Dnr : **151834**

Rapport avseende drift av e-post

Postadress	Besöksadress	Telefon	Telefax	Webbplats	E-post
517 83 Bollebygd	Ballebovägen 2	033–231300	033-231428	www.bollebygd.se	kommunen@bollebygd.se

Inledning

Till följd av stora risker och en allvarlig driftsstörning i kommunens gamla datacenter har kommunstyrelsen fattat beslut om att tillfälligt tillåta att kommunens e-post flyttas till molntjänsten Exchange Online. I nuläget pågår förberedelser inför flytten som beräknas vara färdigställd under maj månad.

Kommunstyrelsen anser att kommunfullmäktige ska ta ställning ta ställning till att antingen fortsätta använda Exchange online eller flytta tillbaka driften till kommunens egna datacenter. I denna rapport avhandlas enbart frågan om flytt av e-post till en molntjänst, i ett längre perspektiv behöver kommunen göra ett strategiskt ställningstagande till molntjänster generellt samt vilka avvägningar som behöver göras inför varje ny molntjänst. Dessutom behöver nuvarande digitaliseringsstrategi uppdateras. Därför har kommunstyrelsen som avsikt att under hösten återkomma med ytterligare ett ärende om digitaliseringsstrategin där frågor som molntjänster, informationssäkerhet och andra strategiskt viktiga frågeställningar belyses.

Rapporten belyser frågan om e-post som molntjänst utifrån perspektiven informationssäkerhet, jurdik, teknik och ekonomi samt innehåller till sist en sammanvägd riskbedömning utifrån samtliga perspektiv.

Informationssäkerhet

Informationssäkerhet handlar om att ge den information kommunen hanterare rätt skydd, att upprätthålla önskad sekretess, riktighet och tillgänglighet, utan att för det skapa hinder för användaren. Det handlar om:

- **Konfidentialitet:** Att informationen skyddas mot obehörig insyn
- **Riktighet:** Att informationen skyddas mot oönskad förändring
- **Tillgänglighet:** Att information görs åtkomlig för behörig person vid rätt tillfälle
- **Spårbarhet:** vikten av att kunna spåra olika händelser

En förutsättning för en god informationssäkerhet är en hög driftssäkerhet i kommunens plattform. Nuvarande strategi för att säkerställa det bygger på att nyttja modern utrustning och programvaror som kontinuerligt upgraderas för att motverka driftsavbrott. Det finns avtal med företag som besitter specialistkompetens inom varje område som bedöms som känsligt som används vid behov. Det möjliggör att IT-enheten kan ha en slimmad organisation med en mer generell beställarkompetens. Den strategin bedöms som nödvändig för att säkerställa en god driftssäkerhet till en rimlig kostnad. IT-enhetens bedömning är att det nya datacentret har en hög driftssäkerhet och inga större investeringar är nödvändiga så länge som e-posten inte driftas lokalt. En hög driftssäkerhet är en av IT-enhetens uttalade mål och något som hela tiden utvecklas.

Ekonomi

Kostnaden för flytten till Exchange online uppgår till ca 50 tkr i form av inköpta konsulttjänster. Merparten av licenserna som behövs finns redan, men det kan behövas någon komplettering beroende på vilka val som görs, se mer nedan om licenser.

Kostnaden för lokal drift beräknas bli ca 2 mnkr under tre år till följd av uppgraderingar av kommunens nya datacenter då det inte är dimensionerat för att drifta e-post server. Kostnaderna avser främst licenser, men även hårdvara och konsulttjänster.

I nuläget arbetar IT-enheten tillsammans med en licenförsörjningspartner för att hitta den ekonomiskt mest fördelaktiga modellen för kommunens behov. Det går därför inte rakt av säga exakt hur stora kostnaderna blir för respektive alternativ men det är ställt helt utom tvivel att e-post som molntjänst kommer innebära en lägre licenskostnad vilket stärker bedömningen att molntjänst är att föredra utifrån ett ekonomiskt perspektiv. I dagsläget är bedömningen att enbart användarlicenser för personal i värsta fall kan komma bli ca 600 tkr dyrare jämfört med molntjänst. Utöver det tillkommer licenskostnader för fler servrar.

Oavsett vilken modell som väljs beräknas båda alternativen rymmas inom befintlig IT-budget. Däremot kommer lokal drift av e-post tränga undan andra projekt som i sin tur kan innebära andra negativa ekonomiska konsekvenser för kommunen.

