Molngruppens redovisning - Teknik, produkter och säkerhetslösningar

Det här är en redovisning av tekniskspåret från eSams arbete i det vi kallat molnfrågan. Arbetet startade under våren 2020 och har bedrivits på flera områden. I den centrala molngruppen ingår för närvarande åtta myndigheter. Till denna gruppering finns flera undergrupper som har fokuserat på olika ämnesområden där ytterligare medlemmar har deltagit. Exempel på aktiviteter i undergrupperna är leverantörsdialoger, erfarenhetsutbyten och juridiska arbeten. Avsikten med denna promemoria är att övergripande beskriva tekniska förutsättningar i molnlösningar. Den gör inte anspråk på att vara heltäckande och kan förändras över tid när förutsättningar förändras. Den första delen är av mer principiell karaktär och hållbar över tid, medan den andra delen är en ögonblicksbild över det tekniska läget. Den senare delen påverkas och förändras snabbt då det tillkommer både nya leverantörer och nya lösningar i de olika tjänsterna.

Som bilaga till promemorian redovisas en fördjupad analys av produkter för digitala möten som del av uppdraget.

Promemorians huvudsakliga målgrupper är flera kategorier av arkitekter, strateger, utvecklare, tekniker och personer på säkerhetsområdet. Den kan även med fördel läsas av beslutsfattare för att få en övergripande inblick i den tekniska komplexiteten. Syftet med promemorian är framför allt att skapa en grundläggande teknisk förståelse och utgöra grund för bra dialoger mellan olika verksamhetsområden inom organisationen. 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.

Introduktion

Att välja tekniska lösningar för att ge verksamheten rätt förutsättningar på ett kostnadseffektivt sätt, är oftast svårt och gäller också för molntjänster. Molntjänster tenderar att inte ingå i traditionell omvärldsbevakning och utmaningar kring t.ex. inlåsningseffekter är viktiga att hantera vid upphandling. Det är viktigt att man samlar in krav och behov både internt och genom omvärldsbevakning samt att överväga alternativa tekniska lösningar. En komplex fråga av den här arten, bör myndigheten inte skynda på.

Väljer myndigheten att använda sig av molntjänster är det viktigt att ha rätt kompetens under hela utrednings- och införandefaserna. Den tekniska lösningen behöver analyseras grundligt vid införande av en eller flera molntjänster.

Principer

Promemorian bygger på den komplexitet som finns bland molntjänster, både avseende leveransmodell och funktionalitet. Vi har tagit fram tre principer som bör styra myndigheters arbete med molntjänster och för att möjliggöra en lagenlig hantering.

Myndigheter kan använda molntjänster när tre principer är uppfyllda;

- Endast information som myndigheten godkänt för molntjänsten, får hanteras i aktuell tjänst,
- att molntjänsten eller tillägg till tjänsten säkerställer skydd mot möjlig leverantörsinsyn,
- molntjänsten är driftsatt i en it-miljö där myndigheten har kontroll, t.ex. egen container.

Förutom de tre principerna 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. Information om detta informationsläckage måste respektive myndighet ställa krav på leverantören att redovisa, för att säkerställa att skyddsvärd information inte röjs.

Teknisk inriktning

Avsnittet ska ge stöd för att kunna agera korrekt och rimligt avseende teknik vid utkontraktering och val av teknisk lösning. Inriktningen är definierad baserat på följande antagande:

> Information som läggs i en it-sourcing (inklusive moln) måste betraktas som delad information om man inte tydligt kan visa motsatsen;
> Tillverkaren av en publik molntjänst har rimligtvis teknisk insyn i hela sin tjänst. Detta gäller även vid specifika skyddslösningar framtagna av samma tillverkare för samma molntjänst.

Antagandet är baserat på lagkrav för molntillverkare att kunna lämna ut kunddata ur sin tjänst vid utlämningsärenden i vissa länder.
Detta föranleder följande förhållningssätt för denna inriktning:

1) Premiera tekniska lösningar där en tredjepart tekniskt skyddar kundens data. Det är inte tillräckligt att enbart förlita sig på skyddslösningar framtagna av molnleverantören. Ingen av leverantörerna ska få oönskad insyn till kunddata med den valda lösningen.
2) Om man måste utgå från inbyggda skyddslösningar eller om tredje part får oönskad insyn, måste den berörda myndigheten hitta alternativa sätt att skydda myndighetens information i tjänsten (se avsnitt ”Tips för att tekniskt skydd av myndighetsinformation i moln”).
3) Endast leverantörer som genom oberoende granskningar, kan påvisa att insyn i kunders information förhindras genom implementerad teknisk arkitektur och design, kan rimligen anlitas av eSams medlemmar. Leverantörer får i detta fall en stor bevisbörda att tydligt visa hur de implementerat sin infrastruktur och att det finns en tillämplig ackreditering av implementerade säkerhetslösningar.

