



Myndigheten för
samhällsskydd
och beredskap

Outsourcing av it-tjänster i kommuner

Innehållsförteckning

| | |
|--|-----------|
| 1. Inledning | 4 |
| 1.1 Bakgrund | 4 |
| 1.2 Informationssäkerhet och upphandling av it-relaterade tjänster .. | 6 |
| 2. Hur använder kommunerna outsourcing, samverkan kring it-tjänster och molntjänster? | 7 |
| 2.1 Omfattningen av outsourcing och samverkan kring it- och molntjänster | 7 |
| 2.2 Varför väljer kommunerna att outsourca sin it-drift? | 8 |
| 2.3 Inom vilka verksamheter har kommunerna använt outsourcing, molntjänster och samverkan om it? | 9 |
| 2.4 Förmågan att hantera störningar vid it-incidenter | 9 |
| 2.5 Säkerhetskrav i upphandlingar | 10 |
| 3. Avslutande reflektioner | 12 |

1. Inledning

1.1 Bakgrund

Kommunerna står för en anseelig del av den samhällsviktiga verksamheten i Sverige. Det finns ingen uttrycklig förteckning över vad som ska ses som samhällsviktig verksamhet. I MSB:s Handlingsplan för skydd av samhällsviktig verksamhet¹ ges istället följande beskrivning:

Med samhällsviktig verksamhet avses en verksamhet som uppfyller minst ett av följande villkor:

- Ett bortfall av, eller en svår störning i verksamheten som ensamt eller tillsammans med motsvarande händelser i andra verksamheter på kort tid kan leda till att en allvarlig kris inträffar i samhället.
- Verksamheten är nödvändig eller mycket väsentlig för att en redan inträffad kris i samhället ska kunna hanteras så att skadeverkningarna blir så små som möjligt.

I samma plan finns även en tabell över de elva samhällssektorer inom vilka merparten av viktiga samhällsfunktioner och samhällsviktiga verksamheter finns:

| SAMHÄLLSSEKTOR | EXEMPEL PÅ VIKTIGA SAMHÄLLSFUNKTIONER |
|---|--|
| Energiförsörjning | Produktion av el, distribution av el, produktion och distribution av fjärrvärme, produktion och distribution av bränslen och drivmedel m.m. |
| Finansiella tjänster | Betalningar, tillgång till kontanter, centrala betalningssystemet, värdepappershandel m.m. |
| Handel och industri | Bygg- och entreprenadverksamhet, detaljhandel, tillverkningsindustri m.m. |
| Hälso- och sjukvård samt omsorg | Akutsjukvård, läkemedels- och materielförsörjning, omsorg om barn, funktionshindrade och äldre, primärvård, psykiatri, socialtjänst, smittskydd för djur och människor m.m. |
| Information och kommunikation | Telefoni (mobil och fast), internet, radiokommunikation, distribution av post, produktion och distribution av dagstidningar, webbaserad information, sociala medier m.m. |
| Kommunalteknisk försörjning | Dricksvattenförsörjning, avloppshantering, renhållning, väghållning m.m. |
| Livsmedel | Distribution av livsmedel, primärproduktion av livsmedel, kontroll av livsmedel, tillverkning av livsmedel m.m. |
| Offentlig förvaltning – ledningsfunktioner – stödfunktioner | Lokal ledning, regional ledning, nationell ledning, begravningsverksamhet, diplomatisk och konsulär verksamhet m.m. |
| Skydd och säkerhet | Domstolsväsendet, åklagarverksamhet, militärt försvar, kriminalvård, kustbevakning, polis, räddningstjänst, alarmeringstjänst, tullkontroll, gränsskydd och immigrationskontroll, bevaknings- och säkerhetsverksamhet m.m. |
| Socialförsäkringar | Allmänna pensionssystemet, sjuk- och arbetslöshetsförsäkringen m.m. |
| Transporter | Flygtransport, järnvägstransport, sjötransport, vägtransport, kollektivtrafik m.m. |

¹ Handlingsplan för skydd av samhällsviktig verksamhet (MSB597, 2013)

Som framgår är det en inte ringa del av den samhällsviktiga verksamheten som sker i kommunal regi.