Juridik

Utkontraktering av it-drift och användning av molntjänster är ett vanligt sätt för kommuner att hantera sin it-drift. Det som i nuläget är aktuellt för Bollebygd är att överväga om kommunen ska ha e-post i molnet. Oaktat om det rör sig om e-post eller andra molntjänster så är de juridiska övervägandena desamma, även om bedömningen är beroende av vilken typ av information det är som ska hanteras i molnet.

Det har gjorts ett flertal utredningar och rättsliga analyser kring användandet av molntjänster inom offentlig sektor, som kommit fram till motstridiga slutsatser. Detta har lett till att det råder en viss osäkerhet när det gäller de rättsliga förutsättningarna för utkontraktering av it-drift till privata tjänsteleverantörer. Osäkerheten gäller främst tolkningen av när en uppgift ska anses röjd enligt sekretess lagstiftningen (OSL) samt överföring av personuppgifter till tredjeland och då framför allt till länder där molntjänstleverantören kan bli skyldig att överlämna information med hänvisning till andra staters rättsordningar, så som t.ex. US CLOUD Act.

Den senaste i raden av utredningar som berör frågan är *”Delbetänkande av It-driftsutredningen (SOU 2021:1)”,* som kom tidigare i år. I delbetänkandet fokuseras på förutsättningarna för bland annat kommuner att utkontraktera it-drift.

Sekretess

I nämnda delbetänkande har man kommit fram till *”att en myndighet som utkontrakterar it-drift har lämnat ut de uppgifter som omfattas av utkontrakteringen till tjänsteleverantören. Detta gäller oavsett om omständigheterna när uppgifterna tillgängliggjordes tjänsteleverantören var sådana att man – t.ex. pga. kryptering eller annan teknisk säkerhetsåtgärd – inte måste ha räknat med att tjänsteleverantören eller någon annan utomstående skulle komma att ta del av uppgifterna. Uppgifterna är röjda enligt offentlighets- och sekretesslagen (2009:400) eftersom ett utlämnande är en form av röjande.”* Detta innebär att uppgifterna anses röjda i och med uppgifterna lämnas ut till molnleverantören oaktat om denne är bunden av US CLOUD Act eller någon liknande reglering..

Det ska dock beaktas att för Bollebygds del i dagsläget endast är aktuellt med e-post i molnet. Det bör också beaktas att användandet av e-post redan i dag innebär att uppgifter lämnas ut till utomstående då andra mailservrar än kommunens används när e-post skickas och tas emot. Genom

att ha riktlinjer kring epostanvändning som reglerar vilken typ av information som får skickas via e-post kan man minimera risken att röjande sker enligt OSL. Redan i dag finns det i kommunens *”Riktlinjer för användning av kommunens datorer”* angivet att det inte är tillåtet att skicka sekretessbelagda eller känsliga personuppgifter via e-post.

GDPR
Det är bara tillåtet att överföra personuppgifter till en mottagare i ett land utanför EU eller EES (tredjeland) om det kan ske på någon av de grunder som anges i kapitel V i dataskyddsförordningen. I ovan angivna delbetänkande anges att det utgör en överföring av personuppgifter till tredjeland när en personuppgiftsansvarig eller ett personuppgiftsbiträde behandlar personuppgifter genom användning av utrustning som finns i tredjeland. Det saknar betydelse hur lång eller kort tid som utrustningen används, och om uppgifterna är krypterade eller pseudonymiserade.

EU kommissionens skyddande standardklausuler kan vara en lämplig skyddsåtgärd som kan läggas till grund för överföring av personuppgifter till tredjeland, om det i mottagarens land finns ett grundläggande rättighetsskydd och en möjlighet att göra detta skydd gällande inför domstol eller annan oberoende instans. EU har upprättat en lista över de länder som uppfyller kravet för en adekvat skyddsnivå.

USA anses i dagsläget inte ha en adekvat skyddsnivå för personuppgifter, mot bakgrund att det grundläggande rättsskyddet i USA inte ger en sådan nivå av skydd som krävs enligt dataskyddsförordningen. EU-domstolen har angett att personuppgifter inte längre lagligen kan överföras till USA (eller behandlas med åtkomst från USA) med stöd av att mottagaren självcertifierat sig enligt Privacy Shield-ramverket. Detta för att alla företag i USA, också om de är certifierade, omfattas av lagstiftning som ger amerikanska myndigheter mycket långtgående möjligheter att begära åtkomst till personuppgifter. EU-domstolens uttalanden om den otillräckliga skyddsnivån för personuppgifter i USA, pekar mot att en överföring just till USA med stöd av EU kommissionens skyddande standardklausuler också kan anses vara otillåten.

