Rapport

Att analysera molntjänster– några utgångspunkter

ES2025-02

Mars 2025

Innehåll

1. Sammanfattning

Den här rapporten syftar till att ge en överblick av några av de frågeställningar som kan bli aktuella och vilka kritiska moment som kan uppstå när en myndighet tänker utkontraktera eller anskaffa en it-förmåga, exempelvis en publik en molntjänst.

Att analysera en molntjänst är komplext och ett sådant arbete innehåller många olika överväganden. Rapporten ger ett stöd till beslutsfattare och andra som berörs när myndigheten ska anskaffa eller utkontraktera en molntjänst.

I rapporten beskrivs olika typer av molntjänster. Flera överväganden behöver göras i en analys inför anskaffning eller utkontraktering, bland annat:

- Identitetshantering. Nästan alla molntjänster har en inloggningsfunktion som myndigheter behöver hantera.
- Informationshantering. En kritisk grundförutsättning för hur myndigheter kan nyttja molntjänster är att informationen värderas och skyddas utifrån konfidentialitet, riktighet och tillgänglighet.
- Kontinuitet. Myndighetens verksamhetskontinuitet måste säkerställas vid utkontraktering, även utifrån ett totalförsvarsperspektiv.
- Tekniska skyddsåtgärder. Som skydd mot säkerhetsincidenter behöver myndigheten vid en anskaffning och utkontraktering säkerställa rätt ställda krav runt tekniska skyddsåtgärder.

Rapporten tar även upp en rekommenderad arbetsmetodik som stöd vid analys av molntjänster. Att arbeta med tvärfunktionella analysgrupper som kombinerar juridisk, teknisk och strategisk kompetens ger ett bra stöd för myndigheten i sin bedömning.

2. Inledning

Att anskaffa eller utkontraktera en förmåga är ett *strategiskt försörjningsbeslut* som kräver noggrann analys. Myndigheten behöver förstå vad anskaffningen eller utkontrakteringen innebär och vilka krav den medför.

Många myndigheter står inför olika överväganden i samband med anskaffning eller utkontraktering av it-system. Trenden visar att fler leverantörer övergår till molnbaserade lösningar i stället för att erbjuda lokala, så kallade on-premiseslösningar. Detta ökar kraven på myndigheters förmåga att analysera och hantera molntjänster.

För att kunna utkontraktera ett system måste myndigheten informationsklassa befintliga interna system och skapa kapacitet för att hantera integrationer med ett eller flera externa system.

En myndighet behöver vara medveten om innebörden och konsekvenserna av att vissa system fungerar som en huvudkälla för information och bör förbereda sig för att hantera olika utmaningar och risker i den valda lösningen. Myndighetens uppdrag ur beredskapsperspektiv måste också beaktas vid val av lösning. Leverantörens förmåga och möjligheter att leva upp till myndighetens krav behöver bedömas.

2.1 Syfte

Syftet med rapporten är att ge en överblick över några av de frågeställningar som kan bli aktuella och vilka kritiska moment som kan uppstå när en myndighet tänker utkontraktera eller anskaffa en molntjänst.

2.2 Avgränsning

Den här rapporten omfattar inte alla överväganden som en myndighet behöver göra. Myndigheten behöver bland annat göra juridiska överväganden beroende av vilka uppgifter som ska utkontrakteras. Flera regelverk kan bli aktuella i varje enskilt fall då omständigheterna och myndigheternas förutsättningar varierar.

För juridiskt stöd hänvisas till eSams vägledning *Utkontraktering – sekretess och dataskydd*[1] som behandlar frågor om sekretess, dataskydd, allmänna handlingar och informationssäkerhet. En annan fråga som myndigheten behöver säkerställa är att

[1] ES2023-06 Vägledning Utkontraktering – sekretess och dataskydd.

avtalen är bra utformade vad gäller villkoren för användandet av tjänsten. För stöd om avtalsvillkor hänvisas till eSams mallar för allmänna it-villkor[2].

2.3 Målgrupp

Rapporten riktar sig till beslutsfattare och andra som berörs när myndigheten ska anskaffa eller utkontraktera en it-förmåga, exempelvis till en publik molntjänst. Rapporten kan även vara av intresse för en bredare krets.

2.4 Medverkande

Rapporten har tagits fram av eSams molngrupp som inkluderar följande kompetenser: digitaliseringsjurister, inköpsspecialister, it-strateger, verksamhetsutvecklare, säkerhetsspecialister, it-arkitekter och it-säkerhetsspecialister.

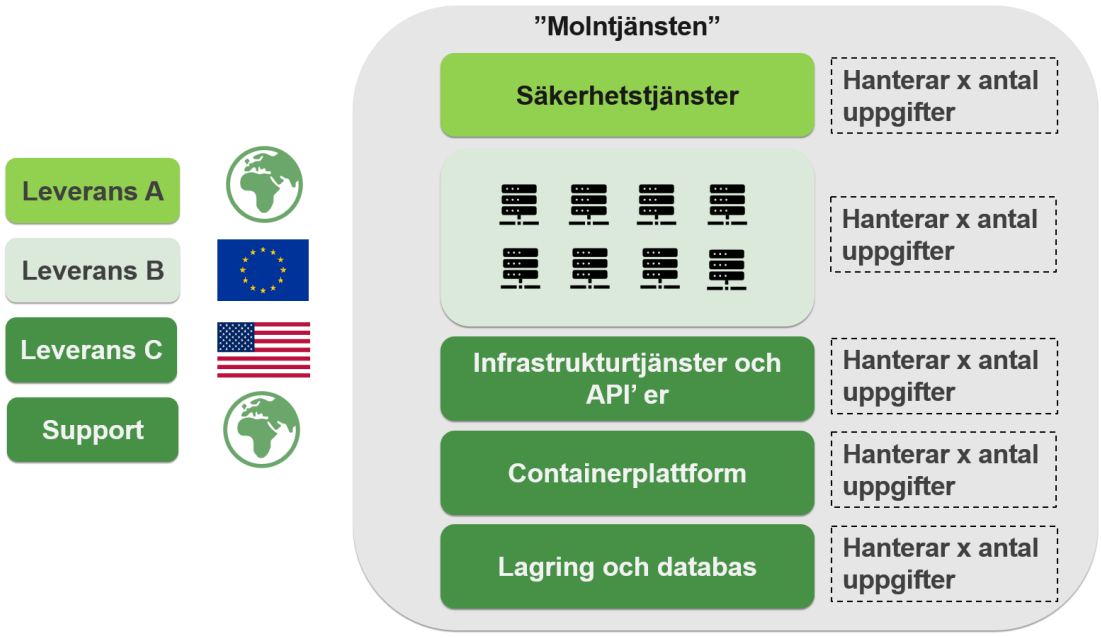
[2] Se typen it-avtal på www.esamverka.se

3. Ägarförhållanden

Det finns olika typer av publika molntjänster. Beroende på typ skiljer sig de rättsliga och tekniska förutsättningarna, liksom hanteringen av skyddsvärd och känslig information. Dessa faktorer kan påverka vilka krav som kan ställas vid en anskaffning. För fördjupning, hänvisas till eSams vägledning *Utkontraktering – sekretess och dataskydd*.

Vissa molntjänster utgår från amerikanskt ägda hyperscalers[3], som är de största leverantörerna på marknaden ur ett globalt perspektiv. Andra molntjänster har underliggande infrastruktur och ägarstruktur baserad i EU/EES eller i Sverige. Några tekniska skillnader för molntjänster beskrivs i kapitel 7 Applikationsdriftsplattform.

Ägandeförhållanden är en viktig del för myndigheten att undersöka då extraterritoriell lagstiftning påverkar bedömningen, liksom att kartlägga vilka underbiträden som används och deras geografiska placering. Detta är av betydelse vid exempelvis bedömningar om tredjelandsöverföring. Det gäller också delkomponenter i molntjänsten som har tillgång till kundinformation, exempelvis för övervakning och support. Dessa delkomponenter kan utgöras av andra externa molntjänster, vilka i sin tur lyder under olika lagar beroende på deras geografiska och juridiska hemvist. Ett exempel på detta är en svensk molntjänst för rekrytering som använder en support- och ärendefunktion baserad på en molntjänstleverantör med säte i USA.



Figur 1, exempel på övergripande uppbyggnad av en globalt konstruerad molntjänst och dess underleverantörer där kundens informationsmängder hanteras

[3] Om hyperscale computing, förklarande artikel läst 241212; https://en.wikipedia.org/wiki/Hyperscale_computing

I eSams vägledning *Utkontraktering – sekretess och dataskydd*, beskrivs vilka bedömningar som behöver göras kring ägandeskap och geografisk placering. Myndigheten behöver också undersöka infrastruktur och vilka komponenter som ingår i tjänsten. I avsnitt 10.3 och 10.4 nedan ges tips på metod för att få fram information om ägarskap, tekniska komponenter m.m.

