Mina Meddelanden

- Risk- och Sårbarhetsanalys för anslutande kommuner

Kornhamnstorg 61
SE-111 27 Stockholm
Sweden

Telefon: +46 (0)8 791 92 00
Telefon: +46 (0)8 791 95 00

www.certezza.net

Inledande sammanfattning

I arbetet med att ta fram riktlinjer för hur kommuner kan går tillväga rent praktiskt för att ansluta sig mot tjänsten Mina Meddelanden, så har Sambruk, i samarbete med SKL, genomfört en risk- och sårbarhetsanalys. Risk- och sårbarhetsanalysen genomfördes i workshopform 5 juni 2014 med deltagare från kommunerna Norrköping och Linköping samt en representant från Skatteverket. Användningsfallet som analysen fokuserade på var en kommuns anslutning till tjänsten och socialtjänstens process för försörjningsstöd.

Resultatet av analysen visar att Skatteverkets tjänst Mina Meddelanden har en potential att bli en viktig pusselbit i kommuners digitalisering och e-förvaltning. Ur ett informationssäkerhetsperspektiv så finns det en del som anslutande kommuner måste tänka på och ta hänsyn till. Likaså måste tjänsten i sig fortsätta att utvecklas så att den till exempel stödjer dubbelriktat kommunikation med medborgarna så att ingen information faller mellan stolarna.

För anslutande kommuner, visar analysen att det är viktigt att ha kontroll på information och processer som är aktuella för att använda Mina Meddelanden. Informationsklassning och riskanalys är väsentligt för korrekt kravställning som garanterar en genomgående rätt informationssäkerhet.

Om digital meddelandehantering till medborgare ska få genomslag så är det viktigt att risken att medborgare upplever detta som krångligt och rörigt på grund av många olika kanaler hanteras. Kommuner måste vara tydliga med hur Mina Meddelanden används i förhållande till övriga e-tjänster, Mina sidor och eventuellt andra digitala kanaler.

Kunskaps- och kompetensbrist lyfts också fram i analysen som ett stort hot mot ett lyckat införande av digital meddelandehantering via tjänsten.

Innehåll

Risk- och sårbarhetsanalys för Mina Meddelanden 4

Grundläggande kriterier för informationssäkerhet 4

Att utföra en risk- och sårbarhetsanalys 4

Hantera riskerna 5

Identifierade risker under workshopen 6

Rekommendationer utifrån riskanalys 17

Risk- och sårbarhetsanalys för Mina Meddelanden

I arbetet med att öka den digital kommunikation med kommuninvånare så genomförs en översyn av hur kommuner kan ansluta sig till den digitala förmedlingstjänsten kallad Mina Meddelanden. Mina Meddelanden är en tjänst som tillhandahålls av Skatteverket. Tjänsten kan användas av kommuner för att digitalt förmedla information, beslut m.m. på ett säkert sätt till den enskilde, fysisk eller juridisk person.

I arbetet med att ta fram riktlinjer för hur kommuner kan går tillväga rent praktiskt för att ansluta sig mot tjänsten Mina Meddelanden, så har Sambruk, i samarbete med SKL, genomfört en risk- och sårbarhetsanalys. Risk- och sårbarhetsanalysen genomfördes i workshopform 5 juni 2014 med deltagare från kommunerna Norrköping och Linköping samt en representant från Skatteverket. Användningsfallet som analysen fokuserade på var en kommuns anslutning till tjänsten och socialtjänstens process för försörjningsstöd.

Grundläggande kriterier för informationssäkerhet

All information som hanteras, transporteras eller lagras i någon form måste skyddas mot oönskad förändring, påverkan eller insyn. Det ska inte vara möjligt för obehöriga att ta del av informationen men de användare som har rätt till informationen ska komma åt den efter behov och inom önskad tid. Det är också av vikt att kunna identifiera vem som har gjort vad med informationen och i datasystemen.

För att säkerställa detta bedömas informationstillgångar utifrån fyra följande egenskaper:

Riktighet:
Att information inte kan förändras vare sig av obehöriga, av misstag eller på grund av funktionsstörning. Informationen ska vara tillförlitlig, korrekt och fullständig.

Konfidentialitet:
Att innehållet i dokument, information och handlingar etc. inte görs tillgängliga eller avslöjas för obehöriga.

