Statens servicecenter

Rapport

En gemensam statlig molntjänst för myndigheternas it-drift

Delrapport i regeringsuppdrag om samordning och omlokalisering av myndighetsfunktioner

Datum: 2017-02-07
Diarienummer: 10052-2016/1121
Rapportnummer: R:001
ISBN: 978-91-88631-00-8 (tryckt)
978-91-88631-01-5 (PDF)
Tryckeri: Ale tryckteam, Bohus

Statens servicecenter
FE 15
801 71 Gävle

Telefon: 0771-456 000
E-post: registrator@statenssc.se
www.statenssc.se

Statens servicecenter

MISSIV

Datum
2017-01-30

Dnr
10052-2016/1121

Er beteckning
Fi2016/00274/SFÖ (delvis)

Regeringen
Finansdepartementet
103 33 Stockholm

Uppdrag till Statens servicecenter rörande samordning och omlokalisering av myndighetsfunktioner

Statens servicecenter fick den 28 januari 2016 i uppdrag av regeringen att analysera och föreslå vilka myndighetsfunktioner som kan vara lämpliga att bedriva samordnat inom staten och utanför storstadsområden. Enligt regeringens beslut ska uppdraget slutredovisas till regeringen (Finansdepartementet) senast den 15 april 2017.

Statens servicecenter överlämnar härmed delrapporten *En gemensam statlig molntjänst för myndigheternas it-drift*.

Detta ärende har avgjorts av generaldirektören Thomas Pålsson efter föredragning av projektledaren Anders Hedberg. Vid den slutliga handläggningen av ärendet har även rättschefen Gustaf Johnssén medverkat.

Thomas Pålsson

Anders Hedberg

Postadress
Statens servicecenter
FE-15
801 71 Gävle

Telefon
0771-456 000

E-post
registrator@statenssc.se

Webbplats
www.statenssc.se

Innehållsförteckning

Bilagor

Sammanfattning

Statens servicecenter har i uppdrag från regeringen att analysera och föreslå vilka myndighetsfunktioner som kan vara lämpliga att bedriva samordnat inom staten och utanför storstadsområden. Uppdraget gäller främst myndighetsfunktioner där det finns möjligheter till stordriftsfördelar, effektiviseringar och kvalitetsförbättringar genom samordning och koncentration. Som en del i uppdraget har förutsättningarna för att skapa en samordnad eller gemensam funktion för delar av statliga myndigheters it-verksamhet analyserats.

En statlig molntjänst bör införas

Statens servicecenter föreslår att merparten av de statliga myndigheternas it-drift bör samordnas i en statlig molntjänst.

En molntjänst är en it-tjänst som tillhandahålls via internet. Motsatsen är de traditionella it-tjänsterna där användaren själv står för inköp av kapacitet, installation, drift, underhåll och utveckling. Molntjänster levererar samma innehåll till användaren som de traditionella it-tjänsterna. Skillnaden är att det enda molntjänsten kräver av användaren är en internetuppkoppling. Alla övriga investeringar ligger hos molntjänstleverantören.

Den statliga molntjänst Statens servicecenter föreslår kommer att erbjuda myndigheterna två tjänster: datorkraft och lagring. För anslutna myndigheter kommer tjänsten att vara helt skalbar och flexibel. Beställning av kapacitet kommer att vara fullt automatiserad.

Den statliga molntjänsten bör till stora delar placeras utanför storstadsområdena

Statens molntjänst bör ha sitt säte utanför storstadsområdena. Dess utvecklingsverksamhet bör förläggas till två orter med stor geografisk distans. Dessutom behövs högst tio datacenter för att driva statens molntjänst. Merparten av dessa bör av säkerhetsskäl placeras i bergrum utanför storstadsområdena.

När statens molntjänst byggs upp bör statens befintliga bergrum, fibernät m.m. användas. Det är effektivt i kostnads-, resurs- och säkerhetshänseende. Statens molntjänst ska också vara helt leverantörsoberoende. Som utgångspunkt bör all programvara ha öppen källkod.

Statens molntjänst kan lämpligen inrättas inom ramen för en befintlig myndighet eller som en ny myndighet. Frågan om organisationsform behöver utredas vidare.

Idag krävs cirka 800 årsarbetskrafter för drift och underhåll av myndigheternas egna datacenter, vilka kommer att avvecklas när statens molntjänst inrättas. För drift och underhåll av statens molntjänst kommer det däremot att endast krävas 200 årsarbetskrafter. Dessa ca 200 arbetstillfällen kommer huvudsakligen att skapas utanför Stockholmsområdet. Dygnet runt under årets alla dagar ska det finnas utvecklare och datacentertekniker på plats på de två orter dit utvecklingsverksamheten förläggs.

En statlig molntjänst skulle hantera många av utmaningarna för myndigheternas it-drift

Idag ansvarar varje statlig myndighet för sin egen it-verksamhet och driften av denna. Det innebär att onödigt stora resurser binds upp i kapital och personal i form av bl.a. hårdvara, redundans, utspridda upphandlingar och drifttekniker. De statliga myndigheterna äger också sammantaget mer än 200 datacenter, som i hög grad är koncentrerade till Stockholm. Det är både sårbart och kostsamt. Eftersom investeringar i en tillräckligt hög it-säkerhet kan upplevas som alltför kostsamt för enskilda myndigheter varierar också it-säkerheten mycket inom statsförvaltningen. Liksom Sverige i stort utsätts också myndigheterna allt mer för cyberangrepp och underrättelseverksamhet mot offentlig it-infrastruktur, vilket underlättas av brister i säkerheten. Särskilt stora säkerhetsrisker kan uppstå när it-drift läggs ut på privata företag.

Att inrätta en statlig molntjänst där merparten av de statliga myndigheternas it-drift samordnas, skulle enligt Statens servicecenter hantera många av dessa utmaningar. Förslaget skulle medföra:

- *Stora besparingar för statskassan*. Tio år efter att statens molntjänst har tagits i drift gör Statens servicecenter bedömningen att de anslutna myndigheternas årliga kostnader för it-drift kommer att vara 30 procent lägre än 2016. Genom att det jämfört med idag kommer att krävas väsentligt färre it-tekniker för att sköta systemen i statens molntjänst bör staten som helhet kunna spara in ca 600 årsarbetskrafter på sådana arbetsuppgifter. Övertaligheten kommer till stor del att uppstå i Stockholmsområdet där det bör finnas goda möjligheter för de berörda att finna nytt arbete.
- *Kraftigt reducerad miljöpåverkan*. Statens molntjänsts datacenter kommer att byggas upp med modern, miljövänlig teknik, och sammantaget ta betydligt mindre lokalytor i anspråk än de dryga 200 datacenter som idag finns i statsförvaltningen. Sammantaget kommer det att medföra en betydande minskning av elförbrukningen för statens it-verksamhet.
- *Enklare för myndigheterna*. De myndigheter som är anslutna till statens molntjänst kommer inte längre att behöva upphandla sin it-drift, vilket innebär kortare ledtider och lägre administrativa kostnader. Statens molntjänst kommer också att i varje givet ögonblick kunna erbjuda myndigheterna den fulla it-kapacitet som de kräver.
- *IT-säkerheten och driftsäkerheten förstärks kraftigt*. Med statens molntjänst kommer it-säkerheten för hela statsförvaltningen att bli mycket hög och utan kompromisser. Likaså kommer driftsäkerheten i statens molntjänst att uppnå en långt högre nivå än vad många myndigheter eller svenska företag i dagsläget är i närheten av.

Sammantaget ser Statens servicecenter alltså en rad fördelar med att samordna merparten av de statliga myndigheternas it-drift i en statlig molntjänst. Det finns också osäkerheter med en sådan förändring, till exempel att staten skulle vidta ett omfattande projekt med viss risk och som medför en relativt stor investering. Bedömningen är dock att fördelarna klart överväger osäkerheterna, i synnerhet i ljuset av de nackdelar som finns med dagens decentraliserade modell för it-verksamheten i staten.

En statlig molntjänst i myndighetsform förordas av många myndigheter

Många statliga myndigheter efterfrågar en samordnad, dynamisk och flexibel it-drift, med fördel organiserad som en statlig molntjänst. Det visar både tidigare studier och möten som Statens servicecenter har haft med 15 av de större myndigheternas it-ledningar. Flera av de tillfrågade myndigheterna anser att statens molntjänst bör inrättas som en statlig myndighet med endast denna uppgift. Även Försvarets radioanstalt har framfört att staten bör bygga en egen molntjänst, med egna statliga datacenter där samtliga relevanta it-säkerhetskrav kan tillgodoses fullt ut.

Samordning av statlig it-drift är också en allmän trend i västvärlden. Flera andra länder, bl.a. Danmark, Finland och Nederländerna, har de senaste åren konsoliderat och samordnat it-verksamheten i staten.

Behov av fortsatt utredningsarbete

Statens servicecenter bedömer att det kommer att ta upp till fem år att införa statens molntjänst från det att regeringen fattar beslut om införandet. Innan statens molntjänst kan inrättas behövs fortsatt utredningsarbete. Det bör bedrivas i två steg.

I steg 1 bör regeringen i närtid initiera ett uppdrag att närmare analysera förutsättningarna för att inrätta statens molntjänst, som underlag inför ett beslut om detta. Utredningen bör utgå från föreliggande rapport. I uppdraget bör ingå att bl.a. närmare analysera lämplig verksamhetsform för den statliga molntjänsten och dess ansvarsområde och uppgifter, juridiska förutsättningar, lämplig takt för att samordna myndigheternas it-drift i en statlig molntjänst och om det ska vara obligatoriskt för myndigheter att ansluta sig till molntjänsten. Även finansieringsfrågor bör ingå i uppdraget. Statens servicecenter menar att statens molntjänst bör vara helt avgiftsfinansierad i drift, men under dess uppbyggnadsfas, dvs. de första fem åren, krävs sannolikt anslagsfinansiering.

I steg 2 behövs mer praktiskt genomförandearbete för att inrätta statens molntjänst. Efter att regeringen har beslutat att statens molntjänst ska inrättas, bör regeringen ge den ovan nämnda utredningen i uppdrag att genomföra bildandet av den nya tjänsten och dess organisation. I uppdraget bör bl.a. ingå att fastställa dimensionering, inklusive bemanning, att beräkna dimensioneringens budgetära konsekvenser och att belysa uppstartskostnader, besparingar och rationaliseringar samt avvecklingskostnader. Även i detta steg torde finansieringsfrågor aktualiseras.

1 Inledning

1.1 Uppdraget

Regeringen har gett Statens servicecenter i uppdrag att analysera och föreslå vilka myndighetsfunktioner som kan vara lämpliga att bedriva samordnat inom staten och utanför storstadsområdena. Uppdraget gäller främst myndighetsfunktioner där det finns möjligheter till stordriftsfördelar, effektiviseringar och kvalitetsförbättringar genom samordning och koncentration.

I delrapporten *Samordning och omlokalisering av myndighetsfunktioner*, som lämnades till regeringen den 1 juni 2016, identifierades ett tiotal myndighetsfunktioner rörande olika typer av verksamhetsstöd som kan vara lämpliga att koncentrera och omlokalisera. Bland de funktioner som bedömdes intressanta och prioriterade att utreda vidare fanns en samordnad eller gemensam funktion för delar av statliga myndigheters it-verksamhet.[1]

Mot bakgrund av detta har Statens servicecenter analyserat hur de delar av it-verksamheten som i princip samtliga statliga myndigheter bedriver på ett likartat sätt kan omlokaliseras och samordnas till en statlig aktör i en statlig molntjänst. Syftet är att för staten som helhet uppnå effektivisering, omlokalisering och ett gemensamt säkerhetsperspektiv för statlig it-verksamhet. Se rapportens bilagor 2 och 5 för en närmare beskrivning av molntjänster.

1.2 Bakgrund

Under de senaste fem åren har ett flertal utredningar gjorts om hur olika delar av statsförvaltningen bedriver sin it-verksamhet. Frågor som har behandlats är till exempel vad it-verksamheten kostar, dess leverantörsberoenden och vilka framtida utmaningar den står inför. Tidigare utredningar redogörs för närmare i kapitel 2.

Generella slutsatser från dessa utredningar är att det finns en stor vilja till att förbättra statsförvaltningen med hjälp av IT samt att statens it-kostnader är avsevärda. Det finns ett flertal problem och utmaningar som behöver hanteras, till exempel att:

- samordningen stundtals är bristfällig,
- det finns en stor inlåsning till enskilda leverantörer,
- myndigheternas beställarkompetens är låg, och att
- upphandlingsprocessen skapar hinder.

[1] Statens servicecenter (2016) *Samordning och omlokalisering av myndighetsfunktioner – delrapport juni 2016*.

Flera utredningar pekar på att inrättandet av en gemensam funktion för delar av statliga myndigheters it-drift skulle kunna hantera många av dessa utmaningar, förslagsvis i form av en gemensam molntjänst.

1.3 Tillvägagångssätt

Vid en analys av förutsättningarna för att eventuellt inrätta en statlig molntjänst finns det många och olikartade perspektiv som behöver beaktas. Det handlar till exempel om geografisk placering, fysisk säkerhet, tillgång till säker elförsörjning och säker datakommunikation, it-säkerhet, kompetens, lagstiftning, stabilitet vid olika katastrofer och val av hårdvaror och programvaror.

I utredningen har Statens servicecenter därför genomfört ett antal aktiviteter för att utreda möjligheterna för en statlig molntjänst. I huvudsak handlar det om fyra aktiviteter, som har bedrivits parallellt:

- En enkät riktad till samtliga myndigheter under regeringen, som genomfördes under september och oktober 2016.
- Dialogmöten med företrädare för it-avdelningarna (it-chefer m.fl.) vid 15 av de största myndigheterna.
- Analys av tidigare utredningar.
- Arbetsmöten med teknisk expertis inom molntjänster.

Vidare har utredningens frågeställningar diskuterats med representanter för ett antal andra myndigheter som utifrån sina myndighetsuppdrag är direkt berörda av frågan om en statlig molntjänst. Dessa myndigheter är Arbetsgivarverket, Datainspektionen, Försvarets radioanstalt (FRA), Konkurrensverket, Myndigheten för samhällsskydd och beredskap (MSB), Post- och telestyrelsen (PTS) samt Affärsverket svenska kraftnät.

Statens servicecenter har även rådfrågat Sunet (Vetenskapsrådet) om deras erfarenheter av storskalig it-infrastruktur och SICS[2] om deras forskning rörande säkerhet, virtualisering och molntjänster.

Vidare har idén om en statlig molntjänst och delar av enkätsvaren presenterats för generaldirektörerna för de myndigheter som ingår i e-samverkansprogrammet. Det skedde vid ett möte den 1 december 2016. Som ett led i att kvalitetssäkra uppdraget har utredningsfrågorna även stämts av med referenspersoner med lång erfarenhet av att leda och styra stora statliga myndigheter. Denna referensgrupp har letts av Statens servicecenters generaldirektör Thomas Pålsson och har i övrigt bestått av Göran Ekström, tidigare generaldirektör för Arbetsgivarverket, Thomas Rolén, kammarrättspresident, Kammarrätten i Stockholm samt Mats Sjöstrand, tidigare generaldirektör för Skatteverket.

[2] Swedish Institute of Computer Science.

Säkerhetschefen Lars Grundström har deltagit i utredningen i egenskap av expert i frågor rörande informations- och cybersäkerhet samt säkerhetsskydd.

Projektledare för arbetet har varit Anders Hedberg och Daniel Melin har varit utredningssekreterare.

1.4 Avgränsningar

Statens servicecenter har inte utrett hur myndigheter under riksdagen, affärsdrivande verk (med undantag för kontakter med Svenska kraftnät), statliga bolag, landsting eller kommuner förhåller sig till en statlig molntjänst.

Statens servicecenter har inte berört eller undersökt vilka applikationer olika myndigheter nyttjar i sin verksamhet. Då syftet endast har varit att se på drift och ägande av den fysiska infrastrukturen ligger sådana frågor utanför uppdraget. Därtill är det respektive myndighets ansvar att inom sin utövning ha de applikationer de behöver.

1.5 Definitioner

Datacenter

Fysisk anläggning för servrar, lagring och kommunikationsutrustning med kyla, elförsörjning och skalskydd.

Molntjänst

En generell beskrivning av en molntjänst är en tjänst som inkluderar drift, övervakning, hårdvara, programvara, lagring, säkerhetskopiering, bandbredd, säkerhet och support. De egenskaper som är typiska för en molntjänst är:

- Tillhandahålls över internet.
- Standardiserad – Tjänsten kan användas av olika användare utan att behöva anpassas särskilt till varje användare, dvs. till sin funktion är tjänsten principiellt likadan för samtliga kunder.
- Skalbarhet – Tjänsten tillåter att prestanda, lagringsmängd, nyttjandegrad o. dyl. snabbt och enkelt kan öka eller minska efter användarens önskemål.
- Enkelhet – Kräver ingen investering i hårdvara eller programvara från användarens sida.
- Tillgänglighet – Tjänsten skapas samtidigt på ett flertal geografiska platser vilket skyddar mot olika hot, avbrott och hinder.

En mer detaljerad redogörelse av molntjänster finns i rapportens bilagor 2 och 5.

Programvara med öppen källkod och proprietär programvara

Med öppen källkod avses en programvara som är licensierad med en licens där de med upphovsrätten till programvaran frånsäger sig vissa legala rättigheter. Detta innebär att

alla som får en kopia av programvaran erhåller rätten att t.ex. ändra, förbättra och kopiera programvaran till vem som helst.

En proprietär programvara har en licens där den som får en kopia av programvaran endast erhåller en nyttjanderätt till programvaran och typiskt är förbjuden att ändra eller kopiera programvaran eller att ta del av programmets källkod.

Redundans

Redundans innebär att funktioner och system dubbleras för att skydda information från störningar och avbrott. Det kan i detta sammanhang t.ex. handla om att spara samma information på två olika platser för att skydda den mot brand och liknande händelser eller att ha två anslutningar till internet för att säkerställa drift även om exempelvis en kabel grävs av.

Server – fysisk och virtuell

En fysisk server är en dator som är placerad i ett datacenter och har som uppgift att köra en central programvara som i sin tur betjänar olika klientdatorer. En server kan också, genom virtualisering, vara värd för virtualiserade servrar. Virtualisering skapas genom en programvara på en fysisk server som delar upp denna i logiska bitar. Varje logisk bit kommer därefter att se ut som en fysisk server för operativsystemet.

Öppna standarder

En öppen standard är enligt e-delegationen (SOU 2009:86) och Statens inköpscentral vid Kammarkollegiet en standard som uppfyller de fyra kriterier som anges i EU:s interoperabilitetsramverk EIF 1.0.[3]

1. Standarden är fastslagen och underhålls av en icke-vinstdrivande organisation och dess fortsatta utveckling sker enligt en öppen beslutsprocess öppen för alla intressenter (konsensus eller majoritetsbeslut etc.).
2. Standarden är publicerad och dess specifikation är tillgänglig antingen kostnadsfritt eller till självkostnadspris. Specifikationen ska vara tillåten att kopiera, distribuera och nyttja antingen kostnadsfritt eller till självkostnadspris.
3. Immaterialrätt kopplad till standarden, t.ex. patent, ska oåterkalleligen tillhandahållas utan krav på ersättning.
4. Det ska inte finnas några begränsningar för användningen eller återanvändningen av standarden.

Internet är exempelvis byggt med öppna standarder som IP, TCP, HTTP och DNS. För dokument är t.ex. PDF och ODF vanliga öppna standarder.

[3] http://ec.europa.eu/idabc/servlets/Docd552.pdf

1.6 Rapportens disposition

Den fortsatta framställningen har disponerats på följande sätt.

I *kapitel 2* redogörs för vad som har framkommit i tolv andra studier som på senare år har gjorts kring IT i statsförvaltningen samt ett antal andra relevanta rapporter.

I *kapitel 3* redovisas resultatet av enkäten till de statliga myndigheterna om hur de i dag hanterar sin it-drift och vilka resurser den förbrukar.

I *kapitel 4* redovisas vad som framkommit vid de dialogmöten Statens servicecenter under hösten 2016 har haft med företrädare för it-avdelningarna vid 15 av de största myndigheterna.

I *kapitel 5* redogörs för andra länders erfarenheter av att samordna statsförvaltningens it-drift.

Kapitel 6 innehåller Statens servicecenters överväganden och förslag.

Kapitel 7 redovisar förslagens konsekvenser.

Kapitel 8 redogör för behov av fortsatt utredningsarbete.

Till rapporten har sex bilagor fogats. Det handlar om regeringens uppdrag till Statens servicecenter (*bilaga 1*) samt ytterligare information om molntjänster i allmänhet (*bilaga 2*), om tidigare gjorda studier (*bilaga 3*), om enkäten (*bilaga 4*), om den tänkta statliga molntjänstens tekniska infrastruktur (*bilaga 5*) och om rättsliga förutsättningar (*bilaga 6*).

2 Tidigare studier

De senaste fem åren har ett brett spektrum av frågeställningar kring IT i statsförvaltningen analyserats i olika offentliga utredningar och av myndigheter, konsulter m.fl. I det följande sammanfattas väsentliga iakttagelser ur tolv sådana studier av betydelse för utredningen samt ett antal andra relevanta rapporter. En mer utförlig redogörelse för innehållet i de refererade studierna återfinns i bilaga 3.

2.1 Problem och utmaningar för statsförvaltningens IT

För de statliga myndigheterna, liksom för samhället i övrigt, är IT av avgörande betydelse för verksamheten. Många samhällsfunktioner är idag beroende av IT för att kunna fungera. Både hos det allmänna och inom näringslivet är en rad verksamheter helt beroende av digitala system för bl.a. styrning, reglering och övervakning.[4]

Någon helt uttömmande beräkning av statens specifika it-kostnader tycks inte föreligga. I en rapport från Ekonomistyrningsverket (ESV) uppskattas dock myndigheternas it-kostnader till 24–30 miljarder kronor per år.[5]

Vid utvecklingen av it-verksamheten behöver myndigheterna hantera flera – inte sällan svårförenliga – krav. Till att börja med måste de givetvis ha effektiva it-system som garanterar god service till medborgarna.

Vidare ska varje myndighet eftersträva hög effektivitet och god hushållning av statens medel i sin verksamhet. Varje myndighet har också ansvar för sin egen verksamhet och dess effektivitet.

Av effektivitetsskäl och ekonomiska skäl väljer, eller åtminstone överväger, många verksamheter idag åtgärder som utkontraktering när det gäller utveckling eller hantering av säkerhetskänsliga it-system. Utkontraktering kan ofta innebära att flera kunders system och information blandas samman i samma fysiska it-miljö vilket innebär att olika kunders information kan hamna i samma lagringsmiljöer, routrar och brandväggar. Av kostnadsskäl väljer leverantören inte sällan lösningar som leder till att system förs samman och virtualiseras.[6]

När samhället blir allt mer beroende av tekniska system måste dessa också vara tillräckligt säkra. En myndighet kan inte delegera ansvaret för sin egen säkerhet till andra.

---

[4] För en beskrivning av denna utveckling se t.ex. SOU 2015:25 *En ny säkerhetsskyddslag* och Riksrevisionen (2016) *Informationssäkerhetsarbete på nio myndigheter – En andra granskning av informationssäkerhet i staten*. RiR 2016:8.

[5] Ekonomistyrningsverket (2015) *Fördjupat IT-kostnadsuppdrag – Slutrapport: Förslag inför framtiden*. ESV 2015:64.

[6] Utvecklingen mot ökad utkontraktering beskrivs i ett flertal av de refererade studierna. Se t.ex. SOU 2015:25 *En ny säkerhetsskyddslag*, Myndigheten för samhällsskydd och beredskap (2015) *Informationssäkerhet – trender 2015* och *Säkerhetspolisens årsbok 2015*.

Även om den upplevda säkerheten i t.ex. en molntjänst kan vara hög så ersätter den inte den egna organisationens ansvar eller säkerhetsarbete.[7] Bl.a. Riksrevisionen har pekat på att myndigheternas arbete med informationssäkerhet ofta ligger på en otillräcklig nivå.[8]

Sammantaget är en slutsats av de refererade studierna att myndigheterna kläms mellan krav på effektiva it-system, låga kostnader, bättre service till medborgarna och hög säkerhet.

En annan svårighet är att myndigheterna vid utkontrakteringen av sina it-system och it-tjänster i allmänhet också måste hantera upphandlingen på egen hand. Till exempel har Riksrevisionen pekat på att viktig kunskap om utkontraktering av IT inte är tillräckligt spridd i statsförvaltningen som helhet. Det finns ingen naturlig drivkraft för myndigheter som genomfört utkontraktering att dela erfarenheterna med andra myndigheter, utan den myndighet som står inför ett ställningstagande kring en möjlig utkontraktering ”tvingas” enligt Riksrevisionen ofta uppfinna hjulet på nytt.[9] I en annan av de refererade studierna sägs också att samverkan mellan myndigheter ofta kan vara svårt beträffande it-lösningar då varken myndigheterna eller regeringen tydligt beslutat hur det ska göras i praktiken.[10]

Mot denna bakgrund är en slutsats av de refererade studierna att många myndigheter upplever det problematiskt att ompröva sin it-drift, och av de som kan och vill är det få som fullföljer p.g.a. frågeställningar kring bland annat säkerhet, personal och upphandling.

2.2 Ökade risker

Regeringen har beskrivit hur digitaliseringen påverkar alla delar av samhället och att digitaliseringens fördelar välkomnas. Samtidigt är de risker och hot den är förknippad med komplexa säkerhetsutmaningar. Några exempel på sådana utmaningar är antagonistiska hot såsom informationsoperationer och elektroniska angrepp mot skyddsvärda informations- och kommunikationssystem, t.ex. i form av dataintrång, sabotage eller spionage, mot totalförsvarets verksamhet. Hit hör också it-angrepp för att bedöma, påverka eller störa samhällsviktiga funktioner som ett förstadium till en väpnad konflikt. IT-angrepp riskerar också att otillbörligt påverka utgången av demokratiska val.[11]

---

[7] Myndigheten för samhällsskydd och beredskap (2015) *Informationssäkerhet – trender 2015*.

[8] Riksrevisionen (2016) *Informationssäkerhetsarbete på nio myndigheter – En andra granskning av informationssäkerhet i staten*. RiR 2016:8.

[9] Riksrevisionen (2011) *IT inom statsförvaltningen – har myndigheterna på ett rimligt sätt prövat frågan om outsourcing bidrar till ökad effektivitet?* RiR 2011:4.

[10] Gartner (2016) *Underlag till arbetet med förvaltningsansvar för gemensamma lösningar och förmågor avseende IT-drift och datorhallar*. På uppdrag av Näringsdepartementet/Regeringskansliet.

[11] Regeringen *Nationell säkerhetsstrategi* från 2017.

Genom att myndigheternas verksamheter alltmer blir beroende av digitala system, så ökar också behovet av säkerhetsfunktioner av olika slag. I ett flertal av de refererade studierna visas också att säkerhetshoten på flera sätt har ökat på senare år.[12] Samtidigt har dock inte it-säkerheten höjts i samma grad.

Den utveckling som beskrivs i de berörda rapporterna kan sammanfattas enligt nedan. Till största delen är resonemanget hämtat från SOU 2015:25 *En ny säkerhetsskyddslag*.

Den utbredda digitaliseringen medför effektivitetsvinster men samtidigt en påtagligt ökad sårbarhet för störningar och avbrott. På senare år har hoten mot rikets säkerhet ytterligare förändrats. Elektroniska angrepp i olika former betraktas som ett av de allvarligare hoten. Antalet it-angrepp ökar i omfattning och blir allt mera riktade och sofistikerade. Till exempel pekar alla tre säkerhetsmyndigheterna på att det blir allt vanligare med externa påverkansoperationer via olika typer av media samt verksamhet inom det så kallade ”cyberområdet” (inträngning i svenska IT- och ledningssystem).[13]

Ytterligare faktorer att beakta är att det sker en ökad koncentration till ett fåtal företag som tillhandahåller tjänster till myndigheter särskilt på it-området och att dessa därmed får tillgång till stora mängder information. Det kan medföra en ökad sårbarhet. Den samlade informationen kan bli mycket omfattande. En effekt av detta kan bli att uppgifter, som var för sig inte är skyddsvärda, i aggregerad form kan komma att utgöra en stor sårbarhet och därför kräva särskilda hänsyn från säkerhetsskyddssynpunkt.