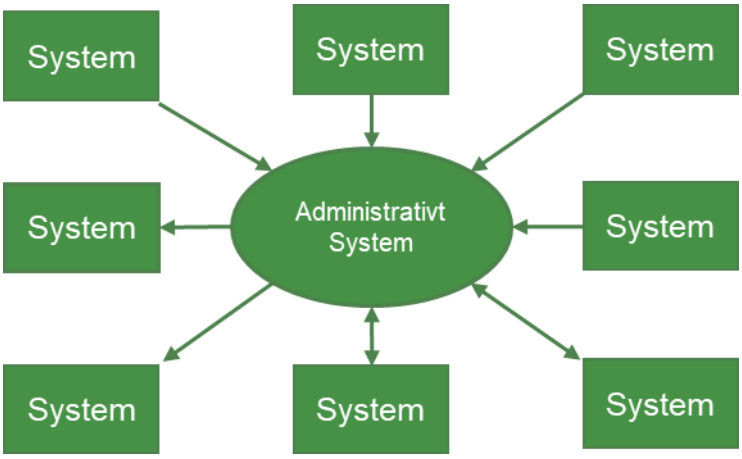
Molntjänster kan även ha olika typer av tillgängliga skyddsåtgärder, de kan exempelvis levereras som en helt separerad privat molntjänst som endast kan nås av den konsumerande organisationen. Det finns även olika former av hybrida molntjänster som gör det möjligt att hantera eller lagra data i sitt eget datacenter.

4. Spindeln i nätet

Vissa interna it-system fungerar som huvudkällor för information till andra system i en organisation. Ett exempel är ekonomisystem, som ofta används av lönesystem och tidsrapporteringssystem och fungerar som en så kallad masterdatakälla för HR-information. De informationsmängder som systemet är masterdatakälla för, ska därför hanteras med omsorg och enligt gällande krav.

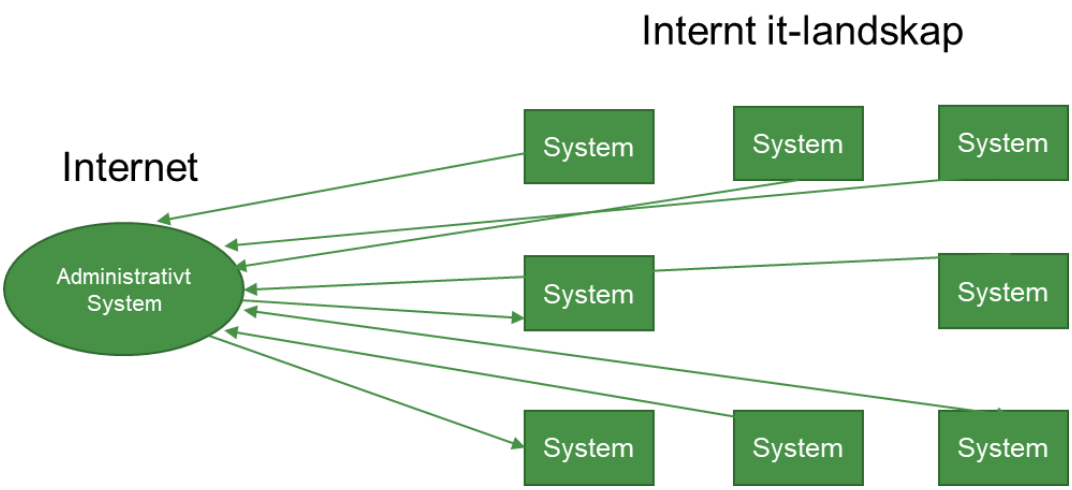
Ekonomisystem och HR-system innehåller ofta verksamhetskritisk information och fungerar som nav för organisationens informationstillgångar. Därför bedöms dessa system i merparten av fallen som verksamhetskritiska.

Myndigheter integrerar ofta sina administrativa system med andra interna eller externa system. Dessa system har en varierad komplexitet. Många myndigheter, framförallt större, har ofta tiotals olika system som utbyter data med sina administrativa system. Migrering eller flytt till annat system är ofta en komplex och tidskrävande process som kan ta flera år att genomföra.



Figur 2, Illustration där administrativt system är central del av integrationer lokalt i eget datacenter

Om en myndighet flyttar till ett sådant system i molnet måste integrationerna hanteras eftersom systemet ingår i ett större ekosystem. Saknar myndigheten förmåga att integrera över internet, kan det bli en utmaning att koppla samman egna datacenter med molntjänsten. Beroende på komplexitet och omfattningen av integrationerna så är det sannolikt att mängden arbete och tid med att upprätta förmågor att hantera externa integrationer skulle vara likvärdig med att migrera masterdatakällan i sig.

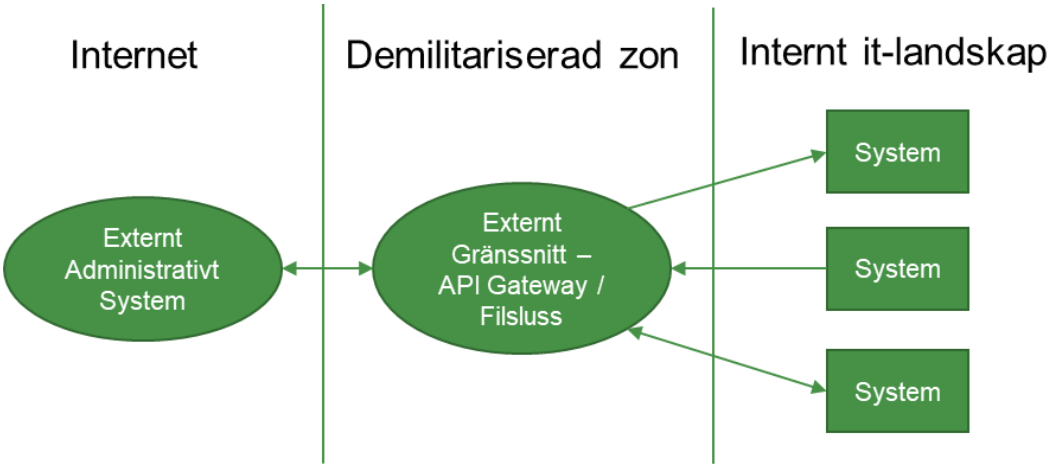


Figur 3, Illustration där den centrala delen placeras utanför egna datacenter

En ytterligare fråga att ta hänsyn till är vilka krav myndigheten har på integrationer när mottagaren är en extern tjänst. Kraven är högre för känsligare informationsmängder, i form av vilken kryptering eller autentisering som krävs för att myndigheten ska få skicka informationen. Det är viktigt att myndigheten delger leverantören sina krav på tjänsten. Det är annars svårt för leverantören att bedöma om de specificerade kraven kan tillgodoses.

5. Externa integrationer

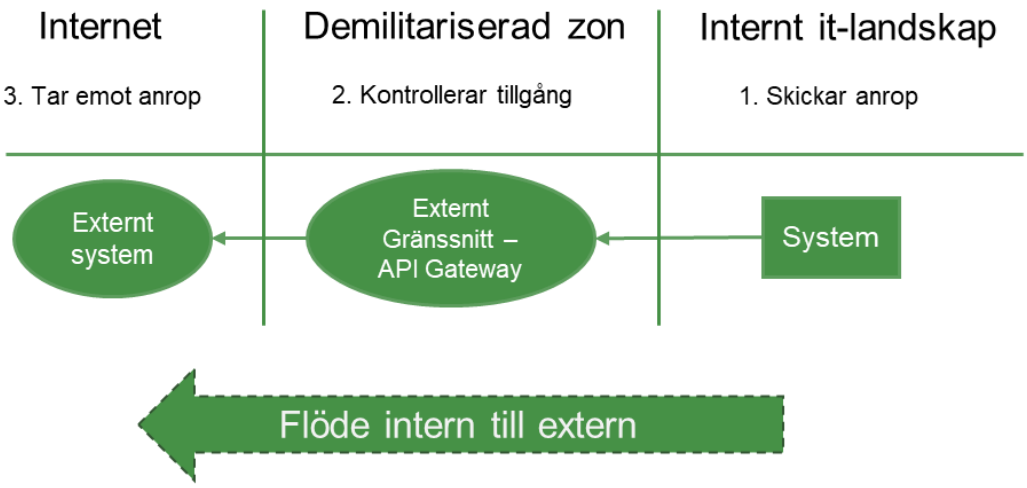
Integrationer i publika molntjänster sker över internet, vilket ställer andra krav än integrationer mot interna system. Myndigheten behöver säkra och godkända lösningar för att hantera olika typer av integrationer, exempelvis via fil eller API (Applikation Programming Interface). Dessa lösningar bör sättas upp enligt myndighetens principer och arkitekturmönster, oftast i ett DMZ/säkerhetszon (demilitariserad zon). För att minska riskerna med att exponera interna system direkt mot internet eller externa system, bör myndigheten följa arkitekturmönster och tekniska skyddsåtgärder. En säker arkitektur kan begränsa exponeringen och samtidigt möjliggöra säkerhetshöjande åtgärder i flera steg, som beskrivs nedan.



