Molntjänster i staten

En ny generation av outsourcing

PENSIONS MYNDIGHETEN

Innehåll

Sammanfattning

Pensionsmyndigheten fick våren 2015 i uppdrag av regeringen att analysera och värdera potentialen för användning av molntjänster i staten, samt att redovisa vilka risker och hinder som eventuellt finns förknippade med användning av molntjänster i statlig verksamhet. Analysen ska också visa hur användning av molntjänster kan bidra till målet om en enklare, öppnare och effektivare förvaltning.

Uppdraget har utförts framför allt under hösten 2015. Under arbetets gång har samråd skett med Myndigheten för samhällsskydd och beredskap (MSB) och med Datainspektionen (DI). Rådgivande samverkan har skett med ett flertal aktörer inom offentlig sektor, med svenska och utländska privata leverantörer, samt forskare och företrädare för organisationer verksamma inom området.

Molntjänster definieras som tjänster som tillhandahålls med nätverksåtkomst och med möjlighet till resursdelning, snabb skalbarhet, självbetjäning och betalning efter användning eller volym. Begreppet inkluderar infrastrukturella tjänster, plattformstjänster och mjukvarutjänster som kan tillhandahållas på olika sätt: från publika tjänster med okänd global lagring till tjänster som dedikeras åt endast en användare och där infrastrukturen kan hanteras av användaren själv eller av annan aktör på en bestämd plats.

En diskussion om såväl potential som förutsättningar för användning av molntjänster behöver alltid ställas i relation till typ av molntjänst, och hur den tillhandahålls. Vi ser molntjänster som en ny generation av outsourcing med de särskilda kännetecken som ryms inom definitionen. Molntjänster skiljer sig dock åt från traditionell outsourcing i bl.a. affärsmodell och hur de organiseras.

Nyttiggörande av potentialen i molntjänster svarar mot centrala politiska mål. Oavsett om vi antar ett brett tillväxt- och hållbarhetsperspektiv, ett konkurrenskraftsperspektiv, främjande av små och medelstora företag, eller ett förvaltningspolitiskt perspektiv så kan molntjänster fylla en viktig roll för att svara mot politiska målsättningar.

För den enskilda myndigheten, och således även aggregerat för staten, är nyttorna flera. Innovation och möjlighet till snabb förnyelse är vid sidan av flexibilitet och skalbarhet, kostnadseffektivitet, tillgänglighet och ökad säkerhet centrala nyttor som ofta kan nås med molntjänster. Användning av molntjänster kan också minska behovet av egen it-personal, t.ex. där det kan vara svårt för en enskild myndighet att upprätthålla spetskompetens. Förvaltningsgemensam utveckling kan förenklas av att använda molntjänster i gränssnittet mellan myndigheter, till exempel stödtjänster där myndigheternas behov är likartade och vid utveckling av myndighetsgemensamma digitala tjänster till kunder. Nyttor av molntjänster kan dock aldrig tas för givna utan måste verifieras av molntjänstkunden, i det här fallet myndigheten själv.

På senare tid har andra nyttor än kostnadseffektivitet kommit att värderas högt av dem som väljer att gå över till molntjänster. Kostnadsbesparingar kan fortfarande förväntas i flertalet fall, men hur stora dessa är varierar beroende på verksamhet, typ av tjänst och hur verksamhetens befintliga it-lösningar ser ut. En bedömning av den ekonomiska besparingspotentialen för staten sammantaget bör användas med försiktighet men är inte utan betydelse.

Alla verksamheter eller delar av verksamheter passar inte lika bra att lägga i molntjänster. Generellt gäller att molntjänster är enklare och mindre kostsamt att införa ju

mindre känslig information det finns i ett system, ju mer självständig och utan integrationer en applikation är eller ju större kostnader som är förknippade med att få en viss funktion. Molntjänster är också intressanta som alternativ till andra lösningar ju mer specifika kompetenser som behövs för att skapa eller upprätthålla en tjänst, ju mindre hela verksamheten eller verksamhetsbudgeten är, samt ju större variationer i kapacitetsbehov som en verksamhet har över tid.

För att kontrollera om det är lagligt att hantera sin information i molnet måste myndigheten i ett tidigt skede göra en s.k. laglighetskontroll. I denna analys behöver bl.a. offentlighets- och sekretesslagen, personuppgiftslagen och arkivlagen ingå, men det kan också krävas en analys av speciallagstiftningar. För att en myndighet ska kunna göra tillförlitliga juridiska bedömningar måste den ha kännedom om vem eller vilka leverantörer som kommer att hantera informationen, hur den kommer att hanteras och var informationen kommer att lagras geografiskt.

Informationssäkerhet är en viktig fråga vid användning av molntjänster. Rätt nivå av säkerhet behöver bestämmas med avseende på konfidentialitet, riktighet, tillgänglighet och spårbarhet. Skyddsåtgärder ska väljas dels med hänsyn till hur skyddsvärd informationen är, men även med hänsyn till vilka specifika risker som finns relaterade till hanteringen av informationen. Informationen behöver exempelvis skyddas mot obehörig åtkomst, avbrott i önskad tillgänglighet samt förlust, förstörelse eller manipulation.

En breddad användning i svenska myndigheter av molntjänster och andra externt levererade it-tjänster aktualiserar frågan om hur den nationella säkerheten påverkas. Frågan behöver få större fokus framåt. Det saknas idag legal eller annan grund för prioritering av samhällsviktiga funktioner vid it-incidenter, något som även har efterfrågats av leverantörerna själva. Ur ett säkerhetsperspektiv behöver olika för- och nackdelar med att välja privata och offentliga leverantörer av molntjänster övervägas. Myndighetsgemensamma kommunikationslösningar, s.k. ”gov net”, kan medföra ökade säkerhetsrisker utifrån koncentrationen av information, men skulle också kunna få positiva effekter i form av gemensam kravbild på säkerhetsnivåer och en gemensam grundnivå för tillgänglighet.

För att driva på och säkerställa att Sverige tillgodogör sig potentialen i molntjänster, föreslår vi följande åtta åtgärder för regeringen.

1. Uppdra till svenska myndigheter att analysera hur de kan använda molntjänster för att utveckla verksamheten och att göra sig beredd att övergå till molntjänstleveranser – att bli ”cloud ready”.
2. Inrätta ett kompetenscenter för anskaffning och användning av externa it-tjänster, dit både verksamhetsföreträdare och upphandlare kan vända sig och där även frågor från privata aktörer kan besvaras.
3. Analysera myndigheters digitala mognad. Undersök i vilken mån de har anlagt ett strategiskt perspektiv på molntjänster för sin egen verksamhet, grad av organisatorisk mognad och operativ beredskap för användning av molntjänster.
4. Fördjupa analysen avseende statliga myndighetsmoln. Undersök intresse och förutsättningar för att inrätta ett eller flera separata myndighetsmolntjänster, s.k. ”gov cloud” Detta skulle kunna ge möjligheter att förenkla användningen av molntjänster även då det är sekretessbelagd information som hanteras.

5. Utred närmare om det är lämpligt och ändamålsenligt att införa en lagreglerad och straffsanktionerad tystnadsplikt för privata leverantörer.
6. Prioritera att se över myndigheternas registerförfattningar och genomför nödvändiga författningsförändringar för att säkerställa bättre förutsättningar för myndigheterna att utföra sina uppdrag på ett effektivt och rättsäkert sätt.
7. Ge Myndigheten för samhällsskydd och beredskap, MSB, i uppdrag att genomföra en riskanalys av användning av molntjänster och andra externa it-tjänster ur ett nationellt perspektiv, och att föreslå eventuella åtgärder.
8. Intensifiera Sveriges närvaro i frågor som rör molntjänster i EU och andra internationella sammanhang. Ett tvärpolitiskt arbetssätt som stöder olika politikområden rekommenderas.

1 Inledning

Föreliggande rapport har tagits fram av Pensionsmyndigheten som svar på regeringsuppdrag att analysera potentialen i molntjänster för statlig verksamhet. I arbetet har vi sökt en bred samverkan med offentlig sektor, privata leverantörer och andra aktörer inom området. Nedan beskrivs uppdraget och dess genomförande.

1.1 Uppdrag

Pensionsmyndighetens uppdrag från regeringen har varit att analysera och värdera potentialen för användning av molntjänster i staten, samt att redovisa vilka risker och hinder som eventuellt finns förknippade med användning av molntjänster i statlig verksamhet. Analysen ska visa hur användning av molntjänster kan bidra till en enklare, öppnare och effektivare förvaltning.

Regeringen framhåller att analysen ska inkludera potentialen för lägre kostnader för it-infrastruktur, kommersiella alternativ för värdskap och drift samt med dessa förknippade risker för inlåsning, samt potentialen för att förenkla och accelerera utveckling av it-lösningar och e-tjänster. Pensionsmyndigheten kan också föreslå åtgärder till regeringen för att potentialen ska kunna realiseras.

Pensionsmyndigheten ska därtill kartlägga och värdera de insatser som EU-kommissionen och Europeiska unionens byrå för nät- och informationssäkerhet, Enisa, har initierat och som kan vara av intresse för myndigheter i Sverige.

Informationssäkerhet, sekretess och den personliga integriteten ska särskilt beaktas i uppdragets olika delar.

Samråd ska enligt uppdraget ske med Myndigheten för samhällsskydd (MSB) och beredskap och Datainspektionen (DI).

1.2 Uppdragets genomförande

I arbetet med uppdraget har följande ansats valts:

- **Öppenhet.** Under arbetet har vi eftersträvat en bred förankring både inom myndighetssfären, mot organisationer och gentemot aktörer på marknaden.
- **Kunskapsackumulering.** Rapporten och dess slutsatser bygger vidare på tidigare arbeten – analyser, utredningar m.m. – från både privata och offentliga organisationer, och sammanfattar i viss mån centrala delar från tidigare arbeten. Vår ambition har också varit att bygga ny kunskap utifrån befintlig kunskap och att uppdatera resonemang och fakta där utveckling har skett sedan tidigare publikationer.
- **Praktisk nytta.** Ambitionen har varit att skapa ett underlag som både utgör ett stöd för Sveriges regering i vad som krävs framåt i faktiska insatser, ramverk etc., men också ett praktiskt stöd för myndigheter som använder eller ser framtida intresse av att anskaffa och använda molntjänster.

Arbetet med uppdraget har bedrivits i projektform med en styrgrupp och en arbetsgrupp bestående av kompetenser inom juridik med inriktning mot molntjänster, it- och informationssäkerhet, it-arkitektur, it-inköp och upphandling, ekonomi och styrning samt projektledning. I styrgruppen för uppdraget har ingått avdelningscheferna Peder Sjölander, Mikael Westberg och Henrik Engström från Pensionsmyndigheten samt enhetschef Fia Ewald från MSB. I arbetsgruppen har

följande personer deltagit för Pensionsmyndigheten: Ingela Alverfors, Claes Svensson, Lars Wahlund, Pedra Herdegen, Sara Kvarnbäck, Daniel George, Carl Rubarth och Alexander Svensson. Från MSB har Maria Bergdahl deltagit i projektgruppen. Arbetet har projektletts av konsult Linda Sterner Varnestig.

Med Datainspektionen har sammanlagt fyra möten hållits inför och under arbetets gång.

Det angreppssätt för arbetet som har valts bygger på följande steg:

1. Materialstudier. Så kallad ”desk research” utgör grunden för bland annat definitioner, strategisk analys, nyttoanalys och juridiska och säkerhetsrelaterade förutsättningar.

2. Rådgivande forum och workshops. I analysen av nytta och potential i staten har vi tagit in synpunkter från såväl de potentiella köparna, myndigheterna, som från marknadsledet. Vi har genom att samla ett antal större myndigheter som deltar i eSamverkansprogrammet, samt Kammarkollegiet, Ekonomistyrningsverket och ytterligare några mindre myndigheter skapat en plattform för dialog och för att i nya gränssnitt behandla de frågor som förknippas med uppdraget. I två olika rådgivande forum har leverantörer av it-tjänster – såväl stora som lite mindre aktörer – delgett sina erfarenheter avseende om molntjänsters potential men också risker, förutsättningar för lyckade molntjänstimplementeringar, trender m.m.

3. Enkätundersökning. Mot bakgrund av kunskap och insikter som våra material-studier och arbetet med de rådgivande grupperingarna har gett, har vi via molntjänst-verktyget Surveymonkey ställt ett antal frågor om molntjänster till köpare i fokus för detta uppdrag, dvs. stora och små myndigheter. 211 myndigheter fick förfrågan, varav ett 20-tal visade sig ha gemensam it-hantering. Totalt svarade 79 procent av de tillfrågade myndigheterna med egen it-verksamhet på hela eller delar av enkäten.

4. Analys och slutsatser. Såväl huvudsakliga slutsatser som områden för förslag till regeringen har diskuterats i projektets arbetsgrupp, styrgrupp och på en övergripande nivå i de tre rådgivande forumen. För framlagda slutsatser och förslag står Pensions-myndigheten.

2 Definition av molntjänster

Sammanfattning

Molntjänster är tjänster som tillhandahålls med nätverksåtkomst och där resursdelning, möjlighet till snabb skalbarhet, självbetjäning och betalning efter användning eller volym är några av de centrala kännetecknen. Begreppet inkluderar infrastrukturella tjänster, plattformstjänster och mjukvarutjänster som kan tillhandahållas på olika sätt: från publika tjänster med okänd (global) lagring, till tjänster som dedikeras åt endast en användare och där infrastrukturen kan hanteras av användaren själv eller annan aktör på bestämd plats. En diskussion av såväl potential som förutsättningar för användning av molntjänster behöver alltid ställas i relation till typ av molntjänst och hur den tillhandahålls.

2.1 Utgångspunkt

För en tydlig och väl grundad analys av potential och förutsättningar för molntjänster i statlig verksamhet krävs först ett resonemang kring begreppet molntjänster och en definition att bygga analysen på.

En ambition har varit att utgå från en vedertagen definition och en definition med bred global spridning. Ytterligare en utgångspunkt har varit att definitionen ska vara tydlig, där eventuella indelningar i olika typer av molntjänster ska vara ömsesidigt uteslutande, dvs. att en molntjänst inte ska kunna klassas som tillhörande två eller flera kategorier samtidigt. En tredje utgångspunkt har varit att söka en definition som även är praktiskt användbar, dvs. enkelt applicerbar på statlig it-verksamhet.

2.2 Begreppets framväxt

Begreppet ”molnet” har sitt ursprung från tiden då internet var någonting relativt nytt och det var vanligt att rita och abstrahera ett nätverk som ett moln. Molntjänster har därefter ofta, särskilt i fenomenets tidiga år, använts 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 (se nedan) behöver alla resonemang kring molntjänster idag dessutom anpassas efter vilken typ av molntjänst som avses och hur molntjänsten tillhandahålls.

2.3 Definition

US National Institute for Standards and Technology (NIST) beskriver molntjänster som en modell "… for enabling convenient, on-demand network access to a shared pool of configurable computing resources … that can be rapidly provisioned and released with minimal effort or service provider interaction"[1]. NIST:s definition är vedertagen i betydelsen väl spridd och har också stått bakom andra organisationers definitioner av molntjänster, däribland organisationen Cloud Sweden.[2]

Swedish Standards Institute, SIS, har antagit en svensk standard som baseras på den av ISO-organisationen fastställda internationella standarden för molnbaserade datortjänster. Den internationella standarden är även rekommenderad av det FN-anknutna standardiseringsorganet ITU-T. SIS svenska översättning av ISO-standarden definierar molnbaserade datortjänster som **”…ett koncept som möjliggör nätverksåtkomst till en skalbar och elastisk pool av delade fysiska eller virtuella resurser som via självbetjäning levereras och administreras på begäran**”.[3]

ISO-standarden fastställdes av SIS i december 2014. Eftersom den är förhållandevis ny är den ännu inte lika spridd som äldre definitioner. I allt väsentligt överensstämmer grundbeskrivningen av datorbaserade molntjänster med t.ex. NIST:s definition. Vi ser att SIS/ISO:s allmänna definition ovan, tillsammans med de huvudegenskaper för molnbaserade datortjänster som ISO/SIS också slår fast (se nedan) fungerar väl som utgångspunkt för analyser och resonemang i detta uppdrag.

[1] The NIST Definition of Cloud Computing, Special Publication 800-145
[2] Arbetsgrupp Molnet i offentliga sektorn, Cloud Sweden, s.1
[3] Informationsteknik – Molnbaserade datortjänster – Översikt och terminologi (ISO/IEC 17788:2014)

De huvudegenskaper (kännetecken) som ISO och SIS har definierat och som ytterligare ramar in begreppet listas nedan:

1. Brett tillgänglig nätverksåtkomst

De fysiska och virtuella resurserna finns tillgängliga över ett nätverk och nås via standardiserade mekanismer vilket främjar användningen av heterogena klientplattformar. Användarna kan komma åt fysiska och virtuella resurser från olika platser med hjälp av olika klienter och enheter så länge det finns tillgängliga nätverk.

2. Uppmätt tjänst

En funktion där den uppmätta leveransen av molntjänster medger att användningen kan övervakas, styras, redovisas och debiteras. Kunderna betalar endast för de resurser de nyttjar. 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.

3. Fleranvändande

Fysiska eller virtuella resurser fördelas på ett sådant sätt att flera användare delar miljö, men deras beräkningar och data är isolerade från och oåtkomliga för varandra. En grupp av användare tillhör oftast samma molntjänstkund, men det kan finnas fall där en grupp av molntjänstanvändare innehåller användare från flera olika kunder, särskilt vid publika moln och partnermoln (se Figur 2 i kap. 2.6 nedan). En viss molntjänstkund kan omvänt ha olika engagemang med en enda molntjänstleverantör.

4. Självbetjäning på begäran

Molntjänstkunden 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.

5. 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 de fysiska eller virtuella resurser som är åtkomliga som obegränsade och de verkar kunna köpas och nyttjas omedelbart, oavsett mängd och när som helst, med förbehåll för eventuella begränsningar i serviceavtal. Den upplevda kundnyttan är att inte behöva oroa sig för begränsade resurser eller för kapacitetsplanering.

6. 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.

2.4 Molntjänster och traditionell outsourcing

Outsourcing brukar definieras som att en aktör via avtal låter en annan aktör sköta en eller flera processer eller funktioner för dennes räkning, vilka annars skulle ha utförts av aktören själv. Sådan utkontraktering, dvs. det som i dagligt tal kallas outsourcing, kan t.ex. ske genom molntjänster.[4] Nedan identifieras några områden av betydelse där vår bedömning är att molntjänster och traditionell outsourcing dock skiljer sig åt.

2.4.1 Affärsrelation och affärsmodell

It-avdelningar outsourcar ofta enstaka it-funktioner (tjänster) eller hela driftmiljöer. Vid traditionell outsourcing är kontrakten vanligen fleråriga och parterna, beställare och leverantör, bygger en långsiktig affärsrelation. Helhetsåtaganden är vanliga och innebär att leverantören behöver lära känna beställarens verksamhet och behov, inklusive långsiktiga utvecklingsbehov och behov i tangerande verksamheter, för att kunna uppfylla åtagandet. Några sådana långa, eller djupa, åtaganden kännetecknar vanligen inte köp av en molntjänst. Molntjänster kan svara mot ytterst temporära behov, ända ner till köp per timme, till exempel vid verksamhetstoppar eller vid genomförande av ett visst projekt eller en viss kampanj i en verksamhet.

Den outsourcade tjänsten har vidare sällan de kännetecken som beskrivs för molntjänster ovan, såsom självbetjäning, betalning efter användning och möjlighet att till synes obegränsat och omedelbart skala upp respektive ner den tjänst som köps. Outsourcing innebär istället typisk ett mått av fasta kostnader och andra fasta parametrar som sätts vid avtalets ingång och baseras på att leverantören upprätthåller en viss funktion över tid.

Medan de senare årens outsourcingtrend inom offentlig sektor har drivits av en ambition att renodla verksamheter och att skala bort sådant som inte är att se som en organisations kärnuppgift, och som man bedömt kunna utföras med större kostnadseffektivitet eller kvalitet av en annan aktör, så är de starka drivkrafterna bakom användningen av molntjänster, vid sidan av en önskad kostnadseffektivitet, också möjligheten till flexibilitet och snabb skalbarhet för verksamheten. Den tekniska utvecklingen tillsammans med användarnas behov har drivit på utvecklingen av molntjänster. Den stora skillnaden jämfört med traditionell outsourcing ligger trots detta i det faktum att molntjänster innebär en annorlunda affärsmodell.

2.4.2 Organisation och roller

Även i organisatoriska termer finns generellt sett skillnader mellan traditionell outsourcing och molntjänster. Medan outsourcing innebär att lägga ut en verksamhet på annan utförare, innebär molntjänster istället att man köper de funktioner som verksamheten annars hade behövt producera.

Inom offentlig förvaltning innebär traditionell outsourcing dessutom ofta verksamhetsövergång, dvs. att den utförande aktören övertar både verksamheten som

[4] Det finns en diskussion om huruvida molntjänster är att betrakta som outsourcing. Vi anser dock, som framgår i detta avsnitt och av rapportens rubrik, att det är en specifik form av outsourcing. Se bl.a. Cloud Computing; CIO Desk Reference, updated Q3 2013 s. 5, Gartner

outsourcas och dessutom övertar den personal som tidigare har utfört arbetet inom den upphandlade verksamheten. Verksamhetsövergång används generellt sett inte vid köp av molntjänster och har så långt vi kan se inte heller prövats som princip vid köp av molntjänster.

Vid traditionell outsourcing är det vanliga att en beställare och en leverantör med ett helhetsåtagande sätter upp speglande förvaltningsorganisationer med tillhörande processer och rutiner som svarar mot just den specifika avtalssituationen. Vid köp av en molntjänst, där tjänsten levereras till flera, används vanligen inte samma speglande förhållningssätt när det kommer till organisation och involverade roller. Såväl förvaltning som utveckling drivs av molnleverantören själv dvs. är inte lika mycket av ett iterativt arbete mellan beställare och leverantör. Däremot ökar kraven på en beställare av molntjänster att själv analysera sitt behov redan innan man går in i en molntjänst.

2.4.3 Teknik

Vid outsourcing kan leverantören antingen tillhandahålla egen infrastruktur, plattformar och system för att fullgöra uppgiften, eller överta och arbeta med de tekniska resurser som ägs av beställaren (den som outsourcar). Det senare förekommer inte vid köp av molntjänst där infrastruktur, plattformar och mjukvara tillhandahålls av leverantören och delas av flera. Ett av de sex kännetecknen för en molntjänst är att molntjänstleverantörer levererar till flera kunder på samma infrastruktur. Därigenom är det möjligt att få större skalfördelar än vid traditionell outsourcing. Internets utbredning har varit en viktig teknisk förutsättning för framväxten av molntjänster. Den tekniska utvecklingen under framför allt 2010-talet har gjort det enklare att dela på datorkapacitet och att automatisera köp och användning av it-tjänster.

2.4.4 Sammanfattning

Sammanfattningsvis konstateras att användning av molntjänster är en form av outsourcing av it om de särskilda kännetecken som beskrivits ovan finns, dvs. om definitionen av en molntjänst uppfylls. Som vi visat ovan finns dock tydliga olikheter i form av drivkrafter och lösningar mellan en traditionell outsourcing och köp av molntjänst.

2.5 Tre typer av molntjänster

Det finns tre internationellt etablerade typer av molntjänster som beskriver tre olika funktionsområden. Tjänstebeskrivningen utgår från tekniskt perspektiv och tjänsterna återfinns i olika tekniska lager – olika nivåer i den tekniska ”stacken” – där man för varje nivå i tjänsten lägger på en teknisk dimension. Då definitionen är globalt spridd väljer vi att i det följande använda de engelska termerna och förkortningarna.

2.5.1 Infrastructure as a Service

Infrastructure as a Service (IaaS) innebär it-infrastrukturella tjänster i nätet, vilket i den svenska versionen av SIS-standarden motsvarar termen ”infrastrukturrelaterad molnfunktionstyp”.

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, lagring och utvecklade och utrullade applikationer i

infrastrukturen. Ibland kan IaaS-kunder ha begränsad kontroll över utvalda nätverkskomponenter, t.ex. brandväggar.

I Pensionsmyndighetens enkät undersöktes bl.a. hur många av myndigheterna som använder sig av infrastrukturella molntjänster idag. Av de som svarade på frågan om de använder olika typer av molntjänster (141 myndigheter av 148) använde cirka 70 procent inte IaaS idag, knappt 30 procent gjorde det och övriga svarade att de inte vet. Infrastrukturella tjänster används med andra ord inte i någon omfattande utsträckning i myndighetssverige idag.

2.5.2 Platform as a Service

Platform as a Service (PaaS) innebär att leverantören tillhandahåller applikationsplattformar via internet eller annat nät, för användare att installera sina egna applikationer i. SIS standard refererar till PaaS som ”plattformsrelaterad molnfunktionstyp”.

Ett exempel på en PaaS-tjänst är utvecklingsmiljöer som tjänst. En PaaS-tjänst inkluderar en underliggande infrastruktur men adderar ett ramverk (programspråk och utvecklingsmiljöer) där man kan köra eller utveckla nya system. Kunden driftsätter alltså egna eller införskaffade applikationer men kan använda 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 applikationer som körs i plattformen, samt konfigureringar i plattformen.

Plattformstjänster används inte heller i någon större utsträckning i myndighetssverige idag. Endast 23 procent av de svarande i myndighetsenkäten anger att använder någon form av plattformstjänst som molntjänst, 73 procent gör det inte och de övriga svarande uppger att de inte vet.

2.5.3 Software as a Service

Software as a Service (SaaS) innebär att leverantören tillhandahåller mjukvara som tjänst, dvs. färdiga eller konfigurerbara applikationer över internet eller annat nät. Tjänstetypen kallas ibland även Applications as a service (AaaS) och i den svenska SIS-standarden refereras den till som ”applikationsrelaterad molnfunktionstyp”. 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.

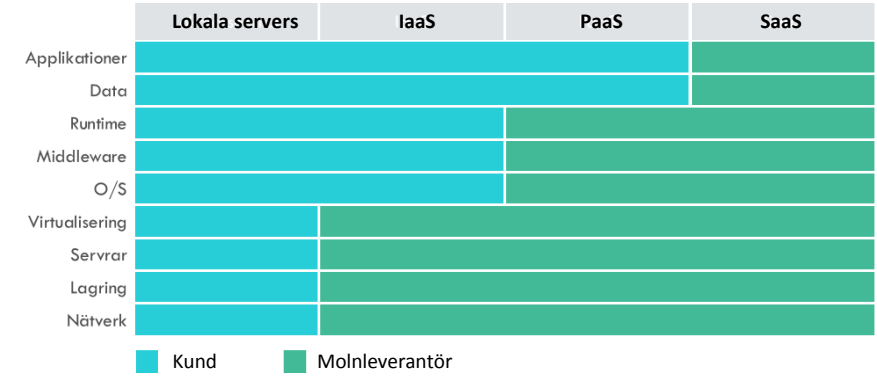


Bild 1 Tjänstegränssnitt per tjänsteområde (bild från Microsoft)

När det kommer till mjukvarutjänsternas användning i statlig sektor är situationen den omvända jämfört med IaaS och PaaS: cirka 78 procent av de svarande anger att de köper mjukvara som tjänst, medan knappt 22 procent inte gör det.

2.6 Olika molntjänsters förhållande till varandra

Den etablerade indelningen i tre olika typer av molntjänster bygger på en teknisk uppdelning där de tre tjänstetyperna placerar sig på olika höjd i den tekniska stacken. De tre tjänstetyperna kan i sin tur beskrivas i termer av s.k. tjänstekategorier som tydliggör olika funktioner som upprätthålls för kunden med molntjänsten. Exempel på sådana tjänstekategorier är t.ex. kommunikation som tjänst, datalagring som tjänst, nätverk som tjänst, identitet som tjänst, säkerhet som tjänst eller skrivbord som tjänst.

Nya tjänstekategorier med funktionsbaserade beskrivningar av molntjänster fortsätter att utvecklas i snabb takt, varför det är riskabelt att inkludera eller exkludera olika tjänstekategorier i vad som ska anses vara en molntjänst. I denna rapport håller vi oss huvudsakligen till definitionen av de tre vedertagna typerna av tjänster. Vi tillåter oss dock att använda tjänstekategorier (dvs. nedbrytningar av de tre tjänstetyperna) som exempel.

Vissa molntjänster befinner sig i gränslandet mellan olika tjänstetyper och kan vara mer svårkategoriserade. En tjänst kan innehålla exempelvis infrastruktur- och plattformstjänster paketerat. IaaS, PaaS och SaaS är dock internationellt vedertagna begrepp och fyller fortfarande en viktig funktion som förklarings- och förenklingsmodell.

SaaS-tjänster kan vid första anblicken uppfattas som ”enklare” – både att använda och att köpa – än infrastrukturella tjänster eller plattformstjänster. Den som köper eller använder en SaaS-tjänst bör dock komma ihåg att man alltid får med en infrastruktur och en plattform i botten, liksom att den som köper en plattformstjänst automatiskt kommer att befinna sig i PaaS-leverantörens infrastruktur.

Bilden nedan visar exempel på tjänstekategorier inom vardera tjänstetyp. Listan kan göras längre.