Ett behov av att skydda systemen är idag påtagligt inom vissa för samhället kritiska sektorer. Teknikutvecklingen och it-samhället innebär också i andra avseenden ändrade förutsättningar för säkerhetsskyddet, t.ex. kan molntjänster försvåra arbetet med säkerhetsskyddsåtgärder.

Tekniken utvecklas ofta betydligt snabbare än säkerhetsarbetet. Den snabba utvecklingen på it-området i kombination med myndigheternas ökande användning av privatägd infrastruktur medför att myndigheternas egna tekniska kompetens minskar. Bristande kontroll över vilka it-produkter som tas in i svensk infrastruktur kan ge nya möjligheter för olika aktörer att inhämta information om och påverka nationella skyddsintressen och tillgångar av strategisk betydelse. Informationssäkerhet inklusive cybersäkerhet anses vara av såväl strategisk som utrikespolitisk och säkerhetspolitisk betydelse. En storskalig it-incident bedöms idag kunna få allvarliga konsekvenser såväl för ekonomisk som för samhällsviktig verksamhet och kritisk infrastruktur.

---

[12] Denna utveckling diskuteras i bl.a. SOU 2015:23 *Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten,* SOU 2015:25 *En ny säkerhetsskyddslag,* Myndigheten för samhällsskydd och beredskap (2015) *Informationssäkerhet – trender 2015*, Riksrevisionen (2016) *Informationssäkerhetsarbete på nio myndigheter – En andra granskning av informationssäkerhet i staten*. RiR 2016:8, samt årsrapporterna för 2015 från säkerhetsmyndigheterna Försvarets radioanstalt, Militära underrättelse- och säkerhetstjänsten och Säkerhetspolisen.

[13] Se årsrapporterna för 2015 från säkerhetsmyndigheterna Försvarets radioanstalt, Militära underrättelse- och säkerhetstjänsten och Säkerhetspolisen.

Även om de externa hoten ökar så är det också viktigt att komma ihåg att många it-incidenter och störningar i informationssystem har icke-antagonistiska orsaker. En inte ovanlig anledning till sådana it-incidenter är fel i programvara eller hårdvara. Andra orsaker kan vara exempelvis processbrister, bristande kvalitetskontroll, slarv, missbedömningar eller rena olycksfall. Störningar i stödsystem som t.ex. elförsörjning och kommunikation genom väderförhållanden och avgrävda kablar är också välkända orsaker till it-incidenter.

Myndigheternas arbete med och kunskap om informationssäkerhet är ofta för låg idag. Enligt Riksrevisionen är säkerhetsarbetet ofta inte implementerat i de ordinarie verksamhetsprocesserna. Det saknas till betydande delar delaktighet och ansvarstagande som bör genomsyra hela myndigheten, och det finns en bristande förståelse för behovet av säkerhetsinvesteringar utan synbar nytta.[14]

Även som beställare behöver myndigheternas kunskap och medvetenhet om säkerhetsaspekter öka. I sin trendrapport pekar MSB bl.a. på att utvecklingsprocessen måste ta hänsyn till säkerhetsaspekten genom hela processen, det går inte att bara skriva om säkerhet i en inledande kravspecifikation. Ett nära samarbete mellan systemutvecklare och experter på informationssäkerhet blir allt viktigare för att uppnå en god säkerhetsnivå. Enligt MSB bör också hela skalan av både enkla och sofistikerade hot och risker vägas in i riskanalysen som görs innan verksamhet utkontrakteras till underleverantörer eller data läggs i molntjänster.[15]

2.3 Molntjänster är en tänkbar lösning

Flera av de studerade rapporterna visar att molntjänster på många sätt har fördelar och kan avhjälpa vissa av de utmaningar myndigheter står inför. Till exempel pekar Gartner i ett uppdrag de gjort åt Näringsdepartementet på att många myndigheter vill ha en professionell extern leverantör som kan hantera t.ex. drift, lagring och virtualisering på ett mer flexibelt och snabbt sätt än deras interna it-verksamhet. Detta skulle då tvinga myndigheterna att bli mer standardiserade, få bättre uppföljning, bli mer professionella, mer effektiva samt eventuellt leda till lägre kostnader.[16]

Även Pensionsmyndigheten framhåller i en rapport att en myndighet som använder molntjänster kan styra om sina resurser mot utveckling och innovation i andra delar av verksamheten, exempelvis utveckling av nya tjänster för medborgare och företag. Myndigheten kan då dra nytta av att en molntjänstleverantör i kraft av sin stora skala och

[14] Riksrevisionen (2016) *Informationssäkerhetsarbete på nio myndigheter – En andra granskning av informationssäkerhet i staten*. RiR 2016:8.

[15] Myndigheten för samhällsskydd och beredskap (2015) *Informationssäkerhet – trender 2015*.

[16] Gartner (2016) *Underlag till arbetet med förvaltningsansvar för gemensamma lösningar och förmågor avseende IT-drift och datorhallar*. På uppdrag av Näringsdepartementet/Regeringskansliet.

specialisering har mycket större möjligheter att arbeta strukturerat och långsiktigt med utveckling och innovation av tjänsten.[17]

Enligt Pensionsmyndigheten kan en molntjänst vidare vara fördelaktig för de myndigheter som har kraftigt varierande behov av it-resurser, t.ex. vid utskicken av myndighetens egna orange kuvert, Skatteverkets hantering av deklarationer samt Valmyndighetens uppgifter vid allmänna val. Flexibiliteten i en molntjänst innebär att när behoven ökar kan organisationen öka sin dator- eller lagringskapacitet, för att sedan minska när efterfrågan är lägre. Detta innebär att myndigheten aldrig behöver köpa kapacitet som inte utnyttjas och att besparingen kan användas till andra värdehöjande aktiviteter.

Pensionsmyndigheten framhåller också att det är eftersträvansvärt att bygga molntjänster med öppen källkod eftersom det ökar nyttan i den offentliga investeringen då koden är återanvändbar. Värdet av öppen källkod framhålls även i flera andra studier.[18]

I sin rapport framhåller Pensionsmyndigheten problemet med s.k. inlåsningseffekter som uppstår om en myndighet på ett eller annat sätt har ett beroende till en specifik leverantör. De kan bl.a. uppstå på grund av en viss leverantörs specifika produkter, tjänster eller teknologi. Men även kompetensmässiga och rättsliga skäl kan medföra att tjänsten varken kan eller får förvaltas av någon annan än den som levererar den för tillfället. Problemet med inlåsningseffekter är även djupgående analyserat i en forskningsrapport från Konkurrensverket.[19]

2.4 Statlig molntjänst är att föredra

Även om molntjänster alltså lyfts fram som en tänkbar lösning på flera av myndigheternas utmaningar, så är det också ett flertal av de berörda rapporterna som betonar att det finns nackdelar för statliga myndigheter med att upphandla en sådan tjänst från en kommersiell aktör och att göra det på egen hand.

Visserligen tyder de refererade studierna på att statsförvaltningen generellt sett är positiv till utkontraktering och molntjänster, men att myndigheterna också – primärt av juridiska skäl – använder sådana tjänster i relativt liten utsträckning. Generellt framstår det också som att statsförvaltningen i hög grad är inlåst till vissa leverantörer och att öppna standarder inte är en prioriterad fråga alternativt att det är i det närmaste omöjligt att dra nytta av öppna standarder p.g.a. inlåsningen till vissa leverantörer.

Mot denna bakgrund lyfter flera av de refererade studierna fram alternativet med en molntjänst via en gemensam statlig lösning som ett bättre alternativ. Några exempel:

[17] Pensionsmyndigheten (2016) *Molntjänster i staten – en ny generation av outsourcing*.

[18] Se t.ex. Ramböll (2016) *Internationell utblick – Öppen programvara inom statsförvaltningen* och Linux Foundation (2016) *Guide to the Open Cloud – Current trends and open source projects*.

[19] Konkurrensverket (2016) *IT-standarder, inlåsning och konkurrens: En analys av policy och praktik inom svensk förvaltning*.

- Gartner visar i sin rapport att en statlig molntjänst enligt flera myndigheter skulle kunna lösa delar av deras problem. I studien lyfte flera myndigheter fram att de ser att en central it-drift bättre kan fokusera på säkerheten ur alla aspekter. Många myndigheter angav att de är oroliga för utländska underrättelsetjänsters avlyssning och bakdörrar i it-utrustningen. Vidare konstaterar Gartner att en statlig myndighet för gemensam it-drift enligt många myndigheter skulle vara en bra möjlighet till samarbete som inte utnyttjats. Många myndigheter påtalade även att det finns behov av att samla it-kompetensen inom statsförvaltningen då det är ett stort antal myndigheter och att it-verksamhet blir ett mer och mer komplext och specialiserat område. Enligt studien är vissa delar av statens information olämplig att lägga hos en extern part, varför en statlig molntjänst skulle vara mycket lämplig. Detta skulle enligt flera myndigheter i studien vara fallet oavsett om det skulle vara ekonomiskt fördelaktigt eftersom de finns ännu större fördelar rörande kompetens, samarbete och informationsdelning.[20]
- Pensionsmyndigheten konstaterar i sin rapport att många aktörer har ställt sig positiva till – och efterfrågar – centralt tillhandahållna molntjänster där myndigheter skulle ha möjlighet att ansluta sig utan egen upphandling. Denna synpunkt hade Pensionsmyndigheten fått från såväl myndigheter som leverantörer, forskare och expertorganisationer. I rapporten framhålls att det inom ramen för ett myndighetsmoln som tillhandahålls av en värdmyndighet till övriga myndigheter kan skapas ett större utrymme för myndigheter att använda molntjänster även när informationen som hanteras omfattas av sekretesslagstiftningen.[21]
- Även FRA har i media uttalat sig positivt om en statlig molntjänst.[22]

Till en del påminner ovanstående om vad E-delegationen framförde i en förstudie 2012. I förstudien konstaterades att det finns en betydande effektiviseringspotential inom myndigheternas it-drift och att denna potential inte kommer att kunna nås genom fortsatt mål- och resultatstyrning av myndigheterna på samma sätt som tidigare.[23]

Mot denna bakgrund föreslogs i E-delegationens förstudie att det ska skapas en myndighetsgemensam aktör, i form av en statlig myndighet, som på regeringens uppdrag effektiviserar myndigheternas it-drift genom koncentration, konsolidering, harmonisering och konkurrensutsättning. Utgångspunkten är att denna etableras som en nationell, statlig aktör med verksamhet på ett litet antal orter. Den nya myndigheten skulle fungera som en s.k. in-house-enhet som medger anslutning genom att myndigheterna kan beställa och utnyttja tjänsterna utan upphandling.

---

[20] Gartner (2016) *Underlag till arbetet med förvaltningsansvar för gemensamma lösningar och förmågor avseende IT-drift och datorhallar*. På uppdrag av Näringsdepartementet/Regeringskansliet.

[21] Pensionsmyndigheten (2016) *Molntjänster i staten – en ny generation av outsourcing*.

[22] http://computersweden.idg.se/2.2683/1.650026/fra-staten-moln

[23] E-delegationen (2012) *Förstudie: Effektiv IT-drift inom staten*.

I förstudien uppskattades den maximala effektiviseringspotentialen till 15–20 procent av driftkostnaderna och att den kan realiseras inom 5–10 år. Det skulle uppnås genom koncentration, konsolidering samt harmonisering av it-miljöerna i syfte att göra driftmiljön mer enhetlig.

Enligt E-delegationens förstudie finns det ett flertal kvalitativa fördelar med att skapa en ny myndighet för it-drift. Det skulle bl.a. ge bättre förutsättningar att garantera driftsäkerheten, bättre hantering av risker samt ökad säkerhet genom samlad hantering av samhällsviktig information. Övriga fördelar är att det skapas en attraktiv statlig arbetsgivare inom it-området som kan säkra tillgången till it-kompetens, att det ger förutsättningar för snabbare införande av myndighetsgemensamma lösningar och att det ger stora besparingar för myndigheterna genom att en professionell aktör sköter upphandling av de varor och tjänster som krävs. De största riskerna är att en stor statlig aktör på marknaden kan upplevas konkurrenshämmande samt att implementeringen av den nya myndigheten inte görs optimalt och att den istället blir en stor trög koloss.

3 Enkätundersökning

I utredningen gjordes en skriftlig enkät bland de statliga myndigheterna om hur de idag hanterar sin it-drift och vilka resurser den förbrukar. Enkätundersökningen, som genomfördes under september och oktober 2016, skickades till samtliga myndigheter under regeringen. Totalt besvarades enkäten av 166 myndigheter.

I detta kapitel redovisas enkätundersökningens resultat. Framställningen är indelad utifrån om de 166 myndigheterna hanterar it-driften i egen regi (vilket gäller för 111 myndigheter) eller har lagt ut den på en annan leverantör (56 myndigheter).[24] Kapitlet tar endast upp den mest väsentliga informationen. I bilaga 4 finns ytterligare information samt bakgrund till undersökningen.

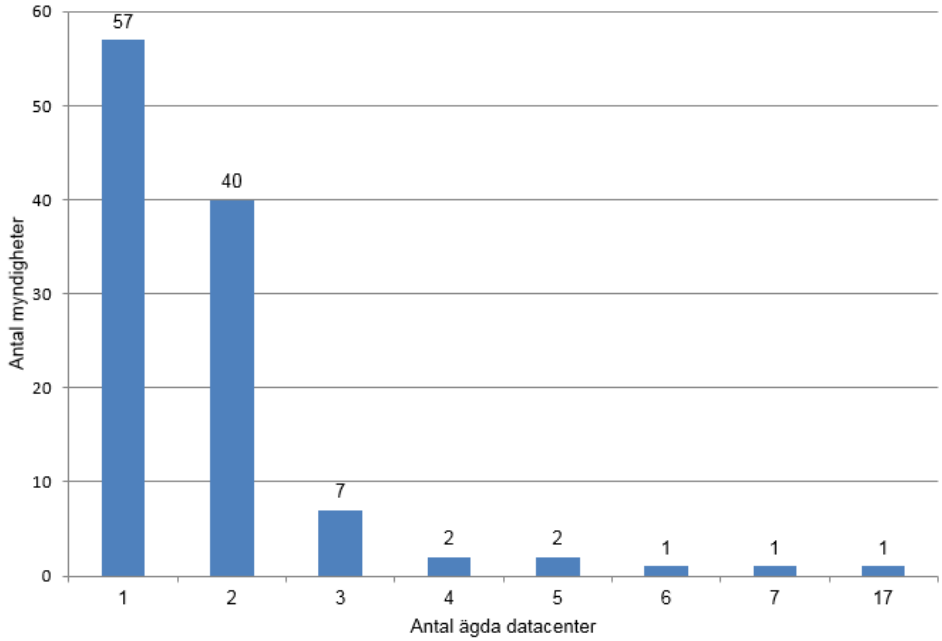
3.1 Myndigheter med egen it-drift

3.1.1 Ett stort statligt ägande av egna datacenter

I enkätundersökningen uppgav alltså 111 myndigheter att de hanterar sin it-drift i egen regi. Tillsammans står de för ett stort statligt ägande av egna datacenter, dvs. fysiska anläggningar för servrar, lagring och kommunikationsutrustning med kyla, elförsörjning och skalskydd.

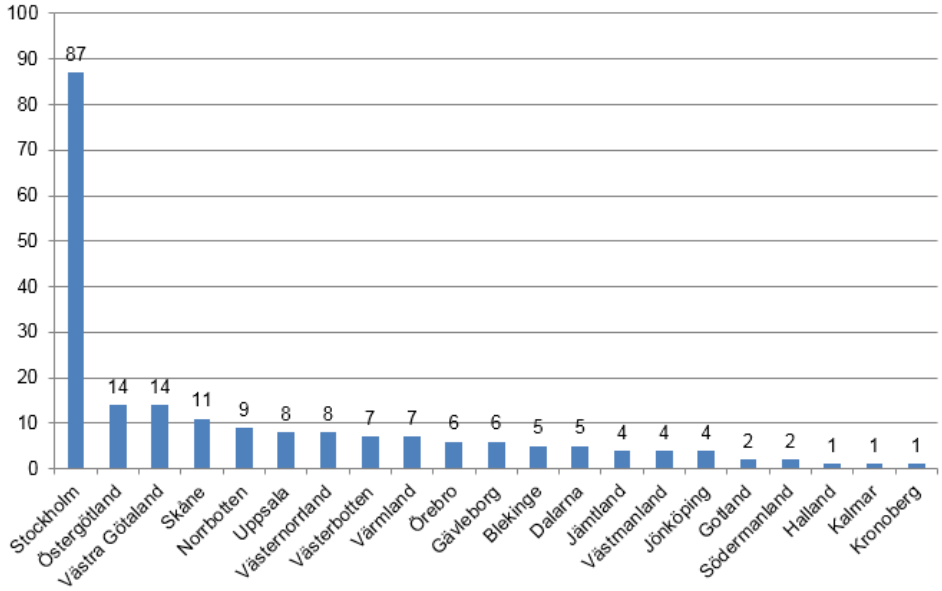
Undersökningen visar att de 111 myndigheterna sammantaget äger 206 datacenter. I dessa datacenter finns cirka 17 500 servrar. Som framgår av diagrammet nedan är det vanligaste att myndigheterna äger ett eller två datacenter; det gäller för totalt 97 av myndigheterna. Några myndigheter har dock klart fler. Den myndighet som äger flest datacenter har totalt 17 stycken.

[24] En myndighet har både egen och utkontrakterad it-drift och förekommer därför i båda kategorierna.



3.1.2 Mycket hög koncentration av datacenter till Stockholm

De totalt 206 datacenter som ägs av de 111 myndigheterna finns utspridda över landet; i varje län finns åtminstone ett datacenter. Det är dock en stor koncentration till framför allt Stockholms län. Som visas i diagrammet nedan har myndigheterna således placerat klart flest datacenter i Stockholms län (87 stycken), följt av Östergötlands län, Västra Götalands län och Skåne län.



Flera myndigheter har datacenter i mer än ett län. 14 myndigheter har datacenter i två län, tre myndigheter har datacenter i tre län och en myndighet har datacenter i totalt nio län.

3.1.3 Flest servrar finns hos stora myndigheter

Som nämndes ovan finns i de 206 datacenter som myndigheterna äger totalt cirka 17 500 servrar. Tabellen nedan visar att dessa framför allt finns hos myndigheter med många anställda.

Antal anställda per myndighet	Antal myndigheter i berörd storlekskategori	Totalt antal servrar hos myndigheterna i storlekskategorin
Upp till 100 anställda	27 myndigheter	157 servrar
101 till 300 anställda	23 myndigheter	415 servrar
301 till 1 000 anställda	31 myndigheter	1 748 servrar
Fler än 1 000 anställda	30 myndigheter	15 264 servrar

3.1.4 Betydande kostnader för egen it-drift

Myndigheterna uppger att deras samlade kostnader för egna datacenter uppgår till cirka 113 miljoner kronor per år. Kostnaderna inkluderar lokaler, el, kyla, larm, skalskydd och brandskydd. Huvuddelen av dessa kostnader bärs av myndigheter med fler än 1 000 anställda, se tabellen nedan.

Antal anställda per myndighet	Antal myndigheter i berörd storlekskategori	Total årskostnad för datacenter för myndigheterna i storlekskategorin
Upp till 100 anställda	27 myndigheter	2,1 miljoner kronor
101 till 300 anställda	23 myndigheter	11,8 miljoner kronor
301 till 1 000 anställda	31 myndigheter	19,7 miljoner kronor
Fler än 1 000 anställda	30 myndigheter	79,7 miljoner kronor

De 111 myndigheterna uppskattar vidare att deras samlade kostnader för servrar, operativsystemlicenser och virtualiseringsprogramvara uppgår till drygt 913 miljoner kronor per år. Som framgår av tabellen nedan är även denna kostnad högst för de största myndigheterna.

Antal anställda per myndighet	Antal myndigheter i berörd storlekskategori	Total årskostnad för servrar och licenser för myndigheterna i storlekskategorin
Upp till 100 anställda	27 myndigheter	6,7 miljoner kronor
101 till 300 anställda	23 myndigheter	29,2 miljoner kronor
301 till 1 000 anställda	31 myndigheter	121,0 miljoner kronor
Fler än 1 000 anställda	30 myndigheter	756,9 miljoner kronor

Sammanlagt innebär det att de totala kostnaderna för de 111 myndigheternas it-drift i egen regi uppgår till drygt 1 000 miljoner kronor per år. Till detta kan läggas den samlade årliga kostnaden på drygt 376 miljoner kronor för it-drift i de myndigheter som lägger ut driften på externa utförare, se avsnitt 3.2.

3.1.5 En stor personalstyrka för drift och underhåll

I de 111 myndigheter som hanterar sin it-drift i egen regi är många personer engagerade i arbetet. Totalt använder myndigheterna motsvarande cirka 800 årsarbetskrafter för drift och underhåll av myndigheternas egna datacenter. Fördelningen mellan myndigheter av olika storlek visas i tabellen nedan.

Antal anställda per myndighet	Antal myndigheter i berörd storlekskategori	Totalt antal årsarbetskrafter i myndigheterna i storlekskategorin
Upp till 100 anställda	27 myndigheter	29 årsarbetskrafter
101 till 300 anställda	23 myndigheter	51 årsarbetskrafter
301 till 1 000 anställda	31 myndigheter	149 årsarbetskrafter
Fler än 1 000 anställda	30 myndigheter	572 årsarbetskrafter

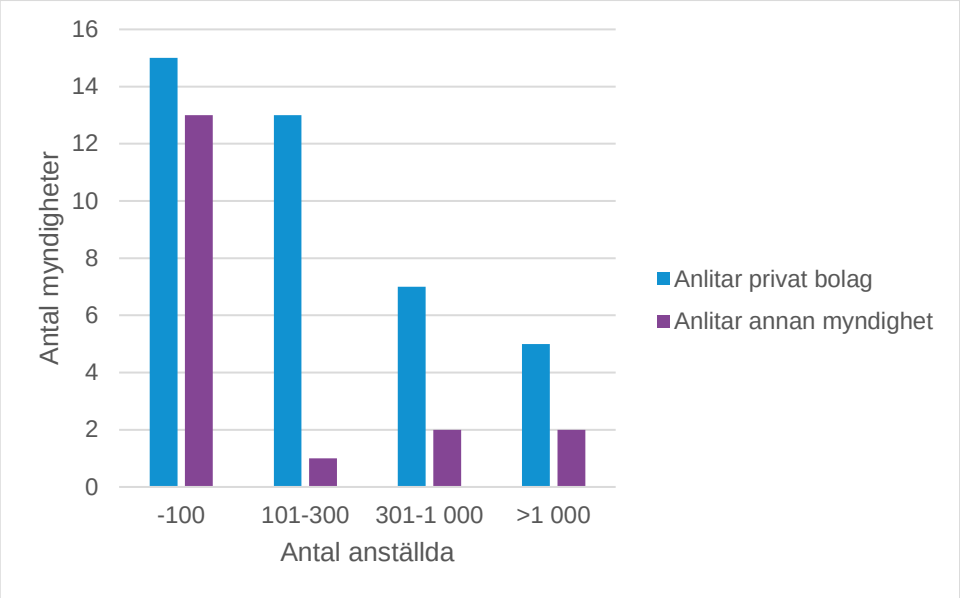
Sammantaget kan alltså sägas att it-driften för de 111 myndigheter som hanterar driften i egen regi medför betydande kostnader. Inklusive personalkostnader kan deras samlade kostnader uppskattas till *drygt 2,2 miljarder kronor per år*.

3.2 Myndigheter med utkontrakterad it-drift

3.2.1 56 myndigheter har lagt ut sin it-drift

Av de 166 myndigheter som har besvarat enkäten är det 56 myndigheter som har lagt ut sin it-drift på en annan leverantör. Det vanligaste är att myndigheterna har utkontrakterat sin it-drift till privata bolag; det har 40 myndigheter gjort. Det är dock 18 myndigheter som lagt ut sin it-drift på andra statliga myndigheter (två av myndigheterna anlitar både privata bolag och en annan myndighet).

Oavsett om myndigheten har lagt ut it-driften på en privat aktör eller en annan myndighet, så är det framför allt mindre myndigheter (med upp till 300 anställda) som har valt att göra på detta sätt, se diagrammet nedan. Till exempel är det endast fem myndigheter med fler än 1 000 anställda som har lagt ut sin it-drift på privata bolag (bland dessa myndigheter återfinns f.ö. även de två myndigheter som anlitar både privata aktörer och en annan myndighet).



3.2.2 Inte lika stora kostnader för utkontrakterad it-drift

Den it-drift som statliga myndigheter lägger ut på andra utförare är mindre omfattande och mindre kostsam än den it-drift som statliga myndigheter bedriver i egen regi. Tabellen nedan visar att totalkostnaden för den utkontrakterade it-driften är drygt 376 miljoner kronor per år.

Antal anställda per myndighet	Antal myndigheter i berörd storlekskategori	Total årskostnad för utkontrakterad it-drift för myndigheterna i storlekskategorin
Upp till 100 anställda	28 myndigheter	49,8 miljoner kronor
101 till 300 anställda	14 myndigheter	37,8 miljoner kronor
301 till 1 000 anställda	9 myndigheter	80,6 miljoner kronor
Fler än 1 000 anställda	5 myndigheter	208,2 miljoner kronor

4 Intervjuundersökning bland myndigheter

Statens servicecenter har under hösten 2016 träffat företrädare för it-avdelningarna vid 15 av de största myndigheterna.[25] Som utgångspunkt för dessa dialogmöten hade Statens servicecenter formulerat en vision om en statlig molntjänst för en samordnad it-drift levererad i en öppen, leverantörsoberoende plattform. Visionen byggde bland annat på de tidigare studier som refererades i kapitel 2. Som underlag fanns också en beskrivning av de förväntade fördelarna med en statlig molntjänst (ekonomiska såväl som säkerhetsmässiga) och en idé om ett tänkt genomförande.

Vid dialogmötena redogjorde Statens servicecenter för denna vision och dess konsekvenser m.m. och bad myndigheterna att lämna sina synpunkter på detta. I det här kapitlet sammanfattas först vad som framkom vid mötena och redovisas därefter respektive myndighets synpunkter mer i detalj.

4.1 Sammanfattning av möten med myndigheters it-avdelningar

I dagsläget äger och förvaltar det stora flertalet av de intervjuade myndigheterna sin egen IT i egna datacenter – undantag från detta är endast Försvarets materielverk, Kronofogden, Pensionsmyndigheten och Statens tjänstepensionsverk. Samtliga av myndigheterna anser att it-drift inte är en kärnverksamhet och att den innebär en stor kapitalbindning.

Genomgående är myndigheterna mycket positiva till en statlig molntjänst. Detta under förutsättning att molntjänsten har mycket hög driftsäkerhet, garanterar it-säkerheten inom molntjänsten samt att tjänsterna är basala drifttjänster.

Enligt visionen ska den statliga molntjänsten som utgångspunkt bygga på principen om leverantörsoberoende, öppna standarder och öppen källkod. Detta mottogs uteslutande positivt av de intervjuade myndigheterna.

Det stora flertalet av myndigheterna anser att statens molntjänst ska realiseras genom att det inrättas en ny myndighet som endast har detta uppdrag.

I den vision Statens servicecenter har formulerat är den statliga molntjänsten tänkt att initialt endast tillhandahålla två tjänster: datorkapacitet respektive lagring. Teoretiskt sett kan molntjänsten även tillhandahålla mer avancerade tjänster, t.ex. för statsförvaltningen gemensam e-post eller webbplatser. Att tillhandahålla sådana tjänster redan från start skulle dock enligt vår bedömning både fördröja projektet och medföra tekniska utmaningar som bör undvikas vid införandet av molntjänsten.

[25] Arbetsförmedlingen, Ekonomistyrningsverket, Försvarets materielverk, Försäkringskassan, Kronofogden, Lantmäteriet, Läkemedelsverket, Migrationsverket, Pensionsmyndigheten, Polisen, Skatteverket, Statens tjänstepensionsverk, Statistiska centralbyrån, Trafikverket samt Tullverket.

Det kan dock noteras att myndigheterna vid dialogmötena pekade på flera ytterligare tjänster som skulle vara önskvärda att införa, när statens molntjänst väl är i full drift med de initiala tjänsterna och när merparten av myndigheternas it-system har flyttats till molntjänsten. Av de ytterligare tjänster som de intervjuade myndigheterna lyfte fram kan bl.a. nämnas:

- Ett gemensamt statligt intranät.
- Ett gemensamt system för e-post.
- En datasjö med ett öppet gränssnitt för all statlig öppen data.
- En gemensam plattform för telefoni.

