Promemoria

Tekniska förutsättningar i molntjänster

ES 2022-05

Juni 2022

Innehåll

1. Inledning

Att välja tekniska lösningar för att på ett legalt, funktionellt, säkert och kostnadseffektivt sätt ge rätt förutsättningar för verksamheten är oftast svårt. Detta gäller också för molntjänster. Molntjänster tenderar att inte ingå i traditionell teknisk omvärldsbevakning och utmaningar kring t.ex. inlåsningseffekter är viktiga att hantera vid upphandling. Det är viktigt att myndigheten samlar in krav och behov både internt och genom omvärldsbevakning samt att överväga alternativa tekniska lösningar.

Upphandling av molntjänster är komplext och därför är det viktigt att göra noggranna analyser och inte fatta beslut utan tillräckligt underlag. När myndigheter väljer att använda sig av molntjänster är det viktigt att ha rätt kompetens under hela utrednings- och införandefasen. Den tekniska aspekten behöver analyseras grundligt inför införande av en eller flera molntjänster. Efter upphandling behöver tjänsten löpande bevakas utifrån denna analys, t.ex. om tjänsten ändras av leverantör.

1.1 Syfte

Avsikten med denna promemoria är att övergripande beskriva krav på tekniska förutsättningar i molntjänster. Den första delen är av mer principiell karaktär och bör vara mer hållbar över tid, medan den andra delen är en ögonblicksbild över det tekniska läget vid promemorians publiceringsdatum. Den senare delen påverkas och förändras snabbt eftersom det tillkommer både nya leverantörer samt förändringar och tillägg i de olika tjänsterna. Syftet är framför allt att skapa en grundläggande teknisk förståelse och utgöra grund för bra dialoger mellan olika verksamhetsområden inom organisationen.

1.2 Avgränsningar

Promemorian gör inte anspråk på att vara heltäckande och kan förändras över tid när förutsättningar i omvärlden förändras. Promemorian ger inte alla svar på eventuella behov av utredning som en organisation kan ställas inför, utan ska kunna fungera som en översiktlig guide på området. Det är viktigt att läsa promemorian i sin helhet och inte dra långtgående slutsatser från enbart delar ur den. Vid en total bedömning av molntjänster måste också andra områden så som ekonomi, juridik, upphandling beaktas och värderas. Dessa områden tas inte upp i denna promemoria. Stöd för dessa områden finns t.ex. i eSams it-villkor, juridiska vägledningar och andra dokument som finns att läsa på eSamverka.se

1.3 Målgrupp

Promemorians huvudsakliga målgrupp är arkitekter, strateger, utvecklare och tekniker. Den kan även med fördel läsas av beslutsfattare för att få en övergripande inblick i den tekniska komplexiteten.

1.4 Medverkande

Arbetet med att ta fram promemorian har genomförts av en särskild arbetsgrupp bestående av Gabor Sebastiani (Arbetsförmedlingen), Jonas Andersson och Daniel Westman (Centrala Studiestödsnämnden), Johnny Carlberg (eSam kansli), Henrik Söderkrantz (Lantmäteriet), Peter Gunnarsson (Skatteverket), Gunnar Wennerholm (Tillväxtverket), Erik Enocksson och Per A Olsson (Trafikverket), Daniel Jönsson (Transportstyrelsen) och Thomas Hansson (Tullverket).

Gruppens arbetsmetodik för framtagande av promemorian är en sammanslagning av erfarenheter från deltagande myndigheter. Gruppen har sammanställt dessa, men inte utfört gemensamma utredningar eller tester. Kvalitetssäkring av promemorian har skett i eSams rättsliga expertgrupp, expertgruppen i säkerhet samt koordineringsgruppen för arkitektur. Beredning har skett via eSams samordningsgrupp.

Samordnare och kontaktperson för denna promemoria är Daniel Jönsson (Transportstyrelsen)

2. Principer

Promemorian beskriver den komplexitet som finns med molntjänster, exempelvis avseende leveransmodell och funktionalitet. Promemorian beskriver övergripande principer som bör styra myndigheters användande av molntjänster för att möjliggöra en lagenlig hantering.

Myndigheter bör kunna använda molntjänster när fem principer är uppfyllda:

1) Molntjänsten får endast hantera av myndigheten godkänd information
2) Att planerad informationsdelning är lämplig med privat aktör
3) Molntjänsten eller tillägg till molntjänsten säkerställer skydd mot otillåten eller olämplig leverantörsinsyn
4) Molntjänsten är i en it-miljö där myndigheten har tillräcklig egen kontroll
5) Kontinuitetsplan finns i händelse av tjänstebortfall, t.ex. vid leverantörs konkurs eller i händelse av uppköp, krissituation mm.

Förutom ovanstående principer är det viktigt att förstå konsekvenserna av eventuella krav från en leverantör på att få tillgång till myndighetens information. Det kan till exempel vara olika bakgrundsjobb för Artificiell Intelligens (AI), säkerhetskopiering och indexering av information. För att säkerställa att skyddsvärd eller olämplig information inte röjs måste respektive myndighet ställa krav på leverantören att redovisa information om sådan hantering.

3. Teknisk inriktning

Det är viktigt att kunna agera korrekt och rimligt avseende teknik vid utkontraktering och val av teknisk lösning. Den tekniska inriktningen är definierad baserat på följande antagande:

> Information som läggs i en extern it-tjänst måste betraktas som delad information om man inte tydligt kan visa på motsatsen
>
> Den som tillhandahåller en molntjänst har rimligtvis teknisk insyn i hela sin tjänst. Detta gäller även vid användning av specifika skyddslösningar framtagna av den som tillhandahåller samma molntjänst

Molntjänstleverantörerna lyder under sitt eget lands lagstiftning i första hand och ibland kan andra länders lagkrav på molntjänstleverantörer tvinga dem att lämna ut kundinformation ur sin tjänst vid exempelvis utlämningsärenden.

Överväg lösningar som ger myndigheten möjlighet att tillhandahålla egna skyddslösningar eller där en tredjepart tekniskt skyddar kundens information. Det är inte tillräckligt att enbart förlita sig på skyddslösningar framtagna av molntjänstleverantören. Ingen av de valda leverantörerna inklusive en tredjepart ska kunna få oönskad insyn till kundens information med den valda lösningen.

När myndigheten utgår från inbyggda skyddslösningar eller om en tredjepart kan få oönskad insyn, måste myndigheten säkerställa att man skyddat myndighetens information i tjänsten (se avsnitt ”Tips för att tekniskt skydda myndighetsinformation i moln”).

Endast leverantörer som genom oberoende granskningar kan påvisa att insyn i kunders information förhindras genom implementerad teknisk arkitektur och design kan rimligtvis anses uppfylla kraven för att anlitas. Leverantörer behöver visa hur de skyddar kundens information och att det finns en tillämplig ackreditering av implementerade säkerhetslösningar.

4. Arbetssätt att utreda molntjänst för myndigheter

Eftersom myndigheter har att förhålla sig till krav i lagar, förordningar och föreskrifter gällande hur information hanteras och eftersom it-sourcing inklusive molntjänster, innebär en informationsdelning med leverantörer, behöver det finnas arbetssätt för att ge myndigheten förutsättningar till en korrekt implementering av molntjänst. För att lyckas med implementeringen behöver en leverantör förstå vikten av att stötta myndigheten med fullständig teknisk transparens då varje molntjänst är unik och detaljer avgör om krav på legalitet och verksamhetskrav kan uppfyllas. I dess enklaste form behöver följande steg genomföras vid bedömning av om en molntjänst kan användas i en viss verksamhet.