Det krävs inte heller någon djuplodande undersökning för att inse att denna verksamhet i de flesta fall är i hög grad beroende av sin informationshantering. Att upprätthålla vård, vattenförsörjning, transportsystem och inte minst lokal ledning blir snabbt mycket svårt om inte den normala informationshanteringen fungerar.

Informationssäkerhet är därför en viktig fråga inte bara för den enskilda kommunen utan för samhället i stort. Under senare år har en aspekt av skydd av information blivit allt viktigare, nämligen hur outsourcing och användande av molntjänster ska kunna ske på ett säkert sätt. Allt fler både privata och offentliga organisationer väljer att i allt högre grad fokusera på sin kärnverksamhet. I stället för att ha drift och förvaltning av sina it-lösningar i den egna organisationen anlitas externa leverantörer för outsourcing eller molntjänster. Att upphandla olika typer av it-relaterade tjänster kan i många fall vara en bra lösning men kräver också en kvalificerad upphandlingsprocess om slutresultat ska bli en effektiv och dessutom säker lösning. Riskanalyser och informationsklassning behöver göras oavsett intern eller extern drift och förvaltning. Liksom även beaktandet av livscykelperspektivet. Det väsentliga är att analysera och hantera skillnaderna i riskbilderna om de skiljer sig.

Förutom att kommunerna har ett antal för samhället mycket viktiga uppgifter är deras förutsättningar att lösa dessa uppgifter varierande. Enbart den skiftande storleken på Sveriges 290 kommuner ger en indikation på hur olika organisationer det handlar om trots att de alla har samma grunduppdrag. Sett ur perspektivet samhällets informationssäkerhet är det en intressant fråga hur kommunerna anser att de har möjlighet att hantera den komplexa uppgiften att hantera sin information på ett säkert sätt. I denna större fråga ingår delfrågan om användandet av outsourcing och molntjänster vilket den här rapporten handlar om.

En viktig faktor att beakta är att outsourcing och användande av kommersiella molntjänster inte är de enda formerna för lösningar där kommunerna frånhänder sig den praktiska driften och förvaltningen av it-system och informationshantering. Det är även vanligt att kommuner inleder både större och mindre samarbeten kring it-drift liksom att man använder olika typer av offentliga molntjänster. Att ha tydliga ansvarsförhållanden i sådana relationer är av samma betydelse som då det handlar om kommersiella tjänster.

Ett antal större it-incidenter har visat på risken för allvarliga konsekvenser då en outsourcingleverantör drabbas av störningar. Se till exempel den så kallade Tieto-incidenten i december 2011, som MSB analyserat närmare i en rapport². I nuläget finns en stark koncentration av outsourcing kommunalt it-stöd. Detta innebär en ännu inte tillräckligt analyserad nationell risk.

² Reflektioner kring samhällets skydd och beredskap vid allvarliga it-incidenter (MSB367, 2012)

Underlag för de resonemang som förs i rapporten är bland annat hämtade från enkäter sammanställda i två projekt som MSB låtit Totalförsvarets forskningsinstitut (FOI)³ och Karlstads universitet⁴ genomföra under 2013. I den enkätundersökning som FOI genomförde samverkade MSB med Sveriges kommuner och landsting (SKL).

1.2 Informationssäkerhet och upphandling av it-relaterade tjänster

Som begreppet antyder syftar informationssäkerhet till att skydda information. Med skydd avses att kunna upprätthålla rätt nivå av

- konfidentialitet
- riktighet
- tillgänglighet
- spårbarhet.

Informationssäkerhet vid upphandling av it-relaterade tjänster handlar därmed om att styra upphandlingsprocessen så att den levererade tjänsten kan upprätthålla de krav på att informationen ska vara skyddad hos leverantören som har definierats i avtalet. Det innebär till exempel att informationen ska vara skyddad från obehörig insyn och förändring hos leverantören samt att informationen och möjligheten att hantera den finns hos kunden på den nivå som överenskommit. Kunden ska också ha möjlighet att granska hur informationen har hanterats hos leverantören.

Grundläggande för samtliga fall då informationshanteringen helt eller i delar läggs ut på en annan part är att ansvaret för informationen och dess säkerhet alltid ligger kvar hos informationsägaren. Mer om det finns att läsa i den vägledning om informationssäkerhet i upphandling som MSB tagit fram⁵.

