INTERNATIONELLA HANDELSHÖGSKOLAN
HÖGSKOLAN I JÖNKÖPING

Integrationsplattformar

Finns det säkerhetsrisker med användandet av integrationsplattformar?

Filosofie kandidatuppsats inom Informatik

Författare: Niklas Bengtsson
Lidia Berhane
Markus Petri
Handledare: Jörgen Lindh

Jönköping December 2006

JÖNKÖPING INTERNATIONAL BUSINESS SCHOOL
Jönköping University

Integration brokers

Are there security issues associated with the use of integration brokers

[Bachelor's thesis within informatics

Author: Niklas Bengtsson
Lidia Berhane
Markus Petri
Tutor: Jörgen Lindh

Jönköping December 2006

Kandidatuppsats inom Informatik

Titel:	**Integrationsplattformar – Finns det säkerhetsrisker med användandet av integrationsplattformar?**
Författare:	**Niklas Bengtsson, Lidia Berhane & Markus Petri**
Handledare:	**Jörgen Lindh**
Datum:	**2006-12-15**
Ämnesord	**Integrationsplattform, SIG Security, EAI, CIA, AAA , SBA**

Sammanfattning

I dagens samhälle ställs det stora krav på att ett företags IT-system skall vara tillgängligt för kommunikation. Kommunikationen kan ske inom och mellan företag. Då dessa kommunicerande aktörer kan ha olika system och arkitekturer som gör det komplicerat att kommunicera med varandra, krävs även någon applikation som hanterar detta problem. Dessa applikationer går under namnet integrationsplattformar. Då dessa plattformar fungerar som ett centralt nav i kommunikationen är det viktigt att säkerheten i dessa är av hög nivå.

Problemet är, *vilka säkerhetsrisker kan tänkas dyka upp vid användandet av integrationsplattformar i ett informationssystem?* Denna fråga ledde oss in på två forskningsfrågor som presenteras nedan:

- Kan denna teknik för applikationsintegration få konsekvenser för säkerheten och i så fall på vilket sätt?
- Hur ser den bakomliggande tekniken för säkerhet ut hos två viktiga integrationsplattformar på marknaden, är dessa likvärdiga så att de säkerhetsrisker som identifieras är giltiga för integrationsplattformar generellt?

Vi började med att definiera termen säkerhet utifrån tidigare kursböcker. När detta var klart kunde vi identifiera potentiella problem som företag kunde ställas inför vid implementation av integrationsplattformar. Därefter använde vi oss av Internet och olika typer av databaser och tidskrifter för att lokalisera fakta och information som behandlar integrationsplattformar för att få en bredare förståelse för hur dessa fungerar. Vi bestämde oss för att använda primärdata vid empiriinsamlingen och valde därför att genomföra intervjuer med leverantörer, tillverkare och kunder av integrationsplattformar för att kunna få olika perspektiv från hela kedjan.

En analys har gjorts av teorin och resultat av intervjun. Analysen ger ett svar på våra två forskningsfrågor utifrån våra emperiska resultat. Vi har dragit slutsatsen att det finns säkerhetsrisker med användandet av integrationsplattformar vid applikationsintegration. De säkerhetsrisker som kan dyka upp vid användandet av integrationsplattformar i ett IS är ett flertal och väldigt beroende av hur integrationsplattformens miljö är sammansatt. Vid införandet av en ny teknik finns det risk att man ärver säkerhetsproblem från den föregående tekniken.

Bachelor's Thesis in Informatics

Title:	**Integration Brokers - Is there security issues associated with the use of integration brokers?**
Author:	**Niklas Bengtsson, Lidia Berhane & Markus Petri**
Tutor:	**Jörgen Lindh**
Date:	**2006-12-15**
Subject terms:	**Integrationsplattform, SIG Security, EAI, CIA, AAA , SBA**

Abstract

In today's modern society there is a great demand on that the company's information's system should be available for communication. Communication can take place within and between different companies. Where the communicating parts can have different system architectures which makes the possibility of communication a complicated matter, there are applications for handling such obstacles. The names for these applications are message/integration brokers. When these applications act as a central hub for communication it is of great importance to maintain a high level of security.

Our main question is, what security risks can emerge when using integration brokers in an information system? This question can be divided into two sub question, being presented below:

- Might this technology for application integration result in consequences regarding security and if so in what way?
- What technology is integrated to ensure security with the two market leading integration brokers, are these two similar enough to make it possible to being regarded as a whole.

We started by defining the term security out of earlier knowledge such as existing literature and academic courses. When this where completed, we could identify which security issues companies could be facing when implementing integration brokers. Afterwards we used internet, different kinds of databases and magazines to localize as much fact and information that handle message brokers to gain a wider understanding of how those works. We decided to use primary data for the empery collection and chose therefore to carry out interviews with supplier, manufacture, and customers to be able to have different perspective from the whole integrations chain.

An analyse have been completed by the theory and the results of the interview. The analyse will give an answer of our two research questions from the result. We have drawn the conclusion of that security issues associated with the use of integration brokers in application integration exist. When inserting a new technique the risk of inherit security problems from the previous technique might appear.

Innehåll

1 Inledning 1
1.1 Bakgrund 1
1.2 Problemdiskussion 3
1.3 Syfte 3
1.4 Avgränsning 3
1.5 Perspektivanalys 3
1.6 Intressenter 4

2 Referensramen 5
2.1 Säkerhet 5
2.1.1 Sekretess, integritet och tillgänglighet 5
2.1.2 Ansvarsskyldighet, autentisering, auktorisering, kryptering och felhantering (AAA) 6
2.1.3 Säkerhetsramverket SIG Security 6
2.1.4 SBA Check 8
2.1.5 Mellanvara, dess koncept och funktion 8
2.1.6 Tidigare tekniker 9
2.2 Integrationsplattformar 11
2.2.1 Viktiga Integrationsplattformar 12
2.3 Sammanfattning av referensramen 15

3 Metod 16
3.1 Kunskapskaraktärisering 16
3.2 Vald metod 16
3.3 Intervjuformulär 18
3.3.1 Upplägg och design 18
3.3.2 Utförande av intervjuer 19
3.4 Datainsamling 20
3.4.1 Kvalitativ intervju 20
3.4.2 Urval av respondenter 20
3.5 Intervjuer 21
3.5.1 Intervjuobjekt typ A 21
3.5.2 Intervjuobjekt typ B 22
3.5.3 Intervjuobjekt typ C 22
3.6 Litteraturstudie 22
3.7 Metodproblematisering 23
3.8 Reliabilitet & Validitet 23

4 Empirisk undersökning 25
4.1 Respondent A 25
4.2 Respondent B 26
4.3 Respondent C 28

5 Analys av respondenternas svar och kopplingen till säkerhetskoncepten 31
5.1 Sekretess, integritet och tillgänglighet (CIA) 31
5.2 Ansvarsskyldighet, autentisering, auktorisering, kryptering och felhantering (AAA) 32

5.3 Jämförelse av Biztalk och Websphere 34
6 Slutsatser 37
7 Slutdiskussion 38
7.1 Egna reflektioner 38
7.2 Framtida forskningsfrågor 38
8 Författarnas tack 39
Referenslista 40
Bilaga 1 Intervjufrågor 42

Figurer

Figur 1-1 Traditionell mellanvara jämfört med en integrationsplattform (Linthicum, 1998). 2
Figur 2-1 Punkt till punkt mellanvara (Linthicum, 2004). 9
Figur 2-2 Många till många mellanvara (Linthicum, 2004). 10
Figur 2-3 RPC (Remote procedure call) (Linthicum, 2004). 10
Figur 2-4 MOM (Message oriented Middleware) (Linthicum, 2004). 11
Figur 2-5 Traditionell mellanvara jämfört med en integrationsplattform (Linthicum, 1998). 12
Figur 3-1 Beskrivning av metodens olika komponenter och vad som metoden ämnar undersöka. 17
Figur 3-2 Iterativ modell som beskriver återkoppling från intervjuver till intervjuunderlaget. 18

Tabeller

Tabell 1 Data i tabellen är sammanställd från (Davies, 2005) och (Milton, 2002). 14
Tabell 2 Presentation av valda respondenter. 21
Tabell 3 Tabell på säkerhetskoncepten på Biztalk och Websphere. 33

1 Inledning

Denna studie kommer att presentera en analys av säkerheten på en övergripande nivå för integrationsplattformar inom den svenska IT-industrin. Integration av företagsapplikationer har blivit ett allt mer populärt område inom applikationsutveckling samt systemarkitektur och är därför som varje ny teknik av högsta intresse att studera.

I samband med vår undran kring IT-säkerhet och applikationsintegration väcktes även nya funderingar kring detta område. Men efter ett antal diskussioner inom området, avgränsades uppsatsens problemområde till säkerhet inom integrationsplattformar då det fanns få studier inom just detta gebit. Författarna utvecklade därefter följande forskningsfråga: *vilka säkerhetsrisker kan tänkas dyka upp vid användandet av integrationsplattformar i ett IS?*

Studien är tänkt att undersöka säkerheten på ett sätt som leder till att man enkelt kan få en överblick över vilka säkerhetsåtgärder som är implementerade i mjukvaran och vilka krav som ställs på säkerhetsmedvetandet i samband med utnyttjandet av denna teknik.

Först går uppsatsen in på vad en integrationsplattform är och dess funktionalitet samt andra tekniskt viktiga aspekter vid datasäkerhet. Därefter kommer generella riktlinjer för säkerhet att presenteras i uppsatsen utifrån befintliga ramverk för bedömning av säkerhet. Med denna bas av information som utgångspunkt kommer säkerheten att undersökas på mjukvaran utifrån intervjuer ställda till leverantörer samt kunder som använder dessa. Därefter presenteras och analyseras säkerheten i de undersökta integrationsplattformarna. Detta kommer leda till en enkel överblick över skillnader och likheter hos dessa, som kan kännetecknas som gemensamma säkerhetsproblem.

Vi kommer även att analysera resultatet och ge våra egna kommentarer angående fördelar och nackdelar med den integrerade säkerheten i denna typ av integrationsapplikation.

1.1 Bakgrund

Det ställs idag krav från managementnivån inom företag att dagens IT-system i en allt högre grad måste vara öppna för kommunikation och vara förberedda för att kunna dela såväl data som affärslogik. Moderna företag har en mängd olika system och applikationer och det krävs någon form av översättare mellan dessa program som gör det möjligt för dem att kommunicera på ett säkert och effektivt sätt.

För att förenkla denna typ av integration har det tagits fram programvaror som går under benämningar som message broker, meddelandehanterare och integrationsplattform. I uppsatsens fortsättning används enbart den sistnämnda benämningen som är en svensk term för denna typ av integrationsapplikationer.