Arbetssätt att utreda molntjänst för myndigheter

Eftersom myndigheter har lagkrav på hur information måste hanteras och eftersom it-sourcing inklusive molntjänster, innebär en informationsdelning med leverantörer, behöver det finnas arbetssätt för att ge myndigheten förutsättningar till en korrekt utredning för att kunna implementera en molntjänst. För att lyckas med utredningen behövs en leverantör som förstår 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? Leverantören och grundlig omvärldsbevakning kring molntjänsten är två metoder som kan användas för denna insamling av information. Kan myndigheten inte tydliggöra denna fråga 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 inklusive en eventuell inplacering i säkerhetsklass. 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. informationsklassning och en rättslig bedömning. Här bör verksamhetsansvarig med fördel ta stöd av myndighetens jurister, personuppgiftsombud samt informations- och it-säkerhetsexperter.
4) Myndigheten behöver, baserat på informationsklassningen, identifiera vilken information som kan röjas utan att det innebär någon skada för myndigheten eller tredje part. Respektive myndighet bör inkludera rättsavdelning och säkerhetsavdelning för att stötta i denna fråga.
5) 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.
6) 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 verksamhetens behov, bör alternativa lösningar utvärderas. När myndigheten ska kartlägga vilken information som exponeras totalt sett i respektive molntjänst (steg 1), kan myndigheten konsultera standarder som t.ex. CSA:s Consensus Assessments Initiative Questionnaire.

Denna metodik för utvärdering av externa tjänster blir allt vanligare. Med hänsyn till det bör respektive myndighet öka sin kompetens för denna typ av upphandling eftersom flertalet leverantörer går från licensieringsmodeller till tjänsteleveransmodeller.

Den gemensamma kompetensen bör finnas inom teknik, juridik, 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.

Utöver respektive myndighets förmåga att kunna genomföra ovanstående analyser, kommer eSam att stötta medlemmarna i egenskap av kompetensnav för att kunna dela erfarenheter och kunskap. 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.

Lösningar

Informationsklassning

En förutsättning för att kunna använda molntjänster är att informationen är informationsklassad. Denna bedömning ska ske innan den läggs i molntjänsten. Klassningen kan bestå av flera perspektiv som är kritiska för myndigheten t.ex. enligt dess föreskrifter. Varje myndighet kan även välja att lägga till aspekter i klassningsmodellen beroende på verksamhet. Vid användning av klassningsmodellen rekommenderas även att klassningen på lämpligt sätt blir digital så att den kan hanteras i it-infrastrukturen. Detta underlättar också hantering av information för eventuellt beslut om att kunna hanteras i en molnlösning.

Ett mål i myndighetens arbete med informationshantering är att det skall vara ”lätt att göra rätt”, vilket ofta krävs av de digitala stödsystem som vi beskriver i detta dokument. Ett annat mål som måste formuleras när en myndighet planerar att införa molntjänster, är hur man ska hantera en situation då fel information hamnar på fel ställe t.ex. sekretessuppgifter i en publik molntjänst. Vem gör vad? Hur kan dessa fel undvikas?

Informationsseparering

En viktig funktion för it-sourcing och till viss del molnleveranser, är att ordna lämpliga separationer i en it-infrastruktur utifrån lagkraven för myndigheters informationshantering. Informationsepareringen bör lämpligtvis utgå ifrån resultatet av informationsklassningen. Att skydda känslig information kan göra det lättare att utkontraktera t.ex. icke-känslig 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.

Berörda lagar ställer inte heller krav på hur en teknisk separation ska göras och de befintliga tekniker som finns, medför stora skillnader mellan myndigheters implementationer både i direkt och indirekt kostnad. 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 multipla företagsklienter och användarkonton. Även teknik för virtuella klienter kan vara ett stöd för myndigheten att på ett enklare sätt, jobba mot den allt mer komplexa it-infrastrukturen. Myndigheterna 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 handlingar kan läggas i molnet eller inte, om de är informationsklassade. Informationsmängder är ofta aggregerad information vilket leder 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 till samma komponenter. Detta möjliggör sedan att t.ex. flytta komponenter med information av låg känslighet, till en molnlösning.