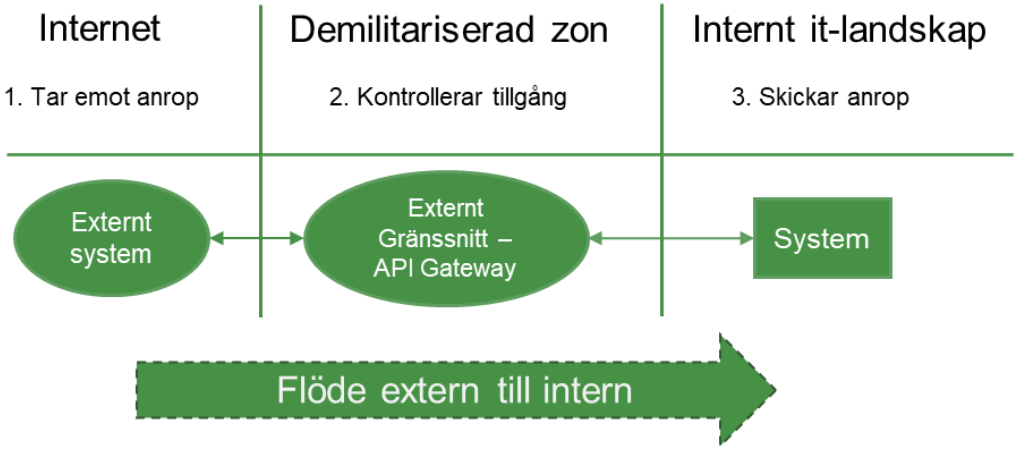
Figur 4, Illustration som visar flödet av information mellan internt och externt system via en API-gateway

De vanligaste lösningarna i den demilitariserade zonen för integration är filsluss och API-gateway. En filsluss fungerar som en lastkaj där aktörer kan ladda upp filer. På lastkajen kan filerna exempelvis skannas för virus eller skadlig kod. Ofta finns regler som förbjuder direkta överföringar, exempelvis att filen ska laddas upp, skannas och sedan hämtas (inte skickas). Detta möjliggör säker filöverföring mellan myndigheten och en extern part. En API-gateway är ett verktyg som används för att hantera de API-anrop man vill kunna skicka från sin egen miljö ut på internet och tvärtom. Den har ofta olika säkerhetsmekanismer, som att endast godkända servrar får skicka och ta emot anrop, både internt och/eller externt, eller kontroll över vilka identiteter och system som får göra anrop. Det finns ofta olika former av tekniska skydd framför en API-gateway som

skyddar mot överbelastningsattacker, som exempelvis attacker av typen distributed denial-of-service[4] (DDoS) och liknade hot via internet.



Figur 5, Illustration som visar flödet av ett anrop från internt system till externt system via en API-gateway



Figur 6, Illustration som visar flödet av ett anrop från externt system till internt system via en API-gateway

Myndigheter befinner sig på olika nivåer av erfarenhet när det gäller externa integrationer – vissa har redan etablerat dessa förmågor och har rutiner etablerade, medan andra ännu inte har påbörjat arbetet. Varje myndighet måste bedöma sin mognadsnivå och planera för att uppnå den nivå som krävs för att hantera externa integrationer. Dessa integrationer är oftast mer komplexa än interna och kräver därför tydliga arbetssätt och systematisk uppföljning. En noggrann uppföljning minskar risken för felaktigt genomförda integrationer som kan leda till säkerhetsbrister.

[4] Om Denial of service-attack, förklarande artikel läst 241212; https://en.wikipedia.org/wiki/Denial-of-service_attack

6. Identitetshantering och federering

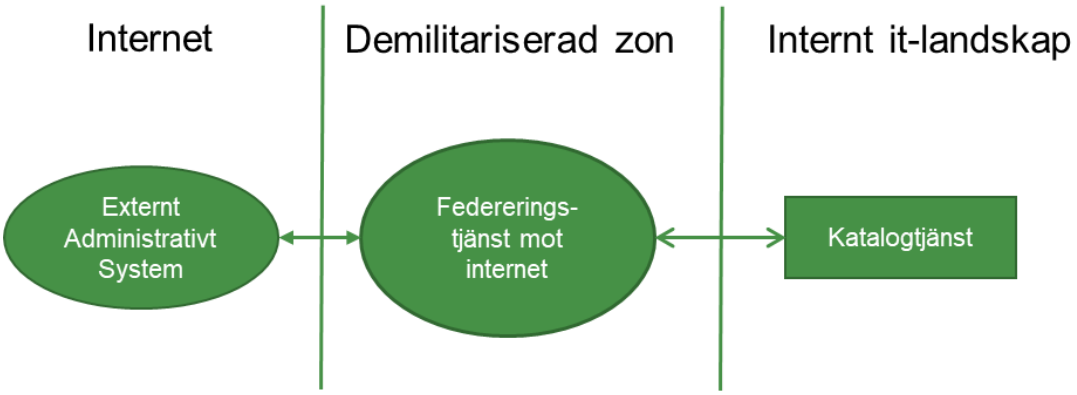
När en myndighet köper it-tjänster eller system som driftas av någon annan, exempelvis i en molntjänst, hanteras dessa som externa system och ligger utanför den interna it-miljön. Även i dessa system och tjänster måste myndigheten kunna hantera inloggningar och behörighetsstyrning, vilket kallas identitetshantering och federering. Då området är komplext, behandlas här endast några centrala aspekter.

6.1 Identitetshantering

En individs digitala identitet fungerar som ett användarnamn och används för att logga in i system eller i tjänster. Denna identitet kopplas även till licenser och behörigheter, vilket ger användaren tillgång till det som den har behörighet att komma åt för att kunna utföra sina arbetsuppgifter. En korrekt och spårbar identitet är nödvändig för att följa upp händelser i en tjänst, både i nutid och i framtiden. Även efter att en person har slutat används identiteten som referens för tidigare aktiviteter. Oftast existerar denna identitet i en katalogtjänst som fungerar som ett register på användarnamn och tillhörande attribut.

6.2 Federering

Federering innebär en it-förmåga som låter administratören koppla ihop den interna katalogtjänsten med interna digitala identiteter och externa katalogtjänster. Vanligtvis sker detta via en applikation i en demilitariserad zon som kan kommunicera med den externa applikationen och dess katalogtjänst. Detta minskar risken för attacker, eftersom den interna katalogtjänsten ofta är ett attraktivt mål för hotaktörer.



Figur 7, bilden visar övergripande federeringsflöde

En federeringstjänst låter myndigheten dela digitala identiteter med externa system och även hantera inloggningar mot externa system och tjänster. Detta möjliggör Single Sign-On (SSO), där slutanvändare endast behöver logga in en gång för att få åtkomst till flera

system. Federeringstjänsten kan också uppfylla krav som multifaktorautentisering (MFA), där en extra autentiseringsfaktor krävs vid inloggning, exempelvis en notis i en företagsapp som användaren måste bekräfta. MFA är särskilt viktigt för att skydda känslig information och förebygga kapning av digitala identiteter.

7. Informationshantering

Myndigheter har olika sätt att hantera sina olika informationsmängder. Processer, modeller och nivåer ser olika ut mellan myndigheter. Detta kapitel tar upp hur informationsmängderna för informationsklassificering, säkerhetskyddsanalys och riskbedömning behöver hanteras av myndigheten kopplat till en analys vid utkontraktering. Beroende på specifik informationsmängd och specifik molntjänst så behöver en anpassad regelverksanalys göras från fall till fall.

7.1 Informationssäkerhet

Informationssäkerhet handlar om att bedöma behov av administrativa, organisatoriska och tekniska åtgärder för att skydda informationen. En viktig del av detta är att genomföra en informationsklassning av den informationsmängd som ska hanteras i en molntjänst. En förutsättning för att skydda informationen på ett adekvat sätt är att känna till dess värde för myndigheten. Det är informationens värde som sätter krav och villkor för hanteringen.

Informationens värde identifieras genom informationsklassning, som sedan resulterar i en bedömning av vilka åtgärder som krävs för att skydda informationen och vilka krav som bör ställas på en molntjänst.

Krav kring följande aspekter av skydd för informationen behöver bedömas:

- **Konfidentialitet**: Endast behöriga ska ha åtkomst till informationen.
- **Riktighet:** Informationen ska vara fullständig och endast kunna ändras av behöriga.
- **Tillgänglighet**: Behöriga ska ha åtkomst till informationen när den behövs.

	Konfidentialitet	Riktighet	Tillgänglighet
4 Ex. Allvarlig			
3 Ex. Betydande			
2 Ex. Måttlig			
1 Ex. Försumbar			

Figur 8, enkel tabell för informationsklassning

Konfidentialitet innebär att informationen hanteras så att den inte avslöjas för obehöriga personer, objekt eller processer.

Utifrån konfidentialitetsaspekten kan informationsmängder exempelvis delas in i följande kategorier:

- Öppen: publik information.
- Intern: Information som inte är allmän handling eller en allmän handling utan skydd av sekretess.
- Känslig: Information vars röjande kan orsaka skada.
- Mycket känslig: Information vars röjande kan leda till stor skada och ofta vara skyddad av sekretess.

Utgå alltid från den egna myndighets informationsklassningsmodell.

Riktighet handlar bl.a. om att skydda informationen från att ändras och att myndigheten ska kunna vara säker på att ingen obehörig har kunnat ändra den.

Vid informationsklassning och riskanalys behöver myndigheten bedöma hur tillgänglig informationen måste vara och om avbrott är acceptabla. För vissa typer av information kan avbrott i dagar eller veckor vara acceptabla, så länge informationen är intakt och går att nå senare. Information som är avställd och arkiverad kanske inte behövs ofta, men det innebär inte att förlust av den accepteras.

Bedömningen avseende konfidentialitet, riktighet och tillgänglighet inkluderar också betydelsen av spårbarhet. Det vill säga att säkerställa informationens riktighet under hela dess livslängd, varifrån den är insamlad, upprättad, av vem samt vem som haft tillgång till informationen under dess livslängd.

När information lämnat myndigheten finns alltid risk för informationsförlust, att informationen förstörs eller att den inte går att återta.

7.2 Myndigheters hantering av information

Efter informationsklassningen bör myndigheten använda en pedagogisk modell för att bedöma molntjänstens förmåga att skydda informationen. Modellen anpassas efter myndighetens specifika behov av att på ett adekvat sätt skydda sin information.