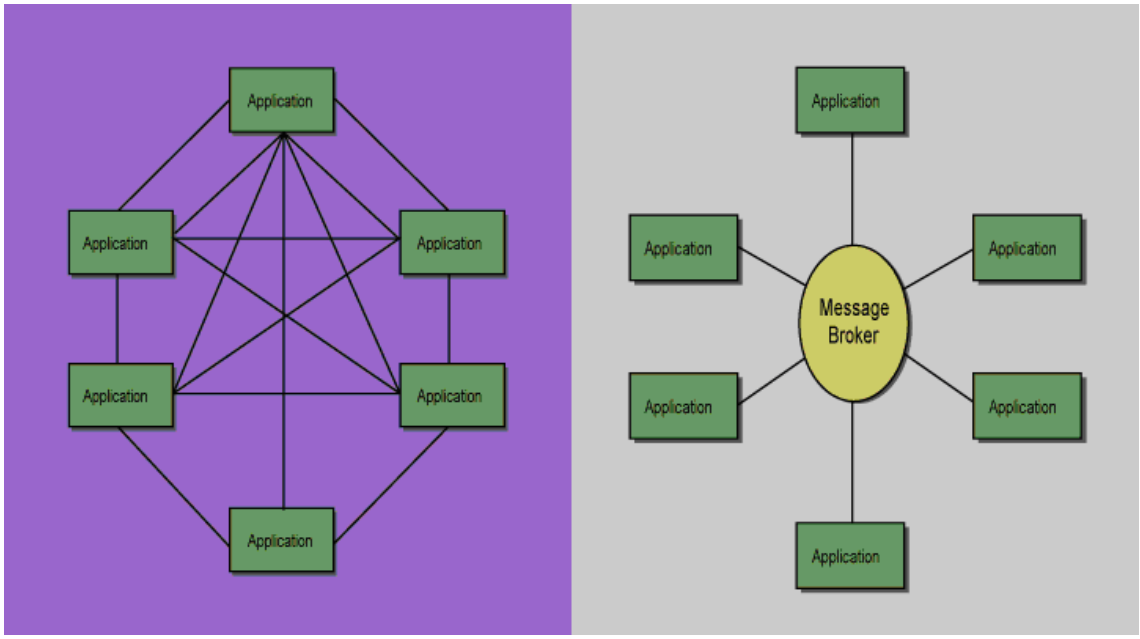
Säkerheten är speciellt viktig i denna typ av programvara då den hanterar kommunikation såväl internt som mellan företag. Att inte uppmärksamma detta och tro att sådana risker inte skulle finnas inom det egna informationssystemet (IS) kan få stora konsekvenser. Det har visat sig att de flesta attacker mot IS sker inifrån, vilket styrks av flera källor så som kända datorprofiler (Tanenbaum, 2003, s. 722) och det hävdas att uppemot 75 % av IT-relaterade misstag, bedrägerier och missbruk görs av före detta eller anställd IT-personal (Milton, 2002). Till detta bör nämnas att företag numera nästan uteslutande använder sig av det publika nätverket Internet för såväl intern s.k. Enterprise Application Integration (EAI) och extern s.k. Business to Business (B2B) integration. När ett program skickar data över

detta nät finns det en ökad risk för störningar, sabotage och medveten alternativt omedveten spridning av information till fel personer eller företag (Bishop, 2004).

Säkerhetsmedvetandet behöver alltså inte enbart gälla det som traditionellt betecknas som säkerhet som t.ex. skydd mot sabotage eller annat skadligt uppsåt. Enligt Mitrovic (2005) krävs vid transporter av meddelanden hög säkerhet och tillgänglighet även för själva kommunikationen. Två parter som skall kommunicera med varandra bör känna trygghet vid informationsutbyte (Mitrovic, 2005). Till detta kommer även aspekter som ökad teknisk komplexitet vilket kan få oönskade följder, eftersom mängden applikationer som är involverade står i relation till antalet kommunikationsproblem som kan uppstå (Linthicum, 1998). För att förhindra uppkomster av detta bör man ha en grundläggande förståelse för vilka programvaror man använder samt vilka risker som finns och hur man kontrollerar dem på ett tillbörligt sätt. Ett sådant exempel skulle kunna vara en integrationsplattform som kan få stora konsekvenser om de inte sköts och hanteras på ett adekvat vis.

Tidigare har punkt till punkt mellanvara (peer to peer middleware (P2P)) använts som individuella applikationer för varje form av integration (Linthicum, 2004). Idag har den gamla typen av teknik lyfts in i en mer generell och abstrakt nivå som kan använda sig av ett antal tekniker för systemintegration. Det är här som integrationsplattformar står att finna. Detta är applikationer vars syfte består i att hantera så stor del av kommunikationen som möjligt mellan informationssystems olika affärsfunktioner och deras respektive applikationer.

Integrationsplattformar möjliggör, genom stöd för kommunikation med ett flertal applikationer, en generell integrationsmjukvara ersätter ett flertal mindre och skapar en central funktion för att hantera denna vilket visas i figur 1 nedan. Det är därför avbrott eller felaktig användning av denna mjukvara kan få allvarliga konsekvenser för ett företags operativa verksamhet, rykte och goodwill hos leverantörer samt kunder (Milton, 2002).



Figur 1-1 Traditionell mellanvara jämfört med en integrationsplattform (Linthicum, 1998).

1.2 Problemdiskussion

Säkerhet är ett komplext begrepp som även inbegriper faktorer som feltolerans och tillgänglighet i systemen och inte enbart fokuserar på interna och externa hot från människor. Vi har i inledningen klargjort tre intressanta områden som överföring av data, samt teknisk komplexitet och centralisering av systemet. Detta väcker intresse kring hur dessa påverkas av användandet av integrationsplattformar.

Microsoft framför en del betänkligheter kring denna teknik på sin hemsida där man säger följande ”*the message broker represents a central point of attack. Compromising the message broker compromises the communication between all the applications that use it*” (MSDN, 2006).

Andra exempel som bör beaktas är även Mitrovic (2005) resonemang kring hur själva hanteringen av kommunikationen går till rent tekniskt och hur denna bedöms ut säkerhetssynpunkt, så som redundans och tålighet mot systemfel.

Vi skall därför utreda konceptet integrationsplattformar och undersöka den säkerhet som finns inbyggd i dessa. Vår huvudfråga är, vilka säkerhetsrisker kan tänkas dyka upp vid användandet av integrationsplattformar i ett IS?

De huvudsakliga frågeställningarna som dyker upp är då följande:

- Kan denna nya teknik för applikationsintegration få konsekvenser för säkerheten och i så fall på vilket sätt?
- Hur ser den bakomliggande tekniken för säkerhet ut hos två viktiga integrationsplattformar på marknaden, är dessa likvärdiga så att de säkerhetsrisker som identifieras är gångbara över integrationsplattformar generellt?

1.3 Syfte

Vi kommer i uppsatsen att undersöka området ”integationsplattformar” och försöka generera en lista över säkerhetsrisker som bör beaktas. Dessutom skall en jämförelse göras mellan två viktiga system för att se om slutsatserna är allmängiltiga över systemen.

1.4 Avgränsning

Vi har begränsat vår undersökning till att endast gälla den svenska marknaden, samt de två mest väldokumenterade integrationsplattformarna, som är Biztalk och Websphere.

Vi begränsar oss även inom området säkerhet, som är en bred term med många olika tolkningar. Därför gjorde vi en avgränsning genom att skapa en egen definition av begreppet med relevanta variabler för uppsatsen.

1.5 Perspektivanalys

Vi har valt att studera vår forskningsfråga kring säkerhet och integrationsplattformar utifrån tillverknings-, kund- och leverantörsperspektiven. På detta sätt kommer vi att få information kring integrationsaplattform samt säkerhet på olika nivåer. Ett tillverkarperspektiv innebär att presenterar företaget bakom produkten till exempel som

säljare. Ett kundperspektiv innebär att man till exempel är användare av produkterna. Med ett leverantörsperspektiv innebär det att man till exempel som konsult leverera tillverkarnas produkt. Uppsatsen kommer att fokusera på att studera deras erfarenheter avseende säkerheten i integrationsplattformar och de problem som de stött på vid arbete med denna teknik.

1.6 Intressenter

Vid skrivandet av uppsatsen har vi identifierat tre olika typer av intressenter kring integrationsplattformar. Vår uppsats kommer att rikta sig mot kunder som kan tänka sig att använda integrationsplattformar i sina informationssystem (IS) som då kan tänkas ha stor nytta av den kunskap vi tar fram. Detta med avseende på möjliga säkerhetsrisker vid användandet av integrationsplattformar. Följaktligen kan även leverantörer av integrationsplattformar tänkas ha nytta av den kunskap som vi tar fram. De kan då se vad andra leverantörer har identifierat för säkerhetsrisker och undersöka om informationen kan användas till att förbättra deras eget tänkande kring säkerhet. Uppsatsen kan även vara av intresse för studenter och utgöra en bas för framtida mer djupgående studier inom detta område.

2 Referensramen

I referensramen kommer du som läsare att få en inblick i vilken teoretisk kunskap som vi har använt oss utav under arbetet med denna uppsats. Först i referensramen kommer vi att beskriva olika typer av traditionell mellanvara och behandla de säkerhetskoncept som vi använt för att få mer information om vad som är viktigt att tänka på vid systemintegrering men även för hemanvändare. Vi beskriver koncept inom IT-säkerhet som, CIA, AAA, SIG security och SBA check. De två första säkerhetskoncepten överlappar som sagt de två senare där CIA respektive AAA ger en teknisk beskrivning av vad som tekniskt sett, kan gå snett och där SIG och SBA check ger konkreta råd på hur man ska bära sig åt för att hantera säkerheten hos ett IS.

Efter säkerheten går vi in djupare på vilken teknik som användes på företag och i organisationer innan integrationsplattformar utvecklades. Denna teknik ligger till grund för utvecklingen och denna speglar hur funktioner implementerade i integrationsplattformen kan ha fungerat innan implementeringen.

Vidare följer en presentation av de två viktiga integrationsplattformar som vi har fokuserat på i uppsatsen. Vi beskriver dessa utifrån den information vi funnit på respektive tillverkares hemsida. Efter presentationen av integrationsplattformarna följer en tabell med identifierad inbyggd säkerhet i dessa två.

2.1 Säkerhet

Vi ska i detta kapitel gå in mer på säkerhetsaspekter som vi beaktar vid utveckling av intervjufrågorna. Vi skall även presentera två svenska organisationer som arbetar kontinuerligt med data- och informationssäkerhet.

Enligt SIG Security (2005) bör säkerheten inkludera områden såsom sekretess, integritet och tillgänglighet. *Sekretess* innebär att man vill undanhålla information och även resurser för utomstående. *Integritet* vill förebygga att information och resurser inte läcker ut. *Tillgänglighet* vill hålla informationen och resurser disponibla för behöriga.

