkapacitet genom ett rikstäckande 12 000 km fibernät som är förlagt i landets banvallar och i viss mån vägar. Trafikverkets nät täcker stora delar av Sverige i över 900 orter. I princip finns två fysiskt skilda förbindelsevägar till varje ort. Fibernätet är öppet för andra operatörer och tjänsteleverantörer och för större företag. Genom samarbetet med lokala accessägare, stadsnät, kan tillgång till sammankopplingar och förbindelser erbjudas till i stort sett alla orter i landet.

Trafikverket erbjuder i dag tjänsterna kapacitet, bandbredd från 2 Mbit/s till 10 Gbit/s, IP-transport och Ethernet med överföringskapacitet från 10 Mbit/s till 10Gbit/s. Nätet och tjänsterna karaktäriseras av hög kapacitet, nätstrukturen ger goda möjligheter att skapa robust nät, det är sammanknutet med flera skyddade knutpunkter samt att det har visst fysiskt skydd.

Teracom

Teracoms nät är i huvudsak uppbyggt med radiolänkteknik. Radiolänknätet används i huvudsak för att distribuera radio och tv-sändningar. Viss överkapacitet hyrs ut till kunder utanför kretsen av rundradio. Teracom finns etablerat på över 600 orter.

Teracom erbjuder i dag tjänsterna kapacitet och IP-transport. Bandbredden för tjänsterna är begränsande, svartfiber är ej tillgängligt.

Svenska Kraftnät

Svenska Kraftnät, SvK, har ett landsomfattande fibernät installerat i SvK:s kraftledningar. Nätet, som totalt är ca 8 500 km långt, består av cirka 6 000 km egen optisk fiber och 2 500 km inhyrd fiber. Det fiberoptiska nätet utgör stommen i det nät som används för att styra och övervaka det svenska kraftnätet. Nätet har god tillgänglighet och robusthet. Det är byggt i ringstrukturer och större noder är redundanta.

Överskottskapaciteten i nätet hyrs ut, framförallt i form av svartfiber, till externa operatörer. SvK:s telenät är helt separerat från övriga telenät i samhället.

Den så kallade fibertriangeln, som förbinder storstadsregionerna Stockholm – Oslo – Göteborg – Malmö – Köpenhamn – Stockholm, drivs av ett separat bolag, Triangelbolaget, där SvK äger 25 %.

SvK erbjuder tjänsterna svartfiber (där det finns överkapacitet i befintliga fiberkablar) och kapacitet till nätägare inom energibranschen.

Nätet karaktäriseras av hög kapacitet och med ringstruktur. Nätet är beroende av elnätets infrastruktur.

Övriga infrastrukturer

Exempel på övriga etablerade infrastrukturer på nationell nivå för behov som finns inom offentlig sektor:

SGSI

Swedish Government Secure Internet, SGSI, är ett skyddat kommunikationsnät som ursprungligen etablerades för kommunikation mellan Svenska myndigheter och med EU-myndigheter. Nätet är utformat för att klara höga krav på tillgänglighet och skydd. Trafiken i nätet är krypterad med ett nationellt godkänt kryptosystem. Endast myndigheter som uppfyller gemensamt fastställda säkerhetskrav får anslutas till nätet. SGSI är anslutet till EU-kommissionens kommunikationsnät s-TESTA (Secure Trans European Services for Telematics between Administrations). s-TESTA är ett skyddat nät för kommunikationen mellan EU:s medlemsstater och EU:s olika organisationer. SGSI uppfyller säkerhetskrav på EU Restricted-nivå. Nätet administreras på överordnande nivå av systemägaren MSB. RPS och FMLOG

ansvarar för drift av knutpunkt och krypteringsutrustning. Nätet är upphandlat av en leverantör.

LstNet

Länsstyrelsernas gemensamma datakommunikationsnät för kommunikation mellan länsstyrelserna samt cirka tjugo statliga myndigheter. Länsstyrelsen i Västra Götalands län ansvarar för drift, ekonomi och administration av nätet. Kraven är höga på tillgänglighet och skydd i LstNet. Känsliga applikationer skyddas med krypto. LstNet har redundant skyddad anslutning till publika nät. Nätet är upphandlat av en leverantör.

Sjunet

Sjunet är avsett för landsting, kommuner och privata vårdgivare med behov av informationsutbyte och skyddad kommunikation oberoende av organisatoriska och geografiska gränser. Sjunet garanterar hög tillgänglighet som ofta är ett krav för förmedling av verksamhetskritisk information. Tillgängligheten garanteras genom avtal med leverantörer samt genom säkerhetsarkitekturen. Sjunet är inte anslutet till Internet. Ett gemensamt regelverk för de organisationer som ansluts till Sjunet skapar tillit. För anslutning till Sjunet krävs ett avtal med systemägaren, Inera AB, som ägs gemensamt av landsting och regioner. Nätet är upphandlat av en leverantör.

FMIP

Försvarsmaktens IP-nät erbjuder Försvarsmakten samt vissa samverkande myndigheter skyddade kommunikationstjänster. Nätets robusthet är specifikt anpassad för Försvarsmaktens krav. Trafiken i nätet krypteras med nationellt godkända kryptosystem. Försvarsmakten är systemägare.

Rakel

Rakelsystemet är ett nationellt digitalt radiokommunikationssystem för samverkan och ledning. Det har byggts ut i hela Sverige för att stärka samhällets krishanteringsförmåga och för att underlätta den dagliga kommunikationen hos organisationer som arbetar med allmän ordning, säkerhet eller hälsa. Rakel bygger på den europeiska teknikstandarden Tetra som även används inom Sveriges grannländer. Det underlättar samarbete och räddningsinsatser över gränserna. Regeringskansliet samt tretton statliga myndigheter använder för närvarande Rakel. Länsstyrelser, Landsting, regioner och kommuner är på väg att anslutas till nätet. Tjänsteerbjudandet är specifikt anpassat för tidskritisk ledning baserad på tal- och textkommunikation. MSB är systemägare.