

**Hur hanteras web services inom
fastighetsautomation?**

(HS-IDA-EA-03-602)

Mattias Elmqvist (a00matel@ida.his.se)

*Institutionen för datavetenskap
Högskolan i Skövde, Box 408
S-54128 Skövde, SWEDEN*

Examensarbete inom informationssystemsutveckling under
vårterminen 2003.

Handledare: Jesper Holgersson

Hur hanteras web services inom fastighetsautomation?

Examensrapport inlämnad av Mattias Elmqvist till Högskolan i Skövde, för Kandidatexamen (B.Sc.) vid Institutionen för Datavetenskap.

2003-06-08

Härmed intygas att allt material i denna rapport, vilket inte är mitt eget, har blivit tydligt identifierat och att inget material är inkluderat som tidigare använts för erhållande av annan examen.

Signerat: _____

Hur hanteras web services inom fastighetsautomation?

Mattias Elmqvist (a00matel@ida.his.se)

Sammanfattning

Detta examensarbete är en studie kring hur säkerhetsaspekter för web services hanteras inom fastighetsautomationsbranschen utifrån W3C:s riktlinjer. W3C är en organisation som godkänner och administrera nya Internetstandarder. Dessa riktlinjer omfattar säkerhet inom web services, men kan även fungera som en mall för både utveckling och användning. Dessa riktlinjer låg till grund för de intervjufrågor som skapades för undersökningen. Undersökningen genomfördes på sex organisationer med en intervjustudie, på grund av arbetets begränsningar användes telefonintervjuer.

Studien syftar till att ge en närmare inblick i säkerhetstänkandet samt de för- och nackdelar som kan associeras till web services, samt utvecklingen av tekniken inom fastighetsautomationsbranschen.

Studien visar att synen på säkerheten och tillämpningarna skilde sig mellan organisationerna och att riktlinjerna inte direkt kunde uppfyllas. Orsaken till detta är skillnaderna mellan organisationerna. Det framkom att det fanns stora potentiella fördelar med web services och organisationerna tror att utvecklingen av web services inom branschen kommer att öka.

Nyckelord: Web services, Organisation, Internet, Fastighetsautomation, Säkerhet

Innehållsförteckning

1	Introduktion	1
2	Web services	3
2.1	Bakgrund till web services	3
2.2	Definition av web services	4
2.3	Exempel på en web services	5
2.4	Standarder inom web services	7
2.4.1	XML (Extensible Markup Language)	7
2.4.2	SOAP (Simple Object Access Protocol).....	8
2.4.3	WSDL (Web Service Description Language).....	8
2.4.4	UDDI (Universal Description, Discovery and Integration).....	8
2.5	Fördelar och nackdelar med web services.....	9
2.5.1	Fördelar	9
2.5.2	Nackdelar	10
2.6	Säkerhet inom web services	10
2.7	Fastighetsautomation	13
3	Problembeskrivning.....	14
3.1	Problemprecisering	15
3.2	Det vetenskapliga bidraget	15
3.3	Avgränsning av problemet	15
3.4	Förväntat resultat	16
4	Metod.....	17
4.1	Tänkbara metoder	17
4.1.1	Intervju.....	17
4.1.2	Enkätundersökning	17
4.2	Vald metod	18
4.3	Metodsteg	18
4.3.1	Intervjuns upplägg	18
4.3.2	Intervjuns utförande.....	19
4.3.3	Undersökningsgrupp.....	19
5	Genomförande.....	20
5.1	Processen	20
5.1.1	Intervjuerna	21

5.2 Presentation av respondenterna	21
5.2.1 Organisation A	21
5.2.2 Organisation B.....	21
5.2.3 Organisation C.....	21
5.2.4 Organisation D	22
5.2.5 Organisation E.....	22
5.2.6 Organisation F.....	22
6 Presentation av intervjusvar	24
6.1 Del 2:.....	24
6.2 Del 3:.....	25
7 Analys	28
7.1 Kategori.....	28
7.2 Analys av de utvalda kategorierna.....	29
7.2.1 Utveckling.....	29
7.2.2 Fördelar/nackdelar med web services.....	30
7.2.3 Tillgängligheten.....	31
7.2.4 Information.....	31
7.2.5 Externa hot	32
7.2.6 Interna hot	33
7.3 Sammankoppling av kategorier till W3C:s riktlinjer.....	34
7.4 Sammanfattande analys av intervjuundersökningen.....	35
7.5 Sammanfattande analys av undersökningen.....	35
8 Resultat och reflektion.....	38
8.1 Hur tillämpas W3C riktlinjer?	38
8.2 För- och nackdelar med web services?	38
8.3 Utveckling av web services inom fastighetsautomation?	39
8.4 Hur hanteras web services inom fastighetsautomation?	39
8.5 Vad betyder resultatet	40
8.6 Reflektioner	40
8.7 Framtida studier	41
Referenser	43
Bilaga 1 Intervjufrågor	
Bilaga 2 Intervjusvar	

1 Introduktion

Detta examensarbete kommer att fokusera på begreppet web services. Eftersom det inte existerar någon bra svensk definition kommer detta begrepp även att användas i den här rapporten. För att förtydliga vad web services är kommer en förklaring att redovisas.

Enligt Pagina (2003) kan web service sammanfattningsvis förklaras som en ny möjlighet att kommunicera mellan flera aktörer genom att samverka mellan olika funktioner och tjänster inom ett system blir tillgängliga utanför systemet till andra datorer och nätverk.

Begreppet web service kan härledas till de svenska begreppen webb och service och kan då förklaras som en ny aktivitet eller åtgärd som kan utföras över Internet genom att olika tjänster bli tillgängliga utanför det egna systemet.

Utvecklingen av web services kan härledas till de förändringar som Internet har genomgått sedan dess uppkomst. Ryman (2000) påpekar att det har skett tre förändringar sedan den *första fasen* som kallades *dokumentwebben*. Denna använde statiska sidor, och möjliggjorde att sprida och marknadsföra sig över större område. *Andra fasen, applikationswebben*, associeras med dynamiska sidor följde av att organisationer ville förbättra kommunikationen med sina partner. Den sista övergången till *tjänstewebben* var tack vare utvecklingen av Internetteknologin som möjliggjorde att organisationer kunde flytta sina huvudoperationer till webben för att nå öka automatisering, snabbare affärsprocesser och global tillgänglighet. Några av de standarder som möjliggjorde detta var bland annat kommunikationsspråket Simple Object Access Protocol (SOAP) och dokument som var skrivna i Extensible Markup Language (XML). Grundstommen i tjänstewebben är web services, dessa kan bestå av en eller flera funktioner som kan aktiveras via Internet. Andra standarder som förknippas är även Web Service Description Language (WSDL) och Universal Description, Discovery, and Intergration (UDDI) dessa används, enligt Eriksson (2002), främst när en organisation söker andra web services som kan implementeras över Internet. WSDL beskriver tjänsten och lagras i en UDDI katalog som är ett sökbart register. Detta underlättar för organisationer att lokalisera tjänsten samt att få information om dess uppbyggnad.

En nackdel som kan associeras till web services är att det inte existerar någon säkerhetsstandard, utan det är upp till organisationerna att implementera någon av de olika säkerhetstillämpningar som finns (Eriksson, 2002). Enligt Hondo, Nagaratnam och Nadalin (2002) kan en organisation öka förståelsen för de risker som kan existera i en organisation, detta kan uppnås om de kan ha en säkerhetsmodell över sina web services. För att realisera detta behöver denna modell illustrera dataflödet genom applikationen och nätverket för att kunna möta de säkerhetskrav som organisationen har satt upp. Organisationen W3C har tagit fram sex omfattande riktlinjer som behandlar säkerheten inom web services. Dessa riktlinjer kan även fungera som en mall för både utveckling och användning av web services samt att dessa kan öka säkerhetstänkandet hos organisationer (Gopalakrishnan och Rajesh, 2003). Eftersom en organisation kan välja att använda web services bara inom de interna systemen eller över Internet kan detta påverka valet av säkerhetstillämpningar för att skydda organisationen. De organisationer som ska undersökas i detta arbete är verksamma inom fastighetsautomationsbranschen där huvudaktiviteten utgörs av styr och reglerteknik. Med web services kan organisationer inom

1 Introduktion

fastighetsautomationsbranschen flytta flera av sina huvudoperationer till webben för att nå ökad automatisering, snabbare affärsprocesser och global tillgänglighet (Tsalgatidou och Pilioura, 2002). I branschen har stora förändringar skett de senaste åren vilket har påverkat denna som helhet mycket tack vare den utvecklade IT-tekniken. Undersökningen som ska genomföras kommer att utgå ifrån W3C:s riktlinjer för att undersöka de eventuella säkerhetstillämpningar som branschen har använt sig av för att skydda sina tjänster. Undersökningen kommer även att försöka definiera de för- och nackdelar som kan associeras till denna teknik samt att försöka klargöra huruvida utvecklingen av denna teknik ser ut inom fastighetsautomationsbranschen. Dessa delpunkter kommer sedan att användas för att besvara rapportens problemprecisering som är *Hur hanteras web services inom fastighetsautomation*.

Undersökningen genomfördes i en intervjustudie där sex organisationer deltog, på grund av de begränsningar som kan relateras till detta arbete som främst omfattar rapportens omfattning och den avsatta tiden användes telefonintervjuer för att genomföra undersökningen. Främsta orsaken till varför intervjuer användes för undersökningen är för att denna metod anses vara den bästa lämpade. Några av de positiva aspekter som kan relateras till användningen av metoden är bland annat lättare att klargöra frågorna samt att den skapar en bättre relation till respondenten på grund av att en del frågor kunde beröra känslig information.

Studien visade att följande aspekter kunde härledas för att besvara rapportens problemprecisering *Hur hanteras web services inom fastighetsautomation*. Dessa aspekter kan sammanfattas enligt följande:

- Web services inom fastighetsautomationsbranschen kan inte direkt sammankopplas till de riktlinjer som W3C har tagit fram som berör säkerheten.
- Det råder ingen tvekan om att utvecklingen av web services inom branschen kommer att öka de närmaste åren och att utvecklingen associeras främst till fördelar.
- Synen på de för- och nackdelar som kan relateras till web services inom branschen är övervägande fördelar.
- Samtliga delfrågor existerar det aspekter som lyfter fram behovet av en standardiserad säkerhet.

Rapporten kommer att läggas upp genom att först beskriva bakgrunden till arbetet genom att förklara web services, säkerheten samt fastighetsautomation. Därefter kommer problemet att presenteras samt motivering till vald metod. Sedan kommer rapportens genomförande och analys att beskrivas innan rapporten avslutas med undersökningens resultat och reflektion av rapporten.

2 Web services

Detta kapitel kommer att beskriva bakgrunden till web services genom att ge en historisk bild över utvecklingen av de olika faktorer som har bidragit till uppkomsten av web services. För att förtydliga web services kommer några definitioner att tas upp samt ett exempel på hur en web service kan fungera. De vanligaste standarderna som relateras till web services samt några potentiella för- respektive nackdelar, kommer att beskrivas innan kapitlet avslutas med ett stycke om säkerheten inom och omkring web services.

2.1 Bakgrund till web services

Internet har genomgått flera olika faser av förändringar sedan dess uppkomst. I den *första fasen*, som även kallas *dokumentwebben*, användes bara statiska dokument som var skrivna i Hyper Text Markup Language (HTML). För att kunna skicka dokumenten transporterades de över Hyper Text Transport Protocoll (HTTP) och för att kunna visa det skickade dokumentet användes en webbläsare som tolkade HTML-koden. Tanken bakom dokumentwebben (eng. Document Web) var att underlätta arbetet för forskare att kunna sprida och ta del av information elektroniskt. Många företag såg denna teknik som en möjlighet att kunna sprida information och marknadsföra sig över större områden (Ryman, 2000).

Enligt Mohan (2002) har Internets utveckling inte bara handlat om ökad informationsspridning för företag utan även om att förbättra samarbetet med kunder, leverantörer och distributörer. Ryman (2000) anser att detta ledde fram till den *andra fasen* i utvecklingen av Internet: *applikationswebben* (eng. Application Web). Applikationswebben gjorde det möjligt för företag att göra transaktioner med sina kunder som tidigare inte hade varit möjlig i samma utsträckning. En bidragande orsak var utvecklingen från statiska dokument till dynamiska genererande HTML-dokument via affärslogiken på webbservern. Några av de tekniker som möjliggjorde detta var Active Server Pages (ASP), Common Gateway Interface (CGI) och Java Server Pages (JSP). Även utvecklingen av webbserver utvecklades till distribuerade webbserverar för att bättre kunna hantera transaktionsbelastning.

Enligt Tsalgatidou och Pilioura (2002) har den växande Internet-teknologin gjort det möjligt för företag att göra affärer på många nya sätt. Många företag har därför valt att flytta sina huvudoperationer till webben för att nå ökad automatisering, snabbare affärsprocesser och global tillgänglighet. Enligt Ryman (2000) räckte inte *applikations- och dokumentwebben* till för att uppnå detta och därför utvecklades *tjänstewebben* (eng. Service Web), som fortfarande håller på att utvecklas. För att kunna realisera detta användes kommunikationsspråket Simple Object Access Protocol (SOAP) mellan de olika serverna och dokumenten som skickades var skrivna i Extensible Markup Language (XML).

Grundstommen av tjänstewebben är olika web services eller även kallade serverbaserade tjänster via Internet. Dessa web services består ofta av en eller flera funktioner som kan aktiveras via Internet. För att en organisation ska kunna använda tjänsten är organisationen tvungen att veta hur tjänsten är uppbyggd. Informationen som finns att tillgå för organisationen är beskriven av Web Service Description Language (WSDL) dokument. För att företag lättare ska kunna lokalisera olika web

services finns dessa i ett sökbart register som kallas Universal Description, Discovery, and Intergration (UDDI) (Ryman, 2000). Enligt Eriksson (2002) existerar och används främst WSDL och UDDI när en organisation söker web services som kan implementeras över Internet, där WSDL är en beskrivning av tjänsten som lagras i en UDDI katalog som består av sökbara register.

Standarderna XML, SOAP, WSDL och UDDI kommer att beskrivas mer i detalj i avsnitten 2.4.1 till och med 2.4.4. Enligt Eriksson (2002) existerar det många olika plattformar och utvecklingsverktyg som kan användas av organisationer för att skapa sina web services. Några exempel är Microsoft .Net och IBM J2EE.

2.2 Definition av web services

Det finns ett flertal olika definitioner på vad web services är och vad det har för betydelse för de parter som tillämpar detta kommunikationssätt. För att ge en klarare bild över vad web services är kommer begreppen web och service först att definieras separat, för att sedan följas av några olika definitioner på begreppet web services.

Enligt Pagina (2003) är webb en förkortning på World Wide Web som kan ses som ett söksystem för Internet. Webben baseras på länkar som använder Internet som överföringsmedium för att kunna sprida information över Internet.

Enligt Nationalencyklopedin (1995) kan service förklaras som en aktivitet eller åtgärd av någon typ som utförs i syfte att utföra en handling.

Dessa två begrepp bildar tillsammans web services. Från ovanstående förklaringar skulle därför följande slutsats kunna dras: att web service är en typ av aktivitet eller funktion som kan användas över Internet.

Enligt Leymann (2001) kan en grov definition av web services vara;

“A web services is any piece of code that can be interacted with based on internet technology” (Leymann, 2001, s. 1).

Av definitionen som presenterades av Leymann skulle en översättning kunna vara att web services är en bit programmerad kod som kan påverkas av Internet-teknologi för olika ändamål.

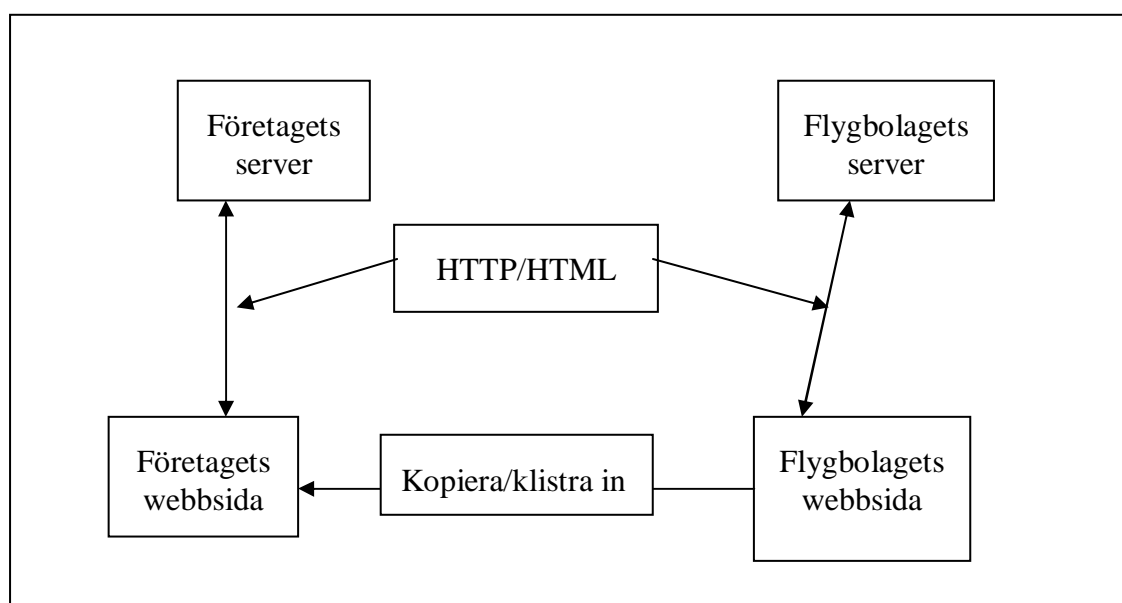
Enligt Pagina (2003) kan web service sammanfattningsvis förklaras som en ny möjlighet att kommunicera mellan flera aktörer genom att samverka mellan olika funktioner och tjänster inom ett system blir tillgänglig utanför systemet till andra datorer och nätverk. Web services har utvecklats genom ett flertal olika standarder. Tanken bakom web services är inte ny utan har uppkommit genom sammanslagning av de utnyttjande standarderna.

Från de ovanstående slutsatserna av begreppen web och service samt definitionerna av web service skulle därför följande slutsats kunna dras att web services är en ny typ av kommunikation. Detta gör det möjligt för organisationer att ha funktioner och tjänster tillgängliga utanför det egna systemet till andra datorer och nätverk. Dessa tjänster och funktioner kan påverkas av Internet-teknologi vilket resulterar i att dessa kan användas över Internet. Även om förklaringen av Pagina är generell anses denna i

detta arbete vara den bästa eftersom det finns en mängd olika konstruktionssätt och tillämpningar som en organisation kan använda sig av för att realisera web services.