Administrativa stödsystem hanterar ofta en större mängd information. Delar av denna information kan vara känslig utifrån ett informationssäkerhetsperspektiv[5]. En myndighet behöver analysera vilken information som hanteras i systemet och vad den kan användas till. Om det ska vara möjligt att flytta informationen till en publik molntjänst, är det avgörande att veta vilken information som ska flyttas. I en publik molntjänst delas

[5] Vid bedömningen av informationens känslighet vid genomförande av informationsklassningen, ska hänsyn tas bland annat till regelverket rörande sekretess och dataskydd. För en ingående beskrivningen av detta regelverk hänvisas till Vägledning Utkontraktering - sekretess och dataskydd.

infrastruktur med andra kunder, och skyddet är inte lika starkt som i ett privat moln. Olika informationsklasser har olika krav, och vissa typer av information kan i värsta fall vara olaglig att dela. Därför måste myndigheten använda sin beslutade process och metod för att genomföra en informationssäkerhetsanalys av den specifika molntjänsten som är aktuell.

Om förutsättningarna ändras under avtalets gång, behöver analysen uppdateras. Analysen ligger sedan till grund för beslut om och hur myndigheten bör agera, vilka skyddsåtgärder som krävs eller om hela eller delar av informationen kan hanteras externt.

Här nedan beskrivs en metod med exempel, i fyra trappsteg för olika nivåer av information.

Steg 1: Information är helt ofarlig att dela med externa parter. Myndigheten kan enkelt bedöma att det är lämpligt att dela denna information i en extern molntjänst.

Exempel på information: Öppen data, information på myndighetens hemsida, myndighetens mässinformation. Informationen kan ha lägre krav på tillgänglighet och riktighet.

Steg 2: Informationen kan innehålla sekretessreglerade uppgifter eller personuppgifter. Här blir analysen mer omfattande och myndigheten måste göra en bedömning utifrån de krav som identifieras i informationsklassningen, om informationen är lämplig att dela med en extern part eller om en extern part kan sköta hanteringen av det it-system som hanterar denna information. Även krav gällande riktighet och tillgänglighet kan vara relevanta i högre grad.

Exempel på information: Projektbeskrivningar, organisationstillhörighet, viss information till allmänheten, information i enklare e-tjänster (icke samhällsbärande).

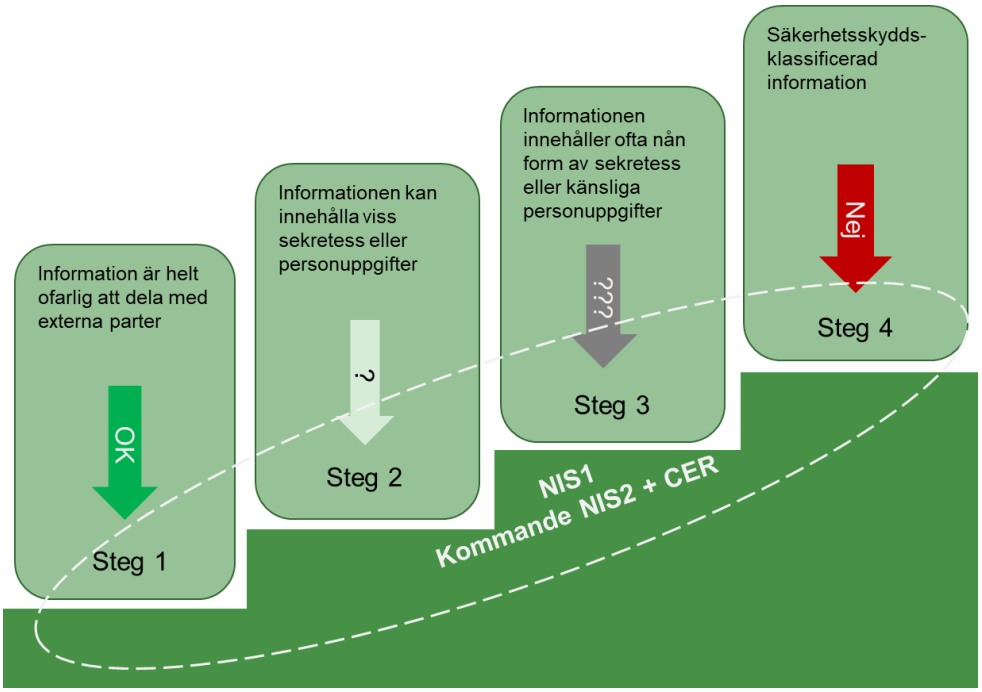
Steg 3: Informationen innehåller ofta någon form av sekretessreglerade uppgifter eller känsliga personuppgifter och kan beröra samhällsviktiga funktioner. För denna information gäller mer omfattande krav för hanteringen av informationen vilket gör det svårare för en molntjänst att leva upp till kravbilden.

Exempel på information: komplexa e-tjänster som är samhällsbärande, säkerhetsbrister, personalärenden, känsliga personuppgifter, skyddade identiteter, information om anläggningar, information om pågående upphandling och upphandlingssekretess etc.

Steg 4: Information som primärt regleras av säkerhetsskyddslagen och Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2022:1). Denna information får inte hanteras i publika molntjänster.

Exempel på information: Ritningar på samhällsviktig infrastruktur och skyddsobjekt, krigsplacering, uppgifter som omfattas av försvarssekretess, beredskapsplanering, informationsmängder som kan medföra fara för liv exempelvis vid terroristaktion eller störning för nationell samhällsfunktion.

Modellen nedan är ett förenklat exempel på hur bedömningen kan göras och ska inte ses som en standardiserad informationssäkerhetsmodell.



Figur 9, Informationssäkerhetsbedömning enligt trappmodellen – Informationsklassning av administrativa system

För hantering av informationen i de olika trappstegen finns bland annat krav från tillsynsmyndigheter.[6] Dessa krav kan ändras, vilket kräver kontinuerlig omvärldsbevakning. Myndigheter måste också i övrigt löpande bedöma tjänstens laglighet och lämplighet.

Ett aktuellt exempel på omvärldsbevakningens betydelse är NATO-medlemskapet och de krav som ställs på myndigheter ur ett informationsperspektiv. NATO har en egen

[6] Exempel på föreskrifter; Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2022.1, Myndigheten för samhällsskydd och beredskap föreskrifter om informationssäkerhet för statliga myndigheter MSBFS 2020:6, föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter MSBFS 2020:7, föreskrifter om rapportering av it-incidenter för statliga myndigheter MSBFS 2020:8 och kommande föreskrifter kopplat till Network and Information Security direktivet (NIS2), Critical Entities Resilience (CER) direktivet och Digital Operational Resilience Act (DORA)

informationsklassningsmodell som sannolikt måste hanteras parallellt med myndigheternas interna modeller. Det kan vara en praktisk utmaning att separera NATO-information, vilket kan leda till smittoeffekter i befintliga it-system. Om separationen inte kan säkerställas tekniskt måste myndighetens vanliga information också hanteras som NATO-information.

7.3 Känsliga informationsmängder

It-system kan innehålla känsliga informationsmängder och administrativa system som löne- och HR-system kan inkludera sekretessbelagda eller känsliga personuppgifter

Exempelvis kan tidsrapportering innehålla information som kan användas för att kartlägga personer. Om myndigheter bedriver känslig verksamhet, säkerhetsskyddsarbete, signalskydd, beredskapsverksamhet eller likande kan det vara möjligt att den känsliga verksamheten kan kartläggas på ett oönskat sätt. Tidrapportering kan även innehålla uppgifter som exempelvis sjukfrånvaro. Fakturor, avtal och statusfält kan också innehålla känslig information.

7.4 Säkerhetsskyddad information i publika molntjänster

Vid säkerhetsskyddade upphandling blir ämnen, innehåll och kontaktpersoner särskilt skyddsvärda och säkerhetsskyddsklassificerade. Denna typ av information kan omfattas av sekretess och kräver noggrann hantering.

Om informationsmängder som ska utkontrakteras bedöms vara säkerhetsskyddade, måste detta utvärderas och hanteras skyndsamt.[7] Hanteringen av informationsmängder som omfattas av säkerhetsskydd omfattas av strikta lagkrav. Detta behöver myndigheten utreda genom egen analys kring säkerhetsskydd för berörda informationsmängder. Om det förekommer säkerhetsskyddad information måste den separeras från övriga informationssystem, t ex administrativa system, såsom ärendehantering och ekonomisystem i enlighet med tillsynsmyndighetens[8] krav. Annars kommer det administrativa systemet påverkas av striktare lagkrav både gällande teknikval och arbetssätt. I en sådan situation kan myndigheten exempelvis inte själv välja arbetssätt, it-utrustning eller kryptering som används kring tjänsten.

[7] Säkerhetspolisen, förklarande artikel läst 241212; https://www.sakerhetspolisen.se/verksamheten/sakerhetsskydd/vagledningar-sakerhetsskydd.html
[8] Säkerhetspolisen, förklarande artikel läst 241212; https://www.sakerhetspolisen.se/verksamheten/sakerhetsskydd/vagledningar-sakerhetsskydd.html

8. Applikationsdriftplattform

En molntjänst kan vara arkitektoniskt och tekniskt uppbyggd på olika sätt, beroende på historik (äldre kodbas) eller behov av att nyttja olika typer av funktionsbaserade molntjänster. Valen påverkar tekniska skyddsåtgärder och hur separation av data kan nås igenom applikation och lagring. Ett äldre system saknar ofta inbyggda funktioner för kundsegmentering och använder istället logisk segmentering, med parallella applikationsinstanser, separation i nätverk och virtualiseringsplattform samt behörighetshantering som segmenterar olika systemkonton för applikationen. Ett nyutvecklat system kan däremot integrera segmenteringsfunktioner direkt i applikationskoden, exempelvis genom multi-tenancy och inbyggd auktorisation.