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 molntjänstteknik 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.

AWS Outposts

Amazon Web Services (AWS) Outposts är en tjänst som levereras av Amazon Web Services. Tjänsten utökar deras traditionella molninfrastruktur, tjänster och verktyg till kundens egna datacenter. Att ha tjänsten inom det egna datacentret ger fördelar för arbetsbelastningar som kräver låg latensåtkomst till lokala system, lokal databehandling eller lokal datalagring.

Lösningen möjliggör att bygga och köra applikationer lokalt och i molnet för en konsekvent hybridupplevelse. Exempelvis kan beräkning, lagring, databas och andra tjänster köras lokalt, medan man kan komma åt hela utbudet av leverantörens molntjänster för att bygga, hantera och skala lokala applikationer.

Lösningen förvaltas delvis av leverantören på distans från den närmaste regionen för att exempelvis installera säkerhetsuppdateringar. Detta innebär att det inte är en helt privat tjänst, utan ett sätt att säkerställa att informationen finns lokalt och möjliggöra bättre prestanda. En av de risker man måste bedöma är huruvida sådan åtkomst är lämplig utifrån de applikationer och data som ska levereras.
Alternativ till AWS Outposts är AWS Snowball Edge, som kan leverera enstaka funktionalitet utan behov av uppkoppling mot närmaste region. Funktionaliteten är dock begränsad till enstaka EC2 instanser och AWS Lambda funktioner ihop med S3. Snowball Edge har till exempel inte tillgång till AWS RDS vilket kan vara ett krav för många myndigheter för att kunna tillgodogöra sig lösningen på ett effektivt sätt.

Azure Stack Hub

Azure Stack Hub är en del av Azure Stack-portföljen från Microsoft och breddar molnlösningen Azure till en lokal instans i myndighetens egna datacenter. Att bredda en molnlösning till myndighetens egen it-infrastruktur är ofta en förutsättning för att kunna genomföra en snabb och effektiv utvecklingsprocess i verksamheten. Detta härrör framförallt i skalbarheten i lösningen där utvecklare har möjlighet att enskilt skapa egna instanser med minimal kringliggande administration.

Fördelen med lösningen är att svarstiderna till övriga system blir snabbare, eftersom tjänsten Azure Stack Hub installeras lokalt. Azure Stack Hub är även byggt för att kunna köras helt avskilt från internet, något som är lämpligt för känsliga it-miljöer eller där myndigheten vill undvika delning av telemetridata med leverantören.

En nackdel med en helt internt frånskild Azure stack-lösning, är att myndigheten får mindre funktionalitet på sin lösning än motsvarande Azure-lösning hos Microsoft.

Om myndigheten har höga krav på korta svarstider, eller om man vill behandla känslig information utan att funktionaliteten finns, bör man analysera om Azure Stack Hub är en lämplig lösning. Det finns möjlighet att behandla känslig information i Azure Stack Hub med en slutprodukt som inte anses känslig. Slutprodukten kan förmedlas vidare och behandlas i den ordinarie molnvarianten av Azure. Eftersom både Azure och Azure Stack Hub delar mycket av programlogik och arkitektur, finns möjlighet till en smidig överföring av information utan stora krav på komplexa integrationer.

Azure Stack Hub förutsätter att en myndighet kan förvalta lösningen självständigt varför det är viktigt att myndigheten har kunskap om plattformen, eftersom det kan uppstå komplicerade problemlösningar.

Google Anthos

Google Anthos är en plattform som likt de andra lösningarna förlänger Googles moln till den egna datahallen. Anthos, är en plattform som i sin helhet ger myndigheten möjlighet att driftsätta egna kubernetes-instanser, också benämnda containers.

Plattformen kan driftsättas på två olika sätt, antingen som virtuell plattform på en infrastruktur som hanteras genom Vmware eller direkt på fysiska instanser (baremetall). Beroende på leveransform, får också myndigheten tillgång till olika typer av funktionalitet.

Vid driftsättning på en Vmware infrastruktur förlitar sig Anthos på den funktionalitet för nätverkshantering som levereras av Vmware. Myndigheten kan sedan konfigurera nätverk mellan de containers som är i drift inom den virtuella Anthos instansen. En stor fördel med driftsättning på en Vmware plattform är att myndigheten får tillgång till driftsättning enbart av granskade containers. Granskning genomförs av Google som säkerställer att den image som används är korrekt genom binary authorization i plattformen.