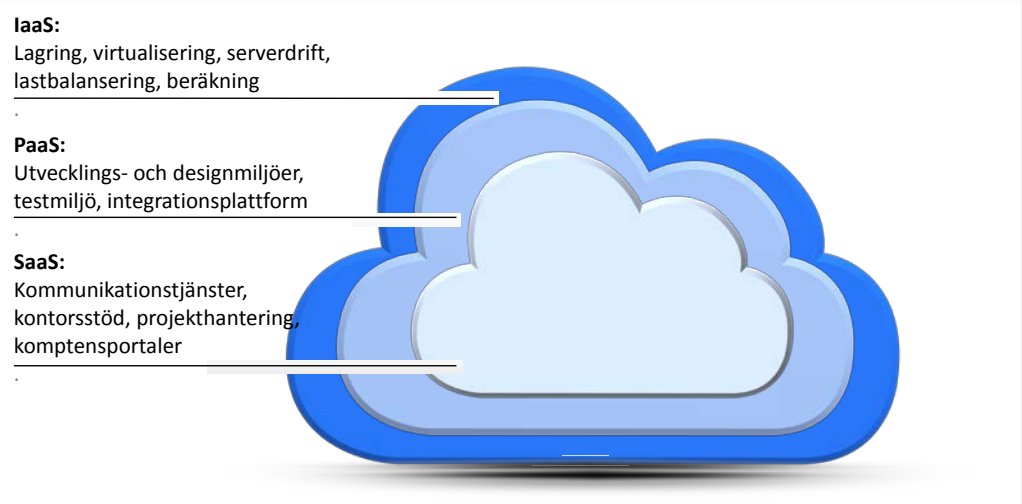


Bild 2 Exempel på olika typer av molntjänster

Över tiden och i takt med att den tekniska utvecklingen fortgår kan vi förvänta oss att nya tjänstetyper och nya tjänster kommer att växa fram. Så kan t.ex. framväxten av s.k. mikrotjänster, dvs. små program som tillhandahåller en viss funktion och som nås via ett programmeringsgränssnitt (API:er), kommer att förändra tjänstestrukturen.

2.7 Modeller för tillhandahållande av molntjänster

NIST och ISO-standarden beskriver fyra sätt att tillhandahålla (organisera) moln-tjänster, s.k. ”service deployment”: publika moln, partnermoln, hybridmoln och privata moln.

2.7.1 Publikt moln

Molntjänsten ägs och hanteras av en molntjänstleverantör (tredje part) som säljer resurser till flera kunder på samma infrastruktur. Tjänster i publika moln är potentiellt tillgängliga för alla som så önskar.

Även i ett publikt moln kan olika kunders information vara olika mycket separerad. Ju mer separerad, desto mindre potentiella skalfördelar. Samtidigt kan säkerhetsmässiga fördelar göra en separering inom det publika molnet rationell.

2.7.2 Partnermoln

Partnermoln, ibland också omnämnda som ett gemenskapsmoln (community cloud) eller branschmoln, erbjuds till en begränsad och väldefinierad grupp av intressenter/ kunder. Molntjänsten levereras åt kunder med likartad kravbild. Den gemensamma kravbilden kan avse t.ex. uppdrag, målsättning, säkerhetskrav och krav på efterlevnad. Partnermolnet ägs/hanteras av en eller flera av kunderna i samarbete, alternativt av, eller tillsammans med, en tredje part, och kan tillhandahållas antingen ”off premises”, utanför byggnaden, eller ”on premises”, dvs. i byggnaden.

En särskild form av partnermoln är myndighetsmoln (government cloud). Ett govern-ment cloud har skapats i t.ex. Storbritannien, för att möta särskilda behov av t.ex. säkerhet. G-cloud och Storbritanniens erfarenheter beskrivs i bilaga 2.

2.7.3 Privat moln

I andra änden av skalan finns privata moln, 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 (jmfr de ovan listade kännetecknen för en molntjänst) krävs att it-resurserna genomgår samma process av t.ex. virtualisering, automatisering och kategorisering/paketering efter regelverk.

2.7.4 Hybridmoln

Termen hybridmoln avser en sammansättning av två eller flera molntyper som möjliggör kopplingar mellan olika tjänster och molntyper.

Hybrida lösningar är idag relativt vanligt och förväntas av många att fortsätta öka. Ett skäl för att skapa hybridmoln kan vara att kombinera fördelarna med snabbhet och kostnadseffektivitet från ett publikt moln med behov av privat molntjänst eller partnermoln i andra delar. Samtidigt bör man i en strategi med hybridlösningar noga analysera i vilken utsträckning de förväntade fördelarna nås.

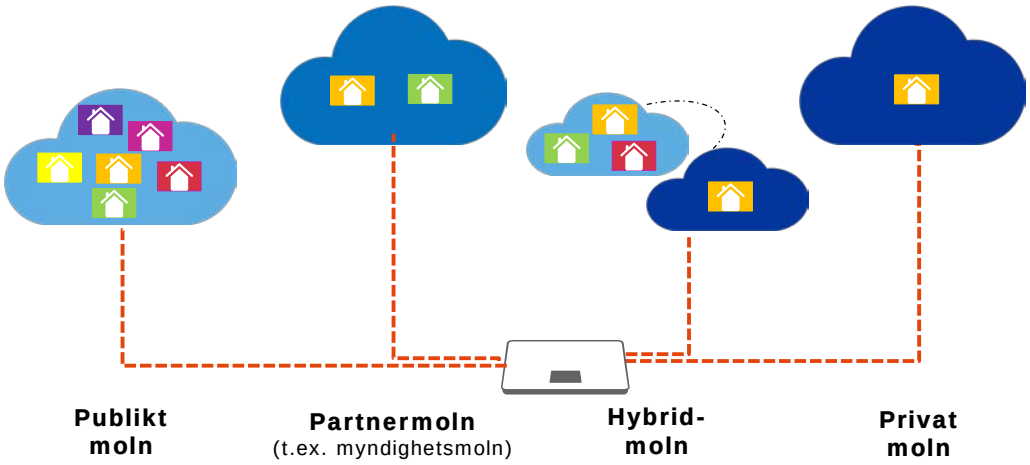


Bild 3 Metoder för tillhandahållande av molntjänster

2.7.5 Överväganden kring val av tillhandahållande

Liksom de tre tjänstetyperna är de fyra beskrivna sätten att tillhandahålla molntjänster en förenkling av verkligheten eftersom det förekommer många olika varianter. En molntjänst vara publik eller privat i olika utsträckning, och vem som tillhandahåller den kan också skilja sig åt. Leverantörer som tillhandahåller branschmoln kallar ibland dessa ”semi-publika”. En analys av leveranssättet behöver göras i det enskilda fallet.

Myndigheter som överväger användning av molntjänster behöver initialt analysera huruvida en viss informationsmängd av olika legala skäl och säkerhetsrelaterade skäl över huvud taget kan hanteras i ett publikt moln eller i ett privat. Därtill måste myndigheten inför upphandlingen även ta ställning till hur säkerheten ser ut för den specifika lösningen, hur informationen behandlas då den transporteras och i vilken mån informationen hålls åtskild, vilka som har tillgång till den och var den lagras geografiskt, samt vilket lands lagstiftning som gäller vid krav på utlämnande av informa-

tion. I kapitel 5 nedan går vi igenom juridiska och säkerhetsrelaterade överväganden för myndigheterna.

2.8 Roller vid köp och leverans av molntjänster

ISO-standarden definierar tre grundläggande roller som kan vara involverade i tillhandahållande och bruk av molntjänster.

2.8.1 Molntjänstkund

Molntjänstkunden är den part i affärsrelationen som nyttjar molntjänsten för sin verksamhet. Molntjänstkunden ingår affärsrelationen antingen med en molntjänstpartner eller med en molntjänstleverantör.

Hos molntjänstkunden berörs internt ett antal roller vid en övergång till molntjänster. Vilka krav som molntjänster ställer på intern kompetens analyserar vi i kapitel 7 nedan.

2.8.2 Molntjänstleverantör

Molntjänstleverantör är den part som tillhandahåller molntjänsten. Denne fokuserar på de aktiviteter som är nödvändiga för att säkra leverans och underhåll av tjänsten, inklusive utrullning, support, övervakning, riskhantering m.m, där de olika aktiviteterna utförs av personer i olika sub-roller.

En molntjänstleverantör kan ha en eller flera underleverantörer som tillhandahåller hela eller delar av den tjänst som molntjänstkunden konsumerar. Även om den centrala relationen och det centrala avtalsförhållandet är det mellan molntjänstleverantören och molntjänstkunden, är det värt att poängtera att en molntjänstkund behöver tillse att t.ex. hantering av personuppgifter hanteras enligt kundens avtalade krav i alla led.

2.8.3 Molntjänstpartner

Ibland finns även en molntjänstpartner som ger stöd eller agerar medhjälpare till antingen molntjänstkunden eller molntjänstleverantören, eller till båda parter. De aktiviteter som en molntjänstpartner utför beror på vilken typ av partnerskap som är aktuellt, men det kan handla om t.ex. granskning av en eller flera molntjänster för molntjänstkundens räkning (”cloud auditor”), eller att förmedla molntjänster mellan leverantör och kund som molntjänstmäklare (”cloud service broker”).

2.8.4 Roller i förändring

Rollen som kund eller beställare, och rollen som leverantör, känns igen från traditionell outsourcing. Vanligtvis blir dock leverantörens roll starkare när det är en molntjänst som tillhandahålls än om leverantören är särskilt upphandlad enbart för en kund i traditionella outsourcingavtal.

Det pågår en diskussion om huruvida molntjänster kommer att föra med sig att antalet molnmäklare växer. Starkt standardiserade tjänster med tydliga prislistor gör att it-köp å ena sidan kan upplevas som enklare att ta ställning till och genomföra. Bilden är dock mer komplex än så. Framväxten av molntjänster och erbjudanden som kombinerar olika tjänster påverkar i vissa fall vilken roll ett enskilt företag har. Ett företag kan i ett läge vara molntjänstleverantör, för att i nästa stund förmedla en kompletterande tjänst till en annan leverantör, vilket innebär att företaget i det senare fallet övergår till en roll som molntjänstpartner.

Med en fortsatt specialisering, ett breddat utbud och en fortsatt utveckling av nya samarbeten mellan leverantörer, är det troligt att även mäklarrollen kommer att fortsätta utvecklas.

3 Strategisk grund för molntjänster

Sammanfattning

Molntjänster kan gynna flera centrala politiska mål. Oavsett om vi antar ett brett tillväxt- och hållbarhetsperspektiv, ett konkurrenskraftsperspektiv, främjande av små och medelstora företag, eller ett förvaltningspolitiskt perspektiv så fyller molntjänster en viktig roll. Det är därför av vikt att de hanteras som en strategisk fråga på makronivå både i svensk politik och inom EU. Vid sidan av makroperspektiven finns också en rad potentiella fördelar eller nyttor för den enskilda statliga aktören. De mest centrala beskrivs i kommande kapitel.

3.1 Digital (r)evolution

Världsekonomin genomgår idag en digital revolution som innebär en mycket snabb och samhällsomspännande omdaning, med nya förutsättningar och stora effekter på såväl individer som företag, myndigheter och andra organisationer. *Molntjänsternas snabba utveckling utgör en frontlinje i den digitalisering vi nu upplever.* Om internet revolutionerade tillgången på information, så revolutionerar molntjänster tillgången till kraft och kapacitet, var och när som helst. Med det följer också möjligheten att få del av helt nya tjänster och funktioner som annars inte hade varit tillgängliga. Nya nyttor uppstår och andra kommer fler till del.

Molntjänster är en viktig fråga för den offentliga sektorn i Sverige idag om man ska åstadkomma omställningsförmåga och effektivitet i offentlig förvaltning. Molntjänster påverkar oss 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. Som tillväxt- och produktivitetsmotor får molntjänster också effekt på de ekonomiska grundförutsättningarna för att bedriva offentlig verksamhet. Positiv påverkan på näringslivet och företagens omsättning leder till att BNP ökar, vilket är positivt för skatteunderlaget (skatteintäkterna). Se vidare 3.2. nedan.

Vi ser att molntjänster är en ledningsfråga för statliga och andra offentliga verksamheter. Även om relevansen av prefixet ”moln-” allt oftare ifrågasätts, är det få personer som tvekar på att det underliggande mönstret – att köpa de funktioner man vill ha som tjänster och att göra det på ett flexibelt och skalbart sätt – är här för att stanna.

Analysen av potentialen i molntjänster tar sitt avstamp i några för molntjänster centrala strategier, med de närings- och förvaltningspolitiska perspektiven i särskilt fokus.

3.2 Näringspolitiska strategier och mål

3.2.1 Tillväxt och välfärd

Tillväxt är centralt för många politikområden, inklusive näringspoltiken. Molntjänsters framväxt kan på flera sätt bidra till centrala mål för tillväxt och välfärd. EU antog 2010 strategin ”Europa 2020 – En strategi för smart och hållbar tillväxt för alla”. Strategin omfattade tre huvudsakliga prioriteringar för den närmaste tioårsperioden:

- *Smart tillväxt* – utveckla en ekonomi baserad på kunskap och innovation
- *Hållbar tillväxt* – främja resurseffektivare, grönare och konkurrenskraftigare ekonomi
- *Tillväxt för alla* – stimulera en ekonomi med hög sysselsättning och ekonomisk, social och territoriell sammanhållning[5]

Utveckling och användning av molntjänster kan bidra positivt på flera sätt till prioriteringarna ovan. Ur ett konkurrenskraftsperspektiv bidrar svenska molntjänstföretag till att Sverige kan bibehålla eller stärka sin spets inom it-området. Omvänt gäller förvisso, att om vi hamnar i ett läge där svenska företag – även små och medelstora företag – inte kan konkurrera med utländska molntjänstleverantörer, så riskerar svensk it-industri att minska och it-kompetensen i landet på sikt att utarmas.

Näringsliv inom olika branscher kan utvecklas snabbare genom molntjänster. Affärsidéer som bygger på användning av flexibla molntjänster ger kommersiellt försteg och fler växande innovativa företag, vilket i sin tur ger förbättrad konkurrenskraft och kan ge fler jobb. Även företag vars affärsidéer inte bygger på att tillhandahålla produkter genom molntjänster gagnas. Företag generellt kan få mer kostnadseffektiva it-lösningar som gör att företagen kan fokusera sina resurser på att utveckla kärnverksamheterna, vilket i nästa steg också främjar ökad konkurrenskraft och kan bidra till fler arbetstillfällen.

För små och medelstora företag, s.k. SME:s, kan enkel access till molntjänster betyda särskilt mycket och även bidra till att överbrygga ”the tyranny of distance” när man vill nå mer avlägsna marknader eller själv befinner sig på distans från sin marknad. Minskad energiåtgång kan åstadkommas genom en mer effektiv it-drift i t.ex. publika molntjänster, vilket stärker hållbarheten i samhället. Molntjänster kan också underlätta framkomsten av nya användbara tjänster som leder till aktivt deltagande i samhällslivet för fler EU-medborgare.

3.2.2 It-politik

It-politik utgör traditionellt en del av den svenska näringspolitiken men genomsyrar och påverkar politiken på ett flertal områden. Samtidigt kan svensk it-politik i delar styras av andra områdesmål, såsom de förvaltningspolitiska målen (se nedan).

Målet för svensk it-politik är att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter.[6] Innovativa och samverkande digitala lösningar ska bidra till en enklare vardag för medborgare och företag. Flera av de myndigheter som var representerade i E-delegationen har tilldelats medel av regeringen för att utveckla digitala lösningar för att stödja individers livshändelser.

Ett delmål för it-politiken är att elektroniska kommunikationer ska vara effektiva, säkra och robusta samt tillgodose användarnas behov. De elektroniska kommunikationerna ska i första hand tillhandahållas genom en väl fungerande marknad, men staten ska ha ett ansvar på områden där allmänna intressen inte enbart kan tillgodoses av marknaden. Synen på effektivitet, säkerhet, robusthet och marknadens kontra

[5] Europa 2020 – En strategi för smart och hållbar tillväxt för alla s. 10, KOM (2010)2020 slutlig

[6] Mål för IT-politik, http://www.regeringen.se/regeringens-politik/it-politik/mal-for-it-politik/, Prop. 2011/12:1, utg. omr. 22, s. 84

statens roll är viktiga utgångspunkter för analysen av molntjänster och bör vara vägledande för framtida initiativ inom området.

3.3 Förvaltningspolitiska strategier och mål

Löpande utveckling och förnyelse av statsförvaltningen är en förutsättning för att regeringens politik ska få genomslag inom alla områden. Utvecklingsarbetet bedrivs både av regeringen och av myndigheterna själva[7].

Regeringen vill se en digitalt samverkande statsförvaltning, en e- förvaltning, som ska vara innovativ, samverkande, rättssäker och effektiv samt ha en väl utvecklad kvalitet, service och tillgänglighet. Målsättningen för en digitalt samverkande statsförvaltning är:

- en enklare vardag för medborgare,
- en öppnare förvaltning som stödjer innovation och delaktighet, samt
- högre kvalitet och effektivitet i verksamheten

I budgetpropositionen för 2015 aviserade regeringen en förstärkt styrning och samordning av övergripande it-användning i statsförvaltningen, i syfte att stimulera digitaliseringen av den svenska offentliga förvaltningen.[8] Regeringens satsningar ska bidra till att nå målen för e-förvaltning samt främja utvecklingen och användningen av gemensamma lösningar och en effektiv it-användning i staten. En förstärkt styrning är en signal från regeringen som visar på en önskan att se snabbare effekter både vad gäller kostnadseffektiv it liksom graden av digitalisering och samverkan i offentlig sektor. Molntjänster, och olika typer av stöd och ramverk kring dessa, är intressanta både som ett sätt att främja kostnadseffektivitet och för att samverka kring tjänster i offentlig sektor.

I strategin ”Unleashing the potential of Cloud Computing in Europe” från 2012 slår EU-kommissionen fast att molntjänster är betydelsefulla för möjligheten att minska myndigheternas kostnader genom minskat behov av egna infrastrukturella investeringar och genom lägre operativa löpande kostnader. Samtidigt kan molntjänster underlätta resan mot effektiva tjänster som är interoperabla, skalbara och digitala. De kan också bidra till bättre användarvänlighet och ökad säkerhet i offentliga tjänster.[9]

3.3.1 Digital agenda

Både på EU-nivå och i den nationella politiken har digitala agendor och strategier för digitalisering tagits fram.[10] Principen ”Digital first” i EU har nyligen följts av ”digitalt först” som regeringens uttalade strategi för Sverige. Digitalt först innebär bl.a. att digitala lösningar ska väljas i första hand. I praktisk vardag kan det innebära att utveckling av medborgartjänster ska formas utifrån kundbehov med utgångspunkt i digitala möjligheter och inte utifrån dagens pappersbaserade processer och rutiner.

Molntjänster kan – rätt anskaffade och implementerade – bidra till att förflytta svensk förvaltning till digitala tjänster med interoperabilititet, snabb skalbarhet och tjänster

[7] Se bl.a. Prop. 2014/15:1
[8] Prop. 2014/15:1
[9] Unleashing the Potential of Cloud Computing in Europe, COM(2012) 529 final s. 5.
[10] Digital Agenda for Europe- A Europe 2020 Initiative (201xx), A Digital Single Market Strategy for Europe (2015) samt It i människans tjänst.– en digital agenda för Sverige (2011) och ”Nu digitaliserar vi det offentliga Sverige”, pressmeddelande från regeringen 2015-10-29

som stöder mobil användning. Molntjänster kan bidra till att nya tjänster kan rullas ut både kostnadseffektivt och snabbt. De kan också användas för plattformar för kommunikation med medborgare och företag.

Regeringen har beslutat om ett råd för digitalisering av det offentliga Sverige. Rådet, som leds av it-minister Mehmet Kaplan och samlar myndighetschefer i några av de större statliga myndigheterna samt kommunala företrädare, ska stötta samverkan mellan statlig och kommunal sektor. Rådet för digitalisering av det offentliga Sverige bör särskilt titta på vilken roll molntjänster kan spela för utvecklingen av offentliga digitala tjänster.

4 Potential för molntjänster i statliga verksamheter

Sammanfattning

Innovation och möjlighet till snabb förnyelse är vid sidan av flexibilitet och skalbarhet, kostnadseffektivitet, tillgänglighet och ökad säkerhet centrala nyttor som ofta kan nås med molntjänster. Användning av molntjänster kan också minska behovet av egen it-personal. Förvaltningsgemensam utveckling kan förenklas av att använda molntjänster i gränssnittet mellan myndigheter. På senare tid har andra nyttor än kostnadseffektivitet kommit att värderas högt vid valet att gå över i molntjänster. Kostnadsbesparingarna varierar beroende på verksamhet, typ av tjänst och hur verksamheten ser ut, men är mer sannolika att uppnå under vissa omständigheter.

4.1 Nyttor på mikronivå

Offentliga aktörers användning av molntjänster diskuteras ofta i termer av juridiska ramar och de krav på säkerhet och sekretess som omgärdar olika typer av statlig och annan förvaltning. Molntjänster erbjuder dock också en stor potential för offentliga verksamheter. De kan, som kapitlet ovan visar, vara en viktig hävstång för att uppnå centrala politiska mål inom både EU och Sverige. Utöver denna makronivå finns fördelar även på mikronivå.[11] Nedan beskrivs ett antal potentiella nyttor eller fördelar med molntjänster för statliga och andra offentliga aktörer:

- Innovation, tjänsteutveckling och möjlighet till snabb förnyelse
- Tillgänglighet
- Ökad flexibilitet och skalbarhet
- Kostnadseffektivitet
- Ökad säkerhet
- Minskat behov av egen it-personal
- Förvaltningsgemensam utveckling.

4.2 Innovation, tjänsteutveckling och möjlighet till snabb förnyelse

Användningen av molntjänster kan ge offentliga verksamheter tillgång till fler nydanande tjänster som dessutom kan tillhandahållas snabbare, eftersom molntjänstleverantören har kortare s.k. ”time to market” än de flesta som utvecklar tjänster i egen regi. Innovativa digitala tjänster kan förändra en myndighets kontakt med sina kunder.

[11] Se bl.a. Affärsnytta med molnet s. 4ff, Cloud Sweden

I privat sektor är möjligheten att hitta nya affärsmöjligheter med hjälp av molnlösningar idag i stort fokus. Helt nya affärsidéer, helt nya företag och även nya konstellationer av företagssamarbeten uppstår i digitaliseringens och molnhanteringens kölvatten. Tjänster som AirBnB, Peer to peer-lån, självkörande bilar som kommunicerar via molntjänster, smarta piller som sänder signaler till vårdgivaren – exemplen på nya affärsidéer som har molntjänstlösningar inbyggda i sitt erbjudande är många. Tillgången till innovativa och nyskapande tjänster förväntas växa lavinartat under de närmaste åren.

Även offentliga verksamheter kan hitta helt nya tjänstemöjligheter som bara kan åstadkommas med hjälp av molntjänster. En möjliggörare för bred framtida användning av digitala tjänster är möjligheten till e-identifiering och -signering. Kanske kan man tänka sig att Sverige i framtiden, likt Estland idag, kan införa ett e-medborgarskap där alla medborgare förses med ett id-kort med e-legitimation. Med detta skulle medborgare och företag kunna nyttja tjänster byggda på myndighetsinformation varifrån som helst. De skulle också kunna koppla ihop olika tjänster och olika informationsflöden och därigenom skapa nya nyttor.

Myndigheter kan genom användning av molntjänster ta del av innovativa lösningar inom it-området som verksamheten inte hade kunnat utveckla i egen regi eller som inte hade uppstått i en traditionell outsourcingrelation.

Den ökade snabbheten kommer av att driftssättning av nya versioner, nya funktioner och nya tjänster sker snabbare och effektivare hos molnleverantören med skalfördelar och god tillgång till resurser med specialistkompetens.

Det nätbaserade distributionssättet gör också att myndigheter och andra aktörer snabbare kan få del av viktiga värden. Nya uppdaterade versioner av tjänsten kan levereras löpande, men kan också dras tillbaka lika snabbt om det skulle visa sig att de inte håller rätt kvalitet. Cyklerna för utveckling blir generellt kortare. Affärs- eller verksamhetsvärden kommer förvaltningen till godo och ökar värdet av de tjänster som myndigheten erbjuder till sina kunder.

Användning av molntjänster kan främja innovation på flera sätt:

1. Myndigheter som använder en molntjänst för sin egen it-drift och underhåll kan styra om mer av egna resurser mot utveckling och innovation i andra delar av verksamheten, t.ex. i utveckling av nya tjänster för medborgare och företag.
2. Molntjänstleverantören har i kraft av skalfördelar och specialisering mycket större möjligheter att arbeta strukturerat och långsiktigt med innovation i it-tjänster. Det gagnar de verksamheter som är kunder i en sådan innovationsstark molnlösning. Samtidigt bör man som köpare vara beredd på att de egna möjligheterna att påverka utvecklingsarbetets riktning minskar. Det kan dock vara ett fullt rationellt vägval om den statliga aktören inte ser att man själv har ekonomiska eller andra resurser för att åstadkomma samma utvecklingsresa och att man litar till molntjänstleverantörens förmåga att bedöma vilka funktioner m.m. som kommer att efterfrågas i framtiden.
3. Molntjänster i sig innebär låg tröskel för strukturförändringar och därmed möjlighet att ta större utvecklingssteg. Detta gäller framför allt de publika molntjänsterna som delas mellan flera.

4. Molntjänster med öppna gränssnitt gör att kunskap och erfarenheter kan ackumuleras och nya molntjänster utvecklas utifrån andra, redan existerande molntjänster. Vinnare på detta är tjänsternas användare som snabbare kan addera nya eller större värden till sina verksamheter.

Genom en bred användning av infrastruktur- och plattformstjänster i molnet, kan en verksamhet i praktiken förnya it-parken oftare än vad som hade varit fallet om man arbetat med en egen it-park och livscykeln kan göras kortare.

I Pensionsmyndighetens myndighetsenkät (oktober 2015) bad vi de svarande myndigheterna att uppge vilka motiv eller skäl som låg bakom att myndigheterna valt molntjänster. Myndigheterna kunde ange flera svarsalternativ som skäl. Totalt angav cirka 23 procent av de svarande möjligheten att få tillgång till nya innovativa tjänster som skäl, och 33 procent möjligheten till snabbare implementering. Uppdelat på typ av tjänst var samma siffror för mjukvarutjänster (SaaS) 25 respektive 40 procent, för plattformstjänster (PaaS) 33 respektive 38 procent, samt för infrastrukturtjänster (IaaS) 24 respektive 38 procent.

4.3 Tillgänglighet

Molntjänster kan verka positivt på tillgängligheten på två olika sätt: tillgänglighet i form av åtkomst och tillgänglighet i form av minskad nertid.

Många molntjänster byggs för att vara enkelt åtkomliga från olika typer av tekniska kommunikationshjälpmedel - olika ”devices” - och från olika typer av webbläsare. Molntjänster, inte minst applikationer, kan alltså göra det lätt att komma åt vardagstjänster för såväl kunder, kunders kunder och för egna anställda. Den som jobbar med t.ex. en e-desktop-tjänst, kommer enkelt att kunna ta del av sina dokument, mail m.m. oavsett vilken teknisk utrustning man väljer att använda, och oavsett var man befinner sig.

En annan form av tillgänglighet som molntjänster kan ge, är tillgänglighet till information om it-tjänsten och den egna tjänstekonsumtionen. I dessa fall skapas en nytta internt på it-avdelningen. Molntjänster levereras ofta via en s.k. ”dashboard” (web-panel) där den som köper tjänsten enkelt kan se hur man nyttjar tjänsten och ändra aktuellt köp efter principen ”pay-per-use”, köp efter användning. Som användare kan man oftast på ett enkelt och tillgängligt sätt övervaka leveransen till den egna verksamheten hos den externa leverantören, som en delmängd av den erbjudna tjänsten.

Tjänsten i sin helhet kan också åtnjuta en högre tillgänglighet i termer av redundans än om t.ex. en myndighet själv hade stått för driften, alternativt om leveransen sker från dedikerade servrar. Tillgänglighet i dessa termer behandlas vidare under rubrik 4.6 Förbättrad säkerhet.

I Pensionsmyndighetens enkät över molntjänster och dess användning i statliga myndigheter kommer tillgänglighet fram som en relativt viktig faktor. Cirka 23 procent av de svarande på denna fråga (87 av 148) uppgav ökad tillgänglighet som ett skäl för användning av molntjänster generellt. För SaaS-tjänster specifikt var det ett skäl som angavs av 43 procent av de svarande (96 svar av 148). För PaaS-tjänster respektive IaaS-tjänster, som inte är lika utbrett bland myndigheterna, var ökad tillgänglighet ett skäl som angavs av hela 62 procent respektive 45 procent av de svarande (21 respektive 29 svar).

4.4 Flexibilitet och skalbarhet

En mycket central del i konceptet med molntjänster är att leverantören erbjuder användaren möjlighet till snabb skalbarhet och flexibilitet över tid. Inte minst när man talar om infrastrukturella molntjänster och plattformstjänster så är detta ofta en central nytta som användaren eftersöker.

Skalbarheten i molntjänster gör det möjligt för kunden att öka respektive minska mängden köpt datakraft beroende på skiftande efterfrågan över olika tidpunkter på året eller olika år, och en möjlighet att automatiskt skala upp eller ner vid oväntade händelser. De mängder av data som ska hanteras i en myndighet varierar ofta över tid.

Exempel på ”högsäsong” kan vara perioden med utskick av Pensionsmyndighetens orange kuvert under vårvintern, eller Skatteverkets hantering av deklarationer lite senare på året. En extrem variant skulle Valmyndigheten kunna stå för, eftersom det vanligen går flera år mellan valen i Sverige och i EU.

Flexibiliteten 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 de ekonomiska resurser man sparar kan användas till andra värdehöjande aktiviteter.

Flexibilitet och skalbarhet är nära förknippat med kostnadseffektivitet och hur stora volymer som konsumeras. Men molntjänsten erbjuder ofta också flexibilitet i termer av att köparen kan anpassa vilka moduler eller funktioner som man vill köpa över tid, till exempel i en SaaS-tjänst, utifrån vilka värden som man vill åstadkomma vid varje tillfälle. Ändringar i verksamhetens innehåll eller omfattning och i vilka tjänster som erbjuds kunderna över tid, kan medföra att man köper tjänster av olika funktionell omfattning.

Det är värt att notera att myndigheter i allt större utsträckning kommer att behöva anpassa sig till att både kunder och anställda kommer att kräva att kunna ta del av sådana funktioner som man är van vid att använda i andra miljöer, till exempel på sin fritid. Det finns också en stark trend av ”bring your own device”, dvs. att man vill kunna arbeta och komma åt information från eget valbar tekniskt hjälpmedel såsom dator, läsplatta eller telefon. Detta är en trend som kan påverka offentlig sektor som arbetsgivare inte minst när nästa generation kommer ut i arbetslivet.