4.2 Myndigheternas uppfattningar och synpunkter

4.2.1 Arbetsförmedlingen

Om den egna it-driften och verksamheten

Företrädare för Arbetsförmedlingen berättade att fokus i dagsläget ligger på att först och främst skapa rätt organisation för IT. Arbetsförmedlingen har helt avvecklat sin tidigare stordator samt har ett pågående projekt att bygga ett nytt datacenter.

Om en statlig molntjänst för samordnad it-drift

Arbetsförmedlingen är mycket positiv till att inte äga och förvalta några egna datacenter samtidigt som de poängterade vikten av att en statlig molntjänst inte ska bry sig om respektive myndighets applikationer eller myndighetsutövning.

Arbetsförmedlingen poängterade att Statens servicecenter bör vara specifika och tydligt ange att det endast är it-infrastruktur som avses med statens molntjänst. Detta då det kan finnas en risk för missförstånd att statens molntjänst kommer att lösa statliga it-problem generellt när det i själva verket bara handlar om säker it-drift.

Det kommer att krävas övervakning av it-system hos både statens molntjänst, för infrastrukturen, och hos respektive myndighet (operativsystem, databas, applikation m.m.). Enligt Arbetsförmedlingen blir det en utmaning att hitta gränsdragningarna och samarbetsformerna mellan vad som hamnar hos respektive myndighet och vad som hamnar i statens molntjänst.

4.2.2 Ekonomistyrningsverket

Om den egna it-driften och verksamheten

Ekonomistyrningsverket (ESV) är i sig inte en av de stora myndigheterna men de ansvarar för statens budgetsystem samt flera andra centrala it-system. Avdelningen för Hermes och IT vid ESV har viss it-drift hos extern leverantör, dock sköts det mesta av ESV:s personal.

Om en statlig molntjänst för samordnad it-drift

ESV funderade på om statens molntjänst kunde skapas av marknaden och bara upphandlas, alternativt om den först skapades inom staten och dess drift därefter utkontrakterades.

Enligt ESV är det viktigt med tydlighet gällande hur statens molntjänst ska prioritera bland olika myndigheter och it-system vid olika former av driftproblem.

När respektive myndighet får färre medarbetare som arbetar med it-drift kan t.ex. säkerheten i internetanslutningen och anslutningen mot statens molntjänst bli problematisk att hålla tillräckligt hög kompetens på.

4.2.3 Försvarets materielverk

Om den egna it-driften och verksamheten

Hemliga it-system hanteras av Försvarets materielverk (FMV) själva medan öppna system är outsourcade till extern leverantör. Stordatorn är helt avvecklad.

FMV har p.g.a. sitt nära förhållande till Försvarsmakten mycket höga säkerhetskrav på stora delar av verksamheten.

Om en statlig molntjänst för samordnad it-drift

FMV är positivt till att flytta sina öppna it-system till statens molntjänst men är tveksamt till att flytta de hemliga it-systemen. Om statens molntjänst minst når upp till FMV:s krav för drift av de hemliga it-systemen kan det bli aktuellt att flytta även dessa.

Om en statlig molntjänst skapas är det mycket viktigt att utveckling, test och produktion är helt separata miljöer.

Ur ett säkerhetsperspektiv anser FMV att:

- Den exakta placeringen av datacenter ska vara hemlig.
- Myndigheter med höga säkerhetskrav ska ha rätt att granska statens molntjänst ur alla aspekter inklusive på plats.
- Endast noggrant granskad hårdvara ska användas.
- Funktion för helpdesk ska utföras av egen anställd och säkerhetsgodkänd personal.

Försvarsmaktens ”Krav på Säkerhetsfunktioner (KSF3)” bör vara lämpligt att använda vid skapandet av statens molntjänst.

FMV tror att det är lämpligast att statens molntjänst realiseras i en egen myndighet.

4.2.4 Försäkringskassan

Om den egna it-driften och verksamheten

Försäkringskassan har relativt nyligen byggt nya datacenter där fokus bl.a. legat på minskad leverantörsinlåsning, snabbrörliga arbetssätt och mer öppen källkod. Stordatorn är helt avvecklad.

För att bättre kunna mäta och jämföra olika it-kostnader har Försäkringskassan studerat behovet av att kunna definiera sådana kostnader, eventuellt med hjälp av ramverket Technology Business Management.

Om en statlig molntjänst för samordnad it-drift

Försäkringskassan ställer sig positiv till förslaget om en statlig molntjänst för sin it-drift. Trots att de ligger långt framme med sin it-drift i egen regi menar Försäkringskassan att fördelarna ändå överväger andra sidor.

Att skapa en central it-drift för staten kräver enligt Försäkringskassan ett stort mått av förankring, både med olika departement och med personalen.

Enligt Försäkringskassan finns det en stor säkerhetsmässig utmaning med utkontraktering till privata aktörer som är väsentligt enklare med en statlig aktör.

4.2.5 Kronofogden

Om den egna it-driften och verksamheten

Kronofogden samarbetar idag med Skatteverket, som sköter all it-drift åt Kronofogden. Skärningen mellan de två myndigheterna skulle enligt Kronofogden kunna användas som en förebild för relationen mellan myndigheter och statens molntjänst.

Om en statlig molntjänst för samordnad it-drift

Kronofogden är mycket positiv till att flytta sin it-drift till statens molntjänst.

Kronofogden anser att it-säkerheten i hela lösningen är den största utmaningen men också den kanske största fördelen. Att upprätthålla sin egen it-säkerhet är en allt större utmaning för Kronofogden och de anser att en statlig molntjänst skulle ha mycket bättre förutsättningar att lyckas med säkerheten än en enskild myndighet.

Nästa utmaning är långsiktig kompetensförsörjning för statens molntjänst. Till viss del kan det lösas med verksamhetsövergångar från befintliga myndigheter enligt Kronofogden. De föreslår att samarbete upprättas med olika universitet och högskolor där vissa utbildningar kan syfta till kunskaper om att bygga molntjänster, hålla dessa säkra m.m.

För att upprätthålla säkerheten och kompetensen krävs det enligt Kronofogden att statens molntjänst erbjuder marknadsmässiga löner för de bästa teknikerna.

Enda möjligheten för att lyckas är enligt Kronofogden att det blir obligatoriskt för alla myndigheter att ansluta sig till statens molntjänst. Att statens molntjänst inte behöver prioritera bland olika myndigheters it-system vid driftproblem utan ser till hela staten är en stor fördel.

Enligt Kronofogden vore det önskvärt om statens molntjänst kunde underlätta forensiska utredningar vid olika former av intrång.

När statens molntjänst är i full drift föreslår Kronofogden att fler centrala it-funktioner skulle kunna realiseras i denna myndighet. Exempelvis gemensamma licensinköp, e-post och intranät. Ännu längre fram borde Platform as a Service (PaaS) och e-arkiv kunna erbjudas.

4.2.6 Lantmäteriet

Om den egna it-driften och verksamheten

Lantmäteriet har i dagsläget stora utmaningar vad gäller utveckling av it-verksamheten och it-systemen. Lantmäteriets verksamhet kräver allt fler system, högre tillgänglighet, hög säkerhet och snabbare utvecklingstakt samtidigt som det är svårt att rekrytera rätt kompetens och hålla kostnaderna i schack.

Trenden på Lantmäteriet är att antalet servrar har fördubblats jämfört med för fem år sedan och att mängden data som lagras ökar med 15 procent per år.

Lantmäteriet har ett pågående projekt för att bygga en egen intern molntjänst. Detta har gett flera värdefulla lärdomar, bl.a. att OpenStack som programvara är bättre än en del proprietära alternativ.

Erfarenheten hos Lantmäteriet är att det är svårt att lyckas med utkontraktering oavsett organisation, men upphandlingsprocessen adderar ytterligare komplexitet och försvårar långsiktiga åtaganden. Det är dessutom lätt att bli inlåst till en leverantör.

Många publika molntjänster är attraktiva men legala skäl håller tillbaka nyttjandet enligt Lantmäteriet.

Om en statlig molntjänst för samordnad it-drift

Lantmäteriet ser bara vinster med en statlig molntjänst utifrån förslaget. Ett exempel på det är att it-säkerheten generellt sett blir bättre när volymen i en lösning ökar.

Det är en kritisk framgångsfaktor att statens molntjänst skapas i en ny myndighet enligt Lantmäteriet.

Lantmäteriet anser att konsolideringsalternativet där en fysisk flytt av myndigheternas befintliga infrastruktur i sina datacenter till nya centrala datacenter inte kommer att fungera då det är för stort och problematiskt.

Enligt Lantmäteriet kommer statens molntjänst att behöva ha ett tjänstenivåavtal (SLA) med anslutna myndigheter. Dels för att myndigheterna ska veta vad de kan förvänta sig,

dels för att statens molntjänst ska ha en tydlig egen målsättning. Om SLA inte uppfylls finns två vanliga principer idag, vite samt ersättningsbefrielse.

Lösningsarkitektur gällande varje myndighets it-system bör enligt Lantmäteriet finnas kvar på respektive myndighet.

Lantmäteriet har stora krav på sig att lämna ut geografisk data som öppen data. I dagsläget är det svårt av både säkerhetsskäl och prestandaskäl. En statlig molntjänst skulle väsentligt underlätta detta.

4.2.7 Läkemedelsverket

Om den egna it-driften och verksamheten

Läkemedelsverket har i princip bara egen drift i egna lokaler. För några specialområden, t.ex. projekthantering och kundhantering (CRM) används publika molntjänster. Kraven på verksamheten ökar hela tiden, framförallt då det är stor samverkan och många gemensamma system inom EU.

Om en statlig molntjänst för samordnad it-drift

Läkemedelsverket är positivt till förslaget om en statlig molntjänst för it-drift.

Läkemedelsverket skulle vilja se fler tjänster, t.ex. PaaS, SaaS och telefoni. Det är viktigt att statens molntjänst redan från början är byggd med dessa tjänster i åtanke då det är på den nivån de verkligen ser värdeskapande.

Statens molntjänst måste enligt Läkemedelsverket vara billigare än egen it-drift. Att den inte kan bli lika billig som de globala publika molntjänsterna är uppenbart då dessa har mycket större skala och inte behöver ta hänsyn till diverse lagstiftning och en statsförvaltning som ska fungera i kristider.

4.2.8 Migrationsverket

Om den egna it-driften och verksamheten

Migrationsverket har haft ett högt tryck på sin it-organisation de senaste åren. Tidigare strategi var att utkontraktera drift för att kunna koncentrera sig på kärnverksamheten och uppnå besparingar. Utkontrakteringen skedde 1997, men Migrationsverket fann flera nackdelar med detta och tog hem driften igen 2007.

Det är i princip förbjudet med publika molntjänster hos Migrationsverket. Detta enbart av legala skäl.

Äldre Unix-system är avvecklade och från 2012 används bara Linux och Windows Server som operativsystem på myndigheten.

Om en statlig molntjänst för samordnad it-drift

Migrationsverket tycker det är mycket lockande att flytta sin it-drift till statens molntjänst. Detta kräver dock att respektive myndighet får tillräckligt lång framförhållning innan migreringen påbörjas samt tillräckligt med tid för att praktiskt genomföra migreringen.

Migrationsverket påpekar att det finns väldigt många detaljer i ett datacenter som sammantaget skapar en komplexitet när system ska migreras. Antalet integrationer mellan olika system och komponenter både internt och externt är många och det krävs en god planering för att en migrering ska ha förutsättningar att lyckas. En seriös migreringsplan behöver beakta komplexiteten i det som flyttas så att kompetensbehov och tidsåtgång estimeras på ett rimligt sätt. Likaså behöver den påverkan som byte av infrastrukturkomponenter innebär belysas. Myndighetens behov består inte bara av servrar, lagring, nätverk etc. som redan finns utan behovet innebär att det ställs krav på en förmåga att snabbt, flexibelt och kostnadseffektivt tillgodose förändrade behov. För att vara ett trovärdigt alternativ krävs enligt Migrationsverket att statens molntjänst bygger ett koncept som tillgodoser höga krav på automation av datacenter och erbjuder en möjlighet att snabbt tillgodose förändrade behov på ett administrativt enkelt sätt.

Enligt Migrationsverket är det viktigt att it-driftskostnaderna blir betydligt lägre för respektive myndighet. Kostnader är dock svåra att jämföra över tid då ny funktionalitet och nya krav ständigt tillkommer.

Pedagogiskt är det enligt Migrationsverket bättre att starta en ny värdmyndighet, eftersom ingen myndighet då har några förutfattade meningar, relationer eller arv som kan påverka. Det krävs en trovärdig och väl underbyggd teknisk modell för att statens molntjänst ska kännas trygg och realistisk att genomföra.

Enligt Migrationsverket skulle det vara en stor vinst om statens molntjänst gjorde det enklare för myndigheter att utbyta data och skapa integrationer med varandra. I framtiden vore det bra med en tjänstekatalog, andra tjänster utöver ren IaaS, logghantering, incidenthantering och en central funktion för it-säkerhet.

4.2.9 Pensionsmyndigheten

Om den egna it-driften och verksamheten

Pensionsmyndigheten har i dagsläget ingen egen it-drift. De köper vissa delar av Försäkringskassan och andra delar av en privat leverantör. De är nöjda med bägge leverantörerna men planerar för att ha all sin it-drift hos Försäkringskassan i framtiden.

Om en statlig molntjänst för samordnad it-drift

Pensionsmyndigheten är positiv till en statlig molntjänst för drift av ren infrastruktur, men ser också att det finns utmaningar utifrån de resonemang som återfinns i deras rapport ”Molntjänster i staten – en ny generation av outsourcing”.

Viktiga förutsättningar för statens molntjänst är enligt Pensionsmyndigheten obligatorisk anslutning av alla myndigheter, tydliga avtal mellan myndigheterna samt tydlig kravställning mellan alla parter.

Pensionsmyndigheten framhåller att även om det bara är datorkraft och datalagring som erbjuds så måste det vara tydligt var gränsen går gällande ägandet av de ingående delarna i ett it-system. T.ex. hårdvara, licenser, applikationer och information.

Enligt Pensionsmyndigheten krävs det en finansieringsmodell för statens molntjänst som håller över tid och inte är volatil. För att bygga upp statens molntjänst krävs det mycket väl tilltaget startkapital samt en tydlig plan för hur migreringen av befintliga it-tjänster ska genomföras.

Vidare måste betalningsmodellen vara tydlig med ”fast pris” på tjänsterna, motsvarande hur den externa marknaden fungerar, för att respektive myndighet ska ha en stabil budgetprocess. Pensionsmyndigheten anser att statens molntjänst ska göra en viss vinst på tjänsterna för att på så sätt ha medel till återinvesteringar och moderniseringar. Det bör också klargöras vad som händer om statens molntjänst blir underfinansierad.

Utmaningar som framhålls är hur ledning och styrning ska gå till, det praktiska genomförandet, uppnå leverantörsoberoendet, den ständiga kapacitetstillväxten, hur konkurrens med den öppna marknaden ska mötas samt problemet med att utvecklingen kan springa ifrån en statlig aktör.

4.2.10 Polisen

Om den egna it-driften och verksamheten

Polisen har idag ca 700 anställda på it-funktionen och har två primära datacenter. Stordatorn är under avveckling, något som ska vara helt klart inom två år.

Kapacitetstillväxten är stor samtidigt som belastningen på it-systemen är relativt jämnt fördelad över året. Ett pågående projekt är skapandet av sju ledningscentraler som ska kunna agera autonomt även vid enorma driftstörningar. Detta inkluderar en delmängd av it-systemen.

Om en statlig molntjänst för samordnad it-drift

Polisen är positiv till statens molntjänst. Det måste vara obligatoriskt för alla myndigheter att anslutas, frivilliga anslutningar har Polisen dåliga erfarenheter av.

Om alla myndigheter som deltar i SGSI (Swedish Government Secure Intranet) är med i statens molntjänst bör dagens SGSI enligt Polisen kunna avvecklas och istället ersättas av säkerhetsregler inom molntjänsten.

Polisen har it-system som kräver speciell hårdvara som kan bli svåra att migrera till statens molntjänst. I de fall myndigheter har it-system med krav på mycket hög tillgänglighet och där detta åstadkoms med spegling, så behöver de antagligen ändra i dessa it-

system så att tillgängligheten uppnås på annat sätt. En fundering Polisen framförde var hur lång tid myndigheterna ska få på sig att för att genomföra sin migrering.

Polisen antar att en naturlig utveckling av statens molntjänst är att i ett senare skede erbjuda fler delar av applikationsstacken, t.ex. operativsystem, containers och databas.

Polisen har i delar säkerhetskrav som kan jämställas med militära krav, vilka måste tillgodoses.

Det bör också påpekas att Polisens Regionledningscentraler är byggda för att kunna agera autonomt. De bör därför inte omfattas av ett anslutningsobligatorium.

4.2.11 Skatteverket

Om den egna it-driften och verksamheten

Skatteverket har idag två datacenter. Av olika skäl flyttas nu det ena datacentret till ett bergrum. Tidigare fanns en del applikationer i stordatormiljö men den är helt avvecklad. Standard för nya applikationer är att dessa körs på Linux.

Om en statlig molntjänst för samordnad it-drift

Skatteverket är mycket positivt till att flytta all sin it-drift till statens molntjänst förutsatt att de egenskaper de behöver finns i tjänsten.

Molntjänsten måste enligt verket skapas i en ny myndighet som endast har detta uppdrag.

Statens molntjänst måste vara tillgänglig 24/7/365 för att vara attraktiv och konkurrenskraftig.

Om tjänster på högre nivå än IaaS ska erbjudas måste en tjänstekatalog skapas enligt Skatteverket.

Enligt Skatteverket behöver statens molntjänst klargöra hur säkerhetsskyddslagen påverkar tjänsten och myndigheterna när de nyttjar tjänsten.

4.2.12 Statens tjänstepensionsverk

Om den egna it-driften och verksamheten

Statens tjänstepensionsverk (SPV) har idag en stor del av kärnverksamheten i stordatormiljö. SPV har analyserat om applikationerna kan flyttas till en modernare arkitektur och bedömer att det sannolikt skulle gå bra.

SPV har outsourcat sin it-drift till två olika företag samt har visst samarbete med Försäkringskassan. SPV har en lång tradition av outsourcing och har noterat att det blir färre och färre företag som klarar av SPV:s säkerhetskrav.

Kapacitetstillväxten är sakta ökande över tid, dock utan tydliga belastningstoppar i itsystemen.

Om en statlig molntjänst för samordnad it-drift

SPV är positivt till förslaget om statens molntjänst och att det bara är de mest basala tjänsterna som erbjuds. Eftersom SPV redan idag outsourcar sin it-drift passar det väl in i verkets strategi att flytta applikationerna till statens molntjänst.

Enligt SPV är det viktigt att återanvända den kompetens och det som redan finns uppbyggt inom staten men att tjänsterna bör organiseras i en myndighet som får detta som kärnuppdrag. Statens molntjänst måste ha en bra struktur och säkerhet när olika myndigheter och leverantörer som de anlitar ska installera och förvalta sina applikationer i tjänsten.

Enligt SPV är det också viktigt att formalisera överenskommelserna på tjänsterna som statens molntjänst levererar till myndigheterna genom någon form av ”serviceavtal”. Dessa överenskommelser bör innehålla en materiell skyldighet för statens molntjänst att leva upp till sina åtaganden, t.ex. genom ett förfarande med rabatter vid bristande leverans, och en möjlighet för en myndighet att lämna samarbetet om kvaliteten visar sig otillräcklig.

SPV framhöll att respektive myndighet kommer att behöva servicedesk för sina applikationer samtidigt som statens molntjänst måste ha en servicedesk för molntjänsten.

Infrastrukturell redundans är både svårt och kostsamt, med en statlig molntjänst blir det enligt SPV möjligt att fördela kostnaderna för mycket hög redundans på ett sådant sätt att det blir kostnadseffektivt för staten som helhet och för respektive myndighet.

Enligt SPV är det viktigt att myndigheterna får information i god tid för att kunna säga upp befintliga avtal i tid. Att myndigheterna inte behöver upphandla tjänster från statens molntjänst enligt LOU gör processen snabbare.

Enligt SPV krävs det en tydlig modell och med hög säkerhet när myndigheter ska utbyta data med varandra inom molntjänsten. SPV menar också att licensmodeller för vissa proprietära programvaror är problematiska i en virtualiserad miljö då leverantörerna tar betalt t.ex. per CPU.

SPV framhåller att statens molntjänst i framtiden även borde kunna tillhandahålla telefoni för staten. Var växelplattformen (som idag är en vanlig server) finns är inte längre relevant och det finns klara stordriftsfördelar rörande drift och operatörstjänster.

4.2.13 Statistiska centralbyrån

Om den egna it-driften och verksamheten

Statistiska centralbyrån (SCB) bedriver större delen av verksamheten i Sverige men har även viss utlandsverksamhet i form av biståndsarbete. SCB rapporterar till och samarbetar med EU:s statistikorgan Eurostat som ansvarar för europeisk statistik. Dessutom har SCB ett samordningsansvar för de knappt 30 statistikansvariga myndigheterna.

SCB har idag två datacenter. Tidigare fanns det en stordator, men den är helt avvecklad. IT-drift är en stor utgiftspost, t.ex. är supportavtal på äldre hårdvara ofta orimligt kostnadsdrivande.

För några år sedan flyttades servrar från Stockholm till Örebro. En applikation som då användes i Stockholm fick så hög fördröjning till servermiljön att de delvis fick bygga om applikationen för att den skulle fungera korrekt. En bra lärdom när myndigheter kommer att ha applikationer distribuerade i landet inom statens molntjänst.

Om en statlig molntjänst för samordnad it-drift

En statlig molntjänst skulle vara mycket positivt för SCB.

SCB poängterar att det är viktigt att skilja på produktionsmiljö, testmiljö och utvecklingsmiljö. Det kommer också att krävas regelverk och mallar för att automatisera och för att styra rättigheter. Det krävs också rigid åtskillnad mellan de olika myndigheterna.

4.2.14 Trafikverket

Om den egna it-driften och verksamheten

Huvuduppgiften är att leverera den IT Trafikverket behöver och den största delen av Trafikverkets it-drift finns i Borlänge, Gävle, Stockholm och Göteborg. IT-avdelningen har knappt 700 anställda som kompletteras av ca 400 konsulter.

IT-miljön är utspridd i landet då delar är direkt knutna till järnvägen, delar till vägnätet och delar till eget mobiltelefonnät. De delarna som är direkt knutna till infrastrukturen är säkerhetskritiska och är ofta kopplade till olika styrsystem.

Trafikverket ansvarar också för ett fibernätverk. I nuvarande uppdrag ligger att nämnda fiber i huvudsak är till för Trafikverkets egen användning och att verket endast säljer överkapacitet.

Om en statlig molntjänst för samordnad it-drift

De administrativa delarna av it-miljön, som inte är direkt knutna till den säkerhetskritiska infrastrukturen, bör i princip vara möjliga att flytta till statens molntjänst och Trafikverket är positiva till att utreda innebörden av det.

Trafikverket anser att statens molntjänst bör skapas i en egen myndighet som endast har detta uppdrag.

Trafikverket poängterar att det stora framtida värdet i en molntjänst ligger i mer värdeadderande tjänster på SaaS-nivån. Statens molntjänst bör planera för att addera lämpliga SaaS-tjänster i framtiden, t.ex. e-post eller projektverktyg.

För att migreringen ska gå smidigt krävs bra vägledningar och stöd från statens molntjänst samt hur myndigheterna ska kunna orkestrera sin it-drift inom statens molntjänst men även då viss it-drift sker i egna lokaler.

4.2.15 Tullverket

Om den egna it-driften och verksamheten

I dagsläget är it-driften koncentrerad till två datacenter i Luleå. Tullverkets IT har en relativt jämn belastning över året. Tullverket har höga krav på sin it-säkerhet och informationssäkerhet, varför FRA regelbundet granskar it-miljön.

Tullverket samarbetar tätt med övriga EU-länder i tullfrågor. Det ställer ytterligare krav på it-systemen och säkerheten.

Enligt Tullverket är det generellt sett en stor utmaning för hela staten att upprätthålla it-säkerheten och informationssäkerheten, delvis p.g.a. svårigheten att rekrytera personal med rätt kompetens. Tullverket har erfarenheter av att myndighetssamverkan lätt innebär svårigheter och otydlighet gällande kostnader och ansvarsfördelning.

Kostnader för programvarulicenser och underhållsavtal har ökat dramatiskt över tid.

Om en statlig molntjänst för samordnad it-drift

Tullverket är positivt till att ansluta sig till en statlig molntjänst och därmed kunna avveckla sina datacenter och all infrastruktur inuti dessa. Detta under förutsättning att molntjänsten är flexibel och säker.

Det finns olika krav på datalagring, hög prestanda till en högre kostnad samt lägre prestanda till en lägre kostnad. Bägge möjligheterna bör finnas i statens molntjänst enligt Tullverket.

Upphandlingsprocessen och överprövningar skapar lätt stora kostnader och långa ledtider enligt Tullverket vilket därmed minskar fördelarna med outsourcing av it-drift. Detta skulle inte vara ett problem för myndigheterna i statens molntjänst.

Tullverket anser att statens molntjänst bör inrättas i en egen myndighet som endast har detta uppdrag för att optimalt kunna fokusera på uppgiften.

Vissa leverantörer av proprietära programvaror har licensieringsmodeller som kan bli en utmaning i statens molntjänst enligt Tullverket.

Efter att molntjänsten är i drift och fungerar ser Tullverket möjligheter till annan samordnad drift, t.ex. intranät, e-post, ärendehantering och verktyg för dataanalys. Även central licenshantering inom staten skulle vara önskvärt.

En möjlighet som öppnas med statens molntjänst är enligt Tullverket att respektive myndighet klassar data från ett visst system som ”öppen data” och att den på så sätt blir tillgänglig för alla andra myndigheter inom molntjänsten. Detta skulle då kunna bli en hävstång för e-förvaltningen.

5 Samordnad it-drift i andra länder

I detta kapitel redovisas hur sex jämförbara länder har valt att samordna statsförvaltningens it-drift.[26] Samordning av statlig it-drift är idag en allmän trend i Norden och övriga OECD-området. Redogörelserna omfattar bl.a. reformernas bakgrund och genomförande samt gjorda erfarenheter. Informationen har primärt inhämtats genom direktkontakter med länderna och i några fall från berörda organs webbplatser.

5.1 Andra länders erfarenheter i korthet

Sammanfattningsvis visar andra länders reformer av att samordna statlig it-drift på följande erfarenheter:

- Flera av de studerade länderna genomför konsolideringar och kraftiga minskningar av antalet statliga datacenter i samband med att de samordnar den statliga it-driften. Ofta förutses också en kraftig besparing för statskassan.
- I flera länder har det tagit längre tid att genomföra en samordning av statsförvaltningens it-drift än vad som förutsågs innan reformen.
- Att samordna statlig it-drift är komplicerat. Komplikationsgraden beror bl.a. på hur många tjänster som ska ingå. Ju fler tjänster som ska samordnas desto mer komplicerat och tidskrävande blir det.
- Anslutningsgraden blir lidande ju mer myndigheterna fråntas självbestämmande över sin IT.
- Flera länder bygger statliga molntjänster.
- Flera av de studerade länderna tänker sig att den samordnade, statliga it-driften även ska inkludera tjänster av typen gemensam e-post och likformiga webbplatser m.m.

5.2 Danmark

I Danmark bildades Statens IT[27] 2009 med målet att effektivisera statsförvaltningen, standardisera it-miljöerna och sänka it-kostnaderna. Statens IT sorterar under finansdepartementet.

Det är frivilligt för myndigheterna att ansluta sig till Statens IT och idag är 10 ministerier med ca 14 000 användare anslutna.

Med fokus på tillgänglighet, stabilitet, effektivitet och informationssäkerhet levererar Statens IT tjänster inom fyra huvudområden:

[26] Danmark, Finland, Frankrike, Kanada, Nederländerna och Storbritannien.

[27] http://statens-it.dk/

- IT-arbetsplats, en basplattform för PC-användare.
- IT-infrastrukturdrift, t.ex. server, lagring och nätverk.
- Standardiserade generella administrativa it-system, t.ex. applikationsdrift av webbplatser och plattformsdrift av databaser.
- Effektivisering av outsourcad it-drift genom standardiserade ramavtal där Statens IT agerar mellanhand mot privata företag som utför själva driften.