2.1.1 Sekretess, integritet och tillgänglighet

Sekretess, integritet och tillgänglighet är huvudkoncepten inom säkerhet och som på engelska benämns confidentiality, integrity and availability (CIA)(Bishop, 2004). För att vi vidare skall utveckla dessa begrepp kommer vi att gå in djupare på vad varje begrepp innebär.

Sekretess handlar om att rätt information ska nå rätt mottagare (Bishop, 2004). Den ska med andra ord inte vara manipulerad av någon annan på vägen och bör på något sätt vara dold så att ingen obehörig kan gå in och läsa datan. Är detta ej möjligt kommer obehöriga att kunna läsa datan och denna kan då bli lika öppen för alla.

För att uppnå att datan ej kan läsas av obehöriga personer används oftast parametrar som endast tillåter mottagaren att läsa data eller att öppna den (Bishop, 2004). För att ytterligare försvåra kan även kryptering göra datan svårare att komma åt. Det är endast krypteringen som möjliggör full sekretess om data skickas utanför systemet över öppna nät.

Integritet eller okränkbarhet är ett koncept som berör information som skickas på ett sådant sätt där det är viktigt att rätt användare får rätt information (Bishop, 2004). Detta är

viktigt då känsliga data ej bör ändras under kommunikationens gång. För att säkerhetsställa detta krävs ett förtroende mellan sändare och mottagare. Informationen bör även skickas över en säker anslutning så att ingen kan gå in under överföringen och ändra i data. Det finns i huvudsak två stycken integritetsaspekter inom data överföring som man bör känna till. Dessa två är dataintegritet och ursprungsintegritet och innebär att innehållet av datan samt ursprunget av datan skall vara som förväntad. För att uppfylla maximal integritet används primärt någon slags av berättigande.

Tillgänglighet är det tredje och sista konceptet som behandlar hur tillgängliga datan är (Bishop, 2004). Då information skickas är det viktigt att mottagaren får information i rätt tid, det är även viktigt att använda informationen och de resurser som finns för att leverera i tid. Tillgängligheten är baserad på samma mekanism som sekretess och integritet men det är dock svårare att uppnå full tillgänglighet då systemen kan förhindra kommunikation vid avbrott eller nertid. För att skydda sig mot detta krävs en väl planerad och fungerande plan för avbrott i systemet.

2.1.2 Ansvarsskyldighet, autentisering, auktorisering, kryptering och felhantering (AAA)

Med a*nsvarsskyldighet* menas att förmågan spåra ansvar och handlingar utan möjlighet till att förvanska dessa uppgifter (Chappell, Chopra, Dubray, Van der Eijk, Evans, Harvey, McGrath, Nickull, Noordzij, Peat & Vegt 2001).

A*utentisering* är en process som säkerställer att ett program, person eller annan entitet är den som den utger sig för att vara (Chapell m.fl. 2001). Auktorisering motsvarar *berättigande* och är den identitetsprocess som ger rättigheter till en resurs, avseende på viken identitet som gör förfrågan (Chapell m.fl. 2001). *Kryptografi* innebär att hålla data hemliga för icke behöriga.

Den grundläggande idén vid hemlighållande av data är att avsändaren applicerar en krypteringsfunktion, baserat på en kodnyckel, på originalmeddelandet (Chapell m.fl. 2001). Ursprungsmeddelandet i klarttext kommer då att efter denna behandling att bli oläsligt för dem som inte har rätt kodnyckel för att återställa texten. Det skall vara tillräckligt svårt för en utomstående part att knäcka krypteringsskyddet och på detta sätt säkerställes säkerheten i kommunikationen (Chapell m.fl. 2001).

Felhantering inkluderar skydd mot intrångsdetektering, åtkomstproblem och hantering av virus (Chapell m.fl. 2001).

2.1.3 Säkerhetsramverket SIG Security

SIG Security är en förening som utvecklar informationssäkerhet inom näringsliv, offentlig förvaltning och samhället i övrigt (SIG Security, 2005). Den bildades 1980 och framstår idag som Sveriges största nätverk som bearbetar säkerhetsfrågor inom informationssäkerhet. De har cirka 1700 medlemmar inom Sverige samt i andra skandinaviska länder.

Enligt SIG Security finns det några krav som en organisation bör följa såsom sekretess, riktighet och tillgänglighet (Karlsson m.fl. 1997). Med *sekretess* vill man undanhålla information och resurser för utomstående. Informationen måste vara *tillgänglig* för de behöriga. Dock ska användarna och den verksamhetens/systemansvarige skapa ett gemensamt beslut av säkerhetsnivån. Detta för att känslig information inte ska avslöjas för

obehöriga *(riktlighet)* eller andra användare utanför säkerhetsnivån. *Riktlighet* innebär att informationen inte ska modifieras på ett obehörigt sätt.

Ett nytt krav som utvecklats av SIG Security (2005) är *integritet*. Med *integritet* vill man förebygga att information och resurser inte läcker ut. Integritetskänslighet är en aspekt som är värd att uppmärksammas eftersom information som sprids kan förstöra eller förändra organisationen. Därför ställs enorma administrativa regler som vid inloggningssystem.

Enligt SIG Security (2005) finns riktlinjer och hjälpmedel för att verksamheter för att uppnå en god säkerhet vid informationshantering. Men för att uppnå detta krävs:

- Ledningens engagemang för säkerhetsarbete
- Riskanalyser
- Struktur och ansvarsfördelningen inom informationssäkerhet
- Administrativa regler och rutiner
- Skyddsåtgärder baserade på genomförda riskanalyser
- Ständig kontroll av säkerhetsnivån gentemot införda skyddsåtgärder och resultat från riskanalyser

Säkerhetsprocessen börjar med att ledningen först och främst tar fram en säkerhetspolicy (SIG Security, 1997). Utifrån denna policy sammanställs sedan riktlinjer och en strategi för arbetsprocessen. Man måste dock ta hänsyn till vissa aspekter vid framställningen som är följande**:**

- Krav och utveckling
- Etik och moral
- Lagar och avtal
- Intressenter kring verksamheten

Inom verksamheter uppstår idag ständiga förändringar inom organisationer, system och hård/mjukvara områden för verksamheter (SIG Security, 1997). Därför är det viktigt att uppdatera och kontrollera förändringar av säkerhetsprocesser.

Säkerhet inom verksamheter ser olika ut beroende på ledningens styrning (SIG Security, 1997). Att följa en säkerhetspolicy är ett krav för verksamheter eftersom det utformar en gemensam skyddsnivå. Säkerhetspolicy är ett dokument som speglar ledningens styrning av säkehetsskydd och informationssäkerhet.

Genom att införa en säkerhetsorganisation kan man bearbeta säkerhetsfrågor på ett strukturerat sätt (SIG Security, 1997). Vid uppbyggnad av en säkerhetsorganisation kan indelningen bestå av följande:

- En operativ säkerhets team: Ansvarar för den dagliga driften och uppehåller säkerheten.
- Ett akut säkerhets team: Hanterar akuta ärenden såsom intrångsförsök i informationssystem.

- En utbildning/informations team: Anställdas kompetens uppdateras och säkerhetsåtgärder informeras.
- Ett projekt/konsult team: Hanterar införandet av skyddsåtgärder (SIG Security, 1997).

Idag finns möjlighet för organisationer att överlåta IT verksamheten till ett serviceföretag (SIG Security, 1997). Man överlåter det operativa ansvaret för informationssäkerhet till ett serviceföretag (outsourcing). Ett krav är ett avtal uppstår mellan de två parterna.

Avtalet ska klargöra att kunden har rätt att kontrollera att serviceföretaget följer överensstämmelsen på kontraktet.

För att kunna undersöka säkerhetskonsekvenser med den nya tekniken av integrationsplattformar samt den bakomliggande tekniken är det viktigt att utgå från en trovärdig källa. Säkerhet är idag en viktig del inom verksamheter och SIG Security har därför utformat trovärdiga riktlinjer och hjälpmedel. Tre viktiga krav som benämns av SIG Security vid säkerhet är; sekretess, tillgänglighet och integritet. SBA Check är ett program som utformats av Svenska Dataföreningen. Med hjälp av detta skapar man en snabb analys av verksamheten för att utforma en god informationssäkerhet. Med hjälp av olika funktioner och checklistor kan man följa upp och skapa säkrare system inom verksamheten.

2.1.4 SBA Check

SBA check är ett program framtaget av Svenska dataföreningen som fungerar som en checklista för företag då en nulägesanalys av informationssäkerheten skall kontrolleras (Dataföreningen, 2006). Programmet är ett smidigt och enkelt program där, lämpligen, säkerhetssamordnaren skall besvara ett antal frågor som är framtagna från olika standarder som till exempel ISO/EIC 17799. Beroende på analysens omfattning kan ett företag få fram en komplett analys av informationssäkerheten på en till två dagar. Företag kan även använda programmet för uppföljning av ändringar samt få konsekvent information om vad som brister i säkerheten. Företag kan, med programmet, även skapa egna checklistor som passar processerna som skall kontrolleras i företaget. När frågorna är besvarade rapporteras resultatet i överskådliga rapporter med hjälp av text och bild. Det finns även funktioner som möjliggör exportering av rapporterna till diverse olika ordbehandlingsprogram. En samkörning av granskning mellan olika avdelningar eller företag kan också användas för att sedan jämföra dessa och ge förslag till varandra för förbättringar. Utifrån programmets tre checklistor har författarna plockat ut frågor som speciellt berör datasäkerhet och säkerhet vid informations utbyte.

2.1.5 Mellanvara, dess koncept och funktion

För att utveckla fördelarna med en integrationsplattform så har vi valt att förklara punkter av mellanvara närmare. Detta för att förklara hur ett liknande system skulle kunna vara uppbyggt innan framtagningen av integrationsplattformar.

Det finns en fysisk och logisk modell inom mellanvara (Linthicum, 1998). Den fysiska modellen har överseende över informationsflödet medan den logiska återger hur information överförs via verksamheter. Mellanvara inkluderar även två kommunikations mekanismer som är asynkronisk och synkronisk. Fördelen med den asynkroniska mekanismen är att applikations processen inte kommer att blockeras. Inom den

synkroniska delen är applikationer tätt inkopplade vilket medför problem med nätverket och den mottagande servern om den ej får svar. Detta för att den sändande applikationen håller förbindelsen öppen samt är stillastående tills denna har fått ett svar från servern. Ytterligare ett problem är applikationer som är involverade, de måste vara tillgängliga för att informationstransaktionen skall kunna utföras. Om mottagaren inte är tillgänglig och information sänds så kan viss data försvinna helt.

2.1.6 Tidigare tekniker

Mellanvara kan delas upp efter hur de fungerar som koncept och under detta stycke kommer dessa att presenteras. Då integrationsplattformar utnyttjar sig av eller utökar dessa är det av historisk vikt att presentera dessa.