Vid driftsättning på en baremetall infrastruktur får myndigheten ett större ansvar att administrera den kringliggande miljön inklusive nätverkstopologi och nätverkssäkerhet. Den Anthos-instans som är installerad på myndighetens hårdvara, har ingen möjlighet att hantera denna del av infrastrukturen vilket innebär en högre administrativ börda. Myndigheten får däremot möjlighet att genomföra direkt nätverksadministration inom Anthos-instansen för de nätverk som är tillförlitliga genom Ingress for Anthos, vilket är den rekommenderade vägen in i Anthos.

Övriga lösningar

Flertalet lösningar har undersökts, men baserat på eSams medlemmar har huvudfokus varit på de tre stora leverantörerna av molntjänster. Utvärderingen av dessa tre ska inte ses som en uttömande utvärdering eftersom det finns alternativ. Varje myndighet bör därför komplettera denna promemoria med sin egen analys med utgångspunkt från det metodstöd som levererats, inför val av teknik.

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.

Säkerhetslösningar för övervakning och kontroll

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.

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 provisionerade 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) Rekommenderat upplägg: 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, se federering ovan.
2) Anonymisering med gallring vid synkronisering. Detta innebär oftast att molntjänsten tappar funktionalitet.
3) En friställd och gallrad molntjänstidentitet. Detta innebär ofta omfattande administration och svårigheter för användarna att arbeta, vilket kan bli ohållbart om man har många molntjänster.
4) Container för molntjänsten utan att telemetri skickas till leverantör. Detta innebär ofta en förlust att samarbeta enkelt med omvärlden t.ex. vid entreprenad.

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.

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

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

Utöver fördelarna kring administration kan containerteknik vara ett lämpligt sätt för myndigheter att använda molntjänster utan att felaktigt dela myndighetsinformation. Genom att hantera containers har myndigheter större möjlighet att styra vilket innehåll som hanteras istället för stora och komplexa system. 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.

Även om containerteknik är en vidareutveckling av virtualiseringstekniken behöver myndigheten ha tillräcklig kontroll på kringfunktioner som säkerhetskopiering och övervakning för att säkerställa korrekt kontinuitetshantering.

Applikationer och utrustning

Smarta sensorer, mötesutrustningar och liknande kan uppdateras från molnet eller styras från en molntjänst av användaren. Myndigheten behöver utgå från informationsvärdet och det aggregerade värdet av informationen om man hanterar många enheter. Det bör gå att undvika personuppgifter i denna typ av utrustning.

Enterprise Mobility Management (EMM) och Unified Endpoint Management (UEM) är tekniska hjälpmedel för styrning och kontroll. Mötesutrustning kan ofta hanteras via moln eller annan lokal lösning. Vilken man väljer behöver bero på vilken information som delas var. Det är också lämpligt att bevaka trafiken som enheterna skickar externt och om möjligt stoppa denna trafik via ex. brandväggar.

Exempel på EMM lösningar är Intune, WorkspaceOne, MobileIron, Blackberry och JAMF. För mobiltelefoner finns Mobile Treat Protection (MTP) lösningar som Zimperium, ATP och Lookout. Ofta används en EMM-plattform för att hantera och förvalta mobiltelefoner och dess inställningar samt för att hantera de applikationer man vill skydda, så kallade ”Managed Apps”. Dessa kontrollerade applikationer kan konfigureras för att bara kunna kommunicera med andra kontrollerade applikationer. På så sätt differentieras information som hanteras från icke-kontrollerade applikationer.

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 styra var information får finnas (lokalt på mobilen, i godkända moln eller hemma på myndigheten). PWA-baserade appar kan publiceras via EMM/UEM verktyg så att de ser ut som vanliga standardappar 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).

Stödsystem för informationshantering

Dessa system kan vara kraftfulla katalysatorer för it-sourcing och molnleveranser. Ett problem är att stora leverantörer levererar dessa lösningar som molntjänster. Till sin natur är innehållet i dessa tjänster (känslig information) inte lämpliga eller möjliga för en egen molnleverans men det finns vissa större och mellanstora leverantörer som tillhandahåller lösningar lokalt (on prem). 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.

CASB – 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.

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.