Tillgänglighet:
Att information och informationstillgångar kan utnyttjas efter behov, i förväntad utsträckning och inom önskad tid utifrån de krav som ställs på verksamheten.

Spårbarhet:
Att, där det finns behov av det, i efterhand entydigt kunna härleda specifika aktiviteter eller händelser till ett identifierat objekt. det ska gå att se vem som tagit del av informationen, vilka förändringar som har hänt och av vem dessa har utförts.

Att utföra en risk- och sårbarhetsanalys

Risk- och sårbarhetsanalysen syfte är att identifiera hot förknippade med förlust av konfidentialitet, riktighet, tillgänglighet och spårbarhet. Därefter bedöms de potentiella konsekvenserna som skulle kunna uppstå om hoten realiserades samt sannorlikheten för förekomster av de identifierade hoten. Utifrån detta fastställs sedan risknivåer för de identifierade hoten.

Själva arbetet arrangerades så att deltagarna fick sätta sig i grupper om fem och diskutera hot som varje gruppmedlem kunde identifiera utifrån den synvinkel han eller hon hade. Dessa hot antecknades och togs sedan upp i storforum där varje hot togs upp och samgrupperades med liknande hot som de andra grupperna identifierat. Hoten bedömdes sedan utefter sannolikhet att inträffa och vilken konsekvens som det skulle medföra om det inträffade. Bedömningen och den sammanvägda vikten av de uppskattade värdena resulterar i en rik, i enlighet med MSB:s[1] modell för risk- och sårbarhetsbedömning.

Hantera riskerna

De risker som identifieras i risk- och sårbarhetsanalysen ska hanteras. Detta görs genom att:

- Införa förebyggande åtgärder som minskar sannorlikheten till en acceptabel nivå.
- Acceptera riskerna om de inte strider mot lagstiftning eller kommunens regler.
- Undvika den aktivitet som orsakar att den identifierade risken blir verklighet.
- Införa reaktiva åtgärder för att minska konsekvenserna av risker, t.ex. genom försäkring och tydlig ansvarsfördelning med andra parter.

Inga åtgärder diskuterades eller presenterades vid workshopen för risk- och sårbarhetsanalysen. De åtgärder som är i detta dokument är åtgärder som bedöms vara relevanta utifrån erfarenhetsmässiga bedömningar som författarna till dokumentet gör.

[1] MSB – Myndigheten för Samhällsskydd och beredskap

Identifierade risker under workshopen

Hoten är nedan beskrivna utifrån den riskbedömning som den sittande församlingen kom fram till, med de bedömt högsta riskerna först.

ID	Beskrivning	Sannolikhet	Konsekvens	Risk
10	Verksamheten är inte förberedd att hantera supportfrågor från med-borgarna eller den egna personalen	Mycket hög	Hög	5

Mer detaljerad beskrivning

När en e-tjänst presenteras för invånarna i kommunen så förväntar invånarna att den kommunala verksamheten själv vet hur lösningen fungerar. Det kan vara allt från att kunna hjälpa till vid inloggning med hjälp av e-legitimation, att skriva ut dokument till att förklara hur svar på ett ärende kan lämnas in digitalt utan att för den skull skickas via det osäkra transportsättet e-post osv. Genom att erbjuda en e-tjänst så erbjuds också en möj-lighet för invånaren att utföra sitt ärende andra tider på dygnet än kontorstid.

För den egna personalen inom kommunen så blir delar av arbetssättet ändrat. Vissa processer kan behöva göras om för att anpassas till ett digitalt flöde istället för hantering av pappersbundna dokument. Systembrister i verksamhetssystemet kan komma att ut-nyttjas genom felaktig användning, genom misstag eller handlingar som inte var förut-sedda, vilket kan resultera i att skyddet för informationstillgången försvagas eller förbigås.

Förslag på åtgärder för att minska risken

- Göra ett noga planerat införande av att digitalt kommunicera med invånarna i den egna förvaltningen
- Genomföra noggranna tester på verksamhetssystemet och dess kringkompo-nenter
- Ta fram detaljerade anvisningar för personalen för att kunna leda invånarna genom e-tjänsten.
- Låta den egna personalen själva utföra handlingar i e-tjänsten i rollen som invånare för att lära känna tjänsten

ID	Beskrivning	Sannolikhet	Konsekvens	Risk
12	Uppföljning av loggar sker för sällan vilket medför att man inte upptäcker brister	Mycket hög	Hög	5

Mer detaljerad beskrivning

Loggposter sparas i system för att antingen i efterhand kunna avgöra vad som inträffat, eller i det fall det finns ett logganalysverktyg till hands, i realtid kunna utföra varningar eller dylikt så att system- eller verksamhetsansvariga ska kunna genomföra åtgärder. För att ha kontroll på digitaliserade processer är logghantering väsentlig. Risken är att dessa loggar inte övervakas, ger larm som ignoreras eller att loggarna inte används som underlag vid revisioner.