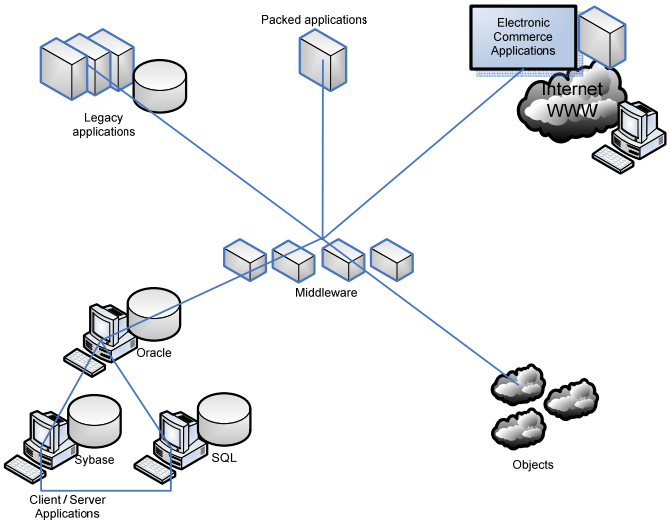
2.1.6.1 Punkt till punkt mellanvara (P2P)

Detta är en enkel funktion som tillåter en applikation att kommunicera med en annan applikation (Linthicum, 1998). Det finns en hel del olika P2P och en av dessa är Meddelandeorienterad mellanvara (MOM). Komplexitet involveras vid fler än två applikationer och därför kan man inte koppla samman MOM med fler än två applikationer åt gången. En typisk P2P kommunikation kan se ut som nedanstående bild.

Figur 2-1 Punkt till punkt mellanvara (Linthicum, 2004).

2.1.6.2 Många till många mellanvara (Many to Many middleware)

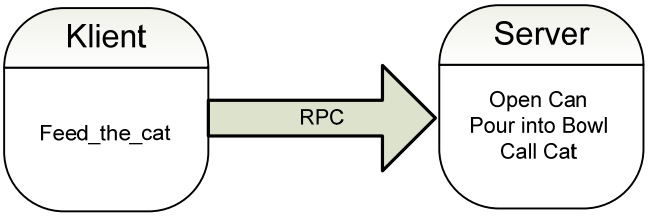
Som namnet antyder länkar denna logiska modell många applikationer till många andra applikationer (Linthicum, 2004). Detta leder till flexibilitet och användbarhet för applikationsintegration vid en problem domän. Det finns många exempel på hur en många till många mellanvara kan användas se figur 4. Bilden visar hur olika applikationer kan kopplas samman med en många till mången mellanvara och detta fungerar sedan som en brygga över till andra applikationer, Internet eller övriga objekt.



Figur 2-2 Många till många mellanvara (Linthicum, 2004).

2.1.6.3 RPCs

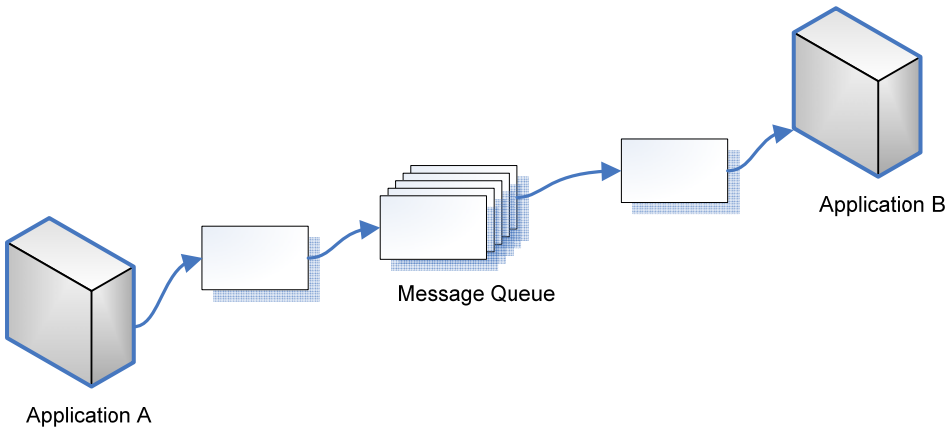
RPCs är den äldsta typen av mellanvara och den enklaste att förstå, har en synkronisk mekanism (Linthicum, 1998). RPC tillåter att en lokal funktion körs på ett remote system. De flesta UNIX system har utvecklat bibliotek och verktyg som en del av dess basoperation. En av de mest omtalade RPC kallas Distrubuted Computing Environment (DCE) och innebär att man kan göra en fjärruppkoppling mot en annan dator. RPC kräver 10 000 till 15 000 instruktioner för att utföra ett anrop mot ett fjärrsystems process och den är inblandad i många andra produkter och teknologier. Detta medför i sin tur att man inte vet när den används. Ett typiskt RPC anrop ser ut som nedanstående bild.



Figur 2-3 RPC (Remote procedure call) (Linthicum, 2004).

2.1.6.4 MOM

MOM, med den engelska översättningen Message oriented middleware, är en påbyggnad av RPC som har en mer självständig konstruktion (Linthicum, 1998). Meddelande skickas som har en struktur det vill säga ett schema och ett innehåll med data. MOM består av två delar nämligen P2P och message queuing (MQ). Integrations plattformar använder sig av MOM vid transportering av meddelanden. Varje MOM har sitt sätt att leverera sitt meddelande. Två av de mest kända MOM produkterna är, MSMQ från Microsoft och MQSeries från IBM. MQSeries produkterna tillhandahåller en ensamstående plattform som kallas för API. Detta medför att ett meddelande kan skickas från en Windows 2000 arbetsstation och vidarebefordras genom t ex UNIX (se figur 6).

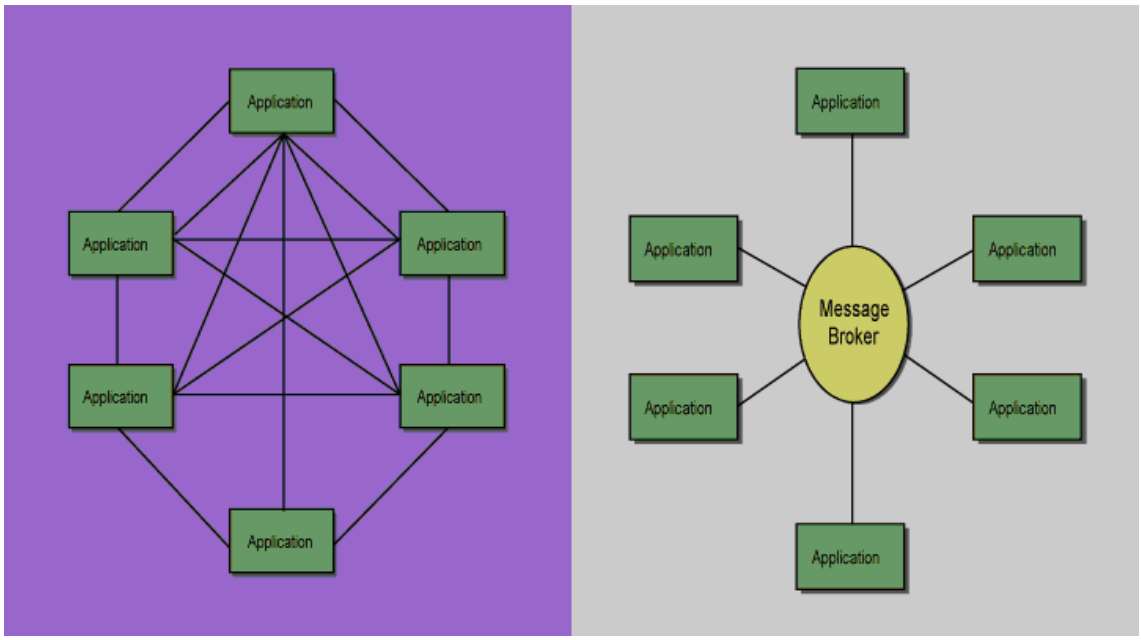


Figur 2-4 MOM (Message oriented Middleware) (Linthicum, 2004).

2.2 Integrationsplattformar

Enligt David S. Linthicum (2004) är en integrationsplattform, även kallad integration broker på engelska, en mekanism och mjukvara som tillåter en entitet att kommunicera med flera andra entiteter

Inom Enterprise applikation integration (EAI) är den största huvudfunktionen att dela information bland olika applikationer eller program (Linthicum, 1998). Med andra ord är värdet med EAI att dela data med andra applikationer. Detta sker till större delen genom olika mellanvaror, RPCs och distribuerade mjukvaror. När denna teknik används är det endast möjligt att skapa P2P kopplingar mellan dessa applikationer. Innebörden av detta blir att integrationen mellan applikationer blir beroende av olika mellanvaror mellan de olika systemen, oftast handlar det om olika typer av mellanvara beroende på vilket system applikationen pratar med. En integrationsplattform löser samma problem genom att fungera som en central förmedlare mellan en eller flera olika applikationer. Denna programvara binder samman det bästa av de olika mellanvaror som finns och kan även prata med befintliga mellanvaror samt skicka information till och från dessa. Integrationsplattformar handhar även funktioner för översättning av data vilket medför att en integrationsplattform kan översätta informationen för, eller till olika system. Nedanstående figur visar hur traditionella mellanvaror kopplas ihop jämfört med hur en integrationsplattform är ihopkopplad.



Figur 2-5 Traditionell mellanvara jämfört med en integrationsplattform (Linthicum, 1998).

2.2.1 Viktiga Integrationsplattformar

Här presenteras två välkända integrationsplattformar på den svenska marknaden som vi kommit i kontakt med efter inledande kommunikation med konsulter inom området som vi stött på under vår inledande forskning. Dessa integrationsplattformar har olika designupplägg och systemarkitektur vilket gör att de inte är möjligt att sätta likhetstecken dem emellan på en teknisk nivå men konceptuellt innehåller de till stor del samma funktionalitet.

2.2.1.1 Biztalk 2006

Biztalk är en integrationsplattform som lanseras av Microsoft (MSDN, 2006). Den är utvecklad på ett ramverk som kallas Net framework. Biztalk kan användas med fördel tillsammans med flera av Microsofts produkter så som, SQL Server 2005, för lagring av meddelanden. Biztalk 2006 som är den senaste versionen av integrationsplattformen stödjer även det nya operativsystemet som är uppbyggt med 64-bitars teknik.

Biztalk är en integrationsplattform som tillhandahåller möjligheten att kommunicera med en uppsjö av olika mjukvaror (MSDN, 2006). Plattformen stödjer olika protokoll och dataformat. Ett exempel kan vara en webservice. Produkten har stöd för grafiskt gränssnitt och kan sköta logiken i hela eller bara en del av en process.

Till integrationsplattformen kan företag koppla andra komponenter som samarbetar med Biztalk (MSDN, 2006). Detta gör det möjligt att följa upp aktiviteter som sker i programmet men även autentisiera information som skickas till eller från system som inte är Windows-baserade. Plattformen tillhandahåller funktioner för att visa information på en mer affärsmässig nivå och/eller en teknisk nivå. Biztalk Server 2006 har möjligheten att koppla samman företags processer genom två huvudprinciper. Den första är att specificera

och implementera den logiska drivningen av processen eller processerna. Den andra är en mekanism för kommunikation mellan applikationerna som processen använder.