³ MSB dnr 2013-3035

⁴ MSB dnr 2013-3300

⁵ Vägledning – informationssäkerhet i upphandling (MSB555, 2013)

2. Hur använder kommunerna outsourcing, samverkan kring it-tjänster och molntjänster?

Att få svar på i vilken omfattning kommuner använder sig av outsourcing och samverkan kring it-tjänster och molntjänster är en intressant men svårlöst uppgift. Det finns ett antal metodproblem som gör att denna rapport får ses som ett inledande steg i ett längre arbete. Ett grundläggande metodproblem är vad som ska definieras som it och som outsourcing, ett annat problem är avgränsningen av vad som ska räknas som it-verksamhet eftersom it numera ofta är inbäddad i kärnverksamhetens processer. En annan faktor som gör metodvalet komplicerat är att den kommunala verksamheten är uppdelad i tämligen fristående förvaltningar som delvis ansvarar för sina egna it-lösningar. Därmed har kommunen på central nivå inte alltid den överblick som skulle krävas för att svara på enkätens frågor.

I den enkät som används som underlag var svarsfrekvensen relativt låg, av de tillfrågade 290 kommunerna svarade 122 stycken vilket motsvarar 42 procent. Vad orsaken till den låga svarsfrekvensen är har inte analyserats närmare men en arbetshypotes kan vara att det är svårt att genom enkäter fånga så komplexa frågor som det här rör sig om. I enkäten förekom till exempel frågor kring samhällsviktig verksamhet och kritiska beroenden vilket är begrepp där flera aktörer inom de tillfrågade kommunerna måste samverka för att kunna ge relevanta svar. Några ytterligare förklaringar kan vara att tidpunkten för enkäten var mindre lämplig och att komplexiteten i frågorna krävde svar från flera olika personer i organisationen vilket gjorde arbetet för mottagarna för omfattande.

Det finns därför anledning att tolka och använda det aktuella resultatet med försiktighet. Nedan redovisas några av de grundläggande reflektioner som enkäten och kompletterande intervjuer gett upphov till.

2.1 Omfattningen av outsourcing och samverkan kring it- och molntjänster

Flera av de tillfrågade kommunerna angav som sagt att frågan kring omfattningen av outsourcing och liknande lösningar inte låter sig besvaras på något enkelt sätt. Problemen ligger bland annat i definitioner av vad som ska räknas som it och svårigheten i att skapa en överblick inom en kommun med tanke på de ofta självständiga verksamheter som finns både i form av förvaltningar och kommunala bolag.

Vad som dock kan sägas är att cirka 80 procent av de kommuner som svarat på enkäten angav att de använde någon form av outsourcing. I det ingår både

användning av kommersiella tjänster vilket 64 procent av kommunerna upphandlat och olika typer av kommunal samverkan som 66 procent ingått i.

En vanlig uppfattning bland de svarande är att trenden går mot allt mer ”mixade” lösningar som är sammansatta delvis av kommunens egna resurser, delvis av upphandlade resurser. Det skapar komplexa beroenden till externa aktörer som kan vara svåra att beskriva men gör också att kommunens egen it-verksamhet allt mer ändras till en samordningsroll. För att utöva denna roll på ett bra sätt krävs generellt en tydlig strategisk inriktning från kommunens ledning, stark beställarkompetens och organisatoriska förutsättningar för att långsiktigt kunna styra it-arkitekturen. I styrningen ingår också att systematiskt följa upp och utvärdera både interna och externa leveranser. Många kommuner håller liksom andra organisationer på att centralisera sin it-verksamhet vilket kan ses som ett steg för att kunna hantera den delvis nya situationen.

2.2 Varför väljer kommunerna att outsourca sin it-drift?

En intressant fråga är varför kommunerna väljer andra lösningar än att sköta sin drift och förvaltning i egen regi. Det mest uppenbara skälet, och det som ofta tolkas som det enda skälet, är naturligtvis ekonomiskt. Att ekonomin skulle vara den enda fördel som kommunerna ser med till exempel outsourcing stämmer dock inte med de svar som lämnats i enkäten. De svarande kommunerna uppger i stället att tillgänglighet och driftssäkerhet är de starkaste faktorerna som påverkar beslutet om outsourcing. Många ser också outsourcing och samverkan som bra sätt att förbättra kommunens kompetensbehov inom it-området liksom även för att förbättra säkerheten.