1) Vilken information exponeras från myndigheten mot molntjänsten? Information från leverantören och grundlig omvärldsbevakning kring molntjänsten kan användas för denna insamling av information. Det är viktigt att inte bara kartlägga den egna myndighetens informationsdelning utan även ta hänsyn till den aggregerade informationen som finns i molntjänsten. Om myndigheten har svårt att få fram all denna information bör molntjänsten som helhet ifrågasättas.
2) För säkerhetskänslig verksamhet finns även icke-tekniska krav som måste hanteras. Ett sådant krav är exempelvis säkerhetsprövning av personal och underleverantörer. Även dessa krav behöver beskrivas och hanteras om molntjänsten avser att stötta sådan verksamhet. För säkerhetsskyddsklassificerade uppgifter tillkommer en annan komplexitet av direkta tekniska krav som molntjänster generellt inte kan leverera. Jämför med försvarsmaktens godkända kryptografiska lösningar.
3) Verksamhetsansvarig på myndigheten behöver utreda vilket värde informationen har genom t.ex. inventering och klassning av information och en rättslig bedömning. Här bör verksamhetsansvarig med fördel ta stöd av jurister, dataskyddsombud samt informations- och it-säkerhetsexperter.
4) Myndigheten behöver utforma krav på skyddsåtgärder utifrån informationsklassningen.
5) Myndigheten behöver identifiera vilken information som kan delas utan att det innebär någon skada för myndigheten eller tredje part. Respektive myndighet bör inkludera juridik och säkerhetsorganisation för att stötta i denna fråga.

6) Myndigheten behöver genom sin säkerhetsstyrning ta ställning till hur skydd av information som inte bör röjas ska se ut, vid etablering av tekniska anslutningar till eller från en molntjänst.
7) Myndigheten behöver hantera upphandlingen av tjänsten kopplat till myndighetens krav på lämpligt sätt.

Efter genomförd bedömning måste myndigheten göra en slutlig utvärdering om tjänsten i dess utformning, med vidtagna åtgärder, uppfyller myndighetens verksamhetsbehov. Om tjänsten bedöms att inte kunna uppfylla nuvarande och kända kommande verksamhetens behov, bör alternativa lösningar utvärderas.

Licenseringsformen för Molntjänster är uteslutande prenumeration även om variationer finns. Det är viktigt att tänka på att de avtal som tecknas för vissa typer av tjänster kommer att förändras under avtalets tid. Ny funktionalitet blir tillgänglig omgående och ibland utan kundens godkännande eller vetskap, det är därför viktigt att ha koll på leverantörens förändringar och villkor som kan förändras ofta.

Inom myndigheten bör det finnas kompetenser inom teknik, juridik, säkerhet, verksamhetsnytta samt inom de vanligaste leveransmodellerna på marknaden. Kompetensen bör även inkluderas i myndighetens ordinarie styrning för att säkerställa att den bibehålls och utvecklas i samma takt som omvärlden.

Ett exempel kan vara att identifiera om myndigheter anlitar samma molnleverantörer och skapar risker genom aggregerad information. Aggregerad och ackumulerad information från flertalet myndigheter driver ofta ett kompletterande skyddsbehov, till skillnad från om enskilda informationsmängder hanteras av en leverantör.

All teknisk delning måste kunna beskrivas i de fall då delning kan uppstå med leverantören. Detta oavsett under vilka förutsättningar om det gäller t.ex. AI, automatiserade jobb, diagnostik, support och telemetri.

5. Artificiell intelligens

Utvecklingen av molntjänster har medfört ett rikare utbud av avancerade analytiska verktyg för analys av data. Artificiell intelligens (AI) erbjuds som en naturlig del av utveckling av molntjänster men finns på olika nivåer hos olika moln erbjudanden.

Artificiell Intelligens i molntjänster skulle kunna levereras som tjänst av de allra flesta molnleverantörer men frågan är vad man menar med en sådan tjänst.

Artificiell Intelligens möter vissa tekniska utmaningar kopplat till information. Det fungerar bäst med stora informationsmängder och det blir enklare om dessa informationsmängder inte måste ha en tvingande behörighetsstruktur. Information måste klassas och ha lämplig hantering beroende på dess tilldelade informationsbedömning. Dessutom måste analys av aggregerad information göras av ansvarig verksamhet när man samlar informationsmängder. Traditionellt samlar man all information för AI-analys som kund. Myndigheter behöver dela informationsmängder utifrån klassning. Detta är försvårande faktorer och offentlig sektor behöver hantera sina informationsmängder innan de kan bearbetas av AI-tjänster. Detta gör också att alla informationsmängder inte kan delas publikt till upphandlade AI-tjänster. En annan utmaning för offentlig sektor att hantera är att statstjänstemannens ansvar inte alltid får automatiseras till en AI-bedömning. Därför behöver vissa AI-tjänster anpassas i dess utformning mot just offentlig sektor. Istället för automatiserat beslut kan fokus bli mer kategoriserande inför manuellt beslut (beslutsstöd).

5.1 Egenskaper i molntjänster för AI

Artificiell Intelligens är ett samlingsbegrepp för lärandealgoritmer och algoritmer inom maskininlärning och djupinlärning.

AI generellt kan exekvera i vanliga molnbaserade datorer (CPU) miljö och även delvis inom maskininlärning men när det gäller djupinlärning som bygger på neurala nät (efterliknar funktionen för biologiska neuronnät) kräver stöd av specifika resurser från grafikprocessorer (GPU) som kopplas via CPU-baserade system. Vikten att det finns stora primärminnen på GPU ökar möjligheten att exekvera större och mer komplexa neurala nät inom molntjänster.

5.2 Discipliner inom molntjänster för AI

Det finns olika utmaningar och inriktningar som kan önskas nyttjas inom molntjänster:

Maskininlärning – CPU-centrerad exekvering

Neurala nät – CPU/GPU-centrerad exekvering

Djupinlärning – GPU-centrerad exekvering

Detta specificerar krav att om man exempelvis skall utföra AI algoritmer av typ djupinlärning så behövs GPU-resurser. Utformning och tillgången av GPU-resursen är avgörande om man skall kunna dra nytta av den. Det innebär gruppering av GPU-resurs och hur stora primärminnen som finns på varje individuell GPU och kommunikationen mellan GPU-grupperingen.

5.3 Data som resurs i Molntjänster för AI

Artificiell Intelligens konsumerar och kräver generellt mycket data för att kunna tränas och valideras.

Exempel är med bildanalys eller språkmodellsträning.

Vid bildanalyser blir det lätt stora mängder data som måste överföras till molnet för att där kunna utföra bildanalys med stora GPU-resurser. Här spelar upplösning på bilderna, hur snabba datalagringstekniken är mot GPUns kapacitet om algoritmen svälter på data eller överflödas av data.

Språkmodellers träning kräver också stora mängder data och kraftiga GPU-kluster. Att överföra stora datamängder till molntjänster och att utföra tunga beräknings algoritmer kan bli kostsamt.

6. Lösningar

6.1 Informationsklassning

En förutsättning för att kunna använda molntjänster är att informationen är informationsklassad. Detta beror på t.ex. gällande behandling av viss typ av skyddsvärd information får myndigheten inte alltid välja teknisk lösning själv. Ett annat exempel är att t.ex. sekretessreglerad information kräver både vissa avtal men också viss tekniska upplägg för att säkerställa konfidentialitet, tillgänglighet och riktighet där myndigheten har tillräcklig egen rådighet kopplat till molntjänsten. Denna bedömning av sin information ska ske innan den läggs i molntjänsten. Klassningen kan bestå av flera perspektiv som är kritiska för myndigheten t.ex. enligt gällande författningar. Varje myndighet kan även välja att lägga till aspekter i sin klassningsmodell beroende på verksamhet. Vid användning av klassningsmodellen rekommenderas även att klassningen på lämpligt sätt blir digital så att den kan hanteras i samverkan med den egna it-infrastrukturen. ”Vilken information skall ligga var?” Detta underlättar också eventuellt beslut om att kunna hantera stora informationsmängder mot flera molntjänster.