2.3 Exempel på en web services

För att på ett enkelt sätt som möjligt förklara hur web services kan tillämpas inom en organisation och de fördelar som organisationen kan vinna kommer en skillnad mellan applikationswebben och web services att göras. Applikationswebben kommer att förklaras med ett exempel, sedan kommer web services att förklaras utifrån detta. Första exemplet visar hur en flygbokning på en resebyrås hemsida kan gå till på applikationswebben då den inte är integrerad med flygbolagets server. Detta kan resultera i att användaren måste besöka flygbolagets hemsida för att få den information t ex flightnummer, avgångstid med mera som resebyrån kräver för att användaren ska kunna fullfölja sin biljettbeställning (Ryman, 2000). Se figur 1 nedan:

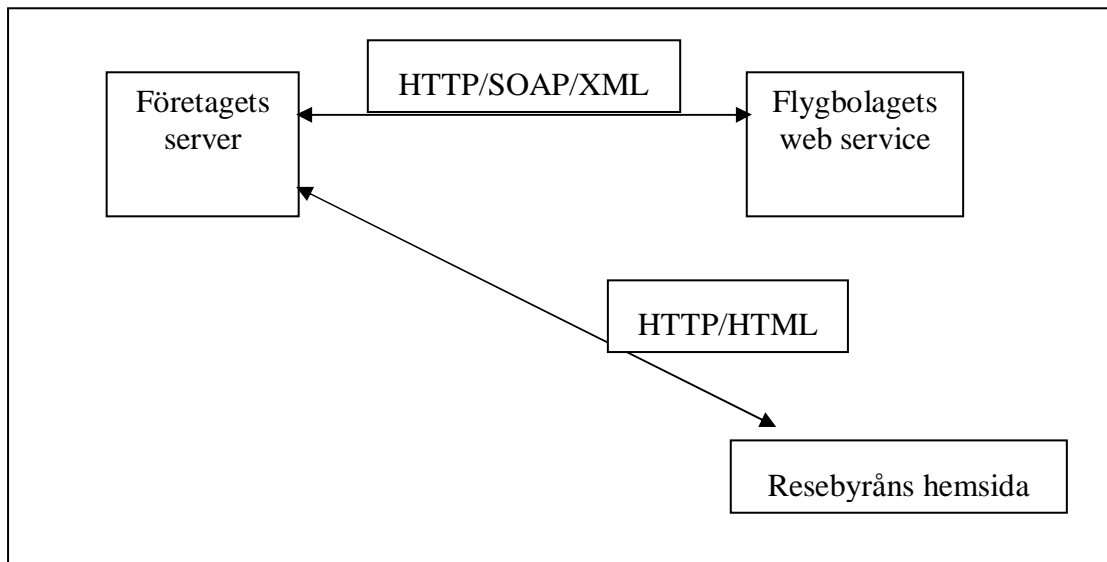


Figur 1: Applikationswebbens brister (efter Ryman, 2000, s.2).

Figuren kan tolkas så att protokollet HTTP används för att skicka HTML-dokument mellan serverna och webbsidorna. Användaren får mata in informationen manuellt från flygbolagets webbsida till företagets webbsida för att göra bokningen.

En lösning på problemet med applikationswebben skulle kunna vara att resebyråns hemsida blev integrerad med flygbolagets system via en web service. Då skulle resebyråns hemsida kunna få tillgång till informationen som flygbolaget har (Ryman, 2000). Flygbolaget skulle kunna implementera en eller flera web services och kan då ses som en provider, det vill säga ägaren till tjänsten. Ägarens uppgift är att publicera och uppdatera de tjänster som ska finnas tillgängliga för användarna t ex resebyråns kunder (Tsalgatidou och Pilioura, 2002). Resebyråns hemsida kan programmeras att erhålla listan från flygbolagets web service automatiskt. Detta resulterar i att användaren inte behöver lämna resebyråns hemsida för att ta reda på den information som applikationen kräver för att kunna utföra tjänsten (Ryman, 2000) Se figur 2 nedan:

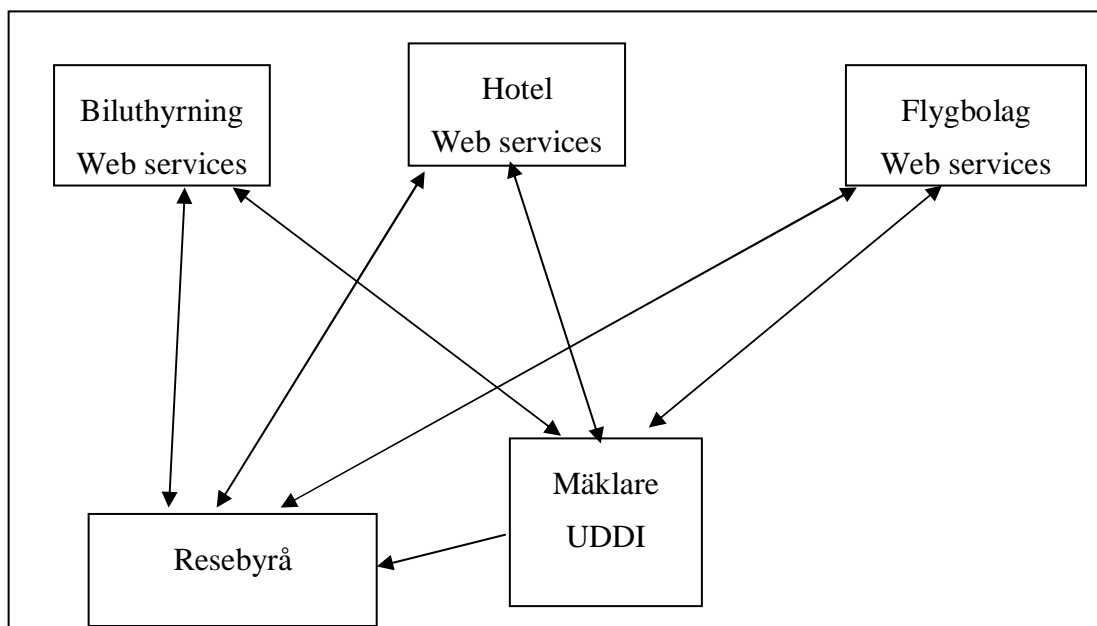
2 Web services



Figur 2: Integreringen mellan två företag (efter Ryman, 2000, s.2).

Företagets server är integrerat med flygbolagets web service och använder HTTP och HTML för att visa informationen på den egna hemsida.

För att göra ovanstående scenario mer realistisk och visa de potentiella fördelarna som kan utnyttjas vid valet att implementera web services kan en utökning av figur 2 göras. Ett exempel kan vara att resebyrå inför flera web services från de arbetspartner som företaget utbyter tjänster med som exempel hotell och bilbokning. I exemplet nedan kan användaren i samband med biljett bokning även boka hotell, bil eller andra eventuella förhandsbokningar. Alla dessa bokningar kan ske utifrån resebyråns hemsida utan någon inblandning av en försäljare (Ryman, 2000). Se figur 3 nedan. Enligt Tsalgatidou och Pilioura (2002) kan en mäklare (broker) ses som en katalog med innehållande register med information om de web services som finns för ett företag (service requester) att tillgå. Ett exempel på en mäklare är Universal Description, Discovery, Integration (UDDI). Detta är den tjänst som resebyrå kan använda för att kunna lokalisera andra tillgängliga web services som resebyrå sedan kan implementera för att öka servicen till sina kunder.



Figur3: Potentiella fördelarna med web service (efter Ryman, 2000, s.3).

Figuren visar hur resebyrån kan implementera flera olika web services från sina partner antingen direkt eller via en mäklare som består av ett UDDI-register.

Med den utvecklingen som Internet har finns det all anledning att anta att applikationswebben inte kommer att vara tillräcklig för organisationer som strävar efter att automatisera och Internet-anpassa sig. Genom att organisationer använder web services kan företag effektivisera och få stora ekonomiska fördelar gentemot de potentiella konkurrenterna som inte använder sig av web services.

2.4 Standarder inom web services

Uppbyggnaden av web services har skett utifrån Internetstandarder. Det som dessa standarder har gemensamt är att de inte fokuserar på implementationen utan på själva protokollet. Företag som har bidragit till utvecklingen av standarder inom web services är företag som Microsoft, IBM och Ariba (Ryman, 2000). I dag har dock en stor del av utvecklingen lämnats över till World Wide Consortium (W3C) som är en organisation vars främsta uppgift är att godkänna och administrera nya Internetstandarder (Eriksson, 2002). Standarderna som generellt sammankopplas med web services är: XML, SOAP, WSDL och UDDI (Ryman, 2000). Eftersom dessa standarder förknippas med web services kan det därför anses vara nödvändigt att övergripande förklara dessa, vilket kan resultera i att helheten av begreppet web services lättare kan fångas. Det finns knappats något annat område i dag där standarder har haft lika stort inflytande på utvecklingen som inom web services (Moorsel, 2002).

2.4.1 XML (Extensible Markup Language)

XML kan ses som ett "märkespråk" som används för att beskriva de olika delarna som ett dokument eller en text kan innehålla. Detta för att andra datorer lätt ska kunna läsa och förstå innehållet. XML härstammar från språk som Standard Generalized Markup Language (SGML) och HTTP (Eriksson, 2002). XML är i dag en standard för hur datakommunikation ska ske mellan olika applikationer som använder XML.

Ett XML-dokument byggs upp av olika sektioner där det finns möjlighet att kryptera vissa delar. För att uppnå en högre säkerhet kan användaren även signera dokumentet digitalt (Hondo, Nagaratnam och Nadalin, 2002).

2.4.2 SOAP (Simple Object Access Protocol)

SOAP utvecklades av Microsoft och var tänkt att användas för att göra Remote Procedure Calls (RPC) över HTTP, vilket innebär att en förfrågan kan utföras mot en annan metod på en distribuerad nod. Men SOAP har utvecklats till att bli en standard för att skicka och ta emot meddelande över Internet. Det har varit ett flertal andra aktörer som har bidragit till utvecklingen av tekniken. Den har sedan blivit överlämnad till W3C se kapitel 2.4 (Ryman, 2000). SOAP är i sitt utförande inte beroende av plattform eller operativsystem. Det är inte heller bundet till ett specifikt språk eller objekt, vilket resulterar i att användningsområdet är väldigt brett. SOAP använder till stor del protokollet HTTP för att skicka information över Internet. Dock kan även andra transportprotokoll användas t ex FTP, SMTP eller TCP/IP. SOAP använder XML för att specificera hur data ska skickas (Tsalgatiou och Pilioura, 2002). SOAP kan definiera två olika typer av meddelanden: begäran (request) och svar (response) detta för att göra det möjligt att kunna begära en tjänst och sedan få tillbaka ett svar. Enligt Tsalgatiou och Pilioura (2002) kan ett meddelande som skickas bestå av en header som kan variera mellan olika transportlager och ett dokument innehållande XML som i sin tur består av tre delar:

1. Kuvert (Envelope) definierar vad som finns i meddelandet.
2. Huvuddel (Header) är inte nödvändig. Innehåller dock viktig information såsom äkthetsbevis och transaktion.
3. Kropp (Body) innehåller själva meddelandet.

2.4.3 WSDL (Web Service Description Language)

WSDL är ett XML-format för att beskriva de olika färdigheterna som en web service har. Informationen som beskrivs är vad web services gör, lokaliseringplats samt hur tjänsten är implementerad. Detta för att en applikation ska kunna använda en tjänst då kravet är att gränssnittet måste vara väl detaljerat (Tsalgatiou och Pilioura, 2002). Informationen som måste förklaras är vilket protokoll som används, vem värden är och vilket portnummer som används. Det måste även finnas information om de olika operationer som kan utföras, och formatet som används för in- och utmeddelanden samt de undantag som kan ske (Ryman, 2000). WSDL har den potentiella fördelen att kunna byggas ut att den kan innehålla information som körningsmiljö och säkerhetsaspekter. Då dessa inte finns tillgängliga tvingas användaren att göra antagande om säkerheten i körningsmiljö av en web service. Genom att kunna fastställa dessa säkerhetsaspekter i XML möjliggör en förenklad tolkning av säkerhetsattribut i olika implementationer (Hondo, et al., 2002).

2.4.4 UDDI (Universal Description, Discovery and Integration)

UDDI kan definieras som en katalog innehållande ett register eller som en mäklare som innehåller en katalog med register. I registret finns de olika företag som tillhandahåller web services över Internet. Detta för att underlätta för leverantörerna och de intressenter som finns att hitta den information som de söker. Några av de företag som har implementerat UDDI-register är IBM, Microsoft och Ariba. En

mycket bra egenskap hos UDDI är att leverantören av tjänsten inte behöver uppdatera några av sina tjänster efter registreringen då detta sker automatiskt (Ryman, 2000). Specifikationen av UDDI består av ett XML-schema för SOAP meddelanden och en beskrivning av UDDI APIs specifikation, d.v.s. de subrutiner eller funktioner som kan anropas för att utföra någonting. Ett UDDI-XML schema definierar fyra datastrukturer: affärsentiteter, affärsservice, bindningsätt samt tmodel:

- **Affärsentitet:** innehåller information om affärsverksamheten som t ex organisationsnamnet, vilka web services som är tillgängliga samt kontaktinformation.
- **Affärsservice:** innehåller en mer detaljerad information om de tjänster som är tillgängliga då varje services kan ha många olika bindningsätt som HTTP och FTP.
- **Bindningsätt:** beskriver den tekniska informationen som tjänsten har.
- **Tmodel:** beskriver vilken specifik specificering eller standard som web services använder.

Med denna information kan ett företag lokalisera andra web services som är kompatibla med deras egna system (Tsalgatiidou och Pilioura, 2002).

2.5 Fördelar och nackdelar med web services

Några av de fördelar och nackdelar som associeras med web services i dag kommer att redovisas nedan. Eftersom begreppet web services är relativt nytt för många aktörer och dess innebörd lite osäker kan det därför vara bra att försöka definiera vad för typ av för- och nackdelar som associeras.

2.5.1 Fördelar

För organisationer som använder web services möjliggör detta att de på ett enkelt och smidigt sätt kan utveckla nya tjänster eller produkter från redan existerande tjänster. Detta kan göras genom att återanvända eller kombinera tidigare redan existerande tjänster. Detta leder till att kostnaden och utvecklingen av nya tjänster minskas och kan ge stora ekonomiska fördelar gentemot konkurrenter på marknaden, eftersom utvecklingsarbete ofta är en tidskrävande och ekonomisk process för en organisation (Tsalgatiidou och Pilioura, 2002). Ytterligare aspekter som kan uppfattas vara fördelar för web services är följande:

- **Teknik:** Web services kräver inte att det finns samma teknik på vardera sidan av kommunikationen. Det enda som krävs är att båda parterna har en SOAP meddelande processor, som består av en mjukvara. Denna teknik kan skrivas av många olika tekniker som t ex en XML-processor (Baker, 2002).
- **Komplexitet:** Med web services minskas komplexiteten i systemen genom inkapsling. Alla komponenter kan ses som services vilket innebär att utvecklare inte behöver ta hänsyn till detaljerna kring implementationen. Det som däremot är viktigt är vad för typ av beteende web services har som organisationen ska använda (Tsalgatiidou och Pilioura, 2002).

2.5.2 Nackdelar

Enligt Eriksson (2002) existerar det två stora aspekter inom web services där de inblandade parterna måste komma fram till en standardiserad lösning. De två områdena är transaktion och säkerhet. I dag finns ett flertal olika tillämpningar på dessa men problemet behöver lösas på ett mer standardiserat sätt. Utöver dessa två aspekter kan även utvecklingen av web services och pålitligheten hos ägaren till tjänsten ses som aspekter som kan associera till nackdelar.

- **Transaktioner:** Problemet med transaktioner över Internet är att det inte sker direkt mellan två servrar utan datatransporten sker över HTTP där data delas upp i paket. De problem som kan uppstå om en transaktion avbryts eller inte kommer fram, måste lösas för att inte påverka organisationer negativt (Eriksson, 2002).
- **Säkerhet:** Säkerhetsrutinerna måste skötas på ett standardiserat sätt eftersom web services gör det möjligt för företag att öppna upp sina system för att dessa ska bli tillgängliga utifrån. Eftersom det inte existerar någon bra lösning hur en användare automatiskt ska godkännas eller inte, skapar detta problem när web services används utanför det interna systemet (Eriksson, 2002).
- **Utvecklingen:** Utvecklingen och spridningen av web services kan hämmas på grund av oenighet mellan de olika aktörer som utvecklar verktyg, plattformar och standarder. Det finns även en trend som visar att några av de utvecklande parterna vill patentera och avgiftsbelägga vissa verktyg. Andra aktörer försvarar däremot öppenheten med att alla delar av web services ska byggas på öppna standarder som är fria att använda för alla parter (Eriksson, 2002).
- **Pålitlighet:** Hur en användare kan vara säker på att ägaren av en web service är pålitlig d.v.s. att tjänsten alltid är tillgänglig och inte försvinner är frågor som måste lösas (Glass, 2000).

2.6 Säkerhet inom web services

Eftersom säkerhet är ett väldigt brett begrepp som kan tillämpas i många olika former beroende på området som begreppet relateras till, kan det vara bra att först definiera vad säkerhet är och vad det kan ha för betydelse för en organisation som tillämpar web services.

Begreppet säkerhet i allmänt avseende kan, enligt Nationalencyklopedin (1995), förklaras vara åtgärder eller egenskaper som reducerar sannolikheten av oönskade händelser eller olyckor.

Begreppet säkerhet relaterad till data kan, enligt Nationalencyklopedin (1995), vara ett generellt begrepp som innefattar allt som rör säkerhet inom databehandling. De delarna som räknas in är datorer, datautrustning, lagrad data, program, bearbetad data, datatransport samt databehandlingens omgivning. Datasäkerheten kan även delas in i tre olika delmål:

1. Tillgängligheten ska kunna säkerställas hos lagrad data.
2. Obehöriga användare ska inte kunna ta del av informationen.
3. Kvalitén ska kunna fastställas på den lagrade informationen i systemet.

För att en organisation ska kunna ha en säkerhetsmodell över sina web services måste denna modell illustrera hur dataflödet kan gå genom en applikation och ett nätverk för att kunna möta de säkerhetskrav som är definierade av organisationen. Detta kan resultera i att man blir medveten om de risker som kan finnas och uppstå i organisationen (Hondo, et al., 2002). Enligt Gopalakrishnan och Rajesh (2003) har organisationen W3C tagit fram sex omfattande riktlinjer som behandlar säkerheten inom web services. Dessa kan även fungera som en mall för både utveckling och användning av web services. De sex riktlinjerna är:

1. Organisationen som äger web servicen ska kunna garantera att web servicen alltid är tillgänglig för de parter som har blivit godkända att använda tjänsten.
2. Organisationen ska kunna garantera att en godkänd partner får tillgång till web servicen eller den lagrade informationen.
3. Organisationen måste kunna garantera att data som skickas till användaren är skyddad.
4. Organisationen måste kunna garantera att data som skickas inte har modifieras under sändningen till mottagare.
5. Organisationen som tillhandahåller web servicen ska inte kunna förneka efter sändningen att informationen är skickad.
6. Organisationen ska kunna garantera att web servicen alltid är nåbar samt att den är skyddad mot hot inom och utanför systemet.

Gopalakrishnan och Rajesh (2003) menar att på grund av att säkerheten inom web services befinner sig i ett tidigt stadium sker det kontinuerlig forskning och utveckling av nya standarder och tillämpningar för att kunna uppnå en fast standard. Säkerhetsaspekterna som existerar i dag inom web services kan delas upp i två olika nivåer.

- **Transportsäkerhet:** Omfattar den säkerhet som finns inbyggd i det valda transportprotokollet som används för att skicka informationen t ex HTTP. De transaktioner som använder HTTP kan använda den grundläggande tillämpningen d.v.s. auktorisering. Detta ger skydd till de första fyra punkterna i W3C lista. Om en högre säkerhet är önskvärd kan HTTPS användas. Detta innebär att Secure Socket Layer (SSL) används och möjliggör att kommunikationen krypteras och dekrypteras mellan webbrowser och en web service. Genom att kombinera HTTP:s grundläggande säkerhet och HTTPS kan en högre säkerhet uppnås som täcker de första fyra punkterna i W3C lista samt erbjuder ett bättre skydd mot punkt 5.
- **SOAP och meddelandesäkerhet:** Omfattar användning av digitala signaturer samt certifikat på XML-nivå. På denna nivå förekommer det en omfattande utveckling och forskning.

Enligt Baker (2002) existerar det ett flertal olika förslag för att lösa säkerhetsaspekterna inom web services. Troligtvis kommer det att dröja innan det kommer en användningsstandard som täcker både intern och extern kommunikation. Det finns ett flertal olika företag som har kommit upp med lösningar på problemet.

2 Web services

Dock existerar det ingen standard för säkerheten när det gäller web services. Säkerhetsstandarderna måste integreras med kommunikationsstandarderna att de aktörer som är inblandade i en process kan kontrolleras på ett enkelt sätt. Enligt Eriksson (2002) är grundtanken med web services att företag och organisationer ska kunna öppna upp sina system för att kunna göra automatiska transaktioner och processer med andra aktörer som tidigare har skett manuellt inom verksamheten. För att kunna säkerställa de olika transaktionerna och den säkerhet som krävs för att kunna använda denna filosofi, krävs det ytterligare standardisering och enighet från de olika parter som är inblandade i utvecklingen av web services (Eriksson, 2002).