Statens IT arbetar mot fyra strategiska mål:

- Hög kundnöjdhet och säker it-drift
- Konkurrenskraftiga priser
- Värdeskapande hos kunderna
- Hög informationssäkerhet

5.3 Finland

Bakgrund och genomförande

Statens center för informations- och kommunikationsteknik, Valtori,[28] inledde sin verksamhet 2014. I samband med det övergick 400 personer inom statsförvaltningen till Valtori.

Valtori ansvarar idag för de branschoberoende it-tjänster som olika delar av den finska statsförvaltningen tidigare producerade. De tjänster och funktioner som levereras är desamma som innan.

Valtoris ”kunder” är alla verk inom statsförvaltningen. Kunderna kan också vara statliga affärsverk, andra myndigheter inom offentlig förvaltning, offentligrättsliga inrättningar, riksdagen och fonder utanför statsbudgeten samt företag och samfund som tillhandahåller offentliga förvaltnings- eller serviceuppgifter.

Valtori har som mål att producera it-tjänster som är konkurrenskraftiga, av hög kvalitet, ekologiska, informationssäkra samt uppfyller kundernas behov.

I dagsläget har Valtori ca 1 100 personer anställda på 42 orter. De underhåller ca 92 000 arbetsstationer, ca 8 900 servrar och ca 60 datacenter.

Valtoris tjänster är en kombination av egna och utifrån köpta tjänster som Valtori anpassar till statsförvaltningens behov. Myndigheterna har bara avtal med Valtori som i sin tur kan uppdra åt extern leverantör att sätta upp och förvalta ett visst it-system.

[28] Statens servicecenter har intervjuat både Valtori och deras externa leverantör vilket utgör bakgrunden till avsnittet.

Valtori tillhandahåller statsförvaltningens gemensamma generella it-tjänster. Valtori sörjer för upphandling, drift, administration och utveckling av de it-lösningar som tillhandahålls centraliserat. Tjänsterna som erbjuds är bl.a. server, stordator, lagring, säkerhetskopiering, operativsystem, katalogtjänst, databas och webbserver.

Valtori har i uppdrag att konsolidera och standardisera de olika myndigheternas it-miljöer. I detta konsolideringsarbete flyttas ibland tjänster till extern leverantör.

Valtoris vision:

- Etablera kostnadseffektiva och skalbara tjänster med ett holistiskt perspektiv.
- Tillgång till tjänster med löpande utveckling.
- Konsolidering och reduktion av antalet statliga datacenter.

Förväntade effekter:

- Förenklade beställnings- och inköpsprocesser
- Kostnadseffektivitet
- Flexibla och skalbara funktioner
- Löpande utveckling och modernisering
- Högkvalitativa och beprövade tjänster
- Skalfördelar som kommer med större volymer

Deras externa leverantör använder vanliga på marknaden förekommande hårdvaror och programvaror. Det förekommer inga krav på öppna standarder, öppen källkod eller granskning av källkod.

Erfarenheter

Att dela infrastruktur och tjänster är en grundförutsättning för att nå kostnadsbesparingar genom höga volymer och processeffektivitet. Detta gäller både avtal, kostnadsfördelning och teknik.

Konsolideringen har tagit mycket längre tid än förväntat. Att konsolidera och standardisera IT tar tid och det fanns en del motstånd mot att delta i den konsoliderade tjänsten.

Valtori har inte reglerat vad som händer om deras externa leverantör blir uppköpt av ett utländskt bolag och hur det kan påverka informationssäkerheten för finska staten. De tekniska miljöer som används hos den externa leverantören är dock till stor del separerade från andra kunder till leverantören. Valtori har också krav på säkerhetsklassad personal hos leverantören.

Sekretess på handlingar som lagras i tjänsten styrs av ett regelverk där standardregeln är att ingen myndighet får tillgång till något hos en annan myndighet. Hela lösningen hos Valtoris externa leverantör har granskats av finländska myndigheter för att säkerställa säkerheten.

5.4 Frankrike

Ansvaret för att modernisera och effektivisera den franska staten ligger hos moderniseringsdepartementet. Inom detta finns en avdelning med ansvar för statens IT, DINSIC.[29] Exempel på det DINSIC gör är öppen data, statens datanätverk och gemensamma administrativa it-system.

År 2013 påbörjades planeringen för att konsolidera franska statens datacenter. Beslut om genomförande fattades 2014. Planen är att på 10 år minska antal datacenter från 117 till 10. Kostnaderna beräknas därmed minska med 30 procent.

Av de 117 datacenter som identifierades för konsolidering var 90 i drift 2015. Vid utgången av 2017 beräknas 50 datacenter återstå i drift.

Den franska staten ställer i ökande grad krav på att it-systemen ska vara tillgängliga dygnet runt under hela året. Därför går det bara att kostnadseffektivt upprätthålla drift på ett fåtal ställen. Ett annat mål är att uppnå en mer snabbrörlig och dynamisk IT för att möta statens kommande behov.

Samtliga 10 moderna datacenter som blir kvar ska vara väldigt standardiserade med hög tillgänglighet och säkerhet. Varje datacenter ska uppnå nivån ”Tier 3” eller ”Tier 3+” (ett mått på hur driftsäkert ett datacenter är, där Tier 4 är högsta nivån) och med lågt PUE-tal (ett värde som anger hur energieffektivt ett datacenter är).

Tjänsterna som ska erbjudas är dels drift av servrar och lagring, dels molntjänst i form av IaaS (Infrastructure as a Service). De har tagit fram en tjänstekatalog och en formaliserad överenskommelse som myndigheterna använder emellan sig.

Respektive datacenter kvarstår i ett visst departements ägo och drift men tar in andra departement som ”kunder”.

5.5 Kanada

Bakgrund och genomförande

På federal förvaltningsnivå skapade Kanada 2011 ett gemensamt servicecenter (Shared Services Canada, SSC[30]). SSC syftar till att konsolidera datacenter, nätverk och e-post för de flesta federala myndigheterna i landet. SSC har en årlig budget på motsvarande 13 miljarder kronor.

[29] Statens servicecenter har fått detaljerad information direkt av DINSIC vilket utgör bakgrunden till avsnittet.

[30] Statens servicecenter har fått detaljerad information direkt av SSC vilket utgör bakgrunden till avsnittet.

I den bakomliggande utredningen konstaterades att Kanadas offentliga it-resurser karakteriseras av fragmentering, duplicering och ineffektivitet. Som ett led i att förbättra effektiviteten genomfördes därför en satsning på att strömlinjeforma och konsolidera driften av datacenter, e-post och nätverk. Effektiviseringsvinsterna som förväntades var:

- Minskade kostnader
- Förbättrad säkerhet för myndighetsdata
- Förbättrad säkerhet för data om kanadensiska medborgare
- Skalekonomiska fördelar och möjliggörande av mer kostnadseffektiv modernisering av it-tjänster

De federala myndigheterna hade innan reformen över 500 datacenter. Några av dessa datacenter hade stor ledig kapacitet medan andra hade för låg kapacitet för att möta behoven. Olika datacenter hade olika säkerhetsstandard och driftsäkerhet. Flera äldre datacenter hade höga energikostnader på grund av omodern teknik. SSC avvecklar nu därför gamla datacenter och reducerar antalet datacenter till högst sju stycken.

De största myndigheterna tvingades av regeringen att flytta sin it-drift till SSC, medan mindre myndigheter gavs valfrihet.

I dagsläget har över 50 gamla datacenter avvecklats och tre nya datacenter har byggts. Konsolideringen av e-post och nätverk är pågående projekt. Det är oklart när all it-drift kommer att vara konsoliderad till sju moderna datacenter.

Erfarenheter

Erfarenheterna från Kanada är bl.a.:

- Det tar mycket längre tid att konsolidera än förväntat.
- Stort förankringsarbete krävs.
- Komplicerat att konsolidera it-infrastruktur.
- Svårt att bygga en ny infrastruktur samtidigt som befintliga it-system ska fungera.
- Komplicerat att skapa en ny organisation med över 6 000 medarbetare som förts samman från många andra myndigheter.

Att flytta personal, kontrakt, licenser, budgetmedel och hårdvara visade sig vara långt mer komplext än förväntat. I efterhand anser de att ett höggradigt standardiserat förfarande hade varit att föredra.

Att skapa SSC utan att tillföra initiala budgetmedel skapade mycket merarbete och avvägningar. Det hade varit bättre om SSC hade fått en egen budget för att skapa organisation och infrastruktur för att därefter skära i övriga myndigheters budgetar.

Enligt SSC är det viktigt att skapa en myndighet som bedriver sin verksamhet mer som ett företag och mindre som en myndighet.

5.6 Nederländerna

År 2011 lanserade den nederländska regeringen en it-strategi för den centrala förvaltningen. Strategin syftade till att utveckla IT på nationell förvaltningsnivå, att stärka övervakningen över storskaliga nationella it-projekt samt att öka it-kompetensen hos den offentliga sektorn.

IT inom den centrala förvaltningen har konsoliderats från 64 datacenter till 4 och inkluderar skapande av standarder, harmonisering av processer och bildandet av gemensamma servicecenter, SSC-ICT.[31] Ministerierna har fört över sin infrastruktur till nya datacenter. Försvarsministeriet är involverat i projektet för att säkerställa att relevanta säkerhetsrutiner implementeras. Därefter ska en it-säkerhetsfunktion för statsförvaltningen inrättas med en harmoniserad it-säkerhetspolicy.

Den nederländska regeringen har varit framgångsrik i sitt arbete med att effektivisera den statliga förvaltningen med olika initiativ och program. Gentemot medborgare och företag har de tidigt drivit frågan om att minska den administrativa bördan och därefter har fokus riktats på att konsolidera myndigheternas it-resurser och uppnå skalfördelar.

År 2014 inleddes ett arbete med att bygga en statlig molntjänst inom ramen för den redan konsoliderade it-driften. I dagsläget har de 400 fysiska servrar med 12 PB lagring spridda över tre datacenter på två orter. Molntjänsten bygger helt på programvarorna OpenStack, KVM och Ceph. Myndigheterna ansluter till molntjänsten via en säker internet-anslutning.

5.7 Storbritannien

År 2011 fastställde den brittiska regeringen en ny it-strategi inklusive en statlig molnstrategi.[32] I molnstrategin slog regeringen fast att molntjänster ska användas i första hand. I it-strategin ingår även en satsning på att skapa en gemensam it-infrastruktur för offentlig sektor för att leverera delade data-, telefoni- och videotjänster.

Molnstrategin innebär en viljeyttring om en övergång från särskilt utvecklade system till mer generella it-tjänster. För att underlätta myndigheternas övergång till molntjänster har därför en digital marknadsplats skapats. Med satsningen på molntjänster hoppas den brittiska regeringen bättre kunna genomföra:

- Standardisering och förenkling av arbetsplatsen
- Standardisering av nätverken
- Rationalisering av datacenter
- Leverans med öppen källkod
- Fokus på öppna standarder och återanvändning

[31] Statens servicecenter har fått detaljerad information direkt av SSC-ICT vilket utgör bakgrunden till avsnittet.

[32] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/266214/government-cloud-strategy_0.pdf

- Mera grön IT
- Bättre informationssäkerhet

Därtill är det tänkt att molntjänster ska underlätta för regeringen att utveckla och förbättra gemensamma tjänster, mer pålitliga projektleveranser, bättre leverantörsstyrning och professionalisering av it-baserad verksamhetsutveckling.

Det finns ett ramavtal för datacenter som är en överenskommelse mellan den brittiska regeringen och Crown Hosting Data Centres,[33] som är delägt av regeringen. Ramavtalet tillhandahåller tillgång till fysiska datacenter för placering av offentliga myndigheters it-system.

Ramavtalet är ett komplement till regeringens molnstrategi, då många av myndigheterna fortfarande har it-system som inte kan flyttas till en molntjänst. Ramavtalet säkerställer att drift av dessa kan fortsätta under lång tid, kostnadseffektivt och säkert. Ramavtalet för datacenter är ett led i ett medvetet arbete från regeringens sida med att konsolidera datacenter inom offentlig sektor.

[33] http://crownhostingdc.co.uk/

6 Överväganden och förslag

6.1 En statlig molntjänst bör införas

Mot bakgrund av vad som har framkommit i utredningen föreslår Statens servicecenter att merparten av de statliga myndigheternas it-drift samordnas i en statlig molntjänst.

I detta kapitel redovisas motiven för förslaget, hur molntjänsten bör byggas upp och organiseras samt vissa juridiska förutsättningar. Förslagets konsekvenser redovisas i kapitel 7.

6.2 Motiv till en samordnad it-drift i en statlig molntjänst

- Det är ineffektivt och kostsamt att varje myndighet har sin egen it-drift och egna datacenter när uppgiften ser likadan ut för varje myndighet, oavsett kärnverksamhet.
- Med dagens lösning binds onödigt stora kapital- och personalresurser upp i bl.a. redundans, utspridda upphandlingar och drifttekniker.
- Det är sårbart och kostsamt när som idag nästan hälften av statens 206 datacenter är koncentrerade till Stockholm.
- Idag finns det stora variationer i it-säkerheten eftersom det inte blir ekonomiskt försvarbart för den enskilda myndigheten att investera i en tillräckligt hög it-säkerhet.
- Svenska säkerhetsmyndigheter (MUST, FRA och Säkerhetspolisen) tecknar samfällt en allt mörkare hotbild med accelererande cyberangrepp och underrättelseverksamhet mot offentlig it-infrastruktur som underlättas av brister i säkerheten. Både FRA och Säkerhetspolisen pekar särskilt på de brister i säkerhetsskyddet som kan uppstå när it-drift läggs ut på privata företag.
- FRA förespråkar att staten bygger en egen molntjänst, med egna statliga datacenter där samtliga relevanta it-säkerhetskrav kan tillgodoses fullt ut.
- Flertalet av de tillfrågade statliga myndigheterna efterfrågar en statligt samordnad it-drift.

IT-drift är en uppgift som i princip ser likadan ut för varje myndighets it-verksamhet. Dess utformning varierar alltså inte beroende på den enskilda myndighetens kärnverksamhet. Enligt Statens servicecenter är det därför av flera skäl ineffektivt för staten som helhet att som i dagens statsförvaltning decentralisera samma sorts uppgift, it-drift, på över 200 olika sätt. Dagens modell medför att onödigt stort kapital och onödigt stora personalresurser binds upp för varje enskild myndighets it-drift. Dessa resurser skulle istället kunna läggas på kärnverksamheten. Dagens modell har också inneburit en hög koncentration av datacenter till Stockholm, där kostnaderna är högst i Sverige för både lokaler och personal.

En statlig molntjänst för samordnad it-drift, med datacenter placerade utanför storstadsområdena, skulle vara betydligt mer effektiv. Idag måste varje myndighet investera i överkapacitet för att klara sina kapacitetstoppar. En molntjänst möjliggör skalbarhet, dvs. att varje enskild myndighet kan köpa den kapacitet myndigheten behöver när denna kapacitet behövs.

Dagens decentraliserade modell medför också att upphandlingsprocessen blir mindre effektiv än vad fallet skulle vara med en samordnad lösning. Idag är upphandling av it-tjänster utspridd på över 200 olika upphandlande myndigheter, vilket medför högre kostnader såväl för lokaler som för inköp av servrar, lagring, support och drift. Kostnaderna blir högre både för själva upphandlingarna och i form av sämre priser då volymen per upphandling är jämförelsevis låg. I bl.a. tidigare studier har det också uppmärksammats en rad problem med myndigheternas beställarroll och hanteringen av upphandlingsprocessen för it-verksamheten. En statlig molntjänst skulle möjliggöra att it-drift kan beställas och byggas med större expertis vilket skulle gynna konkurrensen och ge en effektivare användning av offentliga medel.

Det finns också inlåsningar till enskilda leverantörer vilket ger högre kostnader och är oflexibelt, något som påverkar kärnverksamheten negativt. Det kan exempelvis vara mycket svårt att ta till vara vinster med den tekniska utvecklingen p.g.a. inlåsningen till vissa leverantörer och deras produktlösningar.

Dagens decentraliserade modell är också negativ för it-säkerheten. För många myndigheter är det idag inte ekonomiskt möjligt att investera i en tillräckligt hög it-säkerhet. Det kan däremot ske om it-driften samordnas för hela statsförvaltningen, till nytta för staten som helhet.

På senare år har flera händelser i omvärlden synliggjort behovet för stater och statliga myndigheter att bättre hantera sårbarheten i den offentliga it-infrastrukturen. Myndigheters it-miljöer är ständigt utsatta för attacker, intrång och avlyssning. De proprietära programvaror som ofta används i dag innebär att användaren inte får tillgång till programvarans källkod. Detta innebär att staten inte har insyn i hur programvaran fungerar i detalj. Sådan programvara är därför olämplig i it-system som hanterar känslig information.

Därutöver uppmärksammar de svenska säkerhets- och underrättelsemyndigheterna MUST, FRA och Säkerhetspolisen samfällt att det finns en ökande hotbild mot Sverige och svensk informationsinfrastruktur. De beskriver underrättelseverksamhet och påverkansoperationer mot svenska it-system och en accelererande utveckling av cyberangrepp mot myndigheter och andra institutioner. De understryker också att utkontraktering av myndigheters it-verksamhet ofta ökar sårbarheten. Både FRA och Säkerhetspolisen pekar särskilt på de brister i säkerhetsskyddet som kan uppstå när it-drift läggs ut på privata företag. FRA förespråkar också att staten bör bygga en egen molntjänst, med egna statliga datacenter där relevanta it-säkerhetskrav verkligen kan tillgodoses.

Med dagens decentraliserade modell varierar även driftsäkerheten mellan olika myndigheters it-miljöer. För många myndigheter är det inte ekonomiskt försvarbart att investera i tillräckligt hög driftsäkerhet. Även den stora koncentrationen till Stockholmsområdet påverkar driftsäkerheten i statens it-system, eftersom förutsättningarna för elförsörjning,

enligt Svenska kraftnät, är sämre i Stockholm än på många andra platser i landet. Att istället bygga en distribuerad och robust molntjänst skulle möjliggöra extremt hög tillgänglighet och driftsäkerhet för hela statsförvaltningen samtidigt som det är kostnadseffektivt. Den statliga molntjänsten kan placera sina datacenter på platser i landet med optimal tillgång till el- och fiberförsörjning.

Många statliga myndigheter efterfrågar också en samordnad, dynamisk och flexibel it-drift. Detta framgår tydligt av både tidigare studier och mötena med 15 av de större myndigheternas it-ledningar. En samordnad it-drift i form av en statlig molntjänst är något som de tillfrågade myndigheterna ofta välkomnar och ser fram emot att ansluta sig till.

Samordning av statlig it-drift är en allmän trend i västvärlden. Som framgår av kapitel 5 har flera andra länder genomfört konsolideringar och samordnande reformer för att utveckla och effektivisera it-verksamheten i staten.

Sammantaget finns alltså en rad fördelar med att merparten av de statliga myndigheternas it-drift samordnas i en statlig molntjänst. Det finns också osäkerheter med en sådan förändring, t.ex. att staten skulle vidta ett omfattande projekt med viss risk och som medför en relativt stor investering. Statens servicecenters bedömning är ändå att fördelarna överväger osäkerheterna, i synnerhet i ljuset av de nackdelar som finns med dagens decentraliserade modell.

6.3 Molntjänstens uppbyggnad

- Det krävs maximalt tio datacenter i statens molntjänst för att uppnå maximal effekt till lägsta kostnad.
- Datacenter i statens molntjänst placeras utanför storstadsområdena.
- Statens befintliga tillgångar utnyttjas. Det är kostnadseffektivt, medger en effektiv resursanvändning och är säkerhetsmässigt effektivt.
- I möjligaste mån ska all programvara som används ha öppen källkod.

Det är väsentligt att statens molntjänst bygger på en långsiktig strategi. Molntjänsten bör därför konstrueras så att hela lösningen, ur alla aspekter, blir stabil i minst 25 år.

Statens molntjänst ska präglas av ett öppet arbetssätt, t.ex. genom:

- I möjligaste mån ska all programvara som används ha öppen källkod med licens godkänd av Open Source Initiative.[34]
- Ett öppet deltagande i de grupperingar (s.k. communities) där utvecklingen sker av den öppna källkod som statens molntjänst använder.

[34] https://opensource.org/licenses/alphabetical

- Användning av öppna källor (s.k. repositories) för utvecklingen av statens molntjänsts programvaror.
- Konfigurationen av programvara och hårdvara för statens molntjänst bör vara helt öppen om inte säkerhetskrav förhindrar detta.
- Det bör lämnas publik information om vilken typ av hårdvara statens molntjänst använder.

Statens servicecenter bedömer att maximalt tio datacenter krävs i statens molntjänst för att uppnå maximal effekt till lägsta kostnad. Av säkerhetsskäl bör merparten av datacenter, precis som liknande försvarsanläggningar, placeras i bergrum. Dessa bör finnas utanför storstadsområdena.

Statens molntjänst kan och bör byggas upp på statens befintliga tillgångar i form av t.ex. Fortifikationsverkets bergrum och Svenska kraftnäts och Trafikverkets fiber. Detta har flera fördelar, exempelvis:

- Ledtiderna för att realisera statens molntjänst kortas.
- Eventuella problem med bygglov reduceras.
- Statens befintliga tillgångar utnyttjas. Det är kostnadseffektivt, medger en effektiv resursanvändning och är säkerhetsmässigt effektivt.

Befintliga bergrum kräver omfattande ombyggnad för att anpassas till statens molntjänst, dock utan att ny mark tas i anspråk. Det skulle visserligen kosta mindre att bygga ovan mark än att utnyttja bergrum, men byggnation ovan mark är mer sårbart för fysiska angrepp.

Med hjälp av olika system för larm, övervakning, loggning och statistik kan personalen som sköter drift och övervakning i realtid följa hela tjänstens utnyttjande och avvikelser.

För enstaka myndigheter med synnerliga behov kan s.k. co-location komma att erbjudas. Detta måste dock utredas vidare.

Beträffande Fortifikationsverkets roll i sammanhanget bör vidare nämnas att Fortifikationsverket utgör statens ägarföreträdare för bland annat försvarsfastigheter.[35] Myndigheten är i sin helhet intäktsfinansierad genom uthyrnings- och uppdragsverksamhet.

Fortifikationsverkets bestånd av försvarsfastigheter består av två huvuddelar. I *det öppna beståndet* ingår främst garnisons- samt flottiljområden med tillhörande byggnader samt övnings- och skjutfält. *Det slutna beståndet* utgörs av ändamålsfastigheter för totalförsvarsändamål. I det slutna beståndet ingår anläggningar som exempelvis radarstationer, teleanläggningar, förrådsanläggningar, stridsledningscentraler och ledningsplatser. Vis-

[35] Se förordning (2007:758) med instruktion för Fortifikationsverket och förordning (1993:527) om förvaltning av statliga fastigheter, m.m.

sa av anläggningarna är förlagda i bergutrymmen, inuti dessa berg är oftast ändamålsbyggnader uppförda för respektive verksamhet. Det slutna beståndet omfattas av försvarssekretess.

Inom det slutna beståndet uppför och förvaltar Fortifikationsverket datorcentraler för flera myndighetskunder. I vissa fall är de särskilt uppförda för datorhallsverksamhet, i andra fall sker det genom återbruk, anpassning och utveckling av berganläggningar ursprungligen uppförda för andra ändamål. Fortifikationsverket hyr ut lokaler särskilt anpassade för datorhallsverksamhet som uppfyller högt ställda fortifikatoriska skyddskrav i kombination med tillgänglighetskrav. Tillgång till reservkraft och kyla ingår i verkets normala leverans som även innehåller fastighetsdrift med egen personal i hela konfliktskalan inklusive höjd beredskap.

Mot bakgrund av att vara statens kompetensbärare inom fortifikatoriskt skydd, möjligheter till återbruk av tidigare gjorda investeringar i det slutna beståndet (berganläggningar) inklusive genomförande av nya investeringsprojekt samt förvaltning och drift i egen regi i hela landet utgör Fortifikationsverket en möjlig lokalförsörjare för den statliga molntjänsten. Lokalförsörjningen kan omfatta samtliga eller vissa av de fortifikatoriskt skyddade anläggningarna som föreslås för att realisera den statliga molntjänsten.

En liknande lösning, som kan tjäna som förebild, finns idag i form av att Post- och telestyrelsen (PTS) genom en tecknad huvudöverenskommelse med Fortifikationsverket på ett liknande sätt har valt att lokalförsörja delar av den teleinfrastruktur som ägs av teleoperatörerna och som står under PTS tillsyn inom uppdraget att säkerställa samhällets behov av robusta telekommunikationer i fred, kris och krig. Enligt vad Fortifikationsverket har framfört till oss torde den modell som används gentemot PTS sannolikt kunna tillämpas även inom uppbyggnaden av statens molntjänst.

I bilaga 5 redogörs närmare för molntjänstens tekniska infrastruktur, bland annat gällande lokaler, elförsörjning, nätverk, datorkapacitet, lagring, programvara och administration.

6.4 Molntjänstens organisation

- Statens molntjänsts verksamhetsledning placeras utanför storstadsområdena.
- Utvecklingsverksamheten förläggs till två orter med stor geografisk distans. De bör väljas utifrån perspektivet att finna den bästa kompetensen rörande datacenter.
- Dygnet runt under årets alla dagar finns utvecklare och datacentertekniker på plats på de två orter dit utvecklingsverksamheten förläggs.
- Totalt ca 200 arbetstillfällen skapas för verksamheten. Merparten utanför Stockholmsområdet.

Mot bakgrund av tidigare studier och vad som framförts till Statens servicecenter från större myndigheters it-chefer, finns det primärt två huvudsakliga organisationsformer för att inrätta statens molntjänst. Att det antingen sker inom ramen för en befintlig myndighet eller genom att statens molntjänst inrättas som en nybildad myndighet som endast har detta uppdrag. Frågan om vilken organisationsform som vore lämpligast kräver ytterligare utredningsarbete. Ett förslag om formerna för ett fortsatt utredningsarbete återfinns i kapitel 8.

Principiellt sett bör den centrala organisationen för statens molntjänst inrättas på tre orter med stor geografisk distans. Vid dessa tre orter bör bl.a. följande roller finnas:

- Huvudort (totalt ca 20–25 personer): verksamhetsledning, 1–2 generella administratörer inklusive registrator, internrevisor, säkerhetschef, it-säkerhetsansvarig, informationssäkerhetsansvarig, signalskyddschef, säkerhetshandläggare, kundtjänstansvarig, 2–3 jurister, 3–4 upphandlare, kommunikatör, hållbarhetsansvarig samt intern it-tekniker.
- Primär utvecklingsort (totalt ca 24–30 personer): teknisk chef, 5 datacentertekniker, chef för utveckling och produktion, 10–15 utvecklare (DevOps), driftchef, säkerhetspersonal, 3 kundtjänstpersonal samt intern it-tekniker.
- Sekundär utvecklingsort (totalt ca 20–25 personer): 10–15 utvecklare (DevOps), 5 datacentertekniker, säkerhetspersonal, 3 kundtjänstpersonal samt intern it-tekniker.

Vidare behöver respektive datacenter ha 5 drifttekniker med beredskapstjänstgöring. Dessa tekniker ska inte ha behörighet till molntjänsten utan endast kunna hantera anslutningar av el och fiber, sköta om kylanläggning, installera och byta hårdvara samt övervaka status på hårdvara. Statens servicecenter bedömer att det dessutom behövs 10 personer per datacenter för bevakning.

Det ska dygnet runt och årets alla dagar (24/7/365) finnas utvecklare (DevOps) och datacentertekniker på plats på någon av centralorterna samt bevakningspersonal utanför respektive datacenter. Resurspersoner med verksamhetskritiska uppgifter fördelas mellan centralorterna för att minska risken för störningar p.g.a. sjukdom, väderlek o. dyl.

Samtliga anställda och uppdragstagare hos statens molntjänst ska omfattas av tystnadsplikt i sin anställning. Detta förutsätter att de författningsändringar som föreslagits genomförs (se avsnitt 6.7).

Det finns idag inom statsförvaltningen kvalificerad personal som skulle vara lämplig för att sköta de fysiska datacentren, t.ex. avseende el, kyla, larm och datorer. Kvalificerade tekniker kan erbjudas verksamhetsövergång till statens molntjänst. För arbetet med att bygga, utveckla och förvalta den statliga molntjänsten krävs dock sannolikt att nyrekryteringar sker utanför statsförvaltningen. Detta då molntjänsten ska bygga på modern öppen teknik som i dagsläget är ovanlig bland myndigheterna. Sannolikt finns det därför i dagsläget endast ett fåtal tekniker i statsförvaltningen som är tillräckligt kvalificerade och har tillräcklig potential för denna uppgift.