Ett mål i myndighetens arbete med informationshantering är att det skall vara ”lätt att göra rätt”, vilket ofta krävs av de digitala stödsystem som beskrivs i detta dokument. Ett annat mål som måste formuleras när en myndighet planerar att införa molntjänster, är hur man ska hantera situationen då information hamnat på fel ställe t.ex. sekretessreglerade uppgifter i en publik molntjänst som inte är kravställd för att kunna hantera detta på ett tillfredställande sätt. Krav på kontinuitet ska utredas innan upphandling gällande både tillgänglighet och riktighet i enlighet med myndighetens bedömning och klassning både för information i tjänsten och tjänsten i sig själv. Även vid it-sourcing har myndigheten ett krav på sig gällande spårbarhet och incidentrapportering. De flesta molntjänster har denna rapporteringsförmåga inbyggd i molntjänsten. Om en myndighet har många molntjänster vilka alla har en egen förmåga till spårbarhet så kan det finnas utmaningar att skyndsamt analysera och samköra dessa loggar. En ytterligare aspekt att ta i beaktande är vad som händer med informationen vid eventuell avveckling av tjänsten. Man bör säkerställa att informationen går att exportera i ett strukturerat format för att möjliggöra att den kan importeras i en annan tjänst. Det är viktigt att man avtalat att informationen destrueras hos leverantören efter bevarandetiden, både direkt (lagring i tjänsten) och indirekt (t.ex. backup)

6.2 Informationsseparering

En viktig funktion för it-sourcing och till viss del molnleveranser, är att ordna lämpliga separationer i en it-infrastruktur utifrån författningar som gäller för myndigheters informationshantering. Informationsepareringen bör lämpligtvis utgå ifrån resultatet av informationsklassningen. Att separera skyddsvärd information kan göra det lättare att utkontraktera t.ex. icke-skyddsvärd information. Denna typ av separation är ofta självklar på en konceptuell nivå men på en teknisk nivå kan det istället orsaka följdproblem för verksamhetens behov och inte sällan för den eventuella tekniska skuld som myndigheten kan ha. Praktiskt kan denna separation för större myndigheter vara väldigt svår att genomföra. Tydliga vägledningar bör tas fram för att ge rätt förutsättningar för medarbetare att kunna lagra information på rätt plats. Uppföljning och kontroll blir då en viktig del för att säkerställa efterlevnad.

Författningar ger inte en komplett kravbild på hur en teknisk separation ska göras och de befintliga tekniker som finns medför stora skillnader mellan myndigheters implementationer. En vanlig separation av infrastrukturer är nätverkssegmentering, vilket påverkar myndighetens allmänna digitala arbetssätt. Det är viktigt att ta beslut om vilka system som ska finnas var, vilken information som ska finnas var och hur överföring mellan systemen ska fungera. Traditionellt kombineras nätverkssegmentering med olika instanser av katalogtjänster som finns i respektive segment.

Modern teknik kan numera separera information inom en domän och inom ett nätverk vilket minimerar användarens behov av flera klienter och användarkonton. Även teknik för virtuella klienter, mikrostjänster och mjukvarubaserad it infrastruktur kan vara ett stöd för myndigheten att på ett enklare sätt jobba mot den allt mer komplexa it infrastrukturen. Myndigheten bör eftersträva detta för att göra en mer flexibel och säkrare infrastruktur möjlig, som också klarar att uppfylla myndighetens förändrade behov över tid.

Det kan vara relativt enkelt att bedöma om enskilda handlingar kan läggas i molnet eller inte om de är informationsklassade. Men flera informationsmängder resulterar i en aggregerad informationsmängd vilket kan leda till en högre klassning, som i sin tur minskar de möjligheter som annars funnits för att kunna flytta system till molnet. Då kan informationsseparering vara en lämplig väg. Med detta försöker man dela upp system i mindre komponenter, och styra information med liknande behov av konfidentialitet, tillgänglighet och riktighet till samma it infrastrukturgrupp av komponenter. Detta kan göra det möjligt att t.ex. flytta komponenter med information av låg känslighet, till en molntjänst. Se andra kapitel för fler resonemang kring hur detta kan genomföras och vilka typer av verktyg som kan vara behjälpliga för detta arbete.

För teknisk hantering bl.a. vid klassning och skydd av information, bör tekniska verktyg vara ”on prem” och under egen kontroll utan leverantörens insyn då informationsmängden i dessa tjänster kan vara sekretessreglerad. Verktyg måste även fungera obehindrat under t.ex. cybersäkerhetsangrepp.

6.3 Paketering av tjänster runt säkerhet och administration

Utöver funktionalitet i enskilda it- och molntjänster är det också viktigt hur väl olika tjänster kan integreras och samverka. Inte minst organisationer med mindre it-avdelningar ser en nytta i att kunna upphandla lösningar med någon form av paketering av en samlad funktionalitet där olika tjänster är integrerade. Det kan röra sig om olika grad av integration mellan tjänster för exempelvis produktion av information, delande av information, säkerhet och administration av klienter. Microsoft 365 och Google Workspace är exempel på digitala samarbetsplattformar med sådan integration.

Genom en integration kan den samlade molntjänsten stödja hela processer från kontroll av skadlig kod i mejl, behörighetskontrollerad dokumentproduktion inom och mellan organisationer, kontroll av förekomst av känsliga uppgifter i utgående mejl, ge stöd för kryptering av mejl och andra säkerhetsfunktioner. I Microsoft 365 finns administrations- och säkerhetsfunktioner som katalogtjänst, tjänster för flerfaktorsinloggning, distribution av program och uppdateringar, övervakning av klienter och åtgärder vid avvikelser mm. Detta innebär fördelar för kunden vad avser såväl funktionalitet, driftsäkerhet som säkerhet mot angrepp och det innebär också att administrationen av it-miljön, klienter och programvara förenklas och kan hanteras av färre personer, liksom att test av att olika tjänster fungerar med varandra efter uppdateringar förenklas. För många organisationer är sådant av avgörande betydelse.

Samtidigt innebär en sådan integration olika nackdelar, såsom en stark inlåsningseffekt. Möjliga åtgärder som minimering av känsliga uppgifter, pseudonymisering, anonymisering, kryptering m.m. innebär hinder för att uppnå god balans av kostnad och affärsvärde, enkelhet och nyttan av tjänsterna. För att följa gällande författningar skulle det i många fall behövas parallella tjänster och miljöer för informationsmängder och enheter med olika informationsklassning, vilket knappast är optimalt för vare sig organisationen eller den enskilde handläggaren. Därmed förloras också en stor del av nyttan med integrationen.

Tekniskt kan det uppstå en del problem med dessa tjänster gällande säkerhet och administration. Offentlig sektor har t.ex. krav kring viss spårbarhet (vem har gjort vad och när) och rapporteringsskyldighet, så hur blir den sammansatta förmågan (upphandlad tjänst och den lokala it avdelningen) för kunden runt kontinuitetshantering,

loggning och övervakning? Tappar man tillräcklig egen förmåga vid ny upphandlad tjänst? Betänk att en kund offentligt upphandlat upp till flertalet olika molntjänster för att täcka alla olika it behov i verksamheten. Hur möter man då kraven runt sin egna centrala spårbarhet, hanterbar sammanhållen katalogtjänst, eller hållbart exponerat eget it-nätverk (som är uppkopplad mot alla dessa tjänster)? Hur förhåller sig den egna förmågan gällande tillräcklig uppföljning i relation med dessa externa och interna tjänster?