En komplett integration av integrationsplattformen kan innehålla olika delar som till exempel meddelande scheman, special funktioner eller andra olika funktioner som gör det smidigare och enklare att hantera meddelandehanteringen (MSDN, 2006). Dessa funktioner kan administreras utifrån ett globalt verktyg, Biztalk Server 2006.

Beroende på var någonstans i företagskedjan man befinner sig kan man använda integrationsplattformen till en mängd olika saker (MSDN, 2006). En person som sysslar med företagsanalysering kan fastställa hela flödet i en enskild eller alla processer. Utvecklaren kan därefter skapa en implementation av plattformen som är specifikt konfigurerad för att passa just det företaget. Vidare behövs en administratör som upprättar rätt kommunikationer mellan applikationerna och underhåller plattformen i form av uppdateringar eller utbyggnad av processer. Alla dessa tre aktörer är dock nödvändiga för uppdatering och implementation av integrationsplattformen.

Det ska inte kosta miljontals kronor, inkludera komplicerade program och dyra konsulter för att integrera tillämpningar eller affärsprocesser. Microsoft Biztalk Server är helt integrerad med Visual Studio. NET vilket innebär att utvecklaren kan använda BizTalk Server-komponenter i utvecklingsmiljön i Visual Studio. NET samt bygga om affärsprocesser till webbtjänster Statskontoret (2003).

2.2.1.2 Websphere

Websphere är ytterligare en integrationsplattform, dock är det inte Microsoft som utvecklar Websphere utan IBM (Sadtler, Coumo, Ganci, Haberkorn, Jones, Kovari, Griffith, Marhas & Will 2005). Websphere är baserad på J2EE API från SUN Microsystems vilket är ett ramverk för att skapa och erbjuda plattformsoberoende applikationer i industriell skala. Integrationsplattformen innefattar givetvis meddelandehanteringen men till skillnad från Microsofts produkt så implementerar man Websphere som en modulbaserad arkitektur. Där väljer kunden själv moduler och verktyg efter vilka funktioner som de behöver till verksamheten (Sadtler m.fl., 2005). En annan skillnad som IBM's produkt har i jämförelse med Biztalk är att den är i stort sett plattformsoberoende. Detta på grund av att den använder javamotorn som kan exekvera javakod på den plattform som körs.

Produktfamiljen websphere har dock en paketerad produkt kallad *"Websphere business integration server"* vilken kan jämföras med biztalk 2006. Den innehåller kortfattat en meddelande nav och hantering och orkestrering av affärsprocesser på såväl intern (EAI) som externa nivå (B2B).

Denna modul är uppbyggd på två olika delar för att sköta kommunikationen mellan applikationer. Den första är *"Message-Flows"* som sköter hanteringen av meddelanden till och från en applikation. Detta innebär att den styr vilken väg meddelandet skall ta. Den andra processen kallas *"collaboration"* och denna tar hand om företagets processer, object, händelser och regler. *"Collaboration"* representerar affärsprocesserna och skapar en del av en hög prioriterad process som kallas *"workflow"*.

2.2.1.3 Teknisk säkerhet i integrationsplattformar

Det finns en rad säkerhetsfunktioner och tekniker för detta inbyggda i integrationsplattformar. Vi tänker här presentera en kort sammanfattning som visar vilka tekniker som stöds och kan användas av respektive plattform som vi undersökt. Detta ger då en bättre överblick över på vilka områden som dessa skiljer sig åt tekniskt sett.

När det gäller säkerhet så behöver beslut fattas på en radpunkter avseende vilken nivå av säkerhet som krävs för nedanstående punkter och att dessa överensstämmer med företagets interna säkerhetspolicy och dess krav på säkerhetsnivå och rättigheter (Microsoft, 2001).

- B2B transaktioner
- Interapplikations-transaktioner (kommunikation mellan applikationer och integrationsplattformen)
- Transporttjänster (avseende filer, sänd och ta emot)
- Kryptering
- Allmänna transportprotokoll som får användas (HTTP eller HTTPS)

Säkerhetspunkt		Biztalk	**Websphere**
Kryptering: PKI (Public-key-infrastructure)		IPSec, L2TP, SSL/TSL, och S/MIME	**SSL/TSL, MQ Internet pass through (IPT)**
Autentisering		SSL	**SSL**
Transport protokoll		SSL	**SSL**
Message Queuing avseende • Åtkomstkontroll • Granskning (Auditing)		Kerberos (128-40 bit)	**MCA** **user identifier**
Orchestration Services, (åtkomsträttigheter vid processlagret)		**XSLANG**	**Object Authority Manager (OAM)**

Tabell 1 Data i tabellen är sammanställd från (Davies, 2005) och (Milton, 2002).

2.3 Sammanfattning av referensramen

I referensramen har det presenterats viktiga säkerhetskoncept som vi har tagit i beaktning då vi utformat intervjufrågorna. Vi har även redogjort för hur företags meddelandehantering kan se ut innan en implementation av en integrationsplattform. Vidare presenterades de två viktiga integrationsplattformarna vi fokuserat på i uppsatsen. En sammanställning av implementerad säkerhet i biztalk och websphere är gjord för att redan nu bedöma om säkerheten går att jämföra mellan dessa två.

3 Metod

I detta kapitel redogörs tillvägagångssättet i uppsatsarbetet och hur vi ämnar genomföra arbetet för att besvara våra forskningsfrågor. Då det finns ytterst lite skrivet om detta ämne med applikationsintegration i överensstämmelse med säkerhetsfrågor, har vårt forskningsarbete inte utgått från någon tidigare forskning inom just denna koppling mellan områdena. Det finns ingen tidigare ställd hypotes som vi avser prova utan vår fråga är mer öppen ställd som en undran. Forskningsfrågan kommer vi genom en explorativ ansats att undersöka.

För att komma fram till vårt val av syfte krävdes en hel del diskussioner kring området. Vi inom uppsatsen träffades kontinuerligt under en och halv månad för att göra oss bekanta med området av integrationsplattformar. Sedan kunde vi avgränsa oss inom säkerhet av integrationsplattformar. Att studera ett nytt område är krävande vilket gruppen märkte vid olika situationer som till exempel vid stökning av lämpliga intervjuobjekt.

3.1 Kunskapskaraktärisering

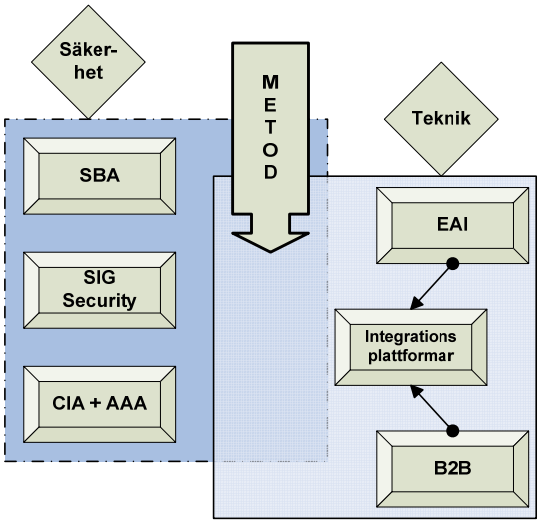
Med litteraturstudie och samtal med kunniga personer har vi kunnat ta beslut om vilken kunskap som vi vill utveckla med uppsatsen. För att göra det möjligt att undersöka de givna forskningsfrågorna ansåg vi att en explorativ kunskapsform skulle bli lämpligast. Enligt Goldkuhl, (1998) innebär denna kunskapsform att man fokuserar sig på att undersöka ett område för att förbättra sin kunskap kring det, men utan att man testar hypoteser.

En kunskapskaraktärisering skapas för att fastställa den kunskap som man skall utveckla inom uppsatsen (Goldkuhl, 1998). Det finns olika typer av kunskapsformer som t ex deskriptiv (egenskapsbestämmande), karaktäriserade (förståelseinriktade), normativ (vägledande) kategoriell, explorativ och med flera andra

Den största och viktigaste punkten i hela uppsatsen ligger i att definiera vad som avses med säkerhet. Detta är en term som är i stort behov av att definieras både för läsaren samt för författarnas arbete. Det är då viktigt att hålla fokus på vad som skall utforskas och vilka de viktiga variablerna är.

3.2 Vald metod

Det första som kommer att presenteras är författarnas egen definition för bedömning av variabler inom säkerhet och hur detta har tagits fram och vad det bygger på. För att uppnå detta följs SIG Security´s säkerhetskoncept och kriterier utifrån verktyget SBA check samt koncept som CIA och AAA.



Figur 3-1 Beskrivning av metodens olika komponenter och vad som metoden ämnar undersöka.

När vi skulle välja på vilket sätt som säkerheten skulle utvärderas utgick vi ifrån att det finns tre viktiga aktörer kring integrationsplattformar. Dessa är utvecklare av produkten, leverantörer av produkten till kund och slutligen kunden som använder produkten. Då vi ämnar undersöka säkerheten och om tekniken kräver uppmärksamhet inom nya områden som inte tidigare varit aktuella, har vi valt att ställa en rad frågor på en konceptuell nivå till tillverkare och leverantörer avseende hur säkerheten påverkas.

På detta vis skall vi utforska om det finns något av intresse som IT-branschen har lärt sig, då denna relativt nya teknik med integrationsplattformar har börjat se en ökad användning på marknaden. Vi resonerade på det viset att slutkunder med stor säkerhet ogärna delar med sig av negativa erfarenheter och information av denna typ är mycket känslig, vilket gjorde att vi inte direkt fokuserar på denna del.

Studien kommer istället att baseras på respondenters svar som vi valt som primärkälla, med förhoppning att de skall vara öppna i denna fråga samt att vi får möjligheten att analysera produkten från två steg i leverantörskedjan samt att dessutom ställa två konkurrerande tekniska plattformar mot varandra. Finns det kunskap om konkurrerande teknik sinsemellan så ger det ytterligare djup i underlaget.

Vi har bestämt oss för att angripa problemet genom att utföra intervjuer som ger en djupare förståelse samt tillräcklig bredd i frågan för berörda parter så som VM-data, Microsoft och IBM. Vår tanke är att på detta sätt skapa oss en så fullständig uppfattning som möjligt, för att ge en förståelse av problem inom säkerhet vid applikationsintegration.

Vi ämnar med denna undersökning att få en övergripande förståelse av problemområdet, där resultatet dock i hög grad bestäms av intervjuobjektens villighet att dela med sig av erfarenheter. Detta leder också till resonemang kring vilka brister och fördelar som detta angreppssätt kan ha vilket behandlas i nedanstående stycke.