Precis som när det gäller OSL ska det dock beaktas att det i dagsläget rör sig om att flytta e-post till molnet. Att kunna skicka och ta emot e-post är en förutsättning för att kunna utföra sina arbetsuppgifter i kommunen. Genom att mail, som skickas och tas emot, kan komma att passera ett flertal servrar innan det når den tänkta mottagaren får det redan idag ansen att överföring av personuppgifter till tredjeland kan ske.

Bedömning juridisk
Sammanfattningsvis kan konstateras att användandet av molntjänster kan anses innebära ett röjande av uppgifter enligt OSL och att överföring av personuppgifter till en mottagare i tredjeland kan innebära en risk för att man inte följer dataskyddslagstiftningen.

Det bör dock beaktas att det för Bollebygds del i dagsläget endast rör sig om att överföra e-post till molnet. Redan idag skickas e-post genom olika servrar som inte är kommunens. Om e-post istället skulle skickas via molnet innebär ingen större skillnad ur ett rättsligt perspektiv. Vid en bedömning om att ha e-post i molnet eller i lokala servrar, blir det alldeles för ensidigt att endast peka ut brister i molntjänster utan att beakta riskerna och bristerna i att ha lokala servrar.

Även om rättsläget för närvarande är osäkert är informationsklassning och riskanalyser ett arbete som är nödvändigt att genomföra, oavsett om informationshanteringen kommer att ske med egen it-drift, hos traditionell systemleverantör eller i molntjänst.

Mot bakgrund av det osäkra rättsläget är det inte möjligt att lämna generella inriktningsrekommendationer. Det är upp till varje kommun att utifrån sina förutsättningar och möjligheter göra sin egen sammantagna riskbedömning för varje informationsbehandling.