Det skulle vara en stor fördel om ett sådant tjänsteutbud med paketering och integreringsmöjligheter inklusive support kunde tillhandahållas av leverantörer inom EU/EES-området. Det är också vanligt att själva informationen i administrativa- och i cybersäkerhetsverktyg klassas som skyddsvärd vilket kan göra det enklare med en svensk tjänsteleverans (ex. SUA avtal). Det kan finnas flera krav på leverantörens personal, exempelvis måste all personal vara svenska medborgare?

6.4 Tekniska byggtips till leverantörer

Hur skall man som en leverantör bygga it-tjänster (molntjänster) för att bäst möta kunder som behöver egen bättre kontroll över tillgång till deras egen information? Här följer några tekniska designtips över vanliga it-tjänstproblem gällande tillräcklig tillgång till kunden information. Dessa designtips rekommenderas oavsett hemvist på tjänsten, det spelar alltså ingen roll om den är ex. en amerikansk eller europeisk.

1) Bygga ett biljettsystem eller en krypteringsbaserad lösning istället för baserat på personuppgift. Undvika personuppgifter för licensaktivering och åtkomst till it-tjänsten. För att garantera att unika slutanvändare ges åtkomst kan en lokal licensfunktion sättas upp som kontrollerar unika åtkomster per upphandlad licens. För tjänster som har en användarkatalog (oavsett global eller regional) bör dessa kunna styras om till sk. proxy uppslag. Via detta upplägg så delas inga personuppgifter med leverantören.
2) Bygga stöd för att styra om all cybersäkerhetsövervakning från kundens nyttjande av tjänsten till annan valfri cybersäkerhetsfunktion. Alternativt bygg dessa cybersäkerhetsfunktioner så att minimalt eller ingen insyn till kundinformation kan ske, samt att ingen kundinformation sparas annat än vid misstänkt incident. All delad kundinformation skall kunna deklareras.
3) Bygga stöd för att styra om all logghantering från kundens nyttjande av tjänsten till annan valfri logghantering.
4) Bygga stöd för att styra om all säkerhetskopiering och återställning från kundens nyttjande av tjänsten till annan valfri återställningslösning.

5) Bygga stöd för att styra om all support hantering från kundens nyttjande av tjänsten till annan valfri supportlösning. Alternativt bygg supportfunktioner så att minimalt eller ingen insyn till kundinformation kan ske, samt att ingen kundinformation sparas i onödan. All delad kundinformation skall kunna deklareras.
6) Bygga stöd för att styra om all övervakning från kundens nyttjande av tjänsten till annan valfri övervakningslösning.
7) Bygga stöd för autentisering och auktorisering mot kund.

6.5 Tips för att tekniskt skydda myndighetsinformation i moln

Tillverkaren av en molntjänst (t.ex. ett amerikanskt bolag) kan enkelt bygga in AI-indexjobb i sin molntjänst. Befintliga lagkrav kan innebära att tillverkaren dels måste kunna lämna ut kunddata, dels att kunden inte får informeras om detta. Leverantören själv kan av öppna eller dolda skäl vilja dra nytta av insyn i myndighetens information och arbetssätt i tjänsten på ett sätt som inte är överenskommet. Frågeställningar och aktiviteter som kan hjälpa:

1) Analysera helheten av informationsutbyte via tjänsten; arbete i tjänsten, administration, arkivering, databaser, filer/lagring, integrationer, konfiguration i tjänsten, nätverkskoppling, personuppgifter, systemkopplingar, säkerhetsåterställning.
2) Hur stort är värdet av informationen för myndigheten? Hur aggregeras värdet när all information samlas i tjänsten?
3) Vilken information, utifrån värdet, behöver skyddas ifrån insyn av en leverantör (ej skyddad information måste anses som utlämnad)?

Sätt upp fungerande skyddslösningar per objekt och område. Här följer några tips och frågeställningar:

1) Överväg att införa och nyttja ett "information governance" stödsystem. Det kan ge allmän kännedom om vilken digital information som har vilket värde på myndigheten. Se kapitel "Stödsystem för informationshantering".
2) Kan informationen i tjänsten skyddas via kryptering? Molntjänster ändras över tid, ställ frågan om det är troligt att en "end-to-end" krypteringsstrategi håller för dessa ändringar. Se kapitel "Kryptering".
3) Separera känslig information från t.ex. kontorsnära eller publik information på myndigheten som en förutsättningsskapande grundåtgärd för it-sourcing (molntjänster). Det är i allmänhet lättare att dela information och öppna it-

infrastrukturaccess, när känslig information redan är skyddad. Det blir även tydligare för verksamheten hur man skall jobba och var system och information skall finnas, om man gjort en smart separation. Se kapitel ”Informationsseparering”.

4) Planerade åtgärder för cybersäkerhet gällande information i molntjänsten, behöver också knytas till värdet av informationen (även aggregerat). Även om skyddsvärd myndighetsinformation mindre troligt förekommer i publika molntjänster, kan fortfarande riktighet och tillgänglighet vara viktigt. Om den inbyggda cybersäkerheten i molntjänsten inte skulle vara tillfredsställande så kanske en tredjepartslösning kan utgöra ett komplement.

5) En del av informationsskyddet kan handla om processer och rutiner i hanteringen av tjänsten (inte bara tekniska skydd) för både administratörer och användare. Produktionssätt tjänsten med en informationsdelningsplan baserad på lagstiftning och organisationens regler t.ex. för hur administration ska bedrivas eller hur arbete ska utföras i tjänsten.

6) För att skydda innehållet i filer kan man överväga en DLP & EDRM-lösning. Filer måste först skapas utanför molntjänsten och namnet på filen får inte i sig innehålla information som är känslig. Se kapitel ”Stödsystem för informationshantering”.

7) För att skydda ett visst fält i en molntjänst (t.ex. i en SaaS) kan man undersöka om CASB lösning kan ge fullgott skydd. Se kapitel “Cloud Access Security Broker”.

8) Personuppgifter kan anonymiseras, ges en egen identitet i tjänsten, enbart exponera uppgiften i kontrollerad miljö (ej publikt) eller lösa identiteten i molntjänsten via proxy-uppslag.

9) DLP, diodteknik eller SDI kan vara ett stöd vid systematisk flytt av information t.ex. integration och systemkoppling för att förhindra ett felaktigt informationsflöde och stoppa manuella fel.

10) Vid systemåterställning och övervakning kan en för molntjänsten extern eller alternativ lösning vara att föredra för att tvinga in dessa delar till myndighetens egna interna lösningar för att undvika att öppna upp känslig it-infrastruktur. Det är en svår fråga eftersom dessa it-komponenter ofta själva genererar en hög informationsklassning för myndigheten.

11) Kontinuitetsplanering är kritiskt men måste inte alltid, beroende på vilken verksamhet som är berörd, innebära stöd i en teknisk lösning. I vissa fall kan en manuell hantering vara tillräckligt.

6.6 Hybridlösningar

Att övergå från egen drift till molntjänster är ett stort steg. Med hänsyn till de krav och lagar som myndigheten omfattas av, behöver en sådan förflyttning ske stegvis. För att göra en koordinerad förflyttning över tid möjlig, är ofta det första steget att använda hybridlösningar. De kan också användas om man vill tillgodogöra sig fördelarna av molntjänst-teknik i de fall myndigheten har kunskap och kapacitet att hantera en egen molnplattform. Problematiken med att uppgifter enbart lagras och behandlas i den interna miljön kvarstår dock i det fallet.