En aspekt av flexibilitet och skalbarhet som ibland nämns, är risken att molntjänstkunder ”överkonsumerar” molntjänster. Eftersom det är lätt att öka kapacitet och volymer, kan det hända att en verksamhet snabbt ökar sina inköp vid behov, men att bristande kontroll därefter uppstår som gör att verksamheter inte skalar ner efter att behovet minskat igen. Detta understryker vikten av att it-avdelningen måste ha full kontroll över vilka tjänster som köps och hur stora volymer som köps, även om köpet görs direkt från verksamheten. Att kunna följa verksamhetens nyttjandegrad i en molntjänst via t.ex. web-paneler eller inbyggda rapporttjänster ger bra möjligheter till kontroll.

Flexibilitet respektive skalbarhet ansågs av de svarande i Pensionsmyndighetens enkät till myndigheterna ofta ha stor betydelse. 87 av de 148 svarande responderade på denna fråga i generella termer. Av dessa angav 49 procent ökad flexibilitet och 39 procent ökad skalbarhet som skäl för nyttjande av molntjänster, vilket gör att de var

bland de nyttor som hölls allra främst. För SaaS-tjänster angav 50 procent ökad flexibilitet och 25 procent ökad skalbarhet som motiv (96 svar). För PaaS-tjänster var samma siffror 48 respektive 62 procent (21 svar) och för IaaS-tjänster 62 respektive 45 procent (29 svar).

4.5 Kostnadseffektivitet

De flesta aktörer, privata som offentliga, strävar mot molntjänster med ett medvetet mål: att spara pengar jämfört att utveckla och förvalta lokala lösningar (vanligt förekommande vid användning av IaaS- och PaaS-tjänster). Som alternativ ambition vill man inte behöva betala mer när man får fler funktioner och nya värden adderas till verksamheten (mer vanligt förekommande vid t.ex. SaaS-tjänster).

Den finansiella påverkan som molntjänster har på en organisation utgår från ett av två perspektiv: antingen det organisationen *inte* behöver göra, som att bygga en ny datahall eller underhålla viss specialistkompetens, eller å andra sidan vad organisationen *kan* göra, som att köpa volymer efter aktuellt behov.

Besparingarna kan vara både direkta och indirekta. Direkta besparingar realiseras när organisationen reducerar sina faktiska kostnader. Indirekta besparingar realiseras t.ex. genom att organisationen kan öka fokus på kärnverksamheten istället för på sin it-miljö, så som vi har beskrivit under tidigare rubriker.

Molntjänster, precis som den traditionella outsourcingen av it som redan förekommer brett, tenderar att ändra verksamheters balans- och resultaträkningar. Inträdeskostnaden är vanligen låg. När kostsamma grundinvesteringar i teknisk infrastruktur och plattformar kan undvikas övergår kostnaden från investering (capex) till driftskostnad (opex). Att gå från capex till opex ger en konsumtionsbaserad inriktning på it-användningen, istället för att avbetalning av it-strukturen sker över tid, och där det i det senare fallet finns en risk för att organisationen sitter fast i föråldrad och kostsam it-infrastuktur under tiden. Skiftet mot operationella kostnader baserade på användning kan också medföra att balansen var i organisationen som it-kostnaderna uppkommer ändras, beroende på aktuell modell för fördelning av myndighetens utgifter.

Var, mer exakt, sker då besparingarna? En grundläggande källa till besparingen utgör principen att betala för nyttjande, dvs. efter volym eller antal användare. Finns det variation i efterfrågan finns det också en möjlighet att utnyttja denna differens för kostnadseffektivisering.

Med en ny infrastrukturell lösning kan data flyttas till servrar som molnleverantörer tillhandahåller med större kostnadseffektivitet, så att egna servrar kan omdirigeras alternativt avvecklas. Vid minskning av antalet servrar kan även antalet datorhallar reduceras. Det medför lägre kostnader för strömförsörjning, kylning, hyra etc.

Molntjänstbaserade lösningar minskar också vanligen kostnaderna för att uppgradera och underhålla mjuk- och hårdvara. I en externt levererad molntjänst ingår dessa som en dold serviceavgift där leverantören av lösningen centralt hanterar uppgraderingar och underhåll. Detta innebär också att organisationen inte behöver tillhandahålla egen arbetskraft i form av sådan it-kompetens som molntjänsten kräver för sin drift.

När man flyttar data till molntjänsten, står molnleverantören för operationella insatser för teknisk säkerhet och informationssäkerhet, utifrån vad som är överenskommet i ingångna avtal. Således följer kostnadsposter för t.ex. säkerhetskopiering och

katastrofsäkring med. Följaktligen behöver inte en användare av molntjänster köpa, installera eller konfigurera hårdvara själv. Konsekvensen av detta blir en trolig avlastning i säkerhetsrelaterade kostnader för arbetskraft och kompetens samt mjuk- och hårdvara.

Andra potentiella finansiella fördelar med molntjänster visavi internt eller externt tillhandahållna tjänster kan vara att kostnaden för anslutning är låg, liksom kostnader för att genomföra förändringar och kostnaden för att avveckla tjänsten (den senare är dock beroende av tjänstens pris för att ta hem data). Eftersom molntjänster av princip innebär att kunden betalar för det kunden använder, kan bättre kostnads- eller pristransparens uppstå. Detta kan dock slå åt två håll: kanske kommer organisationen upptäcka kostnader förknippade med it som tidigare har varit dolda.

Förutom de operationella kostnaderna bör myndigheter alltså beakta andra finansiella aspekter och, vid jämförelse med alternativen till en molntjänst, se till total cost of ownership (TCO).[12]

4.5.1 Förutsättningar för kostnadseffektivisering

Även om skalfördelar i de flesta fall gör tjänsterna relativt sett billigare, reducerar molntjänster inte alltid kostnaderna. Framför allt kan uteblivna kostnadsfördelar bero på att vissa it-tjänster är unika för verksamheten och inte på enkelt sätt kan tillhandahållas genom en standardiserad tjänst som ”commodity”. För att standardiserade, paketerade tjänster ska vara mer kostnadseffektivt för en myndighet krävs ett tillräckligt mått av standardisering och virtualisering i it-miljön, samt att det inte finns många inbyggda beroenden till andra system (integrationer).

Kapacitetskostnader förknippade med att hålla infrastrukturtjänster minskar generellt, både för de organisationer som använder molntjänster och för organisationer som väljer att ha sina data ”on premises”. Lagring blir t.ex. billigare och billigare. Samtidigt är det alltså inte möjligt, med bibehållen kostnadseffektivitet, att gå över till molntjänster med mindre än att it-miljön är förberedd för det. Exempel på förberedelser som behövs för att kunna hämta hem de potentiella kostnadsfördelarna är att man som köpare har konsoliderat it, virtualiserat sina servrar samt standardiserat och automatiserat på ett medvetet sätt.

När myndigheten gör sin kostnadsberäkning, måste samtliga kostnader som ändras räknas med. Kostnader för avveckling eller flytt behöver räknas in, liksom andra omställningskostnader eller kostnader för teknisk anpassning som krävs inför övergången.

Ytterligare en kostnadsaspekt att ta hänsyn till i kalkylen är huruvida tjänsten verkligen är kostnadsneutral i förhållande till behov av uppskalning såväl som nedskalning eller att lägga ut respektive hämta hem data. Dagens molntjänster erbjuder gärna mer eller mindre gratis uppladdning, men när samma data ska laddas ner eller hämtas hem kan det vara betydligt dyrare. Det påverkar kostnaderna både löpande (särskilt om nedladdning behöver göras ofta) och även vid avslut. Inte sällan kan den typen av kostnad vara okänd för köparen.

[12] The Financial Case for Moving to the Cloud s.1ff, Gartner (2015)

Ytterligare en kostnad som är värd att nämna är kostnad för telefonsupport och anpassad support. För en molntjänstleverantör med en brett spridd publik tjänst finns hos den generella supporten en svag vilja att djupdyka i en enskild kunds specifika frågor. Ska man därför ha samma supporttider och kunna gå på djupet, möjligen också med krav att det ska ske på det egna språket, behöver man kanske dessutom köpa till extra support. Kostnadskalkylen måste även ta hänsyn till detta.

På ett högre plan är möjligheten till kostnadseffektivitet beroende av hur väl tjänsten styrs, samt att myndigheten har en god finansiell styrning och bra processer för att följa användningen. Myndigheten behöver arbeta med prognoser och löpande uppföljning av konsumtionen av molntjänster för att säkerställa att skalbarheten utnyttjas på bästa sätt, så att man undviker överköp och outnyttjad kapacitet.[13]

Kraven på säkerhet och graden av tillit till molntjänstleverantören påverkar också kostnadsbilden. Ju mer av lokala säkerhetskrav, krav på lagring eller backup etc, desto mindre blir följaktligen skalfördelarna.

4.5.2 Ekonomisk potential i molntjänster

En intressant fråga är hur stor besparingspotential molntjänster potentiellt erbjuder den statliga sektorn. Som genomgången ovan pekar på, är svaret beroende av vilken typ av verksamhet, vilken tjänst, vilket sätt att tillhandahålla tjänsten osv. som är aktuellt i det enskilda fallet. Vi försöker oss dock nedan på ett resonemang. Som utgångspunkt utgår vi från hur stora de (kända) kostnaderna för it i staten är idag.

Ett flertal initiativ har tagits för att beräkna de totala it-kostnaderna i staten. Under 2014 och 2015 har Ekonomistyrningsverket, ESV, bland annat fått i uppdrag av regeringen att utveckla en modell för att beräkna myndigheternas it-kostnader. Uppdragen har ESV utfört med stöd av en arbetsgrupp med representanter från statliga myndigheter och resultaten har presenterats bland annat i rapporterna *It-kostnads-modell – Ett första steg mot ett gemensamt språk* (ESV 2014:50) och *Fördjupat it-kostnadsuppdrag – Delrapport 2: Kartläggning av it-kostnader* (ESV 2015:58).

Inom ramen för uppdragen ovan har it-kostnader definierats enligt följande: ”it-kostnader är de kostnader som kan härledas till it-funktioner, och begränsas inte nödvändigtvis till it-organisationen. Kostnaderna består av kostnader inkl. avskrivningar (för materiella och immateriella it-investeringar) för drift, förvaltning och utveckling av it-system och utrustning.[14] De totala it-kostnaderna i staten uppskattas uppgå till 24-30 miljarder kronor per år. Detta motsvarar ungefär nio procent av de totala verksamhetskostnaderna.[15] Inom ramen för ESV:s uppdrag ovan har de deltagande myndigheterna fått ange hur stor del av it-verksamheten som outsourcats. 14 procent av it-verksamheten har outsourcats hos de deltagande myndigheterna.[16] Följaktligen är det fortarande en stor andel av it som hanteras internt.

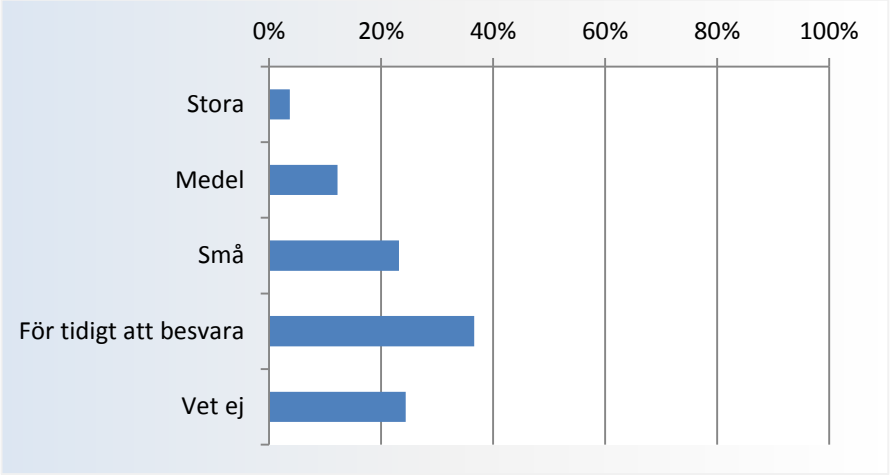
Går det då att göra några antagen om hur stor andel av de totalt 24-30 miljarder kronor som årligen skulle kunna sparas vid användning av molntjänster? Innan vi ger oss in på att säga något om detta vill vi framhålla att övningen som sådan är riskabel, då det finns ett stort antal källor till osäkerhet förknippade med en sådan estimering.

---

[13] How to Budget, Track and Reduce Public Cloud Spending s.12ff, Gartner (2015)
[14] It-kostnadsmodell - Ett första steg mot ett gemensamt språk (ESV 2014:50), s. 17
[15] Fördjupat it-kostnadsuppdrag – Delrapport 2: Kartläggning av it-kostnader (ESV 2015:58), s. 35
[16] Fördjupat it-kostnadsuppdrag – Delrapport 2: Kartläggning av it-kostnader (ESV 2015:58), s. 52

I EU:s strategi för främjande av molntjänster citeras siffror från en enkätundersökning som företaget IDC genomförde 2011 och som publicerades 2012.[17] Där tillfrågades 479 företag om ekonomisk nytta av molntjänster. 81 procent av företagen, dvs. fyra av fem, rapporterade om en kostnadsreduktion om 10-20 procent. 13 procent av företagen, dvs. lite drygt en av tio, rapporterade om kostnadsbesparingar över 30 procent. Undersökningen har några år på nacken och frågan är hur den står sig mot dagens tjänster och erfarenheter.

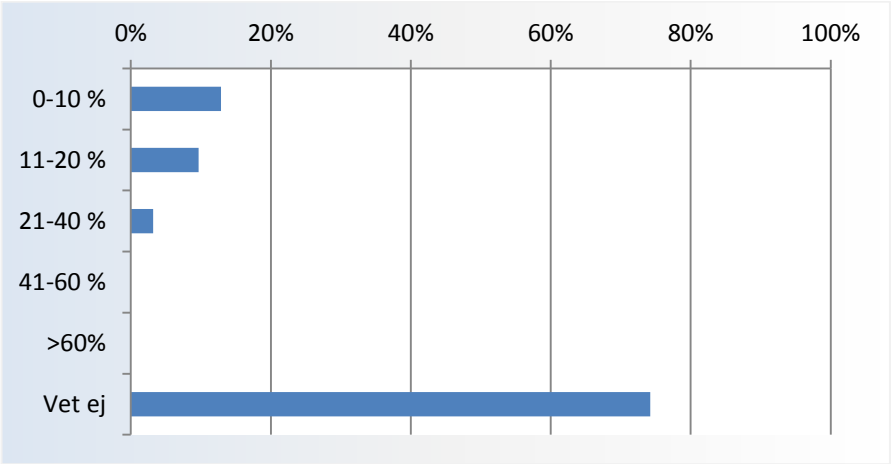
Hur ställer sig då dessa företags förväntade besparingar i relation till förväntade besparingar i offentlig sektor? Pensionsmyndighetens enkät till svenska myndigheter avseende myndigheternas användning av molntjänster pekar på att de förväntade besparingarna av de molntjänster man avser att upphandla inom de närmaste två åren är okänd, alternativt liten. Mörkertalet över antalet osäkra myndigheter kan väntas vara stort då endast 80 av 148 myndigheter har valt att besvara frågan om förväntade besparingar, trots att enkäten var anonym.



Tabell 1 Förväntade ekonomiska besparingar vid köp av molntjänster de närmaste två åren

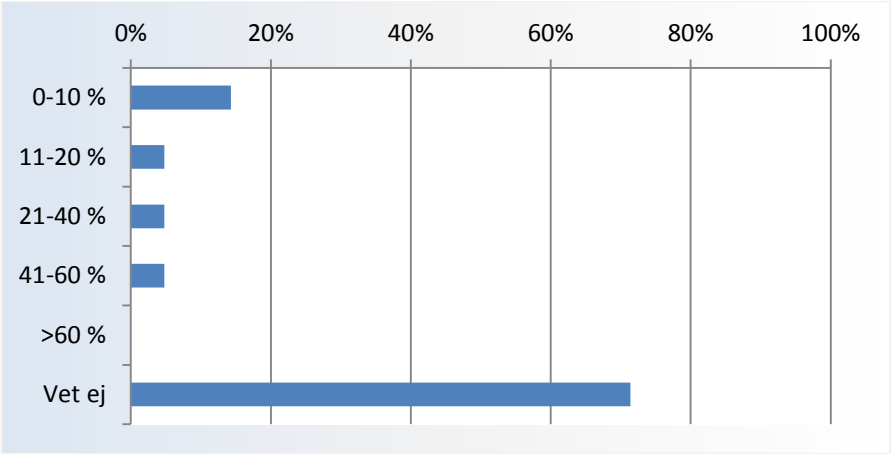
Även när vi frågade om aktuella kostnadsbesparingar vid hittillsvarande köp av molntjänster var bilden långt ifrån entydig. Bara en mindre andel av de tillfrågade svarade på fråga om kostnadsbesparing av IaaS-tjänster. Bland dem som svarade var det en övervägande andel som uppgav att kostnadsbesparingen var förhållandevis liten. För infrastruktur-tjänster svarade merparten, tre av fyra, att man inte kunde uppskatta kostnadseffekter. Vanligaste svaret var annars att kostnadsbesparingar om 0-10 procent respektive 11-20 procent hade uppnåtts.

[17] Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Take-up, IDC (2012)

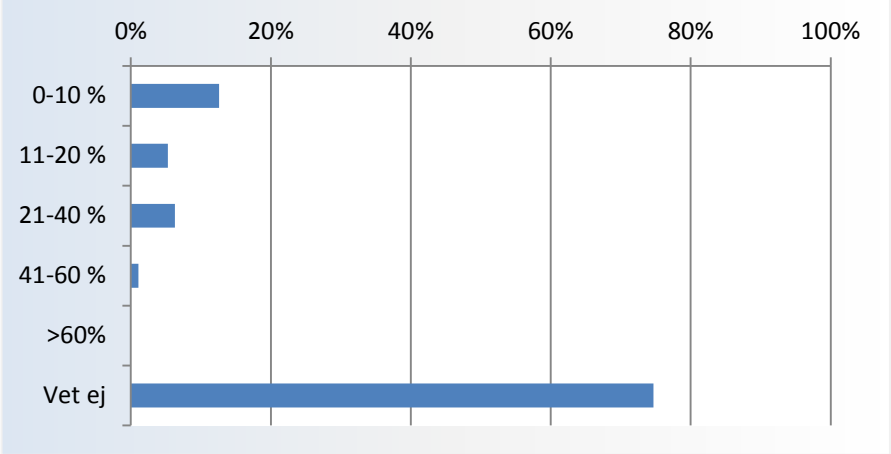


Tabell 2 Uppnådda ekonomiska besparingar av införda IaaS-tjänster

För svar på samma fråga om plattformstjänster och mjukvarutjänster framkom en liknande bild. Flertalet svarande som uppgav att de visste besparingens omfattning uppgav en liten total besparing, 0-10 procent. Några få svarade dock att man uppnått mycket stora besparingar, 41-60 procent, på de olika tjänsteformerna i sin helhet.



Tabell 3 Uppnådda ekonomiska besparingar av införda PaaS-tjänster



Tabell 4 Uppnådda ekonomiska besparingar av införda SaaS-tjänster

Även analysföretaget Gartner, som under många år har räknat på kostnader kring it-tjänster, uppger att bilden av kostnadseffekter varierar och att det är svårt att ge några generella spann för kostnadseffekter av att övergå till molntjänster för olika typer av molntjänster i verksamheter av olika storlekar. I Gartners egna undersökningar varierar möjligheterna till kostnadsbesparingar mellan någon halv procent och uppemot 40 procent.[18] Snarare lyfter Gartner, liksom de leverantörer som vi har pratat med, att kostnadseffekter finns och förväntas av de flesta som går över till molntjänster, men att det framför allt är andra nyttor, såsom innovativitet och snabbhet, som är primär drivkraft för övergång till molntjänster i många verksamheter idag. Ytterligare en aspekt som påverkar kostnadseffekten är vilken typ av molntjänst som nyttjas eller skapas. Privata moln ger således över lag mindre kostnadsfördelar än publika molntjänster där tjänsten och dess infrastruktur m.m. delas av fler.

Samtidigt står it-kostnader för en relativt stor andel av statens totala utgifter varför även mindre kostnadseffekter per myndighet kan ge en kännbar årlig effekt i statskassan. Enkelt räknat på en snittbesparing om 10 procent av de samlade it-kostnaderna enligt ESV:s beräkningar av statens kostnader för it får vi en potentiell besparing om 2,4-3 miljarder kronor årligen jämfört med om myndigheten har kvar en egen it-miljö och producerar sina egna it-tjänster. Dock är det inte sannolikt, inte heller önskvärt ur t.ex. säkerhetssynvinkel, att hela myndigheternas it köps som molntjänster ens på sikt. Därför förutser vi inte heller en så stor potentiell effekt på samhällsnivå. Även om vi antar att den faktiska it-kostnaden i staten skulle ligga högt i ESV:s angivna intervall, dvs. kring 30 miljarder kronor årligen, tror vi ändå att det är mer rimligt att på fem till tio års sikt anta potentiella besparingar i storleksordningen en till två miljarder årligen[19]. Är den faktiska nivån för statens it-kostnader lägre än 30 miljarder drar det givetvis också ner den nominella potentialen. Besparingar i den storleksordningen torde uppstå först vid en bred användning av molntjänster i staten, med femtio procent av it-produktionen eller mer levererad som molntjänster, vilket är ett läge som kommer att ta tid att nå även om myndigheternas intresse för molntjänster är stort. En långsiktig besparingspotential i den storleksordning som nämns ovan förutsätter även att svenska myndigheter gör kostnadseffektiva och väl avvägda upphandlingar i god konkurrens.

Myndigheternas svar visar att de upplever sig vara osäkra på kostnadseffekter för den egna myndigheten av molntjänster. Som en del av beslutsunderlaget vid bedömning av om en del av it-verksamheten ska läggas i en molntjänst bör alltid en lönsamhetskalkyl med förväntade effekter upprättas. Som en del av nyttohemtagningsprocessen bör en uppföljning av realiserade effekter och nyttor göras. Endast 17 procent av de deltagande myndigheterna i ESV:s uppdrag ovan anger att de har en beslutad modell för nyttohemtagning som efterlevs.[20] Förutsättningarna för att följa upp finansiella

---

[18] How to Calculate the Total Cost of Cloud Storage, Gartner Inc, (40% kostnadsbesparing), Gartner (2013) samt Government CIOs See Expected Cloud Cost Savings Evaporates s. 8-9 (0,5% kostnadsbesparing) Gartner (2015)

[19] I estimeringen tar vi inte hänsyn till eventuella transitionskostnader. I detta sammanhang tar vi inte heller hänsyn till de indirekt förekommande värden för medborgare och företag som uppstår då dessa kan ta del av bättre publika molnbaserade tjänster. Sådana tillkommande värden torde i sig också kunna stå för relativt avsevärda belopp, räknat på hela ekonomin, när individer och företag lägger mindre tid på att söka information eller när offentliga insatser blir mer transparenta och träffsäkra i förhållande till myndigheternas uppdrag.

[20] Fördjupat it-kostnadsuppdrag – Delrapport 2: Kartläggning av it-kostnader (ESV 2015:58), s. 24

effekter av införande av molntjänster är således låg, vilket också styrks av svaren i Pensionsmyndighetens enkät.

4.6 Förbättrad säkerhet

Alla verksamheter i offentlig sektor har att beakta krav på it-säkerhet och informationssäkerhet. Säkerhetsfrågor har fått stor uppmärksamhet och är flitigt belyst inom förvaltningen under senare år. Med it-säkerhet avses teknisk säkerhet, vilket i sin tur är en delmängd av informationssäkerhet. Skyddet av information innefattar krav på konfidentialitet, riktighet, tillgänglighet och spårbarhet.

Även om användning av molntjänster innebär säkerhetsmässiga utmaningar som måste hanteras av den offentliga aktören vid en upphandling kan säkerheten också påverkas positivt av de skalfördelar som förknippas med molntjänster. Så kan t.ex. säkerhetsrelaterade fördelar finnas i större och väl etablerade molntjänster där stora resurser satsas på säkerhetsrelaterade åtgärder, eller i tjänster där leverantören ser säkerhet som en central del i erbjudandet. Varje molntjänst måste dock bedömas fristående med avseende på såväl nyttor som risker. I analysen bör säkerhetsrelaterade nyttor såväl som risker inkluderas, med utgångspunkt i den egna verksamhetens krav och behov.

Säkerhetsmässiga fördelar eller nyttor kan t.ex. uppnås om molntjänstleverantören har effektiva och uppdaterade säkerhetslösningar och säkerhetslösningarna i och bakom den erbjudna tjänsten över tid kan hållas på en nivå som inte den enskilda organisationen själv klarar att åstadkomma. För att det ska innebära en säkerhetsmässig fördel krävs att företaget som tillhandahåller tjänsten också har bra rutiner för säkerhet samt god kontroll över efterlevnaden av dessa rutiner. Detta verkar positivt på den tekniska säkerheten (it-säkerheten) och kan även vara positivt för möjligheten att upprätthålla myndighetens behov av konfidentialitet.

När molntjänsten är en del av leverantörens kärnverksamhet är riskerna allvarliga för leverantören om denne *inte* satsar stora resurser på säkerhetsområdet, och de affärsmässiga konsekvenserna för leverantören blir långtgående om leverantören inte har god kontroll över hotbilden och hur riskerna förändras över tid samt har förmåga att ständigt möta dem. Att ligga i framkant inom säkerhetsområdet kan vara en direkt nödvändighet ur en stor leverantörs perspektiv.

Hög säkerhet utgör samtidigt en kostnad. Ju mindre en myndighet är, desto större relativ nytta kan ofta fås av att använda en publik eller annan molntjänst som alternativ till egen drift och eget tillhandahavande av de önskade funktionerna. Säkerhetsrelaterade nyttor eller fördelar är dock inte något som kan tas för givet, utan måste alltid säkerställas vid upphandlingen av tjänsten. När tjänsten väl är i bruk ska tjänsteleverantören garantera efterlevnad i förhållande till kravställan och avtal. Som myndighet och molntjänstkunden har man fortsatt ansvar för att följa upp leveransen.

Ytterligare en potentiell säkerhetsrelaterad nytta med molntjänster avser tillgängligheten och är kopplad till redundans i tjänsten. När leverantören kan styra om leveransen mellan olika fysiska leveransställen minskar risken för avbrott i tjänsten. Förbättrad tillgänglighet innebär en nytta både för den offentliga aktör som använder tjänsten, men också för dess kunder, dvs. för de individer eller företag som har kontakt med en myndighet eller annan offentlig aktör.

4.7 Minskat behov av egen it-kompetens

It-tjänster blir alltmer avancerade och specialiserade. Kostnaden för att utveckla och underhålla it-tjänster tar allt större del av myndigheters budget, ju större del av verksamheten som digitaliseras och automatiseras. Många myndigheter upplever idag att det är svårt att attrahera och behålla spetskompetens för utveckling och förvaltning. Har myndigheten liten användning av ett visst system eller en viss plattform, kan det också vara problematiskt att upprätthålla kompetensnivån över tid.

Har myndigheten höga ambitioner kring innovativiteten i tjänsterna, krävs mycket av såväl medarbetare som chefer.

Minskat behov av egen it-kompetens är ett av de skäl som oftast angavs för de myndigheter som valt molntjänster. 87 av 148 svarade på frågan generellt och av dessa uppgav drygt en tredjedel att minskat behov av egen it-personal var ett motiv för molntjänster. För SaaS-tjänsterna var det hela 52 procent som angav kompetens som ett skäl, för PaaS-tjänster (21 svarande) 33 procent och för de infrastrukturella tjänsterna angav 48 procent av de 29 svarande ett minskat behov av egen it-kompetens som skäl.

Idag tillämpas inte verksamhetsövergång vid köp av publika molntjänster. Det betyder att såväl omställning som avvecklingsplaner för personal kan behövas, då arbetsuppgifter försvinner.

4.8 Förvaltningsgemensam utveckling

Som appliceringen av molntjänster på politiska strategiska mål visade kan användning av molntjänster ha flera positiva effekter på offentliga verksamheter. I grunden är det samma typ av positiva effekter som såväl ett företag som en myndighet kan uppnå genom god användning av molntjänster, såsom skalbarhet, innovativitet, och kostnadseffektivitet. Till detta kan för förvaltningens del läggas ytterligare en aspekt eller nytta, förvaltningsgemensam it och utvecklingen av förvaltningsgemensamma tjänster, vilka blir enklare med användning av molntjänster.

För myndigheter med vana att agera självständigt och med en vilja att kunna kontrollera sin egen verksamhet kan det upplevas problematiskt om en utpekad myndighet ska utveckla och tillhandahålla en tjänst för flera andra myndigheter. Molntjänster öppnar för möjligheten för två eller flera myndigheter att utveckla en gemensam e-tjänst med hjälp av en tredje part. Myndigheterna kan välja att sköta både det aktuella utvecklingsarbetet och testarbetet i en miljö hos en tredje part, och att även driva tjänsten vidare med hjälp av en extern molntjänstleverantör. Eftersom molntjänster är lätta att komma igång med kan man med förhållandevis liten ansträngning testa kund- och användarnyttan i den nya tjänsten.

Andra tänkbara nyttor som kan uppstå i gränssnittet mellan olika myndigheter vid användning av molntjänster är att en större infrastrukturkapacitet kan säkras, att myndigheterna kan utnyttja att de har kapacitetstoppar i verksamheten vid olika tillfällen, att tillgängligheten för kund kan öka genom bättre redundans, eller att priser pressas vid köp av större volymer.

Molntjänster som koncept kan alltså medföra att man sänker tröskeln för att samverka kring it-drift och e-tjänster, vilket i sin tur kan gynna både förekomst och kvalitet i både tjänster mot kund och tjänster för förvaltningen själv.

Statens inköpscentral vid Kammarkollegiet erbjuder sedan 2013 möjlighet för enskilda myndigheter att avropa molntjänster.[21] I de fyra nya ramavtalen ”Programvaror och tjänster" kan varje ramavtalsleverantör själv välja hur den efterfrågade tjänsten ska levereras utifrån myndighetens kravspecifikation i avropsunderlaget. Om kraven uppfylls kan myndigheten erhålla en molntjänst. Inget hinder finns i dagens avtal för att flera myndigheter skulle kunna gå ihop och upphandla från de aktuella avtalen.