Begreppet Cloud Native[9] beskriver tjänster där arkitekturmönster och principer från början designats för leverans av flerkundsanpassad molntjänst. I detta arkitekturmönster ingår det att hela processen för utveckling av kod, distribution av kod och managering av applikation stödjer agila principer, så som DevOps[10] och kontinuerlig leverans[11], med tekniska lösningar för microtjänster[12], som containerbaserad leverans av applikationskod och automatiserade byggkedjor[13]. Cloud Native[14] levereras vanligtvis på Linux med Kubernetes som applikationsplattform. De kan oftast underhållas under dagtid, då principerna bygger på att små förbättringar kan implementeras löpande utan att påverka användarupplevelsen eller tillgängligheten. Ekosystemet för Cloud Native växer kraftigt, många stödsystem för effektiva applikationsleveranser går mot denna typ av arkitektur. På senare år har även flera databashanterare börjat leverera stöd för Cloud Native leverans vilket indikerar att arkitekturen är stabil och robust. Dessutom finns verktyg för att härda trafikmönster, applikationer och API:er, vilket gör applikationer och flerkundsleveranser mer resilient mot cyberattacker.

Begreppet Cloud Hosted beskriver en applikation som har anpassats för att fungera som en publik molntjänst, men som ursprungligen inte byggdes för detta ändamål. Leverantören har ofta behövt anpassa arkitekturen för att få den multikund-kompatibel, exempelvis genom logisk segmentering med parallella applikationsinstanser. Det är möjligt att arbeta med agila principer och automatiserade byggkedjor även i denna arkitektur. Dock når man sällan full automatisering på grund av svårigheter med parallella och kundunika applikationsinstanser.

[9] AWS, förklarande artikel läst 241212 https://aws.amazon.com/what-is/cloud-native
[10] AWS, förklarande artikel läst 241212; https://aws.amazon.com/devops/what-is-devops/
[11] AWS, förklarande artikel läst 241212; https://aws.amazon.com/devops/continuous-delivery/
[12] AWS, förklarande artikel läst 241212; https://aws.amazon.com/what-is/cloud-containers/
[13] AWS, förklarande artikel läst 241212; https://aws.amazon.com/what-is/container-orchestration/
[14] AWS, förklarande artikel läst 241212; https://www.cncf.io/

Cloud Hosted-lösningar levereras vanligtvis på Windows eller Linux som en installerad applikation, i många fall med en mellanmjukvara[15] (middleware) som grund, tex Microsoft Net, Oracle Java, IBM WebSphere, där applikationskoden körs.

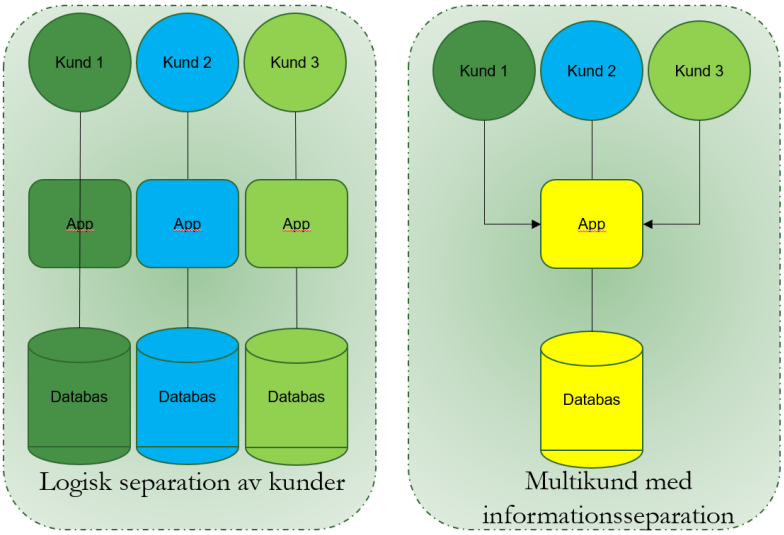
För Cloud Hosted krävs tekniska skyddsåtgärder som är anpassade för denna typ av leverans. Exempel på sådana åtgärder är skydd mot skadlig kod på operativsystemsnivå, logisk segmentering av servers och IPS-skydd (intrusion prevention system) mot internet. De här typen av plattform är ofta måltavlor för skadlig kod, exempelvis ransomware som krypterar lagring och kräver lösen för att låsas upp. Detta drabbar särskilt Windows-plattformar. Ofta används även Vmware för att virtualisera hårdvara i virtuella servers, men även den mjukvaran är utsatt för angrepp.

En Cloud Native-tjänst har delvis andra säkerhetsbehov, även om vissa är gemensamma. Exempel på unika skyddsåtgärder i denna plattform är skydd inom byggkedjorna mot angrepp via försörjningskedjan av mjukvaruberoenden, infektering av skadlig kod i containers. Molntjänster är ofta beroende av andra molntjänster för funktioner som ärendehantering, identitetshantering och integrationer. Dessa beroendekedjor kan vara komplexa att analysera men måste inkluderas i en molnanalys. Varje samverkande molntjänst behöver dessutom egna tekniska skyddsåtgärder. Exempel på gemensamma skyddsåtgärder är:

- API-baserade skydd
- DDoS skydd på olika nivåer (internetleverantör, anslutning och säkerhetszoner)
- IPS (intrusion prevention system)
- Token-hantering för API:er
- Rollbaserad behörighetsstruktur med avancerad identitetsfederering för att undvika angrepp med lösenordsprayning.

Hela miljön måste härdas och byggas enligt god praxis, exempelvis CIS Security[16].

[15] Om middleware, förklarande artikel läst 241212; https://en.wikipedia.org/wiki/Middleware
[16] Center for Internet Security, förklarande artikel läst 241212; https://www.cisecurity.org/cis-benchmarks



Figur 10, Förenklad bild av skillnader mellan Cloud Hosted (vänster) och Cloud Native (höger) för applikationsstacken

9. Kontinuitet

Myndigheten behöver analysera systemet utifrån sina krav på kontinuitet och tillgänglighet. Verksamhetskontinuitet handlar om förmågan att bibehålla eller snabbt återhämta verksamheten, även från en annan plats om det behövs. För att det ska vara möjligt behöver myndigheten analysera och förbereda för alternativa lösningar för att säkerställa sitt myndighetsuppdrag. Teknisk kontinuitet innebär att den tekniska lösningen ska kunna hållas i drift så länge som möjligt, och om det inte går, snabbt kunna återställas.

9.1 Applikationsloggar och incidenthantering

Det mesta som sker i och runt en molntjänst kan loggas, exempelvis förändring av tjänsten, arbete mot tjänsten, support och ändringar i konfiguration.

Myndigheten bör anpassa lösningar för att löpande hämta hem loggar för eget nyttjande av tjänsten samt viktiga förändringar av tjänsten. Detta säkerställer spårbarhet och gör det möjligt att följa användares aktiviteter, spåra viktiga systemändringar, behörighetsändringar och andra administrativa åtgärder. Dessa logghämtningar bör hämtas hem schemalagt.

Leverantören ska ha rutiner för att hjälpa kunder vid incidentrapportering, exempelvis vid intrångsförsök eller sabotage som myndigheten sedan ska rapportera till behörig tillsynsmyndighet samt för att myndigheten ska ha egen kontroll över sin informationshantering. Denna tekniska förmåga ska uppfylla myndighetens ålagda krav på incidentrapportering och myndighetens krav på tillgänglighet och bevarandetid för loggar.

9.2 Flyttbarhet och exithantering

Vid anskaffning eller utveckling bör myndigheten ställa krav på flyttbarhet utifrån totalförsvarstanken - det som myndigheten behöver i fred kommer sannolikt även behövas i krig. Vid kris eller krig kan myndigheten behöva flytta myndighetens it-miljö, vilket gör flyttbarhet till en totalförsvarsfråga. För detta krävs en kartläggning och prioritering av system och tillhörande informationsmängder, inte minst vid utkontraktering av ett system till extern leverantör. Behovet av snabb flyttbarhet gäller oavsett egentillverkad it eller utkontrakterad it.

Flyttbarhet är den planering och arkitektur som behöver göras för att det ska vara möjligt att flytta system och data från en leverantör och driftplats till en annan när avtalsslut, kris

eller krig inträder. När behovet av en flytt uppstår kan system och data migreras. Myndigheten bör vidare överväga om den nya it-tjänsten riskerar att skapa kundinlåsning och om så är fallet planera hur en framtida flytt kan genomföras.

Exithantering (exitplan) handlar om att säkerställa de juridiska och avtalsmässiga förutsättningarna för att kunna genomföra en flytt. Exempelvis måste myndigheten i avtalet säkerställa att den äger informationen, har rätt att hämta ut data från tjänsteleverantörens miljö, att det inte ska ta oskäligt lång tid att genomföra samt att säkerställa att informationen försvinner ur leverantörens miljö.