Oavsett vilken lösning som väljs, är det viktigt att till fullo inse vilka risker som tillkommer, utöver möjligheter. Det kan till exempelvis vara viktigt att på förhand analysera hur myndigheten ska hantera både lösningen som helhet och framtida support. Krävs det till exempel att statistisk information måste skickas till leverantören för felsökning eller att öppna lösningen för fjärråtkomst i syfte att möjliggöra support, så är det samma problemställning som en hybridlösning avsåg att lösa.

En annan aspekt är också att hybridlösningar kan levereras som en hanterad drift, där till exempel övervakning och kontroll av säkerhetsuppdateringar hanteras av leverantören. I dessa fall kan det innebära att delar av infrastrukturen måste göras tillgänglig utanför myndighetens kontroll. Varje myndighet måste analysera hur en sådan leverans kan ske på ett lämpligt sätt med hänsyn till de krav på säkerhet i it-infrastruktur som myndigheten omfattas av. Det är viktigt att ta hänsyn till skillnader mellan olika leverantörers möjligheter att tillhandahålla en leverans som är anpassad efter myndighetens behov.

6.6.1 Var är hybrida it-tjänster på väg idag?

Förhoppningarna har länge varit stora kring hybrida it-tjänster (hybrida moln). Men efter flera års utveckling börjar ett mönster bli tydligt att de mest attraktiva tjänsterna hos leverantörerna primärt erbjuds i molnbaserade tjänster. Även tjänster som går att lägga i en hybrid tjänst delar oftast för mycket information med leverantörer. Ibland blir tjänster i hybridläge oanvändbara för kunden om man isolerar sig åtkomstmässigt från leverantören. Så även för hybrida scenarion av it-sourcing blir informationsdelning oftast ett praktiskt problem. Mest framgång hittar man bland hybrida tjänster baserat på öppen källkod eller alternativ till de stora amerikanska leverantörerna. I alternativ baserad på öppen källkod är det lättare att dels veta var informationen finns och vem man måste dela informationen med (oftast granulärt valbart).

6.6.2 Hybrida lösning från de tre största molnleverantörerna.

Det finns exempel på hybrida molntjänster från Amazon Web Services, Google och Microsoft. Leverantörerna erbjuder följande produkter, AWS Outpost, Google Anthos och Azure Stack Hub. Urvalet har inte ändrats stort de senaste åren men dessa tre kan vara viktiga för offentlig verksamhet att löpande bevaka. Om leverantörerna tekniskt ändrar sina tjänster för att bättre möta offentlig sektors olika krav är det troligt att det är i dessa produkter ändringen kommer ske först. Det finns idag andra leverantörer, exempelvis svenska och europeiska som kan möta offentlig sektors krav men som inte i marknadsandelar platsar in bland dessa tre, vilka skulle kunna ses som fungerande alternativa lösningar. En bredare omvärldsbevakning kan rekommenderas samt att komplettera med sin egen analys med utgångspunkt från det metodstöd som levererats, inför val av teknik.

Att driva en hybridlösning kräver att man noggrant planerar för den kapacitet och löpande kostnad som tillkommer. Det är sannolikt att utrustningen behöver bytas ut med jämna mellanrum vilket kan bli en kostnads- och resursfråga på lång sikt. Denna kostnad skiljer sig markant mot en vanlig molntjänst där just kostnad för utrustning finns inkluderat i priset.

Kan offentlig sektor idag nyttja dessa hybrida lösningar för merparten av sina it behov eller sammanhållande som grundplattform för merparten av sina it behov? Detta måste man bedöma per offentlig verksamhet men troligtvis saknas grundläggande funktion för att kunna göra detta än så länge. Dessa tre produkter ingår idag i större it-ekosystem för respektive leverantör och som kund behöver man fundera på de totala tekniska konsekvenserna i att kliva in i dessa hybrida lösningar idag.

6.6.3 Summering

När man väljer en hybridlösning är det viktigt att ta hänsyn till att leverantörer erbjuder olika grader av förvaltning av lösningen. I de fall man saknar fullständig kunskap och bemanning så kan det vara lämpligt att låta leverantören sköta övervakning och säkerhetsuppdateringar. Är det viktigaste att hela driften ska vara i egen regi, krävs att man har väl utvecklade processer för att sköta övervakning och säkerhetuppdatering själv. Oavsett modell är det viktigt att myndigheten alltid har möjlighet att minimera vad som exponeras mot en leverantör så att känslig information inte riskerar att exponeras på ett felaktigt sätt.

6.7 Öppen källkod

Trenden bland leverantörer av proprietär programvara är att sälja som molntjänst och inte för lokal installation. De organisationer som behöver lokal installation tittar därför oftare på programvara med öppen källkod. Öppen källkod ger både möjlighet att anordna drift i egen regi eller hos en leverantör som erbjuder garantier kring frågor som utlämnande och gallring. Det finns en del generella fördelar och nackdelar gällande öppen källkod och val av upphandlad eller egenutvecklad och konfigurerad it-tjänst. Men det är mer vanligt nuförtiden att under omvärldsbevakning även titta på lösningar baserad på öppen källkod. Molntjänster allmänt byggs ofta med öppen källkod delvis eller helt både i de största molntjänsterna och svenska molntjänster. Nya öppen källkods-lösningar byggs idag oftast för att kunna levereras som molntjänst antingen i egen regi (privat molntjänst) eller från återförsäljare (valfri publik molntjänst).

För en allmän orientering kring öppen källkod, se eSams Råd kring användning och delning av öppen källkod.

Generella fördelar:

- Ofta enklare att styra och kontrollera hur kundinformationen exponeras och till vem i tjänsten.
- Efter förmåga kan kunden påverka och själv utveckla tjänsten bättre efter egna unika kundbehov.
- Tekniska integrationer mellan konkurrerande tekniker är ofta enklare.
- Kontinuitet och suveränitet kan oftast hanteras attraktivt i lösningar som är öppen källkod.
- Upphandlingsförfarande och licenshantering kan bli enklare för kund.
- Kan innebära lägre TCO (Total Cost of Ownership) över tid.

Generella nackdelar:

- Kräver ofta större egen förvaltningsförmåga.
- Kräver ofta större egen teknisk förmåga.
- Vald lösning kan läggas ner vid minskat allmänt intresse för tjänsten.
- Öppen källkodslösningar är sällan marknadsledande i branschen.

- Idag är det svårare generellt att hitta kompetenser på marknaden för öppen källkod. Stor konkurrens och mindre volymer av konsulter.

Två riskområden som bör beaktas gällande öppen källkod är licensmodell och skadlig kod:

6.7.1 Licensmodell

Avsaknad av licens – Om licens saknas så kan det tolkas att upphovsrätten gäller och att källkoden därmed inte är öppen trots att källkoden ligger på en webbplats för öppen källkod. Det bör finnas en licens som ger användaren rätt att nyttja koden.

Lämplig licensmodell - Vissa licensmodeller ger skyldighet att dela sina lösningar vidare. Andra licensmodeller kan kräva att användaren utför en handling som man inte bedömer vara lämplig. Det kan röra sig om en så enkel sak som att i en text i användargränssnittet tacka upphovsmannen. Eventuella motprestationer behöver utvärderas i förhand.

Inte för många licensmodeller - Det finns en stor mängd olika licensmodeller och antalet har ökat. Licenserna förändras dessutom över tid genom att nya licenser uppstår och andra minskar i popularitet. För att ha förutsättning för att kunna bevaka detta behöver man avgränsa sig till några beslutade licensmodeller som man kan använda och bevaka.