3.3 Intervjuformulär

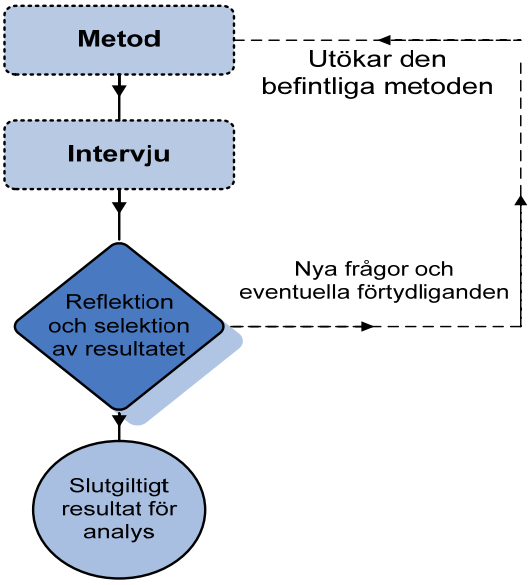
Då vi använder oss utav en semistrukturerad intervju så följer intervjun en grundläggande mall med frågor som vi skall följa under intervjuns gång. På detta vis skall vi täcka av de ämnesområden som vi identifierat som viktiga under vår litteraturstudie. Intervjuformuläret som vi använder oss utav i den empiriska studien kommer att finnas i två olika versioner, dels en med enbart frågor som är den vi skickar ut till intervjuobjekten i förväg dels en version som vi kontinuerligt uppdaterar med nya följdfrågor under varje fråga.

Detta gör vi för att i början av varje fråga låta den intervjuade personen prata fritt om sin egen uppfattning kring frågan och därefter utveckla intervjun vidare baserat på den data som vi kontinuerligt samlar in. Med detta så ämnar vi att tillgodogöra oss resultaten från tidigare intervjuer för att få mer utförliga frågor.

3.3.1 Upplägg och design

I detta avsnitt skall vi enkelt förklara varifrån vi har hämtat frågorna men också förklara deras relation gentemot våra forskningsfrågor.

När vi utformade frågorna inspirerades vi av två stycken väl kända analyseringsverktyg och ett par välkända koncept inom datasäkerhet. Analyseringsverktygen och koncepten finns att läsa om i referensramen. För en komplett lista över våra frågor se bilaga 1. Vi har valt att dela in alla frågor i olika genrer för att enkelt kunna härleda vilket område de behandlar. Vi har även valt att ta med en fri öppen fråga till respondenten för att säkerställa att vi själva ej kommer att undgå relevant information som kan påverka de övriga frågorna i genren. Detta även för att ge oss en återkoppling och uppfattning av om vi har missat någon och ge respondenten en chans att utöka våra frågor för att bättre kunna svara på problemfrågorna.



Figur 3-2 Iterativ modell som beskriver återkoppling från intervjuer till intervjuunderlaget.

3.3.2 Utförande av intervjuer

Innan vi bestämde vilka respondenter som skulle intervjuas, ringde vi till flera olika företag och försökte framföra vår önskan om en intervju. Detta var inget enkelt arbete då det finns relativt få respondenter som var kunniga både inom integrationsplattformar samt säkerhet.

När vi skulle genomföra intervjuerna med respondenterna vi fått kontakt med bestämde vi oss för att först skicka ut frågorna via e-mail i förväg. Detta för att respondenterna skulle ha möjlighet att fundera ut ett bra svar samt att de skulle vara förberedda på frågorna. Respondenterna fick en till två dagar på sig att läsa igenom frågorna för att sedan bli uppringda av oss. Telefonsamtalet spelades in och sammanfattades i skrift. Fanns otydligheter i svaren eller om vi ej ansåg att svaren var fullständiga kontaktades respondenten igen via mail eller telefonkontakt beroende på hur omfattande svar vi behövde. Intervjuerna ligger under kapitel 5 senare i uppsatsen.

3.3.2.1 Generella inledande frågor

Fråga 1-5 är inledande frågor som skall påvisa hur erfarna respondenterna är inom området IT och datasäkerhet. Nästkommande frågor (6-11) är frågor som är hämtade från SIG securitys ramverk (Karlsson, H. G., Keisu, T., Lantz, M., Lundin Andersson, M., Osvald, T., Karlsson, J. (red.). (1997), avseende revision av säkerhetspolicyn, samt programmet SBA check dessa frågor är dock anpassade för att kunna användas i situationer där integrationsplattformar används. Syftet med dessa frågor är att besvara forskningsfråga nummer ett.

3.3.2.2 Användare och inloggning

I denna del av frågeformuläret ställs frågor som har att göra med koncepten CIA och AAAC, men även frågor hämtade ur SIG Securitys ramverk (Karlsson m.fl. 1997). Dessa är dock anpassade till integrationsplattformar. Frågorna, 13-18, hanterar information om hur säker inloggning är, men även säkerheten för användarnamn och lösenord. Dessa frågor syftar till att ge svar på säkerheten utifrån AAA och CIA-koncepten. Frågorna i denna genre syftar till att besvara delar av forskningsfråga två, men berör även forskningsfråga ett till viss del.

3.3.2.3 Säkerhet och avbrottshantering

Frågor inom detta område är utformade utifrån konceptet felhantering och syftar till att ge kunskap om hur företagen påverkas av driftsproblem. Frågorna 19-24 är delvis hämtade från programmet SBA Check men även utformade utifrån felhanterings-konceptet. Frågorna är ställda för att besvara båda forskningsfrågorna till en viss del.

3.3.2.4 Dokumentation

Denna, som är den sista genren, behandlar frågor om hur väldokumenterat systemet är. Frågorna 26-28 besvarar delar av forskningsfråga ett, men ger mer information om vad företagen kan konfigurera själva efter implementationen. Detta för att klargöra gränsen vid ansvarsförhållandet mellan företaget/kunden och dess beroende till leverantören så fort ett fel, eller säkerheten måste åtgärdas. Fråga 28 tar även upp om säkerheten implementeras tillsammans vid leverans eller om slutkunden kan välja att köpa till denna tjänst eller konfigurera säkerheten själva och var ansvarsgränsen går mellan dessa.

3.4 Datainsamling

Både primär och sekundär datainsamling är två effektiva tillvägagångssätt vid forskningsprocesser (Eriksson & Wiedersheim, 1999). Vid primära datainsamlingar utförs egna undersökningar medan sekundära utgår från data som redan samlats från tidigare studier såsom böcker, artiklar och uppsatser.

Vid en intervju skapar man djup förståelse genom att ställa frågor till de utvalda respondenterna (Holme & Solvang 1996). En forskare måste respektera individens integritet vid intervjuer. Vid studiens intervjuer kommer en hel del säkerhetsfrågor att ställas och eftersom detta oftast är känsligt område, krävs det att man visar trovärdighet och respekt.

3.4.1 Kvalitativ intervju

Vid kvalitativa intervjuer finns inga standardiserade mallar att följa och därför är dessa intervjuer tidskrävande (Holme & Solvang, 1996). En intervjuform med minsta styrning leder till att respondenterna påverkar intervjuens utveckling. Anledningen till att man inte använder mallar är för man vill få fram åsikter och värderingar från respondenterna. Vi kommer att använda oss av en semistrukturerad intervju som baseras på ett frågeformulär i fyra etapper.

Syftet med dessa intervjuer är att öka informationsvärdet och skapa en grund för djupare och mer fullständig uppfattning kring ämnet som studeras (Holme & Solvang, 1996). Generaliserbarheten är dock svår att uppnå eftersom ständiga förändringar uppstår vid frågorformuleringar. Metoden är krävande för både forskaren och respondenten (Holme & Solvang, 1996). Forskaren måste ha förmågan att förstå intervjuaren inom problemområden som berättas och respondenterna måste kunna argumentera och förklara sina åsikter.

3.4.2 Urval av respondenter

I detta avsnitt kommer vi att beskriva hur vi gick tillväga vid val intervjuobjekt. Det finns teorier som beskriver olika tillvägagångssätt i hur detta skall gå till och när de olika alternativen passar med val av metod.

Respondenter skall vara representativa, det vill säga tillgängliga vid intervjun (Holme & Solvang 1996). Med representativa menas i vårt fall att respondenterna skall vara kompetenta inom sitt område.

Två vetenskapliga urvalstekniker är sannolikhetsurval och icke sannolikhetsurval. Sannolikhetsurval (slumpmässiga urval) gör det möjligt att förenkla insamlingen av stickprovet till populationen (Holme & Solvang, 1996). Inom icke sannolikhetsurval skall man som forskare agera och utforma en bedömning av populationen.

Icke sannolikhetsurval kommer att användas inom denna studie genom att agera och bedöma respondenter Urvalet av studiens respondenter måste vara trovärdiga, IT inriktade och nyttja integrationsplattformar.

Enligt Holme & Solvang (1996) är det till fördel att inte styra deltagarna för mycket under intervjuprocessen. Detta eftersom man vill åstadkomma synpunkter, åsikter och värderingar. Att kritisk granska data samt utreda källor är avsevärd för att finna relevant information.

Genom att noggrant planera upplägget av frågorna kunde vi uppnå en ömsesidig intervju. För att täcka in syftet valde vi respondenter från våra tre olika perspektiv som kunde ge svar kring säkerhetsfrågor

Vidare är det viktigt att få olika vinklar från intressenterna som använder integrationsplattformar. Genom att plocka aktörer från olika vinklar och olika integrationsplattformar kan de olika leden i kedjan bli upplysta om problem som inte tidigare har uppmärksammats hos dessa. Detta kommer då att leda till att en jämförelse kan göras från de olika stegen vilket leder en överblick om säkerhetsriskerna hos systemen är plattformsoberoende.

Uppsatsens intervjuobjekt har valts med hänseende att täcka två viktiga integrationsplattformar på marknaden. Genom att täcka dessa kan generella slutsatser dras av resultaten som då kan sägas gälla för integrationsplattformar överlag. För att ge en bra representativitet kommer det att väljas ett objekt från leverantörssidan, ett från företaget som tillverkar produkten och en kund som implementerat tekniken. Genom att göra denna koppling mellan tillverkare, leverantör och kund har vi försökt att spegla samma situation ur tre perspektiv. Detta för att skapa en bra spegling av de verkliga förhållandena.

För att illustrera vilken av respondenterna som har kopplingar till de olika systemen och var i kedjan dessa befinner sig har vi valt att göra en tabell där detta framgår.

	Kund	**Leverantör**	Tillverkare
Websphere			**Respondent C**
Biztalk	**Respondent B**	**Respondent A**	

Tabell 2 Presentation av valda respondenter.

3.5 Intervjuer

Här kommer det att presenteras de intervjuobjekt och intervjuer som gjorts med teknisk expertis för de undersökta integrationsplattformarna. Presentationen kommer att ske med intervjuerna uppdelade per applikation med efterföljande nivå.