De två utvecklingsorterna bör väljas utifrån perspektivet att finna den bästa kompetensen rörande datacenter. Lokaliseringen av datacenter behöver utredas noggrannare, med beaktande av bl.a. följande aspekter:

- Säkerhet
- Tillgänglighet
- Belägenhet av lämpliga bergrum
- Var stamnät för el går genom landet samt var distributionsnät går i förhållande till bergrummen
- Var stamnät för fiber går genom landet samt var distributionsnät går i förhållande till bergrummen
- Geografisk belägenhet av de statliga myndigheterna

Med hänsyn till att statens molntjänst kommer att tillhandahålla tjänster som är vitala för statsförvaltningen och samhällets funktion bedöms att större delen av personalen hos statens molntjänst vid arbetsmarknadskonflikt bör ha begränsade stridsåtgärder. Detta då det bör anses som samhällsfarligt om personalen t.ex. strejkar. För att en stridsåtgärd ska klassas som samhällsfarlig ska den störa viktiga samhällsfunktioner eller medföra fara för människors liv och hälsa. Om en konflikt är samhällsfarlig avgörs av en nämnd som tillsätts av de kollektivavtalsslutande parterna. Inom den statliga sektorn av arbetsmarknaden är frågor om samhällsfarliga arbetsmarknadskonflikter hanterade i lagstiftning och avtal. En motsvarande reglering saknas för den privata sektorn.

Det behöver utredas vidare om statens molntjänst ska utgöra en del av totalförsvaret och vad som gäller för verksamheten vid höjd beredskap.

Statens molntjänst ska inte konkurrera med den öppna marknaden gällande konsulttjänster eller andra it-tjänster där det inte finns välgrundade skäl t.ex. i förhållande till specifik lagstiftning eller av totalförsvarsskäl.

6.5 Molntjänstens användning

- Molntjänsten kommer att erbjuda två tjänster: datorkraft och lagring.
- För anslutna myndigheter kommer tjänsten att vara helt skalbar och flexibel.
- Beställning av kapacitet kommer att vara fullt automatiserad.
- Ingen upphandlingsprocess för it-drift krävs för anslutna myndigheter.

Initialt kommer statens molntjänst endast att tillhandahålla två tjänster:

- Datorkapacitet
- Lagring

Båda dessa tjänster kommer att hålla en mycket hög säkerhetsnivå, som blir likadan för alla anslutna myndigheter. Teoretiskt sett skulle det visserligen vara möjligt att tillhandahålla mer avancerade tjänster, men det bör undvikas i ett inledningsskede eftersom

det skulle fördröja projektet. Detta skulle även medföra ett flertal juridiska och tekniska utmaningar som bör undvikas vid molntjänstens införande.

En stor fördel med molntjänsten är att en storskalig delad infrastruktur av detta slag gör det både tekniskt och ekonomiskt möjligt att tillhandahålla i princip vilken prestanda som helst. Dessutom kan förändringar av prestandan normalt göras i princip utan fördröjning. Datorkapaciteten och lagringen är helt flexibel och kan när som helst förändras av den myndighet som använder tjänsten.

Som framgått ska statens molntjänst initialt endast erbjuda datorkapacitet och lagring, dvs. molntjänsten tillhandahåller endast en underliggande infrastruktur. Detta innebär att innehållet i varje it-system (operativsystem och applikationer) är separat och utanför statens molntjänsts kontroll. Statens molntjänst kan se att en viss myndighet använder en viss datorkapacitet i ett visst datacenter och hur mycket data myndigheten lagrar. All administration av datorkapacitet och lagring sker under strikt åtkomstkontroll, och alla händelser som är av betydelse för säkerheten i molntjänsten registreras i en säkerhetslogg med oavvislighetsmekanismer motsvarande de krav som ställs av KSF.[36] Säkerhetsloggen används för spårning av intrång och överskridandet av befogenheter. Tekniskt sett kan alltså personal hos statens molntjänst bereda sig otillbörlig åtkomst till en myndighets data, men inte utan att denna åtgärd loggas på ett sätt som inte kan manipuleras av personalen.

Som framgår av avsnitt 6.7 bedöms att en statlig myndighet som anlitar statens molntjänst kommer att kunna göra detta utan att det föreligger någon rättslig skyldighet för myndigheten att i konkurrens upphandla it-driften, dvs. att lagen (2016:1145) om offentlig upphandling (LOU) inte blir tillämplig. För de myndigheter som använder statens molntjänst undanröjs därmed dagens problem med korta kontrakt, svåra kravspecifikationer, personalövergångar till privata företag[37] samt bekymmer med att ta hem sin it-drift eller flytta den till ny utförare. Myndigheterna slipper också oflexibla avtal för it-drift där alla förändringar gentemot kontrakt ska förhandlas och prissättas, eftersom myndigheter anslutna till statens molntjänst när som helst kan köpa hur mycket kapacitet de vill till fasta priser.

Statens servicecenter förordar att samtliga myndigheter under regeringen i normalfallet flyttar all sin it-drift till statens molntjänst. Undantag bör i princip endast göras för myndigheter med särskilt säkerhetskänslig information, dvs. främst Försvarsmakten, FMV, Totalförsvarets forskningsinstitut, Säkerhetspolisen och FRA. För detta talar bl.a. att statens molntjänst för att kunna bli kostnadseffektiv måste hantera en stor total volym av it-drift. Därmed går det att realisera samordningsvinster och uppnå en effektiv hantering

[36] Försvarsmakten *Krav på IT-säkerhetsförmågor hos IT-system, v3.1* FM2014-5302:1.

[37] Gartner (2016) *Underlag till arbetet med förvaltningsansvar för gemensamma lösningar och förmågor avseende IT-drift och datorhallar*. På uppdrag av Näringsdepartementet/Regeringskansliet.

av it-driften. Tidigare försök har visat att statsförvaltningen inte har den verksamhetslogik som krävs för att, genom exempelvis samverkan och delegationer, mäkta med att uppnå samordningsvinster på it-området för staten som helhet.

Att införa statens molntjänst kommer sannolikt att ta upp till fem år från det att regeringen fattar beslut om införandet. Statens servicecenter bedömer att det praktiska genomförandet på ett övergripande plan kommer att bestå av följande moment, där punkt 4–6 kan göras samtidigt av alla myndigheter:

1. Information till alla myndigheter att de om 4–5 år kommer att kunna flytta sin it-drift till statens molntjänst.
2. Uppbyggnad av statens molntjänst.
3. Test och granskning av statens molntjänst.
4. Respektive myndighet skapar sina virtuella servrar och lagringsytor i statens molntjänst.
5. Respektive myndighet migrerar sina applikationer och data till statens molntjänst.
6. När respektive myndighet har slutfört sin migrering avvecklar de sina befintliga datacenter.

Vissa it-system bör av tekniska skäl initialt undantas från att flyttas till statens molntjänst. Dessa är beräkningskluster (s.k. HPC), stordatorer samt servrar som kräver någon form av specialhårdvara. Anledningen till detta är att det finns svårigheter med att ta hand om den typen av system i en öppen standardiserad molntjänst. I en framtid bör i första hand system som i dagsläget kräver stordator eller speciell hårdvara förändras så att de kan flyttas till molntjänsten.

6.6 Molntjänstens finansiering

- Statens molntjänst blir helt avgiftsfinansierad i drift.
- Under uppbyggnadsfasen krävs anslagsfinansiering.
- En kritisk förutsättning är att den totala volymen av it-drift blir tillräckligt stor för att samordningsvinster och effektivitet ska kunna uppnås.

Varje tjänst i statens molntjänst (datorkapacitet och lagring) ska ha en fast och tydligt redovisad prissättning. Molntjänsten ska bygga på att myndigheterna betalar för den datorkapacitet de faktiskt har använt. Likaså ska lagring betalas i efterskott utifrån den exakta mängden data myndigheten lagrat.

Gentemot myndigheterna ska statens molntjänst tydligt ange vilken tillgänglighet som garanteras. Om molntjänsten under en given månad har misslyckats med att uppnå avtalad tillgänglighet ska ingen ersättning utgå till statens molntjänst för den tjänsten. Detta är ett sätt att över tid hålla statens molntjänst aktiv och kundfokuserad.

För den initiala investeringen under molntjänstens uppbyggnadsfas, under de första fem åren, krävs anslagsfinansiering och finansiering genom räntekontokredit. Om verksamheten skulle vara anslagsfinansierad även därefter, och dessutom bygga på obligatorisk anslutning, skulle det finnas stor risk för att statens molntjänst blir en ineffektiv och trög organisation.

När statens molntjänst väl är i stadigvarande drift ska verksamheten därför inte vara anslagsfinansierad utan finansieras med avgifter som tas ut av de anslutna myndigheterna. Tjänsten måste alltså vara så effektiv att den bär sina egna kostnader, vilket bl.a. garanterar att den hela tiden förblir aktiv och relevant för myndigheterna.

Principen för avgiftssättningen för en tjänst i statens molntjänst ska vara full kostnadstäckning. I full kostnadstäckning bör dock inkluderas en avgiftskomponent som möjliggör för statens molntjänst att kontinuerligt göra nödvändiga nyinvesteringar i hårdvara och vidareutveckla tjänsterna.

En statlig molntjänst kommer sannolikt att befinna sig i ständig tillväxt. Det kommer att kräva finansiering, utrymme samt en design som utgår från detta. Vid införandet av statens molntjänst är utgångspunkten dagens behov och med möjlighet att hantera minst 100 procent mer än detta behov.

6.7 Rättsliga förutsättningar

- De rättsliga förutsättningarna för inrättandet av statens molntjänst behöver utredas inför att tjänsten inrättas. Detta bör ske inom ramen för det utredningsuppdrag som Statens servicecenter föreslår.
- Enligt Statens servicecenters bedömning behövs författningsändringar för att säkerställa att de sekretessreglerade uppgifter som myndigheterna lagrar i molntjänsten har ett tillräckligt skydd.
- Statens servicecenter bedömer att myndigheternas användning av statens molntjänst inte förutsätter att tjänsten upphandlas.

Utgångspunkten är att de anslutna myndigheterna ska kunna lagra och bearbeta alla typer av handlingar och uppgifter i molntjänsten. Den behöver därför utformas så att uppgifterna får det skydd som är nödvändigt med hänsyn till bl.a. regler om sekretess och dataskydd. Detta kommer att kräva att de rättsliga förutsättningarna utreds närmare inför att tjänsten utformas och inrättas. Exakt vilka åtgärder som behöver vidtas beror på hur tjänsten utformas.

E-delegationen har i ett delbetänkande redogjort för de rättsfrågor avseende sekretess som aktualiseras när en myndighet sköter teknisk lagring och bearbetning av handlingar för en annan myndighets räkning.[38] I det följande redogörs därför mycket kortfattat för

[38] SOU 2014:39 *Så enkelt som möjligt för så många som möjligt: Bättre juridiska förutsättningar för samverkan och service*.

de viktigaste övervägandena. I övrigt hänvisas till betänkandet. Statens servicecenter ansluter sig till e-delegationens bedömningar och förslag.

Såsom molntjänsten är föreslagen innebär den att en myndighet utför teknisk lagring och bearbetning av uppgifter för en annan myndighets räkning. Detta innebär att de handlingar som myndigheterna lagrar i tjänsten kommer att vara tillgängliga för molntjänsten på det sätt som avses i 2 kap. 3 § tryckfrihetsförordningen (TF). De är därför att anse som förvarade hos statens molntjänst. Enligt Statens servicecenters bedömning förvaras handlingarna hos molntjänsten som ett led i teknisk bearbetning och lagring för annans räkning. Detta innebär att de enligt 2 kap. 10 § TF inte är allmänna handlingar hos molntjänsten och därför inte ska lämnas ut på begäran.

De anställda hos statens molntjänst kommer att ha tekniska möjligheter att i vissa fall få tillgång till uppgifter som myndigheterna lagrar i molntjänsten. Det faktum att handlingarna inte är allmänna handlingar hos statens molntjänst innebär inte att de har ett tillräckligt skydd i de fall uppgifterna omfattas av sekretess. För att uppgifterna ska skyddas krävs att de omfattas av tystnadsplikt. Uppgifter som förvaras hos en myndighet som led i teknisk bearbetning och lagring för annans räkning omfattas med vissa undantag inte av tystnadsplikt. Det är heller inte möjligt att genom avtal mellan myndigheterna införa en sådan tystnadsplikt för molntjänstens anställda. Det är därför enligt Statens servicecenters bedömning nödvändigt att det införs en tystnadsplikt som omfattar de uppgifter som andra myndigheter lagrar i molntjänsten. Statens servicecenter ansluter i denna fråga till de bedömningar och förslag som e-delegationen lämnat i ovannämnda betänkande.

Statens molntjänst kommer att behandla personuppgifter på uppdrag av andra personuppgiftsansvariga myndigheter, i vart fall för lagring. Dataskyddsförordningens bestämmelser är därför tillämpliga på hanteringen.[39] Utgångspunkten är att statens molntjänst enbart kommer att behandla personuppgifter som personuppgiftsbiträde. Det innebär att varje myndighet som anlitar statens molntjänst kommer att behöva teckna personuppgiftsbiträdesavtal med statens molntjänst. Dataskyddsförordningens bestämmelser ställer höga krav på innehållet i personuppgiftsbiträdesavtal vilket måste beaktas. I rollen som personuppgiftsbiträde kommer statens molntjänst också att få ett självständigt ansvar för att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifterna som behandlas.

Det finns en potentiell risk ur integritetsperspektiv då en stor mängd data om individer kommer att lagras i statens molntjänst. Statens molntjänst kommer dock inte att ha tillgång till några myndigheters data utom i enskilda fall, t.ex. vid en forensisk utredning. När tjänstens utformning och organisering bestäms bör ändå en analys av vilka integritetsrisker det medför att samla statliga myndigheters information i en och samma molntjänst göras.

Det finns två sidor av upphandlingsregelverket att beakta i detta sammanhang, dels när statens molntjänst ska skapas och underhållas, dels när myndigheterna använder statens

[39] EU 2016/670.

molntjänst. När de anslutande myndigheterna ska använda statens molntjänst behöver dessa inte upphandla dessa enligt 3 kap. 17 § LOU samt denna reglerings förtydligande i propositionen 2015/16:195 *Nytt regelverk om upphandling*.[40]

I bilaga 6 beskrivs resonemanget ovan mer i detalj tillsammans med en beskrivning av de övriga författningar som är relevanta i detta sammanhang.

[40] Regeringens proposition 2015/16:195 *Nytt regelverk om upphandling.* Se också bilaga 6 till denna rapport.

7 Förslagets konsekvenser

7.1 Statsfinansiella och miljömässiga effekter

Förslaget om att inrätta en gemensam, statlig molntjänst för myndigheternas it-drift medför:

- Stora besparingar för statskassan,
- kraftigt reducerad miljöpåverkan,
- eliminerat behov av att upphandla it-driften för anslutna myndigheter och därmed kortare ledtider och lägre administrativa kostnader,
- leverantörsoberoende, samt
- den fulla it-kapacitet som statsförvaltningen kräver i varje givet ögonblick.

Förslaget om att inrätta en gemensam, statlig molntjänst för myndigheternas it-drift medför en avsevärd ekonomisk besparing för staten. Med en statlig molntjänst delar myndigheterna på all infrastruktur. Det ger lägre kostnader eftersom varje myndighet inte längre självständigt behöver inneha infrastruktur för värsta tänkbara scenario. Det samlade behovet av hårdvara, kylanläggningar och avbrottsfri kraft minskar betydligt för statsförvaltningen. Det krävs väsentligt färre it-tekniker för att sköta systemen; uppskattningsvis kan staten som helhet spara in ca 600 årsarbetskrafter på sådana arbetsuppgifter. En miljö helt utan leverantörsberoende möjliggör också fullständig konkurrensutsättning av alla delar vilket sänker inköpskostnaden väsentligt jämfört med äldre system där leverantörsinlåsning ofta förekommer.

Vidare kommer den statliga molntjänstens datacenter, högst tio stycken, att byggas upp med modern, miljövänlig teknik. Teknikutvecklingen på detta område har tagit stora kliv de senaste tio åren. Moderna och större datacenter byggs på helt andra sätt idag, vilket innebär att statsförvaltningen genom statens molntjänst kommer att få mycket lägre elkostnader. Det samlade behovet av lokalytor kommer också att bli betydligt mindre med den gemensamma lösningen, och lokalerna kommer dessutom till stor del att ligga utanför storstäderna, vilket sammantaget minskar statens lokalkostnader.

De samlade ledtiderna minskar också för hela statsförvaltningen då nya it-system kan skapas utan att varje enskild myndighet behöver upphandla hårdvara eller programvara. Därtill minskar de administrativa kostnaderna eftersom det blir färre anställda och färre offentliga upphandlingar.

Statens servicecenter bedömer att den ekonomiska besparingen för statsförvaltningen kommer att börja realiseras fem år efter att statens molntjänst tas i drift. Därefter kommer besparingen gradvis att öka i takt med att myndigheterna kan minska sin lokalyta, elförbrukning, serviceavtal, hårdvaruinköp och personal. Efter tio år beräknas statens molntjänst medföra 30 procent lägre kostnader för statsförvaltningens it-drift jämfört med 2016.

De starkt positiva miljökonsekvenserna realiseras betydligt snabbare än de ekonomiska, eftersom effektuttaget från elnätet sjunker för varje avstängd gammal utrustning och den moderna utrustningen kräver väsentligt lägre effekt för att uppnå samma prestanda. Baserat på erfarenheter från andra länder och teknisk expertis som har rådfrågats, bedöms att effektuttaget efter tio år kommer att ha minskat med 80 procent jämfört med hur mycket de anslutna myndigheternas it-drift idag belastar elnätet.

7.2 Effekter på driftsäkerheten för statens IT

Driftsäkerheten i statens molntjänst kommer att uppnå en långt högre nivå än vad många myndigheter eller svenska företag i dagsläget är i närheten av.

Statens molntjänst ska byggas upp utifrån en långsiktig strategi. Hela lösningen ska ur alla aspekter vara stabil i minst 25 år. Detta behövs som målsättning men framförallt för att kunna få ut maximal effektiviseringsvinst.

Statens molntjänst ska byggas på sådant sätt att ett helt datacenter kan vara utslaget utan att någon myndighet på något sätt drabbas av dataförlust eller bristande tillgänglighet. Statens molntjänst måste därför ha mycket höga krav på driftsäkerhet, redundans och överkapacitet för att kunna tillgodose alla myndigheters behov även vid t.ex. en naturkatastrof.

Den fysiska säkerheten består av skalskydd i form av bergrum med larm, brandskydd, inpasseringssystem och inbrottsskydd.

För att uppnå denna nödvändiga och mycket höga tillgänglighet krävs det att varje datacenter har minst två helt separerade framföringsvägar av elektricitet samt minst tre, fysiskt och logiskt, helt separerade framföringsvägar av datakommunikation. Datakommunikationen ska produceras av olika leverantörer och transporteras i olika stamnät genom Sverige. Datacentren ska vara flervägsanslutna till elnätet med olika framföringsvägar. Den övergripande nivån tas fram och förvaltas i samarbete med MSB samt PTS. På den lägre nivån ska samarbete i första hand ske med Trafikverket, Svenska kraftnät och Teracom, i andra hand med kommersiella fibernätleverantörer.

7.3 Effekter för statens it-säkerhet

IT-säkerheten för hela statsförvaltningen kommer att bli mycket hög och utan kompromisser.

IT-säkerheten i statsförvaltningen är mycket varierande idag. Det framgår av både tidigare studier och dialogmötena med it-avdelningarna. Med statens molntjänst kommer den nationella it-säkerheten däremot att få en genomgående mycket hög nivå. Detta då äldre och ibland osäkra, t.ex. bristande skalskydd och redundans, datacenter stängs ner och ersätts med betydligt säkrare, moderna och väl underhållna datacenter.

Att uppnå hög it-säkerhet är både tids- och resurskrävande, och därför av bl.a. ekonomiska skäl inte möjligt för de flesta myndigheter idag. I en statlig molntjänst är det

däremot fullt möjligt och ekonomiskt försvarbart att lägga både tillräckligt med tid och resurser på alla delar av säkerheten.

Hela infrastrukturen måste i statens molntjänst vara 100 procent leverantörsoberoende. Det gäller för både den fysiska infrastrukturen (lokaler, geografisk placering, fiber, el, datorer m.m.) och den logiska (programvaror, design, protokoll, kompetens etc.). Att inte ha ett fullständigt leverantörsoberoende skulle nämligen medföra en oacceptabel risk för att enskilda leverantörer negativt kan påverka molntjänstens tillgänglighet, säkerhet och prestanda.

Statens molntjänst ska vara dynamisk, skalbar och med säkerhet anpassad för varje it-system, t.ex. unika brandväggsregler och separerad lagring, och inte utgå från gamla axiom gällande it-säkerhet. Därmed uppnås högre robusthet i hela tjänsten liksom i de anslutna myndigheternas enskilda it-system.

För att skapa tillräcklig säkerhet och förtroende för statens molntjänst kommer som utgångspunkt att krävas att varje ansluten myndighet och deras it-system betraktas som osäkra och enkla för en antagonist att attackera. I praktiken är detta ett överdrivet antagande, men det behövs för att garantera fullgod säkerhet i statens molntjänst ur alla aspekter.

Samtliga it-system som utgör plattform och stödsystem för statens molntjänst måste vara härdade utifrån antagandet att en angripare kan komma att bryta sig ur en myndighets datorkapacitet eller container. När detta händer måste integriteten hos övriga it-system i största möjliga mån skyddas genom olika typer av hinder och avgränsningar i molntjänsten.

7.4 Konsekvenser för it-branschen

- Förslaget innebär minskade intäkter för de företag som levererar it-drifttjänster till staten.
- Statens molntjänst kommer att behöva upphandla tjänster från företag som tillhandahåller expertis inom molntjänster, datacenter och öppen källkod.

Att bygga en statlig molntjänst, dessutom med öppen källkod och öppen hårdvara, innebär att företag som säljer it-drifttjänster eller proprietär hårdvara och programvara till staten kan komma att förlora kunder. Dessa effekter uppstår huvudsakligen hos utländska företag då svensk hårdvaruindustri är i det närmaste obefintlig och svensk programvaruindustri i mycket liten utsträckning utvecklar programvara av den sort som kommer att användas i statens molntjänst.

Etablerandet av statens molntjänst bedöms innebära en ökad efterfrågan på it-konsulttjänster från företag som kan tillhandahålla expertis inom molntjänster, datacenter och öppen källkod.

7.5 Konsekvenser för arbetstagare

Som framgått av kapitel 3 visar enkäten bland de statliga myndigheterna att de myndigheter som idag bedriver sin it-drift i egen regi sysselsätter motsvarande 800 årsarbetskrafter för detta. Samtidigt bedöms att statens molntjänst kommer att behöva ca 200 årsarbetskrafter för sin verksamhet. Vissa av dessa personer kommer att kunna gå över från andra myndigheter, men sannolikt behöver ett flertal nyrekryteras på marknaden. Sammantaget bedöms alltså att ca 600 årsarbetskrafter kan sparas in genom bildandet av statens molntjänst, vilket i sin tur sannolikt medför att betydande övertalighet sammantaget uppstår i myndigheterna.

Den beskrivna utvecklingen medför flera konsekvenser och utmaningar som måste hanteras inför inrättandet av statens molntjänst:

- Arbetsrättsliga regler om bl.a. verksamhetsövergång kan eventuellt aktualiseras.[41]
- Att rekrytera lämplig kompetens på marknaden kan bli komplicerat. För närvarande upplever många myndigheter brist på it-kompetens. Det visar Arbetsgivarverkets konjunkturbarometer från juli 2016. I den uppgav 54 procent av Arbetsgivarverkets medlemmar att de haft brist på lämpliga sökanden inom it-verksamhet. Bristen bedömdes vara liten när det gäller it-support, men hög bland den kompetens som bygger och utvecklar it-system.[42]

Statens servicecenter bedömer dock att den kvalificerade it-kompetens som behövs kan rekryteras då molntjänsten och den föreslagna tekniken är lockande att få arbeta med.

[41] Närmare information om gällande regler finns bl.a. på Arbetsgivarverkets webbplats. Se också Servicecenterutredningens betänkande SOU 2011:38 *Ett myndighetsgemensamt servicecenter*.

[42] https://www.arbetsgivarverket.se/nyheter--press/nyhetsbrev/arbetsgivarverket-informerar/2016/hogkonjunktur-okar-statliga-medarbetares-rorlighet/

8 Behov av fortsatt utredningsarbete

Statens servicecenter bedömer att det sannolikt kommer att ta upp till fem år att införa statens molntjänst från det att regeringen fattar beslut om införandet. Detta betyder i sin tur att det behövs fortsatt utredningsarbete innan statens molntjänst kan inrättas. I detta kapitel redogörs för de huvudsakliga insatser som behöver göras i det fortsatta arbetet.

Det fortsatta utredningsarbetet bedöms lämpligen bedrivas i två steg:

- Fortsatta och fördjupade analyser som behöver göras innan beslut kan fattas om att inrätta statens molntjänst.
- Mer praktiskt genomförandearbete för att inrätta statens molntjänst efter att beslut om detta väl har fattats.

I *steg 1* föreslår Statens servicecenter att regeringen i närtid initierar ett uppdrag att närmare analysera förutsättningarna för att inrätta statens molntjänst. Uppdraget, som bör bygga på föreliggande rapport, kan ges till en offentlig utredning eller som ett uppdrag till Statens servicecenter eller någon annan lämplig myndighet.

Utredningen bör bl.a. närmare analysera de juridiska förutsättningarna för att inrätta statens molntjänst. I uppdraget bör vidare ingå att utreda förutsättningarna för att samordna myndigheternas it-drift i en statlig molntjänst i den takt som bäst passar den enskilda myndighetens förutsättningar. Utredningen bör också få i uppdrag att undersöka om det ska vara obligatoriskt för myndigheter att ansluta sig till molntjänsten. Den bör vidare utreda lämplig verksamhetsform för statens molntjänst. Det handlar främst om ifall verksamheten ska bedrivas inom ramen för en befintlig myndighet eller i form av en ny statlig myndighet.

Därutöver behöver utredningen fastställa närmare ansvarsområde och uppgifter för den statliga molntjänsten, inklusive de tekniska förutsättningarna för att kunna genomföra en statlig molntjänst för samordnad it-drift.

I *steg 2*, efter att regeringen har beslutat att statens molntjänst ska inrättas, bör regeringen ge utredaren eller myndigheten i uppdrag att genomföra bildandet av den nya tjänsten och dess organisation.

De frågor som aktualiseras i steg 2 bör vara mer praktiskt inriktade, med ett tydligt etableringsperspektiv. Här bör exempelvis dimensionering, inklusive bemanning fastställas. Utredningen bör också beräkna dimensioneringens budgetära konsekvenser och belysa uppstartskostnader, besparingar och rationaliseringar samt avvecklingskostnader. Utredningen behöver även redogöra för hur verksamhetens samtliga kostnader ska finansieras.

Verksamheten kommer att ha behov av ett stort antal varor och tjänster till sitt förfogande redan innan den driftsätts. Om utredningen ansvarar för att anskaffa dessa är det viktigt att det säkerställs att tillräcklig tid ges för att genomföra både utredningens och verksamhetens upphandlingsprocesser som krävs i samband med att verksamheten startar.

Såväl i steg 1 som i steg 2 av det fortsatta utredningsarbetet bör utredningen tillämpa Kommittéförordningen (1998:1474) inklusive §§ 14–16 om kostnadsberäkningar och konsekvensbeskrivningar.

Regeringens uppdrag

REGERINGEN

Regeringsbeslut III 4

2016-01-28 Fi2016/00274/SFÖ (delvis)

Finansdepartementet

Statens servicecenter
FE 15
801 71 Gävle

Uppdrag till Statens servicecenter att föreslå myndighetsfunktioner som är lämpliga att samordna och omlokalisera

Regeringens beslut

Regeringen uppdrar åt Statens servicecenter att analysera och föreslå vilka funktioner inom de statliga myndigheterna som kan vara lämpliga att bedriva samordnat i staten och utanför storstadsområdena. Uppdraget ska genomföras i samverkan med de myndigheter som Statens servicecenter bedömer är berörda. Myndigheter vars verksamhet av sekretess- och säkerhetsskyddskäl inte är lämplig att bedriva samordnat omfattas inte.

Uppdraget omfattar främst myndighetsfunktioner där det finns möjligheter till stordriftsfördelar, effektiviseringar och kvalitetsförbättringar genom samordning och koncentration.