Förslag på åtgärder för att minska risken

- Kravställ på driftansvariga, intern organisation eller extern driftpartner, att logglösning finns på plats för alla ingående delar som stödjer processen.
- Kom överens och avtala om vad som är relevant att logga. Vilka händelser och aktiviteter är viktiga att följa och vad är viktigt att få en notifiering om i fall något går fel.
- Kravställ avseende granskningsfrekvens av loggar, vad som skall granskas av vem och hur granskning skall rapporteras.

ID	Beskrivning	Sannolikhet	Konsekvens	Risk
13	Oklart ansvar hos de olika parterna/ aktörerna/systemen för meddelandet sett ur ett CIA[2]-perspektiv	Mycket hög	Mycket hög	5

Mer detaljerad beskrivning

Vid digitalisering av verksamhetsprocesser i en kommun är det vanligt att flera olika leverantörer, system, aktörer och flera förvaltningar är inblandande. Det kan till exempel vara en leverantör som ansvarar för ett verksamhetssystem men IT-driften är outsourcad till en annan extern leverantör eller sköts av en intern driftsorganisation. Risken för att det finns otydligheter avseende ansvar och gränsdragningar är stor och kan orsaka incidenter samt vara ett stort problem när en incident inträffat[3].

[2] CIA – Confidentiality, Integrity and Availability; engelska för Konfidentialitet, Riktighet och Tillgänglighet.
[3] Alla-skyller-på-alla-syndromet

Förslag på åtgärder för att minska risken

- Kartlägg och dokumentera processer, informationsmängder, informationsflödet samt vilka IT-komponenter som är inblandade.
- Gå igenom vilka aktörer som är involverade i ovan och säkerställ att ansvar, avtal och överenskommelser är heltäckande och korrekta.
- Håll antalet parter nere och se till att någon tar (eller får) ett helhetsansvar.

ID	Beskrivning	Sannolikhet	Konsekvens	Risk
M6	Dålig säkerhet pga. dålig kravställning	Hög	Mycket hög	5

Mer detaljerad beskrivning

Kraven avseende informationssäkerhet måste vara konsekventa över alla komponenter som omfattas och stödjer verksamhetsprocessen. En anledning till dålig kravställning kan vara att kommunen har befintliga komponenter med befintlig kravställning som inte är på rätt nivå. En annan anledning kan vara att det saknas rutin för informationsklassning och riskanalys/riskhantering vilket gör att kravställningen blir felaktig.

Förslag på åtgärder för att minska risken

- Kartlägg och dokumentera processer, informationsmängder, informationsflödet samt vilka IT-komponenter som är inblandade.
- Klassa den hanterade informationen utifrån verksamhetens krav och med hänsyn till eventuella lagar, förordningar och avtal.
- Gör en riskanalys och utifrån riskhanteringen fånga upp vilka skyddsåtgärder som ska finnas på plats för en pålitlig, kvalitativ verksamhet som efterlever krav utifrån lagar, förordningar och avtal.
- Säkerställ att kravställningen på alla ingående komponenter lever upp till informationssäkerhetskraven.

ID	Beskrivning	Sannolikhet	Konsekvens	Risk
8	System som integreras klarar inte av skyddsklassad information	Hög	Hög	4

Mer detaljerad beskrivning

Kommuner har oftast en komplex IT-miljö med ett arv och många olika komponenter. Exempel på olika komponenter är verksamhetssystem, nätverkstjänster, integrationslösningar, flödesmotorer med mer. För att hantera skyddsklassad information så kommer det att ställas krav på olika skyddsåtgärder eller skyddskontroller. Det finns en risk för att dessa skyddsåtgärder eller skyddskontroller inte kan införas på alla system- eller informationsobjekt på grund av ett bristande stöd för detta.