En del av flyttplanen kan vara nyetablering av it-förmåga istället för att den nuvarande lösningen flyttas. Myndigheten behöver då fundera på krav kring kontinuitet, historik, arkiveringskrav (dessutom utlämning) och gallring av sina informationsmängder. Utifrån dessa krav behöver myndigheten avgöra om det är lämpligt för myndigheten att skapa/anskaffa nytt. Vid en planerad exit är frågan om ny driftplats eller leverantör oftast enklare att hantera. Detta beror på att myndigheten sannolikt redan har en ersättningslösning eller har beslutat om avveckling av nuvarande it-lösning.

9.2.1 Molntjänster och flyttbarhet

Suveränitet är en del av flyttbarhet och innebär möjligheten att flytta sin data och tjänster från en driftleverantör till en annan. Vid molntjänster är det oftast svårt eller omöjligt att flytta tjänsten, vilket gör att möjligheten att få ut sin data är en central del av flyttbarhet. Detta innebär att data ska kunna extraheras i sin helhet och i ett läsbart format. I många fall kan detta lösas via ett API. Då ansvarar myndigheten, eller den kommande leverantören, för att genomföra en integration som läser ut data från den tidigare leverantören och importerar den till ett nytt system. Ett vanligt problem är att även om myndigheten har tillgång till data, kan den vara formaterad på ett systemspecifikt sätt. Det krävs då en transformering och omvandling för att passa in i det nya systemet. Exempelvis kan data från ekonomisystem och HR-system vara standardiserad i sitt innehåll men samtidigt mycket systemspecifikt formaterad. Det är också viktigt att säkerställa att det inte sker en informationsförlust vid flytt mellan olika tekniska lösningar.

För att säkerställa flyttbarhet måste myndigheten inkludera en exit- eller flyttklausul i avtalet. Denna ska ge myndigheten rätt att extrahera data från tjänsten och kräva att leverantören bistår i arbetet. Ett annat sätt att behålla sin flyttbarhet och suveränitet är att använda öppna standarder när system byggs. Detta gör det möjligt att leverera systemet på olika infrastrukturtjänster. Även om komplexiteten ofta ökar med systemets storlek, finns det tekniska möjligheter att flytta ett system byggt på öppna standarder från

exempelvis Amazon AWS, Google, Microsoft Azure till annat moln eller till en egen datorhall.

9.2.2 Delade informationsmängder och flyttbarhet

Delade informationsmängder mellan olika verksamhetssystem är allt mer vanligt förekommande och en konsekvens av datadrivet arbetssätt. För myndigheter är det också rekommenderat att minimera antalet kopior av sina informationsmängder för att underlätta arbete med arkivering, långtidslagring, utlämning och gallring. Vid flytt av verksamhetssystem måste informationsmängder följa det högst prioriterade systemet. Detta gäller även om lägre prioriterade verksamhetssystem temporärt kan påverkas negativt (temporärt degraderad drift). En anpassad flyttplan bör dock minimera störningen som kan uppstå till följd av denna problematik.

10. Tekniska skyddsåtgärder

Myndigheten har ansvar för att säkerställa att informationstillgångar har ett tillräckligt skydd mot obehörig åtkomst och att tillgänglighet och riktighet upprätthålls. En tjänst som exponeras mot internet behöver tillämpa olika typer av skyddsåtgärder för att minska risken att informationstillgångarnas riktighet, tillgänglighet och konfidentialitet inte påverkas vid cyberattacker. De nödvändiga skyddsåtgärderna varierar beroende på hur tjänsten är utformad och bör identifieras genom en risk- och sårbarhetsanalys. Vid utkontraktering ska myndigheten säkerställa att leverantören uppfyller alla ställda krav. Vissa krav avseende tekniska skyddsåtgärder framgår av MSB:s föreskrifter[17]. Ytterligare stödmaterial finns på www.informationssäkerhet.se[18] där flera myndigheter samverkar för att sprida kunskap kring informationssäkerhet. Nedan följer exempel på några vanliga skyddsåtgärder med tillhörande beskrivning och rekommendation. Myndigheten behöver kunna revidera leveransen enligt överenskomna krav.

10.1 Logganalysverktyg

Med en stor mängd loggar som ofta är utspridda i olika system och över olika leverantörer, uppstår behov av att samla och analysera dessa i ett centralt system. Ett sådant system blir en viktig komponent i både övervakning av status och i säkerhetsarbete. De flesta myndigheter använder en lösning för säkerhetsinformation och händelsehantering, *Security information and event management* (SIEM), i sin egen it-miljö. Vissa molntjänster kan erbjuda myndigheten möjlighet att ta del av loggar i tolkningsbara format eller som strömmad logginformation. Inledningsvis kan de inbyggda rapporteringsverktygen i respektive molntjänst vara tillräckliga för att ge myndigheten en lägesbild och en statusrapport. För organisationer som nyttjar många molntjänster kan det dock bli problematiskt om varje molntjänst hanteras separat utan möjlighet att samla och analysera informationen centralt för myndigheten. Vid upphandling och avtalstecknade bör myndighenten säkerställa att strömmad logginformation är tillgänglig och kan nås via API, för att läsa in i det logganalysverktyg myndigheten har. Det är viktigt att vara medveten om att hanteringen av loggdata kan innebära betydande kostnader, till exempel för att extrahera logginformation. Samtidigt är denna funktion ofta avgörande för myndighetens förmåga att hantera incidenter.

[17] MSB, förklarande artikel läst 241212; https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/risker-och-sarbarheter-inom-cybersakerhet-och-cyberfysiska-system/
[18] MSB, förklarande artikel läst 241212; https://www.informationssakerhet.se/metodstodet/

10.2 Verktyg för informationsöverföringskontroll

En av de största utmaningarna för myndigheter är att dela känslig information enbart med behöriga personer. När data finns utanför myndighetens it-domän, ofta på flera ställen, kan det bli svårt att hålla reda på var den finns och vem som kommer åt den. Myndigheten måste ha god kunskap om vilken information det handlar om och vilka regelverk som reglerar den.

Zero trust-tekniker syftar till att styra exakt vilka som ska ha åtkomst till information och vilka som inte ska det. Eftersom det är en heltäckande teknik kan det vara svårt och tidskrävande att införa den. Det finns snabbare och enklare verktyg som ger liknande resultat, exempelvis *Cloud access security broker* (CASB). CASB är fördefinierade tjänster som skyddar vissa informationsmängder i utpekade publika tjänster, så att endast myndigheten och godkända samarbetsparters får åtkomst. CASB tjänster kan ha en begränsning i utbudet av it-tjänster man stödjer. På senare år har CASB utvecklats till det som kallas Secure Access Service Edge (SASE). SASE erbjuder fler funktioner för att hantera och styra åtkomst. Det är dock viktigt att känna till att dessa lösningar ofta finns inbyggt hos publika molnleverantörer, vilket gör det nödvändigt att utreda om listor över känsliga informationsobjekt eller listor på vem som får se dessa objekt i sig kan hanteras i molntjänster.

10.3 Överbelastningsskydd

Överbelastningsattacker är en vanlig metod i syfte att påverka myndigheters tillgänglighet och leveransförmåga. För att skydda sig rekommenderas flera lager av överbelastningsskydd som samverkar, från internetleverantör till själva applikationen eller molntjänsten.

10.4 IP-geolokalisering

För att minska risker för attacker kan myndigheten tillämpa ip-geolokaliseringsskydd. Det innebär att trafik från vissa länders internetinfrastruktur blockeras. Exempelvis kan en tjänst exponeras enbart för svensk internetinfrastruktur om kunderna endast befinner sig där. Det finns sätt att ta sig runt detta skydd, men det minskar risken för att bot-nätverk identifierar brister i tjänsterna eller genomför överbelastningsattacker. En nackdel med ip-geolokalisering är att det är nästan omöjligt att anpassa för enstaka kunder i delade tjänster. Därför måste inställningarna i en publik molntjänst ofta anpassas utifrån hela kundgruppens behov. Ett effektivare skydd är att minska tjänstens exponering genom att endast tillåta åtkomst från betrodda nätverk, exempelvis myndighetens externa IP-adress. Detta kan göras med vitlistning. Även om vitlistning

kan kringgås, försvårar det angrepp. Vid behov och där det är möjligt bör certifikatbaserad vitlistning användas för högre säkerhet.

10.5 Brandväggar och IPS/IDS

Brandväggar är idag en självklar del av skyddet, men det är viktigt att begränsa åtkomsten så att tjänsten enbart exponeras för nödvändig trafik. Skyddsåtgärder som Intrusion prevention system (IPS) och Intrusion detection system (IDS) bör också tillämpas, både före och efter sessionsterminering av trafiken som görs i lastbalanseraren. IDS övervakar nätverkstrafiken, identifierar potentiellt skadlig trafik och kan varna för intrångsförsök, medan en IPS fungerar mer proaktivt genom att blockera skadlig trafik automatiskt. Dessa funktioner finns både som enskilda produkter och som inbyggd i vissa brandväggar.

10.6 Penetrationstester och sårbarhetsskanning

Internetexponerade funktioner behöver härdas för att förhindra intrång. När de är härdade bör de testas för att säkerställa att härdningen ger önskat resultat. Sårbarhetsskanning kan utföras antingen internt, inifrån servern eller containern, eller externt, med hjälp av en programvara eller från utsidan mot exponerade tjänster. I sin enklaste form handlar skanningen om att hitta versioner av programvara med kända sårbarheter.