I intervjuer med de kommunala företrädarna har de hävdade att de ser ett samband mellan att kommuner som generellt är benägna att anlita utomstående leverantörer i andra sammanhang även gör det inom it-området. Konkret kan det innebära att en kommun som exempelvis genomfört mer omfattande upphandlingar inom vårdområdet blir mer benägen att även outsourca it.

Svaren ger en indikation om några väsentliga utmaningar för kommunerna som sannolikt kommer att accentueras under de närmaste åren. Det komplexa uppdrag som kommunerna har ställer stora krav på informationshanteringen, vilket i sin tur gör att kommunerna måste ha tillgång till en både hög och bred it-kompetens och till en välutvecklad informationssäkerhet. Samtidigt ställer den ofta pressade ekonomin krav på hög grad av effektivitet i stödfunktioner som it. Att få till stånd långsiktiga lösningar med den omfattande kravbild som kommer att vara en utmanande uppgift för många kommuner och det är i det perspektivet outsourcing, molntjänster och olika typer av samverkan behöver analyseras.

2.3 Inom vilka verksamheter har kommunerna använt outsourcing, molntjänster och samverkan om it?

Som redan framgått menar de svarande att den överblick saknas som skulle behövas för att ge en välgrundad uppfattning om vilka verksamheter inom kommunen som i störst omfattning använder sig av outsourcing, molntjänster eller samverkan med andra kommuner kring it. De it-relaterade tjänsterna kan också vara av mycket olika karaktär i hela spannet från outsourcing av kommunens hela drift till smala molntjänster med mycket begränsade funktioner.

I enkäten har frågor ställts om i vilken omfattning outsourcing med mera skett i skola, social omsorg, teknisk försörjning, samhällsbyggnad, räddningstjänst samt ledning och administration.

Av svaren gällande de undersökta verksamheterna kan vissa slutsatser dras:

- Mindre än fem procent av de tillfrågade kommunerna har outsourcat driften i sin helhet till en kommersiell aktör.
- Mindre än tio procent har lagt ut driften i sin helhet i en kommunal samverkansform (undantaget Räddningstjänsten där siffran är 11 %).
- Däremot är det vanligt att lägga ut enskilda system och tjänster till utomstående part. Det är 80 procent av de tillfrågade kommunerna som uppger att det förekommer i den egna verksamheten.
- I störst omfattning sker outsourcing, samverkan eller användande av molntjänster inom skolverksamheten och den sociala omsorgen, i minst omfattning inom räddningstjänsten.

Att outsourcing och samverkan kring system och tjänster är mycket mer vanligt förekommande än outsourcing av it-drift har sannolikt sin grund i kommunernas obligatoriska uppgifter sker på ett likartat sätt i samtliga kommuner. Därmed finns det uppenbara stordriftsfördelar i att använda samma tjänster liksom det finns en väldefinierad marknad för kommersiella aktörer att verka på.

Av intervjuerna framgår det att flertalet kommuner inte anser sig ha outsourcat drift och förvaltning av stöd för samhällsviktig verksamhet, en uppgift som behöver kvalitetssäkras i en mer djuplodande undersökning med tydligare definitioner att utgå från.

2.4 Förmågan att hantera störningar vid it-incidenter

Många av de tillfrågade kommunerna har alltså överlätit drift och förvaltning i större eller mindre omfattning till externa parter. Det kan innebära risker för störningar vid it-incidenter. För att reducera negativa konsekvenser av störningarna krävs åtgärder både hos kunden och hos leverantören (även vid kommunal samverkan). Leverantörens åtgärder regleras i huvudsak via avtal,

vilket diskuteras närmare i nästa avsnitt, medan kommunen bör ha en genomarbetad kontinuitetsplan som övas och uppdateras regelbundet.

Av enkätssvaren framgår att mindre än 20 procent av de tillfrågade kommunerna tagit fram en kontinuitetsplan som stöd för att kunna hantera en it-incident. Nästan 50 procent uppger att ett arbete pågår för att ta fram en plan. Trots det anser 64 procent att beredskapen för att hantera en sådan störning är ”god” och 8 procent till och med ”mycket god”. Närmare 80 procent bedömer också återhämtningsförmågan på likartat sätt.