DLP – Data Loss Prevention

Kan kontrollera rörelse/flytt av information som t.ex. e-post, FTP, uppladdning till molntjänst och själv leta efter mönster i informationen som t.ex. personnummer, diarienummer osv. 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. DLP fungerar bäst i teknisk sammankoppling med andra stödsystem för informationshantering

EDRM – Enterprise Digital Rights Management

ERDM är dels ett lås med accesslista per fil oavsett var i världen filen finns eller vilken molntjänst filen kan ligga på, dels en integration med de vanligaste klientapplikationerna (t.ex.Acrobat Reader, Autodesk Office osv). 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 en USB-sticka hos en hacker någonstans i världen (när filen kontaktar internet och myndigheten). EDRM löser inte personuppgiftsfrågan med molntjänster och inte heller information som skapas direkt i en molntjänst. EDRM kan däremot se till att leverantör inte kan se innehållet i redan skapade filer, så att man ändå kan samarbeta med omvärlden via viss molntjänst. EDRM fungerar allra bäst när det är tekniskt sammankopplat med övriga stödsystem för informationshantering.

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.

SDI – 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 molnlösningar), 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.

Tips för att tekniskt skydda myndighetsinformation i moln

Tillverkaren av en molntjänst (t.ex. ett amerikanskt bolag) kan bygga vilka AI-indexjobb som helst i sin molntjänst. Befintliga lagkrav kan innebära att tillverkaren dels måste kunna lämna ut kunddata, dels att kunden inte får informeras om detta. Så hur ska myndigheten kunna skydda sig tillräckligt?

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 nyttiga tips:

- Överväg att införa/nyttja ett informationsgovernace stödsystem. Det kan ge allmän kännedom om vilken digital information som har vilket värde, på myndigheten. Se kapitel ”Stödsystem för informationshantering” ovan.
- 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” ovan.
- 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/information skall finnas, om man gjort en smart separation. Se kapitel ”informationsseparering” ovan.
- Planerade åtgärder för cybersäker information i molntjänsten, behöver också knytas till värdet av informationen (även aggregerat). Även om känslig och säkerhetsskyddad myndighetsinformation mindre troligt förekommer i publika molntjänster, kan fortfarande riktighet, spårbarhet och tillgänglighet vara viktigt. Om den inbyggda cybersäkerheten i molntjänsten inte skulle hålla måttet, kanske en tredjepartslösning kan bli en godkänd lösning.
- 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.
- För att skydda filer (innehållet) kan man överväga en DLP & EDRM-lösning. Filer måste först skapas utanför molntjänsten och namnet på filen får inte i sig innehålla fel information (t.ex. säkerhetsskyddad). Se kap ”Stödsystem för informationshantering” ovan.
- 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 kap “CASB – Cloud Access Security Broker” ovan.
- 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. Se kap ”Katalogtjänst synk & SSO” ovan.

- DLP, diodteknik eller SDI kan vara ett stöd vid systematisk flytt av information t.ex. integration/systemkoppling för att förhindra ett felaktigt informationsflöde och stoppa manuella fel.
- Vid systemåterställning och övervakning kan en extern eller alternativ lösning föredras 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 informationsklass för myndigheten.
- 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 tillräcklingt. Myndigheter bör inte vara beroende av annat land i dessa molntjänster vilket också gäller drift och administration.

Slutsatser

En övergång till fullständiga molntjänster kräver att informationen är klassad och att man har separerat informationen i så många olika komponenter som möjligt. Parallellt med detta kan man börja arbeta med hybridlösningar. Det är relativt enkelt att senare göra förflyttningen från hybridlösning som driftas inom organisationen, till en ren molntjänst som driftas i en annan region. När man påbörjar överflyttning av tjänster till molnet är det viktigt att överväga stödsystem för informationshantering, exempelvis att kontrollera molnanvändning för att säkerställa att enbart godkänd information sparas i molnet.

Bilaga

Digitala möten

Digitala möten kan delas upp i tre kategorier för att både kunna utnyttja alla fördelar och samtidigt hantera olika nivåer av konfidentialitet.