Uppdraget ska delredovisas till regeringen (Finansdepartementet) senast den 1 juni 2016 och slutredovisas senast den 15 april 2017. I slutredovisningen ska ingå en konsekvensanalys av förslaget. Konsekvensanalysen ska innehålla bl.a. möjliga besparingar, påverkan på den statliga närvaron i och utanför storstadsområdena samt effekterna för myndigheternas verksamheter och kompetensförsörjning.

Kostnaderna för uppdragets genomförande ska belasta det under utgiftsområde 2 Samhällsekonomi och finansförvaltning för budgetåret 2016 uppförda anslaget 1:18 statens servicecenter, anslagsposten 1.

Bakgrund

Av budgetpropositionen för 2015 framgår att regeringen avser att analysera om det finns behov av att koncentrera även andra myndighetsgemensamma tjänster – utöver de som Statens servicecenter erbjuder

Postadress 103 33 Stockholm
Besöksadress Jakobsgatan 24
Telefonväxel 08-405 10 00
Telefax 08-21 73 86
E-post: fi.registrator@regeringskansliet.se

– inom vilka det finns tydliga skalfördelar och samordningsvinster (prop. 2014/15:1).

I 2015 års ekonomiska vårproposition angav regeringen att den statliga servicen och närvaron på landsbygden bör säkras och förbättras (prop. 2014/15:100). I budgetpropositionen för 2016 angav regeringen att det är viktigt att de statliga myndigheternas lokalisering kan få en större spridning över landet (prop. 2015/16:1). I propositionen konstaterades också att det är viktigt att det finns arbetstillfällen för tjänstemän och akademiker även utanför de större städerna. Regeringen angav vidare att vissa myndighetsfunktioner bör utlokaliseras från storstadsområdena. För att hantera frågan samlat och effektivt aviserades ett regeringsuppdrag till Statens servicecenter att föreslå vilka myndighetsfunktioner inom de statliga myndigheterna som vore lämpliga att utlokalisera.

Analyser och förslag om koncentration och samordning av myndighetsgemensamma tjänster och funktioner finns i bl.a. Servicecenterutredningens betänkande (SOU 2011:38) och i E-delegationens olika betänkanden och förstudier se t.ex. Så enkelt som möjligt för så många som möjligt (SOU 2010:20) och En förvaltning som håller ihop (SOU 2015:66). Servicecenterutredningen föreslog att bl.a. genomförandestöd vid myndighetsspecifika upphandlingar, e-arkiv och e-diarium, kontorsstöd och samordning av it-stöd borde övervägas för koncentration i staten.

Skälen för regeringens beslut

Regeringen har det övergripande ansvaret för att statens resurser används på ett effektivt sätt och för att värna de statliga jobben utanför de större städerna. Syftet med underlaget är att skapa en bild av och bedöma möjligheterna till stordriftsfördelar och koncentration av myndighetsfunktioner. Avsikten är att regeringen efter att uppdraget redovisats ska kunna fatta beslut om uppdrag av mer operativ karaktär till Statens servicecenter och andra myndigheter.

På regeringens vägnar

Magdalena Andersson

Karina Aldén

Kopia till

Statsrådsberedningen FCK
Justitiedepartementet LED
Utrikesdepartementet ADM
Försvarsdepartementet ESL
Socialdepartementet SAM
Finansdepartementet BA, ESA och SSA
Näringsdepartementet RT, KLS
Miljö- och energidepartementet S
Kulturdepartementet LS
Arbetsmarknadsdepartementet SEK
Arbetsgivarverket
Ekonomistyrningsverket
Statskontoret

1 Allmänt om molntjänster

1.1 Begreppet molntjänst

I datorhistorien har det skett en ständig pendling mellan centralisering och decentralisering. I datorernas barndom var datorerna dyra och stora varför de var centraliserade. Med tiden krympte både storleken och kostnaden varför viss datorkraft kunde distribueras. När persondatorerna slog igenom under 1980-talet flyttades datorkraften till användaren och således decentraliserades datorkraften. För it-system som krävde central lagring var det under 1990-talet vanligt med s.k. client/server-lösningar där datorkraften var fördelad mellan centrala datorer och persondatorer.

De senaste åren har trenden varit s.k. molntjänster (eng. cloud computing) där datorkraften är centraliserad och användaren ofta bara behöver en webbläsare eller en mobilapp för att använda tjänsten.

Begreppet ”molntjänst” har sitt ursprung från tiden då internet var någonting relativt nytt och det var vanligt att rita och abstrahera ett nätverk som ett moln.

Molntjänst används som en generell abstraktion för servrar, applikationer, data och tjänster som levereras över internet, ibland med tillägget att kunden efter eget behov själv kan få tillgång till och använda tjänsten. Detta är dock i dagsläget inte tillräckligt som definition. Även med en mer utvecklad definition behöver alla resonemang kring molntjänster idag dessutom anpassas efter vilken typ av molntjänst som avses och hur molntjänsten tillhandahålls.

Typiska egenskaper hos en molntjänst:

Brett tillgänglig åtkomst
De fysiska och virtuella resurserna finns tillgängliga över internet och nås via vanliga protokoll och gränssnitt. Användarna kommer åt resurserna från valfri plats och med valfri dator eller mobiltelefon så länge det finns anslutning mot internet.

Uppmätt tjänst
Molntjänster medger att användningen kan övervakas, styras, redovisas och debiteras varför kunderna endast betalar för de resurser de använt. Ur kundperspektivet är molnbaserade datortjänster värdefulla för användarna genom att dessa tjänster möjliggör en övergång från en affärsmodell med låg effektivitet och lågt utnyttjande av resurser till en med hög effektivitet.

Fleranvändande
Resurser fördelas på ett sådant sätt att flera användare delar miljö, men deras data isoleras från och är oåtkomliga för andra användare. En grupp av användare tillhör oftast samma molntjänstkund, t.ex. en myndighet och dess anställda. Särskilt i publika molntjänster kan det dock förekomma att en grupp av molntjänstanvändare innehåller

användare från flera olika kunder. En viss molntjänstkund kan omvänt ha olika engagemang med en enda molntjänstleverantör.

Självbetjäning på begäran
Användaren kan automatiskt få tillgång till beräkningsresurser vid behov eller efter minimal interaktion med molntjänstleverantören. Detta innebär att molnbaserade datortjänster erbjuder användarna en relativ minskning av de kostnader, den tid och den ansträngning som krävs för att vidta en åtgärd. Det är möjligt eftersom tjänsterna ger användarna möjlighet att göra vad de behöver göra, när de behöver göra det, utan att kräva ytterligare mänskliga användarinteraktioner eller administrationskostnader. Molntjänster kan i vissa fall beställas, sättas upp och börja användas helt utan mänsklig interaktion.

Snabb elasticitet och skalbarhet
Fysiska eller virtuella resurser kan levereras snabbt och elastiskt, i vissa fall automatiskt, så att resurserna snabbt kan ökas eller minskas. För molntjänstkunden framstår ofta resurserna som obegränsade och de verkar kunna köpas och nyttjas omedelbart, oavsett mängd och när som helst, med förbehåll för eventuella begränsningar i serviceavtal. En viktig del i den upplevda kundnyttan är att inte behöva oroa sig för begränsade resurser eller för kapacitetsplanering.

Resursdelning
Tjänstekonceptet innebär funktionalitet för att molntjänstleverantörers fysiska eller virtuella resurser kan läggas samman för att tjäna en eller flera molntjänstkunder. Molntjänstleverantörer kan stödja fleranvändande samtidigt som de kan använda abstraktion som ett sätt att dölja komplexiteten i processen för kunden. Sett ur kundperspektiv innebär det att allt kunden vet är att tjänsten fungerar, medan kunden i allmänhet inte har någon kontroll över – eller kunskap om – hur resurserna tillhandahålls eller var resurserna finns. Dock bör det påpekas att molntjänstkunder skulle kunna ange eller kravställa plats på en viss nivå, t.ex. land, region eller datacenter. Molntjänsten omfördelar en del av kundens ursprungliga arbetsbelastning, t.ex. underhållskrav, till leverantören.

1.2 Typer av molntjänster

Det finns tre internationellt etablerade typer av molntjänster som beskriver tre olika funktionsområden. Tjänstebeskrivningen utgår från ett tekniskt perspektiv och tjänsterna återfinns i olika tekniska lager – olika nivåer i den tekniska ”stacken” – där det för varje nivå i tjänsten adderas en teknisk dimension.

Infrastructure as a Service
Infrastructure as a Service (IaaS) innebär it-infrastrukturella tjänster via internet. Med infrastruktur som tjänst avses att kunden kan skapa och använda resurser hos en eller flera molntjänstleverantörer i form av fysisk hårdvara såsom servrar, nätverk, lagringsutrymme, arkitekturell uppbyggnad, lastbalansering, beräkning etc. Kunden tillhandahåller själv de plattformar och applikationer som körs i infrastrukturen. Kunden har inte kontroll över den underliggande infrastrukturen men äger alltså kontroll över t.ex. operativsystem och applikationer i infrastrukturen. Ibland kan IaaS-kunder ha begränsad kontroll över utvalda nätverkskomponenter, t.ex. brandväggar.

Exempel på svenska leverantörer av IaaS: City Network, Cygate och Elastx. Exempel på globala leverantörer av IaaS: Amazon, Google, IBM och Microsoft.

Platform as a Service
Platform as a Service (PaaS) innebär att leverantören tillhandahåller applikationsplattformar via internet, för användare att installera sina egna applikationer i. Ett exempel på en PaaS-tjänst är utvecklingsmiljö som tjänst. En PaaS-tjänst inkluderar en underliggande infrastruktur men adderar ett ramverk (programspråk och utvecklingsmiljöer) där kunden kan köra eller utveckla nya it-system. Kunden driftsätter alltså egna applikationer som använder språk, bibliotek, tjänster och andra verktyg som leverantören tillhandahåller i plattformen. Liksom i fallet med SaaS (se nedan) kan kunden inte påverka bakomliggande infrastruktur såsom nätverk, servrar, operativsystem eller lagring. Kunden kan dock kontrollera de egna applikationer som körs i plattformen, samt konfigureringar i plattformen.

Exempel på leverantörer av PaaS: Amazon, Google, IBM, Microsoft och Salesforce.

Software as a Service
Software as a Service (SaaS) innebär att leverantören tillhandahåller programvara som tjänst, dvs. färdiga eller konfigurerbara applikationer över internet. Denna tjänstetyp kan levereras på flera sätt och vara tillgänglig genom t.ex. en webbläsare. Leverantören står för allt underhåll. Vid köp av en SaaS-tjänst ingår både underliggande infrastruktur och plattform i tjänsteköpet. Kunden kan inte påverka leverantörens infrastruktur och plattform (nätverk, servrar, operativsystem, lagring, språk och plattformsuppbyggnad) eller andra individuella förmågor, med eventuellt undantag för vissa användarspecifika inställningar kopplat till användaren eller dennes konto.

Exempel på svenska leverantörer av SaaS: Easit, Hypergene och Projectplace. Exempel på globala leverantörer av SaaS: Dropbox, Google, LinkedIn, Microsoft, Salesforce och Twitter.

1.3 Applikationsdrift

Drift av applikationer har i princip utvecklats på följande sätt:

- En applikation på ett operativsystem på en egen hårdvara.
- En applikation i en virtualiserad miljö där flera operativsystem delar på en hårdvara.
- En applikation i en virtualiserad miljö hos en extern leverantörs molntjänst.
- En applikation skapad som en molntjänst-applikation (s.k. container) som från början drar nytta av molntjänsternas skalbarhet och dynamik.

En container innebär att endast de delar som krävs för applikationen samlas ihop i en fil och kan därefter fritt flyttas mellan olika hårdvara och molntjänster. En stor fördel med containers är att dessa kan massproduceras i en molntjänst för att på så sätt hantera ökad och minskad efterfrågan av applikationen. Detta sker genom att applikationen är skapad på så sätt att fler kopior av applikationen startas i molntjänsten när efterfrågan är större

och stängs av när efterfrågan sjunker. På så sätt betalar kunden bara för den datorkraft som verkligen förbrukats samt kan alltid erhålla maximal prestanda.

Det som alltså sker är att applikationen abstraheras allt mer från hårdvaran och därefter abstraheras allt mer från operativsystemet. Det finns flera drivkrafter bakom denna utveckling:

- Utnyttja hårdvaran maximalt
- Lägre kostnader
- Mer energieffektivt
- Mindre yta i datacenter
- Mer dynamisk infrastruktur där en applikation enklare kan flyttas mellan hårdvara och datacenter

1.4 Modeller för tillhandahållande av molntjänster

Det finns fyra vanliga sätt att tillhandahålla molntjänster: publik, partner, hybrid och privat.

Publik molntjänst
Molntjänsten ägs och hanteras av en molntjänstleverantör som säljer resurser till flera kunder på samma infrastruktur. Tjänster i publika molntjänster är potentiellt tillgängliga för alla som så önskar. Även i en publik molntjänst kan olika kunders information vara olika mycket separerad. Ju mer separerad, desto mindre potentiella skalfördelar. Samtidigt kan säkerhetsmässiga fördelar göra en separering inom den publika molntjänsten rationell.

Partnermolntjänst
Partnermolntjänst, ibland också omnämnda som ett gemenskapsmoln eller branschmoln, erbjuds till en begränsad och väldefinierad grupp av kunder. Molntjänsten levereras åt kunder med likartad kravbild. Den gemensamma kravbilden kan avse t.ex. uppdrag, målsättning, säkerhetskrav och krav på efterlevnad. Molntjänsten ägs och hanteras av en eller flera av kunderna i samarbete, alternativt av, eller tillsammans med, en tredje part. En särskild form av partnermolntjänster är myndighetsmoln. Statens molntjänst faller in under detta begrepp.

Privat molntjänst
I andra änden av skalan finns privata molntjänster, där molntjänsten levereras på en infrastruktur dedikerad åt endast en användare. Infrastrukturen kan hanteras av användaren själv eller av en annan aktör. En aktör kan alltså skapa en molntjänst för sig själv ”i huset”. För att kvalificera som molntjänst krävs att it-resurserna genomgår samma process av t.ex. virtualisering, automatisering, kategorisering och paketering efter regelverk.

Hybridmolntjänst
Termen hybridmolntjänst avser en sammansättning av två eller flera typer av molntjänster. Ett skäl för att skapa en hybridmolntjänst kan vara att kombinera fördelarna med snabbhet och kostnadseffektivitet från en publik molntjänst med behov av privat molntjänst eller partnermolntjänst i andra delar. Samtidigt bör en strategi med hybridlösningar noga ha analyserat i vilken utsträckning de förväntade fördelarna nås.

1.5 Sammanfattning

Molntjänster är en viktig fråga för statsförvaltningen idag för att åstadkomma omställningsförmåga och effektivitet. Molntjänster påverkar också genom det genomslag som IT har på alla nivåer – ekonomiskt, socialt och kulturellt. IT har blivit den primära drivkraften för affärs- och verksamhetsutveckling i snart sagt alla verksamheter, offentliga som privata.

Molntjänsters storskalighet och höggradiga likriktning skapar nya möjligheter för mycket hög tillgänglighet och säkerhet till en låg kostnad.

I princip all modern it-drift och applikationsdrift sker idag i molntjänster såvida inte legala krav eller säkerhetskrav förhindrar detta. Ett exempel är Ericsson som har byggt sin egen molntjänst för att stötta deras kunder. Ericsson[43] har, precis som denna rapport föreslår, skapat molntjänsten med programvaran OpenStack och annan programvara med öppen källkod.

[43] https://www.ericsson.com/spotlight/cloud/blog/2016/04/26/openstack-and-nfv-agile-networks-and-open-source-code/

1 Tidigare studier

De senaste fem åren har ett brett spektrum av frågeställningar kring IT i statsförvaltningen analyserats i olika offentliga utredningar och av myndigheter, konsulter m.fl. I det följande refereras ett drygt tiotal sådana studier av betydelse för vår utredning. En tematisk sammanfattning redovisas i rapportens kapitel 2.

1.1 Riksrevisionen

IT inom statsförvaltningen – har myndigheterna på ett rimligt sätt prövat frågan om outsourcing bidrar till ökad effektivitet? (2011)[44]
Riksrevisionen anger inledningsvis att varje myndighet enligt lag och förordning ska eftersträva hög effektivitet och god hushållning av statens medel i sin verksamhet. Riksrevisionens granskning syftade till att undersöka om myndigheterna gjort rimliga prövningar av om de själva ska producera den it-kapacitet myndigheten behöver eller om de ska outsourca hela eller delar av it-verksamheten samt vilka möjliga förklaringar det finns till att myndigheterna inte prövat eller genomfört outsourcing av it-verksamheten.

Riksrevisionens slutsats är att viktig kunskap om sourcing av IT inte är tillräckligt spridd i statsförvaltningen som helhet. Det finns ingen naturlig drivkraft för myndigheter som genomfört outsourcing att dela erfarenheterna med andra myndigheter. Varje myndighet har ansvar för sin egen verksamhet och dess effektivitet. Problemet blir därför ofta att en myndighet som står inför ett ställningstagande kring en möjlig outsourcing ”tvingas” uppfinna hjulet på nytt. Riksrevisionen menar att detta innebär ett för myndigheten onödigt risktagande eftersom en outsourcingprocess är mycket komplex. Riksrevisionen konstaterar att svenska myndigheter generellt sett brister i it-beställarkompetens, effektiviseringskrav på it-verksamheten samt kontroll över it-verksamhetens kostnader.

1.2 E-delegationen

Förstudie: Effektiv IT-drift inom staten (2012)
Förstudien konstaterade att det finns en betydande effektiviseringspotential inom myndigheternas it-drift och att denna potential inte kommer att kunna nås genom fortsatt mål- och resultatstyrning av myndigheterna på samma sätt som tidigare.

Förstudien föreslog att det ska skapas en myndighetsgemensam aktör, i form av en statlig myndighet, som på regeringens uppdrag effektiviserar myndigheternas it-drift genom koncentration, konsolidering, harmonisering och konkurrensutsättning. Utgångspunkten är att denna etableras som en nationell, statlig aktör med verksamhet på ett litet antal orter. Den nya myndigheten kommer att fungera som en s.k. in-house-enhet som medger anslutning genom ”administrativt” överlämnande samt att myndigheterna kan beställa och utnyttja tjänsterna utan upphandling.

[44] http://www.riksrevisionen.se/PageFiles/8528/Anpassad_11_4_IT%20inom%20statsf%c3%b6rvaltningen.pdf

Förstudien uppskattade att den maximala effektiviseringspotentialen är 15–20 procent av driftkostnaderna och att den går att effektuera inom 5–10 år. Detta sker genom koncentration, konsolidering samt harmonisering av it-miljöerna i syfte att göra driftmiljön mer enhetlig.

De kvalitativa fördelarna med förslaget att skapa en ny myndighet för it-drift är bl.a. att det ger bättre förutsättningar att garantera driftsäkerheten, bättre hantering av risker samt att det ger ökad säkerhet genom samlad hantering av samhällsviktig information. Övriga fördelar är att det skapas en attraktiv statlig arbetsgivare inom it-området som kan säkra tillgången till it-kompetens, att det ger förutsättningar för snabbare införande av myndighetsgemensamma lösningar och att myndigheterna sparar mycket resurser genom att en professionell aktör sköter upphandling av de varor och tjänster som krävs. Nackdelarna är förknippade med riskerna kring styrmodellen och konkurrenssituationen. De största riskerna är att en stor statlig aktör på marknaden kan upplevas konkurrenshämmande samt att implementeringen av den nya myndigheten inte görs optimalt och istället blir en stor trög koloss.

1.3 Ekonomistyrningsverket

Fördjupat IT-kostnadsuppdrag – Slutrapport: Förslag inför framtiden (2015)[45]
Ekonomistyrningsverket (ESV) anger i rapporten att det finns ett värde i att stödet till myndigheterna hålls samman genom stöd till samarbete, samverkan och samordning för gemensamma e-förvaltningsinitiativ och i arbetet med verksamhetseffektiviseringar. ESV skriver vidare att varje myndighet har sina egna uppgifter att utföra och mål att uppfylla men att dessa mål inte är avskilda från andra uppgifter och mål i statsförvaltningen. Statsförvaltningen måste således bli bättre på att samarbeta, samverka och samordnas så att de stordriftsfördelar som finns i industrialiseringen av IT tas tillvara.

ESV konstaterar vidare att statsförvaltningen måste stärka sin samlade kompetens inom IT, digitalisering och verksamhetsutveckling och att det är angeläget att regeringen stärker styrningen och kontrollen av IT i statsförvaltningen för att ta till vara möjligheterna det ger och säkra statsförvaltningens effektivitet och resurshushållning.

Inom uppdraget skulle ESV hämta in information om vilka strategiska it-projekt som ett antal myndigheter driver och som bedöms ha en högre risk vad gäller nytta och budget. ESV skulle också kartlägga myndigheternas it-kostnader, dessa uppskattades till 24–30 miljarder kronor per år.

[45] http://www.esv.se/contentassets/a65daa4235d147969840c915e5b5e9b0/esv-2015-64-slutrapport-forslag-infor-framtiden.pdf

1.4 Justitiedepartementet

Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten, SOU 2015:23 (2015)[46]
Utredningen (NISU 2014) anger att ansvaret för helhetsbilden över samhällets samlade it-relaterade hotbild är en uppgift som bör åvila offentliga organ. Staten står för resurser och en kontinuitet, som inte kan vare sig krävas eller garanteras av någon annan aktör. För att hantera allvarligare incidenter, som kan komma att påverka den nationella säkerheten eller nationella intressen, måste givetvis staten ha det övergripande ansvaret.

För att på ett tydligt sätt visa hur staten axlar detta ansvar föreslår utredningen att regeringen vidtar åtgärder för att skapa större säkerhet kring den information och de system för dess överföring som staten har ett omedelbart inflytande över.

Utredningen konstaterade vidare:

- Statlig upphandling på it-området bör innehålla hänvisning till för staten gällande standarder och krav på certifiering i de situationer där säkerhetsnivåer har fastställts för respektive verksamhet.
- När det gäller tjänster och produkter som ska användas för kommunikation inom staten bör upphandlande myndighet överväga möjligheten att tillämpa lagen om upphandling på försvars- och säkerhetsområdet.

När samhället blir allt mer beroende av tekniska system måste dessa vara tillräckligt säkra. I det moderna samhället blir konsekvenserna av driftavbrott i informationssystem större och mer oöverskådliga. Utveckling av programvara och tjänster ställer höga krav på både beställarkompetens och säkerhetsmedvetande hos beställaren för att uppnå tillräcklig säkerhetsnivå. Den ökade delningen av information ger ökad osäkerhet om vem som äger data t.ex. vid lagring i kommersiella molntjänster.

Många it-incidenter och störningar i informationssystem har icke-antagonistiska orsaker. En inte ovanlig anledning till sådana it-incidenter är fel i programvara eller hårdvara. Störningar i stödsystem som t.ex. elförsörjning och kommunikation genom väderförhållanden och avgrävda kablar är också välkända orsaker till it-incidenter.

1.5 Justitiedepartementet

En ny säkerhetsskyddslag, SOU 2015:25 (2015)[47]
Utredningen om säkerhetsskyddslagen syftade till att modernisera säkerhetsskyddslagen och säkerhetsskyddsförordningen. Säkerhetsskyddet ska inriktas mot verksamhet som

[46] http://www.regeringen.se/contentassets/8ae8ef6d5d3f45058c981cbab4e297de/informations--och-cybersakerhet-i-sverige.-strategi-och-atgarder-for-saker-information-i-staten-sou-201523

[47] http://www.regeringen.se/contentassets/08d4b02afbc348edad916de817105a9c/en-ny-sakerhetsskyddslag-sou-201525

innebär hantering av säkerhetsskyddsklassificerade uppgifter och uppgifter som är av betydelse för Sveriges säkerhet.

Verksamhet av betydelse för Sveriges säkerhet innefattar all säkerhetskänslig verksamhet, t.ex. hantering av it-system eller sammanställningar av uppgifter som är av central betydelse för ett fungerande samhälle.

Sedan den nuvarande säkerhetsskyddslagen trädde i kraft har hoten mot rikets säkerhet ytterligare förändrats. Elektroniska angrepp i olika former betraktas som ett av de allvarligare hoten. Antalet it-angrepp ökar i omfattning och blir allt mera riktade och sofistikerade. Ytterligare faktorer att beakta är koncentrationen av uppdrag och tjänster på it-området till ett fåtal företag. Denna ökade koncentration till ett fåtal företag som tillhandahåller tjänster till myndigheter särskilt på it-området och som därmed får tillgång till stora mängder information kan medföra en ökad sårbarhet. Den samlade informationen kan bli mycket omfattande och kräver därför särskilda hänsyn från säkerhetsskyddssynpunkt.

En rad verksamheter, både hos det allmänna och inom näringslivet, är helt beroende av digitala system för bl.a. styrning, reglering och övervakning. Ett behov av att skydda systemen är i dag påtagligt inom vissa för samhället kritiska sektorer. Teknikutvecklingen och it-samhället innebär också i andra avseenden ändrade förutsättningar för säkerhetsskyddet, t.ex. kan molntjänster försvåra arbetet med säkerhetsskyddsåtgärder.

Den utbredda digitaliseringen medför effektivitetsvinster men samtidigt en påtagligt ökad sårbarhet för störningar och avbrott. Öppenheten kräver också att den information som görs tillgänglig inte kan förvanskas. Tekniken utvecklas ofta betydligt snabbare än säkerhetsarbetet. Den snabba utvecklingen på it-området i kombination med myndigheternas ökande nyttjande av privatägd infrastruktur medför att myndigheternas egna tekniska kompetens minskar. Bristande kontroll över vilka it-produkter som tas in i svensk infrastruktur kan ge nya möjligheter för olika aktörer att inhämta information om och påverka nationella skyddsintressen och tillgångar av strategisk betydelse. Informationssäkerhet inklusive cybersäkerhet anses vara av såväl strategisk som utrikespolitisk och säkerhetspolitisk betydelse. En storskalig it-incident bedöms i dag kunna få allvarliga konsekvenser såväl för ekonomisk som för samhällsviktig verksamhet och kritisk infrastruktur.

Lagring av stora mängder uppgifter i it-system har ökat kraftigt och fortsätter öka närmast lavinartat i takt med ökade tekniska möjligheter och ökade ambitioner i samhället. Effekten av detta kan bli att uppgifter, som var för sig inte är skyddsvärda, i aggregerad form kan komma att utgöra en stor sårbarhet. Den pågående koncentrationen av it-drift till ett litet antal stora leverantörer skapar nya sårbarheter i samhället.

I dag finns en övervägande del av de verksamheter som är viktiga för det svenska samhällets funktionalitet inte under direkt statligt inflytande. Av effektivitetsskäl och ekonomiska skäl väljer eller åtminstone överväger många verksamheter i dag åtgärder som utkontraktering när det gäller utveckling eller hantering av säkerhetskänsliga it-system. Utkontraktering kan ofta innebära att flera kunders system och information blandas samman i fysiska datasystem vilket innebär att olika kunders data kan hamna i samma

lagringsmiljöer, routrar och brandväggar. Av kostnadsskäl väljer leverantören inte sällan lösningar som leder till att system förs samman och virtualiseras.

Säkerhetsskyddsanalysen är av central betydelse för säkerhetsskyddet. I förslaget till ny lagtext framgår det att den som avser att inrätta ett it-system som ska användas för säkerhetskänslig verksamhet ska analysera vilka krav på skydd som finns och se till att säkerhetsskyddet utformas så att dessa krav tillgodoses. Aggregering av uppgifter i it-systemen bör särskilt beaktas. Det innebär att ett it-system som kan förväntas innehålla en omfattande mängd uppgifter på en viss nivå kan behöva ett säkerhetsskydd som är högre än vad nivån som sådan motiverar.

Bestämmelserna om säkerhetsskyddad upphandling och säkerhetsskyddsavtal ska gälla för upphandlingar eller ingående av kontrakt där det förekommer information i informationssäkerhetsklassen konfidentiell eller däröver, eller som i övrigt avser säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet.

Myndigheter ska, innan de behandlar säkerhetsskyddsklassificerade uppgifter i ett it-system utanför deras kontroll, försäkra sig om ett tillräckligt säkerhetsskydd. Om säkerhetsskyddsklassificerade uppgifter ska kommuniceras och skyddas med hjälp av kryptografiska funktioner, ska dessa ha godkänts av Försvarsmakten.