När det gäller övning säger nästan 60 procent att någon övning kring scenariot större it-incident aldrig genomförts. Bland de återstående som svarat att övningar genomförts säger den absoluta merparten att övningar endast sällan genomförs.

Sammantaget ger dessa svar kring kommunernas beredskap för hantera it-incidenter en något motsägelsefull bild av situationen. Å ena sidan menar de tillfrågade att beredskapen företrädesvis är god, å andra sidan saknar huvuddelen av dem planering och följaktligen övning för att klara av en it-incident utan att samhällspåverkande störningar uppstår.

2.5 Säkerhetskrav i upphandlingar

Upphandling av it-relaterade tjänster är en uppgift som kräver långsiktighet och en sammansatt kompetens. Att dessutom arbeta in nödvändiga krav på informationssäkerhet i upphandlingen har visat sig vara en svår utmaning för de flesta offentliga organisationer. I den undersökning av ett antal avrop från Kammarkollegiets ramavtal för it-tjänster som MSB låtit Karlstads universitet genomföra framkom att de undersökta avtalen i hög grad saknade relevanta krav på informationssäkerhet. De krav som formulerats var i samtliga fall inriktade på enstaka frågor och kan inte ses som resultatet av en systematisk genomgång av kundens behov utifrån en genomarbetad riskanalys.

Med denna bakgrund är det även för stora myndigheter (som dessutom har föreskriftskrav på sig att bedriva ett systematiskt informationssäkerhetsarbete⁶) ett avancerat projekt att genomföra en upphandling av it-relaterade tjänster där informationssäkerhet är en integrerad del. Det belyser kommunernas svårigheter eftersom de ofta har betydligt mindre resurser att hantera upphandlingar. I enkäten till kommunerna gjordes ett val att endast ställa en fråga kring kraven på tillgänglighet, det vill säga en av de fyra aspekter som informationssäkerheten syftar till att uppnå. Svaren i enkäten visar att även detta avgränsade säkerhetsperspektiv är otillfredsställande reglerat enligt kommunerna. Så många som 60 procent anger att regleringen av leverantörens skyldigheter vid it-incidenter saknas eller är otillfredsställande. Det bör observeras att vad kommunerna svarat på här är sannolikt främst regleringen av relationen med kommersiella aktörer. I andra sammanhang finns problemen med att hitta former för överenskommelser mellan offentliga verksamheter, där överenskommelserna

⁶ MSBFS 2009:10

kan fylla samma funktion som kommersiella avtal. Det perspektivet måste vägas in även här.

För att göra en framgångsrik upphandling behöver det finnas en beställarkompetens under själva upphandlingskedet, men också under hela den tid som avtalet gäller. Samma sak gäller då offentliga verksamheter ingår i samarbeten med varandra. Att beställarkompetensen måste finnas kontinuerligt kan vara lätt att glömma bort men är en nog så viktig faktor för att kommunen i det här fallet ska få en fungerande it-lösning. Eftersom särskilt små kommuner är sällanköpare av it-tjänster hamnar de ofta i underläge gentemot leverantören och riskerar att göra en dålig affär. En sammansatt beställarkompetens som också följer med under hela affärens eller samarbetets livscykel är därför en nödvändig förutsättning.

Kraven på informationssäkerhet uppstår i verksamheten vilket är värt att understryka då beställarkompetensen diskuteras – verksamheten är både riskägare och har också kompetensen att se till sitt behov av säkerhet. Det behovet måste dock omformuleras i en kravspecifikation eller ett underlag för samarbete och då behövs kompetens inom bland annat it, juridik och upphandling.

I enkäten ombads kommunerna att på en fem-gradig skala ange hur svårt de tycker att det är att genomföra en it-upphandling i de tre ovan nämnda avseendena: it, juridik och upphandling. Medelvärdet översteg i samtliga fall tre på skalan vilket visar att man uppfattar detta som en svår uppgift. Det som bedömdes som allra svårast var den juridiska aspekten.