Enligt Eriksson (2002) är den kanske viktigaste säkerhetsaspekten hur frågan om behörighet ska lösas. Denna process kommer troligtvis att bestå av en automatisk process för att godkänna användarens tillgång till systemet eller inte. I dag finns ingen bra lösning på detta. Det gäller då främst uppkoppling över Internet och inte mellan olika interna system. En annan viktig del som behöver få en standardisering är hur transaktioner ska kunna säkerställas då dessa transporteras över HTTP där datamängden delas upp i små paket som skickas den snabbaste vägen mellan sändaren och mottagaren. Eftersom datatransporten inte sker över en fast förbindelse mellan två servrar kan avbrott i sändningen leda till flera olika problem som måste kunna elimineras för att säkerställa sändning och mottagning (Eriksson, 2002).

Enligt DeJesus (2001) ökar problematiken med säkerheten inom web services då det ofta är datorer som kopplar upp sig för att begära en tjänst, vilket försvårar användandet av lösenord och namn som inloggning, eftersom datorerna kopplar upp sig med IP-nummer. Enligt Pagina (2003) kan ett IP-nummer förklaras som en identifierare för de datorer som deltar i någon transaktion på Internet. Ett IP-nummer består av ett unikt 32-bitarsvärde (4 byte) och skrivs vanligen som ”punktade oktetter” där värdena separeras med punkter.

Eftersom web services är ”statesless” det vill säga att informationen om klienten inte sparas efter själva processen måste därför varje ny uppkoppling godkännas. En lösning på problemet med IP-nummer kan vara att bara godkända IP-nummer får tillgång till tjänsten eller genom att använda sig av standardverifieringen som associeras till det använda transportprotokollet som används, exempelvis HTTP (DeJesus, 2001).

Enligt DeJesus (2001) kan några tänkbara attacker mot web services vara följande. Eftersom web services använder sig av HTTP-protokollet för att skicka data i form av ett SOAP-meddelande är det lätt för attacker som ”snooper attacker” vilket innebär avläsning av trafiken som skickas via olika nät. Ytterligare ett problem som kan uppkomma är en ”denial of service attack”, vilket innebär att ägaren av tjänsten blir bombarderad av förfrågningar till tjänsten att datorn till slut hänger sig. Detta kan generellt lösas sig genom att neka de återkommande IP-numren eller att använda krypteringsmetod som t ex SSL. För web services kan detta leda till stora problem då vissa tjänster är beroende av andra och kan därför skapa en dominoeffekt som kan få vissa tjänster att sluta fungera eller helt slås ut (DeJesus, 2001).

Riskerna och farhågorna som främst existerar inom web services är att informationen kan modifieras eller försvinna när informationen skickas från en organisation till en annan. Eftersom web service transaktioner skickar SOAP-meddelande i form av XML-kod kan denna information bli direkt läsbar för individer som snappar upp

meddelandet när det t ex transporteras över Internet (Gopalakrishnan och Rajesh, 2003). Ratnasingam (2002) påpekar att det finns en stor risk för organisationer att använda Internet för att göra transaktioner då Internet saknar egen säkerhet och har en öppen arkitektur som är tillgänglig för alla användare.

2.7 Fastighetsautomation

När det gäller den framtagna informationen om fastighetsautomation har en konsult inom området tillfrågats för att få fram uppgifter som kan anses vara relevant för arbetet. Orsaken till att konsulten inte presenteras är på grund av att personen vill vara anonym, konsulten är verksam inom området och har lång erfarenheten inom fastighetsautomationsbranschen. Anledningen till detta förfarande är att information har varit svår att få tag på. Generellt har all övrig information inom området varit förvinklad och därför inte ansetts vara relevant.

Behovet av att kunna styra och reglera har funnits ända från början av vår tekniska tidsålder. Det som i dag kallar för styr och övervakning inom fastighetsautomation var tidigare uppdelat som egna separata funktionsdelar: styrning, reglering och övervakning. Styrningen hanterade till- och frånslag av t ex pumpar och fläktar. Regleringen bestod av funktions-specifika reglerenheter, där varje reglerfunktion krävde sin typ av regulator, t ex temperaturreglering. Regulatorerna för fastighetsautomation var från början elektromekaniska eller pneumatiska. Övervakningen av fastighetsinstallationer omfattade oftast en centralt placerad larmtablå med optisk och akustisk indikering. På larmtablå kunde man se kontaktsvar från t ex utlösta motorskydd. I takt med att minidatorn föddes utvecklades också digitala system för styr- och övervakning inom fastighetsautomation. Men det var först när PC-datorerna kom som utvecklingen av systemen blev vad vi i dag med gemensamt namn kallar för styr och övervakning, d.v.s. funktioner för styrning, reglering, larm och övervakning är integrerade i samma system. De PC-baserade övervakningssystemen var ursprungligen uppbyggda som enanvändarsystem, d.v.s. med endast en fast operatörsplats. I takt med utvecklingen av PC-datorer och nätverk blev det också möjligt med fleranvändarsystem baserade på fasta klientprogram för varje tillkommande användare. Internet och webbt teknik kan nu ersätta fasta operatörs/klientprogram och erbjuda ett geografiskt oberoende operatörsgränssnitt.

Några av de problem som oftast relateras till fastighetsautomation är integreringen av data samt kompatibilitet. En stor förändring som håller på att ske är övergången till redan existerande standarder inom IT-branschen som t ex möjligheten att använda bredband/nätverk och webbt teknik som överföringsmedia för signaler och information. Denna övergång har resulterat i några fördelar- och nackdelar, en av de stora fördelarna är att det inte finns någon geografisk begränsning för informationen samt ökad flexibilitet. Den största nackdelen som tillkommer med den nya tekniken är främst behovet av ökad säkerhet. Främst för att informationen blir mer tillgänglig och sårbar.

3 Problembeskrivning

För organisationer som är intresserade av att använda Internet som ett medium för att erbjuda andra organisationer eller privata kunder sina tjänster är konceptet web services en väg att realisera detta. Dock tillkommer det några problem när organisationer använder sig av Internet som en plattform för sina tjänster (Ratnasingam, 2002).

Vissa tjänster som organisationer distribuerar är inte alltid gratis, eller ska inte vara tillgängliga för alla användare på Internet. En del tjänster kan innehålla känslig information som kan skada företaget på ett flertal olika sätt om denna information blir tillgänglig för utomstående personer som inte har rättigheten att läsa eller ta del av denna. Då Internet räknas av många människor som en allmän plats ökar detta kraven på att företagen måste utveckla och säkerställa en tillräcklig hög säkerhetsnivå som möjligt för att undvika sabotage eller otillåten tillgång till sina system (Ratnasingam, 2002). Enligt Eriksson (2002) kan web services göra det möjligt för företag att omstrukturera och effektivisera sin organisation kommer detta att leda till att de interna systemen kan komma att öppnas upp. Detta för att kunna utföra vissa specifika tjänster som andra behöver komma åt. Genom att de interna systemen öppnas upp ökar detta kraven på att organisationerna måste kunna säkerställa de krav som uppkommer med detta. Organisationer måste kunna definiera den säkerhetsnivå som krävs för att säkerställa deras system och data (Eriksson, 2002).

Eftersom Baker (2002), påpekar att det inte existerar någon direkt standard för säkerheten inom web services utan att det existerar ett flertal olika säkerhetstillämpningar för organisationer. Detta resulterar i att det är upp till organisationen själv att avgöra vad för typ av säkerhets tillämpning som organisationen tror sig behöva (Eriksson, 2002).

Eftersom en organisation kan välja att använda web services bara inom de interna systemen eller över Internet kan detta påverka valet av säkerhetstillämpningar för att organisationen ska kunna skydda sig. På grund av att säkerheten inom web services inte definitivt kan fastställas kan det därför anses vara relevant att undersöka vad för typ av tillämpningar det finns och hur organisationer har valt att implementera sina web services. De organisationer som ska undersökas i detta arbete är verksamma inom fastighetsautomationsbranschen där huvudaktiviteten utgörs av styr- och reglerteknik. I denna bransch har stora förändringar skett de senaste åren vilket har påverkat branschen som helhet mycket tack vare den utvecklade IT-tekniken.

Enligt Tsalgatidou och Pilioura (2002) har denna växande Internet-teknologi gjort det möjligt för organisationer att göra affärer på många nya sätt. Många organisationer har därför valt att flytta sina huvudoperationer till webben för att nå ökad automatisering, snabbare affärsprocesser och global tillgänglighet. Undersökningen kommer att genomföras genom att undersöka huruvida de framtagna riktlinjerna från W3C kan relateras till branschens web services.

3.1 Problemprecisering

Problemställningen som denna rapport avser att undersöka och som kommer att ligga som grund för undersökningen är *hur web services hanteras inom fastighetsautomation*, utifrån W3C:s riktlinjer som presenterades i kapitel 2.6. Undersökningen avser även att försöka ta fram de respektive för- och nackdelar som associeras med web services inom branschen samt att definiera utvecklingen av den här tekniken. För att besvara rapportens huvudproblemställning kommer främst första delfrågan att användas. Delpunkt två syftar till att ta fram för- och nackdelar med web services inom fastighetsautomationen, medan del tre är tänkt att ge en bild över utvecklingen av tekniken inom branschen. Samtliga delfrågor kommer förhoppningsvis leda till en bättre förståelse av problempreciseringen och de två sista delfrågorna kommer troligtvist att bidra med information som kan vara relevant för att kunna besvara problempreciseringen.

Hur hanteras web services inom fastighetsautomation?

- Hur tillämpas W3C riktlinjer?
- För och nackdelar med web services?
- Utveckling av web services inom fastighetsautomation?

3.2 Det vetenskapliga bidraget

För många organisationer är web services det nästa naturliga steget att ta i strävan att automatisera och Internet-anpassa sig. Med web services kan organisationer bland annat effektivisera verksamheten vilket kan leda till stora ekonomiska fördelar gentemot de konkurrenter som inte använder sig av detta. Eftersom de inte existerar någon direkt standard för säkerheten tvingas därför organisationerna själva att avgöra vad för typ av säkerhetsnivå och åtgärder som behövs för att de ska kunna säkerställa tjänsterna. Detta är väldigt viktigt eftersom de interna systemen kan komma att öppnas upp för att göra informationen mer lätt tillgänglig. Förhoppningsvis kommer denna rapport och den planerade undersökningen att kunna bidra med främst två aspekter som kan anses vara av stor vikt för de organisationer som använder, eller är i utvecklingsstadiet av web services inom fastighetsautomationsbranschen. Dessa två aspekter kan sammanfattas vara följande:

- Kan bidra till en ökad medvetenhet om säkerheten hos organisationer inom fastighetsautomationsbranschen.
- W3C:s riktlinjer omfattar säkerheten inom web services, kan även fungera som en mall för utveckling och användning.

3.3 Avgränsning av problemet

Examensarbetet kommer att fokusera på säkerhetsaspekter inom fastighetsbranschen där ett flertal system har installerats för att underlätta övervakning och driftunderhåll, för olika parter som sköter underhållningen av de interna systemen och kan sammanfatta fastighetsautomationen. De interna systemen övervakar till stora delar energiförsörjningen. Examensarbetet kommer inte att gå in på teknisknivå när det gäller säkerhetslösningar för web services eller olika typer av organisationer för att precisera vad respektive organisationstyp anses behöva för tillämpningar.

3.4 Förväntat resultat

Examensarbetet skall avgöra huruvida W3C riktlinjer för web services på säkerhets tillämpningar överensstämmer med de tillämpningarna organisationer har gjort inom web services. Med tanke på de många olika former och typer av organisationer och tjänster som kan tänkas tillämpa web services i någon grad är det troligt att synen på säkerhetstillämpningar markant kommer att skilja sig åt.

En av orsakerna till skillnaderna kan vara ifall tjänsten är tillgänglig över Internet eller inom ett lokalt nätverk, samt om tjänsten tillhandahålls till kunden från någon extern organisation eller om tjänsten finns i systemet. Troligtvis kommer även organisationerna att anse att fördelarna med web services är fler än de nackdelar som organisationerna kan associera till. Synen på utvecklingen inom fastighetsautomation kommer nog att visa på att det finns flera områden där web services kan användas.

4 Metod

Kapitlet kommer att beskriva några olika metoder som kan tänkas användas för rapportens undersökning. En metod kommer att väljas ut för att sedan ligga till grund för genomförandet i rapporten. Metoden kommer att presenteras i delkapitel 4.2.

4.1 Tänkbara metoder

Några av de tänkbara metoder som kan användas för att samla in information är, enligt Andersen och Schwenche (1998), intervjuundersökning, enkätundersökning och observation. Användningsområdet och tillämpningarna som dessa metoder har kan variera beroende på undersökningens syfte och omfattning. Jag kommer att redovisa de metoder som kan användas i denna undersökning för att under delkapitel 4.2 motivera vilken metod som har valts ut för att användas i undersökningen.

4.1.1 Intervju

Intervjutekniken används för att samla in information från ett antal ställda frågor. Enligt Patel och Davidson (1994) brukar en intervju förknippas med ett fysiskt möte mellan två parter. Dock kan intervjuer även genomföras via ett telefonsamtal.

Enligt Patel och Davidson (1994) existerar det två aspekter som behöver beaktas innan en intervjuundersökning kan genomföras. Första aspekten är vilken grad av standardisering som ska tillämpas och kan sammanfattas i hur mycket ansvar intervjuaren har när det gäller frågornas utformning och ordning. Den andra aspekten är intervjuens strukturering och innebär i vilken utsträckning som intervjupersonen kan tolka frågorna utifrån sin egen inställning eller tidigare erfarenhet.

En fördel med att använda intervjuer i undersökningen är att det under processen finns möjlighet att klargöra och förtydliga frågorna samt få en diskussion kring de ställda frågorna. Ytterligare en fördel med att använda intervju till denna undersökning är att de eventuella frågetecken och missförstånd som kan uppstå, kan minimeras och ökar då svarens relevans till frågeställningen i bakgrunden. De nackdelar som finns med att använda intervjuer i undersökningen är att det kan vara svårt att få tag i rätt personer som besitter den eftersökta kunskapen samt att de personer som intervjuas kanske inte är villiga att svara på undersökningens frågor (Patel och Davidson, 1994).

4.1.2 Enkätundersökning

En enkätundersökning innebär att ett formulär med ett antal frågor skickas till den eller de utvalda personerna som undersökningen omfattar. Strukturen på ett frågeformulär kan variera från frågor med fasta svarsalternativ till mer öppna frågor där uppgiftslämnaren själv skriver ner ett passande svar (Andersen och Schwenche, 1998).

Enligt Andersen och Schwenche (1998) är frågeformulär bättre än intervjuer när antalet personer som ska undersökas är stort eller är utspridda över ett geografiskt område eller på något sätt är svåra att få tag på. Arbetets undersökning kommer troligtvis inte att innefatta en tillräckligt stor grupp för att en enkätundersökning är att föredra. Några av nackdelarna som associeras till denna metod är aspekter som

bortfall av svar, misstolkningar från uppgiftslämnaren samt att möjligheten att följa upp en fråga eller få tydligare svar är sämre än intervjuer. Detta kan resultera i att sammanställningen av svaren blir missledande och undersökningen kan därför tappa sin trovärdighet

4.2 Vald metod

Enligt Patel och Davidsson (1994) är både intervjuer och enkäter metoder för att samla in information från ett antal frågor som ställs eller skickas till de berörda parterna. Intervjuundersökning är, enligt Andersen och Schwenche (1998), en bra metod att använda då de som ska intervjuas består av en liten grupp personer, och då frågorna kan beröra information som kan uppfattas vara känslig. Det kan även vara en stor fördel att använda intervju när det inte existerar några klara svarsalternativ då detta ger möjlighet att ställa nya frågor under processen. Det minimerar också risken med att få missvisande svar, samt att eventuella missförstånd kan förklaras. Eftersom intervjuer bygger på frågor påpekar Patel och Davidsson (1994) att undersökningen är beroende av respondentens vilja att svara på de ställda frågorna.

Av de presenterade metoderna anses därför intervjuer vara det bästa alternativet för rapportens syfte. Detta för att gruppen, som undersökningen omfattar inte består av en tillräcklig stor grupp för att en enkätundersökning är att föredra, samt att delar av intervjun kan beröra känslig information. För att kunna få den information som undersökningen söker är det bästa sättet att använda en strukturerad intervju. Detta möjliggör lättare jämförelse mellan de olika svaren och kan få fram likheter och skillnader mellan de parter som var med i undersökningen.

På grund av de begränsningar som arbetet har i tid och omfattning kommer därför telefonintervjuer att användas. Frågorna kommer att skickas ut i förväg, detta för att respondenten ska kunna läsa igenom frågorna och förbereda sig för undersökningen. Undersökningens frågor kommer att vara fastställda under processen, detta för att enklare kunna jämföra svaren efter undersökningen.

4.3 Metodsteg

Kapitlet kommer att ta upp hur intervjufrågorna utformades och hur intervjuerna genomfördes i undersökningen.

4.3.1 Intervjuns upplägg

För att kunna få ett så bra resultat som möjligt från intervjuerna skickades frågorna några dagar innan intervjun per mail till respondenten som var delaktig i undersökningen. Detta för att ge respondenten tillräckligt utrymme och tid för att kunna förbereda sig på vad som kommer att tas upp och förhoppningsvis resulterar detta i en bättre undersökning.

Varje intervju beräknades ta cirka 30 minuter och frågorna var indelade i tre delar. Anledningen till detta upplägg är att genom en inledande del övergå till de frågor som är framtagna för att besvara frågeställningen i problemområdet.

4.3.2 Intervjuns utförande

Intervjuerna kommer att genomföras via telefon, detta eftersom att personerna som ska delta i undersökningen är utspridda över ett stort geografiskt område samt de begränsningar som beskrevs i kapitel 4.2. Detta begränsar möjligheten att genomföra fysiska intervjuer, men förhoppningsvis kommer detta inte att påverka genomförandet i undersökningen negativt. Intervjufrågorna kommer att ligga som grund för rapportens resultat.

4.3.3 Undersökningsgrupp

Undersökningen kommer att utföras på några organisationer inom fastighetsautomationsbranschen som har köpt, installerat och tillhandahåller driften av fastighetsautomation. För att hitta passande respondenter till undersökningen, kommer en konsult inom området att tillfrågas. Detta kommer förhoppningsvis att resultera i att arbetet med att söka efter organisationer kan förenklas samt att de organisationer som kommer att användas uppfyller undersökningens krav bättre.

5 Genomförande

Kapitlet tar upp genomförandet av undersökningen som denna rapport har gjort. För att samla in information har intervjuer valts att användas. Bakgrunden till intervjufrågorna kommer att redovisas samt en presentation av respondenterna och deras organisationer. De sammanställda intervju svaren kommer att presentera nedan. En mer ingående presentation finns i bilaga 2.

5.1 Processen

Undersökningen var tänkt från början att genomföras på organisationer inom fastighetsbranschen som har köpt in och använder automationsutrustning i fastigheterna. På grund av att dessa organisationer inte själva installerar, utvecklar eller underhåller systemen genomfördes undersökningen i stället på den grupp som antas ha störst erfarenhet och kunskap inom problemområdet. Gruppen som undersöktes är verksam inom fastighetsautomationsbranschen genom installation, utveckling samt underhåll. Denna grupp består av organisationer som arbetar genom att installera och underhålla fastighetsautomationssystem för fastighetsägare i Sverige. Dessa organisationer antas besitta den kunskap och erfarenhet som denna rapport är beroende av. Eftersom samtliga organisationer har varit aktiva inom den valda branschen under en längre tid kan de antas vara den grupp som är mest medveten om web services, dess utveckling samt de eventuella säkerhetsproblem som kan relateras till tekniken. Med all sannolikhet kommer förändringen som genomfördes att innebära bättre svar då de personer som intervjuades har större kunskap och erfarenhet inom problemområdet.