Förslag på åtgärder för att minska risken

- Kartlägg och dokumentera processer, informationsmängder, informationsflödet samt vilka IT-komponenter som är inblandade.
- Klassa den hanterade informationen utifrån verksamhetens krav och med hänsyn till eventuella lagar, förordningar och avtal.
- Gör en riskanalys och utifrån riskhanteringen fånga upp vilka skyddsåtgärder som ska finnas på plats för en pålitlig, kvalitativ verksamhet som efterlever krav utifrån lagar, förordningar och avtal.
- Säkerställ att kravställningen på alla ingående komponenter realiseras i praktiken.
- För eventuella komponenter som inte har stöd för detta, ta fram en handlings-plan för hur detta ska lösas.

ID	Beskrivning	Sannolikhet	Konsekvens	Risk
9	Bristande integration med privata utförare, t.ex. beslut om förskoleplats hos privat utförare	Mycket hög	Låg	4

Mer detaljerad beskrivning

Idag kan inte privata utförare ansluta sig till tjänsten Mina Meddelanden. Konsekvensen av detta blir att dialogen med medborgare kan vara annorlunda från kommun till kommun men också mellan olika förvaltningar i samma kommun beroende på om privata utförare är inblandade.

Förslag på åtgärder för att minska risken

- Informera medborgare om problematiken.
- Informera, diskutera och kom överens med privata utförare om lösning.
- Dokumentera hur förmedling av meddelanden skall gå till när privata utförare är inblandade.
- Näringsdepartementets uppdatering/förändring av Förordning (2003:770) om statliga myndigheters elektroniska informationsutbyte kommer förhoppningsvis göra detta möjligt på sikt.

ID	Beskrivning	Sannolikhet	Konsekvens	Risk
11	Informationen klassas olika eller för lågt	Hög	Hög	4

Mer detaljerad beskrivning

Att informationsklassa olika kan medföra att det ställs olika krav på skyddsåtgärder och skyddskontroller vilket kan resultera i olika användarupplevelser av tjänsterna. Den stora risken är att informationen klassas för lågt av någon aktör för att minska kostnaderna eller undvika något som kan vara ett påstått onödigt hinder. Konsekvensen kan då bli att informationen inte får tillräckligt skydd.

Förslag på åtgärder för att minska risken

- Via dialog och samarbete kommuner emellan kan likvärdiga nivåer av klassning uppnås.
- Per avtal förvisa sig om att information som passerar organisationsgränser behåller sin skyddsnivå.

ID	Beskrivning	Sannolikhet	Konsekvens	Risk
15	Dold kostnad vid transition/övergång mellan leverantörer vid förnyad upphandling	Hög	Hög	4

Mer detaljerad beskrivning

I och med digitalisering och kommuners anslutning till tjänsten Mina Meddelanden så kan en del kommuner välja att upphandla vissa delar av externa leverantörer[4]. När eller om en kommun anlitar en extern part för leverans av vissa tjänster finns alltid en risk för extra kostnader vid leverantörsbyte. Det vi syftar på är eventuella kostnader för att avsluta tjänst och flytta över information från en leverantör för att starta upp motsvarande tjänst hos en annan leverantör.

Förslag på åtgärder för att minska risken

- Vid upphandling av tjänster som levereras externt ta alltid med "exit"-lösningar i upphandlingskrav och avtal. Hur skall leverantör vara behjälplig vid avslutande av tjänst? Vad ska leverantören ansvara för? Hanteras kostnaden för avslutsaktiviteter inom befintligt avtal eller kan leverantören att ta ut en kostnad för detta?

[4] Detta faktum är inte endast förknippat med kommuners anslutning till Mina Meddelanden utan är en vardag för många kommuner redan idag.

ID	Beskrivning	Sannolikhet	Konsekvens	Risk
17	Den säkra integrationen blir leverantörsstyrd och kan ge inlåsningseffekt	Hög	Hög	4

Mer detaljerad beskrivning

En del leverantörer kan komma att erbjuda kommuner egna lösningar gällande integration, kanalväxel och förmedlingstjänst som är specifika för det system som de levererar. Risken finns att dessa leverantörsspecifika lösningar är starkt knutna och anpassade till leverantörens system. Om kommunen vill bredda sitt användande av Mina Meddelanden till att omfatta information från andra verksamhetssystem så är det inte säkert att det är möjligt tillsammans med gjorda investeringar. Kommunen kan bli tvungen att göra nya integrationer, kanalväxel och förmedlingstjänst. Komplexiteten och kostnader i kommunens IT-miljö ökar med flera leverantörsspecifika lösningar.