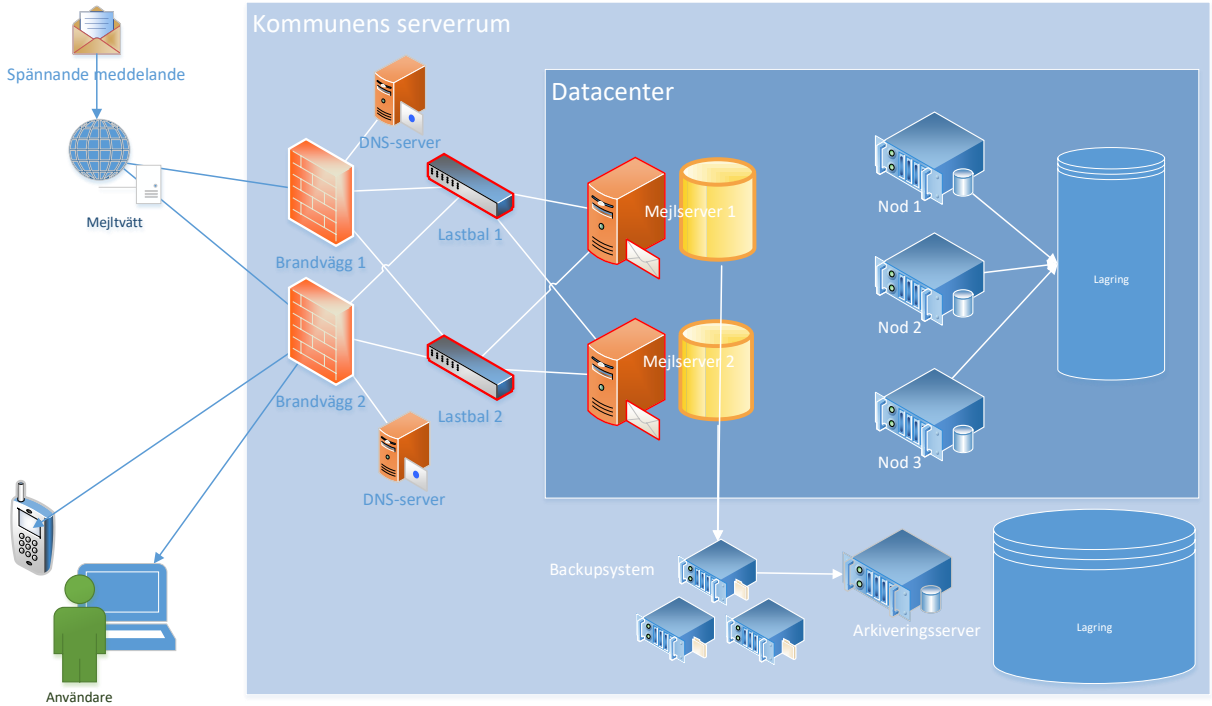
Teknik

I Bollebygd finns i dagsläget två datacenter, ett nytt och ett gammalt. Det gamla datacentret är från 2016 och bedöms sedan en tid tillbaka har nått sin beräknade livslängd och är inte lämplig att använda i en skarp produktionsmiljö.

Under 2019/2020 upphandlades och driftsattes det nya datacenter i Bollebygd kommun. Planen har sedan dess varit att använda e-post som en molntjänst eftersom det på många sätt är en säkrare och mer ekonomiskt fördelaktig lösning. I samband med kravställningen i upphandlingen fanns därför inte förutsättningarna med att det nya datacentret skulle drifta en e-postserver och därför dimensionerades inte heller datacentret för det. Något formellt beslut om att övergå till en molntjänst fattades dock inte, och bedömningen vid den tidpunkten var att det inte var särskilt kontroversiellt, många kommuner hade redan flyttat till exchange online och det sågs som relativt oproblematiskt. Succesivt har tjänster flyttas över till nya datacentret och numera finns det enbart kvar e-post på det gamla datacentret. Planen är att när samtliga driftstjänster är borta från gamla datacentret ska det förflyttas fysiskt och konfigureras som en recovery site för att skapa redundans i kommunens drift. Om det nya datacentret av någon anledning slås ut ska det gamla datacentret kunna gå in och alla tjänster ska kunna fungera som vanligt.

Nedan följer en beskrivning över de två olika alternativen

E-post driftas i lokalt datacenter



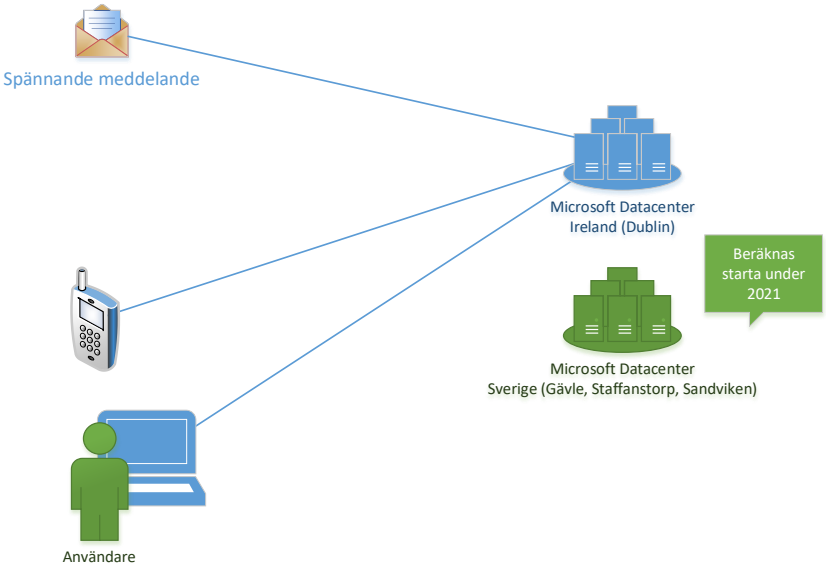
Riskbedömning av lokal drift
Det gamla datacentret har nått sin end-of-life som produktionsmiljö och det finns stor risk att allvarliga incidenter uppstår som kan innebära att större delen av kommunens servrar slås ut. Eftersom både gamla och nya datacentret finns på samma fysiska plats finns det en risk att driftstörningar i det gamla datacentret påverkar även det nya datacentret. Konsekvenserna kan bli så allvarliga så att alla kommunens servrar går ner vilket i praktiken innebär att inga system, skrivare eller mappar kan nås från klienterna.

