Riskbedömning avseende Exchange online

Denna riskbedömning är ett pågående arbete som primärt var tänkt att användas som ett beslutsunderlag inför kommunfullmäktiges ställningstagande avseende flytt av e-post server från lokal drift till molnet i juni. Till följd av en allvarlig driftsincident och att omgående ställningstagande behövs kommer detta preliminära underlag att användas som riskbedömning avseende ett tillfälligt beslut om Exchange online till dess att kommunfullmäktige fattar annat beslut. Denna riskbedömning kommer kompletteras innan ärendet skickas till kommunfullmäktige.

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.

Standardavtalsklausuler anses 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. Undantag kan dock göras om mottagaren till personuppgifterna anslutit sig till den så kallade Privacy Shield Act, Privacy Shield Act är dock under prövning i EU.

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, passerar ett flertal servrar innan det når den tänkta mottagaren får det redan idag ansen att överföring av personuppgifter till tredjeland kan ske.

Sammanfattning Juridik

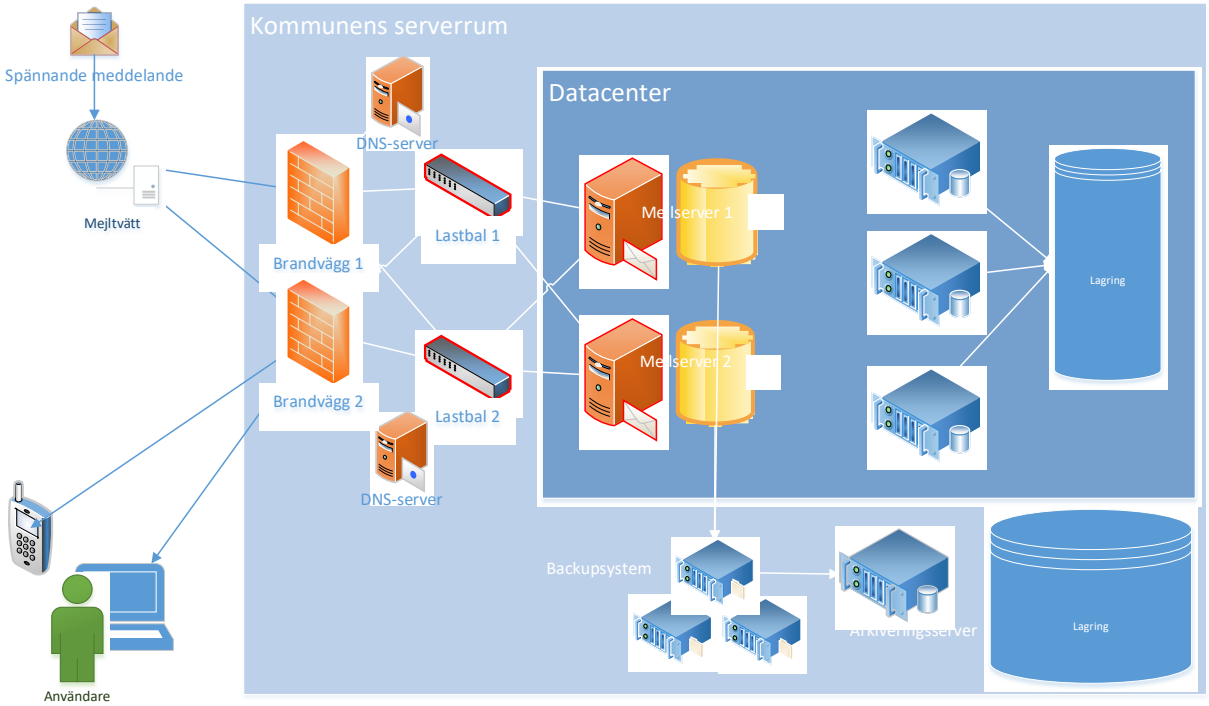
Sammanfattningsvis kan man konstatera att användandet av molntjänster kan anses innebära ett röjande av uppgifter enligt OSL och att överföring av personuppgifter till en mottagare i tredjeland kan innebära en risk för att man inte följer dataskyddslagstiftningen.

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.