Sårbarhetsskanning bör genomföras regelbundet, då nya sårbarheter snabbt kan upptäckas och utnyttjas vid attacker. Det är en fördel om myndigheten får tillgång till leverantörens egna sårbarhetsanalyser då detta stärker den egna myndighetens sårbarhetsanalys.

Även programmeringsfel och konfigurationsfel kan utgöra sårbarheter. De är inte kopplade till specifika programvaruversioner och kräver andra metoder för att upptäckas. Penetrationstester är ett sätt där man testar kända metoder för att hitta sådana fel. Till stor del kan myndigheten använda sig av programvaror för tester men bör vid behov anlita specialister för bredare eller nischade tester. Det är bättre att göra tester innan tjänsten exponeras mot internet än att riskera att obehöriga upptäcker sårbarheter utan att rapportera dem. Penetrationstester och sårbarhetsskanning kan inte göras på en köpt tjänst utan en överenskommelse med leverantören. Därför är det viktigt att myndigheten vid upphandling av tjänster ställer krav på att leverantören utför dessa tester och att myndigheten har rätt att ta del av resultaten. Alternativt att leverantören själv anlitar oberoende part för att göra penetrationstester och sårbarhetsscanningar. Det är då viktigt att myndigheter får ta del av resultat eller summering av testerna för att kunna

upprätthålla krav ställda på myndigheten, eller få del av intyg på genomfört test samt rapportering av antalet identifierade brister och allvarlighetsgraden samt förhållande till tidigare resultat. Lämpligt att ställa krav på åtgärdsplan och att få information om det är kritiskt.

10.7 Lastbalansering, reverse proxy och terminering

För att åstadkomma hög tillgänglighet används ofta någon form av lastbalansering framför en applikation. Lastbalanseringen fördelar trafik mellan flera noder och kan styra om trafiken till en fungerande nod om en del av tjänsten har gått ner. Myndigheten bör se över möjligheten att lägga till ytterligare skyddsåtgärder framför applikationen, eftersom trafiken ofta hanteras (terminernas) i detta lager. En vanlig förmåga är så kallad web application firewall (WAF), som ger ett extra lager av säkerhet för den applikation som exponeras. En WAF skyddar mot tusentals kända exploits, skadlig kod och attackvektorer som kan vara svåra att hantera enbart i webapplikationen. Beroende på leverantören av lastbalanserare, reverse proxy eller WAF finns det fler skyddsmetoder som kan användas i detta lager.

10.8 API-Säkerhet

API:er är en känslig del av applikationen eftersom de oftast används för utbyte av information mellan system. För att skydda dessa bör åtkomst säkras med autentisering och auktorisering. En vanlig lösning idag är att använda en API-gateway, som begränsar åtkomsten och autentisera användare. Transportkryptering, som exempelvis TLS, ska alltid tillämpas. När det är möjligt bör även totalsträckskryptering nyttjas. Det är vanligt att API:er utsätts för överbelastningsattacker och det är därför viktigt att ha skydd som t.ex. rate limiting eller throttling. Innehållsvalidering av inkommande data kan bidra till att stoppa attacker som använder felaktiga eller skadliga indata. API-nycklar som hanteras och lagras i molntjänster behöver skyddas för att inte kunna nyttjas av skadliga aktörer. Exempelvis genom att hantera nycklar i designerade nyckelhanteringslösningar och säkerställa att de inte exponeras i skript, källkod eller motsvarande.

10.9 Autentisering

Om informationstillgångar i tjänsten inte är tänkta att vara publika måste den skyddas av ett lager för auktorisering och autentisering. Stark autentisering (tvåfaktor) bör alltid användas och för myndigheter är stark autentisering ofta ett krav. Trafik som inte har autentiserats ska stoppas så tidigt i kedjan som möjligt för att minska möjliga attackvektorer.

10.10 Skydd mot skadlig kod

Om applikationen hanterar filer måste den ha skydd mot att skadlig kod sprids via filöverföring. Detta kan göras antingen genom antivirusskydd på applikationsservern eller via centralt skydd, exempelvis ICAP-integration med en befintlig filtvätt.

Det vanligaste skyddet mot skadlig kod är mönsterbaserat, där programvaran letar efter mönster i den kompilerade koden och skannar alla filer som den har tillgång till. Det ger ett ganska bra skydd mot känd skadlig kod, eftersom leverantörerna är snabba med att uppdatera informationen när man hittar nya exempel. Det finns moderna lösningar som bygger på att man identifierar skadlig kod via beteende i stället för via mönster i koden. Fördelen är att dessa lösningar inte kräver uppdatering för varje mindre förändring i den skadliga koden. Skadlig kod kan komma in i en it-miljö på flera sätt. Ett vanligt sätt är via e-post eller webbläsare. Därför ska man inte använda e-post eller webbläsare i servermiljöer.

För mer information, se eSams vägledning om ransomware.[19]

10.11 Härdning av applikation och server

Om skadlig kod eller överbelastningsattack når applikationen ska den vara härdad för att minimera skador och förhindra spridning. Ta bort tjänster som inte används eller behövs. Det kan vara att minska behörigheterna för körande processer och tjänster, använda antivirus samt begränsa brandväggsöppningar etc. Servrar och infrastruktur rekommenderas att inte ha direktåtkomst mot internet, dvs. trafik ut från servrar och infrastruktur. Detta försvårar bland annat för skadlig kod att ”ringa hem” och ladda ner eller upp information för att skapa mer omfattande skada.

10.12 Segmentering och separation

En attack mot en applikation ska inte kunna sprida sig till andra applikationer eller kunder. För att minimera risken bör applikationer och system segmenteras, det vill säga separeras från andra system. Detta kan uppnås med härdade brandväggsregler, olika nätsegment med mera. Utöver blockerande funktioner behövs även detekterande funktioner i brandvägg eller logganalysverktyg. Dessa kan också integreras med skydd mot skadlig kod i server och nätverkslager.

[19] ES2024-16 Vägledning Ransomeware.

10.13 Backup och lagring

Ransomware-attacker blir allt vanligare. Vid dessa attacker stjäl angriparen data och krypterar kundens information. I flera fall har även backup påverkats, vilket inneburit stora informations- och kapitalförluster för den drabbade myndigheter. Om informationstillgångarna är kritiska ska backup låsas även för administratören (immutable), med tillägget att backup också separeras från applikationslagret. Där det är möjligt bör backuperna vara ”offline” och inte nåbara från applikationslagret.

10.14 Kundisolerad area i publik molntjänst

Alla större globala molnleverantörer har en “privat area”-tjänst som kallas *trusted execution environment* (TEE). Det är en virtuell digital plats i den publika molntjänsten som bara kunden har åtkomst till. Denna teknik byggs vanligtvis upp genom att kontrollen flyttas från molnleverantören till hårdvaruleverantörer i datacentret, exempelvis via chipset och processorer. AMD, ARM och Intel har olika exklusiva avtal för TEE-tjänster för AWS, Google och Microsofts publika molntjänster. TEE-tekniken har begränsningar och kan endast användas med vissa tjänster inom molnleverantörens utbud. Dessutom innebär tekniken att utländska privata bolag fortsatt hanterar myndighetens informationsmängder och får inflytande över dess digitaliseringsprocess. Denna typ av teknologi kräver oftast specialanpassade applikationer och kan leda till ökade kostnader för hela it-miljön. Sveriges cybercampus har beskrivit tekniken[20] och arbetar för att skapa en helt oberoende TEE-lösning för svensk offentlig förvaltning.

[20] Länk till MSB cybersäkerhetsmässa 2024; https://youtu.be/Yu8K83zfA1U?feature=shared&t=9193

11. Arbetsmetoder för analys av molntjänst

Det kan vara svårt att få fram information om hur en molntjänst fungerar, är uppbyggd och hur myndighetens informationsmängder exponeras när tjänsten används. En bra dialog med leverantören är en viktig utgångspunkt, men det räcker ofta inte för att få en fullständig bild och förståelse för underliggande teknik. I vissa situationer kan det bli svårt att ha dialog med leverantören exempelvis vid upphandling och då behöver myndigheten hitta information på andra sätt. Myndigheten behöver därför har en god uppfattning om lösningarna innan anskaffningsprocessen är påbörjad. En Request for information (RFI) kan vara ett bra sätt att skapa sig en bild av möjliga lösningar och vilka krav som behöver ställas på själva anskaffning. Ofta behöver myndigheten leta alternativa informationskällor och kunna värdera dessa utifrån risk för tillrättalagd information m.m.

Nedan följer några tips på arbetsmetoder och informationskällor för analys av molntjänster.

11.1 Tvärfunktionell analysgrupp

Analys av molntjänster är komplext och en del myndigheter har därför startat analysgrupper för att hantera dessa, så kallade molngrupper. Fördelen med en stående analysgrupp är att dess effektivitet och leveranskvalitet ökar med antalet genomförda analyser. Genom en tvärfunktionell sammansättning där olika kompetensområden arbetar tillsammans så belyses olika aspekter av analysen. En tvärfunktionell grupp bör inkludera kompetens inom teknik, juridik, anskaffning och informationssäkerhet. Ytterligare kompetenser kan behövas beroende på vilken analys som ska utföras. En fördel med en tvärfunktionell analysgrupp är möjligheten till mer kvalificerade beslut och underlag innan myndigheten ingår i ett avtal. Annars finns risk för nya komplikationer i senare skeden under systemets införande och därefter.