Förslag på åtgärder för att minska risken

- Även om kommunen börjar i litet format gällande anslutning och användande av Mina Meddelanden så säkerställ att det som görs bygger på standarder och kan återanvändas.
- Om kommunen väljer decentraliserade lösningar för varje specifikt verksamhets-system så skall det vara ett medvetet val som man förstår och accepterar konsekvenserna av.

ID	Beskrivning	Sannolikhet	Konsekvens	Risk
18	Försenad utveckling av VH-stöd pga. beroende till andra kommuner/kunder till leverantören	Hög	Hög	4

Mer detaljerad beskrivning

Många kommuner har samma verksamhetssystem och leverantörer inom många områden. Om en leverantör leverarar samma system till fler kommuner kan specifika önskemål från enskild kommun försenas eller försvåras på grund av beroenden till andra kommuners anpassningar.

Förslag på åtgärder för att minska risken

- Sammarbeta med andra kommuner med samma leverantör och verksamhets-system. I den mån det är möjligt samordna processer och arbetssätt.
- Se till att, tillsammans med andra kommuner med samma leverantör och verksamhetssystem, bli en enad stark kund.

ID	Beskrivning	Sannolikhet	Konsekvens	Risk
1	Minskad användning av tjänsten pga. olika implementationer, design; stuprörstänk; förvirrande med kommunens egna "mina ärenden".	Hög	Låg	3

Mer detaljerad beskrivning

Om digitaliseringen av verksamhetsprocesser och användningen av Mina Meddelanden blir för krånglig eller förvirrande för medborgarna är risken att de inte använder tjänsten. En stor konsekvens av detta skulle kunna bli att digitalisering och e-förvaltning avstannar lite på grund av lågt användande. Trots att detta är allvarligt så är konsekvensen för denna risk satt till låg. Anledningen är insikten att det troligen ändå kommer behöva ha en pappershantering en lång tid framöver för vissa kategorier av medborgare. Dock bör man se allvarligt på om kommunen riskerar bristande förtroende hos medborgare på grund av kvalitetsbrister.

Förslag på åtgärder för att minska risken

- Ta fram en kommunikationsplan och strategi för e-tjänster och medborgare.
- Samordna initiativ för att kommunicera digitalt med medborgare inom kommunens alla olika verksamheter.
- Ha ett samarbete och erfarenhetsutbyte med andra kommuner och SKL för mer enhetliga lösningar avseende digital kommunikation mot medborgare i Sverige.

ID	Beskrivning	Sannolikhet	Konsekvens	Risk
3	Att det inte går att digitalt signera beslutsunderlag.	Mycket hög	Försumbar	3

Mer detaljerad beskrivning

Vissa beslut och beslutsunderlag måste signeras. Idag är det väldigt få kommuner som har infrastruktur, rutiner och systemstöd för att göra detta digitalt. Anledningen till att konsekvensen är satt till försumbar är att det finns fortfarande en hel del som kan kommuniceras till medborgarna via Mina Meddelanden där inga signeringskrav föreligger. Parallellt kan kommunen börja se över lösningar och rutiner för digitalsignering.

Förslag på åtgärder för att minska risken

- Prioritera införande av Mina Meddelanden för processer där digitala signaturer inte är ett krav.
- Genomför en förstudie, ta fram strategi och handlingsplan för införande av digitala signaturer för kommunen.

ID	Beskrivning	Sannolikhet	Konsekvens	Risk
5	Verksamhetssystemet kan/vill inte anpassas till Mina Meddelanden eller att de inte kan hantera fellägen (exceptions)	Låg	Mycket hög	3

Mer detaljerad beskrivning

Det finns en liten risk att vissa verksamhetssystem inte kan anpassas till att fungera på ett bra sätt ihop med Mina Meddelanden. T.ex. kan det bli problem att hantera särfall och att reagera på korrekt sätt när fel (exceptions) uppstår.