Säkra digitala möten	Digitala möten	Digital konferens
Säkerhetsskyddsklassificerad information	**Lägre informationsklass**	**Öppen information**
Godkända system för hantering av informationen	Möten med omvärlden Kontorstelefon Status	Avlyssning spelar ingen roll. Ingen teknisk koppling till myndigheten.
Teknikförslag (förslag utifrån givna förutsättningar i en fiktiv myndighet)		
Cisco Meeting, Next cloud, Pexip	Skype för företag	Google meeting, Slack, Zoom, Goto meetings, Microsoft Teams, Webex

Det är viktigt att tänka på hur man skyddar myndighetens information från t.ex. misstag i informationsdelning eller personuppgifter när man deltar i digitala möten med omvärldens egna mötesplattformar.

I digitala möten kan det som sägs muntligen, delas på skärm, deltagares personuppgifter, fildelning, sådant som skrivs i chatt och loggas/lagras i mötet bli problematiskt ur ett tekniskt och juridiskt perspektiv.

Det är också viktigt att planera i förväg för hur teknikförslagen är tänkta att användas. Exempelvis kan ett agentlöst deltagande och spärr för filutbyte via webbläsare, vara ett alternativ. Programvarorna kan också paketeras för mötesklienter så att användaren får mer ansvar för att själv att hantera informationen.

Telemetri/metadata

Telemetri är utlämning av information till leverantör som i sin tur kan sälja informationen vidare. Det borde vara självklart att man kan slå av funktioner för att skicka metadata till leverantören eller dess samarbetsparter, 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. Datat kan utbytas med andra leverantörer och det är i den processen som aggregerad information om en användare eller dennes enhet kan uppstå. Det kan i många fall kan jämställas med ett fingeravtryck.

Myndigheten bör utreda dels vilken telemetri som genomförs i it-lösningen och vad man kan göra för att stoppa konfiguration, dels eventuella hinder i form av t.ex. brandväggsregler i dialog med leverantören. Informationsägare som t.ex. teknisk förvaltare på myndigheten, bör även bedöma all telemetridata och innehåll i diagnostikloggar (felsökningsloggar) för att bedöma vilken information som är ok att dela fritt med leverantör.

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

Information som användaren tillhandahåller

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

Automatiskt insamlad information

- Användarstatistik och loggar
- Transaktionsdata (från vem, till vem, när, var, vad)
- Enhets- och anslutningsinformation (Telefonnummer, IMEI, Geotaggar, GPS-position, kameramodell, IP-adresser)

- Kakor (Cookies)
- Statusinformation (Online, Offline mm)
- Bilder och kontakter

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
- Mikrofon
- Kamera
- Röststyrningsrobotar som t.ex. Siri
- Kalender

Fördjupad analys av produkter

Här redovisas en fördjupad analys av produkter för digitala möten som del av uppdraget. Huvudfokus har varit på två produkter baserat på aktuella frågeställningar hos eSams medlemmar.

Utvärderingen av produkterna är inte uttömmande eftersom det finns alternativ och det ska inte heller tolkas som att dessa två rekommenderas att använda, utifrån denna promemoria.

Zoom

Zoom är ett sammarbetsverktyg som är enkelt och intuitivt att använda när man väl installerat klienten. Zoom lagrar användaruppgifter och annan metadata i molntjänsten även vid ”on prem” lösning. Klienten finns för flera olika plattformar och operativsystem, Windows, MacOS, iOS, Android m.fl. Det finns även ett tillägg för webbläsarna Firefox och Chrome för att kunna schemalägga Zoom-möten i sin Googlekalender. Zoom drivs av ett amerikanskt företag (Zoom Video Communications, Inc) som tillhandahåller videotelefoni- och chat-tjänster genom en molnbaserad IT-

plattform som används i samband med videokonferenser, distansarbete, distansundervisning och underhåll av sociala nätverk. Företagets tjänster konkurrerar bland annat med Skype, Google Hangouts och Facebook Messenger.

Man bör ta ställning till om man ska använda gratistjänsterna Pro, Business eller Enterprise eller om man ska använda Zoom On-Premise. Zoom On-Premise kan övervägas om man har krav på att mötestrafiken (video, röst, chat och dokumentdelning) inte ska hamna i en publik molntjänst. Man använder sig istället av connectorer, eller virtuella maskiner, för att styra innehållet till en privat molntjänst. Man ska dock vara observant på att användarinformation och metadata fortfarande hanteras i den publika molntjänsten.