Det är lätt att fokus hamnar på anskaffning, integritetsaspekter och dataskydd, men även teknik och integrationsaspekter behöver noga analyseras. Risken är annars att det uppstår problem med brister i säkerhet, teknik och senare eventuellt migrering samt att avsluta tjänsten på ett korrekt sätt.

11.2 Resurspool inom teknisk hantering och analys av tjänster

Förutom en molngrupp kan det vara fördelaktigt för myndigheten att ha en grupp av mer tekniskt kunniga medarbetare. Denna grupp stöttar molngruppen genom kompetens inom exempelvis löpande hantering av tjänster, såsom hantering av molntjänster, scripting och programmering av tjänster, samt kompetenser inom it-säkerhet. Genom att tillföra tekniska resurser tidigt kan molngruppen genomföra djupare och snabbare analyser. Detta gör det möjligt att identifiera skillnader mellan leverantörens löften och det som faktiskt levereras. Med djupare kunskap och mer erfarenhet kan den stöttande gruppen leverera mer kvalitativa analysresultat tidigare, vilket kan vara fördel i urvalsprocess och kravställning. Myndigheten kan därigenom lägga mindre resurser på analys men ändå få ett önskat utfall. Om anskaffningen är komplex eller rör verksamhetskritiska system, bör myndigheten överväga konsultstöd inom exempelvis penetrationstestning, säkerhetsanalys eller teknisk analys. Konsulten kan stötta i analysarbetet och samtidigt överföra kompetens till myndighetens egen personal i ett tidigt skede.

Analys av en publik molntjänst behöver ske löpande, framförallt för komplexa tjänster. Det är mycket vanligt att en leverantör byter underliggande komponenter, ändrar villkor eller funktioner och inkluderar andra molntjänster, vilket kan påverka analysens tidigare resultat och kräva en ny bedömning.

11.3 Kartlägga ägarskap och underbiträden

För att kartlägga ägarförhållanden och identifiera vilka underbiträden som används i en publik molntjänst kan följande källor vara aktuella, för att få en initial och övergripande uppfattning om förhållandena. Myndigheten behöver söka information om tjänsten på olika platser och nedan följer förslag på sådana platser. De flesta publika tjänster har informationssidor om dataskydd och underleverantörer. Dessa sidor innehåller ofta information om hur tjänstens dataskydd, integritet och informationshantering ser ut, och hur leverantören arbetar med detta. Här får man ofta en första bild av användning av underbiträden och ägarförhållanden. Leverantörer kan ibland erbjuda publicerade dokument som DPA (Data Processing Agreement) / DTIA-(Data Transfer Impact Assessment). Dessa dokument beskriver dataskydd i tjänsten, underbiträden, informationshantering och aktuella tredjelandsöverföringar.

- En webbsökning på företagsnamnet kan ofta ge information om ägare och eventuell noteringsplats aktiehandel.

- Webbplatser för aktiehandel har ofta samlingssidor med affärsinformation, exempelvis om större transaktioner och uppköp, även långt tillbaka i tiden.
- Källor som Wikipedia innehåller ofta ägarförhållanden och ägarhistorik. Informationen bör dock alltid verifieras med mer pålitliga källor.

11.4 Byggkomponenter i tjänsten

Leverantörer kan ibland vara ovilliga att dela information om komponenter, eftersom de betraktar den som konkurrenskänslig. För att få fram uppgifter om vilka komponenter som bygger upp tjänsten kan dessa källor vara användbara.

- Leverantörens information om tjänsten.
- Information om tjänstens uppbyggnad kan ofta finnas i öppna användar- och supportforum. Finns inte sådana forum kan man även leta bland leverantörens supportforum.
- Via webbläsarens funktion för analys av sidinnehåll, F12-utvecklarverktygen, går det att hitta information om delkomponenter och externa tjänster som tjänsten använder.
- Via leverantörens jobbannonser på sociala medier (t.ex. Linkedin) går det ibland att hitta information om vilka tekniska tjänster och byggkomponenter som ingår i deras lösningar.

Vid anskaffning behöver verksamheten ha tagit höjd för att identifiera och kontrollera leverantörskedjan för att säkerställa att alla led är skyddade mot sårbarheter och cyberhot och andra identifierade krav utifrån skyddsvärde.

Vid utkontraktering behövs en kartläggning av leverantörskedjan för både mjukvaror och underliggande tjänster för att identifiera alla aktörer och deras respektive roller där informationsflöden och kritiska beroenden mellan leverantörer och komponenter är dokumenterade. Uppdatera säkerhetsåtgärder och rutiner och följ upp regelbundet.

Genomför regelbundna riskbedömningar för att identifiera potentiella sårbarheter och hot i leverantörskedjan. Använd standardiserade metoder för riskbedömning, t.ex. ISO 27001.

11.5 Faktagranskning av framtagen information

Efter att informationsinsamling och bearbetning har genomförts bör leverantören få möjlighet att faktagranska och kommentera de data som förs fram. Leverantören kan

ifrågasätta vissa uppgifter men bör också kunna förklara de fynd som analysgruppen gjort. Om det är stor skillnad mellan vad leverantören presenterat om tjänsten och vad analysgruppens kartläggning visar, bör myndigheten vara försiktig i sin slutgiltiga bedömning.

11.6 Nyttja ISO standarder som stöd

Oavsett om myndigheten är certifierad enligt ISO27000 eller inte, finns det inom ISO-serien två standarder som kan stödja ett strukturerat riskarbete kopplat till säkrare anskaffning av molntjänster:

- ISO27017[21] omfattar riktlinjer för säkerhetsåtgärder för molntjänster.
- ISO27018[22] omfattar riktlinjer för skydd av personuppgifter i publika molntjänster

Dessa standarder är kopplade till ISO27002 (tekniska skyddsåtgärder). Arbete pågår att även länka ISO27000-kraven till riskerna definierade i NIST-ramverket. För myndigheter som redan har brutit ner sina säkerhetskrav enligt ISO27000 kan dessa standarder fungera som en användbar struktur för att definiera rätt risker och ställa lämpliga krav, med förslag på både tekniska och organisatoriska åtgärder. Även andra myndigheter, som inte specificerat sina krav i detalj, men ändå följer författningskraven[23], kan ändå hitta inspiration i dessa ISO-standarder. De kan ge inspiration till hur säkrare molntjänstanskaffning kan genomföras.

[21] Informationsteknik - Säkerhetstekniker - Riktlinjer för säkerhetsåtgärder för molntjänster baserade på SS-EN ISO/IEC 27002 (ISO/IEC 27017:2015); https://www.sis.se/produkter/informationsteknik-kontorsutrustning/itsakerhet/ss-en-isoiec-270172021/
[22] Riktlinjer för skydd av personuppgifter i publika molntjänster som hanterar personuppgifter (ISO/IEC 27018:2019); https://www.sis.se/produkter/informationsteknik-kontorsutrustning/programutveckling-och-systemdokumentation/ss-en-isoiec-270182020/
[23] T.ex. MSBFS 2020:6 föreskrifter om informationssäkerhet för statliga myndigheter.

12. Slutord

Denna rapport ger en överblick i frågor och utmaningar som kan bli aktuella vid anskaffning av molntjänster. När en myndighet samlat in relevant information och kartlagt alla viktiga aspekter ökar chanserna för att fatta välgrundade beslut.

Det är avgörande att myndigheten har fått tillräckligt bra underlag dels från leverantören, dels genom sin egen kartläggning. Att få tillräckligt bra underlag är idag ofta svårt och kräver både tid och hög kompetens av myndigheten. Vissa leverantörer kan se svårigheter i att dela information om sin tjänst med kunder. Samverkan med andra myndigheters experter och analysgrupper är därför en fördel i att genomföra kvalitativa analyser. Vid bristfälligt underlag bör myndigheten ta ställning till om det är möjligt att gå vidare utan att ha alla rättsliga, tekniska och säkerhetsmässiga detaljer inför ett beslut om att använda en molntjänst.

eSam är ett medlemsdrivet program för samverkan mellan myndigheter så att den offentliga förvaltningens digitalisering underlättas. Våra medlemmar vill tillvarata digitaliseringens möjligheter, både för att underlätta vardagen för privatpersoner och företag och för att använda våra gemensamma resurser ansvarsfullt och effektivt. Det gör eSams medlemmar bland annat genom att göra gemensamma analyser och att ta fram stöd och vägledningar.

Alla publikationer finns på esamverka.se

I eSam ingår Arbetsförmedlingen, Arbetsmiljöverket, Bolagsverket, Boverket, Centrala Studiestödsnämnden, Domstolsverket, E-hälsomyndigheten, Ekonomistyrningsverket, Finansinspektionen, Folkhälsomyndigheten, Försäkringskassan, Havs- och vattenmyndigheten, Inspektionen för vård och omsorg, Jordbruksverket, Kemikalieinspektionen, Kriminalvården, Kronofogdemyndigheten, Kustbevakningen, Lantmäteriet, Livsmedelsverket, Länsstyrelserna, Migrationsverket, Naturvårdsverket, Pensionsmyndigheten, Riksantikvarieämbetet, Riksarkivet, Rättsmedicinalverket, Sida, Skatteverket, Skolverket, Statens institutionsstyrelse, Statens servicecenter, Statens tjänstepensionsverk, Statens veterinärmedicinska anstalt, Statistiska centralbyrån, Tillväxtverket, Trafikverket, Transportstyrelsen, Tullverket, Universitets- och högskolerådet samt Utbetalningsmyndigheten. (Juni 2024.)