Ytterligare ett sätt på vilket myndigheter kan samverka kring molntjänster är om en tjänst tillhandahålls centralt för alla myndigheter och myndigheterna kan ansluta sig utan eget avrop eller upphandling. Sådana typer av statliga molntjänstsatsningar, s.k. ”government cloud solutions” finns i flera andra länder. Några sådana beskriver vi i bilaga 2 till denna rapport. Det som kallas myndighetsmoln kan i praktiken vara flera olika myndighetsmoln och tjänster, inom olika områden och då kanske även med olika säkerhetskrav och säkerhetsnivåer.

Exempel på tjänster som används brett i statlig sektor och som potentiellt skulle kunna erbjudas som statliga molntjänster är t.ex (inom IaaS och PaaS): servertjänster (Windows och Linux), lagring (potentiellt även krypterad lagring), backup, antvirusstöd, interna brandväggar, webåtkomst, stöd för identitetsfederationer i enlighet med E-legitimationsnämndens arkitektur, bussteknik och stöd för microtjänster med API:er. Även nättjänster; likt Swedish Government Secure Intranet (SGSI) och Sjunet, skulle kunna erbjudas.[22]

SaaS-tjänster som har bred användning, och som eventuellt skulle kunna erbjudas i statligt moln för offentlig sektor är e-post, projektytor, kompetenssystem, utbildningssystem, planeringssystem, ”Min ärendeöversikt”, ”Min profil”, bokningssystem, e-arkiv, enkätfunktioner och digitala tolktjänster.

Ett krav på gemensamma statliga molntjänster bör vara att man ska kunna uppnå samma typ av nyttor som med molntjänster som handlas upp separat på en marknad; såsom snabbhet, skalbarhet, flexibilitet, tillgänglighet och kostnadseffektivitet. Det är eftersträvansvärt att bygga tjänster på öppen källkod eftersom det ökar nyttan i den offentliga investeringen då koden är återanvändbar. Säkerhetsnivån bör vara generellt hög i myndighetslösningar, men kan också vara skiktad i olika valbara nivåer.

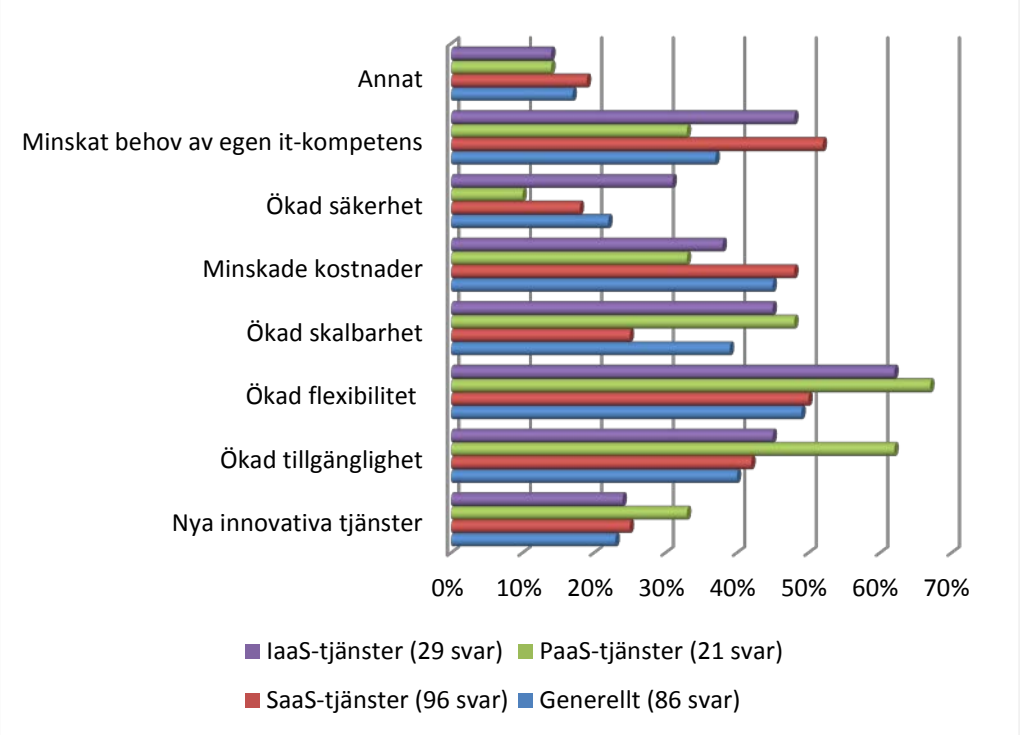
4.9 Vilka nyttor väger tyngst?

Det är viktigt att framhålla att bara den enskilda myndigheten, eller myndigheter i samverkan, kan avgöra vilka skäl som skulle kunna vara avgörande för att satsa på en molntjänst. Det finns dock en tydlig trend i såväl offentlig som privat sektor att kostnadsfördelar ensamma sällan utgör grundval för övergång till en molntjänst.

[21] Se www.avropa.se

[22] SGSI är ett intranät, skiljt från internet, för säker och krypterad kommunikation mellan myndigheter i Sverige och i Europa. Nätet är utformat för att klara höga krav på tillgänglighet och driftsäkerhet. SGSI får bara användas av myndigheter som uppfyller höga krav på IT-säkerhet. I Sverige använder myndigheter SGSI som ett säkert nätverk för utbyte av känslig information och minskar därmed IT-säkerhetsrisker. Sjunet är ett kvalitetssäkrat kommunikationsnät framtaget och anpassat för vård och omsorg. Sjunet har en garanterad tillgänglighet och ställs ofta som krav för att sprida verksamhetskritisk information.

Vår enkätundersökning och kunskapsinhämtning från leverantörer och analysföretag visar att kostnadsaspekter inte längre alltid är det enda, och kanske inte heller alltid det främsta, argumentet för att övergå till att använda en molntjänst. Bilden är härvidlag densamma i både privat och offentlig sektor. Både flexibilitet, skalbarhet och innovativitet hamnar idag långt upp på listan över motiv för molntjänster i privat sektor, tillsammans med ett motiv som har visat sig starkt inte minst för statliga myndigheter, vilket är att minska behovet av egna it-kompetenser. Det kan vara så, att offentlig sektor möter en större utmaning än privata företag, när det gäller att kunna attrahera och behålla spetskompetens för tjänsteutveckling.



Tabell 5 Motiv för användning av molntjänster i svenska myndigheter idag (flervalsalternativ)

4.10 Var finns den största potentialen i molntjänster?

För att kunna svara på frågan i rubriken behöver man, förutom att ta i beaktande juridiska och säkerhetsrelaterade krav, gå tillbaka till varje enskild myndighet och göra en analys av respektive myndighets it-miljö och it-portfölj, titta på livscykler för plattformar och system och analysera möjligheten att på ett kostnadseffektivt sätt avskilja informationsmängder som är aktuella för hantering i en molntjänst.

Analysen kommer att ge olika resultat beroende på vilken myndighet och vilken information man omfattar. En driftstung myndighet kan mycket väl finna att den, givet att de juridiska och säkerhetsmässiga förutsättningarna för myndigheten kan mötas, kan hitta stora kostnadsfördelar med att gå över till infrastrukturtjänster. En annan myndighet som drivs av snabb utveckling av digital verksamhet, kan finna att mjukvarutjänster kan addera stort värde till verksamheten genom innovativitet och nya tjänster eller genom att ge organisationen en helt annan snabbhet i implementeringar.

Vi erfar att många myndigheter upplever att det är svårt att veta vilken information som är lämplig eller möjlig att lägga i molntjänster. När det gäller vad som passar bäst att ”lägga i molnet” kan det något förenklat sägas att molntjänster är enklare att införa:

- ju mindre känslig information det finns i ett system. Få organisationer börjar t.ex. med att köpa verksamhetens kärnsystem som molntjänster,
- ju mer självständig och utan integrationer en applikation är,
- ju mindre behovet är av just denna tjänst i relation till hur kostsam den är att bygga internt,
- ju mer specifika kompetenser den egna personalen måste ha för att kunna underhålla tjänsten,
- ju större variationerna är i behov och belastning över tid, dvs. ju mer organisationen kan tjäna på att köpa varierande kapacitet och slippa binda kapital och resurser över tid,
- ju mindre verksamheten är och ju större den relativa kostnaden därmed är för att investera i egen infrastruktur, specialistkompetens m.m. på ett område.

I kapitel 5 nedan fördjupar vi resonemanget om juridiska, säkerhetsrelaterade och praktiska förutsättningar för att kunna använda molntjänster och ta tillvara deras fulla potential.

5 Förutsättningar för användning av molntjänster i statliga verksamheter

De potentiella nyttorna av molntjänster för myndigheter och andra statliga verksamheter är alltså stora och användningen av molntjänster kan förväntas öka markant under de närmaste åren.

Samtidigt upplever många myndigheter att det finns konkreta hinder mot att tillvarata potentialen i molntjänster. Som största upplevda hinder för att använda molntjänster uppges i vår enkätundersökning säkerhetsrelaterade frågor samt oklarheter kring juridiska förutsättningar för nyttjande av molntjänster.

Svenska myndigheter efterfrågar en större klarhet i vad myndigheter kan och får använda molntjänster till, och hur man som ledningsperson, strateg, inköpare eller jurist i en offentlig verksamhet ska tänka kring dessa utmaningar. Av det skälet har vi i uppdraget valt att göra en noggrann genomgång av inte minst det rättsliga läget. I detta kapitel presenteras juridiska resonemang och slutsatser i sammandrag. Analysen finns att läsa i sin helhet i bilaga 1.

Näst efter den juridiska genomgången går vi igenom några av de största säkerhetsmässiga utmaningarna vid köp av molntjänster, och hur myndigheter kan hantera dessa. Därefter görs en genomgång av säkerhetsaspekter på en nationell nivå.

Slutligen i detta kapitel går vi igenom vissa praktiska förutsättningar som behöver övervägas om statliga verksamheter ska kunna använda molntjänster på ett sätt som gör att potentiella fördelar, inklusive positiva kostnadseffekter, kan uppnås.

5.1 Juridiska förutsättningar för nyttjande av molntjänster

Sammanfattning

För att kontrollera om det är förenligt med gällande rätt för en myndighet att hantera sin information i molnet måste myndigheten göra en s.k. laglighetskontroll. Det regelverk som myndigheten har att beakta är omfattande och kan bl.a. inkludera offentlighets- och sekretesslagen, personuppgiftslagen och arkivlagen. För att myndigheten ska kunna göra tillförlitliga juridiska bedömningar måste myndigheten ha kännedom om vem eller vilka leverantörer som kommer att hantera informationen, hur den kommer att hanteras och var informationen kommer att lagras geografiskt.

I detta avsnitt redogörs kortfattat för de juridiska förutsättningar som ska vara uppfyllda för att en myndighet ska kunna hantera sin information i en molntjänst. Redogörelsen är på inget sätt uttömmande utan en myndighet måste i varje enskilt fall ta ställning till vilka lagar och regler som är tillämpliga för att få en komplett juridisk bild i förhållande till den tänkta molntjänsten. Den fullständiga juridiska analysen återfinns i bilaga 1.

5.1.1 Klockan är 15.00, vet du var dina data är?

Den som hanterar sin information i molnet förlorar som regel den absoluta kontrollen över informationen. Molnet kännetecknas av att informationen flödar över nationsgränserna på ett sätt som är omöjligt för en molnkund att överblicka och än mindre kontrollera. Informationen kan finnas på ett datacenter i Europa på förmiddagen och på andra sidan jordklotet vid midnatt. Ett beslut att hantera sin information i molnet fattas trots det ibland utan större betänkligheter t.ex. när molnkunden i en snabb avvägning bedömer att fördelarna med att använda en molntjänst väger tyngre än riskerna i förhållande till informationens känslighet. Vanligen påverkas kundens beslut av om molntjänstleverantören är en välkänd aktör med ett gott säkerhetsmässigt rykte. Oavsett vilken typ av information som en kund tänker hantera i molnet är det dock osannolikt att han eller hon skulle besluta att använda en molntjänst om risken är stor att informationen hamnar i orätta händer eller avsiktligen ändras eller raderas. För att man ska kunna avgöra om det är tillåtet enligt lag att hantera viss information i molnet måste man veta vem eller vilka som hanterar informationen, hur informationen hanteras samt var den befinner sig geografiskt. Utan kännedom om dessa faktorer är det omöjligt att bedöma lagligheten av informationshantering i molnet.

5.1.2 Vem kan man lita på?

Ur juridisk synvinkel skiljer sig inte användningen av molntjänster från vanlig outsourcing. Det är samma lagar som aktualiseras och kunden ska göra samma typer av avvägningar och bedömningar som vid traditionell outsourcing. Det sammantagna regelverket som myndigheter har att följa är dock både omfattande och komplext vilket leder till att myndigheter ofta upplever en stor osäkerhet kring hur det ska tolkas och tillämpas. Vad som ytterligare kan komplicera bilden är att kunden i sina juridiska bedömningar måste beakta andra, ibland ovissa, omständigheter jämfört med vanlig outsourcing. Kunden kan inte räkna med att kunna diktera avtalsvillkoren eller att informationen kommer att hanteras inom Sveriges gränser eller ens inom Europa. Kunden måste beakta att informationen kan komma att hanteras av molntjänstleverantörens underleverantörer och att informationen, om den hanteras utanför Sveriges gränser, kommer att exponeras för andra länders rättsordningar.

Vid inköp av en publik molntjänst är det vanligt att kunden inte har någon personlig kontakt med molntjänstleverantören utan kontrakt ingås över internet eller via en molntjänstpartner. För att kunden ska få en uppfattning om hur, var och av vem dennes data kommer att hanteras krävs att kunden noga granskar molntjänstleverantörens avtal, policydokument m.m. Kunden kan emellertid inte alltid räkna med att svaren på de frågor som kunden ska ställa, står att finna i dessa dokument.

Det finns ett par faktorer som i allmänhet uppfattas som försvårande, i synnerhet vid användning av publika molntjänster. Framför allt gäller det bristande transparens i molntjänstleverantörens verksamhet och behandling av personuppgifter. Om molntjänstleverantören anlitar egna underleverantörer, som också kommer att hantera kundens information, kan det bidra ytterligare till låg transparens. En konsekvens av låg transparens är att kunden får dålig insyn i molntjänstleverantörens verksamhet och därmed får svårt att utöva nödvändig kontroll över leverantörens hantering av kundens information.

5.1.3 En myndighet är inte vilken molnkund som helst

Användning av molntjänster kan ha en tendens att grunda sig på att kunden känner förtroende för molntjänstleverantören. Kunden litar på att leverantören behandlar kundens information på ett säkert sätt, att ingen obehörig får del av informationen och att informationen alltid är tillgänglig trots att kunden inte har några, eller mycket små, möjligheter att faktiskt kontrollera hur molntjänstleverantören hanterar informationen.

En myndighet kan emellertid inte grunda ett avtalsförhållande med en molntjänstleverantör på enbart förtroende för leverantören, eftersom myndighetens informationshantering är styrd av ett stort antal lagar och regler. För att skapa ett relevant förtroendeförhållande måste myndigheten kunna verifiera de utfästelser som leverantören gör om hur denne kommer att hantera myndighetens information. Myndigheten måste grunda sin tilltro till molntjänstleverantören på förekomsten av konkreta verktyg som möjliggör för myndigheten att verifiera leverantörens utfästelser. Myndigheten måste förvissa sig om att det finns legala förutsättningar att just *den* molntjänstleverantören kan uppfylla just *de* krav som myndigheten har för att hanteringen ska vara tillåten i sin helhet. Endast under dessa förhållanden kan myndigheten få tillräcklig insyn i, och kontroll över, var dennes data är och hur och av vem den hanteras.

5.1.3.1 Laglighetskontrollera

Vilka legala krav som ställs när uppgifter från myndigheter ska hanteras i molnet beror bl.a. på vilken typ av information det är fråga om. När en myndighet ska kontrollera lagligheten av hanteringen av information i en molntjänst bör myndigheten redan ha bestämt vad som är syftet med att hantera informationen i den tänkta tjänsten och vilka funktioner myndigheten eftersträvar i tjänsten.

Laglighetskontrollen görs lämpligast som en integrerad del av myndighetens informationsklassning och riskanalys. Myndigheten behöver, utöver laglighetskontrollen, även kartlägga hur känslig informationen är ur ett individ-, verksamhets- och samhällsperspektiv för att kunna bedöma om det över huvud taget är lämpligt att hantera informationen i en molntjänst.

I laglighetskontrollen ska myndigheten beakta om uppgifterna som ska lämnas ut till molntjänstleverantören är sekretessreglerade, om det är allmänna handlingar och om informationen innehåller personuppgifter. När myndigheten vet vilken typ av information som ska hanteras måste den ta ställning till vilka regler som är tillämpliga i t.ex.

tryckfrihetsförordningen, offentlighets- och sekretesslagen, arkivlagen, personuppgiftslagen eller sin egen registerförfattning.

Mot bakgrund av det sammantagna regelverket som är tillämpligt på den planerade hanteringen ska myndigheten sammanställa och specificera de krav som molntjänstleverantören måste uppfylla för att hanteringen ska vara tillåten enligt lag. Myndighetens kravsammanställning ska återspeglas i de avtalsvillkor som upprättas mellan parterna. Att myndigheten genomför noga genomtänkta och väl förberedda upphandlingar har således avgörande betydelse för att myndigheten ska ha förutsättningar att anlita en molntjänstleverantör som kan tillgodose myndighetens krav.

5.1.3.2 Sekretesspröva och säkerhetsskydda

När myndigheten har kartlagt innehållet i informationen blir nästa steg att beakta om informationen innehåller uppgifter som är sekretessreglerade i offentlighets- och sekretesslagen (2009:400) och om informationen omfattas av säkerhetsskyddslagen (1996:627). Om säkerhetsskyddslagen är tillämplig behöver myndigheten, utöver sekretessprövningen, utreda om det är möjligt för myndigheten att uppfylla lagens krav på god informationssäkerhet, säkerhetsskyddsavtal, säkerhetsprövning av personal m.m. Det lär i synnerhet vara mycket problematiskt att teckna säkerhetsskyddsavtal med en global molntjänstleverantör och säkerhetspröva anställda som är utländska medborgare med arbetsplats utanför Sveriges gränser. I realiteten rör det sig sannolikt om ytterst få fall, där information som omfattas av säkerhetsskyddslagen, kan hanteras i en molntjänst. Att hantera information som omfattas av säkerhetsskyddslagen i en publik molntjänst bör därmed vara helt uteslutet.

Är säkerhetsskyddslagen inte tillämplig kan myndigheten lämna ut informationen till en molntjänstleverantör om informationen inte är sekretessreglerad. Är informationen sekretessreglerad ska myndigheten pröva om det är förenligt med offentlighets- och sekretesslagen att lämna ut informationen till den aktuella molntjänstleverantören eller om sekretess utgör hinder för ett utlämnande. Vid sekretessprövningen måste myndigheten uppmärksamma att prövningen inte enbart ska göras i förhållande till molntjänstleverantören utan också i förhållande till eventuella underleverantörer som anlitas av molntjänstleverantören och som kommer att hantera myndighetens information.

Under vissa förhållanden kan en avtalsreglerad tystnadsplikt medföra att informationen, utan hinder av sekretess, kan lämnas ut till molntjänstleverantören. Det gäller dock normalt inte uppgifter som t.ex. är av särskilt integritetskänsligt slag eller som har ett särskilt uttalat skyddsbehov med hänsyn till Sveriges internationella relationer eller rikets säkerhet (enligt säkerhetsskyddslagen). Myndigheten behöver också ta hänsyn till om det finns andra omständigheter som talar för att det är olämpligt att lämna ut informationen till molntjänstleverantören. En sådan omständighet kan vara att informationen exponeras för andra länders rättsordningar om den lagras utanför Sveriges gränser. Informationen blir därmed potentiellt tillgänglig för t.ex. andra länders myndigheter.

Myndigheten bör inte förlita sig på en avtalsreglerad tystnadsplikt, oavsett graden av känslighet i informationen, om molntjänstleverantören anlitar fler än någon enstaka underleverantör eller regelbundet byter underleverantörer. Myndigheten måste kunna kontrollera och följa upp att leverantörerna efterlever avtalsvillkoren. När molntjänstleverantören anlitar ett stort antal underleverantörer eller regelbundet byter under-

leverantörer, blir myndighetens möjlighet att följa upp avtalsefterlevnaden starkt begränsad. Detta gäller i synnerhet när underleverantörerna är etablerade utanför Sveriges gränser.

Uppgifter som bedöms vara sekretessbelagda i förhållande till leverantören kan inte hanteras i en molntjänst, även om tystnadsplikt kan regleras i avtal. Det förekommer emellertid diskussioner om det är möjligt att lämna ut sekretessbelagda uppgifter till externa it-leverantörer under förutsättning att uppgifterna inte röjs för leverantören.[23] Om myndigheten krypterar informationen innan den överlämnas till molntjänst-leverantören ligger det nära till hands att uppgifterna inte kan anses röjda för leverantören och att frågan om sekretess hindrar ett utlämnande, därigenom faller.[24] En förutsättning är förstås att myndigheten behåller krypteringsnyckeln och att leverantören inte har någon möjlighet att ta del av uppgifterna i läsbart format eller uppfatta de sekretessbelagda uppgifterna på annat sätt.[25] Det är givetvis en förutsättning att uppgifterna är krypteringsskyddade på samma sätt hos eventuella underleverantörer och att lämpliga avtalsvillkor upprättas mellan parterna för att förhindra att leverantören tar del av uppgifterna om en sådan möjlighet trots allt skulle uppstå. Myndigheten ska också ha tillgång till konkreta verktyg för att kunna granska leverantörens hantering och kontrollera att denne efterlever avtalsvillkoren.

5.1.3.3 Integritetssäkra

Nästa steg i myndighetens laglighetskontroll är att granska om den planerade behandlingen är förenlig med integritetsskyddslagstiftningen dvs. personuppgiftslagen (1998:204) eller den registerförfattning som myndigheten ska tillämpa.

Personuppgiftslagens reglering anses ofta vara den största utmaningen vid behandling av personuppgifter i en molntjänst. Det beror sannolikt på att personuppgiftslagen ställer höga krav på att den personuppgiftsansvariga myndigheten ska ha insyn i och kunna utöva kontroll över den behandling av personuppgifter som utförs av ett personuppgiftsbiträde i form av t.ex. en molntjänstleverantör.

Myndighetens kontroll av lagligheten enligt personuppgiftslagen ska ske i två steg. Först och främst måste myndigheten konstatera att den behandling av personuppgifter som ska utföras är tillåten för myndigheten enligt personuppgiftslagen eller aktuell registerförfattning. Därefter ska myndigheten kontrollera om det finns förutsättningar för myndigheten att uppdra åt ett personuppgiftsbiträde att utföra behandlingen. I denna granskning ska myndigheten beakta hur och var molntjänstleverantören bedriver sin verksamhet och kontrollera att leverantören kan acceptera de krav myndigheten ställer på personuppgiftsbehandlingen. Om molntjänstleverantören anlitar egna underleverantörer för att behandla myndighetens personuppgifter ska myndighetens prövning ske gentemot var och en av dessa underleverantörer.

Personuppgiftslagen hindrar inte att en molntjänstleverantör anlitar egna underleverantörer. Det är däremot ett krav att den personuppgiftsansvariga myndigheten har lämnat sitt samtycke till detta. Myndigheten måste också säkerställa att den har kännedom om samtliga underleverantörer och att det finns förutsättningar att binda underleverantörerna vid samma avtalsvillkor som tecknas med molntjänstleverantören.

---

[23] Se E-delegationens förstudie om sekretess vid outsourcing, Fi 2009:01/2015/4, 2015-03-09.
[24] Om den krypterade informationen innehåller personuppgifter är dock personuppgiftslagen alltjämt tillämplig.
[25] Det är oklart om, och i så fall i vilken omfattning, denna typ av kryptering tillhandahålls på marknaden i dagsläget.

Myndigheten ska dessutom kontrollera om personuppgifterna kommer att överföras till tredje land dvs. ett land utanför EU/EES-området. Om så är fallet ska myndigheten se till att det finns ett lagligt stöd som möjliggör en sådan överföring. I skrivande stund är det i princip endast EU-kommissionens standardavtalsklausuler som kan användas som lagligt stöd för att föra över personuppgifter till en molntjänstleverantör i tredje land.

Slutligen ska den personuppgiftsansvariga myndigheten teckna ett personuppgiftsbiträdesavtal med molntjänstleverantören.[26] I biträdesavtalet ska myndigheten ge molntjänstleverantören instruktioner om hur denne får behandla myndighetens personuppgifter och fastställa vilka säkerhetsåtgärder leverantören ska vidta för att skydda uppgifterna.

5.1.3.4 Allmänna handlingar - bevara eller gallra

Om myndigheten har konstaterat att integritetsskyddslagstiftningen inte uppställer något hinder för myndigheten att hantera sin information i en molntjänst är nästa steg i laglighetskontrollen att kontrollera om allmänna handlingar kan komma att hanteras i tjänsten. Har myndigheten inte för avsikt att hantera allmänna handlingar i tjänsten måste myndigheten uppmärksamma om leverantörens uppdrag går utöver enbart teknisk lagring eller teknisk bearbetning. Har molntjänstleverantören ett sådant uppdrag kan handlingarna komma att ändra status i tryckfrihetsförordningens mening. Handlingar som ännu inte är allmänna och som myndigheten lämnar ut till molntjänstleverantören kommer nämligen normalt att betraktas som expedierade och därmed allmänna enligt tryckfrihetsförordningen. Handlingarna kan då bli föremål för utlämnande i enlighet med tryckfrihetsförordningen.

Om själva syftet redan från början är att molntjänstleverantören ska hantera allmänna handlingar på uppdrag av myndigheten behöver myndigheten kontrollera att det finns förutsättningar att uppfylla offentlighets- och sekretesslagens krav på en god offentlighetsstruktur och arkivlagens (1990:782) krav på bevarande och gallring m.m. Utgångspunkten är att allmänna handlingar ska bevaras och att gallring får ske endast i enlighet med Riksarkivets föreskrifter eller beslut, om det inte finns särskilda gallringsföreskrifter i lag eller förordning. Det är dock viktigt att föreskriven gallring faktiskt utförs, inte minst av integritetsskäl. Myndigheten behöver därför säkerställa att leverantören slutligt raderar uppgifter som har gallrats av myndigheten. Ska handlingarna i stället bevaras ska myndigheten kontrollera att leverantören har förutsättningar att långtidsbevara handlingar eller att det finns realistiska möjligheter för myndigheten att hämta hem sina allmänna handlingar eller överföra informationen till en annan leverantör vid behov.

Riksarkivet har tagit fram föreskrifter och allmänna råd om elektroniska handlingar (upptagningar för automatiserad behandling). Föreskrifterna ställer långtgående krav på att myndigheten ska ha kontroll över sina elektroniska handlingar och insyn i

[26] Enligt de enkätsvar som har inkommit inom ramen för utredningen har 40 procent av respondenterna svarat att de har tecknat personuppgiftsbiträdesavtal vid andvändning av SaaS-tjänster. Motsvarande siffror för PaaS- och IaaS-tjänster är 43 respektive 56 procent.

externa leverantörers hantering av handlingarna samt upprätthålla en god informationssäkerhet.[27]

5.1.3.5 Upphandla

Upphandlingslagstiftningen kan anses utgöra det nav som den juridiska analysen rör sig kring vid inköp av en molntjänst. När myndigheten har sammanställt vilka rättsliga förutsättningar som ska vara uppfyllda för att den aktuella informationen ska kunna hanteras i en molntjänst ska myndigheten formulera dessa krav i upphandlingsunderlaget. Det är centralt att samtliga legala krav som myndigheten har identifierat i sin laglighetskontroll återspeglas i upphandlingsunderlaget. Av denna anledning är det av stor vikt att myndigheten utför ett gediget analysarbete som kan utmynna i en kravställning som uppfyller alla myndighetens behov såväl ur ett rättsligt perspektiv som ur övriga verksamhetsperspektiv.

Det förekommer, i synnerhet vid direktupphandlingar av publika molntjänster, att en myndighet måste acceptera att det är molntjänstleverantörens standardavtal som reglerar förhållandet mellan parterna. En sådan omständighet fråntar dock inte myndigheten dess ansvar för att kontrollera att molntjänstleverantörens avtalsvillkor ger förutsättningar för myndigheten att uppfylla de legala krav som myndigheten har identifierat vid sin laglighetskontroll.

5.1.4 Avslutande kommentarer

Många myndigheter anser att de juridiska frågeställningarna är svåra att hantera vid en planerad användning av molntjänster. Som genomgången har visat finns det dock ingen enskild, specifik bestämmelse som *alltid* utgör ett hinder för en myndighet att hantera sin information i en molntjänst. Myndigheten måste göra en laglighetskontroll i varje enskilt fall utifrån de bestämmelser som är tillämpliga på den specifika situationen. Det är resultatet av laglighetskontrollen som kommer vara avgörande för om myndigheten kan hantera den aktuella informationen i en molntjänst eller inte. I ett fall kan det vara offentlighets- och sekretesslagen som sätter stopp för myndighetens planerade inköp av en molntjänst och i ett annat fall kan det vara personuppgiftslagen eller arkivlagen.

Oavsett vilken typ av it-leverantör som anlitas av en myndighet ska myndighetens fokus vara att skydda den information som hanteras och säkerställa att informationen hanteras på ett lagligt sätt. Offentlighets- och sekretesslagstiftningen ska, utöver att skydda allmänna intressen, skydda den enskilde mot skada och men som kan uppstå om sekretessbelagda uppgifter röjs. Integritetsskyddslagstiftningen ska skydda den enskilde mot kränkning av den personliga integriteten. Arkivlagstiftningen ska säkerställa att den enskilde kan utöva sina demokratiska rättigheter genom att kunna ta del av myndighetens information och få insyn i dess verksamhet. Avtalsvillkoren mellan myndigheten och molntjänstleverantören ska säkerställa att myndigheten kan uppfylla samtliga krav som lagstiftningen ställer när informationen hanteras i en molntjänst.