Det är inte bara den enskilda kommunen som har intresse av att inarbeta informationssäkerhet i sina upphandlingar utan hela samhället. Det finns dock dimensioner av informationssäkerheten som den enskilda kommunen inte kan påverka i någon högre grad. En sådan dimension av nationellt intresse är att i fråga om kommersiell outsourcing har kommunerna anlitat ett fåtal kommersiella aktörer, vilket framkommer i enkäten. Det ger en nationell koncentration som inte den enskilda kommunen är medveten om och knappast kan undvika att medverka till. En större it-incident hos någon av dessa leverantörer kan därför innebära en risk för störning som påverkar viktiga funktioner i samhället.

3. Avslutande reflektioner

De översiktliga studier som MSB nu låtit genomföra indikerar vissa trender och omständigheter som är av betydelse för det fortsatta arbetet med samhällets informationssäkerhet.

Kommunerna och annan offentlig verksamhet använder sig i allt högre grad både av kommersiella tjänster och av samverkan myndigheter emellan kring informationshantering. Gränserna mellan egen it och gemensamma tjänster blir allt mer uppluckrade och it-arkitekturen består i allt högre grad av en samverkan mellan olika aktörer. Det ställer nya krav på de enskilda aktörerna att säkerställa sin egen verksamhets behov och på att reglera ansvarsförhållandena i det allt mer komplexa beroendeförhållandena. En observation är att det i nuläget saknas överblick och tydlig reglering av helheten. Det saknas också genomarbetade utvärderingar av vilken typ av lösningar som på lång sikt bäst motsvarar offentliga organisationers behov av kostnadseffektivitet, kvalitet och säkerhet.

Möjligheten till ändamålsenlig styrning av de många relationer som idag finns inom informationshanteringsområdet bör utredas närmare. Styrning förutsätter beställarkompetens hos kunderna men sannolikt också ett ökat stöd för de många kunder som finns inom den offentliga sektorn, i form av vägledningar med mera. Trenden med ett kontinuerligt utökat samarbete mellan offentliga organisationer gör det lämpligt att närmare utreda hur dessa kan sluta fungerande överenskommelser med liknande funktion som kommersiella avtal. Det förutsätter också ett etablerat synsätt på roller och ansvar kring informationshanteringen och att det synsättet tillämpas i frågor som påverkar informationssäkerheten både för de enskilda aktörerna och i en gemensam lösning.

Denna analys har ett speciellt fokus på kommunernas situation. Uppenbarligen finns här ett antal förbättringsområden vilket de svarande kommunerna beskrivit, som till exempel behovet av stark beställarkompetens och möjligheten att strategiskt hålla ihop sin informationsförsörjning oavsett om den levereras av egna resurser eller utomstående. En mer grundläggande fråga är dock kommunernas riskmedvetande kring dessa frågor eftersom en realistisk uppfattning om de risker en organisation är utsatt för är förutsättningen för ett systematiskt säkerhetsarbete. Enkätsvaren som tagits fram tyder på att kommunerna generellt inte haft riskanalyser ur ett informationssäkerhetsperspektiv som en integrerad del i sina upphandlingar av it-relaterade tjänster. Samma förhållande förefaller gälla även i ett antal av de samarbeten kring informationshantering som drivs mellan kommuner. Att informationssäkerhet inte får en avgörande betydelse i utformningen av upphandlingsprocessen leder både till sämre avtal och till att kommunen inte tydliggör sitt eget ansvar för att lösningarna ska fungera på ett tillfredsställande sätt i normalläge och vid störningar. Ett tydligt tecken i denna riktning är de

enkätsvar som visar att kommunerna själva ofta upplever avtalen som otillfredsställande. Att så många av de svarande kommunerna saknar kontinuitetsplanering är en annan varningssignal.

Ett systematiskt informationssäkerhetsarbete ger metodstöd för att hantera upphandling av och samarbete kring stöd för informationshantering. Utifrån kommunernas ansvar för samhällsviktig verksamhet bör det ses som en ur samhällsperspektiv prioriterad fråga att ge ytterligare stöd för ett systematiskt informationssäkerhetsarbete. Kommunernas likartade uppdrag bör utnyttjas för att ta fram enhetliga stöd som kan leda fram till att informationssäkerhet blir en integrerad del i både outsourcing, molntjänster och samverkan med andra offentliga organisationer.