Att finna kompetenta respondenter inom säkerhet av integrationsplattformar var en krävande process. Under mässan Next Step våren 2006 i Jönköping kom vi i kontakt med WM data. Där diskuterades konsulternas erfarenhet av det aktuella området vi skulle skriva om. På detta sätt kom vi kontakt med en av våra respondenter. Genom denna respondent fick vi även ytterligare information om kompetenta personer kring säkerhets området av integrationsplattformar och på så vis kom vi i kontakt med vår andra respondent. Den tredje respondenten var en privat kontakt inom gruppen.

3.5.1 Intervjuobjekt typ A

Utifrån respondent A har vi fått ett leverantörsperspektiv på våra ställda frågor. Respondenten har jobbat inom IT-Branshen i elva år och har tidigare jobbat som

processingenjör inom kemibranschen. Respondenten har civil ingenjörs utbildning och är väl insatt i de flesta integrationsplattformarna på marknaden.

3.5.2 Intervjuobjekt typ B

Respondent B kommer att ge oss ett kundperspektiv av integrationsplattformen Biztalk. Respondenten i fråga har arbetat inom IT-branschen i sju år varav tre av dessa inom Integration. Med en Civilingenjör examen i Industriell Ekonomi, systemadministratör på Chalmers och tidigare erfarenhet av eget IT-konsultbolag har vi fått uttömmande svar på våra frågor. Som systemadministratör och ansvarig för datanät/system under flera år fick denna respondent en hel del erfarenhet inom IT-säkerhet.

3.5.3 Intervjuobjekt typ C

Respondent C arbetar inte direkt med tekniken själv men har mycket indirekt erfarenhet av säkerhetsproblem vid applikationsintegration med 25 år i branschen. Han tillhör säljorganisationen hos IBM och innehar inga industriella certifieringar inom säkerhetsområdet. Respondenten påpekar att denna del sköts av IBM's specialister på säkerhet inom deras tivoli-organisation. Vårt intervjuobjekt arbetar med att sälja infrastrukturkomponenter för applikationsintegration och upplever sig kunna mycket om säkerhet vid integration mellan system, men har endast arbetat med IBM's produkter.

3.6 Litteraturstudie

Med sekundär datainsamlig har den bakomliggande tekniken av integrationsplattformen beskrivits i vår uppsats. Denna har gjorts med första ansats och hjälp utifrån David S. Linthicum´s *Next Generation Application Integration - from simple information to webservices (*Linthicum, 2004). För att finna ytterligare information om integrationsplattformar och dess säkerhet har sökord såsom middleware, messagebrokers, integrationsplattformar, SIG Security och EAI (Enterprise Application Integration) använts.

De första sökorden utom SIG fick vi från Linthicum's bok (Linthicum 2004) och SBA-check fick vi som tips från vår handledare. Han gav oss en cd-skiva med det kontrollprogrammet vilket gav oss en start som inte var teknikfokuserad utan tog upp detta på en användarnivå.

Med hjälp av Internet undersöktes alla dessa sökord via olika sökmotorer och databaser såsom Google, Scholar Google, Books 24x7, Högskolebibliotekets e-bibliotek ebrary, Julia och DIVA. Resultatet av dessa sökord var enorma, speciellt av sökordet "messagebrokers". Detta skapade därför i början en hel del förvirring eftersom många olika definitioner hittades. Vi avgränsade oss därför inom trovärdiga och kompetenta Internet källor inom detta område som till exempel Microsoft och IBM. Datainsamling av vår säkerhetsaspekt kunde utformas utifrån föreningen SIG Security´s hemsida.

Informationen vi hittat om integrationsplattformar har varit bra men inte tillräcklig. Det råder troligen brist på kunskap inom området eftersom det är nytt. Men att hitta information om de olika säkerhetsaspekterna har varit betydligt enklare eftersom mer kunskap finns inom området.

3.7 Metodproblematisering

En svaghet i metoden ligger vid bedömningen av allvarlighetsgraden hos de identifierade säkerhetsriskerna. Intervjuobjekten har inte själva kvantifierat detta, utan denna bedömning görs av författarna genom våra egna uppfattningar och subjektiva bedömning.

Då vi i vår studie inte utgår ifrån någon befintlig hypotes inom vårt studieområde, utförs inga stora datainsamlingar och därför användas inte den kvantitativa metoden vilket resulterar i en kvalitativ analys och uppskattning utan några mätbara värden eller sannolikheter. Det kan även hända att det kommer att ske ett visst undanhållande av fakta från respektive tillverkares håll för att framställa den egna lösningen i bättre dagar.

Till styrkorna hör att det finns en total saknad på koppling mellan exempel på säkerhetsbrister och den påverkade, vilket borde ge en större vilja och förmåga att kunna dela med sig av erfarenheter från verksamheten.

Kvalitativa metoder är anpassningsbara och ger goda utredningar men nackdelen är ändringsbarheten (Holme & Solvang, 1996).

3.8 Reliabilitet & Validitet

Inom vetenskapliga studier är det viktigt att man uppger trovärdigheten hos den insamlade information och att man noggrant undersökt de källor man använder sig av.

Vid rapportering av en kvalitativ metod är det viktigt att uppge validitet (giltighet) och reliabilitet (pålitlighet). Detta för att framföra att man varit trovärdig i de mätningar man gjort men är detta inte lika relevant att presentera inom den kvantitativa metoden (Holme och Solvang, 1996).

Enligt Holme och Solvang (1996) definieras reliabiliteten som följande: *”Reliabilitet fastställs av hur mätningar utförs och hur noggrann man är vid bearbetningen av det forskningsmaterial som samlats in, och validitet är beroende av vad man mäter.”*

Hög reliabilitet uppnår man genom god planering, noggrannhet och kontroll av förstudier. Genom att utarbeta instruktioner och rutiner för de olika faserna i forskningen kan man uppnå hög reliabilitet. Genom att studera olika perspektiv av integrationsplattformar har vi försökt att eftersträva hög reliabilitet.

Inom intervjuer har vi respekterat personernas integritet och därför erbjudit anonymitet. Vi har därför inte uppgivit några namn på respondenterna utan istället tilltalat dem som intervjuobjekt A, B och C.

Vid insamling av primärdata vid våra intervjuer kommer vi att kontrollera att frågorna besvarats riktigt. För att hantera detta kommer vi att skicka ut frågorna i förväg via e-post. Detta för att låta respondenterna få god tid att läsa igenom frågorna och ta ställning till eventuella svar. Sedan kommer vi att kontakta dem och utföra telefonintervjuer. Detta kommer leda till hög reliabilitet.

En nackdel är att ingen direkt personkontakt har funnits vid intervjutillfällena, vilket medför att abstrakta resonemang inte har kunnat åskådliggöras visuellt för författarna. Detta kan ge en viss osäkerhetsfaktor om svaren har tolkats rätt.

Validitet handlar om att mäta det som är relevant och att använda rätt saker vid rätt tillfällen (Gunnarson, 2002). Det finns både en inre och yttre validitet (Svenning, 1996).

Den inre handlar om kopplingen mellan teori och empiri, medans den yttre validiteten berör hela omgivningen.

Kvalitativ operationaliseringsprocess innebär att man utgår från teori till empiri (Solvang & Holme 1997). Operationalisering ska vara täckande, fruktbar, enkel och tydlig. Detta innebär att inte ha stort avstånd till respondenterna.

För att uppnå validitet kommer vi att försöka finna svar på våra problemställningar genom de tre olika perspektiven (tillverkar, leverantör och – kundperspektiv). Med en empirisk studie utifrån dessa olika perspektiv kommer en tydligare kunskap att exponeras och leda till en god validitet. Men detta endast om frågorna är välformulerade och konkreta. Vi kommer därför att i förväg sända ut intervjufrågorna via mejl för förberedda respondenterna och reducera risken för missuppfattning. Genom olika uppfattningar om integrationsplattftormar från dessa kommer vi att undersöka om säkerhetsrisker finns. Med hjälp av de utformade intervjufrågorna ska vi få svar på våra forskningsfrågor från trovärdiga säkerhetskoncept. Vi kommer att utgå från teori om den bakomliggande tekniken för att sedan utarbeta en empirisk studie för att kunna ge en täckande kunskap för att sedan undersöka området.

4 Empirisk undersökning

Våra huvudfrågor berör konsekvenser för säkerheten vid implementation av en integrationsplattform, samt hur den bakomliggande tekniken för säkerhet ser ut hos två viktiga integrationsplattformar och om dessa gångbara överlag. För att svara på detta har vi med hjälp av intervjuer samlat information som sedan har sammanställts. För att koppla de variabler vi har beskrivit i referensramen och hur dessa har anknytning till frågorna som vi ställt till respondenterna har vi förklarat i kapitel 2.2

Nedan presenteras resultatet av den empiriska insamlingen gjord utifrån respondenternas tre olika perspektiv. Sammanfattningarna är strukturerade efter frågeformuläret från och med fråga 6 då tidigare frågor inte har någon direkt anknytning till forskningsfrågorna.

Det skall tilläggas att det från början gjordes ett försök att genomföra intervjun per e-post. På detta sätt var det enklare att få kontakt och svar, men vi märkte att resultatet som vi fick tillbaka var av typen ja eller nej. Vi övergick istället till muntlig intervju och ställde mer ingående frågor. Det gav oss mer utvecklande svar, där intervjuobjektet dessutom skulle hjälpa oss med förståelsen av det teoretiska ramverket och hur tekniken fungerade i praktiken.

4.1 Respondent A

Utvecklingen för säkerhetsfunktioner hos integrationsplattformar ser lovande ut. *”Utpekande är Microsofts strategi med SSO (Single sign on).”* När det gäller Biztalk som kopplas till Microsoft Windows så styrs säkerheten mycket av operativsystemet. Websphere som i grunden är något säkrare styrs också till stor del av operativsystemet. Säkerhetsrisker som uppkommer i samband med användande av integrationsplattformar är sådant som har följt med ifrån den gamla tekniken. Exempel på detta kan vara, transport av känslig data och system som behöver öppna sig för att möjliggöra åtkomst av data. *”I en automatiserad process där integrations-plattformen ska göra många saker samtidigt, så krävs det stor tillåtelse för integrationsplattformen att göra saker i många olika system och detta kan ses som en säkerhetsrisk.”* Detta löses dock genom att skapa ett konto med mycket funktionalitet men nödvändigtvis inte mycket rättigheter.