Enligt vår uppfattning är den lagstiftning som aktualiseras, vid hantering av myndighetsinformation i en molntjänst, i och för sig ändamålsenlig i förhållande till ett av

[27] Riksarkivets föreskrifter och allmänna råd om elektroniska handlingar (upptagningar för automatiserad behandling) (RA-FS 2009:1) och Riksarkivets föreskrifter och allmänna råd om tekniska krav för elektroniska handlingar (upptagningar för automatiserad behandling) (RA-FS 2009:2).

sina syften nämligen att värna om den enskildes rättigheter. Det sammantagna regelverket är dock omfattande, komplext och svårt för myndigheterna att tillämpa. Vidare kan det konstateras att offentlighets- och sekretesslagen kan utgöra ett hinder för myndigheter att anlita inte bara molntjänstleverantörer, utan alla typer av privata leverantörer som tillhandahåller it-tjänster. Sekretessreglerade uppgifter som t.ex. är av särskilt integritetskänsligt slag får inte lämnas ut till en utomstående aktör med mindre än att denne är bunden av en lagreglerad tystnadsplikt. Mot denna bakgrund anser vi att det finns anledning att se över möjligheten att införa en lagreglerad tystnadsplikt för dem som i sitt arbete hos privata it-leverantörer tar del av myndigheters uppgifter. En sådan tystnadsplikt skulle kunna medföra att myndigheterna, när det i övrigt är lämpligt, i större utsträckning kan anlita privata it-leverantörer, t.ex. molntjänstleverantörer, för hantering av uppgifter som omfattas av sekretess.

5.2 Säkerhetsaspekter för myndigheter som använder molntjänster

Sammanfattning

Informationssäkerhet är en viktig fråga vid användning av molntjänster. Rätt nivå på säkerhet behöver bestämmas med avseende på konfidentialitet, riktighet, tillgänglighet och spårbarhet. Skyddsåtgärder ska väljas dels med hänsyn till hur skyddsvärd informationen är, dels med hänsyn till vilka specifika risker som finns relaterade till hanteringen av informationen. Informationen behöver exempelvis skyddas mot obehörig åtkomst, avbrott i önskad tillgänglighet samt förlust, förstörelse eller manipulation. Det kan också vara viktigt att ha möjlighet att spåra hur, och av vem, informationen har hanterats, vilket kan vara en större utmaning vid nyttjande av framför allt publika molntjänster. Många svenska myndigheter behöver stärka sitt säkerhetsrelaterade arbete och införa ett systematiskt arbetssätt kring säkerhet för att kunna möta utmaningarna i molntjänster.

Molntjänster erbjuder, som vi sett ovan, potentiella fördelar som exempelvis kostnadsbesparingar och möjlighet till förbättrade tjänster och verksamhetsresultat i myndigheter. En övergång till molntjänster kan i många fall också innebära att säkerheten förbättras på olika sätt, exempelvis genom bättre säkerhetslösningar eller högre kompetens inom säkerhetsområdet hos leverantören än hos kunden. Det finns dock ett antal säkerhetsrisker, inte minst i publika molntjänster, som man behöver känna till och som behöver värderas. Initialt måste därför myndigheten noggrant överväga om riskerna med externa komponenter i informationshanteringen kan hanteras eller att riskerna i övrigt uppvägs av de fördelar som finns med tjänsten. Nedan beskrivs ett antal potentiella risker, följt av information om myndigheternas arbete med informationssäkerhet.

5.2.1 Potentiella säkerhetsrisker

Molntjänster innebär (oftast) att verksamheten överlämnar sin informationshantering till en utomstående part. Det kan därmed bli svårt för myndigheten att kontrollera till exempel fysiskt skydd och andra säkerhetsåtgärder som omger de resurser som hanterar den aktuella informationen hos den utomstående parten. I synnerhet gäller detta om informationen lagras i ett annat land.

Nedan belyser vi kortfattat några exempel på risker och hot som vi ser som särskilt centrala för en myndighet att beakta inför en eventuell användning av molntjänst[28]. Vi vill dock betona, att flera av riskerna även förekommer eller kan förekomma vid traditionell outsourcing och en del även vid egen it-drift hos myndigheten. Vi vill också framhålla, att genomgången inte heller tar hänsyn till de specifika risker som finns förknippade med att utveckla och tillhandahålla it-tjänster i egen regi.

- **Bristande insyn och kontroll**

Som visades i den juridiska genomgången är möjligheten till insyn och kontroll central vid ett beslut om huruvida en offentlig verksamhet kan använda sig av en molntjänst. Det finns inneboende utmaningar med molntjänster när det gäller att få tillräcklig insyn i alla nödvändiga delar för att myndigheten ska kunna känna sig trygg med att information hanteras på rätt sätt, att kraven efterlevs och att eventuella risker hanteras på ett lämpligt och korrekt sätt. Inte minst gäller detta hos den valda leverantörens eventuella underleverantörer.

- **Otydlighet i ansvar och roller**

En säker informationshantering bygger på att det finns uttalade och tydliga ansvarsförhållanden. Det är kunden som ansvarar för att detta framgår av avtalet mellan kunden och leverantören.

Ett möjligt misstag är att kunden gör underförstådda antaganden om att leverantören genomför olika typer av säkerhetsaktiviteter, som exempelvis regelbundna tester med återläsning av säkerhetskopierad information, penetrationstester och skydd mot skadlig kod. Det kan även finnas en tendens att negligera säkerhetsfrågorna i ett partnermoln utifrån den underförstådda uppfattningen att de andra parterna redan har genomfört analyser och säkerhetsåtgärder. Det går dock inte att värdera risker enbart utifrån en specifik teknisk eller organisatorisk lösning. Den enskilda myndigheten måste alltid se till helheten av sina egna behov och vad den aktuella lösningen kan erbjuda.

- **Avvikelser mellan krav och leverans**

Vid kravställning mot en extern leverantör, som inte har kunskap eller djupare förståelse för verksamhetens interna och externa krav, kan det finnas en risk att fel introduceras i ledet mellan att krav beskrivs och att krav tolkas. Ju större kravmassa det handlar om, desto större är risken att en avvikelse introduceras.

En särskild utmaning infinner sig när det uppstår en avvikelse mellan ett krav som är omsatt i avtalsvillkor och den faktiska leveransen, t.ex. vid en större it-incident. För kunden är det svårt att avgöra vilken *faktisk* prioritering man kommer att få i ett sådant läge, oavsett stipulerade avtal. Prioriteringen av återställelsearbete hos en privat leverantör sker ytterst på affärsmässiga grunder, vilket sannolikt skulle kunna medföra att en liten kund med ett platinaavtal (avtal med högsta servicenivå och höga krav på informationssäkerhet) inte kommer att prioriteras framför en större och affärsmässigt

[28] Se bl.a. Vägledning – informationssäkerhet i upphandling s.48 ff, MSB555 (2013), samt artikel Det är superlätt att flytta till en molntjänst – men har du funderat på hur du flyttar därifrån?, Computer Sweden (2015).

viktig kund om kostnaden för att bryta mot avtalet med den mindre kunden är betydligt lägre än kostnaden för att förlora en större kund.

I fallet när myndigheter erbjuder varandra tjänster har den köpande myndigheten svårt att påverka sin situation eftersom incitamentsstyrningen via SLA (servicenivåavtal) och ekonomisk kompensation inte är en del av relationen mellan kund och leverantör.

- **Permanent förlust av data**

Permanent dataförlust kan uppkomma till följd av en rad olika händelser. Dataförlust kan ske genom avsiktliga handlingar, t.ex. brottsliga handlingar såsom stöld eller dataintrång, eller avsiktlig (felaktig) borttagning av datafiler eller program. Det kan också vara oavsiktligt, t.ex. på grund av administrativa misstag och raderingar. Fel i hård- eller mjukvara, krascher etc. kan också uppstå. Även naturkatastrofer såsom jordbävningar eller eldsvådor kan ge dataförlust. Molntjänster med god redundans kan dock hjälpa till att säkra information relativt andra lösningar.

- **Obehörig åtkomst**

Att använda en molntjänst innebär per definition att en myndighet låter en annan aktör tillhandahålla stöd för den egna informationshanteringen. Därmed finns också en risk för obehörig åtkomst utanför myndighetens kontroll. Den obehöriga åtkomsten kan potentiellt ske i olika former, t.ex. att molntjänstleverantörens personal har för vida åtkomsträttigheter eller att det genom otillräcklig styrning inte sker en tillräcklig separation mellan olika kunders information. Att större mängder information samlas hos enskilda aktörer kan också utgöra en dragningskraft för kriminalitet och andra former av antagonistiska hot. När kommunikation av information sker, inte minst över internet så som oftast är fallet för molntjänster, kan obehöriga försöka skaffa sig åtkomst till informationen.

- **Risker med delad miljö**

En kund hos en leverantör kan sällan välja sina medkunder. Detta kan i sig leda till vissa risker, då en eller flera medkunder skulle kunna ägna sig åt aktiviteter som potentiellt kan komma att påverka leverantörens övriga kunder. Skulle det pågå kriminell verksamhet hos en kund kan det exempelvis leda till att servrar beslagtas av polisen under en längre tid av utredning. Detta skulle i sin tur påverka samtliga kunder som har information på den aktuella servern. Vissa organisationer, även helt legitima verksamheter, kan oftare än andra vara utsatta för olika typer av attacker, exempelvis överbelastningsattacker. Attackerna kan i sådana fall även drabba andra kunder hos leverantören.

- **Otillgängliga molntjänster**

Fel i såväl hård- som mjukvara kan leda till tillgänglighetsincidenter. Detta bör beaktas särskilt i ett beredskapsperspektiv. Varje myndighet som använder molntjänster bör självklart ha en kontinuitetshantering som även innefattar de molntjänster man är beroende av för att upprätthålla sin verksamhet.

Molntjänster behöver dock inte i sig innebära en försämrad tillgänglighet utan kan även leda till att myndigheter kan få en bättre tillgänglighet jämfört med om myndigheten driftar och förvaltar sina it-lösningar själv. Detta förutsätter dock att myndigheten ingår väl underbyggda avtal som specificerar tillgänglighetskrav och viten på relevanta nivåer.

- **Kompetensförlust**

Kundens egen kompetens inom det aktuella it-området som placeras i en molntjänst kommer sannolikt att sjunka över tid, när utveckling och förvaltning av tjänsten ligger hos leverantören. Skulle myndigheten av någon anledning vilja eller tvingas att ta tillbaka verksamheten till den egna organisationen kan detta således bli utmanande ur ett kompetensperspektiv. Likaså kan det vara svårare för myndigheten att värdera olika tekniska lösningar vid en ny upphandling. Tillfälligt kompetensstöd kan då behövas. Man kan se en övergång till molntjänster som en kompetensmässig förskjutning från utförare till beställare, vilket kräver delvis helt nya roller.

- **Inlåsning**

Inlåsningseffekter kan uppstå 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. Det kan även bero på kompetensmässiga och rättsliga skäl, vilket kan medföra att tjänsten varken kan eller får förvaltas av någon annan än den som levererar den för tillfället.

- **Förändringar i leverantörsförhållanden**

Vilka underleverantörer som molntjänstleverantören använder sig av och ansvarsförhållandet parterna emellan, kan vara föränderligt under avtalsperioden. Om en leverantör köps upp kan det leda till att avtalsvillkor inte längre gäller och att ett akut återtagande av informationen/tjänsten till myndigheten skulle kunna bli nödvändig. Leverantören av molntjänsten kan även gå i konkurs, vilket kan medföra plötslig otillgänglighet av tjänsten och potentiell inlåsning av information hos molntjänstleverantören. Ett annat scenario är att leverantören genom uppköp kommer att flytta drift av tjänsten till ett annat land med ett annat legalt regelverk.

- **Inkompatibla säkerhetslösningar**

Om avtalsprocessen inte leder fram till ett klarläggande av vilka säkerhetsåtgärder som ska vidtas och vem som är ansvarig för dessa, kan detta leda till andra typer av problem. Ett sådant är att kunden och leverantörens säkerhetsåtgärder interagerar på ett negativt sätt, till exempel att kundens brandväggar förhindrar molntjänstleverantörens sårbarhetsanalyser.

5.2.2 Viktigt att säkerställa rätt nivå av skydd

Informationssäkerhet handlar i stort om att säkerställa rätt nivå av skydd med avseende på att *rätt information* (riktighet), finns tillgänglig för *rätt person* (konfidentialitet), vid *rätt tidpunkt* (tillgänglighet). Utöver detta ska det även gå att säkerställa *vem som har gjort vad* med informationen (spårbarhet).

Skyddsåtgärder ska väljas dels med hänsyn till hur skyddsvärd informationen är och vilka specifika risker som finns relaterade till hanteringen av informationen. Andra faktorer att ta hänsyn till är organisationens riskaptit och kostnaderna för olika skyddsåtgärder. Informationen behöver exempelvis skyddas mot obehörig åtkomst, avbrott i önskad tillgänglighet samt förlust, förstörelse eller manipulation. Det kan också vara viktigt att ha möjlighet att spåra hur, och av vem, informationen hanterats för att till exempel kunna avgöra vem som har gjort vad med informationen.

Rätt nivå på informationssäkerhet ska säkerställa myndighetens möjligheter att hantera informationen på ett korrekt sätt. För att verksamheten ska kunna identifiera rätt nivå ska myndigheten ta utgångspunkt i myndighetens informationsklassificering men även

göra en specifik riskanalys relaterat till den information man avser att behandla i en tilltänkt molntjänst.

5.2.2.1 Informationssäkerhet för myndigheter

För att en organisation ska kunna skapa och upprätthålla en god informationssäkerhet är det lämpligt att införa ett ledningssystem för informationssäkerhet (LIS). Av MSB:s föreskrift 29 framgår att statliga myndigheter ska arbeta systematiskt med informationssäkerhet och införa och tillämpa ett ledningssystem i enlighet med den svenska och internationella standarden för informationssäkerhet SS-ISO/IEC 27001 och 27002. Detta innebär bland annat att myndigheten ska ta de steg som beskrivs i bilden nedan.

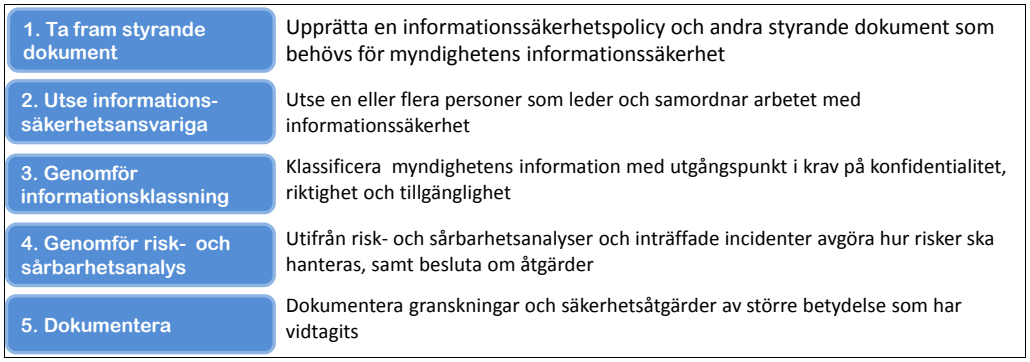


Bild 4 Grundläggande steg i myndigheters säkerhetsarbete

Under 2014 genomförde MSB en kartläggning av hur statliga myndigheter tillämpar MBS:s föreskrifter om statliga myndigheters informationssäkerhet samt hur myndigheterna i övrigt arbetar med informationssäkerhet.[30] Även Riksrevisionen genomförde samma år en granskning i syfte att utreda om arbetet med informationssäkerhet i den civila statsförvaltningen är ändamålsenlig utifrån en ökande hotbild. Resultatet sammanställdes i en rapport som visade att det fanns stora brister i statens arbete med informationssäkerhet.[31] Här finns således ett viktigt område för förbättring inom statlig sektor, oavsett om man använder molntjänster eller inte. Molntjänster kan genom sin karaktär dock accentuera vikten av ett bra informationssäkerhetsarbete. Att myndigheter implementerar ledningssystem för informationssäkerhet och inför ett strukturerat arbetssätt kring informationssäkerhetsfrågor i sin verksamhet är ett viktigt första steg på vägen mot att åstadkomma en säker och ändamålsenlig användning av molntjänster.

I E-delegationens strategi från 2012 finns ett antal strategiska mål inom informationssäkerhetsområdet som svensk e-förvaltning bör ha en tydlig inriktning att uppnå. Även de mål som finns i 2012 års regeringsstrategi för en digitalt samverkande förvaltning uttrycker en tydlig inriktning när det gäller att höja informationssäkerheten inom myndigheterna. [32] Informationssäkerhet ses i strategin som en förutsättning för en hållbar utveckling av digitala tjänster: ”*Statsförvaltningen behöver därför fortsätta att arbeta systematiskt med informationssäkerhet och ställa förvaltningsgemensamma*

[29]MSB:s föreskrifter MSBFS 2009:10
[30] En bild av myndigheternas informationssäkerhetsarbete – tillämpning av MSB:s föreskrifter, publ.nr: MSB740
[31] Informationssäkerheten i den civila förvaltningen, RiR 2014:23
[32] Regeringens strategi för en digitalt samverkande statsförvaltning, N2012.37

säkerhetskrav då externa leverantörer anlitas. En förbättrad informationssäkerhet innebär att utvecklingen och förvaltningen av tjänster kan effektiviseras, samtidigt som kvaliteten ökar."

Det finns alltså en inriktning – i olika former – för att skapa tillräcklig säkerhet kring den normala hanteringen av informationen inom statliga myndigheter. Denna inriktning inkluderar även information som hanteras i molntjänster.

5.2.2.2 Förslag till ny säkerhetsskyddslagstiftning

Säkerhetsskyddslagen (1996:627) ställer krav på särskilda skyddsåtgärder för den information som kan påverka rikets säkerhet. Säkerhetsskyddsregleringen ses för närvarande över. I mars 2015 presenterade regeringens utredare ett förslag till en ny säkerhetsskyddslag.[33] Syftet med översynen var bland annat att säkerställa att en ny lag svarar mot de förändrade kraven på säkerhetsskyddet, bl.a. avseende utvecklingen på informationsteknikområdet, en ökad internationell samverkan, en ökad sårbarhet i samhällsviktiga funktioner och att säkerhetskänslig verksamhet i allt större omfattning bedrivs i enskild regi.

Utredningen förutser att tillämpningsområdet för den nya lagen kommer att behöva vara något vidare än idag. Bland annat har skyddet av informationens riktighet och tillgänglighet förtydligats. Samtidigt överlämnas det även i fortsättningen åt verksamhetsutövarna själva att primärt bedöma om de bedriver någon säkerhetskänslig verksamhet och att, om så är fallet, göra den svåra avgränsningen mellan vad som ska betraktas som skyddsvärt enligt säkerhetsskyddslagstiftning och vad som ska falla utanför lagens tillämpningsområde. Det torde bli så med det nya förslaget att fler verksamhetsutövare på det civila området än idag kommer att behöva göra en kvalificerad säkerhetsanalys enligt säkerhetsskyddsförordningen.

Reglerna rörande säkerhetsskydd begränsar redan idag möjligheterna att använda molntjänster. Det är därför av stor betydelse att följa utvecklingen på säkerhetsskyddsområdet för att på ett korrekt sätt kunna bedöma i vilken utsträckning och hur molntjänster kan användas i verksamheten. Får säkerhetsskyddet – såsom föreslagits – ett ytterligare något utvidgat tillämpningsområde kommer denna bedömning att bli än viktigare.

5.3 Nationella perspektiv på molntjänster i staten och informationssäkerhet

Sammanfattning

En breddad användning i svenska myndigheter av molntjänster och andra externt levererade it-tjänster aktualiserar frågan om hur den nationella säkerheten påverkas. Frågan behöver få större fokus framåt. Användning av externa it-tjänster ger organisatorisk koncentration samt teknisk och fysisk koncentration. Ackumulering av större mängder av information kan även utgöra ett mål för olika typer av antagonism. Det saknas idag legal eller annan grund för prioritering av samhällsviktiga funktioner vid it-incidenter, något som har efterfrågats av leverantörerna själva. Ur ett säkerhetsperspektiv finns olika för- och nackdelar med att välja privata och offentliga leverantörer av molntjänster, vilka behöver beaktas.

[33] En ny säkerhetsskyddslag, SOU 2015:25

Myndighetsgemensamma kommunikationslösningar, s.k. ”gov net”, kan medföra ökade säkerhetsrisker, men skulle också kunna få positiva effekter med gemensam kravbild på säkerhetsnivåer och en gemensam grundnivå avseende tillgänglighet.

5.3.1 Konsekvenser av ökad användning av molntjänster

Informationssäkerhet i förhållande till molntjänster i staten kan ses i två dimensioner; dels myndighetens behov av informationssäkerhet, dels frågeställningar som kan hänföras till den samlade nationella bilden. Ur ett nationellt perspektiv går det att identifiera några generella konsekvenser av en allt mer omfattande användning av molntjänster i statlig verksamhet. Dessa beskrivs nedan.

5.3.1.1 Organisatorisk koncentration

I de flesta fall kommer en ökad användning av molntjänster att innebära en ökad organisatorisk koncentration kring hantering av vissa typer av information. Ett exempel på detta är då en myndighet åtar sig att vara värdmyndighet för en tjänst som handhar viss informationshantering för andra myndigheter och ibland även för kommuner och landsting. Ett annat exempel är när många myndigheter lägger ut delar av sin informationshantering hos samma kommersiella leverantör. En hybrid av dessa två varianter är när en myndighet fungerar som en förmedlare av molntjänster som i praktiken levereras av en kommersiell aktör, vilket är fallet med Statens servicecenter.

Den organisatoriska koncentrationen innebär både en möjlighet och en risk i detta sammanhang. Möjligheten ligger i att skapa en gemensam organisatorisk styrning av informationssäkerheten, till exempel genom styrning av krav, roller, begrepp och regler, vilket kan ge högre grad av förutsägbarhet i fråga om vilka krav som kommer att ställas på molntjänster och bättre förutsättningar för både privata och offentliga leverantörer. Komplexa säkerhetsåtgärder, som till exempel kontinuitetshantering, skulle sannolikt också vara möjliga att genomföra på ett bättre sätt än i dag genom att enhetliga metoder kan tillämpas. Erfarenheter från större it-incidenter tyder på att stora leverantörer ofta har möjlighet att utveckla specialiserad kompetens som kan kallas in vid behov. Ytterligare en aspekt att beakta är att den organisatoriska koncentrationen kan ge en bättre förmåga till uppdaterad nationell lägesbild eftersom underlaget till lägesbilden finns att söka hos färre aktörer.

Samma faktorer som innebär en möjlig höjning av informationssäkerhet skulle samtidigt kunna leda till en ökad risk. En bristfällig styrning hos en myndighet som agerar leverantör påverkar fler om den sker med många myndigheter som användare, än om en enskild myndighet underskattar sitt eget behov av informationssäkerhet. Sett ur ett nationellt perspektiv är det en stor risk om många myndigheter blir drabbade av störningar samtidigt, särskilt om det rör sig om samhällsviktig verksamhet.

Riskbilden varierar även med vilken organisation det är som koncentrationen uppstår hos. Det är till exempel en väsentlig skillnad på en svensk värdmyndighet och ett utländskt företag med komplex ägarstruktur.

5.3.1.2 Teknisk och fysisk koncentration

En ökad användning av molntjänster kan innebära en teknisk och fysisk koncentration av de stöd som används för vissa delar av myndigheters informationshantering, jämfört med om myndigheterna driftar och förvaltar sin egen it-miljö och egna it-lösningar.

Den tekniska koncentrationen kan ge underlag för en mer avancerad teknisk miljö som ständigt vidareutvecklas. Om rätt krav ställs kan tekniska säkerhetsåtgärder upprätthållas på en mycket hög nivå.

De risker som uppstår om många myndigheter finns i samma tekniska miljö är dock avsevärda. Många större störningar som drabbat svenska myndigheter har sitt ursprung i fel vid uppdateringar eller hårdvaruproblem. En bugg i applikationen eller en felaktig uppdatering kan leda till stora störningar och brist på tillgänglighet på nationell nivå.

En viktig lärdom vid den så kallade Tieto-incidenten i november 2011 var att MSB hade svårt att få klarhet i vilka myndigheter och andra aktörer som hade drabbats av incidenten. Om det hade funnits ett register över de offentliga kunderna i en viss tjänst eller miljö skulle åtminstone dessa snabbt kunna ha identifierats, vilket i sin tur skulle ha underlättat för MSB vad gäller uppdraget att skapa en nationell lägesbild samt ett strukturerat återställelsearbete. Dessutom skulle det ha varit möjligt att få en överblick över koncentrationen av myndigheters informationshantering hos olika leverantörer.

Därtill kommer olika former av antagonistiska hot mot den tekniska miljön som får samma konsekvenser. Här måste särskilt risken för överförda hot mellan organisationer uppmärksammas. Det räcker därmed inte att varje ingående myndighet gör sin egen riskanalys, utan det måste göras täta riskanalyser över helheten. Risker måste identifieras och värderas för olika typer av molntjänster eftersom utfallet kan bli mycket olika beroende på om det är en koncentration av IaaS, PaaS eller SaaS. För en publik molntjänst kan det vara svårt att genomföra eftersom det skulle kräva information både om leverantörens övriga kunder och om leverantörens tekniska säkerhetsåtgärder i stort, information som kan vara omöjlig för leverantören att lämna ut eftersom det i vissa fall skulle strida mot ingångna avtal med andra kunder och mot leverantörens affärsintresse.

Även risken för situationer där en större mängd information förloras eller hamnar i orätta händer måste tas på stort allvar. Det finns en trend av allt fler intrång i lösningar som hanterar större mängder av personuppgifter, vilket exempelvis skett inom den amerikanska hälso- och sjukvården.

5.3.1.3 Prioritering av samhällsviktiga funktioner vid it-incidenter

Vid större incidenter måste en prioritering ske av vilka kunder som ska få del av den begränsade funktionalitet som finns kvar och vilka som ska prioriteras i återställelsearbetet. Bristande möjligheter till prioritering i återställelsearbete är inte ett problem enbart för den enskilda myndigheten, utan även ur ett nationellt säkerhetsperspektiv. Det finns ett behov av att verksamheter som är kritiska för samhällets funktionalitet bör prioriteras framför mindre samhällsviktig verksamhet. Privata leverantörer har även vid inträffade incidenter efterfrågat ett stöd för att kunna agera så att samhällsviktig verksamhet kan prioriteras, dvs. det finns en förståelse för problemet och också en vilja att se till samhällsperspektivet. Hur ett stöd för sådan prioritering kan utvecklas och förvaltas är en fråga som måste analyseras närmare.

5.3.1.4 Fredstida krissituationer och höjd beredskap

Med tanke på det beroende som många myndigheter kommer att ha till fungerande molntjänster för att kunna upprätthålla sin verksamhet måste hänsyn även tas till behov vid kriser och situationer då beredskapen höjs. Enligt ansvarsprincipen i den svenska krisberedskapen har varje myndighet ansvar för att säkerställa sin egen

verksamhet, men vid höjd beredskap måste även den nationella situationen beaktas. Detta görs bland annat inom ramen för arbetet med civilt försvar. Ett av målen för det civila försvaret är att säkerställa de viktigaste samhällsfunktionerna. Behovet av att göra prioriteringar mellan olika myndigheters tillgång till molntjänster kan då komma i konflikt med kommersiella överenskommelser. Hur detta ska hanteras finns det idag inga lösningar på.

Att många myndigheter samtidigt kan drabbas av incidenter tillför ett riskelement utöver varje enskild myndighets egen risk. Av detta följer att det kan tillkomma en extra kostnad för en ökad robusthet för tjänsten som helhet, så att den även kan stå emot störningar vid kriser och höjd beredskap. Hur denna kostnad ska finansieras och fördelas mellan kundmyndigheter är något som behöver analyseras vidare.

5.3.1.5 Ackumulering av information

Ackumulering av större mängder av information kan utgöra ett mål för olika typer av antagonism. Förutom den ovan beskrivna trenden mot fler riktade försök av olika typer av aktörer att få åtkomst till källor av ackumulerad information, såsom person-uppgifter, har det även framkommit att vissa statsmakter har använt sina underrättelse-verksamheter för att skaffa information genom att göra intrång i både offentliga och kommersiella tjänster.

När information ackumuleras i olika tjänster hos samma leverantör finns också möjligheten att sammanställa ny information som då kan bli känslig på ett annat sätt än när varje informationsmängd hanterades separat. Att så inte får ske måste regleras tydligt i avtal eller överenskommelse. Om leverantören utvecklar nya tjänster som innebär att information ur olika källor sammanförs kan nya informationsmängder skapas som står utan en tydlig informationsägare. Om kunden inte är medveten om detta görs det inte heller en förnyad informationsklassning med korrekt kravställning.

5.3.1.6 Kommunikation och infrastruktur

Utöver avbrott som beror på kapacitetsbrist eller nertid av kommunikationsvägarna medför också koncentrationen av datatrafik att kommunikationstjänsten i sig behöver analyseras ur ett säkerhetsperspektiv. Det kan antas att den ackumulerade informationsmängden även hanteras i gemensamma kommunikationslösningar, vilket gör att även den kan antas vara intressant för en eventuell antagonist.

En gemensam kravställning på kommunikationslösningen skulle kunna få positiva effekter i form av att alla ”in- och utgångar” till en molntjänst har samma kravbild ur ett säkerhetsperspektiv och att statliga aktörer skulle kunna få en gemensam grundnivå avseende tillgänglighet.