6.7.2 Skadlig kod

Avsaknad av ansvar - Användning av öppen källkod sker utan garantier eller ansvar från upphovspersonerna.

Sårbar kod - Källkod som inte uppdateras eller inte förvaltas av något ”community” kan innehålla sårbarheter som därmed inte åtgärdas.

Skadlig kod - Det har förekommit att någon medvetet byggt in svagheter i öppen källkod.

Exempel på kompenserande åtgärder

- För att kompensera upphovspersonernas ansvarsfrihet kan en lösning baserad på öppen källkod köpas av en leverantör som förbinder sig att ta ansvar för källkoden.

- En leverantör kan anlitas för att granska källkoden och utfärda en garanti för att källkoden inte är skadlig.
- Källkoden kan granskas maskinellt med verktyg för statisk kodanalys.
- Binärkoden kan granskas maskinellt med verktyg för sårbarhetsanalys.

7. Säkerhetslösningar för övervakning och kontroll

7.1 Kryptering

Kryptering förmedlas ofta som en lösning för myndigheters användning av molntjänster men kryptering bör snarare jämställas ett stöd till andra tekniska lösningar. En lösning baserad på kryptering behöver uppfylla en mängd krav åt myndigheten för att vara användbar.

1) Lösningen behöver fungera under en längre tidsperiod, över flera år.
2) Lösningen behöver hålla en hög grad av resiliens och måste fungera även vid t.ex. handhavandefel och stört läge.
3) Lösningen måste använda ett, i förhållande till skyddsvärdet, lämpligt krypto.
4) Att endast myndigheten har tillgång till krypteringsnycklarna och inte leverantören.
5) Att informationen krypteras innan den blir tillgänglig i molntjänsten.
6) Att myndigheten kan säkerställa krypteringens säkerhet i alla led.

För den händelse att kryptering bedöms vara den tekniska lösning som möjliggör användning av molntjänster, måste myndigheten avgöra vilken känslig information som ska delas med molntjänsten och hur denna kan krypteras i samtliga led.

Detta kan t.ex. vara under tiden som information skapas, nätverkstrafiken vid kopiering och flytt, cachelagring av information i molntjänsten, lagring av information i molntjänsten, vid loggning, vid säkerhetskopiering och vid övervakning av molntjänsten. Myndigheten måste också undersöka hur detta inverkar på den funktionalitet som molntjänsten kan leverera.

Flertalet leverantörer har implementerat ett krypteringsschema som benämns ”double-key encryption”, också känt som ”envelope encryption”. Detta innebär att information krypteras med både leverantörens och kundens nyckel. Principen är att enbart kunden har tillgång till dennes nyckel. Detta innebär dock att när kunden ska använda informationen måste både kundens och leverantörens nycklar användas för att dekryptera informationen och genomföra bearbetningen vilket leder till att information förekommer i klartext hos leverantören under behandlingen.

7.2 Federation eller synkronisering av katalogtjänst

För att möjliggöra samarbete kring molntjänster har myndigheter möjlighet att nyttja federation av både identiteter och behörigheter. Federation innebär att en myndighet förlänger sin katalogtjänst för myndighetens identiteter och behörigheter mot berörd tjänst. Detta innebär att en tjänst inte ensidigt måste hantera separata identiteter som en del av tjänsten, utan kan använda de som en myndighet redan etablerat i sin ordinarie organisation. Federation sker vanligtvis genom SAML2.0 OpenID, WS-Trust, WS-Federation eller OAuth.

Inför varje federation måste ansvarig myndighet säkerställa att den information som exponeras mot en federationstjänst får exponeras. Vidare ansvarar respektive myndighet för att enbart exponera det absolut nödvändigaste som en tjänst kräver, för att möjliggöra en federation.

Om möjligheten till federation inte finns för att använda företagsidentiteter i en molntjänst, kan leverantören oftast tillhandahålla en lösning för kontosynkronisering. Syftet är att användaren inte ska behöva flera konton överallt utan kunna använda redan tilldelade i så lång utsträckning som möjligt. Hos de större leverantörerna kan en myndighet genomföra en synkronisering för att sedan nyttja dessa molnidentiteter i leverantörens molntjänster (ibland även tredjepartslösningar).

I dessa synkroniseringslösningar kan en myndighet ibland styra vad som ska inkluderas och hur synkroniseringen ska genomföras. Känsliga roller på en myndighet kan ofta behöva exkluderas (vilket innebär att dessa personer inte får tillgång till molntjänsten) och en myndighet får även möjlighet att anonymisera identiteter som en del av synkroniseringen. I likhet med federationslösningar kan det dock bli problematiskt med personuppgifter.

Sammanfattningsvis finns fyra spår för de beskrivna tekniklösningarna:

1) Molntjänsten löser ut identiteten via proxy-uppslag mot myndighetens egen katalogtjänst t.ex. på DMZ, eller en motsvarande federationslösning mot molntjänsten, där enbart rätt information exponeras
2) Pseudonymisering med gallring vid synkronisering. Detta innebär oftast att molntjänsten tappar funktionalitet

3) En friställd och gallrad molntjänstidentitet (ej samma som på myndigheten). Detta innebär ofta en omfattande administration och svårigheter för användarna att arbeta. Det blir ohållbart om man har många molntjänster

4) Egen kontrollerad container (i egen eller upphandlad datorhall) för molntjänsten och utan att telemetri skickas till leverantör. Detta innebär ofta en förlust att samarbeta enkelt med omvärlden t.ex. vid entreprenad

7.3 Containertekniker

Till skillnad från tidigare fysisk infrastruktur och tidigare virtualiseringstekniker är containerteknik en vidareutveckling som bryter upp den traditionella serverstrukturen ytterligare. Jämfört med virtuella servrar bryter containertekniken ner dessa ytterligare i enstaka applikationscontainers. Istället för ett operativsystem används då en containerplattform (t.ex. Kubernetes) som ger den funktionalitet en applikation kräver, utan det arbete som krävs för att t.ex. installera ett operativsystem. Detta innebär att containers många gånger är enklare att driftsätta och avveckla än traditionella virtuella servrar. Containerteknik kan även utgöra ett viktigt strategiskt val vid applikationsdrift, eller applikationsutveckling.

Många publika molntjänster tillämpar containerteknik för leverans av kunders miljöer. Det förenklar leverantörens egna interna process att driftsätta, uppdatera och lösa redundansutmaningar i molntjänstens egna datacenter. Om en myndighet på samma sätt tillämpar containerteknik i sin ordinarie infrastruktur möjliggör det en enklare integration mot molntjänster i en hybridlösning.

Bland annat AWS Outposts och Google Anthos har stöd för en distribuerad molntjänsteleverans om en myndighet sedan tidigare använder containers som är kompatibla.

Containerteknik kan vara ett lämpligt sätt för myndigheter att använda molntjänster utan att felaktigt dela myndighetsinformation. Detta beror på att många leverantörer själva bygger sina molntjänster i containerteknik vilken skulle kunna gå att återanvända ute hos myndigheten, i en egen it-miljö. Det är ytterst viktigt att myndigheten har full koll på hur kringliggande telemetridata exponeras utanför containern. Vidare behöver myndigheten

ha kontroll över eventuell synkronisering av molninformation mellan containers vilket även kan gå mellan datorhallar.