Frågorna som arbetades fram för undersökningen har koppling till problemprecisering i arbetet. Sammanlagt resulterade detta i att tolv frågor togs fram för att kunna besvara problemet (se bilaga 1). När frågorna var färdigställda kontaktades en konsult inom området som tittade igenom frågorna och kom med förbättringsförslag. Detta resulterade troligtvis i att frågorna blev bättre utformade och att eventuella missförstånd kunde minimeras innan undersökningen påbörjades. Hade detta inte varit möjligt hade undersökningen troligtvis resulterats i flera feltolkningar från respondentens sida, vilket hade påverkat undersökningen och resultatet. För att kunna hitta lämpliga organisationer till undersökningen erbjöd konsulten att komma med några alternativ. De framtagna organisationerna kontaktades och informerades om arbetets innehåll och syftet. Då antalet organisationer var för få för att genomföra undersökningen användes bland annat Internet för att leta rätt på ytterligare organisationer till undersökningen. För att lättare kunna jämföra svaren utgick organisationerna från ett genomfört projekt eller de tjänster som dessa ansåg sig bäst passa in på att besvara frågorna. De kontaktade företagen valde själva ut den mest lämpade personen inom organisationen att besvara undersökningens frågor. På grund av att vissa delar av intervjun kommer att beröra information som organisationerna kan uppfatta vara känsliga kommer därför svaren och presentationen av organisationerna att göras anonymt. Detta beslut har även varit önskvärt från de organisationer som har deltagit i undersökningen.

När intervjuerna hade genomförts började processen att sammanställa de olika svaren, varje intervjutillfälle dokumenterades genom bandupptagning för att underlätta processen. För ytterligare information om processen se kapitel 6.

5.1.1 Intervjuerna

Telefonintervjuerna som genomfördes, tog cirka 30 minuter vardera. Frågorna som ställdes var indelade i tre delar. Främsta orsaken till att dela upp intervjun var att börja med några inledande frågor för att sedan övergå till de frågor som är tänkta att besvara problemområdet som presenterades i kapitel 3.1. Frågorna i den första delen av intervjun var inledande och syftade till att få fram information om respondenten samt information om organisationen. Denna information kommer sedan att användas för att presentera organisationen. Den andra delen av intervjufrågorna syftade till att få fram övergripande information om organisationen och deras webbtjänster, samt ge information som är tänkt att besvara problempreciseringens delfrågor. Den sista delen av intervjufrågorna är framtagna från W3C:s riktlinjer som presenterades i kapitel 2.6 och syftar till att få fram information som är tänkt att besvara problempreciseringen. Frågorna som användes under undersökningen kommer att presenteras och motiveras i bilaga 1.

5.2 Presentation av respondenterna

Här nedan kommer en sammanställning av samtliga respondenter som var delaktiga i undersökningen. Presentationen av de sex deltagande organisationer kommer att ske anonymt (för ytterligare information se 5.1) och kommer därför att benämnas enligt följande: A, B, C, D, E och F.

5.2.1 Organisation A

Företaget köper in och installerar hård- och mjukvara hos kunden och gör de eventuella förändringar som är nödvändiga för att passa kundens önskemål. Företaget består av ca 100 personer och är verksamma inom 3 olika branscher, var av en är fastighetsautomation. Personen som representerar organisationen arbetar som projektledare inom företaget och säljer projektarbeten.

5.2.2 Organisation B

Fastighetsägaren kan sägas vara en väldigt stor organisation och har fastigheter utspridda över hela Sverige. Personen som representerar organisationen hanterar och har byggt upp ett webb-baserat övervakningssystem för en specifik fastighetsägare i Sverige. Dennes främsta arbetsuppgift är att underhålla och utveckla det befintliga systemet.

5.2.3 Organisation C

Organisationens främsta arbetsuppgift är styr- och reglerentreprenör. De utför främst konstruktion och installation av styr- och reglerutrustning i fastigheter. De har även på senare tid med hjälp av ny teknik kunnat erbjuda tjänster som kommunikation och distribution av övervakning av de olika installerade systemen i fastigheterna via deras lokala nätverk. De tjänster som brukar erbjudas är främst fastighetsövervakning. Kunden kan välja hur mycket kontroll han vill ha. Organisationen har idag tagit hela ansvaret för fastigheter över hela Sverige. De servicebolag organisation använder är anslutna till detta system och får ut larm oftast via sms eller mail. Alla styrsystem

programmeras av företaget samt de tjänster som företaget kan erbjuda. Personen som representerar organisationen arbetar som programmerare och systemintegratör.

5.2.4 Organisation D

Organisationen sysslar främst med fastighetsautomation vilket innebär att de får en beställning av en kund som vill att delar av, eller hela fastigheter, ska automatiseras. Om det finns något befintligt system som de kan koppla in sig på, bygger de upp systemet utifrån detta. I fall kunden vill komma åt systemet bygger de ett överordnat system där kunden kan titta på driftbilder och få fram olika värden. När organisationen ska implementera ett system används både egna system men även andra system och komponenter. De anpassas sedan utifrån hur kunden vill ha systemet och de tjänster som ska finnas. Det egna systemet som har byggts upp är utvecklat av standarder från W3C. Organisationen köper in och utvecklar en hel del egna system för att sedan efter kundens önskemål bygga upp och modifiera en slutlig lösning som installeras i en fastighet. Personen som representerar organisationen arbetar främst med programmering och att utveckla webb-baserade ”scada-system” som är ett system för att styra övervakning i fastigheter.

5.2.5 Organisation E

När organisationen säljer ett kontrakt till ett företag kan de via webben själva med Internet som ett verktyg gå in och trimma in kundens fastigheter samt ha övervakning av systemet. Genom att organisationen får larm sända till sig via SMTP-meddelanden kan de via Internet gå in och återställa larmet och justera felaktigheter. Organisationen kan även erbjuda en energistatistikrapportering över webben från en av deras partner till slutkunden. Deras system som installeras i fastigheten skickar information som mail till detta program som automatiskt genererar en rapport. Denna läggs sedan ut över nätet där slutkunden med sitt lösenord kan ta del av informationen, samt även inspektera sin egen fastighet. De kan även ha länkar från fastighetens hemsida direkt till tjänsterna. När organisationen säljer ett styrsystem kan våra kunderna köpa andra tjänster från deras partner. Oftast skickar systemet information till detta system som autogenererar t ex en statistikrapport.

Organisationen köper in olika komponenter, installerar och programmerar dem själva. En av dessa är t ex energiövervakning där de installerar och mäter energiövervakningen i fastigheten. Tjänsten skickas via SMTP-meddelande till deras partner och kunden får informationen mot en ersättning. Informationen kan visas i kronor, kilowattimmar eller i annat önskvärt format. Det finns möjlighet att ha med flera fastigheter i rapporten samt att se skillnaderna mellan dessa. Personen som representerar organisationen arbetar som projektansvarig med främsta arbetsuppgift som projektledare och säljare.

5.2.6 Organisation F

Organisationen säljer främst produkter till sina dotterbolag som i sin tur erbjuder sina tjänster och lösningar på problemen till slutkunderna, t ex fastighetsägarna. Normalt sätt strävar de mer efter att kommunicera på beslutsfattande nivå, t ex inom fastighetsägande företag, för att med webbtjänsten hjälpa fastighetsägaren. Personen som representerade organisationen är produktchef och arbetar främst med att definiera

5 Genomförande

och underhålla produktportföljen som innefattar presentation om information från ett visst system till användaren. Detta handlar främst om olika visualiseringsprodukter så som deras webbaserade produkter, klientserverbaserade programvaror eller operatörspaneler.

6 Presentation av intervjusvar

Svaren som framkommit från intervjutillfällena har sammanställts genom att information som inte har ansetts vara relevant för frågan har tagits bort. Svaren har däremot i stora drag fått behålla både struktur och innehåll. Samtliga svar kommer att redovisas anonymt. Detta beslut togs tidigare i processen för att försöka undvika avvaktande svar samt att skapa ett bättre förhållande under intervjuerna. Det insamlade materialet presenteras i bilaga nr 2. Orsaken till detta är att det finns önskemål från vissa aktörer att kunna ta del av materialet samt att rapportens analys kommer att utgå från denna information. Här nedan kommer en kort sammanfattning av svaren på intervjufrågorna att redovisas. Informationen kommer sedan att användas för att presentera de framtagna kategorierna i kapitel 7.1. Första delen av intervjun, som innehåller de inledande frågorna samt fråga 5 på den andra delen som berör organisationen, kommer inte att redovisas eftersom dessa frågor användes för att presentera organisationen och respondenten (se kapitel 5.2).

6.1 Del 2:

Använder er organisation idag någon typ av webbtjänst?

- *På vilket sätt är tjänsten uppbyggd och hur fungerar den?*

Samtliga organisationer tillhandahåller själva eller har implementerat tjänster som används över Internet eller inom interna nät. De flesta av tjänsterna används för att styra och övervaka fastigheter och kan skicka information om t ex klimat, larmhantering, säkerhet och driftdata.

Vad är begreppet web service för er?

- *Anser ni att er webb tjänst är en web service varför/varför inte?*
- *Hur ser utvecklingen ut inom er bransch gällande webb-baserade tjänster?*

Organisationernas syn på begreppet web services och hur detta begrepp kan relateras till automationsbranschen är varierande i den bemärkelsen att frågetecken existerar. Organisation A:s syn på begreppet är att det är något som rör sig dynamiskt, t ex att styra en fläkt på distans över Internet, anser även att det existerar en skillnad i funktionaliteten mellan vanliga webbtjänster och web services. Tekniken har skapat möjligheten att kunna styra en maskin utan en fysisk kabel. Organisation B kopplar begreppet till Microsoft dot.Net och anser inte direkt att deras tjänst är en web service men tror att web services kommer att bli väldigt stort och underlätta många situationer i framtiden som t ex i integreringen av de befintliga systemen. För organisation C är begreppet nytt och har tolkat det som att kunna erbjuda mer automatiserade webbtjänster av olika slag. ”En av de stora framtida fördelarna med web services är att det finns en klar vilja i vår bransch att kunna distribuera ut insamlat material på ett enkelt sätt.” Organisation D anser inte att de har web services men påpekar att det skulle kunna användas för att hämta data från olika styrdata. Detta kan göra att web services och XML kommer att bli stort inom fastighetsautomation. Organisation E

anser att de använder sig av web services och att det kommer att bli det nästa naturliga steget för deras bransch att ta. Organisation F anser att deras webbtjänst är en web services främst för att de använder SOAP och XML i systemet.

Vilka för/nackdelar anser ni att det finns med att använda web service?

Samtliga organisationer anser att det finns stora fördelar med att använda sig av web services i fastighetsautomation. Några av de fördelar som organisationerna ansåg vara de största kan sammanfattas vara: organisation A ser fördelar med att använda sig av öppna standarder och slipper då i regel att göra installationer på klienterna hos användarna. Organisation C understryker att investeringskostnaderna kan hållas nere genom att investera på ett ställe som kunderna sedan kan utnyttja och slipper då ha egna system. Organisation D menar att den största fördelen med web services är tillgängligheten och att implementeringen kommer att bli lättare i Microsoft dot.Net än i OPC. Organisation F tror att de typer av tjänster som finns kommer att öka genom att man kan koppla ihop olika typer av tjänster som i dag redan finns, dessa kan sedan kopplas ihop med de installerade systemen. En av nackdelarna som kan associeras till web services är enligt organisation B att öppna upp system för att göra funktioner mer tillgängliga, detta för risken med intrång kan öka.

Vilka får ta del av informationen i organisationen?

- *Hur begränsas tillgängligheten av information av web servicen?*

De grupper av personer som får ta del av informationen, enligt organisationerna, är de grupper som har behörighet till detta. Majoriteten av organisationerna använder sig av behörighetsnivåer med inloggning för att begränsa vissa delar av informationen från användarna.

6.2 Del 3:

Hur tillgänglig är tjänsten och informationen för de parter som använder web servicen?

- *Vad är det för typ av information som tjänsten visar?*
- *Hur kan informationen visas?*
- *Vilka tekniker använder ni för att göra det möjligt?*

Samtliga organisationer hävdar att tjänsten och informationen alltid ska vara tillgänglig för dem som använder dessa. Den informationen som finns tillgänglig är främst tekniska värden som mätvärden, larm, reglerparametrar och driftbilder i grafiska bilder, samt driftstatus, temperatur och historik. De olika sätten som informationen kan visas beror på om tjänsten och informationen är åtkomlig över Internet eller om det är inom ett lokalt nät, för att visa informationen används främst en webbrowser och webbserver. Organisationerna C och D använder XML i deras system där C använder detta mellan de olika systemen för att transportera data för att kunna presentera den på ett bra sätt. Några av de tekniker som används är följande:

6 Presentation av intervjusvar

Organisation A använder webbrowser och kan visa Asp sidor samt java applets för att göra det möjligt. Organisation B använder förutom webbrowser ett litet separat program som tar hand om larmhanteringen. Detta kan, när mailet är korrekt utformat skicka informationen till behörig användare via sms. Organisation E vet inte vad det finns förutom web server men informationen finns tillgänglig via deras hemsida för användarna.

Hur kan ni garantera att de olika parterna som har blivit godkända att få tillgång till web servicen eller den lagrade informationen verkligen får det?

- *Har ni några riktlinjer för tillgång till web servicen?*

Samtliga organisationer påpekar att de parter som använder tjänsten eller informationen ska mer eller mindre alltid kunna få tillgång till tjänsten eller den lagrade informationen. Organisation A och E pointerar att tillgängligheten som tjänsten ska ha tecknar aktören med de parter som ska använda tjänsten och att den viktigaste funktionen är larmhanteringen. Organisationerna C, D och F kan garantera i den mån det är möjligt att deras egen utrustning, d.v.s. webbserver, fungerar och är tillgängliga över Internet. Organisation F menar att det är svårt att garantera informationen när den har nått Internetgränsen, eftersom det finns en annan infrastruktur där.

Anser ni att informationen som skickas är känslig och behöver skyddas?

- *På vilket sätt är informationen känslig?*
- *Hur skyddar ni informationen?*

Samtliga organisationer hävdar att informationen inte är direkt känslig eller utgörs av kritisk data. Organisation D påpekar att det största hotet som finns är möjligheten att kunna ändra i systemen. Generellt handlar den skickade informationen om skötsel av fastigheter och dylik information som kan relateras till dessa system. Alla organisationer använder ett eller flera olika skydd för att skydda informationen, det vanligaste skyddet är inloggning. Organisationerna C och F använder även skydd som brandväggar och kryptering. Organisationen B menar att informationen som skickas inte är lika känslig som den informationen som en användare kan komma åt inom systemet och påpekar att det finns önskemål om att göra systemet säkrare.

Finns det något skydd som gör att informationen inte kan modifieras under sändningen, i så fall vilket?

- *Vad skulle kunna hända om informationen ändrades under sändningen?*

Fyra av de tillfrågade organisationerna B, C och D anser sig inte ha något direkt skydd för att förhindra att information modifieras under sändningen och kan därför ses som ett problem. Flera av organisationerna kan ställa in tillåtna gränsvärden i systemet vilket kan förhindra att extrema värden kommer in. Bara en av organisationerna (F) påpekar att de inte kan garantera att något kan hända, använder dock skydd som SSL för att förhindra att informationen ska kunna ändras.

Konsekvensen av vad ett förändrat meddelande kan få, skiljer sig i mellan organisationerna och det främsta exemplet är att organisation B hävdar att om larmailen skulle förändras skulle det kunna leda till stora problem.

Finns det möjlighet att förneka att information har skickats till mottagaren?

- *Finns det någon anledning till att göra detta eller inte?*

Tre av organisationerna A, C, och E påpekar att det inte finns någon anledning till att förneka att informationen har skickats, eftersom alla händelser loggas i systemet. Organisation B, D och F påpekar att det kan finnas möjlighet till att förneka att informationen har skickats, dock hävdar B att de inte ser någon anledning till att göra detta. Organisation D och F påpekar att eftersom inte systemen lagrar händelserna går det därför att förneka, denna funktion är troligtvis något som kommer att läggas till i systemet.

Anser ni att det existerar några externa hot för web servicen i organisationen, i så fall vilka?

- *Vad är externa hot för er organisation?*
- *Vad används för skydd eller åtgärder mot dessa?*

Samtliga organisationer är överens om att det existerar externa hot för deras tjänst, en av organisationerna (E) påpekar dock att de inte anser att det finns några direkta externa hot. Organisationen D påpekar att de vanligaste är att tjänsten bara är intern och är därför inte lika utsatt, dock ökar kravet om tjänsten ska vara tillgänglig över Internet. De hot som har kommit fram är följande: obehörigt intrång, virus och hackning. Samtliga organisationer använder sig främst av inloggning, dock är andra skydd som brandväggar, viruskydd, kryptering och vpn-tunnlar förekommande.

Anser ni att det existerar några interna hot för web servicen i organisationen, i så fall vilka?

- *Vad är interna hot för er organisation?*
- *Vad används för skydd eller åtgärder mot dessa?*

Tre av organisationerna A, E, F anser inte att det finns några direkta interna hot för deras tjänst och övriga organisationer definierar främst följande: misskötsel, sabotage och att användare slarvar. Det främsta skyddet som används av samtliga organisationer är inloggning, en av organisationerna (F) drar en parallell mellan de externa och de interna hoten och använder därför samma skydd för dessa.

7 Analys

I detta kapitel kommer först kategorierna att presenteras och motiveras som intervjusvaren blev uppdelade i. Kategorierna kommer att presentera det material som associeras till dessa, samt att en analys av det presenterade materialet kommer att presenteras. Därefter kommer en sammankoppling till W3C:s riktlinjer att presenteras utifrån de kategorier som kan härledas till dessa, kapitlet kommer att avslutas med en sammanfattande analys av intervjuundersökningen och rapportens undersökning. Analysen kommer att utgå ifrån det presenterade materialet som återfinns som bilaga 2.

Arbetets undersökning genomfördes på sex olika organisationer som är aktiva inom fastighetsautomationsbranschen genom utveckling, installation och underhåll. Samtliga organisationer har besvarat de ställda frågorna utifrån ett genomfört projekt eller andra tjänster som respondenten har tyckt passa bättre in på intervjufrågorna. De som kommer att redovisas är främst de som har varit relevanta för problemställningen, för mer utförliga svar hänvisas till sammanställningen av intervjuerna som återfinns i bilaga 2 och sammanfattningen i kapitel 6.

7.1 Kategori

Efter genomgång av undersökningens intervjuer har följande kategorier skapats utifrån intervju svaren. Anledningen till att kategorierna togs fram var att vissa av de ställda frågorna berörde samma information. Det kändes därför naturligt att sammanställa svaren till en kategori i stället för att presentera dem separat. Kategorierna kommer att innehålla en sammanställd presentation av relevanta intervju svar. Det kommer även att finnas en analysdel efter varje presenterad kategori.

De framtagna kategorierna kommer här nedan att presenteras och motiveras för att under kapitel 7.2 presentera det framarbetade resultatet och analysen:

- **Utveckling:** Syftet med denna kategori är att försöka att belysa och uppskatta utvecklingen av web services inom fastighetsautomationen samt att försöka definiera hur denna teknik kommer att användas inom den här branschen.
- **Fördelar/nackdelar med web services:** Syftet med denna kategori är att samla in de för- och nackdelar som organisationerna anser att web services har för deras bransch. Informationen kommer sedan att användas för att försöka klassificera respondenternas syn och för att kunna sammanställa samtliga för- och nackdelar som har framkommit.
- **Tillgänglighet:** Är en sammanslagning av frågorna 1 och 2 av intervjudel 2. Syftet med denna sammanställning är att jag har försökt att i fråga nr 1 få information om hur tillgänglig tjänsten ska vara för de personer som använda den. För att sedan i fråga 2 få information om hur väl organisationerna kan garantera att tjänsten är det.
- **Information:** Är en sammanslagning av frågorna 3, 4 och 5 på den andra intervjudelen. Orsaken till sammanställningen är att dessa frågor berör den informationen som web servicen använder och skickar. För att lättare kunna presentera en enhetlig bild kommer dessa frågor att presenteras tillsammans.