En annan säkerhetsaspekt rör ägande och kontroll över infrastrukturen till molntjänsterna. Förutom att det är svårt att påverka exempelvis prioritering vid en incident när man inte kontrollerar infrastrukturen kan det även förekomma komplexa ägar- och förvaltningsstrukturer av kommunikationslösningarna som blir svåra att överblicka. Den statliga utredningen *Informations- och cybersäkerhet i Sverige* konstaterar att det i Sverige i dag finns ett stort behov av myndighetsgemensam infrastruktur för säker kommunikation som ett verktyg för svenska myndigheters informationshantering, där

molntjänster skulle kunna vara ett sådant område. [34] Utredningen har inte närmare gått in på för- och nackdelar med gemensam infrastruktur.

5.3.2 Säkerhetsaspekter vid användning av offentliga leverantörer av molntjänster

Genom E-delegationen och andra initiativ har regeringen gett en tydlig inriktning mot att Sverige ska bli ledande inom e-förvaltningsområdet. Molntjänster driver utvecklingen av enkelt tillgängliga tjänster för medborgare och företag, och samverkan mellan myndigheter. Nationella säkerhetsaspekter aktualiseras då myndigheter i rollen som offentlig leverantör erbjuder molntjänster till andra myndigheter eller till kommuner och landsting, som till exempel eHälsomyndigheten.

Ett principiellt problem som uppmärksammats bland annat inom E-delegationens arbete med informationssäkerhet vad gäller MSB:s föreskrifter, MSBFS 2009:10, är följande. När myndigheter i allt högre grad samverkar kring informationshanteringen, bland annat genom att erbjuda varandra tillgång till molntjänster, uppstår ett utrymme mellan myndigheterna som bildar en faktisk gråzon. I denna gråzon förefaller det som att den interna informationssäkerhetsstyrningen i många fall inte tillämpats vare sig hos värdmyndigheten eller hos kundmyndigheten. Ett fungerande rollspel kring informationssäkerheten har alltså inte alltid etablerats mellan myndigheterna. Konsekvensen blir att många centrala säkerhetsaktiviteter inte blir genomförda alternativt inte blir genomförda på rätt sätt.

MSB tog i samverkan med andra myndigheter i E-delegationen fram ett enkelt stöd för myndigheter i leverantörsroller inför utveckling av en e-tjänst. I denna checklista är fastställande av ansvar i hela livscykeln för en tjänst ett bärande tema. En sammanhållande kedja av styrning måste vidare finnas. Informationen får heller inte hanteras på något annat sätt än det som överenskommits med värdmyndigheten.

Det är sannolikt önskvärt att efterlikna en marknadssituation då myndigheter utvecklar tjänster som erbjuds till andra myndigheter. Görs en kundanalys innan utvecklingsarbetet startar kan kundens krav på säkerhet fångas. Analysen kan undanröja systemfel som annars riskerar att permanentas om lösningens design inte går att förändra. Kraven på säkerhet gäller inte endast tekniska lösningar och funktionalitet utan också mer omfattande organisatoriska åtgärder som kontinuitets- och incidenthantering.

Ett annat behov som kan fångas vid en inledande analys är om molntjänsten behöver levereras med flera skyddsnivåer, vilket kan ha stor betydelse när det gäller säkerhet men även påverkar ekonomin i tjänsten. Den levererande myndigheten måste också skapa en process för hantering av fortlöpande kravställning angående säkerhet från kunder samt en process för uppföljning.

Hur kan en myndighet som molntjänstkund genomdriva en överenskommelse om en säkerhetsåtgärd om den levererande myndigheten, värdmyndigheten, inte vill effektuera det, och möjligheter att utkräva vite och andra etablerade styrfunktioner saknas? I vissa fall har värdmyndigheten bestämt skyddsnivån. Det förekommer också att regeringen fattar beslut som leder till att myndigheter åläggs att använda en tjänst. Ur ett säkerhetsperspektiv uppstår då frågan om vem som är riskägaren.

---

[34] Informations- och cybersäkerhet i Sverige, SOU 2015:23 s. 248ff

Kundmyndigheten fråntas möjligheten till kravställning utifrån sin egen riskbedömning, samtidigt som värdmyndigheten inte har förutsättning att bedöma risken för kundmyndigheternas verksamhet. Sammantaget leder detta till en situation där ansvaret för informationssäkerheten hamnar i ett ingemansland där varken informationsägare eller system-/tjänsteägare har överblick över risker och åtgärder.

5.3.3 Säkerhetsaspekter vid användning av privata leverantörer av molntjänster

Privata leverantörer av molntjänster kan anlitas på ett antal olika sätt och i olika omfattning, vilket ger olika möjligheter till styrning av informationssäkerhet och också medför olika risker. Gemensamt är att det i de allra flesta fall sluts ett juridiskt bindande avtal till skillnad mot när myndigheter erbjuder varandra tjänster. Däremot gäller inte MSBFS 2009:10 för privata leverantörer, vilket gör att kunden inte kan förutsätta att leverantören har ett systematiskt informationssäkerhetsarbete. Att få insyn i hur informationssäkerheten i tjänsterna är utformad är svårt i förhållande till egen drift och förvaltning men också i förhållande till en lösning med en offentlig aktör som molntjänstleverantör åt andra myndigheter. Detta ökar behovet av att redan i underlaget för anskaffningen ställa tydliga krav på villkoren för uppföljning av efterlevnad av kraven. Den bristande insynen gör det också svårt att vid en incident snabbt skapa en lägesbild över hur samhällsviktig verksamhet drabbats av incidentens konsekvenser. Den obligatorisk rapportering av it-incidenter som lades fram i förslag från NISU, och som nu i december 2015 beslutades av regeringen, gäller endast för statliga myndigheter och blir efter vad vi erfar inte tillämplig för dessa leverantörer. [35]

En fördel med privata leverantörer ur säkerhetssynpunkt kan vara att många av de privata leverantörerna är specialiserade på att paketera tjänster och att god säkerhet är viktigt ur affärsmässig synvinkel. Ett antagande skulle kunna vara att de även kan inkludera säkerhet i sina tjänster på ett för kunden fördelaktigt sätt om de får en gemensam och tydlig kravbild, till exempel i form av definierade skyddsnivåer. Detta skulle kunna leda till ekonomiska fördelar för både kund och leverantör samt en förbättrad informationssäkerhet på nationell nivå.

5.4 Vad krävs för att använda molntjänster och tillgodogöra sig fördelarna?

Sammanfattning

För att kunna ta tillvara kostnadsfördelar och andra verksamhetsmässiga fördelar i molntjänster fullt ut krävs en teknisk och organisatorisk mognad och att myndigheten har analyserat hur molntjänsters möjligheter kan användas ur ett verksamhetsstrategiskt perspektiv. Det finns ett antal analyser och åtgärder som myndigheterna kan och bör företa redan innan man överväger upphandling av molntjänster, om myndigheten vill förbättra sina möjligheter att tillvarata potentialen i molntjänsterna.

[35] NISU är en förkortning för informationssäkerhetsutredningen Informations- och cybersäkerhet i Sverige (SOU 2015:23). Regeringens beslut om obligatorisk it-incidentrapportering framgår av pressmeddelande http://www.regeringen.se/pressmeddelanden/2015/12/regeringen-infor-krav-pa-it-incidentrapportering-for-statliga-myndigheter/

Ytterligare en dimension av förutsättningar vid sidan av de rättsliga och säkerhetsrelaterade är möjligheten för den enskilda myndigheten att tillgodogöra sig de potentiella nyttorna av molntjänster, vilket har att göra med såväl teknisk som organisatorisk mognad. Vi har tidigare i rapporten nämnt att vissa verksamheter lämpar sig bättre än andra för molntjänster, inte minst i starten. Till exempel är information i stödtjänster oftast lättare att ”lägga i molnet” än information i kärnsystem. Vi vill i detta sammanhang lyfta fram ett antal faktorer som är viktiga för myndigheter att tänka på inför användning av molntjänster:[36]

- **Applicera den legala analysen och säkerhetskraven på myndighetens specifika situation**

Utöver generella krav på myndigheter, vilka specifika lagar och regler lyder myndigheten under? Vad innebär de i t.ex. termer av specifika informationssäkerhetsrelaterade krav? Finns behov av särskilda lösningar för identitetshantering m.m? Finns särskilda informationsmängder som inte får hamna utanför myndighetens kontroll? Om myndigheten inte sedan tidigare har gjort informationsklassning eller bestämt skyddsnivå för olika informationsmängder bör det göras i detta skede.

- **Inventera vilka molntjänster som finns i bruk**

Kartlägg vilka molntjänster som redan används ute i myndighetens verksamhet – och ta kontrollen över dem. Eftersom det är enkelt kan ansluta sig till molntjänster är det sannolikt att det finns fler molntjänster i myndighetens miljö än myndigheten idag vet om. Kontroll är i detta sammanhang viktigare än kostnadsaspekterna.

- **Analysera organisationens generella mognad**

Finns styrmodeller, förvaltning och processledning på plats som garant för att kunna följa molntjänster genom olika delar av organisationen? Behöver styrningen eller organisationen förbättras i någon del? Finns det en tydlig beslutsmodell? Finns alla nödvändiga kompetenser inom t.ex. it, juridik, inköp och verksamhet som kan hantera digitaliseringens och molntjänsternas utmaningar såväl som möjligheter? Kanske behövs det både teknisk och affärsmässig utbildning för att kunna bedöma hur molntjänster bäst skulle kunna användas i den egna verksamheten. Flera leverantörer vittnar också om, att den interna förändringsresan ofta kan vara det främsta hindret.

- **Analysera myndighetens tekniska förutsättningar**

Hur molnvänlig är it-miljön och it-portföljen? Är system och servrar i slutet av en livscykel. Kan molntjänster vara ett alternativ? Är arbetsplatser med klientutrustning i slutet av livscykeln och kan virtuella klienter i så fall vara ett alternativ? Ta fram eller granska myndighetens systemkarta. Viss information kan finnas i system med många anpassningar, många integrationer och beroenden till andra system etc. Dessa kan behöva undantas molntjänster, alternativt sätts en plan för hur de ska kunna separeras och förberedas för en transit till en molntjänst över tid. Ett vägval inom it-avdelningen kan vara huruvida myndigheten ser tillräckligt stora fördelar i molntjänster för att även

[36] Sammanställningen baserar sig bl.a. på samtal och informationsmaterial från uppdragets två rådgivande molnforum för leverantörer. Se även The Top 10 Cloud Myths, Gartner (2014), för överblick över vanliga misstag i resonemang kring molntjänster.

flytta existerande tekniska last (s.k. ”legacy”) i äldre komplexa systembyggen och i monolitiska system till molntjänster, eller om det bara ska användas vid nya tjänster.

- **Ta fram en strategi för när, och hur, myndigheten ska använda sig av externa tjänster, baserat på myndighetens verksamhetsstrategi**

Molntjänster förändrar sättet på vilket man konsumerar it och kan förändra verksamheter i grunden. Utifrån myndighetens verksamhetsstrategi bör man identifiera hur molntjänster kan fylla en roll i att ta myndigheten från nuläge till sin framtida målbild. Molntjänster bör särskilt övervägas när myndigheter ska inrätta nya tjänster eller verksamheter. Slutsatserna kan beskrivas i en sourcingstrategi eller motsvarande[37]. Sök därför de lågt hängande frukterna, framgångar föder också trygghet. Värt att notera är att privata kunder som går över till molntjänster enligt vad vi erfar ofta har som ambition att investeringen måste betala sig förhållandevis snabbt. Transitionskostnader, kostnader för utbildning m.m. ska helst betala sig inom 6-12 månader.

- **Gör en ekonomisk kalkyl**

Jämför kostnaden för anskaffning och användande av en montjänst, inklusive eventuella kostnader som uppkommer i senare skede och kostnader som uppstår utanför it-avdelningen, med dagens lösning (i egen regi eller traditionell outsourcing). Räkna även in de potentiella fördelar i form av bättre kvalitet, bättre tjänster, snabbare anpassningar etc. som kan uppkomma när myndigheten går över till en molntjänst, och översätt även sådana förväntade värden till nominella termer. Kalkylen påverkas även av om myndigheten avser att minska eller ställa om den interna kompetensen till följd av övergången till molntjänstleveranser.

- **Börja med att standardisera och virtualisera - och gör eventuellt ett privat moln för myndighetens it**

Standardisering och virtualisering av klienter och servrar kan i sig, dvs. oaktat eventuella molntjänster, ge stora kostnadsfördelar. Analysföretaget Gartner beskriver ”renovate the core” som en mycket viktig åtgärd innan man lägger över sin information i molnet. Hellre än att lägga tid och resurser på att föra över s.k. legacysystem till molntjänstlösningar, bör kraften läggas på att applicera molntjänster i de delar av verksamheten där de verkligen kan addera värde. Separering av olika itsystem och tydliga gränssnitt, t.ex. med kända API:er, ökar möjligheterna att använda även publika molntjänster i framtiden. Om myndigheten överväger att skapa privata molntjänster bör den initialt göra jämförelser med motsvarande publika molntjänster och satsa på att uppnå samma typ av nyttor. Man bör också vara beredd på att involvera verksamhetspersonal samt att göra förändringar i organisation, processer och arbetssätt.[38]

[37] Strategier för molntjänster har behandlats av bl.a. Gartner. Se t.ex. The Three Rationales Behind Cloud Computing Strategies (2014) och Designing a Cloud Strategy Document (2015)

[38] Six reasons Private Clouds Fail, and How to Succeed s. 1ff, Gartner (2014)

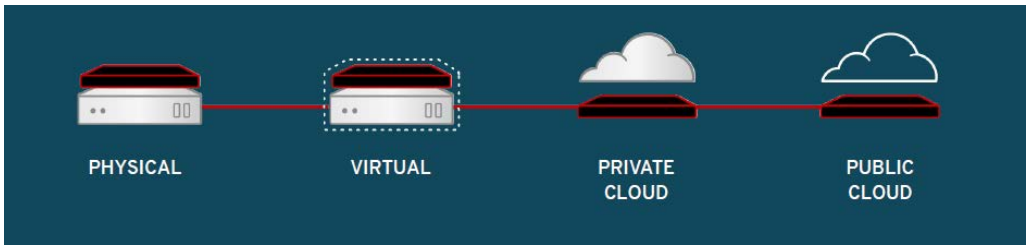


Bild 5 Olika tekniska plattformar existerar parallellt under en lång tid (bild från Redhat)

Listan ovan visar att svenska myndigheter kan vidta ett antal olika åtgärder för att göra sig redo för molntjänster. Som tidigare nämnts erfar vi att många myndigheter efterfrågar stöd i en sådan resa och i hur man ska tänka vid upphandling. Vi ser att det vore en intressant att samla sådan kompetens på ett nationellt plan.

6 Anskaffning av molntjänster i statliga verksamheter

Sammanfattning

Kammarkollegiet har tagit fram ramavtalet Programvaror och tjänster där molntjänster ingår. Få avrop har hittills gjorts men fler väntas. Under 2016 lanseras ramavtalen Datacenter samt It-drift som också innehåller molntjänster. Egen anskaffning är fortfarande vanligast. Att bedöma framtida användning av en molntjänst och huruvida myndigheten kan hålla sig inom tröskelvärdet kan vara förenat med vissa svårigheter. It-avdelningarna har sällan kännedom om alla molntjänster som har köpts eller som används inom myndigheten, så kallad ”skugg-it”.

Nedan beskrivs olika sätt på vilka anskaffning av molntjänster från privata leverantörer kan ske idag.

6.1 Avrop från ramavtal inom ramen för statlig inköpssamordning

Statens inköpscentral vid Kammarkollegiet ansvarar för ett antal nationella ramavtal inom it och telekom. Sedan våren/hösten 2015 finns i Sverige fyra ramavtal som även rymmer molntjänster. Samtliga fyra delområden inom ramavtalen "Programvaror och tjänster" har molntjänster som en av de möjliga leveransformerna.

Hittills har endast ett mindre antal avrop av molntjänster genomförts på dessa avtal, vilket delvis kan bero på att det är vanligt förekommande att myndigheter i slutet av en avtalsperiod brukar ”gardera” sig med att genomföra köp på de gamla avtalen.

Under 2016 planerar Kammarkollegiet att ta ytterligare två ramavtal i drift inom vilka molntjänster kommer att kunna avropas: ramavtal för Datacenter samt It-drift. Båda ramavtalen väntas träda i kraft kring halvårsskiftet.

Kammarkollegiet ansvarar för att skapa ramavtalen och de grundläggande kraven på informationssäkerhet i dessa. Kammarkollegiet tar också fram olika allmänna anvisningar beroende på hur tjänsten levereras. Ansvaret för att teckna personuppgiftsbiträdesavtal och ställa specifika säkerhetskrav m.m. ligger på den avropande myndigheten. Erfarenheterna visar att det finns brister hos myndigheterna att ställa säkerhetskrav och upprätta nödvändiga juridiska dokument vid avrop från nationella ramavtal, något som dock borde vara en lika överhängande risk vid annan typ av upphandling.

Redan idag utvecklar Kammarkollegiet fiktiva exempelavtal som stöd för myndigheterna. Vår bedömning är dock att myndigheterna behöver ytterligare stöd inom fler områden, inklusive praktiskt tillämpade vägledningar och riktlinjer.

Kammarkollegiet har i dagsläget valt en väg där molntjänster ryms i samma ramavtal som andra sourcinglösningar. Utvärderingar av erfarenheterna från dessa första ramavtal på området bör göras över de närmaste åren. I det sammanhanget kan man överväga om det finns behov av att i framtida ramavtal eventuellt särskilja på (publika) molntjänster och andra tjänster, eller på annat sätt tydliggöra krav som är förknippade särskilt med olika typer av molntjänster.

Ytterligare en aspekt av nationella ramavtal är hur många aktörer som tilldelas ramavtal och vilka krav man ställer på företagens storlek. Som säkerhetsanalysen har visat, är det också en nackdel i sig att ramavtal med få leverantörer tenderar att ge effekten av att svenska myndigheter lägger ”många ägg i samma korg”. Mindre svenska leverantörer kan samtidigt konstatera att de inte kan konkurrera på lika villkor utan behöver gå in som underkonsulter till större internationella bolag.

Avtalsförhållanden i flera led verkar inte positivt för transparensen och möjligheterna för myndigheten att utkräva ansvar eller följa informationens hantering över tid. En trend inom molntjänster är också att molntjänsterna och molntjänstleverantörerna blir alltmer nischade för att kunna bli alltmer effektiva och innovativa. Om man då paketerar upphandlingar med ett flertal tjänster finns det en risk att man inte fångar fördelar av molntjänster som befinner sig i framkant i utvecklingen.

En lösning för att minska risken för att alla statliga myndigheter ska hamna hos ett fåtal leverantörer, samtidigt som möjligheten för små och medelstora leverantörers deltagande i upphandlingen ökar, är att upphandla ramavtal för olika ”storlekar” på avropande myndighet. Kammarkollegiet har till exempel i den aktuella upphandlingen av it-drifttjänster infört olika nivåer delat in anbudsområden i nivåer med olika krav på anbudsgivarnas storlek.

Det är önskvärt att krav ställs på inrapportering till Kammarkollegiet, eller annan myndighet, av aktuella avtal gällande molntjänster och andra externa it-tjänster.

6.2 Egen anskaffning av molntjänster

Det är idag oklart i vilken omfattning enskilda myndigheter har upphandlat stora avtal eller ramavtal för molntjänster. Om det överhuvudtaget förekommer är omfattningen med största sannolikhet minimal. Om många myndigheter skapar egna avtalskonstruktioner för molntjänster skulle det potentiellt kunna få effekter på nationell nivå exempelvis i termer av lägre kostnadseffektivitet. Man får inte heller per automatik samordning av säkerhetskraven som vid ett samordnat ramavtal.

En vanlig form för upphandling av molntjänster i offentlig sektor idag är direktupphandling. Molntjänster kan liksom andra tjänster upphandlas i direktupphandling så länge upphandlingen av det totala behovet inom området befinner sig under tröskelvärdet, som idag är cirka 505 000 kronor (liknande tjänster under viss avtalsperiod). En upphandlingsrelaterad utmaning som är särskilt stor för molntjänster, är att det är lätt att komma igång med en molntjänst, t.ex. vid utveckling av en ny e-tjänst. Arbetet kan starta innan slutmålet är känt.

När myndigheten sedan går från initiala analyser och enklare konstruktioner, till att addera fler funktioner, fler och större informationsmängder, utöka samverkan mellan

aktörer etc. så har förutsättningarna drastiskt ändrats. Inte bara kan man ha kommit över gränsen för direktupphandling. Man kan även ha ett läge där det krävs nya riskanalyser och en eventuell omvärdering av olika former av krav. I det läget är det inte säkert att den molntjänst man arbetar genom kan uppfylla kraven i den nya situationen.

Den variant av anslutning till molntjänster som är mest svåröverskådlig är de tjänster som enskilda medarbetare kan börja använda för hantering av myndighetens information utan föregående upphandling (vanligtvis SaaS-tjänster). Det kan röra sig om tjänster för projekthantering eller dokumentlagring. Ofta sker detta utan riskbedömning från den enskilde medarbetaren eller arbetsgivaren. It-avdelningen känner i många fall inte ens till att ett köp har skett eller att en tjänst har börjat användas, ett fenomen som brukar kallas för ”skugg-it”. Den låga tröskeln för att komma igång med en molntjänst inom framför allt mjukvarutjänster medför risker för den myndigheten och kan även ge risker på nationell nivå om många har samma beteende. Eftersom det ofta är samma tjänster det handlar om kan den totala mängden information som kommer från olika myndigheter bli mycket omfattande.

För den här typen av tjänster sluts oftast inga kundspecifika avtal. För att reducera risken i användningen är en tänkbar lösning att göra en gemensam nationell bedömning kring vilken typ av information som kan hanteras i tjänsterna, samt ta fram vägledning som innehåller stöd för hur hanteringen ska regleras i den enskilda myndigheten.

7 Krav på roller och kompetenser

Sammanfattning

Med molntjänsters intåg förändras kraven på vilka roller och vilka kompetenser som behöver finnas inom myndigheten. Personalbehovet minskar inte minst vid köp av IaaS-tjänster. Istället kan kompetens på akademisk nivå inom it behövas. It-arkitekter och verksamhetsarkitekter behöver förstå molntjänsternas möjligheter och begränsningar i verksamhetsutvecklingen. Om molntjänster kan vara aktuellt vid en upphandling blir det än viktigare med sammansatta team där såväl verksamhetsutvecklare, jurister, säkerhetsexperter och it-personal ser och förstår möjligheter med moln-tjänster, men också på ett effektivt sätt kan möta utmaningarna med lämpliga åtgärder och säkerställa en lyckad implementering och förändringsresa.

En myndighet som använder sig av molntjänster behöver se över profilen hos sin it-personal. Det krävs generellt en annan typ av personal inom myndigheten när myndigheten väljer att outsourca en verksamhet. Detta blir ännu tydligare vid köp av molntjänster.

Behovet av personal för operativ drift försvinner om inte infrastruktur och plattformar längre driftas av myndigheten själv. Den önskade profilen på personalen ändras när driftsfrågorna ändrar karaktär. T.ex. kan myndigheten behöva personal med analytisk kompetens och kunskaper på akademisk nivå inom it.

Vid köp av SaaS-tjänster minskar även behovet av teknisk personal som tillhandahåller slutanvändarapplikationer och myndighetsanpassad hårdvara, då åtkomsten till SaaS-tjänster sker via ett internetgränssnitt. It styr inte längre uppgraderingstakten av applikationer eftersom molntjänstleverantören ansvarar för uppgraderingar. Däremot

kan det krävas verksamhetsutvecklare och personal med kompetens inom förändringsledning för att säkerställa att tjänsterna och deras funktionalitet används på ett effektivt och säkert sätt inom verksamheten.

Vissa internt producerade tjänster kan baseras på teknik där myndigheten har problem att hålla egen kompetens och där konsulter måste anlitas vid uppgraderingar etc. Detta är ofta fallet då produkten är ovanlig och det endast finns ett fåtal som har efterfrågad kompetens eller då behovet inte utgör en heltidstjänst. Vid köp av molntjänst behöver inte myndigheten stå för eller upphandla denna typ av specialistkompetens.

Både verksamhetsarkitekter och it-arkitekter behöver förstå hur molntjänster kan användas i verksamhetens utveveckling och fortsatt it-uppbyggnad. Det blir centralt att kunna se helheten i en tjänst och hur olika molnlösningar och andra lösningar interagerar. Myndigheter som vill gå över till molntjänster bör därför överväga att inrätta en molntjänstansvarig arkitekt.

Behovet av beställarkompetens ökar då man planerar att anskaffa en publik molntjänst med små eller inga möjligheter att ”skruva på” tjänstens innehåll eller utförande i senare läge. Vid upphandling av standardiserad molntjänst blir varken leverantörens kunskap om den enskilda kunden, eller möjligheten att anpassa efter enskild organisation, desamma. Därför blir en god kravställan i starten ännu viktigare.

Det gäller att ha mycket god kontroll över att myndigheten sätter upp relevanta krav på bland annat tjänstens utförande, servicenivåer och säkerhet. Ett flertal olika kompetenser, ett ”molntjänstteam”, rekommenderas från start då man planerar för upphandling av en molntjänst. Teamet bör förutom it-kompetens innehålla juristkompetens inom molntjänster och avtalsfrågor för molntjänster, säkerhetsexpertis som har kunskap om verksamhetens informationsmängder och fallgropar vid molntjänster, företrädare för de verksamhetsfunktioner där utveckling ska ske eller där kundvärden ska skapas, samt också företrädare för inköpsverksamheten som har kunskap om olika kännetecken för molntjänster och hur utmaningar kan mötas i konkreta krav.

Under hela tjänstens livslängd behöver myndigheten säkerställa god avtals- och leverantörsstyrning. Eftersom marknaden för molntjänster är förhållandevis ny och utvecklas snabbt, bör myndigheten själv eller genom experter se till att hålla sig a jour med marknadsutvecklingen inom området så att nya nyttor fångas i framtida tjänsteköp[39].

[39] Key Skills Needed for Successful Deployment of Cloud Computing in Government s.1ff, Gartner (2014)

8 Marknaden för molntjänster

Sammanfattning

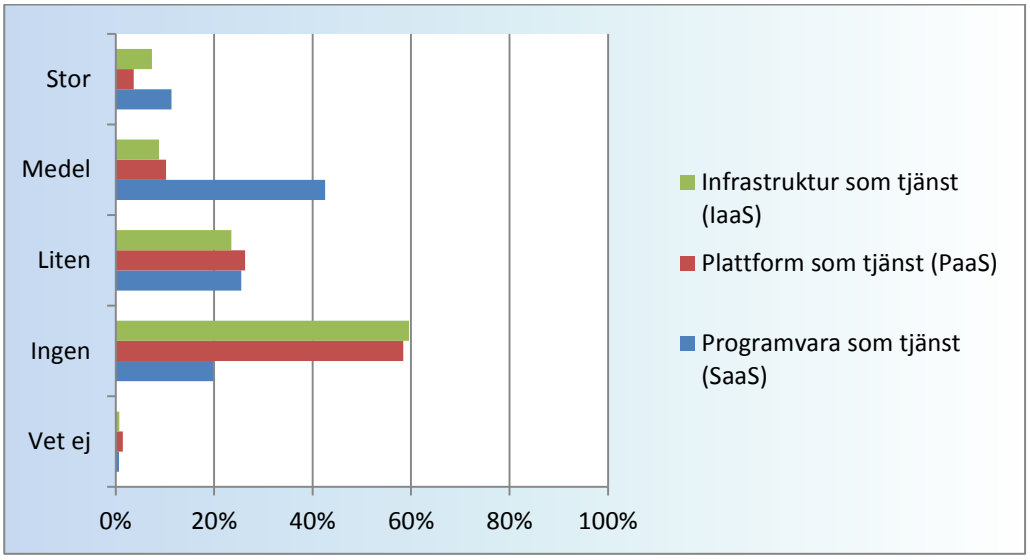
Inom offentlig sektor i Sverige har framför allt SaaS-tjänsterna fått en stor utbredning. Svenska myndigheter ser dock en stor framtida potential med molntjänster, inklusive infrastruktur- och plattformstjänster. Inom två år uppger merparten av tillfrågade myndigheter att de kommer att köpa både SaaS-, PaaS- och IaaS-tjänster. De trender som möter myndigheterna på molntjänstmarknaden är bland annat allt större datahantering och billigare IaaS-tjänster, men också fler molntjänster och standardiserade tjänster generellt. Det skapas allt fler nischade molntjänster och hybridlösningar blir allt vanligare. Molntjänsterna byggs i större utsträckning som mikrotjänster för olika funktioner. Tjänsterna rymmer också alltmer intelligens. Trenden att verksamhetens behov driver på köp av molntjänster håller i sig.

8.1 Molntjänster i statlig verksamhet

8.1.1 *Användning av molntjänster idag*

Pensionsmyndighetens myndighetsenkät ger en indikativ bild av myndigheters användning av molntjänster hösten 2015. De 148 svarande myndigheterna (79 procent av de tillfrågade med egen it-verksamhet) representerar ett ungefärligt tvärsnitt av statliga myndigheter områdes- och storleksmässigt. Flertalet svarande arbetar inom myndigheternas it-organisationer.

Undersökningen visar att drygt hälften av myndigheterna, 53 procent, har medelstor eller stor erfarenhet av Software as a Service (SaaS). För tjänstetyperna Platform as a Service (PaaS), respektive Infrastructure as a Service (IaaS) är samma värden mer modesta 15 respektive 16 procent. Totalt sett använder 77 procent mjukvarutjänster, 23 procent plattformstjänster och 26 procent infrastrukturtjänster. Det syns i exemplifieringar i svaren att myndigheternas kategorisering av vad som tillhör en viss tjänstetyp tolkas olika och kan skilja sig åt.



Tabell 6 Myndigheters erfarenhet av molntjänster

Siffrorna i vår underökning hösten 2015 skiljer sig något åt från de siffror som presenterades i E-delegationens uppföljning för 2013, där 65 procent av de svarande

uppgav att de i någon utsträckning använde sig av molntjänster för programvara, och 46 procent i någon utsträckning använde sig av molntjänster för infrastruktur[40]. E-delegationens uppföljning redovisar inte plattformstjänster separat varför en del av svaren rörande infrastruktur torde kunna avse plattformstjänster. För programvara som tjänst noteras samtidigt en ökning. Den faktiska siffran skulle kunna vara ännu högre. Användning av SaaS-tjänster drivs primärt av behov och önskemål från verksamheten utanför it-avdelningen. Eftersom fyra av fem svarande i vår enkät arbetar inom myndigheternas it-avdelningar finns det sannolikt ett mörkertal för användning av programvarutjänster som inte it-avdelningen känner till (s.k. skugg it).