Förslag på åtgärder för att minska risken

- Dokumentera och säkerställ att ingående komponenters förmågor uppfyller kraven för anpassning till Mina Meddelanden

ID	Beskrivning	Sannolikhet	Konsekvens	Risk
19	Minskad möjlighet till revision/ uppföljning/logguppföljning	Låg	Mycket hög	3

Mer detaljerad beskrivning

Om en kommun väljer en extern leverantör av vissa av de ingående komponenterna i lösningen så finns en risk för minskad kontroll och uppföljningsmöjligheter. Det här gäller för alla upphandlade tjänster som levereras externt som till exempel molntjänster.

Förslag på åtgärder för att minska risken

- Kravställ i upphandling och avtal gällande rätt att göra revision, ta del av logginformation, incidenthantering och rapportering.

ID	Beskrivning	Sannolikhet	Konsekvens	Risk
21	Sårbarheter hos andra kunder till leverantören "spiller över" till andra kunder.	Mycket låg	Hög	3

Mer detaljerad beskrivning

Om en kommun väljer en extern leverantör av vissa av de ingående komponenterna i lösningen så kan hot och sårbarheter hos leverantören eller leverantörens andra kunder påverka kommunen.

Förslag på åtgärder för att minska risken

- Om det föreligger höga krav avseende konfidentialitet, integritet, tillgänglighet och spårbarhet kravställ i upphandling och avtal gällande kommunens separation mot leverantörens och andra kunders miljöer.

ID	Beskrivning	Sannolikhet	Konsekvens	Risk
2	Missade tidsfrister på grund av att digitala meddelande inte läses i tid eller att användaren inte går in i Mina Meddelanden.	Låg	Låg	2

Mer detaljerad beskrivning

Att tidsfrister, till exempel överklagan, skulle missas på grund av att medborgaren inte kontrollerar sin brevlåda och därmed missar information anses relativt osannorlikt. Har en person anmält sig för digitalt informationsutbyte så finns troligtvis engagemang och kunskap. För övriga finns under överskådlig tid fortfarande informationsutbyte via papper. För kommuners digitalisering och effektivisering bör man dock få över så många personer som möjligt så snabbt som möjligt till digitalt informationsutbyte.

I övrigt finns en problematik med tidsfrister och möjligheten att säkerställa att en person faktiskt läst och tagit till sig information. Med Mina Meddelanden har kommunen endast möjlighet att säkerställa när information levererats till personens brevlåda.

Förslag på åtgärder för att minska risken

- Kommuner kan komplettera möjligheten med leveransbekräftelser från Mina Meddelanden med till exempel en länk i meddelandet till en bekräftelselösning vid sidan om.

ID	Beskrivning	Sannolikhet	Konsekvens	Risk
7	Digitalt inkommen handling prioriteras i handläggningen före andra aktiviteter (uppsökande, telefontid mm)	Låg	Låg	2

Mer detaljerad beskrivning

Inkomna handlingar måste hanteras inom viss tid. Även om en digital hantering förväntas att effektivisera så finns en liten risk att all fokus för personalresurser blir just kring denna hantering. Konsekvensen kan bli att andra uppsökandeaktiviteter blir nedprioriterade.

Förslag på åtgärder för att minska risken

- Planera utnyttjande av personalresurser och strukturera arbetsinstruktioner och rutiner så att även uppsökande aktiviteter utförs.

ID	Beskrivning	Sannolikhet	Konsekvens	Risk
22	Överbelastningsattacker (antingen hos leverantören eller hos kommunen) orsakar stopp i tjänsten.	Hög	Mycket låg	2

Mer detaljerad beskrivning

Överbelastningsattacker sker regelbundet, dock så är tjänsten Mina Meddelanden inte tidskritisk. Överbelastningsattacker sker under begränsad tid och tillgängligheten berörs endast under själva attacken.

Förslag på åtgärder för att minska risken

- Ha rutiner för att informera användare om eventuella tillgänglighetsproblem.

ID	Beskrivning	Sannolikhet	Konsekvens	Risk
4	Användaren har inte tillgång till dator, skrivare, scanner, eID.	Mycket låg	Mycket låg	1

Mer detaljerad beskrivning

Vissa besked via Mina Meddelanden kan det finnas behov av att skrivas ut. Det kan handla om biståndsbeslut som behöver bifogas i annan kommunikation (t.ex. med hyresvärdar) eller underlag (kvitton mm) som behöver bifogas som beslutsunderlag. Att skriva ut något som klassas känsligt på offentliga skrivare (t.ex. bibliotek) kan vara något som bromsar användandet hos invånarna.