- **Externa hot:** Syftet med denna kategori är att ta upp de olika externa hoten som organisationerna anser existera. För att lättare kunna presentera organisationernas samtliga hot på ett enhetligt sätt kommer därför detta att göras under denna punkt. Information om vilka skydd eller åtgärder som används för att eliminera dessa hot kommer också att redovisas.
- **Interna hot:** Denna kategori behandlar samma information som den ovanstående punkten, fast i relation till de interna hoten som kan existera. För ytterligare information se externa hot.

7.2 Analys av de utvalda kategorierna

De sex framtagna kategorierna kommer att presentera informationen som intervjuerna har kommit fram till. Informationen kommer att presenteras under den kategori som anses bäst passa in på innehållet. Varje kategori kommer att lyfta fram de viktigaste aspekterna, efter varje avslutad kategori kommer en reflektion att göras på innehållet.

7.2.1 Utveckling

Samtliga organisationer är överens om att utvecklingen inom web service och webbtekniken håller på att utvecklas inom deras bransch och att det finns en rad olika positiva förändringar som håller på att ske. Organisation A påpekar att det är tekniken som är ny och inte applikationerna då deras bransch redan på 70-80-talet kunde fjärrstyra enheter via modem. En av fördelarna med tekniken är att kunna styra en maskin utan en fysisk kabel mellan anläggningarna. *"Inom vår bransch finns det en klar vilja att kunna distribuera ut insamlad information på ett enkelt sätt. Det sker genom en ökning av integrationen mellan de olika systemen som använder sig av förbestämda standarder"* anser organisation C. Genom att använda XML kommer det att bli mycket enklare med provningar, adresseringar, programmering, driftsättningar och framför allt visualiseringar över nätet, anser organisation E. Ytterligare en aspekt som organisation E tror kommer få stor betydelse i framtiden är att det kommer att bli möjligt att få upp flödet från varje komponent, och kan då få det som en finansiell rapport. Två av organisationerna D och F lyfter fram utvecklingen av dataservern "OPC" som är en branschstandard och används inom fastighetsautomation för att hämta data från styrdatorer. OPC har tidigare varit D.COM baserat men de nya standarderna är SOAP och XML baserade och använder web services. Troligtvis kommer OPC mer att handla om hur man definierar en web service, samt hur den kommer att se ut och fungera.

Till den sammanställda bilden av utvecklingen av web services inom fastighetsautomation har samtliga organisationer tillsammans lyft fram aspekter som talar för att deras bransch som helhet har börjat acceptera detta. Trots organisationernas skilda åsikter om utvecklingen kan helheten ändå sammanfattas som att branschen ser flera områden där web services kommer att kunna underlätta. En av orsakerna till varför samtliga organisationer har skilda åsikter om utvecklingen och var web services kommer att vara användbara, kan vara de skillnader som existerar mellan dessa organisationer. En av de skillnaderna kan vara att vissa organisationer enbart köper in och modifierar enheter, och andra organisationer utvecklar egna program och system. Ytterligare faktorer kan vara om organisationen tillhandahåller egna tjänster till sina kunder eller om tjänsterna är associerade med det

installerade systemet. Informationen om fastighetsautomation som presenterades i kapitel 2.7 visar klart att branschen har börjat använda redan existerande standarder och IT-lösningar, och att det finns potentiella fördelar med detta. Utvecklingen kommer därför troligtvis att påverka branschen genom en ökning av web services. Detta för att web services enligt Tsalgatidou och Pilioura (2002) möjliggör för organisationer kan flytta sina huvudoperationer till webben för att nå ökad automatisering, snabbare affärsprocesser och global tillgänglighet. Som var den största orsaken till varför Internet utvecklades till tjänstewebben enligt (Ryman, 2000). På grund av utvecklingen som web services har kommer även denna teknik med stor sannolikhet att påverka och underlätta för organisationer inom fastighetsautomation som strävar efter att nå ökad automatisering, snabbare affärsprocesser och global tillgänglighet. Med stor sannolikhet kommer denna förändring att innebära för organisationerna att de för- och nackdelar som togs upp i kapitel 2.7 kommer att förstärkas. Detta genom att den geografiska begränsningen för informationen och flexibiliteten kommer att öka, nackdelen som har tillkommit inom fastighetsautomation genom att använda sig av existerande standarder inom IT-branschen kommer med användning av web services att öka behovet av säkerhet. Detta främst för att informationen kommer att bli mer tillgänglig och sårbar, vilket ökar kraven på en standardisering av säkerheten inom web services. För en mer sammanställd bild över vad utvecklingen av web services inom fastighetsautomationsbranschen kommer att resultera i se kapitel 8.2.

7.2.2 Fördelar/nackdelar med web services

Samtliga organisationer är överens att fördelarna med att använda web services inom fastighetsautomation är fler än de nackdelar som kan associeras till tekniken. Det är främst tre organisationer som har tagit upp aspekter som kan uppfattas som negativa. Organisationerna B och C påpekar att en nackdel med att öppna upp sina system för att göra funktioner mer tillgängliga d.v.s. webbaserat, är att säkerhetstänkandet måste öka då risken för intrång och hackning kan öka. Ytterligare en nackdel inom fastighetsautomationen enligt organisation F är att tidskritiska system kan vara svåra att implementera med web service. Detta eftersom protokollet är ”pratigt” och svårt att packa i. Några av de fördelar som har framkommit menar organisation A kan vara att använda sig av öppna standarder och att det inte är nödvändigt att göra installationer på klienterna. Genom att kunna investera på ett ställe påpekar organisation C att det finns stora möjligheter att hålla nere investeringskostnaderna för kunderna och att dessa kan ta del av den teknik och investeringen som organisationen har gjort. Detta kommer troligtvis även att effektivisera för kunden genom minskad teknik och kravet på egna system. Tillgängligheten kommer att öka främst genom att kunna genomföra implementeringar i Microsofts dot.Net i stället för att göra det i OPC som är betydligt svårare, de anser organisation D vara en av de främst fördelarna med tekniken. Detta då webbtekniken är framtidens teknik och kommer att utvecklas mycket mer. Organisation E tror att de kommer att påverka deras bransch i och med att webbtjänsterna kommer att öka genom att koppla ihop olika typer av tjänster som i dag redan finns i de systemen vi installerar. Fördelarna är att tekniken är väl definierad och enkel att använda sig av från alla typer av miljöer och kan därför ses som en vedertagen standard som kommer att vara mycket stark i framtiden.

Till den sammanställda bilden av organisationernas syn på de för- och nackdelar som kan associeras till begreppet web services inom fastighetsautomation kan följande

slutsatser göras: att dessa skiljer sig mellan samtliga organisationer. Troligtvis kan skillnaderna i åsikterna spegla huruvida organisationen använder tjänsten och systemet samt syftet med funktionen. Den sammanslagna bilden är dock att fördelarna som kan relateras till web services är betydligt fler än nackdelarna och borde innefatta att web services har klara fördelar som är önskvärda inom fastighetsautomation. De få nackdelar som har tagits upp bör inte förkastas i den mån att dessa inte anses som viktiga, detta eftersom en av nackdelarna som har tagits upp berör säkerhetstänkandet. Denna aspekt speglar därför svårigheterna med att tillämpa en tillräcklig hög säkerhetspolicy för att eliminera de eventuella hoten. Detta är just en av de nackdelar som Eriksson (2002) presenterade i kapitel 2.5 som berör komplexiteten med att använda web services för organisationer genom att öppna upp sina system för att dessa ska bli tillgängliga utifrån. Nackdelen kan även associeras till den nackdel som togs upp i kapitel 2.7 som beskriver fastighetsautomation, att ökningen av standarder inom IT-branschen leder till ett större behov av säkerhetstillämpningar. För en mer sammanställd bild över de respektive för- och nackdelar som kan anses vara de viktigaste och som har framkommit efter undersökningen se kapitel 8.2.

7.2.3 Tillgängligheten

Samtliga organisationer betonar vikten av att tjänsten och informationen alltid ska vara tillgängliga för de grupper som använder denna tjänst eller information. Organisation B betonar dock att vissa delar kan påverkas negativt om systemet eller delar av detta havererar, dock ska grundfunktionerna alltid vara tillgängliga. Generellt tecknar aktören ett avtal med de parter som ska använda tjänsten och i detta avtal specificeras även riktlinjer och garantier om tjänstens tillgänglighet. Organisationerna A och B anser att de viktigaste vitala funktionerna är övervakningen och larmhanteringen. Organisationerna C och F kan garantera i den mån det är möjligt att deras webbservrar alltid fungerar och är tillgängliga för de grupper som använder tjänsten. Organisation F betonar även att det är viktigt att webbservern står i rätt förbindelse med Internet och att det är svårt att garantera informationen när den har nått Internetgränsen eftersom det finns en annan infrastruktur där.

Den sammanställda bilden över organisationernas syn på den tillgängligheten som tjänsten eller informationen ska ha är att den alltid ska vara tillgänglig för användaren. Generellt brukar aktören teckna ett avtal med de parter som ska använda tjänsten eller informationen och kan då sätta upp de riktlinjer och krav som ska finnas. Endast två av organisationerna kan garantera i den mån det är möjligt att tillgängligheten på tjänsten inte försämras, detta genom att övervaka och drifthålla sitt eget system. Orsaken till varför de övriga inte har betonat detta kan troligtvis vara att deras tjänster skiljer sig från dessa samt att organisationerna C och F tillhanda har tjänster till fastighetsägaren över Internet.

7.2.4 Information

Samtliga organisationer anser inte att informationen som skickas är extremt känslig och utgör därför inte ett stort potentiellt hot. Dock finns det flera olika aspekter som organisationerna har tagit upp vilket har påverkat organisationerna i den mån att samtliga använder någon eller några typer av skydd för att kunna säkerställa informationen. Flera av organisationerna använder inloggning för att skydda informationen, organisationerna C och F använder även brandväggar och SSL för att

uppnå en högre säkerhet. Av de tillfrågande organisationerna är det bara C och F som använder något typ av skydd för att informationen inte ska modifieras under sändningen. Skyddet som används är kryptering d.v.s. SSL. Organisation C pointerar vikten av att kunna säkerställa informationen och menar att ett förändrat meddelande kan få förödande konsekvenser, dock betonar C och D att många system har vissa tillåtna gränsvärden detta kan ses som ett extra skydd. Tre av organisationerna påpekar att det inte finns möjlighet att förneka att informationen har skickats eftersom alla händelser loggas automatiskt i systemet. Av de övriga organisationer existerar det en tveksamhet till frågan och där organisation B hävdar att det kanske finns möjlighet att förneka sändningen av informationen men ser ingen anledning till detta. Den enda organisationen som i dag hävdar att det går att förneka är D eftersom händelser inte lagras i systemet men det är en funktion som troligtvis kommer att läggas till.

Samtliga organisationer anser inte att informationen som skickats är extremet känslig, dock har alla organisationer ett eller flera olika skydd för att säkerställa informationen. Eftersom organisationerna använder olika skydd borde följande slutsats kunna göras, synen på informationen och de olika åtgärderna som kan användas skiljer sig åt. En av orsakerna till detta kan vara att även tjänsterna sinsemellan skiljer sig åt, samt ifall tjänsten är åtkomlig över Internet eller inom ett lokalt nätverk. Några av de skydd som organisationerna använder är inloggning, lösenord, brandväggar och kryptering samt att många system inom fastighetsautomation kan ha förinställda gränsvärden. Synen på informationen och de eventuella skydd som kan användas för att säkerställa informationen har visat sig att de två organisationer som tillhandahåller tjänster till kunderna har vidtagit en högre säkerhetsåtgärd. Detta genom att använda kryptering SSL. Som enligt DeJesus (2001) kan skydda mot eventuella hot som "snooper attacker" och "denial of service attack" vilket resulterar i att tjänsten och organisationen får en högre säkerhet. Med all sannolikhet minskas även risken med att informationen kan försvinna eller modifieras när den skickas över Internet från en organisation till en annan, är aspekter som påpekas av (Gopalakrishnan och Rajesh, 2003). Av de tillfrågade organisationerna är det bara ett fåtal som använder system som loggar händelser och kan därför inte förneka att information skickats. Svaret på varför det skiljer sig mellan organisationerna kan kanske vara uppbyggnaden i systemen och organisationerna.

7.2.5 Externa hot

Samtliga organisationer är överens om att det existerar externa hot för web servicen, dock skiljer sig synen på vad detta hot innefattar. Organisation D påpekar att det vanligaste är att tjänsten och funktionerna bara är tillgängliga inom ett internt nätverk, och är därför inte lika utsatta för externa hot men att hotbilden ökar när tjänsterna är åtkomliga över Internet. Den gemensamma hotbilden för organisationerna är att obehöriga kan komma in i systemet d.v.s. "hackning", sabotage eller virus, och de kan få olika typer av konsekvenser beroende på säkerheten som organisationen har. Organisation E menar att de inte anser att dessa tjänster är attraktiva för någon annan än de som använder den, men understryker inte nödvändigheten av skydd. Samtliga organisationer använder ett eller flertal olika skydd för att försäkra sig om att en maximal säkerhetsnivå tillämpas. De skydd som samtliga använder är främst brandväggar och inloggning, andra skydd som existerar är virusskydd och det används av organisationerna B, C, E och F. Den enda organisationen som använder sig av kryptering är C, och har även skärmat av hårdvaran för organisationen för att uppnå ytterligare säkerhet. Organisation D tror att de kommer att använda VPN-tunnel för

att koppla upp automationsutrustningen som finns i fastigheterna för att få en högre säkerhet.

På grund av att samtliga organisationer har lyft fram faktorer som kan anses vara externa hot borde därför följande slutsats kunna dras: att det existerar externa hot inom automationsbranschen för deras web services. Dock varierar synen på dessa hot. Eftersom synsätten har varit olika angående de externa hoten är det därför naturligt att de åtgärder som dessa organisationer har använt sig av för att eliminera hoten och uppnå en hög säkerhet skiljer sig. Vilket bekräftar Baker (2002), påstående att det inte existerar någon direkt standard för säkerheten inom web services. Utan att det är upptill organisationen själva att avgöra vad för typ av säkerhets tillämpning som organisationen tror sig behöva (Eriksson, 2002). Genom att endast använda tjänsten inom ett lokalt nätverk kan det, enligt Ratnasingam (2002), minska risken med de problem som kan uppstå över Internet, detta främst för att tjänsten inte blir tillgänglig utanför det egna nätet. Några av de tänkbara attacker som DeJesus (2001) lyfte fram i kapitel 2.6 kan ett av de skydd som organisationerna använder d.v.s. krypteringsmetoden SSL vara ett fungerande skydd för både ”snooper attacker” och ”denial of service attack”.

7.2.6 Interna hot

Tre av organisationerna A, E och F anser inte att det direkt existerar några interna hot för web servicen eller för organisationen dock har samtliga lyft fram aspekter som kan relateras som hot. Organisationerna A och E anser att interna hot kan relateras till slarv och manuella fel eller att en användare gör för mycket förändringar eller nedladdningar på distans in i systemet som har en negativ inverkan. Även organisationerna B och C anser att interna hot kan relateras till misskötsel och misstag. Organisation B påpekar även att aspekter som sabotage eller att någon kommer in fysiskt i systemet för att förstöra är allvarligare än andra hot. De åtgärder som organisationerna har tagit fram för att skydda sina tjänster är varierande, dock använder majoriteten av organisationerna inloggning som det främsta skyddet, organisation C använder även behörighetsnivåer för att kunna begränsa möjligheten för användarna. Den organisation som skiljer sig från de övriga är F som har lyft fram att de använder samma skydd för de interna hoten som för de externa och kan sammanfattas vara följande: viruskydd, brandväggar och inloggning. Organisation B anser att säkerhetsaspekter är ett stort problem inom alla organisationer och branscher, men att det inom fastighetsautomation oftast finns intern säkerhet som är låst inom applikationsutrustningen och som inte är påverkningbar från en dator. Detta kan ses som ett extra skydd som ökar möjligheten att skydda applikationsutrustningen.

Av den sammanställda bilden från de tillfrågade organisationerna och deras syn på existerande hot för web servicen samt de eventuella skydd som används har svaren varierat i den bemärkelsen att organisationernas syn skiljer sig från varandra. Den sammanslagna bilden av de interna hot som existerar kan sammanfattningsvis utgöras av händelser som kan relateras främst till skötsel och underhåll. Av de sex tillfrågade organisationerna var det bara tre som lyfte fram en annan aspekt som kan innefatta sabotage eller förstörelse. Av dessa två framkomna aspekterna kan därför följande slutsatser dras att synen på existerande interna hot skiljer sig mellan organisationerna och deras åtgärder för att minimera dessa hot.

7.3 Sammankoppling av kategorier till W3C:s riktlinjer

Av de framtagna kategorierna från kapitel 7.1, kan följande kategorier: *Tillgänglighet*, *Information*, *Externa hot* och *Interna hot* sammanfattningsvis beröra de framtagna riktlinjerna från W3C, som presenterades i kapitel 2.6. Av det presenterade materialet och analysen av dessa kategorier i kapitel 7.2 kan därför följande slutsatser dras huruvida organisationer inom fastighetsautomationsbranschen kan uppfylla de kriterier som W3C har tagit fram. För mer information om W3C:s kategorier se kapitel 2.6. Sammankopplingen mellan dessa kategorier och riktlinjerna presenteras nedan:

Tillgänglighet: avser att undersöka de två första punkterna av riktlinjerna. Av dessa kan följande slutsatser dras: samtliga organisationer anser att tjänsten och informationen alltid ska vara tillgänglig. De eventuella riktlinjer som avser att uppfylla tillgängligheten tecknar organisationerna oftast med de kunder som använder tjänsten. De organisationer som tillhandahåller tjänster till kunden har en högre säkerhetsaspekt för att kunna garantera detta. På grund av att organisationerna anser att tjänsten alltid ska vara tillgänglig kan denna punkt anses uppfylla W3C:s två första kriterier.

Information: avser att undersöka punkterna 3, 4 och 5 av riktlinjerna. Av kategorin kan följande slutsats dras att organisationerna inte direkt anser att informationen är känslig. De åtgärder som kan skydda informationen både under sändning och från att modifieras är skydd som SSL. Detta används dock inte av samtliga organisationer och därför anses dessa punkter inte kunna relateras till W3C. För att organisationerna inte ska kunna förneka att informationen har skickats måste systemet automatiskt lagra de händelser som inträffar, denna aspekt kan inte heller uppnås av samtliga organisationer och anses därför inte kunna relateras till W3C.

Interna hot: avser att undersöka den första aspekten av punkt 6 av riktlinjerna. Eftersom W3C inte har definierat vad interna hot kan vara samt vilka eventuella skydd som är nödvändiga, antas detta därför vara upp till respektive organisation att själva avgöra. De eventuella slutsatser som kan dras är att organisationerna anser att det existera aspekter som kan relateras till interna hot. Synen på vad interna hot innefattar är inte enhetlig. Detta gäller även de nödvändiga åtgärder eller skydd som kan vidtagas för att oskadliggöra hoten. På grund av detta anses inte denna punkt direkt kunna efterstävas inom fastighetsautomationsbranschen.

Externa hot: avser att undersöka den andra aspekten i punkt 6 av riktlinjerna. Eftersom inte denna punkt heller har definierats av W3C, kan även denna aspekt vara upp till respektive organisation att lösa. På grund av att samtliga organisationer anser att externa hot existerar samt att de eventuella åtgärder som används varierar, anses inte heller denna riktlinje kunna efterstävas inom fastighetsautomationsbranschen.