1.6 Statens inköpscentral (Kammarkollegiet)

Förstudierapport Datacenter, servrar, lagring, nätverksprodukter samt närliggande produkter och tjänster (2015)[48]
Rapporten skriver om trenden att öppna samarbetsprojekt är något som snabbt har kommit att förändra marknaden för både servrar, lagring och nätverk. Inom ramen för dessa projekt samarbetar en stor mängd konkurrerande företag om utvecklingen av grundläggande programvara. Dessa företag, och även andra företag, kan sedan sälja denna programvara med olika former av värdeadderande tjänster eller programvara.

Det finns flera lockelser för kunder att bygga sitt datacenter på denna typ av programvara. Dels minskar kundens risk att bli inlåst till en proprietär programvaruleverantör, dels kan kund erhålla hybriddrift om marknaden tillhandahåller molntjänster byggda på samma underliggande programvara som kundens eget datacenter. Både svenska och globala molntjänstleverantörer erbjuder molntjänster baserade på dessa projekt, främst OpenStack.

Antalet verksamheter som använder IaaS i offentlig sektor är lågt enligt ett analysföretag som rapporten hänvisar till, enbart 10 procent anger att de specifikt använder sig av IaaS. När dessutom internationella aktörer är så pass dominerande på den svenska marknaden kan det vara svårt att efterleva de juridiska krav som finns på datalagring och integritetsskydd.

[48] http://www.avropa.se/globalassets/forstudierapporter-vt--it/forstudie-datacenter-servrar-lagring-natverksprodukter-samt-narliggande-produkter-och-tjanster.pdf

1.7 Myndigheten för samhällsskydd och beredskap

Informationssäkerhet – trender 2015 (2015)[49]
Myndigheten för samhällsskydd och beredskaps (MSB) trendrapport, gjord i samarbete med Rikskriminalpolisen, Försvarsmakten och FRA, är tänkt som ett underlag för fortsatt stöd i det säkerhetsarbete som måste bedrivas i alla delar av samhället.

Av de trender som anges är dessa mest relevanta i förhållande till en statlig molntjänst:

- Kunskapen och medvetenheten om säkerhetsaspekter på beställarsidan behöver ökas.
- Utvecklingsprocessen måste ta hänsyn till säkerhetsaspekten genom hela processen, det går inte att bara skriva om säkerhet i en inledande kravspecifikation. Ett nära samarbete mellan systemutvecklare och informationssäkerhetsexperter blir allt viktigare för att uppnå en god säkerhetsnivå.
- Utvecklingen mot en allt mer centraliserad it-hantering fortsätter. Medan varje verksamhet för tio år sedan själv hade hand om sina it-system lägger allt fler nu ut sådana funktioner på externa leverantörer, t.ex. i molntjänster. Ibland är det bara lagrings- och beräkningskapacitet som hyrs, men allt oftare hyrs också hela it-system. Drivkraften är kundernas önskan att sänka sina fasta kostnader – det blir mycket billigare om hundra bolag delar på ett datacenter än om var och en ska ha sin egen lösning.
- Stordriftsfördelarna gör det troligt att molntjänsterna är här för att stanna, men dessa ställer stora krav på beställaren för att inte leda till oönskade risker.
- Kunden får aldrig mer än vad den kravställer och betalar för, vare sig med utkontrakterade system eller med egen drift och utveckling.
- Utvecklingen med outsourcing leder ofrånkomligen till att allt fler ägg läggs i samma korg och att konsekvenserna av såväl attacker som icke-antagonistiska driftavbrott blir mer svåröverskådliga.
- Hela skalan av både enkla och sofistikerade hot och risker bör vägas in i riskanalysen som görs innan verksamhet utkontrakteras till underleverantörer eller data läggs i molntjänster.
- Floran av tänkbara angreppsscenarier bör dock inte leda till att risken med driftstörningar underskattas, oavsett om de är en följd av angrepp eller inte. Haverierna hos Tieto och Evry är exempel på hur centraliserad drift under olyckliga omständigheter plötsligt leder till oväntade och svårförutsägbara problem för stora och till synes orelaterade delar av samhället. Komplexiteten i molnmiljön samt det faktum att ingen idag har en överblick över de beroenden som uppstått gör riskanalyser till en stor utmaning.
- Molntjänsterna aktualiserar att ansvar allt oftare är utspritt över flera organisationer, trots att säkerhet förutsätter tydlighet och gott samarbete. Säkerhet kan inte läggas ut på andra – även om den upplevda säkerheten i en molntjänst kan vara hög så ersätter den inte den egna organisationens ansvar eller säkerhetsarbete. Det utspridda

[49] https://www.msb.se/RibData/Filer/pdf/27494.pdf

ansvaret medför svårigheter i att utvärdera tjänster, koordinera parterna och att bygga en gemensam och effektiv säkerhetskultur över organisationsgränserna. Det kan också vara problematiskt att få tillgång till data och att bedriva såväl förebyggande arbete som forensiska granskningar.

- Standardisering, både av teknik och av kontrakt, samt bättre uppföljning av avtal är en del av lösningen på problemen.
- Offentlig sektor kläms mellan olika krav, där it-systemen förväntas både vara effektiva och spara pengar, erbjuda medborgarna bättre service och vara säkra.
- Ibland är det inte avtal som är problemet, utan avsaknaden av avtal. Samverkan mellan offentliga aktörer avseende it-system blir allt vanligare, men är ofta inte reglerad i några avtal. Det betyder att det inte går att utkräva ansvar via en rättsprocess om något går fel. Offentliga aktörer borde sluta fungerande överenskommelser med varandra, med liknande funktion som kommersiella avtal eftersom en viktig faktor för riskhantering är ekonomiska incitament. Aktörer som verkar på en konkurrensutsatt marknad förefaller vara mer proaktiva än exempelvis kommuner. En särskild svårighet är att många offentliga aktörer samverkar avtalslöst med varandra och skulle behöva kunna ingå överenskommelser som svarar mot kommersiella avtal. Utan ansvarsfördelning har de svårt att uppnå någon mogen incidenthantering.
- En målbild för en informationssäkerhetskultur att sträva mot skulle kunna vara flygsäkerhetskulturen inom flygvapnet. Där rapporterar piloter utan att skämmas regelmässigt misstag som de gjort och stärker därmed den framtida säkerheten.

1.8 Gartner

Underlag till arbetet med förvaltningsansvar för gemensamma lösningar och förmågor avseende IT-drift och datorhallar (2016)[50]
Rapporten drar slutsatsen att myndigheterna vill ha en professionell extern leverantör som kan hantera t.ex. drift, lagring och virtualisering på ett mer flexibelt och snabbt sätt än deras interna it-verksamhet. Detta skulle då tvinga myndigheterna att bli mer standardiserade, få bättre uppföljning, bli mer professionella, mer effektiva samt eventuellt leda till lägre kostnader.

Det som talar emot att anlita en extern kommersiell leverantör är bl.a.

- Att it-verksamheterna sällan ser ett värde i att outsourca sig själva,
- svårt och resurskrävande att genomföra upphandlingar,
- stora risker vid övertagande och senare byte av leverantör,
- bristfällig kontroll över sin it-arkitektur och drift,
- bristande beställarkompetens,
- komplicerat med personalövergången,
- legal osäkerhet, samt
- osäkerhet när det gäller säkerhetsklassad personal hos leverantören.

[50] På uppdrag av Näringsdepartementet/Regeringskansliet.

I rapporten framgår det att en del av myndigheterna anser att en statlig molntjänst skulle kunna lösa delar av problemen. Myndigheterna lyfte själva fram att de ser att en central it-drift bättre kan fokusera på säkerheten ur alla aspekter. Många myndigheter anger att de är oroliga för utländska underrättelsetjänsters avlyssning och bakdörrar i it-utrustningen.

Myndigheterna ansåg att samverkan mellan myndigheter är svårt då varken myndigheterna eller regeringen tydligt beslutat hur det ska göras i praktiken. Samtidigt kan det kännas tryggare med en lösning internt inom staten där det finns likartade säkerhetskrav och värdegrund.

Rapporten konstaterar att enligt många myndigheter är en statlig myndighet för gemensam it-drift en bra möjlighet till samarbete som inte utnyttjats. Staten borde ha ett koncerntänk. Myndigheterna påtalar även att det finns behov av att samla it-kompetensen inom statsförvaltningen då det är ett stort antal myndigheter och att it-verksamhet blir mer och mer komplext och specialiserat. Vissa delar av statens information är olämplig att lägga hos en extern part och därför vore en statlig molntjänst mycket lämplig. Detta menar myndigheterna gäller oavsett om det skulle vara ekonomiskt fördelaktigt då fördelarna rörande kompetens, samarbete och informationsdelning anses vara ännu viktigare.

1.9 Ramböll

Internationell utblick – Öppen programvara inom statsförvaltningen (2016)[51]
Uppdraget syftade till att ge en sammanfattande överblick över trender och utveckling kring öppen källkod i Sverige och andra länder.

Programvara med öppen källkod är fri för vem som helst att nyttja, ändra, förbättra och sprida utan tillstånd från upphovsrättsinnehavaren. I statsförvaltningen har programvara med öppen källkod ofta benämnts som ”öppen programvara”.

I rapporten sammanfattas vilka gynnsamma effekter användningen av öppna programvaror har jämfört med proprietära programvaror:

- Minskade leverantörsberoenden till enskilda leverantörer.
- Minskade kompetensmässiga inlåsningseffekter för användarna.
- Ökad innovationskraft genom bättre konkurrens på marknaden för programvaror.
- Lägre licenskostnader.
- Minskade it-omkostnader.
- Ökad skalbarhet genom möjlighet att återanvända programvaran i andra sammanhang.
- Ökad flexibilitet genom bättre möjlighet att testa och anpassa programvaran.

[51] På uppdrag av Näringsdepartementet/Regeringskansliet.

1.10 Pensionsmyndigheten

Molntjänster i staten – en ny generation av outsourcing (2016)[52]
Rapporten påtalar att en myndighet som använder en molntjänst kan styra om sina resurser mot utveckling och innovation i andra delar av verksamheten, exempelvis utveckling av nya tjänster för medborgare och företag. Myndigheten kan då dra nytta av att en molntjänstleverantör i kraft av sin stora skala och specialisering har mycket större möjligheter att arbeta strukturerat och långsiktigt med utveckling och innovation av tjänsten.

En molntjänst skulle vidare vara fördelaktig för de myndigheter som har kraftigt varierande behov av it-resurser, t.ex. vid utskicken av orange kuvert från Pensionsmyndigheten, Skatteverkets hantering av deklarationer samt Valmyndigheten vid allmänna val. Flexibiliteten i en molntjänst innebär att när datamängderna ökar kan organisationen öka sin process- eller lagringskapacitet, för att sedan minska när efterfrågan är lägre. Detta innebär att myndigheten aldrig behöver köpa kapacitet som inte utnyttjas och att besparingen kan användas till andra värdehöjande aktiviteter.

Det är eftersträvansvärt att bygga molntjänster med öppen källkod eftersom det ökar nyttan i den offentliga investeringen då koden är återanvändbar.

Rapporten framhåller problemet med s.k. inlåsningseffekter som uppstår om myndigheten på ett eller annat sätt har ett beroende till en specifik leverantör. De kan bland annat uppstå på grund av en viss leverantörs specifika produkter, tjänster eller teknologi, men även kompetensmässiga och rättsliga skäl kan medföra att tjänsten varken kan eller får förvaltas av någon annan än den som levererar den för tillfället.

Under uppdraget visade det sig att många aktörer är positiva till – och efterfrågar – centralt tillhandahållna molntjänster där myndigheter skulle ha möjlighet att ansluta sig utan egen upphandling. Denna inställning framkom från såväl myndigheter som leverantörer, forskare och expertorganisationer. Inom ramen för ett myndighetsmoln som tillhandahålls av en värdmyndighet till övriga myndigheter kan ett större utrymme skapas för myndigheter att använda molntjänster även när informationen som hanteras omfattas av sekretesslagstiftningen.

Som bilaga till rapporten finns en gedigen juridisk analys där ett flertal lagar analyseras gällande myndigheters nyttjande av molntjänster. Primärt är det offentlighets- och sekretesslagen, personuppgiftslagen och arkivlagen som är de största utmaningarna för ett legalt nyttjande av kommersiella molntjänster.

[52] https://www.pensionsmyndigheten.se/content/dam/pensionsmyndigheten/blanketter---broschyrer---faktablad/svar-p%C3%A5-regeringsuppdrag/2016/Uppdrag%20att%20analysera%20potentialen%20f%C3%B6r%20anv%C3%A4ndning%20av%20molntj%C3%A4nster%20i%20staten%20.pdf

1.11 Riksrevisionen

Informationssäkerhetsarbete på nio myndigheter – En andra granskning av informationssäkerhet i staten (2016)[53]
Riksrevisionen konstaterar att många samhällsfunktioner idag är beroende av IT för att kunna fungera. Olika tekniska system är dessutom ofta beroende av varandra eller tekniskt sammankopplande, vilket utgör en sårbarhetsfaktor i sig genom att störningar kan få konsekvenser som är svåra att både förutse och hantera.

Statens olika hot eller risker varierar från exempelvis stater, statsunderstödda aktörer, terrorister och organiserad brottslighet till fel och störningar som inte orsakas av antagonister utan beror på program- eller hårdvarufel, processbrister, bristande kvalitetskontroll, slarv, missbedömningar eller rena olycksfall.

Riksrevisionens samlade slutsats är att arbetet med informationssäkerhet på de granskade myndigheterna ligger på en nivå som är märkbart under vad som är tillräckligt. En viktig förklaring till det är att förståelsen för vikten av en god informationssäkerhet överlag är alltför liten. Riksrevisionen antar därför att den bild som framträder vid de granskade myndigheterna även gäller för flertalet andra myndigheter i statsförvaltningen.

Riksrevisionen menar att säkerhetsarbetet ofta inte implementeras i de ordinarie verksamhetsprocesserna. Det saknas till betydande delar delaktighet och ansvarstagande som bör genomsyra hela myndigheten, och det finns en bristande förståelse för behovet av säkerhetsinvesteringar utan synbar nytta.

Riksrevisionen konstaterar att arbetet med informationssäkerhet på de granskade myndigheterna sker på varierande sätt, trots att betydande delar av detta arbete borde vara generiskt till sin karaktär. Det kan också konstateras att de delar av informationssäkerhetsarbetet som omfattar it-säkerhet och fysiskt skalskydd överlag visar sig bättre än de organisatoriska delarna, även om det för it-säkerhet finns förbättringspotential.

1.12 Konkurrensverket

IT-standarder, inlåsning och konkurrens: En analys av policy och praktik inom svensk förvaltning (2016)[54]
Forskare vid Högskolan i Skövde har genomfört ett uppdragsforskningsprojekt på uppdrag av Konkurrensverket där de redovisar en kartläggning av hur krav på användning av olika typer av it-standarder påverkar förutsättningarna för konkurrens för olika aktörer på marknaden.

Begreppet inlåsningseffekt kan förklaras som ett varaktigt beroende av en viss leverantör bortom gränserna för en enskild upphandling. Beställaren blir vid framtida behov av underhåll, uppgradering och komplettering tvungen, av tekniska, ekonomiska och/eller

[53] http://riksrevisionen.se/PageFiles/24458/RiR_2016_8_INFOSAK2_WEBB.pdf

[54] http://www.konkurrensverket.se/globalassets/publikationer/uppdragsforskning/forsk_rapport_2016-2.pdf

rättsliga skäl, att anlita det företag som har levererat it-systemet. En typisk effekt av inlåsning är att det för beställaren, på kort sikt, är mer kostnadseffektivt att behålla nuvarande it-system men på lång sikt är det dels förödande att beställaren inte själv kan styra över sin it-miljö, dels sällan kostnadseffektivt.

Studien visade att det bland beslutsfattare finns en mycket begränsad insikt och medvetenhet om hur genomförandet av it-projekt kan leda till olika former av inlåsning. En överväldigande majoritet av alla analyserade it-projekt som genomförts av myndigheter genomförs utifrån en redan inlåst situation med krav som utgår ifrån ett starkt beroende till olika specifika teknologier och leverantörer vilket påverkar förutsättningarna för genomförandet. I flera fall kommer genomförandet av ett it-projekt att ytterligare cementera en redan inlåst situation så att organisationen blir än mer inlåst. Studien har inte identifierat något enda projekt där exit-kostnader kalkylerats på ett sätt som belastar den ursprungliga investeringen. Studien har inte heller identifierat någon enda situation i något enda it-projekt där organisationen aktivt tagit steg för att ”låsa upp” en redan existerande inlåsning.

1.13 Årsrapporter från säkerhetsmyndigheter

Militära underrättelse- och säkerhetstjänstens (MUST) Årsöversikt 2015[55]
Det svenska närområdet har fått ökad militärstrategisk betydelse som en arena för säkerhetspolitiska markeringar och militärstrategisk positionering. Den säkerhetspolitiska utvecklingen i närområdet är den största faktorn i förändringen av hotbilden. Det förekommer även underrättelseverksamhet riktad mot den allt snabbare tekniska utvecklingen i samhället.

Den främmande underrättelseverksamhet som bedrivs i Sverige är omfattande och kartlägger företrädare för Sverige och Försvarsmaktens verksamhet. Utländska underrättelseofficerare som är stationerade i Sverige under diplomatiska täckbefattningar kartlägger såväl Försvarsmaktens förmåga och verksamhet, som civila samhällsviktiga funktioner.

Exempel på underrättelser från senare tid är den ökande globala terrorismen, nya former av krigföring, påverkansoperationer via olika typer av media samt verksamhet inom det så kallade ”cyberområdet” (inträngning i svenska IT- och ledningssystem).

Säkerhetshot mot Sverige och Försvarsmakten kan förekomma i form av underrättelseverksamhet, sabotage, subversiv verksamhet (bl.a. påverkanskampanjer med hjälp av media), terrorism och kriminalitet.

Försvarets radioanstalts (FRA) Årsrapport 2015[56]
Det tilltagande terrorhotet kommer i kölvattnet av en förmörkad säkerhetspolitisk utveckling i vårt närområde. Parallellt med detta växer också cyberhoten i form av både

[55] http://www.forsvarsmakten.se/siteassets/3-organisation-forband/hogkvarteret/20160301-must-arsoversikt.pdf

[56] http://fra.se/download/18.7fa21d9714ce119787c8000198/FRA-arsrapport-2015.pdf

underrättelseinhämtning och andra typer av cyberoperationer där vi får räkna med att det kan finnas hot som innebär att viktiga samhällsfunktioner för svensk säkerhet och välfärd kan störas eller slås ut.

Parallellt med konflikter av mer traditionellt slag, växer också insikterna om andra former av maktmedel som bygger på psykologisk krigföring och propaganda. Såväl Säkerhetspolisen som MUST har varnat för en ökning av främmande underrättelseverksamhet riktad mot Sverige. Medier rapporterar ofta om olika former av cyberangrepp och nationer anklagar varandra öppet för att bedriva avancerat cyberspionage.

Flera länder bedriver underrättelseverksamhet riktad mot Sverige. De som ligger bakom kan vara intresserade av politiska och militära frågor, men även industrispionage förekommer. En del av den främmande underrättelseverksamheten sker genom avancerade cyberangrepp. Det kan också röra sig om agenter som spionerar mot Sverige.

Det är idag vanligt att stater och statsunderstödda aktörer använder cyberangrepp som ett sätt att bedriva underrättelseverksamhet. FRA har sett en accelererande utveckling av avancerade cyberangrepp i det globala nätet. Under 2015 har angrepp upptäckts mot forskningsinstitutioner, industri, myndigheter och andra mål i Sverige.

En tydlig trend är att många offentliga verksamheter outsourcar delar av sin it-verksamhet. Dessa tappar då kompetens och får svårare att se till att säkerhetskrav beaktas. En annan tydlig trend är ökad mobilitet. Mobila enheter är idag i allt högre grad en del av myndigheternas totala it-struktur och innebär nya utmaningar för informationssäkerheten.

FRA har som svar på två regeringsuppdrag tagit fram ett system, ett så kallat tekniskt detekterings- och varningssystem, som kan larma om allvarliga angrepp på it-system. Systemet är en del av det tekniska stöd som FRA erbjuder och finns idag hos ett fåtal organisationer. Det finns en efterfrågan på systemet och FRA har fått i uppdrag att kunna erbjuda det till fler samhällsviktiga verksamheter under de kommande åren. Systemet är tänkt att vara en nyckelkomponent i ett framtida nationellt cyberförsvar för de mest skyddsvärda verksamheterna.

Utöver årsrapporten, och synnerligen intressant i denna utredning, har FRA uttalat sig positivt om en statlig molntjänst i media.[57]

Säkerhetspolisens årsbok 2015[58]
Utvecklingen i vårt närområde har lett till en alltmer osäker situation, framför allt genom Rysslands agerande. Säkerhetsläget är mer spänt än på länge. Säkerhetspolisen noterar att konflikter kan avgöras utan storskaliga militära angrepp, genom så kallad icke-linjär

[57] http://computersweden.idg.se/2.2683/1.650026/fra-staten-moln

[58] http://www.sakerhetspolisen.se/download/18.1beef5fc14cb83963e7273f/1458212474047/Sapo_arsbok15_webb.pdf

krigföring exempelvis påverkansoperationer och ekonomiska påtryckningar. Det är också en utveckling som träffar Säkerhetspolisens ansvarsområde.

Utländska underrättelsetjänster bedriver politisk, ekonomisk, militär och teknisk-vetenskaplig underrättelseverksamhet samt flyktingspionage i Sverige. Många länder bedriver underrättelseverksamhet i och mot Sverige eller svenska mål utomlands. Detta görs för att få tillgång till information och teknologi. Andra stater försöker också påverka Sveriges politiska beslutsfattande exempelvis genom att försöka vinna upphandlingar hos bland annat svenska myndigheter.

Utländsk underrättelseverksamhet kan, i kombination med otillräckligt säkerhetsskydd för verksamheter av betydelse för Sveriges säkerhet, leda till att totalförsvarsförmågan undermineras.

En allt större del av det utländska spionaget bedrivs med hjälp av teknisk inhämtning. För att inhämta information använder utländsk makt olika metoder. Ett sätt att hålla spionaget dolt är att använda sig av elektroniska angrepp (it-intrång). Ofta kan en agent på insidan bidra till att göra det elektroniska spionaget möjligt. Den tekniska utvecklingen gör att ett alltmer sofistikerat tekniskt spionage är möjligt, samt att sårbarheterna i vårt samhälle ständigt ökar.

Utländsk makt använder:

- Öppna källor som inte är hemliga, så som stora mängder myndighetsinformation, personuppgifter på internet, tidningar och böcker.
- Agenter som kan hämta ut information eller möjliggöra andra typer av inhämtning, exempelvis it-intrång.
- Signalspaning för inhämtning av olika typer av signaler, t.ex. mobiltelefonsamtal.
- Intrång i datorer i skyddsvärda verksamheter i syfte att stjäla information eller att förbereda sabotage.

Svenska myndigheter har krav på sig att vara både effektiva och sparsamma. Därför är det vanligt att myndigheter överlåter till en leverantör att utföra stora delar av myndighetens verksamhet. Leverantören kan i sin tur anlita flertalet underleverantörer. Ett exempel på verksamhet som kan läggas ut till leverantör är drift och underhåll av it-system.

Outsourcing av IT innebär ofta att leverantören placerar olika kunders system och information i samma fysiska datorsystem. Detta medför en ökad risk eftersom en störning i en kunds system kan orsaka störningar eller avbrott hos flera andra kunders system. Hamnar en stor mängd hemlig information hos en enskild leverantör riskerar denne dessutom att bli ett attraktivt mål för bl.a. andra länders underrättelseinhämtning. Den mängd information som samlas hos en leverantör kan medföra att leverantörens verksamhet sammantaget är av stor betydelse för rikets säkerhet.

Att skydda det mest skyddsvärda kräver ett långsiktigt och medvetet agerande.

1.14 Regeringen

Nationell säkerhetsstrategi (2017)[59]
Regeringen inleder med att konstatera att den teknologiska utvecklingen har skapat starka ömsesidiga beroenden där känsligheten för störningar i viktiga samhällsfunktioner har ökat. Vidare har IT förbättrat tillvaron för de allra flesta, men det blir alltmer tydligt hur den också kan användas i antagonistiska syften av både stater och individer.

Regeringen poängterar att Sveriges förmåga att förebygga, motstå och hantera kriser och situationer under höjd beredskap ska vara stark. Samtidigt ligger det vardagliga ansvaret för olika typer av samhällsviktig verksamhet idag hos många olika aktörer. Det innebär att alla dessa behöver ta aktivt ansvar för en god beredskap. En förutsättning för detta är ett grundligt säkerhetsskyddsarbete. Att upprätthålla en fungerande infrastruktur och flöden för försörjning, handel och ekonomi är ett nationellt intresse.

Digitaliseringen påverkar alla delar av vårt samhälle. Samtidigt som digitaliseringens fördelar välkomnas står det klart att de risker och hot som den är förknippad med är några av våra mest komplexa säkerhetsutmaningar. Några exempel på sådana utmaningar är antagonistiska hot såsom informationsoperationer och elektroniska angrepp mot skyddsvärda informations- och kommunikationssystem, t.ex. i form av dataintrång, sabotage eller spionage, exempelvis mot totalförsvarets verksamhet. IT-angrepp för att bedöma, påverka eller störa samhällsviktiga funktioner som ett förstadium till en väpnad konflikt hör också hit. IT-angrepp riskerar också att otillbörligt påverka utgången av demokratiska val.

Det sker en ständigt växande hantering av information i elektroniska kommunikationsnät och it-system. Sociala medier, ”big data”, molntjänster, artificiell intelligens och vad som börjat benämnas sakernas internet är andra områden där stora datamängder hanteras. När det uppstår brister i hanteringen av information, och i synnerhet i dess säkerhet, riskerar detta att få omfattande konsekvenser både för samhället i stort och för enskilda invånares integritet. Tilliten till digitaliseringen kan äventyras.

IT-tjänster i moderna verksamheter är ofta komplexa och utspridda. Det gäller såväl fysiskt och organisatoriskt som nationellt och globalt. Informationen om oss själva, och om våra tekniska lösningar, blir i allt högre grad allmänt tillgängliga. Detta medför att hot blir svårare att upptäcka, att riskerna blir mer svårbedömda och att beroenden blir svårare att överskåda.

Målet för regeringens it-politik är att Sverige ska vara bäst i världen på att utnyttja digitaliseringens möjligheter samtidigt som sårbarheten som ofrånkomligen följer av digitaliseringen hanteras. IT-system med hög driftsäkerhet och starkt skydd mot externa attacker är av mycket stor vikt för säkerheten i samhället och för möjligheterna att hantera olika krisförlopp. En god informations- och cybersäkerhet utmärks av att samtliga aktörer känner tillit till information och dess hantering på alla nivåer i samhället. De mest

[59] http://www.regeringen.se/48db21/globalassets/regeringen/block/aktualitetsblock/statsradsberedningen/nationell-sakerhetsstrategi.pdf

skyddsvärda verksamheterna ska dessutom svara upp mot de krav som ställs i säkerhetsskyddslagstiftningen. En förutsättning för detta är en utvecklad samordning och samverkan mellan myndigheter och andra aktörer, för att identifiera vad som ska skyddas och vilka ytterligare säkerhetsåtgärder som behöver sättas in. En robust cyberförsvarsförmåga är en viktig del av regeringens samlade ansats att stå emot riktade angrepp och försök till påverkan.

1.15 Linux Foundation

Guide to the Open Cloud – Current trends and open source projects (2016)[60]
Linux Foundation är en amerikansk icke vinstdrivande organisation vars syfte är att vara en neutral part som styr utvecklingen runt operativsystemet Linux samt ett 20-tal andra programvaror.

Rapporten noterar att merparten av alla nya framgångsrika it-baserade företag bygger sin infrastruktur med molntjänster baserade på öppen källkod, t.ex. Netflix, Facebook, LinkedIn, Twitter och Amazon. Syftet är primärt att kunna skapa en snabbrörlig miljö där nya tjänster kan skapas på ett kostnadseffektivt och dynamiskt sätt. Vidare har i princip alla företag som tillhandahåller publika molntjänster byggt sina molntjänster med öppen källkod, t.ex. Google, Amazon och IBM.

Molntjänsters tidigare stora förtjänst i att flytta kostnader från kapitalbindning (s.k. capex) till operativa kostnader (s.k. opex) har mer och mer tagits över av fördelen att molntjänster är så flexibla och dynamiska. Av detta följer även att fördelen med öppen källkod har flyttats från dess låga kostnader till dess inbyggda flexibilitet och värdeskapande.