7.4 EMM - Applikationer, IoT managering och mobil utrustning

BYOD (ej myndighetsägda klienter), Smarta sensorer (IoT), mötesutrustningar (bokningstavlor och dashboard för samlad företagsinformation) och mobila enheter uppdateras ofta från publika molntjänster idag. Det kan vara uppdateringar, inställningar, backup av klienten, eller rena informationstjänster som är tänkta att hanteras via publika molntjänster direkt ut mot enheten. Myndigheten behöver fundera på vilken egen information som delas direkt eller indirekt via detta upplägg (t.ex. backuper, filer, bilder, GNSS och rörelser, e-post, loggar, chatt, personuppgifter, lista över säkerhetsbrister och säkerhetsinställningar osv). Kan ett sådant upplägg nyttjas av myndigheten? Kan myndighetens informationsmängder stoppas från delning med otillåten annan part?

Enterprise Mobility Management (EMM) och Unified Endpoint Management (UEM) är tekniska hjälpmedel för styrning och kontroll av framförallt myndighetens mobila enheter men också BYOD, IoT-enheter och viss mötesutrustning kan kontrolleras. EMM/UEM kan anskaffas både som publik molntjänst och som ”on prem” lösning och om man överväger molnalternativet bör myndigheten utreda om det är en fungerande anskaffning med tanke på den information som kan hamna i molntjänsten. Ett EMM/UEM verktyg kan också användas för att hantera och styra så att otillåten information inte hamnar utanför myndighetens kontroll (t.ex. hos app- eller mobiltillverkaren). Det är också lämpligt att bevaka trafiken som enheterna skickar externt och om möjligt hindra och styra denna trafik via t.ex. brandväggar och VPN/mVPN. EMM/UEM kan användas för att skicka ut VPN-profil till enheterna.

För mobiltelefoner finns också Mobile Treat Protection (MTP) lösningar där man ytterligare kan minimera risken för informationsläckage genom att analysera och varna för riskfyllt beteende i den mobila enheten och dess appar. I enheten körs ofta olika applikationer, här kallade appar, och användandet av vissa appar kan inbära otillåten eller oönskad informationsdelning eftersom informationen ofta behandlas och lagras i en molntjänst. EMM/UEM-plattformar har förmåga att hantera vissa appar med avseende på hur myndighetens information får hanteras. Hanterade appar kan konfigureras att endast kunna kommunicera med andra hanterade appar. Appar som inte är hanterade kan på så sätt förhindras åtkomst till myndighetens information. Vidare kan man i EMM/UEM oftast styra vilka hanterade appar som får omfattas av mobilens backup som då kan hamna hos mobil- eller apptillverkare) eller inte.

För mer detaljer, se eSams promemoria kring mobila informationssystem som avses publiceras vid senare tillfälle.

7.4.1 Råd till myndigheter för app-utveckling

Myndigheter kan med fördel införa en strategi mot Progressive Web Apps (PWA) eller ”responsiva” webtjänster vid app-utveckling. Detta låter myndigheten med egen applikationsutveckling styra var information får finnas (lokalt på mobilen, i godkända moln eller hemma på myndigheten) istället för att bara skaffa publika appar som generellt bara lagrar information i publika molntjänster. PWA-baserade appar kan publiceras via EMM/UEM verktyg så att de ser ut som vanliga standard appar för mobilanvändare. För eventuell beredskap och kontinuitetskrav innebär PWA även att appar går att nå via webbläsare på en dator lika väl som på mobiltelefon vid viss teknisk störning. Undantag från denna strategi är myndighetens eventuella behov att nå ut direkt till medborgare eller behov av att appen måste kunna nyttja notisfunktionen i mobilen (PWA kan bara notifiera användare inne i appen).

7.5 Stödsystem för informationshantering

Dessa system kan vara kraftfulla katalysatorer för it-sourcing och molnleveranser. Ett problem är att leverantörer ibland erbjuder dessa lösningar som molntjänster. Till sin natur är innehållet i dessa tjänster känsligt och inte lämpligt eller möjligt för molnleverans, men det finns leverantörer som tillhandahåller lösningar för egen drift. En svår utmaning med dessa stödsystem är att de blir mycket kraftfullare när de är tekniskt sammankopplade. Väljer man dessa lösningar bör det göras utifrån en tänkt och fungerande teknisk sammankoppling.

7.5.1 Cloud Access Security Broker

När man ska bygga upp ett lager av åtgärder för att säkra upp molntjänsten, kan en teknik som kallas Cloud Access Security Broker (CASB) vara intressant. Tekniken lovar att göra både synlighet och kontroll möjlig i molntjänster. Molnsäkerhet är huvudfokus men det finns också en möjlighet till kostnadsbesparing. Till exempel har tekniken möjlighet att upptäcka molntjänster som används och sedan rapportera dessa detaljer. Tekniken ger även möjlighet att upptäcka nyttjande av molntjänster som en myndighet bedömt inte är lämplig.

Om man flyttar mer data och system till molnet, måste man se till att de följer reglerna för att säkerställa säkerheten och integriteten för informationen.

När känsligt innehåll upptäcks i eller på väg till molnet, kan CASB-teknik möjliggöra att detaljer skickas vidare till lokala system för vidare analys. Tanken är att det ska hjälpa till att identifiera och stoppa skadlig aktivitet innan det eskalerar. Det innebär att även kunna skanna och åtgärda hot över interna och externa nätverk i realtid, när någon försöker dela eller ladda upp en infekterad fil.

CASB teknik kan också tillhandahålla datasäkerhet genom kryptering, vilket skyddar mot insyn av externa parter.

7.5.2 Data Loss Prevention

Kan kontrollera rörelse och flytt av information som t.ex. e-post, FTP, uppladdning till molntjänst och själv leta efter mönster i informationen som t.ex. personnummer, diarienummer. Det går oftast att ställa in tre nivåer av stöd eller reaktion i DLP; stoppa helt, varna för den tänkta rörelsen eller bara logga händelsen. Reglerna kan sättas upp centralt efter myndighetens egna regelverk t.ex. hur pågående upphandling får skickas externt och internt. DLP ger inget skydd när filer väl hamnat fel men i vissa scenarion kan DLP flytta information från fel plats till rätt plats. DLP fungerar bäst i teknisk sammankoppling med andra stödsystem för informationshantering.

7.5.3 Enterprise Digital Rights Management

ERDM är dels ett lås med accesslista per fil oavsett var filen finns eller vilken molntjänst filen kan ligga på, dels en integration med de vanligaste klientapplikationerna (t.ex. Acrobat Reader, Autodesk Office). EDRM sätter ett krypteringsskydd på varje fil för att skydda från oönskad access till innehållet. Filer kan tas bort med EDRM av ägaren av filen, även om de finns på ett USB minne hos någon obehörig när filen kontaktar internet och myndigheten. EDRM löser inte alla problem med att nyttja molntjänster, t.ex. personuppgiftsfrågan eller när information skapas direkt i en molntjänst. EDRM kan däremot se till att t.ex. en leverantör inte kan se innehållet i redan skapade filer, så att man ändå kan samarbeta med omvärlden via en molntjänst. EDRM fungerar allra bäst när det är tekniskt sammankopplat med övriga stödsystem för informationshantering.

7.5.4 Information governance

Information governance ger informationsägaren möjlighet att se och hantera all sin information. Det är ett företagsverktyg som centralt hanterar en informationsklassningsmodell och kopplar denna mot informationsmängder i organisationens alla it-system. Det kan vara arbetsrum, fil-areor, tabeller och alla större it-system. Man kan säga att det är den centrala sanningen om hur olika

informationsmängder är klassade digitalt. Information governance system skyddar inte informationen utan behöver kopplas samman tekniskt, med övriga stödsystem.