Efter dessa kopplingar som har redovisats, anses det att W3C:s riktlinjer inte direkt kan uppfyllas av organisationer inom fastighetsautomationsbranschen. Detta behöver nödvändigtvis inte betyda att organisationerna inte har tillämpat en tillräckligt hög säkerhetsnivå eller att det existerar ett flertal direkta svagheter i dessa organisationer och tjänster. Detta främst för att W3C inte tar upp vad dessa riktlinjer kan ha för betydelse eller vad konsekvensen skulle kunna bli i fall inte någon eller samtliga punkter kan uppfyllas. Trots slutsatsen att organisationerna inte direkt kan uppfylla W3C:s riktlinjer betyder inte det att dessa inte kan vara relevanta för organisationer inom branschen. Eftersom det inte existerar någon bakomliggande information kan

det därför tolkas att respektive organisation får utgå ifrån vad de anser är nödvändigt och kan då använda dessa riktlinjer mer som en mall i strävan att säkerställa sina tjänster och organisation.

7.4 Sammanfattande analys av intervjuundersökningen

Undersökningen som genomfördes är inte felfri i den bemärkelsen att undersökningen inte skulle kunna ha gjorts annorlunda. Valet att ta kontakt med sex organisationer inom automationsbranschen för att sedan genomföra undersökningen kan ha varit för få, resultatet som framkommit kan därför troligtvis skilja sig från ett mer omfattande arbete. På grund av de begränsningar som arbetet har i tid och omfattning skulle det inte ha varit möjligt att genomföra en större omfattande undersökning. Samtliga organisationer har visat ett stort intresse för undersökningen och arbetet, främst för att många organisationer i dag använder Internet och att de ser en stor fördel med att använda sig av detta och de tekniker som kan härledas till detta.

Av de undersökta organisationerna visade det sig att begreppet web services var relativt främmande och att det varierade mellan organisationerna i deras åsikter och tankar om detta begrepp. Alla organisationer har i dag någon typ av webbaserad tjänst som de anser har en högre funktionalitet och syfte än en vanlig webbtjänst. Av de sex organisationer som var delaktiga i undersökningen var det främst tre som direkt ansåg att de använde sig av web services på något sätt. Trots detta resultat har samtliga organisationer valts att användas i rapporten, detta på grund av att samtliga organisationer har liknande tjänster med samma funktionalitet. Samt att definitionen på web services av Pagina, (2003) förklarar begreppet enbart som ett nytt kommunikationssätt, för mer information se kapitel 2.2.

Dock har denna information som framkommit under och efter processen därmed bidragit till en större osäkerhet i det insamlade materialet. Dessvärre resulterade även första intervjun i en väldigt dålig ljudupptagning som kan ha resulterat i att felaktiga tolkningar gjordes. Troligtvis hade dessa aspekter som framkommit minimerats om en mer detaljerad förundersökning hade gjorts inom fastighetsautomationsbranschen innan undersökningen hade påbörjats. Detta hade kanske kunnat påverka undersökningen genom att problempreciseringen hade omformulerats och i stället utgått ifrån fastighetsautomationsstandarder och tekniker som kan associeras till web services. Främsta orsaken till varför inte problempreciseringen och strukturen på rapporten har gjorts om, är främst för att web services associeras till Internet-teknologi och att utvecklingen har skett utifrån Internetstandarder. Dessvärre hade nog inte dokumentationen av intervjuerna varit möjlig att påverka. Detta främst för att utrustningen testades noggrant innan den första intervjun genomfördes. Trots detta upplägg uppstod de tekniska problem som påverkade dokumentationen.

7.5 Sammanfattande analys av undersökningen

Efter undersökningen och analysen av det presenterade materialet, har följande slutsatser gjorts för att besvara den presenterade problemställningen, för mer information om problemställningen se kapitel 3.1. Av de kategorier som undersökningen resulterade i kommer de viktigaste resultaten att redovisas under respektive kategori.

Utveckling:

Utvecklingen av web services och webbtekniken inom fastighetsautomation kan sammanfattas med att dessa tekniker håller på att utvecklas inom deras bransch och att det finns en rad olika positiva förändringar som håller på att ske. Några av de fördelar som organisationerna kan få är t ex att kunna styra en maskin utan en fysisk kabel mellan anläggningarna samt att XML kommer att förenkla provningar, adresseringar, programmering, driftsättningar och framför allt visualiseringar över nätet. Inom branschen finns det en klar vilja att kunna distribuera ut insamlad information, detta kan förenklas genom en ökning av integrationen mellan de olika systemen, genom att använda förbestämda standarder. Ytterligare en aspekt är att dataservern OPC som är en branschstandard har utökats med de nya standarderna som XML, SOAP och web services.

För och nackdelar med web services:

De fördelar som organisationerna inom fastighetsautomation associera till begreppet web service är fler än de nackdelar som kommit fram. De aspekter som kan relateras till fördelarna kan sammanfattningsvis vara användning av öppna standarder, minskande investeringskostnader, ökad tillgänglighet och lättare att implementera klienter. Ytterligare en fördel är att web services är väl definierat och enkel att använda sig av från alla typer av miljöer och att det verkar vara en vedertagen standard. De nackdelar som har associerats till web services inom fastighetsautomation är främst behovet av ökade säkerhetsaspekter. En annan aspekt är att det är ett ganska "pratigt" protokoll rent bandbreddmässigt, d.v.s. mycket bits som ska skickas över nätet som måste packas in d.v.s. hög overhead som kan göra tidskriftiska system svåra att implementera.

Tillgänglighet:

Organisationerna betonar vikten av att tjänsten och informationen alltid ska vara tillgänglig för de grupper som använder denna tjänst eller information. De eventuella riktlinjer eller kraven som finns för tjänsten brukar bestämmas när aktören tecknar avtal med de grupper som ska använda tjänsten. De organisationer som tillhandahåller egna tjänster till kunder kan i den mån det är möjligt garantera tillgängligheten på tjänsten.

Information:

Samtliga organisationer anser inte att informationen är direkt känslig eller utgör ett direkt hot, dock skyddas informationen genom ett eller flera skydd. De olika skydden som används är inloggning, lösenord, brandväggar och kryptering samt att det ofta är möjligt inom fastighetsautomation att ställa in gränsvärden i applikationerna. För att kunna förhindra modifiering av meddelanden används enbart kryptering. Det enda sättet för organisationerna att inte förneka att information har skickats är i fall systemet loggar händelserna.

Externa hot:

Samtliga organisationer är överens om att det existerar externa hot för tjänsten. De eventuella hoten som organisationerna har betonat är obehöriga i systemet, hackning, virus samt sabotage. För att säkerställa tjänsten och systemen använder organisationerna några olika skydd för att minimera de eventuella hoten som kan förekomma. Åtgärderna som används kan sammanfattas vara brandväggar, inloggning, virussydd och kryptering.

Interna hot:

Det som har uppfattas vara interna hot för organisationerna inom fastighetsautomation kan sammanfattas enligt följande. Att bilden av de interna hot som existerar för dessa tjänster och organisationer utgörs främst av händelser som kan relateras till skötsel och underhåll. Dessa händelser kan utgörs av slarv, manuella fel, för hög grad av nedladdningar, misstag och misskötsel. De åtgärder som organisationerna använder är främst inloggning, virussydd och brandväggar. Inom fastighetsautomation existerar det även ofta intern säkerhet som är låst inom applikationsutrusningen och som inte är påverkingsbar från en dator. Detta kan ses som ett extra skydd som ökar möjligheten att skydda applikationsutrustningen.

Sammankoppling av kategorier till W3C:s riktlinjer:

Av de framtagna kategorier som intervjufrågorna resulterade i som är avsedda för att undersöka huruvida W3C:s riktlinjer kan tillämpas inom fastighetsautomationsbranschen. Följande slutsatser framkommit nämligen att av de sex riktlinjerna var det främst riktlinje 1 och 2 som direkt kunde uppfyllas av organisationerna inom den utvalda branschen. De övriga riktlinjer anses inte kunna uppfyllas av organisationerna och främsta orsaken till detta är skillnaderna mellan organisationerna. På grund av att W3C inte har definierat respektive riktlinje och att riktlinjerna är utformade så att en organisation måste kunna "garantera" respektive punkt kan dessa anses vara för hårda. Trots denna reflektion kan W3C:s riktlinjer troligtvis ändå fungera som en mall för organisationerna i deras strävan att utveckla och använda sig av web services inom fastighetsautomation.

8 Resultat och reflektion

I detta kapitel kommer de resultat som har framkommit av undersökningen att presenteras. De kommer att besvara rapportens problemprecisering. Kapitlet kommer även att reflektera över vad resultatet kan betyda samt ge en reflektion över rapportens process. Kapitlet kommer att avslutas med att ge några förslag till fortsatta studier.

För att besvara ”hur hanteras web services inom fastighetsautomation utifrån W3C:s riktlinjer” som är rapportens huvudproblemprecisering, har dessa riktlinjer legat som grund för intervjufrågorna, svaren har sedan kategoriserats för att lättare kunna presenteras. Författarna Hondo, et al. (2000) betonar vikten av att en organisation måste vara medvetna om de risker som kan finnas och uppstå för web services inom en organisation. Detta kan göras genom att en säkerhetsmodell skapas över hur dataflödet kan gå i en web service. Denna säkerhetsmodell skulle kunna vara W3C:s riktlinjer som behandlar säkerhet men som även kan fungera som en mall för utveckling och användning av web services (Gopalakrishnan och Rajesh, 2003).

8.1 Hur tillämpas W3C riktlinjer?

Sammanfattningsvis kan följande slutsatser göras att organisationernas syn på W3C:s riktlinjer inte är enhetlig och kan därför betyda att synen på säkerheten och tillämpningarna skiljer sig mellan dessa. Troligtvis beror detta på ett flertal olika aspekter, vilket även bekräftar det förväntade resultatet att skillnader skulle finnas inom branschen. En av faktorerna är skillnader mellan organisationerna och tillämpningarna i deras tjänster samt i fall tjänsten är åtkomlig över Internet eller inte. Andra faktorer kan vara tjänstens placering d.v.s. om den är placerad i fastighetsautomationssystemet eller hos organisationen, där den används ut till systemet. Dessa organisationer som tillhandahåller tjänster ut till kunden har vidtagit en högre säkerhetsnivå än de övriga, vilket troligtvis beror på att kunderna köper dessa tjänster och organisationerna vill kunna säkerställa dessa. Åtgärderna som organisationerna använder borde därför vara utifrån deras syn tillräckliga för att säkerställa sina tjänster och organisationer dock existerar det en önskan om en standardiserad lösning på säkerheten. Vilket skulle underlätta för organisationerna att höja säkerheten för deras web services och organisationer.

Trots denna slutsats kan W3C:s riktlinjer ändå anses vara av intresse för organisationer inom fastighetsautomationsbranschen eftersom dessa kan användas för utveckling och användning av web services. För att organisationer ska kunna få en ökad säkerhet måste medvetenheten om säkerheten och de eventuella hot som finns öka. Detta skulle bland annat kunna uppnås genom att tillämpa dessa riktlinjer.

8.2 För- och nackdelar med web services?

Organisationernas sammanslagna bild över de eventuella för- och nackdelar som kan associeras till web services inom fastighetsautomation, bekräftar det förväntade resultatet. Detta för att de positiva aspekterna som kom fram var fler än de negativa, dock berör en av de negativa aspekterna säkerheten inom web services. Vilket ytterligare bekräftar problematiken med säkerheten och behovet av en standardiserad lösning. Detta skulle underlätta för organisationer att implementera och säkerställa

8 Resultat och reflektion

sina tjänster och organisationer. Några av de för- och nackdelar som kommit fram kan sammanfattas vara följande:

Fördelar som kan associeras till web services inom fastighetsautomation:

- Användning av öppna standarder.
- Minskande investeringskostnader.
- Ökad tillgänglighet.
- Lättare att implementera klienter.
- Väl definierat och enkelt att använda sig av från alla typer av miljöer och att det verkar vara en vedertagen standard.

Nackdelar som kan associeras till web services inom fastighetsautomation:

- Ökande säkerhetsaspekter.
- Tidskritiska system kan vara svåra att implementera med web services på grund av att protokollet är stort och måste packas för att skickas över nätet.

8.3 Utveckling av web services inom fastighetsautomation?

Det råder ingen tvekan om att utvecklingen av IT-tekniken och användningen av dessa standarder vilket kan omfatta web services inom automationsbranschen är väl användbar och kommer att påverka branschen som helhet. Svaret på denna fråga bekräftar det förväntade resultatet om att det finns en utveckling av web services inom fastighetsautomation och att utvecklingen associeras främst till positiva förändringar.

Några av de positiva aspekterna som kan följa med utveckling av web services och dessa standarder kan sammanfattas vara följande:

- Styra en maskin utan en fysisk kabel mellan anläggningar.
- XML kommer att underlätta bland annat provningar, adresseringar, programmering, driftsättningar och framför allt visualiseringar över nätet.
- Ökad integration mellan systemen.
- Branschstandarder har utvecklats med SOAP, XML och web services.

Utvecklingen av web services inom fastighetsautomationsbranschen kommer med all sannolikhet att erbjuda organisationer ökad automatisering, snabbare affärsprocesser och global tillgänglighet. Detta kommer troligtvis för web services att resultera i ett öka behovet av säkerheten inom organisationerna, detta främst för att informationen kommer att bli mer tillgänglig och sårbar, vilket ökar kraven på en standardisering av säkerheten inom web services.

8.4 Hur hanteras web services inom fastighetsautomation?

Av de presenterade delfrågorna kan följande slutsats dras för att besvara problempreciseringen: att web services inom fastighetsautomationsbranschen inte direkt kan sammankopplas till de riktlinjer som W3C har tagit fram som berör

8 Resultat och reflektion

säkerheten. Det råder ingen tvekan om att utvecklingen av web services inom branschen kommer att öka de närmaste åren och att utvecklingen associeras främst till fördelar. Synen på de för- och nackdelar som kan relateras till web services inom branschen är övervägande fördelar. Dock belyser samtliga frågor säkerhetsaspekter som kan relateras till web services och den ökande användningen av Internet-standarder vilket starkt betonar behov av en standardiserad säkerhet för web services.

8.5 Vad betyder resultatet

Resultatet som rapporten har presenterat under kapitel 8.4 kan därför följande slutsatser deras för att besvara vad resultatet betyder. Dessa aspekter kan sammanfattningsvis beröra tre punkter, där den första punktens konsekvenser kommer att leda till de två andra punkterna. Dessa aspekter är följande:

- Utvecklingen av web services inom fastighetsautomationsbranschen kommer att erbjuda organisationer ökad automatisering, snabbare affärsprocesser och global tillgänglighet.
- Informationen kommer att bli mer tillgänglig och sårbar, vilket ökar kraven på en standardisering av säkerheten inom web services.
- Resultatet och undersökningen bekräftar problemet med att det inte finns en standardiserad säkerhetslösning för web services.

8.6 Reflektioner

Undersökningen och resultatet som jag har kommit fram till kan ha påverkats av några olika faktorer. En sådan faktor kan vara min tolkning av begreppet web service som är ett stort begrepp och parallellt jag drog till fastighetsautomationsbranschen, vilket är ett område där det i dag sker stor förändring och utveckling. I dag känns inte denna bransch fullt mogen för att göra en undersökning som rapporten genomförde och detta kan därför ha resulterat i felaktiga slutsatser. Undersökningen som genomfördes och som ligger som grund för slutsatsen av rapporten kan anses ofullständig, de olika faktorer som har påverkat undersökningen är främst att begreppet web services inte direkt används inom den undersökta branschen. Samt att organisationernas osäkerhet till innebörden av begreppet är stort. Ytterligare en faktor som kan ha påverkat undersökningen och slutsatsen i rapporten kan ha varit beslutet att använda samtliga organisationer, trots att tre organisationer inte direkt kunde medge att de använde sig av web services. Undersökningen samt resultatet skulle ha kunnat vara annorlunda om arbetet och undersökningen hade utgått ifrån begrepp och standarder som existerar inom den undersökta branschen. Informationen som har bearbetats vid sidan av intervjuerna visar tydligt att branschen som helhet går mer mot standarder och tillvägagångssätt som används inom renodlade IT-lösningar i stället för att utveckla egna tillämpningar och standarder. Det råder ingen tvekan om att web service kan komma att påverka fastighetsbranschen som helhet, men det är i dag för tidigt att dra slutsatser om vilken omfattning och tillämpning som detta IT-relaterade begreppet kommer att få.

8 Resultat och reflektion

Valet att använda intervjustudie i undersökningen kan räknas som lyckat främst eftersom en större helhetsbild har kunna skapas utifrån de grupper som deltog i undersökningen. Ytterligare en fördel som kan associeras till valet av metod är att undersökningen lyckades lyfte fram aspekter som visar att det existerar en stor variation av organisationer inom branschen. De främsta skillnaderna är organisationernas arbetssätt och deras specialisering. Dessa två skillnader kan vara ifall organisationen enbart bygger upp ett system till kunden eller om organisationen även kan erbjuda tjänster som kunden kan använda efter implementeringen. Det framkom även en skillnad mellan hur mycket utveckling som organisationerna hade samt ifall majoriteten av systemen implementeras och användes lokalt eller över Internet. Förmodligen hade inte denna information framkommit på samma sätt om en annan metod hade använts i undersökningen.

Resultatet som har framkommit av undersökningen och som har presenterats styrker de problem som kan associeras till säkerheten inom web services och betonar att det är nödvändigt att en standardiserad lösning på säkerheten kan tillkomma. För information om de problemen som associeras med säkerheten se kapitel 2.6.

Trots de olika faktorer som har tagits upp och som kan ha påverkat undersökningen och slutsatsen på ett missvisande sätt, anser jag att slutsatsen ändå kan vara av intresse för aktörer inom fastighetsautomationsbranschen. Mycket på grund av att rapporten belyser några av de eventuella problem som kan uppstå och finnas vid användning av web services. Förhoppningsvis kan rapporten bidra till att organisationer inom fastighetsautomationsbranschen kan få en ökad medvetenhet av de säkerhetsrisker som finns associerade till web services.

Främsta orsaken till varför inte organisationerna ansågs uppfylla W3C:s riktlinjer är för att riktlinjerna inte är definierade och att de är formulerade på ett sådant sätt att en organisation ska kunna garantera dessa. Vilket kan vara svårt för en organisation att kunna uppfylla samtliga riktlinjer när de är formulerade på detta sätt. För mer information om W3C:s riktlinjer se kapitel 2.6, 7.3 och 8.1. De framtagna riktlinjerna från W3C kan naturligtvis bidra till vägledning både när det gäller säkerhetstänkande, utveckling och användning av web services. Detta kan vara extra viktigt eftersom branschen håller på att förändras och att det finns aspekter som pekar på en stark utveckling av web services och en ökad användning av Internetstandarder. För organisationer inom fastighetsautomationsbranschen kommer denna utveckling att innebära att de kan flytta flera huvudoperationer till webben för att nå ökad automatisering, snabbare affärsprocesser och global tillgänglighet.

Resultatet och slutsatsen av rapporten om *hur hanteras web services inom fastighetsautomation* är troligtvis inte specifik för enbart denna bransch utan kan relateras till andra organisationer inom olika branscher. Detta för att web services är det nästa naturliga steget för organisationer som stävar för att nå ökad automatisering, snabbare affärsprocesser och global tillgänglighet. För att detta ska få den genomslagskraft som många hoppas på måste en standardiserad säkerhetslösning för web services tillkomma, detta för att organisationerna ska kunna säkerställa sina web services.

8.7 Framtida studier

Eftersom begreppet web service är relativt nytt och kan tillämpas på flera olika sätt kan en framtida studie inom ramen av rapporten vara att i stället utgå ifrån de

8 Resultat och reflektion

standarder och tekniker som existerar inom den undersökta branschen. Eftersom det finns många skillnader och likheter mellan dessa tekniker och begreppet web services, kan det vara intressant att se vilka skillnader eller likheter som faktiskt existerar. Eftersom ämnesområdet i rapporten är stort men har begränsats till att undersöka problemställningen som presenterades i kapitel 3.1, kan därför ett flertal olika framtida arbeten tänkas för de områden som rapporten inte har tagit upp. Några av dessa områden skulle kunna vara framtida aspekter för web services som t ex utveckling eller nya standarder inom web services. Skulle även kunna tänkas att en studie kring de tekniska aspekterna på begreppet skulle vara av intresse för aktörer som vill implementera web services.