Det finns få konkreta planer eller strategier framtagna som tar ställning till framtida användning av molntjänster hos den enskilda myndigheten. Det är framförallt ökad flexibilitet och minskat behov av it-kompetens som sägs driva på användning av molntjänster i statlig sektor idag, vid sidan av ekonomiska skäl som dock sällan är huvudskälet. Detta är också konsistent med hur det ser ut i näringslivet, där pendeln har svängt från fokus på kostnadseffektivitet som enda/primär drivkraft till allt fler idag betonar värdet av kort ”time to market” och innovativitet.

8.1.2 *Framtida användning*

Enkätundersökningen ger stöd för att molntjänster är en kraftigt ökande företeelse även i offentlig sektor. Av de svarande uppger hela 88 procent att de inom två år kommer att köpa SaaS-tjänster, 70 procent anger att man kommer att köpa PaaS-tjänster som molntjänster och 73 procent uppger att man kommer att köpa infrastrukturella molntjänster inom två år. Den övervägande delen av myndigheterna rör sig alltså åt det hållet. Motiv för att man framåt avser att använda molntjänster är framförallt minskade kostnader, ökad flexibilitet, ökad skalbarhet, ökad tillgänglighet, snabbare implementering och minskat behov av egen it-personal.

Den information som man under de två närmaste åren vill lägga i molnet är verksamhetsinformation med och utan kundens personuppgifter, personaluppgifter samt mer myndighetsspecifika uppgifter. Myndigheterna är ganska vaga i att beskriva exakt vilka tjänster som kan molnläggas framöver. Några respondenter nämner serverdrift, lagring och backuphantering. På programvarusidan nämns specifikt Microsoft Office365, Exchange och Lync.

8.2 Generella marknadstrender

Marknaden för molntjänster växer snabbt. Nedan beskrivs kort några aktuella trender på marknaden.

- **Datamängderna ökar samtidigt som infrastrukturella tjänster blir billigare**

Den globala datatrafiken väntas flerdubblas på några år. Datacentertrafiken växer med 25 procent årligen de närmaste åren. Molndatacentertrafiken växer samtidigt med 33 procent årligen. Molndatacenter stödjer ökad virtualisering, standardisering och automatisering.

Infrastrukturella tjänster såsom lagring och processorkraft kommer att sjunka i pris, vilket medför att aktörer som idag erbjuder infrastrukturella tjänster kommer att söka

[40] Uppföljning av myndigheternas arbete med e-förvaltning och e-tjänster 2013 s 46, E-delegationen 2013-11-05

värden längre upp i den tekniska stacken. Relationer och roller för olika bolag i it-branschen har redan börjat förändras, en företeelse som kommer att fortsätta.

Ju mer data som cirkulerar, desto viktigare kommer det också vara för köparna att försöka hålla koll på sina data. Tjänster dyker upp som siktar just på att kunden ska kunna följa var data befinner sig.

- **Fler standardiserade tjänster och fler molntjänster**

Allt fler leverantörer vill ha tjänster som kan användas av många, utan kundspecifika specialanpassningar. Många leverantörer kommer i framtiden inte att vilja uppdatera äldre kundspecifika lösningar på äldre plattformar. Detta driver sannolikt myndigheter in i molntjänster, i värsta fall illa förberedda. Samtidigt blir utbudet av molntjänster allt större och nya tjänstekategorier skapas.

- **Fler nischade molntjänster**

Vissa aktörer ser att det kommer växa fram allt fler nischade molntjänster, där kund-företag – eller myndigheter – med liknande rättsliga krav och krav på säkerhet finns i ett anpassat moln. Till exempel byggs nu infrastrukturella tjänster för försäkrings-branschen hos en svensk leverantör.

- **Intelligenta molntjänster**

Intelligensen i molntjänster förväntas öka. Vi kommer i ökad utsträckning se att inte bara tekniken i sig, utan algoritmer i molnet, ger alltmer nytta. Algoritmerna hjälper till att känna igen mönster och man kan göra blixtsnabba sannolikhetmässiga beräk-ningar samtidigt som datorn använder tidigare inhämtad kunskap. IBM:s smarta dator Dr Watson är ett exempel på artificiell intelligens. Serviceguiden Amelia som kan förstå och svara på frågor som en människa är ett annat exempel på artificiell intelli-gens som kan förändra även offentliga verksamheter.

- **Fler mikrotjänster**

Förekomsten av s.k. mikrotjänster i molntjänsterna ökar. Mikrotjänster är ett sätt att konstruera mjukvarutjänster genom att bygga program för olika funktioner vilka kommunicerar sinsemellan med t.ex. ett API. Mikrotjänsterna kan tillhandahållas och uppdateras var och en för sig. De kan manageras med hög automatik och kan lagras separerat och med redundans i olika servrar. Så kallade ”message brokers” kan knyta samman tjänsterna men även översätta mellan olika tekniska protokoll.

- **Fler hybridlösningar och fler privata moln**

Hybridstrategier, t.ex. där man i delar använder privata molntjänster och i delar publika, kommer att bli allt vanligare på marknaden. Även användningen av publika molntjänster kommer således att öka. Hybridlösningar används i vissa fall som ett ”mellansteg” där man inte kan eller vill gå direkt över till publika molntjänster med dagens ramverk och tjänsteutbud. Parallellt med hybridlösningarna sätts det också upp fler privata moln och det skapas portaler över molntjänsterna.

- **Fler direktkopplingar av tjänster mot nätverk**

Både säkerhetsaspekter och jakten på högre prestanda kan bidra till att det blir fler tjänster där man inte köper internetkopplingen separat utan som del av t.ex. en infrastruktur-tjänst. Fler leverantörer väntas använda egen fiber när man kopplar upp sig mot de stora näten.

- **Verksamheten köper it**

It och internet finns i allt. Så gott som alla verksamhetsprojekt i offentlig sektor innehåller idag it-komponenter, inte minst i ljuset av den pågående digitaliseringen. Det kommer bli allt svårare att skilja mellan vad som är it-avdelningens kostnader och vad som är verksamhetens it-kostnader. Inköpen av molntjänster från verksamhetssidan kommer att fortsätta öka. It-budgetar kan komma att vara rätt stabila över tid, medan allt mer it-investeringar görs via verksamhetsbudgeten då molntjänster blir en central del i t.ex. tjänsteutveckling.

9 Vad händer i vår omvärld?

Sammanfattning

Cloud Security Alliance är en intresseorganisation som Sverige bör följa vidare på nära håll, på såväl global som på nationell nivå. Eventuell fortsatt aktivitet i Cloud Sweden kan också vara intressant ur nationellt perspektiv. EU-nivån lämpar sig också bra för Sverige att följa och verka på i frågor som gäller t.ex. standarder och regleringsfrågor. Arbetet i Enisa, som verkar på bred front med frågor som rör säkerhet och molntjänster, är av intresse för Sverige.

Aktiviteten i det nordiska samarbetet på området tycks ha avstannat. Vi bedömer att det fortfarande kan finnas potential för samverkan på nordisk nivå i vissa frågor. Skulle det t.ex. finnas ett intresse för myndighetsgemensamma molntjänster som inte motsvaras av ett tillräckligt stort intresse från it-industrin att tillhandahålla sådana på ett kostnadseffektivt sätt, kan samarbete i nordiska molntjänster eventuellt övervägas.

9.1 Globala initiativ och nationella initiativ

9.1.1 Cloud Security Alliance

Cloud Security Alliance[41] (CSA) är en global medlemsdriven organisation vars syfte är att öka medvetenheten om, och främja användningen av, säkra molnmiljöer. CSA har en mångfacetterad verksamhet och är bl.a. aktiva inom olika forskningsprojekt huvudsakligen inriktade på säkerhet i molnet. Vidare har CSA utvecklat ett antal verktyg för att kontrollera och utvärdera säkerheten hos molntjänstleverantörer bl.a. en certifieringsmodell i tre nivåer (STAR) och en s.k. Cloud Controls Matrix, en matris för att jämföra t.ex. lagstiftningens krav med innehållet i olika standarder m.m. STAR och Cloud Controls Matrix är ramverk som bedöms intressanta för Sverige.

CSA har ett s.k. Swedish Chapter som bedriver nationellt arbete i Sverige för att öka kunskapen om molntjänster och främja utvecklingen av säkra molntjänster. Den svenska avdelningen har bl.a. tagit fram en checklista för införskaffande, användning och lämnande av molntjänster.[42]

9.1.2 Cloud Sweden

Cloud Sweden har funnits sedan år 2010 och är ett oberoende kompetensnätverk kring frågor som rör molntjänster. Cloud Sweden verkar för kvalitativ kompetens och samverkan över gränserna och nätverket har byggt upp ett kompetenscenter kring moln-

[41] https://cloudsecurityalliance.org/

[42] En praktisk och lite enklare checklista för införskaffande, användning och lämnande av molntjänster ver. 1.0, CSA , publicerad 2015-08-24

frågor som finns tillgängligt på webben.[43] På Cloud Swedens webbsidor finns dokumentation och nyheter fram till 2013. Enligt uppgift är dock nätverket fortfarande aktivt, bland annat nätverkets juridiska expertgrupp.

9.2 Europeiska unionen

EU:s strategiska ramverk och insatsområden

Grunden för EU:s arbete med molntjänster är den europeiska strategin ”Unleashing the potential of cloud computing in Europe” som presenterades 2012.

Som ett led i att förverkliga strategin och öka användningen av molntjänster i Europa har EU identifierat tre insatsområden: arbete med standarder, säkra och rimliga avtalsvillkor, samt inrättande av ett europeiskt partnerskap för molntjänster, European Partnership (ECP). Ett antal arbetsgrupper har formats för att stötta arbetet.

Nedanstående bild beskriver på ett översiktligt plan de olika delarna i EU:s samlade satsning.

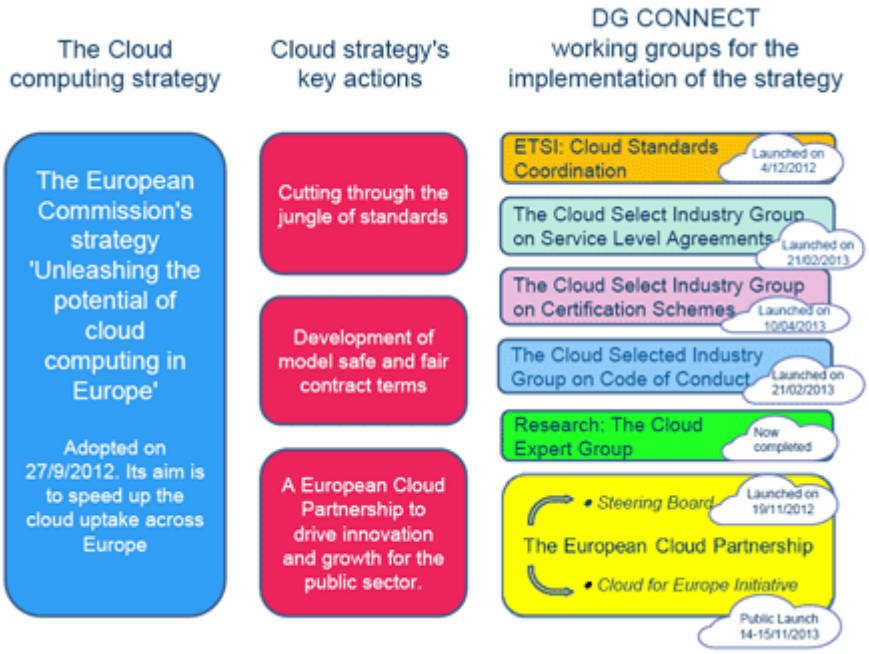


Bild 6 Insatsområden och arbetsgrupper inom EU:s satsning på molntjänster

Inom ramen för samarbetet i ECP har en strategi tagits fram, ”Establishing a Trusted Cloud Europe”.[44] I strategin betonas behovet av gemensamma ramverk och områden för europeiskt kunskapsutbyte och samverkan lyfts fram, t.ex. på områdena standarder, Code of Conduct, Fair Contracts, SLA:er och användningsfall.

Av de hittills uppnådda resultaten i de olika arbetsgruppernas insatser kan bl.a. nämnas Cloud Certification Schemes List (CCSL) som har tagits fram i samarbete med Enisa. CCSL tillhandhålls på Enisas webbplats och syftet är bl.a. att ge molntjänstkunder en överblick av befintliga certifieringar som finns tillgängliga för moln-

[43] http://cloudsweden.se/
[44] Establishing a Trusted Cloud Europe, European Cloud Partnership 2014

tjänstleverantörer att ansluta sig till eller certifiera sig mot.[45] Listan ska även kunna användas för att jämföra innehållet i olika typer av certifieringar. Vidare pågår arbete för att ta fram en uppförandekod som svarar mot bestämmelserna i dataskyddsdirektivet.

EU:s insatser ska bidra till en av unionen estimerad nettoeffekt om 2,5 miljoner jobb och en ökning av EU-ländernas BNP med c:a 160 miljarder Euro eller motsvarande en procent av BNP till år 2020. För en ekonomi som Sveriges motsvarar en procent av BNP lite under 40 miljarder kronor. I relation till den estimerade potentialen för kostnadsbesparingar av molntjänster i förvaltningen är summan betydande. Det finns goda argument för Sverige, och svenska företag, forskningssamhället m.fl. att engagera sig i utvecklingen och programmen på EU-nivå.

Enisa – den europeiska säkerhetsskyddsmyndigheten

Enisa - European Union Agnecy for Network and Information Security - är EU:s nätverks- och informationssäkerhetsbyrå. Enisa har funnits i cirka tio år. I Sverige ansvarar PTS för samordning och informationsspridning genom en National Liasion Officer. En tjänsteman från Näringsdepartementet representerar Sverige i Enisas styrelse. Organsiationen samlar även experter från industri, akademi och konsumentorganisationer. Enisa är en aktiv myndighet som tillhandahåller riktlinjer och ”good practicies”, operativt stöd m.m. till stöd myndigheter. Enisa stöder även EU i arbetet med digital agenda för Europa. På Enisas hemsida kan man som offentlig aktör bl.a. hitta nyheter och goda exempel från EU- och EFTA-länder.

EU-finansierade projekt

Ett stort antal molntjänstrelaterade projekt pågår runtom i Europa och svenska aktörer är delaktiga i vissa av dem. Inom ramen för detta arbete har det inte varit möjligt att göra en djupare ”due diligence” av olika EU-projekt. Det kan dock konstateras att det pågår ett stort antal projekt inom området. Vi beskriver några av dessa projekt nedan.

- **Cloud for Europe** stöder användning av molntjänster i offentlig sektor genom samarbete mellan myndigheter och industri. Projektet identifierar hinder för användning av molntjänster och använder innovationsupphandling som instrument för att hitta lösningar som stöder tilliten till, och ökar nyttan av, molntjänster. Ytterligare ett syfte är att ge offentliga upphandlare bättre information om hur molntjänster kan användas i offentliga verksamheter.
- **A4Cloud –** Cloud Accountability Project förenar industri, forskning - däribland Karlstads universitet - och Cloud Security Alliance. Projektet ska bl.a. ge medborgare möjlighet att kontrollera hur deras personuppgifter används av företag och organisationer och ge medborgarna möjlighet att se till att deras personuppgifter inte används på otillåtna sätt, för ändamål som de inte har godkänt eller att de sprids till obehöriga.
- **PICSE** [46] (Procurement Innovation for Cloud Services in Europe) är ett projekt vars främsta syfte är att ta fram en plattform för upphandlande myndigheter och enheter i unionen och att öka kunskapen, användandet och förståelsen för upphandling av molntjänster.

[45] https://resilience.enisa.europa.eu/cloud-computing-certification
[46] http://www.picse.eu/

Både Cloud for Europe, A4Cloud och PICSE är projekt inom områden som torde vara av högt intresse för Sverige och svenska myndigheter att följa – såväl att se hur upphandling av molntjänster kan underlättas på ett sätt så att mervärde skapas, samt att se hur individers personuppgifter kan följas, är centrala frågor för ökad användning och bättre nyttiggörande av fördelarna med molntjänster.

Ytterligare några exempel på EU-finansierade projekt inom området molntjänster är följande:

- **CREDENTIAL** är ett forskningsprojekt som genom avancerad krypteringsteknologi och starka autentiseringsmekanismer ska förbättra integritetsskyddet i molntjänster. [47]
- **Prisma Cloud** är ett projekt som arbetar med säkerhetslösningar genom kryptering och krypteringsmetoder, där syftet är att förbättra säkerhet och integritetsskydd ”end-to-end”. [48]
- **SPECS** (Secure Provisioning of Cloud Services based on SLA Managements) är ett projekt som syftar till att utveckla och implementera ett ramverk för öppen källkod för molntjänsten Security as a Service (PaaS-tjänst).[49] SPECS ska tillhandahålla verktyg för att förhandla säkerhet i molntjänsters Service Level Agreements, att följa upp efterlevnad i realtid och att kunna agera när de avtalade säkerhetsnivåerna inte möts.
- **SLA Ready** är ett projekt som vänder sig till små och medelstora företag och som ska ge dessa verktyg för att planera och driva igenom säkerhetskrav genom praktiska vägledningar, utbildningsmaterial och en social marknadsplats för erfarenhetsutbyte m.m.[50]
- **Cumulus project** syftar till att utveckla modeller, processer och verktyg som kan stödja säkerhetscertifieringar av IaaS-, PaaS- och SaaS-tjänster.[51]

9.3 Nordiska ministerrådet

Även på nordisk nivå har frågan om molntjänsters användning och betydelse för inte minst offentlig sektor lyfts. Nordiska ministerrådet släppte 2011 rapporten *Nordic Public Sector Cloud Computing – a discussion paper*[52] som tagits fram inom ramen för en nordisk arbetsgrupp och efter intervjuer av bl.a. it-chefer och it-strateger i nationella och kommunala offentliga organisationer i de olika länderna. Sverige deltog i arbetsgruppen med expertis från Kammarkollegiet. Vissa informationsfilmer har också tagits fram på nordisk nivå.

I rapporten från 2011 identifierades en rad nyttor med molntjänster och man konstaterade att de nordiska länderna skulle kunna övervinna hinder för övergång till molntjänster genom ett närmare samarbete och genom att ta fram en gemensam nordisk strategi eller policy för molntjänster. Därtill föreslogs insatser inom fem

[47] http://credential.eu/
[48] https://prismacloud.eu/
[49] http://www.specs-project.eu/
[50] http://slaready.eu/
[51] http://cumulus-project.eu/
[52] Nordic Public Sector Cloud Computing – discussion paper, Tema Nord 2011:566

områden: kunskapsdelning, regelverk, standardisering, upphandling samt insatser för att attrahera datacenter till de nordiska länderna.

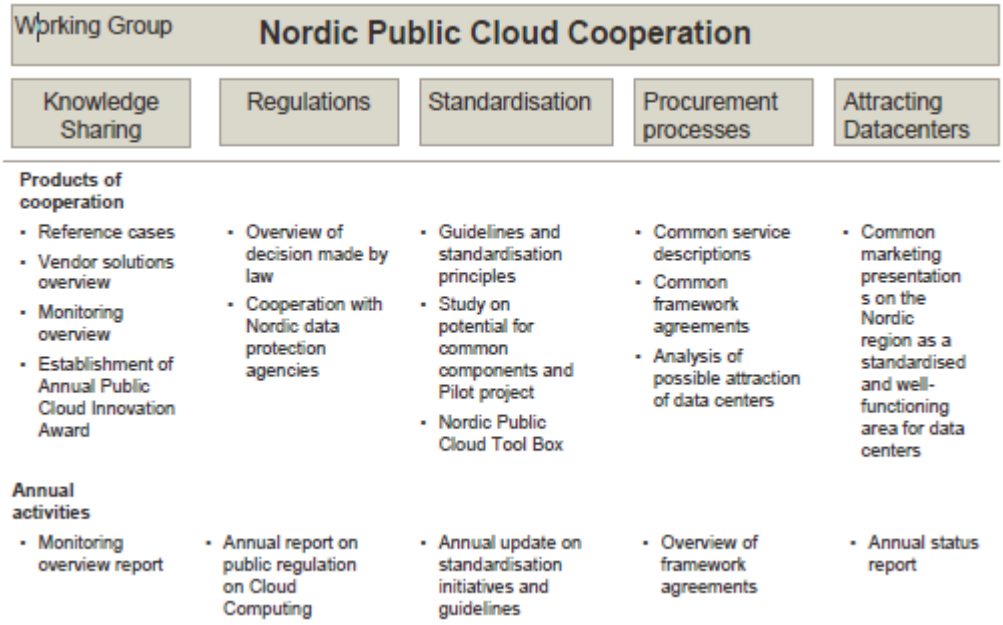


Bild 7 Förslag på nordiskt samarbete med insatser inom fem områden (2011)

Såvitt vi i denna utredning har kunnat se har få – om några – av de föreslagna gemensamma insatserna hittills förverkligats. Flera av förslagen behåller dock sin relevans än idag.

9.4 Sverige och den internationella arenan

Cloud Security Alliance är en intresseorganisation som är intressant för den svenska staten att följa vidare på nära håll, på såväl global som på nationell nivå. Sverige deltar också i flera EU-projekt. Inom ramen för detta arbete har det inte varit möjligt att göra en djupare ”due diligence” av olika EU-projekt. Det kan dock konstateras att det pågår ett stort antal forsknings- och utvecklingsprojekt som delvis är EU-finansierade. Även Enisa arbetar på bred front med frågor som rör säkerhet och molntjänster. EU-nivån lämpar sig också bra för Sverige att följa och verka på i frågor som gäller t.ex. standarder och regelringsfrågor.

Det kan fortfarande finnas potential för samverkan på nordisk nivå i vissa frågor. Skulle det finnas ett myndighetsintresse för statliga molntjänster som inte motsvaras av ett tillräckligt stort intresse från it-industrin att tillhandahålla sådana på ett kostnadseffektivt sätt, kan eventuellt överväga samarbete i nordiskt moln eventuellt övervägas.

Slutsatser och förslag

10 Slutsatser

10.1 Molntjänster - en ny generation av outsourcing

Molntjänster är inte längre något nytt. Framväxten av molntjänster är ett naturligt utvecklingssteg inom it-branschen, ett steg som på ett radikalt sätt kan förändra förutsättningar för offentliga aktörer att fullgöra sina uppdrag och utveckla sina tjänster och verksamheter. Det är därför viktigt att myndigheter och andra statliga aktörer utvecklar tydliga strategier för om, och hur, man kan använda molntjänster för att förnya och utveckla svensk förvaltning. Att köpa molntjänster är ett nytt sätt att köpa externa tjänster, och därmed en ny form av outsourcing som ställer nya krav på organisationerna.

Molntjänster rymmer viktiga potentiella nyttor för myndigheter, enskilt och i samverkan. Molntjänster som företeelse är här för att stanna. Vi ser att användningen av molntjänster kommer att öka i både privat och offentlig sektor i Sverige. För framför allt små och medelstora företag, liksom små och medelstora myndigheter, kan vinsterna vara särskilt stora. Molntjänster innebär ett nytt sätt att köpa it-tjänster, eller om man så vill en ny generation av outsourcing. Molntjänster understryker som vi har visat vikten av att arbeta med tvärfunktionella team i upphandlingsfasen, men påverkar också vilka kompetenser och roller som finns kvar på it-avdelningen efter att anskaffningen är gjord.

Att köpa it som molntjänster kan ge nyttor i form av flexibilitet och skalbarhet, innovativitet, nya affärsmöjligheter, snabbhet, kostnadseffektivitet, kompetensfördelar och fördelar i termer av säkerhet. Fördelarna kommer dock inte automatiskt utan måste som vid all anskaffning föregås av tydliga strategiska och taktiska rambeslut och en grundlig juridisk analys.

10.2 Potential i molntjänster med rätt strategi

Molntjänster kan se ut och distribueras på olika sätt, och utvecklingen inom området står inte stilla. Till exempel ser vi nu hur s.k. mikrotjänster, dvs. komponenter av mjukvarutjänster som vardera levererar en viss funktionalitet och som liksom ”traditionella” molntjänster tillhandahålls nätbaserat, vinner mark. När myndigheter väljer sin strategi för molntjänster bör det ske noggrant, alltid utifrån verksamhetens ram och utifrån de förutsättningar som olika typer av tjänster vid varje tillfälle kan ge.

En strategi för molntjänster kan t.ex. vara en del av en större strategi för hur myndigheten ser på att använda sig av externa it-leverantörer (sourcingstrategi) och myndighetens strategi för it, vilken i sin tur bör vara kopplad både till myndighetens uppdrag och verksamhetens inriktning och behov inklusive de specifika lagar och regler som myndigheten har att följa. I en strategi för it som t.ex. ger följande prioritering för investeringar i it: ”1. Återanvänd => 2. Köp tjänst => 3. Bygg själv”, så skulle steget ”Köp tjänst” kunna ersättas med ”Köp som molntjänst där så är tillämpligt”.

Att göra rättvisande kostnadskalkyler för molntjänster är svårt om steget är långt mellan nuläget med den befintliga it-miljön och det nyläge man förväntar sig att nå med hjälp av molntjänster. Nya typer av (direkta och indirekta) värden kan adderas med en molntjänst jämfört med vad gamla system och plattformar kan erbjuda. Samtidigt kan det finnas interna kostnader förknippade med att övergå till användning av en molntjänst som inte direkt härrör till anskaffningen av själva molntjänsten. Det är vanligen enklare, och mest rekommenderat, för den som vill gå över till moln-

baserade tjänster att starta med nya tjänster där man inte sitter fast i äldre it-system (s.k. ”legacy”).

Vi har också visat på att olika verksamheter och olika delar av verksamheter lämpar sig olika bra för molntjänster. I slutändan är det bara verksamheten själv som, med stöd av en rättslig analys och verksamhetsorienterad analys kan avgöra vilken verksamhet och vilken information som kan hanteras ”i molnet”. Lite förenklat kan man säga att det är enklare att flytta information till molntjänster ju mindre känslig informationen är, ju mer självständig en applikation är och ju större variationer i kapacitet det finns över tid, dvs. desto större potential för besparingar finns det.

Förberedelser för användning av molntjänster innebär att myndigheten analyserar sin it-portfölj, de juridiska förutsättningarna och sätter verksamhetsrelaterade mål för användning av molntjänster över tid. Det innebär också att myndigheten ska ha infört LIS, klassificerat sin information och analyserat skyddsvärdet av olika typer av information. Det kan också innebära att man standardiserar serverparken, virtualiserar, genomför strategisk automatisering eller skapar tydliga gränssnitt vid systemintegrationer med s.k. containerkoncept.

I ett första steg kanske myndigheten skapar ett internt moln. Exakt vilka förberedande åtgärder som behöver vidtas för att få en effektiv övergång till en eller flera molntjänster avgörs av respektive myndighet. När myndigheten inom ramen för säkerhetsarbetet gör en risk- och sårbarhetsanalys bör den ta hänsyn till specifika risker med olika typer av molntjänster. På så sätt kan riskerna också mötas med åtgärder, t.ex. kryptering och anonymisering, och man kan ställa krav som styr mot ”rätt” typ av molntjänst och modell för tillhandahållande.

10.3 Vikten av balans och relevanta alternativ

Vår analys visar att det inte är möjligt eller önskvärt att kategoriskt säga att en viss typ av information alltid eller aldrig kan hanteras i en molntjänst. Svaret på frågan beror dels på vilken typ av molntjänst och tillhandahållande som man talar om, dels vilken typ av information som ska hanteras och för vilket verksamhetsändamål den ska användas. Verksamhetsansvarig myndighet måste alltid göra en egen analys utifrån tolkningen av uppdraget, valet av verksamhetsstrategi, strategi för it samt egna rättsliga bedömningar.

Ansvaret för avgörandet vilar på ledningen i den aktuella verksamheten. Eftersom molntjänster kan vara av så strategisk karaktär för verksamhetens utveckling bör frågan om hur molntjänster kan användas i verksamhetsutveckling tas upp till diskussion i myndighetens ledningsgrupp.

I många fall handlar det om att hitta en balans mellan nyttor som innovativitet, snabbhet, flexibilitet och kostnadseffektivitet, med vad som är juridiskt möjligt och säkerhetsmässigt motiverat. Viktigt att betona är att säkerhetsaspekter lika gärna kan tala till molntjänsternas fördel.

Vi har sett att det är svårt för myndigheter att använda framför allt publika molntjänster i vissa lägen. Det gäller t.ex. när uppgifter är sekretessreglerade och inte får lämnas ut, situationer där en molntjänstleverantör inte kan anses uppfylla personuppgiftslagens krav på insyn och kontroll, eller där avtalsvillkor medger leverantörsbehandling av personuppgifter för egna ändamål. Andra försvårande omständigheter kan vara att molntjänstleverantören inte kan uppfylla arkivlagens krav på bevarande eller gallring eller att leverantören inte uppfyller andra lämplighets- eller laglighets-

prövningar, t.ex. den speciallagstiftning som myndigheten har att följa. Hybrida lösningar, privata molntjänster och s.k. partnermoln kan dock vara värdefulla alternativ där publika molntjänster inte är möjliga, och fortfarande ge intressanta fördelar i form av kostnadseffektivisering, bättre tjänster, flexibilitet och skalbarhet som man annars vanligen söker i de publika tjänsterna.

Vi befinner oss i ett läge där det råder oklarhet och osäkerhet kring hur skyddad information/data är i andra länder, både inom och utanför EU:s gränser. Både geografi, dvs. land som valts för fysisk lagring, och leverantörens nationella hemvist kan spela en roll för om främmande makt kan ta del av information. Statliga myndigheter behöver samtidigt ställa höga krav på säkerhet och, när det kommer till hantering av data, säkra ett fullgott skydd av sina medborgares personuppgifter. Detta medför en rad säkerhetskrav och andra krav som standardiserade molntjänster och leverantörer med publika molntjänster inte alltid kan leva upp till.