Fördelarna med att vara en aktiv deltagare i sammanslutningar kring öppen källkod (s.k. communities) är sammanfattningsvis:

- Bättre kvalitet på programvaran.
- Bättre säkerhet i programvaran samt snabbare åtgärder då sårbarheter eller fel upptäcks.
- Full transparens i källkoden.
- Möjlighet att påverka och förändra programvarans utveckling.
- Försäkring mot inlåsningseffekter.
- Lägre kostnader.

[60] https://www.linux.com/publications/2016-guide-open-cloud

1 Enkät till myndigheter

Inom ramen för utredningen genomförde Statens servicecenter under september och oktober 2016 en skriftlig enkät bland de statliga myndigheterna om hur de i dag hanterar sin it-drift och vilka resurser den förbrukar. Enkätundersökningens svarsfrekvens, resultat m.m. har redovisats i rapportens kapitel 3. Enkäten omfattade dock fler frågor än de som redogörs för där, denna kompletterande information återfinns nedan.

Respondenterna skulle initialt ange sitt verksamhetsområde samt antal anställda. Därefter kom en fråga, som redovisas i rapportens kapitel 3, om myndigheten hade egna datacenter i egna lokaler där de äger utrustningen samt har egen personal som sköter om utrustningen eller om den utkontrakterat sin it-drift. Här bör påpekas att, för att förtydliga, sammanhanget angav vissa tänkbara gränsdragningsproblem:

- Att t.ex. ett fastighetsbolag äger fastigheten men myndigheten äger allting inuti datacentret innebar att datacentret är myndighetens.
- Att externa leverantörer delvis sköter om utrustning i myndighetens lokaler innebar att datacentret är myndighetens.
- Att myndigheten äger utrustningen men den finns i någon annans datacenter innebar att it-driften ansågs utkontrakterad.

I rapportens kapitel 3 redovisas ett antal uppgifter om statsförvaltningens it-miljöer och kostnader. Nedan redovisas ytterligare information om detta som framkom i enkäten, men inte redovisas i kapitel 3.

1.1 Myndigheter med egen drift

1.1.1 Lagringsyta

Antal anställda per myndighet	Antal myndigheter i berörd storlekskategori	Total lagringsyta hos myndigheterna i storlekskategorin
Upp till 100 anställda	27 myndigheter	512 TB
101 till 300 anställda	23 myndigheter	3 152 TB
301 till 1 000 anställda	31 myndigheter	32 917 TB
Fler än 1 000 anställda	30 myndigheter	28 126 TB

Totalt är lagringsytan (rådatavolym) drygt 64 000 TB.

1.1.2 Installerade instanser av operativsystem

Antal anställda per myndighet	Antal myndigheter i berörd storlekskategori	Totalt antal installerade OS hos myndigheterna i storlekskategorin
Upp till 100 anställda	27 myndigheter	644 stycken
101 till 300 anställda	23 myndigheter	2 468 stycken
301 till 1 000 anställda	31 myndigheter	7 909 stycken
Fler än 1 000 anställda	30 myndigheter	45 357 stycken

Totalt används drygt 56 000 installerade instanser av operativsystem.

1.2 Myndigheter med utkontrakterad it-drift

1.2.1 Antal utkontrakterade servrar

Antal anställda per myndighet	Antal myndigheter i berörd storlekskategori	Totalt antal utkontrakterade servrar hos myndigheterna i storlekskategorin
Upp till 100 anställda	28 myndigheter	298 stycken
101 till 300 anställda	14 myndigheter	875 stycken
301 till 1 000 anställda	9 myndigheter	3 218 stycken
Fler än 1 000 anställda	5 myndigheter	2 790 stycken

Totalt finns det nästan 7 200 utkontrakterade servrar.

1.2.2 Total utkontrakterad lagringsyta

Antal anställda per myndighet	Antal myndigheter i berörd storlekskategori	Total utkontrakterad lagringsyta hos myndigheterna i storlekskategorin
Upp till 100 anställda	28 myndigheter	151 TB
101 till 300 anställda	14 myndigheter	282 TB
301 till 1 000 anställda	9 myndigheter	7 986 TB
Fler än 1 000 anställda	5 myndigheter	2 958 TB

Totalt är den utkontrakterade lagringsytan drygt 11 000 TB.

1 Teknisk infrastruktur för molntjänsten

1.1 Övergripande teknisk arkitektur

Statens servicecenters förslag om en statlig molntjänst bygger på att den ska ha en teknisk arkitektur som gör att molntjänsten ska fungera i kristid och vid olika naturkatastrofer, men inte måste fungera vid krig.

Granskning av regelverk, teknisk säkerhet samt molntjänstens robusthet behöver utföras regelbundet av relevanta tillsynsmyndigheter och expertmyndigheter, t.ex. Försvarets radioanstalt (FRA), Militära underrättelse- och säkerhetstjänsten (MUST), Myndigheten för samhällsskydd och beredskap (MSB) och Post- och telestyrelsen (PTS).

Statens molntjänst ska konstrueras utifrån antagandet att samtliga gäster (myndigheternas it-system) är enkla mål för en angripare. Av den anledningen tas extra höjd för att skydda molntjänsten i sig själv mot att någon utomstående angripare obehörigen lyckas ta sig in i gästernas it-system. Samtliga delar av molntjänsten måste härdas med antagandet att en angripare kan bryta sig ur en virtuell maskin eller en container. Detta måste kunna ske utan att integriteten hos övriga it-system påverkas negativt.

Inuti respektive datacenter är molntjänsten fysiskt och logiskt separerad i minst fyra delar:

- Produktionsmiljö
- Produktionsmiljö för it-system som har hemliga handlingar (H/R)
- Testmiljö
- Utvecklingsmiljö

1.2 Lokaler

Merparten av den statliga molntjänstens datacenter ska till samtliga delar inrymmas i bergrum samt klassas som skyddsobjekt. Bergrummen behöver kylas. Det behöver utredas om det ska ske genom värmeväxling till luften eller om värmeväxling ska ske till grundvattnet, dvs. bergkyla. I det fall ett datacenter är beläget nära ett vattendrag kan värmeväxling till omgivande vatten vara ett alternativ. Eventuellt kan energieffektiv frikyla[61] för värmeväxling nyttjas då hotbilden är låg för att vid förhöjd hotnivå genomföra värmeväxlingen på annat sätt för att öka eller bibehålla skadetåligheten.

[61] Värmeväxling utan bruk av kylmaskin, dvs. nyttja naturlig värmesänka som omgivningsluft, vattendrag, grundvatten etc. som har en lägre temperatur än det som ska kylas.

1.3 Elförsörjning

För att säkerställa säker elförsörjning ska varje datacenter ha helt separerad elförsörjning från minst två håll, redundans gällande transformatorstationer samt säker försörjning på både regional och nationell nivå.

Varje datacenter måste ha egen avbrottsfri kraft för att skydda sig mot eventuella avbrott i den externa elförsörjningen. I huvudsak löses det med flera dieselaggregat per datacenter som skapar egen elförsörjning under längre tid. Dieselaggregat tar några minuter att starta varför batterier krävs under tiden. Traditionellt har det lösts med ett rum fyllt med batterier. Batterierna behöver hållas tempererade, underhållas samt bytas ut med jämna mellanrum. Hårdvara som följer OCP:s specifikationer (se avsnittet Datorkapacitet nedan) har inbyggda batterier varför inga externa batterier krävs.

1.4 Nätverk inne i datacenter (LAN)

Det fysiska nätverket inne i ett datacenter använder Ethernet med minst 25 Gbps per anslutning.

Växlar och routrar ska vara av minst två olika fabrikat för att skydda molntjänsten mot fel i hårdvara och fel vid uppgradering av hårdvara, förhindra bruk av leverantörsspecifika protokoll samt försvåra för en antagonist att ta över hela infrastrukturen. I första hand ska de växlar som används följa OCP:s specifikationer (se avsnittet Datorkapacitet nedan) och använda öppen källkod.

Underliggande nätverk, transportnät, använder endast IPv6. Överliggande nätverk, nätverksvirtualisering, för respektive myndighets data kan hantera alla protokoll, på både lager 2 och 3 i OSI-modellen,[62] som myndigheten vill använda. I dagsläget finns två programvaror som är lämpliga för att skapa nätverksvirtualisering, OpenDaylight[63] och OpenContrail.[64] Endast en av dessa bör användas, vilken som är lämpligast får avgöras vid en senare tidpunkt.

Respektive myndighet har sin egen IP-adressplan, vilken är helt oberoende av alla andra adressplaner i statens molntjänst.

1.5 Nätverk mellan datacenter inom statens molntjänst (WAN)

Samtliga datacenter ansluts med egna fiberförbindelser till minst tre andra datacenter. De tre förbindelserna ska, från ändpunkt till ändpunkt, vara fysiskt separerade i förhållande till varandra.

---

[62] https://sv.wikipedia.org/wiki/OSI-modellen

[63] https://www.opendaylight.org

[64] http://www.opencontrail.org

Statens molntjänsts WAN (Wide Area Network) har alltid transportskydd på länknivå motsvarande den nivå som används för skydd av hemliga handlingar (HEMLIG/ RESTRICTED).

Kapaciteten mellan datacenter får aldrig vara en begränsande faktor, initialt motsvarar detta uppskattningsvis en kapacitet med lägst 100 Gbps per anslutning.

Det finns myndigheter som har befintliga dubblerade it-system, och där dessa måste finnas i två separata datacenter, med krav på extremt liten tidsfördröjning mellan respektive del av systemet. Sådana it-system kan bli en utmaning att lösa i statens molntjänst då den geografiska spridningen i sig skapar fördröjning. Det finns flera sätt att lösa detta på. Frågan får därför tas upp i särskild ordning när dessa myndigheters it-system ska flyttas till statens molntjänst.

1.6 Anslutning mot internet

Respektive datacenter har en, eller flera, anslutningar till internet med en sammanlagd kapacitet om lägst 100 Gbps. Alternativ väg mot internet går över WAN via annat datacenter.

Minst tre internetoperatörer (ISP), spritt över samtliga datacenter, krävs för att upprätthålla tillräcklig stabilitet och robusthet.

Utöver anslutning mot minst tre internetoperatörer ska statens molntjänst anslutas mot samtliga nationella internetknutpunkter som idag drivs av Netnod,[65] dvs. Stockholm, Göteborg, Malmö, Sundsvall och Luleå.

Respektive anslutning mot internet ska ha skydd mot överbelastningsattacker.

1.7 Myndigheternas anslutning till statens molntjänst

Myndigheterna ansluts primärt med krypterade tunnlar över internet (Virtual Private Network, VPN). Direkt anslutning av myndigheter mot statens molntjänst, företrädesvis via separat optisk kanal, kan realiseras efter behov.

Utrustning för VPN ska vara av minst två olika fabrikat för att skydda molntjänsten mot fel i hårdvara och fel vid uppgradering av hårdvara, förhindra bruk av leverantörsspecifika protokoll samt försvåra för en antagonist att ta över hela infrastrukturen.

Myndigheter med krav på redundans köper internet från flera internetoperatörer och konfigurerar sina krypterade tunnlar att anslutas till olika datacenter.

Respektive myndighet avgör själv vilken bandbredd de behöver.

[65] Netnod är ett neutralt, oberoende och icke-vinstdrivande företag som driver infrastruktur för den svenska delen av internet. Netnod ägs av Stiftelsen för Telematikens utveckling.

Anslutning mot SGSI (Swedish Government Secure Intranet) behöver utredas vidare. Det effektivaste vore om kommunikation motsvarande SGSI kan realiseras inom statens molntjänst.

1.8 Datorkapacitet

Initialt används endast servrar med processorer med x86-arkitektur då den i dagsläget är i särklass vanligast och även väl beprövad i molntjänster. I framtiden bör statens molntjänst kunna utökas med andra arkitekturer, t.ex. ARM och Power.

Datorer ska vara av minst två olika fabrikat för att skydda molntjänsten mot fel i hårdvara och fel vid uppgradering av hårdvara, förhindra bruk av leverantörsspecifika protokoll samt försvåra för en antagonist att ta över hela infrastrukturen. Den öppna arkitekturen Open Compute Project (OCP)[66] bör användas i första hand för servrar, lagringssystem, nätverksutrustning och rack.

Initialt kommer tre olika sorters datorkapacitet att erbjudas:

- Långtidsstabila virtuella servrar. Dessa används t.ex. vid migrering från virtualiserade eller fysiska servrar och som förväntas vara tillgängliga kontinuerligt över lång tid.
- Servrar med instanslagring. Dessa används för it-system anpassade till moderna molntjänster och har vanligen en högre omsättning än långtidsstabila servrar.
- Paketerade virtuella it-system, s.k. containers.

Statens molntjänst bör inte erbjuda drift av fysisk hårdvara (s.k. bare metal) för en myndighets specifika it-system. Om speciella krav på sådan drift finns måste detta utredas vidare.

1.9 Datalagring

Datalagring kan realiseras på flera olika sätt och till olika kostnad. För att statens molntjänst ska kunna erbjuda myndigheterna prestandaalternativ till olika kostnad kommer:

- Datalagring att byggas med flera tekniker för blocklagring, t.ex. Ceph[67] och Gluster.[68]
- Lagringsmedia från flera leverantörer att användas.
- Lagringsmedia att baseras på olika teknik, t.ex. hårddisk och flash-minne.

[66] http://www.opencompute.org

[67] http://ceph.com

[68] https://www.gluster.org

Det är en fördel om minst två programvaror för blocklagring används då det minskar risken för sårbarheters negativa effekt samt risken för dataförlust beroende på felaktigheter i programvaran.

Säkerhetskopiering hanteras av respektive myndighet, t.ex. genom kopiering av data till annat datacenter.

Tillgänglighet till data hanteras i molntjänsten genom att data replikeras.

Initialt erbjuds inte objektlagring som tjänst, men kan skapas av myndigheterna själva inom molntjänsten.

1.10 Programvara

I dagsläget bedömer Statens servicecenter att endast en programvara finns för att skapa datorkapacitet som dels har öppen källkod, dels har ett aktivt globalt nätverk av utvecklare och intressenter. Att använda något annat än OpenStack[69] är därför inte realistiskt. I framtiden kan det komma lämpligare programvara varför statens molntjänst måste skapas på ett sådant sätt att det då går att byta eller komplettera.

Virtualiseringslagret kan skapas på flera sätt, OpenStack använder primärt Linux och KVM[70] varför dessa är lämpligast. I framtiden kan andra programvaror tillkomma.

Datalagring kan också skapas på flera sätt. I dagsläget bedömer Statens servicecenter Ceph och Gluster som de mest lämpliga. I framtiden kan flera andra tillkomma.

Det finns flera programvaror för nätverksvirtualisering och utvecklingstakten inom området är hög. OpenContrail och OpenDaylight är de mest lämpliga att utvärdera vidare.

För automatisering och resursstyrning är Puppet[71] eller Saltstack[72] lämpligast då de är de vanligast förekommande programvarorna för detta ändamål som har öppen källkod.

Katalogtjänsten för att hantera alla resurser bör använda OpenLDAP[73] eller 389 Directory Server[74] då dessa är väl beprövade programvaror med öppen källkod och som klarar av att hantera en stor mängd objekt.

Licenser för myndigheternas programvaror upphandlas och administreras av myndigheterna själva. När myndigheterna bygger moderna skalbara applikationer som utnyttjar

[69] http://www.openstack.org

[70] http://www.linux-kvm.org

[71] https://puppet.com

[72] https://saltstack.com/

[73] http://www.openldap.org

[74] http://directory.fedoraproject.org

statens molntjänsts skalbarhet och flexibilitet kan det bli komplicerat för myndigheterna att använda proprietära programvaror som licensieras per server eller per processor. Moderna skalbara applikationer fungerar som så att nya virtuella servrar startas och stoppas dynamiskt beroende på behoven av datorkraft. Det blir således mycket utmanande att veta hur många instanser av en viss proprietär programvara som används. Programvara med öppen källkod har inte detta problem. Statens molntjänst skulle kunna förhandla med dessa leverantörer av proprietär programvara för hela statsförvaltningens räkning med målet att förenkla för alla parter.

1.11 Administration

En myndighet som är i behov av en tjänst i statens molntjänst beställer denna tjänst i en webbaserad administrationsportal hos statens molntjänst. Administrationsportalen kommer i sin tur, helt automatiskt, att tilldela resurser och konfigurera tjänsten. Tjänsten blir därefter omedelbart tillgänglig för myndigheten att använda.

I administrationsportalen kan myndigheten även administrera sin del av statens molntjänst, se all statistik om sina tjänster, dess tillgänglighet och resursutnyttjande. Detta är kritiskt både för att skapa transparens och för myndigheternas planering. Automatiserad administration erbjuds via ett öppet programmerbart applikationsgränssnitt (API).

Autentisering till administrationsportalen sker via myndighetens egen legitimeringstjänst (Identity Provider, IDP) och kan endast ge tillgång till respektive myndighets nätverk och tjänster.

Beställda tjänster kommer automatiskt att läggas till i faktureringssystemet och debiteras myndigheten i efterskott. Val av faktureringssystem, i första hand med öppen källkod, och anslutning mot Statens servicecenters befintliga tjänster för ekonomiadministration och personaladministration behöver utredas vidare.

1 Rättsliga förutsättningar

Utöver redovisningen i rapportens avsnitt 6.7 redogörs här för mer detaljer kring olika lagar, förordningar och författningar som påverkar statens molntjänst. I det fortsatta arbetet behöver närmare analyseras hur olika författningskrav kan uppfyllas i molntjänsten.

1.1 Tryckfrihetsförordning

Tryckfrihetsförordningen, TF, reglerar bl.a. allmänna handlingars offentlighet. Under förutsättning att statens molntjänst endast har i uppdrag att tekniskt bearbeta eller tekniskt lagra handlingar för en myndighets räkning, är inte handlingarna att anses som allmänna hos statens molntjänst. Detta framgår av 2 kap. 10 § TF. En handling som endast tekniskt bearbetas eller tekniskt lagras för en myndighets räkning blir inte en inkommen handling hos statens molntjänst. Detta framgår av 2 kap. 6 § TF.

1.2 Offentlighets- och sekretesslag

Uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400), OSL, måste ha bibehållen sekretess även när driften av det it-system som innehåller dessa uppgifter hanteras inom statens molntjänst. Utöver de författningsändringar som beskrivs i avsnitt 6.7 kommer detta att kräva en mängd åtgärder som gäller organisation, avtalsvillkor, säkerhetsåtgärder m.m.

Utmaningarna i OSL gällande andra länders rättsordningar samt underleverantörer kan inte bli tillämpliga eftersom statens molntjänst ägs av staten och drift och underhåll utförs i Sverige av statligt anställd personal.

1.3 Lag om offentlig upphandling

Det finns två sidor av lagen om offentlig upphandling (2016:1145), LOU, att beakta i detta sammanhang, dels när statens molntjänst ska skapas och underhållas, dels när myndigheterna använder statens molntjänst.

När tjänster som omfattar hantering av säkerhetsskyddsklassificerade uppgifter upphandlas, bör det ske enligt lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet (LUFS). LUFS gäller för myndigheter som upphandlar militär utrustning, utrustning av känslig karaktär, byggentreprenader, varor och tjänster som hör ihop med detta eller som särskilt ska användas för militära syften eller byggentreprenader av känslig karaktär. Det bör övervägas i vilken utsträckning LUFS är tillämplig på de olika upphandlingar som görs för att inrätta molntjänsten.

I 3 kap. 17 § LOU anges att lagen inte gäller för upphandling mellan två eller flera upphandlande myndigheter, om

1. upphandlingen syftar till att upprätta eller reglera formerna för ett samarbete mellan myndigheterna som ska säkerställa att de offentliga tjänster som myndigheterna ska utföra tillhandahålls för att uppnå myndigheternas gemensamma mål,
2. samarbetet styrs endast av överväganden som hänger samman med allmänintresset, och
3. myndigheterna på den öppna marknaden utövar mindre än 20 procent av den verksamhet som berörs av samarbetet.

Regeringen anför i författningskommentaren att detta innebär att samarbeten mellan statliga myndigheter normalt inte kan anses vila på kontrakt i upphandlingsrättslig mening.[75]

Då statens molntjänsts åtagande endast handlar om en omfördelning av visst utförande, it-drift, inom staten, som är en juridisk person, bedömer Statens servicecenter att LOU inte ska tillämpas när en myndighet anlitar statens molntjänst för sin it-drift.

1.4 Dataskyddsbestämmelser

Eftersom statens molntjänst kommer att behandla personuppgifter på uppdrag av andra personuppgiftsansvariga myndigheter, i vart fall för lagring, blir bestämmelser om dataskydd i personuppgiftslagen (1998:204) och i EU:s dataskyddsförordning tillämpliga på hanteringen.

Utgångspunkten är att statens molntjänst enbart kommer att behandla personuppgifter som personuppgiftsbiträde. Det innebär att varje myndighet som anlitar statens molntjänst kommer att behöva teckna personuppgiftsbiträdesöverenskommelse med statens molntjänst. Dataskyddsförordningens bestämmelser ställer, i jämförelse med personuppgiftslagen, höga krav på innehållet i personuppgiftsbiträdesavtal vilket måste beaktas. I rollen som personuppgiftsbiträde kommer statens molntjänst också att få ett självständigt ansvar för att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifterna som behandlas.

Det finns en potentiell risk ur integritetsperspektiv då en stor mängd data om individer kommer att lagras i statens molntjänst. Statens molntjänst kommer dock, precis som anges i rapportens avsnitt 6.5, i normalfallet inte att ha tillgång till några myndigheters data.

1.5 Arkivlag och Riksarkivets föreskrifter (RA-FS)

Arkivlagen (1990:782) och RA-FS reglerar bl.a. hur myndigheter ska sköta sina arkiv. Det är respektive myndighets ansvar att försäkra sig om att arkivlagen och därtill hörande föreskrifter efterlevs oavsett var och hur den aktuella informationen lagras fysiskt och

[75] Prop. 2015/16:195, s 400–402.

geografiskt. Statens molntjänst behöver ha tekniska möjligheter för att kunna verifiera att, och när, handlingar som har gallrats är oåterkalleligt utplånade.

1.6 MSB:s föreskrifter

Den statliga molntjänsten måste, liksom all annan statlig IT, uppfylla de föreskrifter som tas fram av MSB. De föreskrifter som f.n. aktualiseras är:

- MSBFS 2016:1 Statliga myndigheters informationssäkerhet
- MSBFS 2016:2 Statliga myndigheters rapportering av it-incidenter
- MSBFS 2016:7 Statliga myndigheters risk- och sårbarhetsanalyser

Statens molntjänst måste bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett adekvat ledningssystem samt ha en säkerhetsfunktion med tillräckliga resurser för detta arbete. Det kommer att vara kritiskt att upprätthålla informationssäkerhet, driftsäkerhet och it-säkerhet i alla delar av statens molntjänst.

MSBFS 2016:1 anger att i de fall en myndighet anlitar en annan myndighet för att fullgöra uppgifter som regleras av 2016:1 ska de berörda myndigheterna tydligt dokumentera sitt samarbete. Av dokumentationen ska framgå vilken myndighet som är ansvarig för att uppfylla kraven som ställs i 2016:1. Informationsklassning utförs av den myndighet som äger informationen.

MSBFS 2016:2 anger hur statliga myndigheter ska rapportera it-incidenter som allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för, eller i tjänster som myndigheten levererar till en annan organisation.

MSBFS 2016:7 anger att risk- och sårbarhetsanalysen ska beskriva myndigheten, dess ansvarsområde och arbetsprocess samt ett antal faktorer av betydelse för säkerheten. Det handlar om:

- identifierad samhällsviktig verksamhet inom myndighetens ansvarsområde som är av nationell betydelse,
- identifierade kritiska beroenden för den identifierade samhällsviktiga verksamheten,
- identifierade och analyserade hot och risker,
- bedömning av den generella krisberedskapen,
- identifierade sårbarheter och brister, samt
- genomförda, pågående och planerade åtgärder samt behov av ytterligare åtgärder.

1.7 Säkerhetsskydd

Säkerhetsskyddslagen (1996:627) samt säkerhetsskyddsförordningen (1996:633) reglerar skydd mot spionerі, sabotage, terroristbrott och andra brott som kan hota rikets säkerhet samt skydd av uppgifter som omfattas av sekretess enligt OSL och som rör rikets säkerhet.

Säkerhetsskyddet ska förebygga:

1. att uppgifter som omfattas av sekretess och som rör rikets säkerhet obehörigen röjs, ändras eller förstörs (informationssäkerhet),
2. att obehöriga får tillträde till platser där de kan få tillgång till uppgifter som avses i 1 eller där verksamhet som har betydelse för rikets säkerhet bedrivs (tillträdesbegränsning), och
3. att personer som inte är pålitliga från säkerhetssynpunkt deltar i verksamhet som har betydelse för rikets säkerhet (säkerhetsprövning). Säkerhetsskyddet ska även i övrigt förebygga terrorism.

Statens molntjänsts storskalighet kommer i sig att innebära att säkerhetsskyddslagen blir tillämplig då t.ex. sabotage skulle få stora konsekvenser för statens operativa förmåga.

Därutöver kommer handlingar som omfattas av sekretess enligt OSL att förkomma inom statens molntjänst varför säkerhetsskyddslagen blir tillämplig.

1.8 Totalförsvar och höjd beredskap

Lag (1992:1403) om totalförsvar och höjd beredskap reglerar när beredskapen ska höjas för landets försvarsförmåga. Vid höjd beredskap ska de organisationer och företag som är skyldiga att fortsätta sin verksamhet i krig vidta de särskilda åtgärder i fråga om planering och inriktning av verksamheten som är nödvändiga för att de ska kunna fullgöra dessa skyldigheter.

Förordning (2015:1053) om totalförsvar och höjd beredskap syftar till att statliga myndigheter genom sin verksamhet ska minska sårbarheten i samhället och utveckla en god förmåga att hantera sina uppgifter inför och vid höjd beredskap.

Statens molntjänst ska i sin verksamhet beakta totalförsvarets krav. I statens molntjänsts planering för totalförsvaret ska ingå att under höjd beredskap fortsätta att bedriva verksamheten så långt det är möjligt med hänsyn till tillgången på personal och förhållandena i övrigt.

Det bör utredas vidare om, och i så fall vilka delar av, statens molntjänst som ska omfattas av totalförsvaret och vad som gäller för verksamheten vid höjd beredskap.

1.9 Förordning om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap

Förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap syftar till att statliga myndigheter genom sin verksamhet ska minska sårbarheten i samhället och utveckla en god förmåga att hantera sina uppgifter under fredstida krissituationer och inför och vid höjd beredskap.

Med krisberedskap avses förmågan att genom utbildning, övning och andra åtgärder samt genom den organisation och de strukturer som skapas före, under och efter en kris förebygga, motstå och hantera krissituationer.

Statens molntjänst måste i syfte att stärka sin egen och samhällets krisberedskap analysera om det finns sådan sårbarhet eller sådana hot och risker som synnerligen allvarligt kan försämra förmågan till verksamhet inom området. Vid denna analys ska särskilt beaktas:

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

1.10 Signalskydd

Säkerhetsskyddsförordningen (1996:633) reglerar, utöver vad som nämns i avsnittet Säkerhetsskydd ovan, att hemliga uppgifter endast får krypteras med kryptosystem som har godkänts av Försvarsmakten.

I förordningen om totalförsvar och höjd beredskap anges, utöver vad som nämns i avsnittet Totalförsvar och höjd beredskap ovan, vilka myndigheter som ska ha säkra kryptografiska funktioner. Vidare anges att det är MSB som beslutar om vilka dessa övriga myndigheter är.

Försvarsmaktens föreskrifter om signalskyddstjänsten inom totalförsvaret (FFS 2005:2) gäller för statliga myndigheter som tilldelats säkra kryptografiska funktioner och reglerar formerna för signalskyddstjänstens bedrivande. Vidare regleras att varje myndighet som innehar ett signalskyddssystem ska ha en signalskyddschef som ansvarar för att leda och samordna signalskyddstjänsten inom myndigheten.

MSB:s föreskrifter om civila myndigheters kryptoberedskap (MSBFS 2009:11) reglerar bl.a. att civila myndigheter som tilldelats säkra kryptografiska funktioner, under ordinarie kontorstid, ska vara beredda att hantera kryptosystem avsedda för samverkan då hemliga uppgifter eller andra skyddsvärda uppgifter som rör samhällsskydd och beredskap ska utväxlas.