7.5.5 Software Defined Infrastructure

It-säkerhet fungerar bäst i lager. SDI kan hjälpa till med detta genom att låta själva it-infrastrukturen som t.ex. nätverket, lagringsskåpen, servrar, datorer och mobiler få veta vilken information som får finnas var. Viss typ av klassad information får bara exponeras på vissa platser, mot vissa roller. Detta kan i hög omfattning underlätta it-sourcing (vad får ligga i molntjänster), men också vilka roller på myndigheten som ska få vilken tillgång till information (t.ex. utvecklare, övervakning, kontorsarbetare, resande kollegor eller upphandlad entreprenad). SDI skyddar bara supporterad egen it-infrastruktur och inte okänd it-infrastruktur (t.ex. molntjänster) eller enklare nisch-hårdvara. Något system måste också mata SDI med hur information är klassad. SDI kan bli ett bra skydd för att rätt information synkas på rätt sätt i t.ex. en hybrid datacenterlösning eller ut mot företagsklienter (t.ex. ingen känslig information har access under VPN-uppkoppling). SDI fungerar allra bäst tekniskt sammankopplat med övriga stödsystem för informationshantering.

8. Metadata och telemetri

Metadata är per definition ”data som beskriver annan data” och telemetri är ”överföring av data från ett objekt”. Telemetri är i praktiken utlämning av information till leverantör som i sin tur kan sälja informationen vidare eller dra egen direkt nytta av. Det borde vara självklart att man kan stänga av funktioner för att skicka metadata till leverantören eller dess samarbetspartners, men det är sällan en realitet.

Metadata kan t.ex. visa vem eller vad som kommunicerar med vem eller vad, när, hur länge och var. Data kan utbytas med andra leverantörer och det är i den processen som aggregerad information om användare och deras enheter kan uppstå. Det samlade informationen kan i många betraktas som ett digitalt fingeravtryck.

Myndigheten bör utreda dels vilken telemetri som genomförs i it-lösningen och vad man kan göra för att konfigurera denna, dels eventuella hinder i form av t.ex. brandväggsregler i dialog med leverantören. Informationsägare som t.ex. teknisk förvaltare på myndigheten bör analysera all telemetridata och innehåll i diagnostikloggar (felsökningsloggar) för att bedöma vilken information som är ok att dela med leverantör. För mindre offentliga verksamheter blir detta svårare att hantera och man får helt enkelt vara tydlig mot leverantörer att detta är ett problem man förväntar sig att de hjälper myndigheter att hantera korrekt. Leverantörer bör kunna förklara hur de tekniskt undviker att ta del av icke delad myndighetsinformation.

Olika tekniska lösningar beskrivs ofta i termer att de är krypterade "end to end", exempelvis mellan två telefoner i en konversation, vilket skulle skydda just den informationstypen. Information som inte är direkt relaterad till konversationen som metadata samlas emellertid ofta in av leverantörer i okrypterad form. Informationen delas ofta in i tre kategorier: Information som användaren tillhandahåller, automatiskt insamlad information och tredjepartsinformation. Nedan följer några exempel från varje kategori:

8.1 Information som användaren tillhandahåller

- Information om kontot (telefonnummer, e-postadress m.m.)
- Meddelanden och texter som skrivs
- Användarens kontakter
- Eventuella supportärenden

8.2 Automatiskt insamlad information

- Användarstatistik och loggar
- Transaktionsdata (från vem, till vem, när, var, vad)
- Enhets- och anslutningsinformation (telefonnummer, IMEI, geotaggar, GNSS-position, kameramodell, IP-adresser)
- Kakor (cookies)
- Statusinformation (online, offline m.m.)
- Bilder och kontakter

8.3 Tredjepartsinformation

Tredjepartsinformation är information som andra än leverantören tillhandahåller om användaren.

En leverantör kan alltså ha tillgång till en hel del information från en mobiltelefon och utöver de som nämns ovan, är även nedanstående information ofta tillåtna om man inte förhindrar det manuellt:

- Platsdata
- Kontakter
- Bilder
- Bilders metadata som t.ex. tid, plats och datum
- Mikrofon
- Kamera
- Röststyrningsrobotar som t.ex. Siri
- Kalender

9. Slutsatser

Vid t.ex. en anskaffning av it-lösning skall man veta att teknikens roll i den totala sourcing bedömningen spelar en väldigt viktig roll. Det finns ofta en gråzon vilket område som ansvarar för olika detaljproblem, t.ex. är det område teknik, juridik, säkerhet eller inköp. Som tekniker måste man se sin roll i detta grupparbete för att få fram en hållbar bedömning. Det finns ofta tekniska aspekter man kan ta till för att möjliggöra en it-sourcing, men inte alltid. Inte minst viktigt kan dessa tekniska observationer vara av vikt för leverantörerna för att de skall förstå hur man kan bygga lösningar för att uppfylla myndigheters krav (kund-leverantörs dialog). Målsättningen med promemorian är att hjälpa till att bli mer insatt kring de tekniska utmaningarna med it-sourcing för offentlig verksamhet. Promemorian skall kompletteras med stöd från flera andra sakområden inför en totalbedömning för en it-sourcing.

Några av de verktyg som tas upp i denna promemoria samt kombination av teknisk lösning med beslutat arbetssätt kan möjliggöra vissa scenarion för viss offentlig verksamhet i en it-sourcing. Arbetsgruppen ser inte att alla it sourcingar måste förbjudas eller att alla it-sourcingar nu kan tillåtas. Av den anledningen har promemorians fokus varit på att beskriva en metod för att kunna göra en egen unik kvalitativ bedömning.

En avslutande reflektion är att för majoriteten av offentlig verksamhet finns det svåra problem med anskaffning av molntjänster. Verktygen som beskrivs i denna promemoria kan ibland inte vara tillräckligt för att stora delar av offentlig verksamhet ska kunna anskaffa flertalet molntjänster. Många av dessa problem kan gå att hantera med bättre tekniska lösningar från leverantörer. Lösningar som bättre kan möta myndigheternas krav (bl.a. gällande lagstiftning). Därmed önskar arbetsgruppen att även it-branschen tar till sig tankarna i denna promemoria.

En övergång till fullständiga molntjänster kräver att svenska lagar och regler följs, att informationen är klassad och att man har separerat informationen på lämpligt sätt. När man påbörjar överflyttning av tjänster till molnet är det viktigt att överväga beskrivna säkerhetslösningar för övervakning och kontroll samt stödsystem för informationshantering för att säkerställa att enbart godkänd information sparas i molntjänsten.

eSam är ett medlemsdrivet program för samverkan mellan myndigheter för att underlätta och påskynda digitaliseringen inom det offentliga. eSam bildades 2015 som en frivillig fortsättning på E-delegationen. En viktig uppgift för eSam är att ta fram stöd och vägledningar som ger förutsättningar för att öka den digitala samverkan inom offentlig förvaltning.

Alla stöddokument finns på esamverka.se

I eSam ingår Arbetsförmedlingen, Bolagsverket, Boverket, Centrala Studiestödsnämnden, Domstolsverket, e-Hälsomyndigheten, Ekonomistyrningsverket, Folkhälsomyndigheten, Försäkringskassan, Havs- och vattenmyndigheten, Inspektionen för vård och omsorg, Jordbruksverket, Kriminalvården, Kronofogdemyndigheten, Lantmäteriet, Länsstyrelserna, Migrationsverket, Naturvårdsverket, Patent- och Registreringsverket, Pensionsmyndigheten, Riksarkivet, Rättsmedicinalverket, Sida, Skatteverket, Skolverket, Statens institutionsstyrelse, Statens servicecenter, Statens tjänstepensionsverk, Statistiska centralbyrån, Tillväxtverket, Trafikverket, Transportstyrelsen, Tullverket och Universitets- och högskolerådet (juni 2022)