10.4 Efterfrågan på myndighetsmoln

Fortfarande finns osäkerheter kring hur skyddat ett lands data egentligen kan vara om de lagras utanför Sverige. Det har konstaterats att Safe Harbor-överenskommelsen mellan EU och USA har fallit i och med att EU-domstolen inte bedömer att den ger tillräckligt skydd av personuppgifter. Flera aktörer har kommit fram till eller kommer att komma fram till att steget är för stort för att kunna hantera hela eller delar av sin information i en global molntjänst.

Under arbetet med uppdraget har det visat sig att många aktörer är positiva till – och efterfrågar – centrala satsningar för att stötta användningen av molntjänster och till centralt tillhandahållna molntjänster där myndigheter skulle ha möjlighet att ansluta sig utan egen upphandling. En positiv inställning till en svensk satsning på gemensamma statliga molntjänster visar sig i enkätsvar och i samtal med såväl myndigheter som leverantörer, forskare och expertorganisationer. Vissa aktörer lyfter även ett nordiskt samarbete kring molntjänster som en möjlighet, eftersom de nordiska länderna har en historia av samarbete och liknande offentlig kultur. En initial bedömning är att ett svenskt myndighetsmoln, som följer svensk lagstiftning, vore lättare att åstadkomma än ett nordiskt myndighetsmoln.

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. Om handlingarna innehåller personuppgifter bör t.ex. absolut sekretess enligt offentlighet- och sekretesslagstiftningen gälla hos värdmyndigheten.[53] Det bör vidare vara möjligt att lagreglera att annan information som hanteras av värdmyndigheten inom ramen för ett myndighetsmoln ska omfattas av absolut sekretess hos värdmyndigheten. Samtidigt kan man införa en ny sekretessbrytande bestämmelse som gör det tydligt att även uppgifter som omfattas av absolut sekretess kan lämnas ut, av den uppdragsgivande myndigheten, till värdmyndigheten.

[53] 40 kap. 5 § OSL föreskriver att sekretess gäller i verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon annans räkning av personuppgifter som avses i personuppgiftslagen (1998:204) för uppgift om en enskilds personliga eller ekonomiska förhållanden.

Om driften av myndighetsmolnet överlämnas till privaträttsliga aktörer, skulle en lagreglerad tystnadsplikt kunna införas även för dem som i sitt arbete hos sådana aktörer tar del av myndigheternas uppgifter.[54]

10.5 Juridiken upplevs onödigt hindrande

Vår genomgång av de centrala juridiska frågorna har visat att det normalt inte finns någon specifik bestämmelse som i sig alltid utgör ett hinder för en myndighet att använda molntjänster. Samtidigt visar svaren i den enkät som gått ut till samtliga statliga myndigheter att det ofta är de juridiska frågeställningarna som är särskilt problematiska för en myndighet att lösa vid ett planerat inköp av en molntjänst. Vi bedömer att myndigheterna upplever en osäkerhet kring juridiska frågor som rör digitalisering i allmänhet och molntjänster i synnerhet samt att det saknas en tydlighet i hur regelverket ska tolkas och tillämpas. En orsak är att de regelverk som ska appliceras är tämligen komplexa och omfattande. Vidare handlar tillämpningen av regelverken ofta i praktiken om att säkerställa en rimlig balans mellan behovet av integritetsskydd och effektivitet vilket är en grannlaga uppgift.

Vi bedömer också att en mycket väsentlig orsak till att myndigheterna upplever att det finns juridiska hinder eller i varje fall stora svårigheter att använda molntjänster är en bristande utveckling av regelverken. Tekniken har utvecklats på närmast explosionsartat sätt som ingen kunde förutse bara för ett tiotal år sedan. Samtidigt har inte något samlat grepp tagits i fråga om de regelverk som ska tillämpas för att myndigheterna ska kunna realisera potentialen i den nya tekniken. Detta har inneburit beaktansvärda svårigheter för myndigheterna att kunna hänga med i utvecklingen, eftersom de är tvungna att tillämpa otidsenliga författningar inom ett svåröverblickbart och fragmenterat rättsområde med bristande enhetlighet och struktur och normtekniska lösningar.

Under senare tid har ett antal förslag lagts fram som, om de genomförs, också kan komma att underlätta användningen av molntjänster. E-delegationen har i sitt slutbetänkande (SOU 2015:66) pekat på ett antal faktorer som nödvändiga förutsättningar för att nå målen för e-förvaltningsutvecklingen. Vissa av dessa faktorer är relevanta även för myndigheters möjligheter att fullt ut kunna tillgodogöra sig potentialen i molntjänster. Här kan bl.a. nämnas lagstiftarens förmåga att omhänderta och driva på nödvändiga författningsändringar och att det finns ett behov av balans mellan effektivitet och integritet. En ytterligare lagstiftningsåtgärd som skulle kunna underlätta för en myndighet att uppdra åt en privat aktör att hantera myndighetens information är, som vi beskrivit ovan, att införa en lagreglerad tystnadsplikt för privata aktörer.

Vidare vill vi framhålla förslaget till ny myndighetsdatalag (SOU 2015:39) som bl.a. tydliggör under vilka förutsättningar ett personuppgiftsbiträde får anlita en underleverantör och vilka krav som ställs på myndighetens arbete med säkerhet för att skydda personuppgifterna som behandlas. Personuppgiftsbiträden har funnits sedan länge men fått en annan roll i och med att styrkeförhållandet mellan parterna har

[54] Författningsbestämmelser om tystnadsplikt för personal i privaträttsligt bedriven verksamhet finns bl.a. i 29 kap. 14 § skollagen (2010:800), 15 kap. 1 § socialtjänstlagen (2001:453), 6 kap. 12 § patientsäkerhetslagen (2010:659) och 15 § lagen (1997:736) om färdtjänst, avseende enskilt bedriven skolverksamhet, socialtjänst, hälso- och sjukvård respektive färdtjänst.

förändrats t.ex. när en personuppgiftsansvarig myndighet anlitar en global moln-tjänstleverantör. Av denna anledning är det viktigt för myndigheter att kunna peka på konkreta och tydliga lagkrav som måste uppfyllas av leverantören för att myndigheten ska kunna använda den aktuella tjänsten. Ett genomförande av förslaget till ny myndighetsdatalag skulle också innebära att den splittrade lagstiftningstekniken inom området för myndigheternas personuppgiftsbehandling åtgärdades. Genom att tillämpa samma lag eller åtminstone lagar som har samma lagstiftningsteknik och systematik skulle mycket vara vunnet i och med att kunskapsutbytet och kunskapsåtervinningen rörande tillämpningen skulle kunna öka avsevärt.

Det finns alltså ett behov av att regeringen hanterar vissa lagstiftningsfrågor som påverkar den framtida utvecklingen och användningen av molntjänster. Myndigheter ska ha förutsättningar att kunna utföra sitt uppdrag på ett effektivt och rättssäkert sätt och därför behöver det säkerställas att regelverken som myndigheterna ska tillämpa inte hindrar detta på grund av bristande systematik och olika normtekniska lösningar. Med tanke på den snabba tekniska utvecklingen är det viktigt att det finns en bra beredskap att hantera behoven av lagstiftningsåtgärder vartefter de uppstår.

11 Förslag

Pensionsmyndigheten kan enligt uppdragsbeskrivningen återkomma till regeringen med förslag på åtgärder för att potentialen i molntjänster ska realiseras. Mot bakgrund av ovanstående rapport, analyser och slutsatser föreslår vi följande åtgärder till regeringen.

11.1 Klargör regeringens viljeriktning - ett myndighetssverige som är ”cloud ready”

Uppdra till svenska myndigheter att analysera hur man kan använda externa tjänster, och att däri beakta om och i så fall under vilka förutsättningar som myndigheten kan använda sig av molntjänster, för att fullt ut använda digitaliseringens möjligheter och åstadkomma enkla och effektiva tjänster, en öppnare förvaltning samt kostnads-effektivitet i statens it.

Sveriges mål är att vara bäst i världen på att använda digitaliseringens möjligheter. Molntjänster kan bidra till att vi kan nå det målet. Aktörer i olika roller lyfter vikten av att Sverige på ett nationellt plan tydliggör vad som är *möjligt* och vad som är *önskvärt* när det kommer till statliga aktörers användning av molntjänster. Även om det inte kan ses som önskvärt att regeringen tar beslut kring användningen av it-tjänster för enskilda myndigheter, ska inte vikten av generell signalverkan från regeringen underskattas när det gäller att få igång myndigheternas arbete med att tillvarata fördelar av molntjänster.

Om en myndighet i sin analys kommer fram till att molntjänster på sikt kan användas för hela eller delar av sin verksamhet, behöver myndigheten förbereda sin verksamhet - göra sig ”cloud ready”. Regeringen bör uppmuntra myndigheter i Sverige att göra sig redo för övergång till molntjänster där så är möjligt.

När det gäller nya tjänster eller nya verksamheter eller små myndigheter, finns det skäl att särskilt överväga möjligheten att i första hand lösa behovet av tjänster genom användning av skalbara molntjänster. Detta bör vara en föredragen väg framför att bygga en egen it-infrastruktur eller köpa alternativt utveckla egna applikationer. Finns

inte ett it-arv som försvårar den digitala transformationen skulle det logiska resultatet kunna bli att myndigheten i första hand upphandlar molntjänster.

11.2 Inrätta kompetenscenter för anskaffning och användning av externa it-tjänster

Utse en myndighet eller annan aktör som ska tillhandahålla ett kompetenscenter för vägledning och kunskapsutbyte mellan myndigheter i frågor som rör anskaffning och användning av externa it-tjänster. Kompetenscentret ska ge stöd och vägledning till offentliga aktörer i statlig, kommunal och landstingskommunal sektor samt till potentiella leverantörer. Kompetenscentret ska även agera nod för ett nationellt myndighetsnätverk för molntjänster.

Att arbeta med molntjänster kräver bred insikt från en offentlig organisation i tekniska, juridiska, säkerhetsrelaterade och ekonomiska frågor. Det behövs också en förmåga i organisationen att förstå hur montjänster kan användas i affärs- eller verksamhetsutveckling. Samtidigt förekommer en rad olika internationella riktlinjer, standarder och certifieringar. För många myndigheter, särskilt de mindre, är möjligheterna att följa utvecklingen på området begränsade.

För att tillvarata potentialen i molntjänster behöver myndigheter i alla sektorer kunna få stöd och vägledning när de ska köpa externa tjänster. Kunskapen som samlas i ett kompetenscenter behöver vara både bred och djup. Stödet behöver vara både flexibelt och kraftfullt och kräver en organisation för löpande förvaltning. Den aktör som utses som ansvarig bör ha egen erfarenhet av operativ it och erfarenhet av alla perspektiv på externa tjänster – juridik, säkerhet, teknik, organisation m.m. Samarbete bör ske med bl.a. MSB för praktiskt stöd inom området säkerhet. Det bör finnas möjlighet för nyckelpersoner inom it-avdelningar, jurister, säkerhetsexperter, verksamhetsutvecklare m.fl. att söka konsultativt stöd hos kompetenscentret.

Som en del i satsningen på ett kompetenscenter ska den ansvariga aktören tillhandahålla en webportal där man samlar information om internationella standarder, riktlinjer, juridiska och säkerhetsrelaterade vägledningar, avtalsexempel, information om internationella certifieringar m.m. Där bör också finnas aktuell information om EU-projekt och nyheter om andra aktiviteter av intresse på EU-nivå och internationellt. Portalen bör även kunna tillhandahålla blogg eller digitala grupperingar där myndigheter kan utbyta erfarenheter från inköp av molntjänster och erfarenheter av implementeringsprocesser. Till kunskapscentret ska ett nationellt nätverk mellan kontaktpersoner för molntjänstfrågor på olika myndigheter knytas.

11.3 Analysera myndigheters digitala mognad

Uppdra till en alternativt flera myndigheter att analysera svenska myndigheters digitala mognad. I analysen ska ingå att kartlägga om och hur myndigheterna avser att använda molntjänster för att fullt ut använda digitalisringens möjligheter och åstad-komma enkla och effektiva tjänster, en öppnare förvaltning samt kostnadseffektivitet i statens it. Analysen ska omfatta en genomgång av myndigheternas strategier, organi-satoriska mognad och operativa beredskap.

Ekonomistyrningsverket (ESV) fick i regleringsbrevet för 2015 i uppdrag att följa upp digitaliseringen i staten. Det finns ett behov av ett liknande uppdrag kring uppföljning av hur myndigheter använder sig av externa tjänster inklusive molntjänster, och vilken mognad de har för att göra det.

I en analys av digital mognad ska ingå att följa upp förekomsten av strategier för it och sourcingstrategier på respektive myndighet, och att i samband med detta kartlägga om och hur myndigheterna avser att använda molntjänster. Den organisatoriska mognaden, inklusive tydliga roller och ansvar, ska granskas, liksom den operativa beredskapen och de operativa förberedelserna.

Analysen ska även ge svar på i vilken utsträckning myndigheterna har implementerat ett ledningssystem för informationssäkerhet (LIS), inklusive genomförande av informationsklassning och identifiering av skyddsnivåer för sin information som svarar mot kraven på molntjänster, samt gjort nödvändiga rättsliga analyser.

Den sammantagna analysen ska ge svar på i vilken utsträckning myndigheterna är ”cloud ready” dvs. i vilken utsträckning det finns förutsättningar att ta tillvara fördelar av molntjänster såväl på myndighets- som nationell nivå. Analysen utgör ett verktyg för benchmarking även mellan myndigheter. Resultatet av analysen ska förvaltas över tid. Tillvägagångssättet behöver därför medge mätbarhet över tid eftersom den eller de ansvariga även bör göra uppföljningar, så att regeringen kan följa progressen för statlig it-mognad i sin helhet och ha möjlighet att agera utifrån den bild som framkommer.

11.4 Genomför en fördjupad analys av statliga myndighetsmoln

Fördjupa analysen av förutsättningarna för att inrätta ett eller flera statliga myndighetsmoln och myndighetsgemensamma tjänster i Sverige. I uppdraget ska ingå att bedöma om statliga myndighetsmoln bör byggas på en myndighetsgemensam informations- och kommunikationsinfrastruktur. Den fördjupade analysen bör beakta specifika behov och möjligheter för olika typer av tjänster. Behoven bör belysas utifrån rättsliga och verksamhetsmässiga förutsättningar för myndigheter som befinner sig inom olika delsektorer samt ta ställning till olika alternativ för tillhandahållande och drift. Analysen ska ta hänsyn till internationella erfarenheter på området.

Mot bakgrund av dagens juridiska och säkerhetsmässiga förutsättningar och trösklar för att börja använda molntjänster ser vi en risk för en fortsatt långsam utveckling av användningen av molntjänster i Sverige. Särskilt små och medelstora myndigheter riskerar att halka efter i den snabba utvecklingen där it ofta står för en allt större del av myndigheternas totala kostnader. Samtidigt framkommer att det finns ett positivt intresse för statliga satsningar på myndighetsmoln hos myndigheter, leverantörer och andra aktörer.

Statliga myndighetsmoln, s.k. ”gov cloud”, skulle kunna ge möjligheter att lösa utmaningarna med molntjänster även då det är sekretessbelagd information som hanteras.

I den fördjupade analysen ska man bedöma om och hur en eventuell myndighetsgemensam informations- och kommunikationsinfrastruktur, ett s.k. ”gov net”, kan användas för statliga molntjänster, som ett sätt att utveckla och upprätthålla en god informationssäkerhet samt för att få god funktionalitet och kostnadseffektivitet. Analysen ska även omfatta en bedömning av om det finns behov av krav på certifiering samt föreslå övergripande kriterier för myndigheters anslutning. Analysen ska även beakta de juridiska aspekterna och eventuella behov av lagändringar.

Vid förslag på mjukvarutjänster som kan tillhandahållas i ett statligt myndighetsmoln ska regeringens ambitioner avseende samverkan inom e-förvaltning och utveckling av digitala tjänster tas tillvara.

11.5 Utred en lagreglerad tystnadsplikt för privata leverantörer av it-tjänster

Utred om det är lämpligt och ändamålsenligt att införa en lagreglerad och straffsanktionerad tystnadsplikt för privata leverantörer av it-tjänster, i syfte att underlätta för myndigheter att uppdra åt dessa aktörer att hantera myndighetens sekretessreglerade information.

Myndigheter behöver kunna anlita privata leverantörer av it-tjänster för att kunna få kostnadseffektiva och moderna it-lösningar som stödjer verksamhetens utveckling. I dagsläget kan offentlighets- och sekretesslagens bestämmelser hindra myndigheter från att lämna ut vissa typer av sekretessbelagda uppgifter till privata it-leverantörer eftersom det saknas straffrättsligt sanktionerade tystnadsplikter för anställda hos sådana aktörer. Det handlar t.ex. om uppgifter av särskilt integritetskänsligt slag som rör enskilda och som inte bedöms kunna lämnas ut ens om leverantören och dess anställda ingår en avtalsrättslig tystnadspliktsförbindelse.

Om leverantören i stället lyder under en i lag reglerad och straffsanktionerad tystnadsplikt borde det ges större utrymme för myndigheten att lämna ut uppgifterna till leverantören, utan hinder av sekretess, och om det i övrigt är lämpligt, eftersom risken för att uppgifterna obehörigen sprids torde vara relativt låg. Vi anser att regeringen ska överväga att låta utreda närmare om det är lämpligt och ändamålsenligt att införa en lagreglerad och straffsanktionerad tystnadsplikt för privata leverantörer av it-tjänster.

11.6 Prioritera en översyn av myndigheternas registerförfattningar

Prioritera en översyn av myndigheternas registerförfattningar och genomför nödvändiga författningsändringar för att säkerställa att myndigheterna ges bättre förutsättningar att utföra sina uppdrag på ett effektivt och rättssäkert sätt.

Myndigheterna ska ha förutsättningar att kunna utföra sitt uppdrag på ett effektivt och rättssäkert sätt. Det behöver därför säkerställas att regelverken som myndigheterna ska tillämpa inte hindrar effektivitet och rättssäkerhet på grund av bristande systematik och olika normtekniska lösningar. Myndigheterna upplever en osäkerhet kring juridiska frågor som rör digitalisering i allmänhet och molntjänster i synnerhet. Det är i varierande grad otydligt för myndigheterna hur regelverken ska tolkas och tillämpas.

I ljuset av den nya dataskyddsförordningen framstår det som än mer angeläget att regeringen prioriterar frågan om en översyn av myndigheternas registerförfattningar. Översynen bör ske samlat och med lika utgångspunkter när det gäller systematik och författningsteknik. Förslaget till en ny myndighetsdatalag bör kunna utgöra en utgångspunkt för en sådan samlad översyn.

11.7 Genomför en analys av nationella risker och ge förslag på åtgärder

Ge MSB i uppdrag att genomföra en initial fördjupad riskanalys av molntjänstanvändning och användning av andra externa it-tjänster utifrån ett nationellt perspektiv. I uppdraget ska ingå att analysera och beskriva hur informationen om den samlade bilden av myndigheternas externa it-tjänster bäst kan användas för att reducera risker på nationell nivå.

Att svenska myndigheter bedriver ett strukturerat informationssäkerhetsarbete blir alltmer centralt. Som nämnts ovan finns det ett behov av att stärka myndigheternas arbete med informationssäkerhet. Det finns parallellt med detta ett behov av att stärka arbetet med informationssäkerhet på ett nationellt plan för att åstadkomma ökat samhällsskydd.

Hur mycket information av en viss typ eller en viss informationsklass som finns samlat hos en specifik leverantör är idag inte känt, varken av de enskilda myndigheterna eller av någon central aktör såsom MSB. I takt med att allt fler offentliga verksamheter outsourcar sin it och att vi ser en allt större användning av molntjänster och andra former av outsourcing blir det viktigt att anlägga en samhällsskyddsaspekt som tar hänsyn till en nationell bild av säkerhetsläget.

En riskanalys ska inte endast analysera riskerna vid användning av molntjänster utan även göra en bedömning i förhållande till andra alternativ att hantera de funktioner som molntjänster kan användas till. I det sammanhanget är det viktigt att även lyfta fram de fördelar ett användande av molntjänster kan ge.

Riskanalysen ska väga de identifierade riskerna för molntjänster mot risker vid andra alternativa it-lösningar. Som alltid vid beslut om åtgärder utifrån riskanalyser måste man sedan även väga riskerna mot de potentiella nyttorna.

11.8 Stärk det svenska engagemanget i internationella forum

Intensifiera Sveriges närvaro i frågor som rör molntjänster i EU och andra internationella sammanhang. Ett tvärpolitiskt arbetssätt som stöder olika politikområden rekommenderas.

Tydliga argument för molntjänster står att finna både inom tillväxt- och näringspolitiken, inom handelspolitiken och inom förvaltningspolitiken. Som exempel kan nämnas regeringens it-politiska mål och ambitioner avseende utveckling av en digital förvaltning med ”digitalt först”, satsning på enkla och effektiva tjänster, samt kostnadseffektivitet i statens it. Uppdraget har visat att molntjänster kan vara en möjliggörare och motor för utveckling av e-förvaltningen.

Molntjänster är samtidigt inte en nationell företeelse utan en global fråga. Vi har uppfattat att det finns en oro för att Europa halkar efter i utvecklingen avseende molntjänster och att europeiska företag och offentlig sektor därmed inte tar tillvara potentialen på det sätt man skulle kunna.

Det framkommer samtidigt från arbetet att Sverige som neutralt land, med en hög it-mognad, en utvecklad it-industri och ett gott renommé, skulle kunna spela en viktigare roll i olika internationella sammanhang än vad som är fallet idag, inte minst inom EU. Vi föreslår därför en förstärkt svensk närvaro i frågor som rör molntjänster, med en tvärpolitisk ansats.

Källförteckning

Skriftliga källor

Publikationer

A Digital Single Market Strategy for Europe, Meddelande från EU-kommissionen SWD(2015) 100 final

Affärsnytta med molnet, Cloud Sweden (okänt år)

Arbetsgrupp ”Molnet i offentliga sektorn”, Cloud Sweden, daterad 2013-06-07

Cloud Computing; CIO Desk Reference Chapter 31, updated Q3 2013, Gartner G00262311 (2013)

Designing a Cloud Strategy Document, Gartner G00272867 (2015)

En bild av myndigheternas informationssäkerhetsarbete – tillämpning av MSB:s föreskrifter, Myndigheten för samhällsskydd och beredskap MSB740

En ny säkerhetsskyddslag, SOU 2015:25

En praktisk och lite enklare checklista för införskaffande, användning och lämnande av molntjänster, Cloud Security Alliance, version 1.0 publicerad 2015-08-24

Europa 2020 – En strategi för smart och hållbar tillväxt för alla s. 10, Meddelande från EU-kommissionen KOM (2010)2020 slutlig

Fördjupat it-kostnadsuppdrag – Delrapport 2: Kartläggning av it-kostnader (ESV 2015:58)

Government CIOs See Expected Cloud Cost Savings Evaporate, Gartner G00272823 (2015)

How to Budget, Track and Reduce Public Cloud Spending, Gartner G00272868 (2015)

How to Calculate the Total Cost of Cloud Storage, Gartner G00255331 (2013)

Informations- och cybersäkerhet i Sverige, SOU 2015:23 s. 248ff

Informationssäkerheten i den civila förvaltningen, Riksrevisionens granskningsrapport RiR 2014:23

Informationsteknik – Molnbaserade datortjänster – Översikt och terminologi. (ISO/IEC 17788:2014) Standard antagen 2014-12-16

It i människans tjänst - en digital agenda för Sverige (2011)

It-kostnadsmodell - Ett första steg mot ett gemensamt språk (ESV 2014:50), s. 17

Key Skills Needed for Successful Deployment of Cloud Computing in Government, Gartner G00261217 (2014)

Med medborgaren i centrum. Regeringens strategi för en digitalt samverkande statsförvaltning, N2012.37 (2012)

Nordic Public Sector Cloud Computing – a discussion paper, Tema Nord 2011:566

Sekretess vid outsourcing, förstudie från E-delegationen, Fi 2009:01/2015/4, 2015-03-09

Six reasons Private Clouds Fail, and How to Succeed, Gartner G00270366 (2014)

The Financial Case for Moving to the Cloud, Gartner G00273943 (2015)

The NIST Definition of Cloud Computing, National Institute of Standards and Technology, US Department of Commerce, Special Publication 800-145

The Three Rationales Behind Cloud Computing Strategies, Gartner G00270141 (2014)

The Top 10 Cloud Myths, Gartner G00270265 (2014)

Unleashing the Potential of Cloud Computing in Europe, COM(2012) 529 final

Vägledning – informationssäkerhet i upphandling, MSB555 (april 2013)

Prop. 2011/12:1, Budgetproposition, Utgiftsområde 22 Kommunikationer

Prop. 2014/15:1 Budgetproposition, Utgiftsområde 22 Kommunikationer

Riksarkivets föreskrifter och allmänna råd om elektroniska handlingar (upptagningar för automatiserad behandling), RA-FS 2009:1

Riksarkivets föreskrifter och allmänna råd om tekniska krav för elektroniska handlingar (upptagningar för automatiserad behandling), RA-FS 2009:2

Uppföljning av myndigheternas arbete med e-förvaltning och e.tjänster 2013, Rapport från E-delegationen 2013-11-05

Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Take-up, IDC (2012)

Lagar, förordningar, föreskrifter m.m.

Arkivlagen (1990:782)

Lagen (1997:736) om färdtjänst, avseende enskilt bedriven skolverksamhet, socialtjänst, hälso- och sjukvård respektive färdtjänst

Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet, MSBFS 2009:10

Offentlighet- och sekretesslagen (2009:400)

Patientsäkerhetslagen (2010:659)

Personuppgiftslagen (1998:204)

Skollagen (2010:800)

Socialtjänstlagen (2001:453)

Not. I den fullständiga juridiska analysen i bilaga 1 till huvudrapporten finns ytterligare hänvisningar till de källor i form av lagar, förordningar m.m. som ligger till grund för det juridiska grundarbetet och slutsatserna som återges i huvudrapporten.

Artiklar och webbsidor

Cloud Security Alliance´s webbplats, https://cloudsecurityalliance.org/

Cloud Swedens webbplats, http://cloudsweden.se/

Det är superlätt att flytta till en molntjänst – men har du funderat på hur du flyttar därifrån? Computer Sweden, webbpublicering 2015-05-11

Digital Agenda for Europe- A Europe 2020 Initiative, EU:s webbsida http://ec.europa.eu/digital-agenda/digital-agenda-europe (nedladdad september 2015)

Kammarkollegiets webbsida www.avropa.se (nedladdad november 2015)

EU-projekt PICSE, webbisda http://www.picse.eu/ (nedladdad december 2015)

EU-projekt Credential, webbsida http://credential.eu/ (nedladdad december 2015)

EU-projekt Prisma Cloud, webbsida https://prismacloud.eu/ (nedladdad december 2015)

EU-projekt SPECS, webbsida http://www.specs-project.eu/ (nedladdad december 2015)

EU-projekt SLA Ready, webbisda http://slaready.eu/ (nedladdad december 2015)

EU-projekt Cumulus, webbsida http://cumulus-project.eu/ (nedladdad december 2015)

Mål för IT-politik, Regeringens hemsida http://www.regeringen.se/regeringens-politik/it-politik/mal-for-it-politik/ (nedladdad september 2015)

Nu digitaliserar vi Sverige, pressmeddelande publicerat på regeringens hemsida 2015-10-29

Regeringen inför krav på it-incidentrapportering för statliga myndigheter, pressmeddelande publicerat på regeringens hemsida 2015-12-17

Enkät

Enkätundersökning ställd till 211 svenska myndigheter, utförd av Pensionsmyndigheten via verktyget SurveyMonkey (www.surveymonkey.com) under oktober 2015.

Enkäten bestod av 48 frågor om myndighetens storlek och verksamhetsområde, myndighetens erfarenheter och användning av olika molntjänster, motiv för användning av molntjänster, effekter och eventuella ekonomiska besparingar, frågor om informationssäkerhet, upphandlingsaspekter, om planerad användning av molntjänstertjänster samt om upplevda hinder eller risker med molntjänster.

Totalt 211 mail till myndigheter skickades ut. Vissa myndigheter hänvisade till annan myndighet för sin it-verksamhet, varför det slutliga antalet mottagare blev 188 myndigheter. 148 svar på hela eller delar av enkäten mottogs (svarsfrekvens 79 %).

Muntliga källor

Pensionsmyndigheten har bedrivit arbetet i samråd med Myndigheten för samhällsskydd och beredskap (deltagande i styr- och arbetsgrupp) samt Datainspektionen (genom avstämningsmöten på olika nivåer). Därutöver har ett antal referensgrupperingar och bilaterala möten på ett mycket positivt sätt bidragit till att kompettera de skriftliga källorna.

Referensgrupp för myndigheter

I referensgruppen för myndigheter har följande myndigheter deltagit: Skatteverket, Försäkringskassan, Lantmäteriet, Jordbruksverket, Migrationsverket, Regeringskansliet (IT-avdelningen), Polisen, Kammarkollegiet, Ekonomistyrningsverket, Riksutställningar, eHälsomyndigheten samt Inspektionen för vård och omsorg.

Forum för dialog - Stora molnforum

Representanter från följande företag har deltagit i den rådgivande grupperingen Stora Molnforum: Google, Amazon, Microsoft, Cisco, HP, Tieto, Atea, IBM, Ericsson, Redhat och Gartner.

Forum för dialog - Lilla molnforum

Representanter från följande företag har deltagit i den rådgivande grupperingen Lilla Molnforum: Bahnhof, CityNetwork, Elastx, Excanto och Projectplace/Planview.

Möten och presentationer

Separata möten hållits med experter på Kammarkollegiet och juridiska experter och företrädare för Cloud Sweden.

Presentationer och dialoger har skett inom ramen för aktiviteter med deltagande från Cloud Security Alliance, informationssäkerhetsnätverket SNITS samt eSamverkansprogrammet.