Referenser

Andersen, E.S. och Schwenche, E., (1998) *Projektarbete- en vägledning för studenter*. Studentlitteratur i Lund.

Baker, S., (2002) *Web Services and CORBA*. LNCS. 2519, pp. 618-632.

De Jesus, E., (2001) *Security implications of Web Services*.

Tillgängligt på Internet:
<http://www.webservicesarchitect.com/content/articles/deJesus01.asp>
[Hämtad 03.03.02]

Eriksson, I., (2002) *CIO-Sweden – Web services*. Nov2002, Vol. 4, pp. 20-27.

Glass, G.,(2000) *The Web services revolution: Part 1*.

Tillgängligt på Internet: <http://www-106.ibm.com/developerworks/webservices/library/ws-peer1.html>

Gottschalk, K., Graham, S., Kreger, H., och Snell, J., (2002) *Introduction to Web services architectur*. IBM systems journal, vol. 41, Issue 2, pp. 170-177.

Gopalakrishnan, U och Rajesh Kumar, R., (2003) *Web services security, part 1*.

Tillgängligt på Internet: <http://www-106.ibm.com/developerworks/webservices/library/ws-sec1.html>
[Hämtad 03.03.14]

Hondo, M., Nagaratnam, N., och Nadalin, A., (2002) *Securing Web services*. IBM systems journal, Vol. 41, Issue 2, pp. 228-241.

Leymann, F., (2001) *Web Services and their composition*.LNCS 2077, pp.1

Mohan, C., (2002) *Dynamic E-business: Trends in Web Services*. LNCS.2444, pp. 1-5.

Nationalencyklopedin, (1995) Höganäs: Bokförlaget Bra Böcker AB.

Pagina., (2003) Tillgängligt på Internet: <http://pcforall.idg.se/tjanster/dataordboken/>
[Hämtad 03.02.25]

Patel, P och Bo Davidsson, B., (1994) *Forskningsmetodikens grunder att planera, genomföra och rapportera en undersökning*. Studentlitteratur i Lund.

Ryman, A., (2000) *Understanding web services*.

Tillgängligt på Internet:
<http://www7.software.ibm.com/vad.nsf/Data/Document4362?OpenDocument&p=1&BCT=3#>. [Hämtad 03.02.25]

Ratnasingam, P., (2002) *The importance of technology trust in web services security*. Information & computer security. ,pp. 255-260

Referenser

Tsalgatiidou, A., och Pilioura, T., (2002) *An Overview of Standards and Related Technology in Web Services*. Vol. 12, pp. 135-162.

Bilaga 1

Del 1: Inledande frågor

Namn på respondent:

Företagsnamn:

Storlek:

Befattning inom företaget:

Arbetsuppgift:

De inledande frågorna ställdes för att ge information som namn på respondent, personens befattning och arbetsuppgift inom företaget. Svaren på dessa frågor kommer att användas i presentationen av organisationerna i kapitel 5.2. Syftet med dessa inledande frågor är att få veta respondentens kunskaper och erfarenhet inom undersökningens område.

Del 2:

1. Använder er organisation i dag någon typ av webbtjänst?

- *På vilket sätt är tjänsten uppbyggd och hur fungerar den?*

Frågan ställdes för att få information om organisationen i dag har någon typ av webbtjänst samt hur denna tjänst är uppbyggd och fungerar. Syftet med frågan är att undersöka om organisationens webbtjänst är eller använder sig av web services på något sätt.

2. Vad är begreppet web service för er?

- *Anser ni att er webbtjänst är en web service varför/varför inte?*
- *Hur ser utvecklingen ut inom er bransch gällande webbaserade tjänster?*

Frågan ställdes för att ge en klarare bild över hur organisationen har tolkat begreppet web service och huruvida organisationen anser att deras webbtjänst är en web service eller inte. För att få en insikt i hur webbaserade tjänster inom automation och fastighetsbranschen ser ut ställdes därför den sista delfrågan.

3. Vilka för/nackdelar anser ni att det finns med att använda web service?

Frågan ställdes för att försöka få fram de för - respektive nackdelar som kan förknippas med begreppet web service inom fastighetsautomation. Syftet med frågan är att få information för att lättare kunna definiera branschens syn på web services.

4. Vilka får ta del av informationen i organisationen?

- *Hur begränsas tillgängligheten av information av web servicen?*

Frågan ställdes för att kunna definiera vilka som har rättigheter eller inte till informationen, samt hur organisationen har begränsat tillgängligheten på denna. Syftet med frågan är se hur organisationen resonerar kring tillgängligheten av informationen.

5. Beskriv organisationen kortfattat?

Syftet med varför frågan ställdes var för att ge en klarare bild över vad organisationen gör.

Del 3:

1. Hur tillgänglig är tjänsten och informationen för de parter som använder web servicen?

- *Vad är det för typ av information som tjänsten visar?*
- *Hur kan informationen visas?*
- *Vilka tekniker använder ni för att göra det möjligt?*

Frågan ska besvara hur tillgängligheten är på informationen och tjänsten för de grupper som använder sig av denna tjänst. För att få mer information om tjänsten och informationen ställdes delfrågorna som förhoppningsvis bidrar till en bättre helhetsbild. Syftet med frågan är för att i fråga 2 försöka definiera om dessa parter verkligen kan få tillgång.

2. Hur kan ni garantera att de olika parterna som har blivit godkända att få tillgång till web servicen eller den lagrade informationen verkligen får det?

- *Har ni några riktlinjer för tillgång till web servicen?*

Syftet med frågan är att försöka koppla svaret från fråga 1 för att se om organisationen verkligen kan garantera att dessa får tillgång till tjänsten, samt få information om de riktlinjer som kan finnas för detta.

3. Anser ni att informationen som skickas är känslig och behöver skyddas?

- *På vilket sätt är informationen känslig?*
- *Hur skyddar ni informationen?*

Syftet med frågan är att få information om hur känslig organisationen anser att informationen är som skickas. Delfrågorna ska försöka att lyfta fram varför organisationen tycker att den är känslig samt vilka eventuella skydd som används för att skydda informationen.

4. Finns det något skydd som gör att informationen inte kan modifieras under sändningen, i så fall vilket?

- *Vad skulle kunna hända om informationen ändrades under sändningen?*

Frågan ställdes för att få svar på om organisationen använder något skydd som förhindrar att informationen förändras under sändning samt eventuella konsekvenser som ett förändrat meddelande kan ha.

Bilaga 1

5. Finns det möjlighet att förneka att information har skickats till mottagaren?

- *Finns det någon anledning till att göra detta eller inte?*

Syftet med frågan är att undersöka om organisationen på något sätt kan styra eller påverka händelser som har inträffat, samt att få information om orsaken till detta.

6. Anser ni att det existerar några externa hot för web servicen i organisationen, i så fall vilka?

- *Vad är externa hot för er organisation?*
- *Vad används för skydd eller åtgärder mot dessa?*

Frågan ställdes för att få information om organisationen anser att det existerar några externa hot för web servicen. För att bättre kunna definiera hoten samt se vilka åtgärder eller skydd som organisationen har tillämpat ställdes delfrågorna.

7. Anser ni att det existerar några interna hot för web servicen i organisationen, i så fall vilka?

- *Vad är interna hot för er organisation?*
- *Vad används för skydd eller åtgärder mot dessa?*

Syftet med frågan är att få information om organisationen anser att det existerar några interna hot för web servicen. För att bättre kunna definiera de interna hoten samt se vilka åtgärder eller skydd som organisationen har tillämpat ställdes delfrågorna.

Bilaga 2

Använder er organisation i dag någon typ av webb tjänst?

- *På vilket sätt är tjänsten uppbyggd och hur fungerar den?*

Organisation A: Använder en webbsida, java applets och på andra sidan finns det en soft pc styrning. Tjänsten innehåller bland annat styrning av t ex fläktar detta via ett webbgränssnitt. Går även att styra och samla in värden, som databasen loggar. Är främst styrparametrar, användaren kan koppla upp sig online för att se dynamiska värden i realtid kan även spela in värden över temperaturer. Kan även gå och titta på historiska värden kan få ut för att jämföra olika tider per år att se på.

Organisation B: Använder det systemet som jag håller på att bygga upp. Fastighetsägaren har ett antal fastigheter där vissa lokaler används för bland annat forskning, inom dessa existerar det bland annat känslig utrustning. För att garantera att lokalerna är funktionella rent tekniskt sätt används ett webbaserat intranät, för att övervaka och styra t ex klimat, larmhantering och luftflöden samt säkerhet som skalskydd. För att få en slimmad organisation finns det mycket teknik i husen för att t ex hantera hissar, larm, klimat, skalskydd och brandlarm. Vi har kopplat upp dessa mot de lokala webbserverna som finns i husen. Om man surfar in på dem kan man ta del av den informationen som finns i automationsutrustningen. Dessa samlar in klimatdata som temperatur, fukt och luftflöden lokalt i webbservern och skickar ner det till en SQL-server som är placerad centralt och loggar data. För att kunna hantera alla de olika webbserverna finns det en portal som tar emot email och kollar varifrån det kommer, om det är något viktigt kan portalen vidarebefogade meddelandet till jourpersonalen. Distributionen sker ofta via sms-meddelande. Det finns även en vanlig webbserver som är publicerad ut mot Internet som man går in på först via portalen därifrån kan man sedan slussas ut till de lokala webbserverna i husen. Jourpersonalen ska snabbt kunna gå in och kolla hur det är via Internet, är dock inte helt utvecklat än. Håller på att arbeta med detta för att göra det ännu enklare och mobilare. Tanken är att kunna ha ett övervakningssystem i fickan. Genom att öppna upp kan vissa personer surfa in på utvalda delar inom systemet. Webbserverna i husen är alla olika och kan ses som specifika. Dessa skickar ut larm och loggdata och svarar på förfrågningar samt visar informationen via webbfönster. En anledning till att öppna upp mot Internet är bland annat för att hyresgästen ska kunna komma åt informationen på valda delar om de är berättigade till det.

Organisation C: I dag erbjuder vi främst övervakningstjänster till våra kunder som omfattar larmhantering. Vi har system som är uppkopplade ut till ett antal fastigheter som får in information som t ex driftdata och larm. Detta sker genom att kunden har en dator som företaget kopplar upp sig mot. Uppkopplingen kan ske både över Internet eller modemuppkoppling beroende på kundens önskemål. Tjänsten gäller främst övervakning av de olika styrsystemen som finns i fastigheterna och vid ett larm kan detta skickas ut i form av sms eller mail till de olika servicebolag som organisationen använder. När ett larm genereras tar styrsystemen kontakt med huvuddatorn, där en del av denna är en webbserver som speglar ut informationen på Internet. För att kunden ska få kontakt med sitt system måste den kontakta företagets

Bilaga 2

webbserver som är uppkopplad mot hårdvaran i fastigheterna. I några fall använder vi även Vpn tunnlar in mot olika fastighetsnäten.

Organisation D: Finns bara ett fall som använder tjänsten ut över Internet, det vanligaste är att bygga upp ett intranät i fastigheten där det finns några styrdatorer som är kopplade i ett nätverk. Systemet har en webbserver och i den finns även en dataserver som kommunicerar med styrdatorerna genom att man kan hämta och skicka data ner till dem. Denna tjänst kan även läggas ut på Internet och skötas därifrån, annars går det bara att göra på det lokala nätverket, eller via en ras-koppling som innebär att man via modem ringer upp.

Organisation E: Systemen som vi säljer är uppkopplingsbara mot webben och de tjänster som vi har till systemen är webbaserade, där webben kan ses som ett visualiseringsverktyg och mediabärare av informationen. Tjänsterna som finns är styrning och övervakning av fastigheter, men framför allt energiövervakning. Styrsystemet i fastigheten skickar information automatiskt som ASCII-kod via ett SMTP-meddelande till programmet, deras server lägger upp informationen i en rapport på nätet till kunden eller oss beroende på vem som sköter driften. Är kanske inte en ren webbtjänst men vi använder webben som ett verktyg. Vi sätter även upp fastigheterna på nätet, vilket gör att kunden kan komma åt informationen, vi gör installation av systemet och även hemsidan, detta kallar vi "WDC" d.v.s. webbdatorcentral.

Vi installerar ett styrsystem som kan kopplas upp till Internet, vi kan sedan koppla upp oss till detta system via en Bredbandsanslutning. Varje fastighet är sedan en egen hemsida för att man ska kunna ta del av informationen. Centralt i huset sätter vi upp en "vcd" som innehåller en industri pc med Linux programvara som automatiskt konvertera informationen i fastigheten till en förstålig hemsida ute på nätet. Vi har en dynamisk IP-adress för att underlätta uppkopplingen. Genom Internet kan vi komma åt denna fastighet utan att behöva ha några specialprogram.

Organisation F: När det gäller webbtjänster har vi några olika produkter som vi kan implementera. För små installationer har vi en inbyggd webbserver i ett "imbedded" system, som kopplas till mindre system och fastigheter, för att kunna surfa in och ta del av fastighetens status, samt påverka klimat. Vi har även en variant för större system med samma funktioner som har en pc-baserad server. Där kan man på samma sätt surfa in och göra ändringar. Vi har även en annan lösning på en webbtjänst som kan vara mer intressant att utgå ifrån, denna tjänst riktar sig främst mot beslutfattare hos fastighetsägaren. Detta för att få fram en övergripande bild över hur fastigheten sköts och drivs som t ex energiförbrukning och larmstatistik m, m. Detta använder vi även för kommunikation med kunden, för att förmedla information. Tjänsten har vi utvecklat själva från grunden och är utvecklad för våra kunder i Skandinavium. Vi har en server placerad i företaget och används

Tjänsten är uppbyggd med en Oracle databas där all information finns, systemet som är byggt på databasen står i förbindelse med våra automationssystem ute hos kunderna, kan vara både våra inbyggda eller pc-system. Denna hämtar in t ex loggkurvor, eller uppmätta värden ute i fastigheterna, tar in larm-statistik osv. Informationen lagras på servern för att antingen först presenteras på webben för

Bilaga 2

användarna eller kan våra experter processa data. Detta görs för att bland annat säkerställa systemet, informationen blir sen tillgänglig för användaren

Vad är begreppet web service för er?

- *Anser ni att er webb tjänst är en web service varför/varför inte?*
- *Hur ser utvecklingen ut inom er bransch gällande webb baserade tjänster?*

Organisation A: Web services är för mig något som rör sig dynamiskt där användaren kan manövrera och påverka t ex en fläkt i Skövde men befinna sig i Lund, mot att bara söka efter HTML-dokument. Det finns en skillnad mellan web services och webbtjänster, vi anser att vi har web service. Utvecklingen: Trenden är inget nytt däremot är median ny, t ex bredband, intranät, anslutning mellan orter och företag in till maskiner. I vår bransch kunde vi redan på 70-80 talet fjärrstyra enheter via modem. Tekniken är ny inte applikationerna, den har gett möjligheten att kunna styra en maskin utan att behöva ha en fysisk kabel mellan anläggningarna.

Organisation B: Kopplar begreppet web services hårt till dot.Net och kan ses som en motsvarighet till Microsoft vanliga tjänster fast i webbmiljö där en server har en tjänst som är kopplad mot webbtrafiken. Vi anser inte direkt att vår webbtjänst är en web service, men har dock stora förhoppningar att det ska bli det på sikt. Genom att man kan hitta en standardiserad modell som organisationer kan använda sig av i utvecklingen av sina tjänster. Vi tror att det kommer att bli web services i framtiden och hoppas att det kommer att lösa många problem som existerar inom webbaserad fastighetsövervakning. Idag har inkompatibilitet d.v.s. att man kan underlätta att ta över från en annan aktör, lättare upphandlingar och komplettera befintliga system. I dag är det en djungel. Varje enskild webbserver ute på plats lever i sin egen värld, man kan göra stora vinster genom att kunna föra över data mellan olika webbservrar och olika fabrikat. Kan man då transportera signaler eller data och göra saker emellan med automatik vore det en väldigt bra. Det finns i dag en vilja hos fastighetsägarna och folk runt omkring att integrera systemen i varandra, detta är möjligt tack var utvecklingen inom Internet och dessa standarder. Web services kan verkligen vara till nytta i integreringen av de olika systemen, detta kan komma att spela en stor roll eftersom det oftast finns information på flera ställen som måste slås samman för att få en bättre helhets bild.

Organisation C: Är ett nytt begrepp men har tolkat det som att kunna erbjuda mer automatiserade webbtjänster av olika slag. Vår webbtjänst är i dag en tjänst ut mot Internet där en vanlig klient kan surfa in och göra vissa förbestämda funktioner. Vi tror inte att vår webbtjänst är en web service, begreppet är nytt och det finns en osäkerhet på vad begreppet web services innefattar och betyder för vår bransch. Inom vår bransch finns det en klar vilja att kunna distribuera ut insamlad information på ett enkelt sätt. Svårt att säga i vilken form web services kommer att ha för fastighetsbranschen. Men hoppas att integrationen mellan olika system kan öka genom att använda sig av förbestämda standarder.

Bilaga 2

Organisation D: Vi använder inte direkt det i vår applikation däremot skulle man kunna använda det för att hämta data från de olika styrdatorerna som t ex energiförbrukning eller kanske kunna skriva ner ett börvärde till applikationen. Det finns en standard inom vår bransch som heter OPC som är en dataserver, en generell API för att hämta data från styrdatorer oavsett vad man har för något i systemet. Standarden OPC håller på att ta fram en standard för att kunna hämta data i XML-format. Vi tror att det kommer bli mer web services i framtiden och att XML kommer att bli stort inom fastighetsautomation. En väldigt bra web services för oss skulle vara om våra leverantörers prislista på teknik och system skulle kunna uppdateras i XML-format över Internet via ren HTTP.

Organisation E: Om vi tittar på vad vi säljer är det just det t ex statistik, rapporteringar och såna bitar och tillgängligheten på nätet. Ja det tycker jag på sätt och vis, det beror på vad man menar vi bygger ingen portal i dag som kunden kan logga in på utan säljer den tillsammans med vår partner. Har i dag inlett ett samarbete med ett företag som säljer utrustningar där vi kommer att använda deras portal för att få in kalkylpriser, anbud eller kunna beställa programmerade enheter. Detta kommer att betyda att vi använder deras portal mer eller mindre för att göra vårt jobb, eller delar av vårt. Vi kan t ex om vi har en standardfunktion i en fastighet t ex ett luftbehandlingsaggregat som behöver automatiseras kan jag gå in och logga in med vårt företagslösenord få/kunna beställa en burk direkt eller alternativt begära en offert och få priset och få leveransinformationen direkt till oss via mail.

I vår bransch kommer det att komma som nästa steg, för varje produkt eller komponent kommer att bli lättare att nå och skala, när man bygger dynamiska bilder är det java applets som man jobbar med i dag. Tror att XML kommer att slå igenom för det kommer att bli mycket enklare med provningar, adresseringar, programmering, driftsättningar och framför allt visualiseringar över nätet. Kommer att kunna få flödet från varje komponent upp, så att man kan få det som en finansiell rapport.

Organisation F: Vår webbtjänst är nog inte en web service enligt min definition. Som jag ser det är web service något som gör att informationen och innehållet blir tillgängligt för andra system att kunna kommunicera med. Detta gäller främst system till system kommunikation än system till människa. Vi har i dag system till system kommunikation men är inte baserad på SOAP och XML som är den gängse definitionen på web service begreppet. Fast på ett sätt är det vi använder förresten, vi har SOAP och XML kommunikation mellan vår centralserver och våra installerade system ute hos kunderna. Detta används bara för den interna kommunikationen och inte till kunden eller något annat. Vi tror att det är på stark frammarsch verkar vara den enda gemensamma nämnaren för Java och Dot.Net och göra att dessa två kan kommunicera på ett lätt sätt. Vi har märkt att Distributed Component Object Model (DCOM) fungerar bäst på lokala nätverk och är ganska svåra att använda den tekniken över andra typer av nätverk. Internet ställer helt andra krav på vad som ska användas. OPC har tidigare varit DCOM baserat men de nya standarderna är SOAP och XML-baserade och använder även web services. Det finns ingen motsats till OPC och web services som vi ser det, utan OPC kommer mera att handla om hur man definierar hur web services kommer att se ut och fungera, det är som jag ser det d.v.s. OPC är ett protokoll ovanför web services. Vi planerar att börja använda detta mer i framtiden.