Teknik/Informationssäkerhet

I dagsläget driftas kommunens e-post server på ett lokalt datacenter som har varit i drift sedan 2016. Under 2020 togs ett nytt datacenter i drift men det dimensionerade aldrig för att klara av att drifta kommunens e-postserver. Planen har sedan lång tid tillbaka istället varit att använda en molntjänst, Exchange online, som levereras av Microsoft eftersom det på många sätt är en säkrare och mer ekonomisk lösning. Nedan följer en beskrivning över de två olika tekniska alternativen

E-post driftas i lokalt datacenter (nuvarande lösning)



Riskbedömning av nuvarande lösning

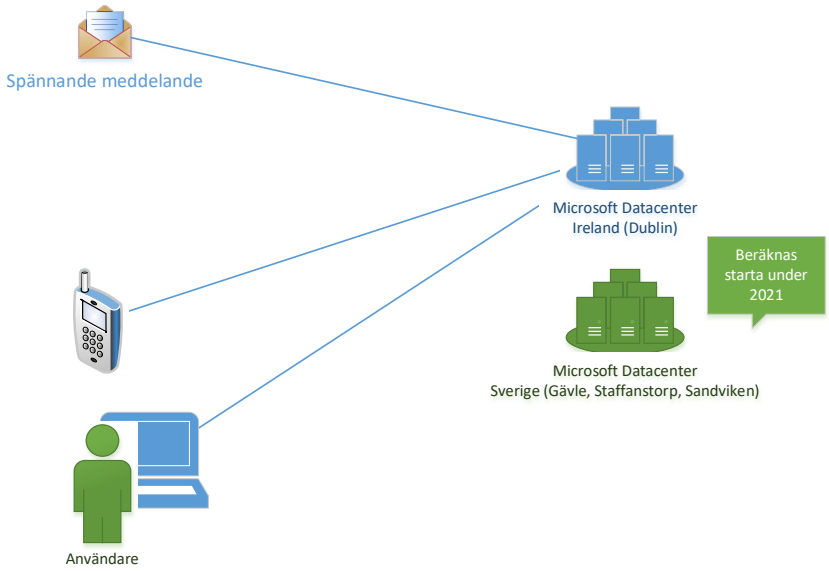
Det gamla datacentret har nått sin end-of-life och det finns stor risk att allvarliga incidenter uppstår som kan innebära att större delen av kommunens servrar slås ut. Eftersom både gamla och nya datacentret finns på samma fysiska plats finns det en risk att driftstörningar i det gamla datacentret påverkar även det nya datacentret. Se vidare för incidentrapport 2021-04-17 – 2021-04-20 för utförligare information. För att kunna ta gamla datacentret ur produktionsdrift behöver en lösning hittas för mailservern. Förvaltningens bedömer att det finns en stor risk för nya och eventuellt ännu allvarligare incidenter om inte en nedstängning av gamla datacentret görs omgående. 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.

Utöver detta ger nedanstående tabell en bedömning av för- och nackdelar med en mailmiljö i lokal drift, oaktat de driftsproblem som är förknippande med befintliga äldre datacenter.

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 tjänst 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	

Sammanfattning teknik

En lösning måste snarast hitta som innebär att gamla datacentret kan tas ur drift. Det finns egentligen två möjliga vägar, det ena är att flytta befintlig e-postserver till en ny lokal server med en mer driftsäker miljö. Det andra alternativet är att genomföra en migrering till Exchange online. Då nuvarande datacenter inte är dimensionerad för att drifta e-post servrar behöver antingen datacentret kompletteras eller ett helt nytt datacenter byggs upp. Detta kommer kosta stora summor och ta flera månader att genomföra och är alltså i praktiken ingen lösning för det akuta problem som finns. Förvaltningens bedömning är att den enda realistiska möjligheten för att säkra en god driftssäkerhet är att omgående migrera mailen till exchange online.

Sammanfattande bedömning

Som framgår av denna riskbedömning finns det för- och nackdelar med att migrera mailen. Utifrån tekniska, informationssäkerhetsmässiga, ekonomiska och organisatoriska risker finns stora fördelar med en migrering. Det finns egentligen inget starkt skäl alls utifrån dessa perspektiv att fortsätta drifta mailen lokalt.

Utifrån ett juridiskt perspektiv finns däremot starkare 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. En större informationsinsats till samtliga användare är också planerad att initierad under april/maj som kommer löpa under två år som avser informationssäkerhet och dataskydd. Sammanfattningsvis kan även konstateras att en mängd organisationer och kommuner redan i dagsläget använder Exchange online och att det hittills, vad vi känner till, inte inneburit någon sanktionsavgift.

Förvaltningens bedömning att de risker som finns av att inte migrera mailen kraftigt överväger de risker som finns med en migrering och rekommenderar därför kommunstyrelsen att godkänna en tillfällig migrering till Exchange online till dess att kommunfullmäktige kan ta ställning till frågan. I de fall kommunfullmäktige inte godkänner migreringen behöver förvaltningen ytterligare några månader på sig att bygga ut befintligt datacenter och genomföra ett återtagande. Förvaltningen rekommenderar därför att godkännande gäller tom 2021-12-31.