Det nya datacentret är inte dimensionerat för e-post och det innebär en stor risk att flytta tillbaka e-posten till gamla datacentret. Det omöjliggör även en recovery site för att utöka driftsäkerheten ytterligare.

Ett alternativ för att drifta e-posten på en lokal server är att komplettera och bygga ut det nya datacentret så att det har kapacitet att drifta även e-posten. Kostnaden beräknas till ca 2 mnkr och kommer innebära en stor påfrestning för befintlig personal då det är ett mycket omfattande arbete. I nedanstående tabell finns en bedömning av för- och nackdelar med en mailmiljö i lokal drift, oaktat de driftsproblem som är förknippande med det gamla datacentret.

Fördelar	**Nackdelar**
Möjlighet till full kontroll över lösningen	Svårt att bygga ett säkert system i en liten skala till en rimlig kostnad.
Full kontroll på vart informationen lagras	Hårdvara och mjukvara måste förnyas regelbundet
Möjlighet till specialanpassad lösning i fall behovet finns	Utmanande att prognostisera för en framtida tillväxt och välja rätt storlek på system/lösning
	Höga up-front kostnader
	Krävs specialistkompetens av systemförvaltarna
	Ett ständigt hot, speciellt då Exchange on-prem är en prioriterad måltavla för hackers

E-post som molntjänst via Exchange online (Microsoft)



I nedanstående tabell sammanfattas de fördelar och nackdelar som finns utifrån ett tekniskt perspektiv med e-post som tjänst via Exchange online.

Fördelar	Nackdelar
Microsoft garanterar 99,9% upptid på Exchange Online och Office 365	Höga licenskostnader i fall du ger allt till alla
Ingen egen hårdvara krävs	
Förutsägbara kostnader, betala för det du använder	
Alltid uppdaterad	
Möjlighet till moderna säkerhetslösningar	
Möjlighet att efterleva GDPR med inbyggda verktyg i Exchange Online och Office 365	

Bedömning teknisk
Det finns egentligen två alternativ som bedöms möjliga, det ena är att flytta tillbaka e-posten till en ny lokal server med en mer driftsäker miljö än det gamla datacentret. Det andra alternativet är att vara kvar i molntjänsten. Då nuvarande datacenter inte är dimensionerad för att drifta e-post servrar kommer ganska stora kostnader uppstå och kommer ta lång tid att genomföra. Molntjänsten bedöms som betydligt bättre utifrån driftssäkerhet och är den lösning som starkt rekommenderas utifrån ett tekniskt perspektiv.

Kommunstyrelsen avråder från att flytta tillbaka e-posten till det gamla datacentret.

Sammanfattande bedömning

Frågan om molntjänst eller lokal drift innehåller inget rätt eller fel, det finns inte heller några generella inriktningsbeslut att förhålla sig till utan det måste för varje ny information som behandlas genomföras en klassificering och riskbedömning för att välja den mest lämpliga åtgärden. I vissa fall kommer det väga över för att nyttja en molntjänst och ibland kommer bedömningen landa i lokal drift.

Som framgår av denna riskbedömning finns det för- och nackdelar med att flytta e-posten till en molntjänst. Utifrån tekniska, informationssäkerhetsmässiga och ekonomiska risker finns stora fördelar med en migrering.

Utifrån ett juridiskt perspektiv finns däremot större risker som talar emot en migrering jämfört med de som talar för. Det innebär inte att nuvarande lösning är helt oproblematisk utifrån ett dataskyddsperspektiv. Det finns dock saker som kan göras för att motverka den risken genom att t.ex. använda sig av moderna informationssäkerhetslösningar och att ta fram riktlinjer för vilken information som hanteras i mailen. I dagsläget ska inte uppgifter som innehåller sekretess eller känsliga personuppgifter lagras i mailen, dessa ska istället hanteras i lokalt driftade verksamhetssystem/ärendehanteringssystem. En större informationsinsats till samtliga användare är också planerad att initieras under april/maj som kommer löpa under två år som avser informationssäkerhet och dataskydd för att öka medvetenheten om rutiner och riktlinjer. Slutligen kan även konstateras att en mängd organisationer och kommuner redan i dagsläget använder e-post som molntjänst och att det hittills, vad vi känner till, inte inneburit någon sanktionsavgift.

En sammanfattande bedömning är att de risker som finns med lokal drift är större än de som finns vid e-post som molntjänst och rekommenderar därför kommunfullmäktige att godkänna