Vilka för/nackdelar anser ni att det finns med att använda web service?

Organisation A: Ser enbart fördelar om man gör det på rätt sätt d.v.s. att man använder sig av öppna standarder. En stor fördel är att man slipper i regel att göra installationer på klienterna hos användaren om man håller strikt på att inte installera specialprogram.

Organisation B: Anser inte att det existerar några klara nackdelar, dock tillkommer en säkerhetsaspekt när man öppnar upp system för att göra funktioner mer tillgängliga d.v.s. webbaserade. De risker som ökar är främst intrång.

Organisation C: Finns klara fördelar genom att man kan hålla ner investeringskostnader för kunderna genom att man investerar på ett ställe, kunderna kan sedan ta del av tekniken och investeringarna som vi har gjort. Det kommer troligtvis att effektivisera även för kunderna genom att de slipper ha egna system och att tekniken kan minskas, vilket underlättar både implementation och driften av de olika systemen. Nackdelar är klart säkerhetsaspekter när man börjar distribuera ut system vilket kan öka risken för t ex hackning. Det är viktigt att man ställer högre krav och tänker på säkerheten i alla leden, nackdelen är dock att detta är väldigt dyrt.

Organisationen D: Den största fördelen som vi ser med web services är främst tillgängligheten och att det kommer att bli lättare att implementera klienter i t ex dot.Net än att göra det i OPC där det är ganska komplext. En nackdel skulle vara om klienten måste fråga servern eller om servern kan rapportera förändringar till klienten. Eftersom HTTP protokollet som används i dag inte är uppbyggd att förändringar kan skickas automatiskt, detta kan belasta nätverket eftersom uppdateringar kan ske två gånger i sekunden med 100 dynamiska värden. I D.COM kan man skicka information vid händelse och det finns även en callback funktion hos klienten. Vi vet dock inte om det går att skriva händelseuppdateringar i web services i dag.

Organisation E: Finns inga direkta nackdelar inom vårans bransch, webbtekniken är en framtidens teknik. Den kommer troligtvis att utvecklas mycket mer och vi kommer nog att använda webbtjänster mer. Vårans bransch kommer troligtvis inom en snar framtid att få flera tjänster över Internet. Web services är för mig någonting som kan utnyttjas på någon portal över nätet. Portal kan exempel vara en dator eller en hemsida. De typer av tjänster som finns kommer att öka genom att man kan koppla ihop olika typer av tjänster som i dag redan finns som kan kopplas ihop med de systemen som vi installerar.

Organisation F: Fördelarna är att det är ganska väl definierat och enkelt att använda sig av från alla typer av miljöer och att det verkar vara en vedertagen standard som kommer att vara mycket stark i framtiden. Nackdelen är att det är ganska "pratigt" protokoll rent bandbreddmässigt, det är ganska mycket bits som ska skickas över nätet som måste packas in d.v.s. hög overhead som gör tidskriftiska system svåra att implementera med hjälp av web service.

Vilka får ta del av informationen i organisationen?

- *Hur begränsas tillgängligheten av information av web servicen?*

Organisation A: Informationen ligger öppet i systemet, alla kan surfa dit och titta men för att ändra behöver man logga in och ha behörighet.

Organisation B: Hela förvaltningsorganisationen samt vissa av hyresgästerna som bor och arbetar i husen får ta del av informationen. För att kunna begränsa vissa delar av informationen i systemet har olika behörighetsnivåer med inloggning byggts in. Andra åtgärder är brandväggar, isa server, certifikat, https, 128 bitar kryptering. Vi börjar prata om att använda oss av en ”pinkodsos” dock minskar detta användarvänligheten och kan då försämra systemet eftersom de måste vara enkla. Det finns en avvägning mellan säkerhet och användbarhet.

Organisation C: De kunder som har köpt tjänsterna kan komma åt informationen i en behörighets hierarki via inloggning.

Organisation D: De användare som har fått behörighet att använda systemet har tillträde till den via inloggning med behörighetsnivåer. Detta sker via en lokal webbinloggning i det lokala nätverket som är kundens egna nät. Klienterna i huset är sällan inkopplade fysiskt på samma nätverk, vi har byggt upp ett separat fastighetsnät och på det nätet ligger webbservern.

Organisation E: Alla får ta del av informationen, är främst teknikerna i företaget som arbetar med systemet och tekniken. Detta sker via inloggning med fyra olika nivåer: titta, service, användare och system underhåll dessa har olika inloggningar och lösenord. Slutkunden får bestämma vilka som ska ha tillträde till systemet. Ofta är vi med under garantiperioden som brukar sträcka sig normalt två år. Vi tecknar även service avtal med våra kunder, och övervakar sedan detta via webben för att se till att det är optimalt.

Organisation F: Den informationen som samlas in från de installerade systemen ute i fastigheterna sparas i vårans databas och informationen skickar med SOAP. Informationen är tillgänglig för våra interna experter i organisationen och slutkunderna som finns utanför organisationen. Informationen som är tillgänglig inom organisationen skiljer sig från den informationen som kunden får, detta för att vissa värden måste bearbetas och behandlas innan den kan vara tillgänglig för kunden. Genom detta kan experterna få fram värdefull information och dra slutsatser om hur systemet fungerar som annars inte skulle vara möjligt att få fram av kunden. När kunden loggar in kan denna se systemets status och eventuella åtgärder som är nödvändiga eller möjliga att genomföra.

Bilaga 2

1. Hur tillgänglig är tjänsten och informationen för de parter som använder webbservicen?

- *Vad är det för typ av information som tjänsten visar?*
- *Hur kan informationen visas?*
- *Vilka tekniker använder ni för att göra det möjligt?*

Organisation A: Tjänsten och informationen ska alltid vara tillgänglig för de parter som använder denna tjänst, informationen som visas är främst tekniska värden som mätvärden, reglerparametrar och drifttillstånd i grafiska bilder. Alla som stöder webbläsare kan visa ASP sidor, java applets.

Organisation B: Tjänsten och informationen i systemet ska alltid vara tillgänglig, vissa delar kan dock påverkas negativt om något går sönder eller ner, dock ska grundfunktionerna alltid vara tillgängliga. Informationen som visas är främst information om klimat, status på säkerhetsfunktioner samt olika personlarm som t ex hisslarm. Tekniken som gör det möjligt att visa informationen är främst Webbbrowser, det finns ett separat program för själva larmhanteringen. Larmen kommer in via webbserven och tas omhand av programmet, när mailet är korrekt utformat kan information skicka vidare via sms till behörig person.

Organisation C: Tjänsten och informationen ska alltid vara tillgänglig. Informationen som tjänsten visar är de parametrar som t ex larm, aktuella driftdata som temperatur, driftstatus, historik m, m och visas över webben. Tekniker som används är asp, HTML-programmering, databas, webbrowser, server. XML används mellan de olika systemen för att transportera över data för att kunna presentera den på ett bra sätt. Generellt visas informationen i textform men det går även att visa informationen som interaktiva bilder, då används flash där XML hanterar indata.

Organisation D: Tjänsten och informationen ska alltid vara tillgänglig, i detta fall har vi satt upp klienter i alla apparat rum där fläktar och pumpar står. Användaren kan starta Internet Explorer och kan då komma åt aktuella data i realtids värden, uppdateringar sker två gånger per sekund. Det går även att se larm, trender och loggar hur temperaturen har varit under en tid. Informationen visas grafiskt. Servern har XML och använder COM-objekt för att skapa de dynamiska sidorna som skickas till klienten.

Organisation E: Är alltid tillgänglig när avtalet tecknas kan kunden bestämma hur ofta informationen ska uppdateras och visualiseras, kan lagra gamla rapporter. Dessa kan användas av fastighetsägaren för optimeringssyfte, budget syfte och rapportering samt jämföra olika perioder. Är främst styrparametrar, datavärden och mätvärden från temperaturmätare och uträknade värden. Informationen visas över Internet och finns tillgänglig på hemsidan. Vet inte direkt vad det är för tekniker förutom webbserver.

Organisation F: När en kund skriver kontrakt med oss prenumerera han på den här tjänsten, vi utser en administratör ute hos kunden som får inloggning och lösenord till

Bilaga 2

systemet. Kunden administrerar sedan själv de interna användarna och lägger upp dessa på våran server. Sedan kan varje användare gå in och modifiera hur denna vill ha informationen på sitt eget konto. Den främsta typen av information som visas är energi- och budgetuppföljning när det gäller fastigheterna, larm och underhållningsstatistik och olika typer av rapporter i text eller diagramform. Teknikerna som vi använder är databas-drivna, väderna genereras utifrån databasen automatiskt, de grafiska delar använder vi SVG som är en standard för att visa grafik på webben.

2. Hur kan ni garantera att de olika parterna som har blivit godkända att få tillgång till web servicen eller den lagrade informationen verkligen får det?

- *Har ni några riktlinjer för tillgång till web servicen?*

Organisation A: Tillgängligheten som tjänsten ska ha tecknar aktören med de parter som ska använda tjänsten. Men överlag ska dessa alltid kunna få tillgång till tjänsten och informationen, den viktigaste funktionen är larmhantering där larm kan skickas ut som mail och sms till dem som ska få informationen.

Organisation B: Hyfsat i alla fall, de vitala funktionerna är övervakade och om något händer får man information om vad som är fel, detta sker automatiskt. Riktlinjerna för webbtjänsten är att den alltid vara uppe och igång, detta är väldigt viktigt.

Organisation C: Vi ser till att webbservrar snurrar 24 timmar om dygnet och att de är åtkomliga över Internet, dock är det svårt att garantera på klient-sidan.

Organisation D: Den ska alltid vara tillgänglig, riktlinjerna är att server delen ska fungera då den sköter larmfunktionen och ska helst inte stanna förutom vid service av systemet.

Organisation E: Kunden bestämmer vilka som ska få tillgång till det och våran partner sätter upp detta, vi är mer som en mellan hand som säljer produkten.

Organisation F: Det vi kan garantera är en viss tillgänglighet på webbservern, och att den står i förbindelse med Internet på rätt sätt. Vi har även en egen driftcentral där vi också har våra egna servrar som övervakas dygnet runt. Det är svårare att garantera informationen när den har nått Internetgränsen, eftersom det finns en annan infrastruktur där. Om kunden får problem brukar vi hjälpa till att fixa problemet. Vi vill också kunna garantera att inte fel personer kommer åt informationen, de skydd som används är inloggning och lösenord samt att informationen krypteras med SSL.

Bilaga 2

3. Anser ni att informationen som skickas är känslig och behöver skyddas?

- *På vilket sätt är informationen känslig?*
- *Hur skyddar ni informationen?*

Organisation A: Informationen är inte känslig för att det handlar generellt om skötsel av fastigheter som inte behöver skyddas. Informationen skyddas dock mot utomstående, men det finns inga avancerade tekniker för detta.

Organisation B: Informationen som skickas är inte lika känslig som den informationen som en användare kan komma åt. Eftersom en användare kan gå in och t ex stänga av fläktar eller andra viktiga funktioner i lokalerna. Informationen skyddas främst genom inloggning med användarnivåer i systemet som begränsar användarens möjligheter att modifiera systemet. Finns önskemål om att göra systemet säkrare och vi håller på att ta fram olika alternativ för att få högre säkerhet.

Organisation C: Informationen kan i viss mån vara känslig om man skulle kunna läsa av flöden kan då kanske kunna styra vissa parametrar, detta kräver dock kunskap om systemen. Det främsta skyddet som används är möjligheten att kryptera trafiken med SSL, vi har även brandväggar in mot systemet för att skydda serverna.

Organisation D: Informationen överlag är inte känslig fast möjligheten att kunna ändra är det, informationen skyddas generellt med inloggning. För att kunna göra något i systemet måste man först vara inloggad.

Organisation E: Vi anser inte att den är känslig vi använder Internet som en budbärare. Tekniken har gjort det möjligt att kommunicera och att jobba med komponenter som är uppkopplingbara till TCP/IP. Informationen skyddas främst med inloggning men kan även installera hårdvariga brandväggar i systemen om det skulle behövas. Om vi använder radiolan mellan två byggnader krypterar vi trafiken.

Organisation F: Min personliga åsikt är att det inte är särskild känslig information och att information inte är kritisk som skickas, vi har dock tagit det säkra före det osäkra och erbjuder den nivå av säkerhet som vi har d.v.s. inloggning, brandväggar, lösenord och SSL.

4. Finns det något skydd som gör att informationen inte kan modifieras under sändningen, i så fall vilket?

- *Vad skulle kunna hända om informationen ändrades under sändningen?*

Organisation A: Det är inte relevant om någon skulle påverka mätvärdet innan det skickas, en användare kan inte mata in orimliga värden i systemet för då larmas styrningen.

Bilaga 2

Organisation B: I dag existerar det inget direkt skydd för att förhindra att informationen ska modifieras, dock är alla mailservrarna placerade på insidan av brandväggen. Det finns bara en väg in i systemet d.v.s. ett IP-nummer. Det kan ställa till med stora problem om larmmailen blir modifierad, men om andra värden skulle förändras är det inte lika farligt.

Organisation C: Det existerar inget direkt skydd för att inte kunna modifiera data förutom kryptering. Om informationen skulle ändras skulle det kunna få förödande konsekvenser, dock har många system vissa tillåtna gränsvärden.

Organisation D: I dag existerar det inga skydd för informationen under sändning, det är dock inte bra om ett meddelande skulle förändras under sändningen. Vi kan ställa in gränsvärden i systemet vilket ökar säkerheten.

Organisation E: Systemet loggar alla händelser och inloggningar som inte kan raderas.

Organisation F: Det främsta skyddet som vi använder är SSL, hittills har ingen knäckt det. Det borde inte kunna hända något, däremot går vi inte ut och garanterar detta. Har svårt att tro på att det skulle kunna hända något. Vi anser att det är viktigare att skydda data som ligger lagrad och detta gör vi med Oracle på våran centrala server.

5. Finns det möjlighet att förneka att information har skickats till mottagaren?

- *Finns det någon anledning till att göra detta eller inte?*

Organisation A: Det finns ingen möjlighet att förneka att informationen har skickas eftersom all information lagras i databasen automatiskt

Organisation B: Möjlighet finns kanske att förneka att information har skickats dock ser vi ingen anledning att göra detta.

Organisation C: Kan finnas möjligheter att förneka att information har skickats, dock loggas allt i systemet vilket gör det svårt att efteråt förneka något.

Organisation D: Det går att förneka att information har skickats eftersom systemet inte loggar händelserna, men det är en funktion som vi troligtvis kommer att lägga till.

Organisation E: Det går inte att förneka att informationen har skickats eftersom allt loggas i systemet. Det enda sättet är att förstöra systemet och då förloras informationen. Informationen sparas inte i rörliga hårddiskar utan i fasta minnen t ex flashminnen som bara kan läsas av.

Bilaga 2

Organisation F: Vi kan nog logga händelser och kan då avgöra om någon har varit inne eller de händelser som har skett i systemet. Kommunikationen som sker är mer eller mindre enkelriktade och innebär att systemen där ute skickar in till den centrala servern.

6. Anser ni att det existerar några externa hot för web servicen i organisationen, i så fall vilka?

- *Vad är externa hot för er organisation?*
- *Vad används för skydd eller åtgärder mot dessa?*

Organisation A: Externa hot kan sammanfattas vara människor som inte har behörighet att använda systemen men av någon orsak kommer åt dessa och gör vissa ändringar som kan få olika grader av följder. Skydden som används är främst brandväggar och inloggning.

Organisation B: Externa hot för webbtjänsten är främst hot som intrång, virus samt eventuellt spionage. Inom systemet finns det brandväggar, inloggning och virussydd. En extra säkerhet är att ingen mailtrafik får förekomma utifrån och in.

Organisation C: Externa hot för oss är främst om webbserven blir utsatt för någon extern attack eller virus. Tekniker som används inom organisationen är inloggning, virussydd, brandväggar och kryptering som HTTPS annars används HTTP. Vi har även rent fysiskt skärmat av hårdvaran för att minimera risker som stöld och eventuella katastrofer som brand och vattenskador.

Organisation D: Om tjänsten läggs ut på Internet ökar hotbilden genom hackning, majoriteten av systemen som har byggts upp är interna men önskan att ha det över Internet har ökat den senaste tiden. Tror dock att vi kommer att använda oss av vpn-tunnel med brandvägg för att öka skyddet. Det främsta skyddet är inloggning med behörighets nivåer.

Organisation E: Det är inte den typen av tjänst som vi ser att det existerar några externa hot, är inte attraktiv för någon annan än de som använder den. Vi ser inte att det skulle vara intressant för någon att hacka sig in. Det skulle teoretiskt kunna vara att man kopplar upp denna utrustning på fastighetens interna nät skulle man kanske kunna ta sig in bakvägen in till företagets server om de är kopplade till samma server. Vi brukar sätta upp denna utrustning utanför företagets brandvägg och på detta sätt skydda den med en egen brandvägg. De interna hoten är sabotage och hackning. De främsta skydden som används är inloggning, brandvägg och att webbdatabascentralen har virussydd som uppdateras med jämna mellan rum.

Organisation F: Det skulle kunna vara om andra parter uppgav sig att vara något av våra system och skickar in information som behandlas av vår server är dock långsökt. Andra hot skulle kunna vara hackning och virus. De skydd som vi främst har är virussydd, brandväggar och inloggning.

Bilaga 2

7. Anser ni att det existerar några interna hot för web servicen i organisationen, i så fall vilka?

- *Vad är interna hot för er organisation?*
- *Vad används för skydd eller åtgärder mot dessa?*

Organisation A: Vi ser inga direkt interna hot, men det skulle kunna vara att användare slarvar och gör vissa manuella fel som kan påverka systemet negativt.

Organisation B: Till interna hot räknar vi främst misskötsel av systemet, utebliven service eller sabotage från någon användare. Största hotet är om någon kommer in fysiskt för att sabotera. För att öka säkerheten håller organisationen en låg profil. I dag är inte den interna säkerheten inräknad i organisationens säkerhetspolicy och detta kan ses som ett problem. Generellt är säkerhetsaspekter ett stort problem inom alla organisationer och branscher. Främsta skyddet är inloggning, samt att det finns intern säkerhet som är låst inom applikationsutrusningen som inte är påverkningbar från en dator.

Organisation C: Eftersom systemen även är ihopkopplade i ett internt nätverk, existerar det risker som om någon begår misstag som gör att information kan försvinna, skyddet som finns är främst inloggning med behörighets nivåer i systemet.

Organisation D: Om någon slutar i företaget och vill skada det, samt rena sabotage. I dag finns det ett problem med säkerhetsluckorna i Internets informationsserver vilket kan vara lätt att forcera för att komma in i systemet. Det skydd som vi använder i dag är inloggning.

Organisation E: Vi ser inte att det finns några direkta interna hot för tjänsten. Denna tjänst gör våra anläggningar mera tillgängliga. Det som skulle kunna vara ett internt hot är om någon gör för mycket förändringar eller nerladdningar av program på distans d.v.s. använder systemet för att ladda ner nya applikationsprogram till anläggningen i stället för att befinna sig på plats. Vi har som policy att befinna sig ute på plats för att kontrollera att allt verkligen fungerar. Det som ska göras på distans är injustering av parametrar, förändringar av inställningsvärden och börvärden, kvittering av larm. Nedladdning av program, skulle kunna vara ett internt hot om våra tekniker slarvar. Skydd som används är inloggning.

Organisation F: Vi anser inte att det finns direkt några interna hot, det skulle kunna vara samma som de externa hoten eller om det finns personer inom företaget som vill förstöra något. De skydd som vi använder är de som används för de externa hoten.