För att sammanfatta säkerhetsläget runt Zoom-tjänsten kan följande punkter ge en fingervisning om vad man bör beakta innan tjänsten tas i bruk:

- Det har funnits oklarheter i Zooms marknadsföringsmaterial om kryptering vilket har skapat ett förtroendeglapp.
- Om en organisation använder lämplig tjänst (oftast Business eller Enterprise-tjänsten) samt konfigurerar denna med t.ex. SSO så är Zoom en relativt säker digital mötesplats när mötesinnehållet är av ringa värde.
- Undvik gratisvarianten eftersom den saknar funktionen att använda administrativa tvingande inställningskontroller.
- Flera av de åtgärder som gör möten säkrare, är avstängda som standard. Dessa måste aktiveras för att förhindra att någon medvetet eller omedvetet gör fel.
- Använd Business eller Enterprise. Slå på MFA eller SSO och justera mötesinställningarna för en ökad säkerhet.
- Använd slumpade möteskoder.
- Använd lösenord för att ansluta till möten.
- Använd väntrumsfunktionen.
- Lås mötet för nya anslutande deltagare innan mötet startar.
- Använd alltid den senaste versionen.
- Utbilda användare att hantera och kontrollera sina möten, klassificera information samt mötesetikett.

Teams

Syftet med Teams är ett nytt sätt att samarbeta digitalt, inte en ersättare för Skype för företag. Båda produkterna kommer att samexistera men de mest innovativa samarbetsfunktionerna finner man i Teams. Teams riktar sig mot friare och öppnare

samarbeten, hantering av känslig information är inte en grundtanke med Teams, det kräver en annan plattform för samarbete (exempelvis Skype för företag).

Teams som plattform har stora anpassningsmöjligheter för kunden men det är inte en egen fristående mjukvara.

- Kundens Active Directory (AD) måste delas i en molntjänst för att kunna användas. Det är en del av licenshanteringen.
- Teams kräver SharePoint Online (indirekt OneDrive for business). Kravet kommer från fildelning men är ett grundkrav även om fildelning kan stängas av centralt. Syftet med Teams är den bredaste definitionen av digitalt samarbete. Filer kan inte läggas i SharePoint installerat on prem.
- Teams kräver en Exchange server. Beroende på vilken version som används on prem, kan det finnas begränsad funktionalitet med Teams men on prem Exchange är tillåtet (till skillnad från SharePoint).
- AI och Indexeringsjobb sker löpande runt Teams och går inte att stänga av eftersom de är kritiska funktioner. Funktioner som kategorisering av audit loggar, eller ”noise cancellation” teknik av störande bakgrundsljud kan också finnas.
- Det finns flera integrationer med andra plattformar som redan är förberedda. Kunden kan centralt slå av eller på dessa (Facebook, Youtube osv).
- Teams är en del av Office365. Som myndighetsanställd måste man ha ett Office365-konto för att kunna bjuda in till ett möte i Teams. Det kan däremot fungera att ansluta som gäst i ett Teams-möte som anordnas av annan användare om mötesarrangörens organisation så tillåter. Att gå från ingenting till Teams ställer en stor mängd underliggande krav, det blir inte bara Teams man skall konfigurera utan också en stor mängd andra IT lösningar.
- Teams har en stor mängd säkerhetsfunktionalitet inbyggt. Detta bygger på en version av en säkerhetmolntjänst, och det finns t.ex. en inbyggd DLP funktion för Teams. Detta innebär ytterligare en integration att hantera (förutom SharePoint, Exchange osv).
- När ett team skapas i Teams så skapas också tekniska ytor i alla underliggande system automatiskt. Detta är styrkan jämfört med t.ex. Skype för företag där ett SharePoint arbetsrum måste skapas manuell och för sig. Funktionen är inte valfri i Teams, utan sker varje gång ett nytt team sätts upp.
- Med Teams följer också en hantering av Planner och Yammer för företagskunder (förutom DLP, SharePoint, Exchange osv).

- Det finns en plattform kallad Stream, där alla möten spelas in och lagras. Detta skapas också automatiskt för varje möte och för alla team i Teams. Det gör det lätt att i efterhand se möten som man missat (om man är behörig). Som användare av Teams måste denna information också tas i beaktande.
- Det finns stor möjlighet att Teams kan matcha lagkrav mot myndigheter för loggning samt audit. Många detaljer loggas och arkiveras. Som kund kan man styra vilka loggar och förutsättningar som skall gälla för vilken tid.
- I Teams finns ”Live Event”, en liknande funktion som finns i Zoom. Den kan hantera många samtidiga videoströmmar i ett möte och har också funktionalitet för gruppdiskussionsrum.