Förslag på åtgärder för att minska risken

- Vid anmälan för digitalt informationsutbyte, var tydliga med vad som gäller och att det finns pappersalternativ
- De som anmält sig för digitalt informationsutbyte har troligtvis den utrustning som behövs. För de som inte har utrustning eller förutsättningar så finns fortfarande möjlighet till pappersmässigt informationsutbyte.

ID	Beskrivning	Sannolikhet	Konsekvens	Risk
6	Meddelanden adresserade till hushållet (inte den enskilde) ska läsas av båda/alla	Mycket låg	Låg	1

Mer detaljerad beskrivning

Meddelanden adresserade till hushållet går via lösningen (digitalt eller pappermässigt) som respektive medlem i hushållet har anmält sig till. Det kan bli problem att få det adresserat och kvitterat av båda i hushållet. Tvärtom när meddelanden som inte är avsedda för hushållet sprids till flera medlemmar i hushållet.

Förslag på åtgärder för att minska risken

- Var tydliga med vad som gäller för att anmäla sig för digitalt informationsutbyte och att det finns pappersalternativ

ID	Beskrivning	Sannolikhet	Konsekvens	Risk
20	Förändringar i legala krav utanför Sveriges gränser/jurisdiktion påverkar informationssäkerheten i leveransen	Mycket låg	Låg	1

Mer detaljerad beskrivning

Om delar eller komponenter i IT-miljön upphandlas externt och dessa hamnar utanför Sveriges gränser/jurisdiktion kan legala krav ställa till problem. Även om det är OK vid upphandling och avtalsskrivande så kan förändringar över tid ställa till problem.

Förslag på åtgärder för att minska risken

- Detta är en generell risk för alla externt upphandlade tjänster och måste hanteras i kravställning inför upphandlingen och vid avtalsskrivandet.

ID	Beskrivning	Sannolikhet	Konsekvens	Risk
23	Haveri hos tjänsteleverantör	Låg	Mycket låg	1

Mer detaljerad beskrivning

Om delar eller komponenter i IT-miljön upphandlas externt och finns hos en tjänste-leverantör så finns en risk att haveri hos leverantören påverkar leveransen. Mina Med-delande tjänsten i sig är inte tidskritisk. Om det blir problem med digital distribution av information kan kommunen använda pappersvägen.

Förslag på åtgärder för att minska risken

- Som en del i kontinuitetsplanering för verksamheten ta fram reservrutiner som ska användas vid tjänstebortfall.

Rekommendationer utifrån riskanalys

Att ansluta till tjänsten Mina Meddelanden ger kommuner ytterligare en pusselbit till e-förvaltning och digitalisering av verksamhetsprocesser. Denna riskanalys visar dock att det är en del som kommuner bör göra och fundera över innan anslutningen. Ur ett informationssäkerhetsperspektiv är det viktigaste att identifiera processer, information och IT-komponenter för att identifiera lagkrav, informationsklassa och göra riskanalys. Utifrån detta har man en bra grund för en korrekt kravställning avseende informationssäkerhet för anslutning och användning av tjänsten.

En viktig frågeställning som kom upp under riskanalysen gällde digitala signaturer. Om kommunen ska digitalisera sina verksamhetsprocesser finns det då saker som måste signeras digitalt för distribution till medborgare? Om det gör det så måste kommuner ha en strategi för hur en sådan lösning kommer på plats i forma av infrastruktur och anpassade verksamhetssystem med mer.

Utöver informationssäkerhetsperspektivet så identifierades ett hot mot en bredd användning av Mina Meddelanden i form av ett det blir för otydligt och trassligt för medborgarna. Här måste kommuner ha en tydlig strategi för kommunikationen mot medborgarna och hur Mina Meddelanden skall förhålla sig mot övriga e-tjänster och eventuella Mina Sidor.

Under riskanalysen identifierades också behovet av kunskap och kompetens som till en viss del även har en påverkan på informationssäkerheten. Fokus i diskussionerna under analysen var dock att kunna hjälpa och stödja medborgarna i användandet.

För framtiden och ett breddanvändande i kommunerna av Mina Meddelanden så måste själva tjänsten utvecklas så att dubbelriktad kommunikation med medborgarna möjliggörs digitalt.

Carl Önne Peter Lidholm
Informationssäkerhetskonsulter

Certezza AB