Kostnaderna för säkerhet, underhåll och drift har ökat markant. Dels via en sträng säkerhetspolicy på företag, och det finns ofta en dålig förståelse för att integrationsplattformen trots allt är relativt säker. *”När kunder inte vet riktigt vad en Integrationsplattform är, och att den har massa säkerhetsfunktioner som man kan välja att använda eller inte använda. Integration är väldigt populärt vilket medför diskussioner och mer intresse kring integration, därav dålig förståelse för systemen”.* Vid implementering av en integrationsplattform försöker respondentens företag så långt som möjligt följa kundens säkerhetspolicy. Respondentens företag har olika *”best practices”* som överensstämmer med tillverkarens. Undantaget är när säkerhetsprojekt körs hos kunden. I detta scenario har kunden oftast ett eget sätt att lösa detta och man väljer då att följa kundens plan över integrationsprojektet. Vid vissa fall behöver kunden hjälp med detta och då finns respondentens företag där för att hjälpa till. Har företaget inte egna *”best practises”* så tar respondentens företag fram detta i samråd med kunden. Det kan även hända att ett företags interna säkerhetspolicy behöver ändras för att förenkla drift och underhåll av plattformen.

När det handlar om användarhantering för konsulter och anpassning till applikationen så sätter man olika användarnamn beroende på vilken Windows grupp denna tillhör. *”Olika*

konsulter hamnar i olika grupper beroende på operativsystemet och får på detta sätt olika rättigheter till funktioner beroende på grupp." I övrigt så har varje användare en unik identitet i de fall tjänsten används av ett applikationskonto. Detta är det vanligaste sättet att göra, dock så lyder inte ett applikationskonto under samma regler som ett vanligt konto. Detta skulle vara alldeles för kostsamt och ohållbart i längden på grund av frekventa lösenordsbyten. Det finns möjlighet till att ge användarna direktåtkomst till de tjänster som de fått behörighet att använda. Beroende på vilken lösning man har så släpper integrationen in och ut olika användare, detta för att förhindra att systemet kodas om för mycket.

Relevanta händelser loggas ur ett säkerhetsperspektiv oftast, men då detta är kostsamt och kräver mycket prestanda loggas inte all information. Loggningen kan även stängas av under kontrollerade former för att sedan förlita sig på omgivande systems loggning. Funktioner som syftar till att göra det omöjligt för en användare att förneka eller avvisa en viss handling finns i systemet. Beroende på vilken funktion man använder för att vidarebefordra informationen, och vilken typ av meddelande det handlar om så loggas detta. Loggning sker oftast både i mottagande och sändande applikation, det krävs dock inte att hela meddelandet loggas. Är loggningen tillräckligt bra så kan man se när meddelandet är skickat utan att behöva logga hela kommunikationen och meddelandet. *"Ibland finns det behov av att helt sonika stänga av loggningsfunktionen under kontrollerade former och istället förlita sig på omgivande systems loggning."* Detta beror helt på hur kritisk information som skickas. Även verifiering av riktighet, fullständighet och ursprung beaktas vid kommunikation.

Då det gäller avbrottshantering har enligt respondenten analyser gjorts och man kan i princip säga att samtliga processer på företaget riskerar att stoppas om en integrationsplattform stannar. Detta är speciellt viktigt då en integrationsplattform riskerar att vara en *"single-point-of-falure"* för hela företaget om inte tillräcklig driftsäkerhet är vidtagen. Detta kan gälla allt ifrån produktion i fabriker till beställning av kaffe till fikarummet. Konsekvenserna blir då missnöjda kunder och medarbetare. Det finns dock planer för att organisationsverksamhe-ten kan fortgå inom erforderlig tid efter ett avbrott eller fel i kritiska rutiner. En lösning på detta är att man skapar redundans i systemet.

Begränsningar i uppkopplingstiden kan användas där det är relevant. Oftast skickas ett enkelt meddelande till eller från integrationsplattformen och då blir uppkopplingstiden naturligt begränsad vid asynkrona anrop. *"Vid synkron kommunikation, alltså när sändare förväntar sig ett svar i samma anrop används sedvanliga timeouts beroende på vilken typ av kommunikation som görs."*

Användardokumentation som omfattar system och drift finns men är oftast undermåligt dokumenterad. Däremot finns det dokumentation som anger vilka säkerhetsåtgärder som administratören kan påverka. Säkerhetskonfiguration kan ingå vid installation men säljs även som en separat tjänst. Detta beror mycket på val och plattform och övrig plattforms-standard. Stora leverantörer som även levererar andra produkter relevanta för plattformens existens, till exempel operativsystem och databaser, har en säkerhetskonfiguration som är kopplad till deras egen och även konkurrenternas. Typiskt är det små leverantörer där man tillsammans med leverantören behöver fundera på en separat tjänst.

4.2 Respondent B

Utvecklingen för säkerhetsfunktioner inom integrationsplattformar är väldigt olika beroende på hur säkerhetskritiska system man implementerar i. Enligt respondent B har Biztalk i stort sett inga säkerhetsfunktioner. *"Men genom autentisiering på databasen som*

integrationsplattformen jobbar mot kan man få en säkrare inloggning". Kryptering är även viktig aspekt för utförandet av kommunikation.

Vid en implementation av en integrationsplattform finns inga funktioner påslagna och ej heller avslagna. *"Detta innebär att man själv kan välja vilken säkerhetsnivå man skall använda"*. Men detta beror på de omgivande systemen och vilka protokoll som man använder. Biztalk bör inte sättas utanför brandväggen om inte ett extra lager skapas.

Enligt respondenten finns inga säkerhetsrisker i samband med användandet integrationsplattformar då företaget använder ett WAN. På detta sätt blir integrationsplattformar inte är mer eller mindre öppna än resten av nätverket och ännu har inga problem uppstått.

Säkerheten vid processorkestreringen är även begränsad till databas eller operativsystemnivå. "*Det är sedan upp till den som designar integrationslösningen att bara ge rättigheter till informationen som de användare som skall ha tillgång till den får detta"*. Men det är även meningen att användaren skall använda data på den lokala databasen och därmed justeras behörigheten beroende på vilken rättigheter användaren har. *"Dock så finns ju alltid en risk att folk hackar sig in i en integrationsplattform och försöker stjäla information"*.

Man har inte upplevt ökade krav på kostnader för hantering av säkerhet i samband med användandet av integrationsplattformar. Respondent B har genom sin leverantör fått tillgång till ett antal best practices. *"Om man följer de "best practises" som följer med produkten så är denna uppbyggd på ett sätt så att systemet blir säkert"* Men oftast tar leverantörerna fram egna implementationer. Vid implementering kan policyn innanför brandväggen oftast behövas justeras.

För tillgång till information i ett bolag krävs ofta behörigeter och sådana behörigheter är oftast uppsatta i affärssystem och ofta på högre nivå än datamodellen. Det betyder att integrerad data/meddelanden ofta saknar information om behörighet. Detta innebär att man måste lita på att integrationsplattformen inte läcker känslig information och att mottagande system har tillräcklig säkerhets/behörighetslösning.

Många företagare använder inte Biztalk för integrationer eftersom det är en relativt ny produkt. Respondenten anser att det finns mycket kvar att göra med produkten och att den inte är riktigt mogen för marknaden ännu. *"Biztalk ses dock som en stor utmanare gentemot andra olika integrations plattformar på grund av att Biztalk är i nuläget liten och billig"*.

För att hantera användarhantering för konsulter som anpassar applikationen har företaget som respondent B arbetar för tagit fram arkitekturdokument och utvecklingshandböcker.

Varje användare har en unik användaridentitet för inloggning, och autentisiering sker mot active directory via LDAP. Däremot kan användarna ha direktåtkomst till vissa tjänster, men tills vidare låter kunden endast användare med behörighet att ha tillgång till allt.

Man har ännu inte gjort någon analys/design på säkerhetsperspektivet vid loggning. Respondenten vet att de relevanta händelser sparas under en fastställd tidsperiod men denne kan inte uttala sig om detta är tillräckligt säkert.

Analys av konsekvenser för att utreda olika typer av avbrott är en del av den strukturerade designprocessen för integrationer. Det finns även planer för att organisationsverksamheten där integrationsplattformen implementeras ska kunna återställas efter ett avbrott. *"Det körs för närvarande ett Katastrof-och-Kontinuitets-projekt för alla driftkritiska system (inklusive integrationsplattform) för att adressera denna fråga."*

Företaget använder ingen högteknologisk kvitteringsteknik för loggning. Man loggar alla mottagna och skickade meddelanden oförändrade om det bedöms meningsfullt vid designen av integrationen/flödet. Om det fanns ett behov av att införa ett säkrare loggningssystem skulle detta utformas men så är inte fallet.

Man beaktar behovet av verifiering av riktighet, fullständighet och ursprung för elektronisk överförd data vid kommunikation. Detta genom att lagra kompletta mottagna meddelande för varje avsändande system och integration då det anses meningsfullt. Beroende på hur överföringen sker finns det olika begränsningar. Det finns olika protokoll vid överföring av meddelanden. Respondenten anger tydligt att man idag inte ser kunden som någon säkerhetsrisk. När uppkoppling sker direkt mot integrationsplattformen så finns restriktioner för detta. (lösenord, nätverkssäkerhet, affärsavtal mm), uppkopplingsbegränsningen ställs in i protokollet. Vid RPC anrop sker detta automatiskt samt att det finns ett behov att *"känna"* motparten. Men dock ses inte detta som en central angreppspunkt. Skulle det ske uppkopplingar mot databasen så sker det via autentisiering.

Företaget har dokumentation som omfattar system-, drift- samt användardokumentation. Men planering pågår om att få dokumentation och lösning granskad av någon extern firma. Detta för att man är medveten om att dokumentationen inte är fullständig. Respondenten säger att denna *"kan inte direkt tänka på några säkerhetsåtgärder som administratören kan påverka och ej heller några dokumenterade sådana."*

Säkerhetskonfigurationen är en del av integrationen och levereras samtidigt vid köp av plattformen. *"Säkerhetskonfiguratione är en del av integrationen och det är därmed viktigt att inte öppna upp mer konton än nödvändigt"*. När outsourcing görs med företag som implementerar produkten så kan vissa säkerhetsrisker uppkomma. Dock så anser respondenten att inköp av färdiga lösningar kan vara bristfälliga, *"Då krävs även att man reglerar säkerhetslösningar i kontraktet (kravspecifikation), dessa skall även kontrolleras mot kravspecifikationen efter implementation"*.

4.3 Respondent C

Enligt respondent C kunde ingen information kring inloggningsprocessen och användaren uppges eftersom det ligger på en implementationsnivå som är styrd av leverantören (respondent C har ett tillverkarperspektiv för Websphere). Säkerhet är behovsstyrd efter de krav som ställs från verksamheten. Ett exempel där enorma krav ställs på säkerhet är inom bank och militär.

Det råder höga kostnader vid införandet av säkerhet i samband med användandet av integrationsplattformar. Respondent C uppgav att femtio procent av resurskostnaden vid integration läggs på adaptrar och att dessa är både dyra i inköp och spelar en viktig roll vid säkerheten *"En adapter för SAP-system kostar 500 000 SEK för att komma igång med dessa, detta är en kostnad som överskrider en ganska stor Biztalk-infrastruktur". Stora komplexa applikationssystem måste dock prata med resten av världen"*.

När man utgår från en serverbaserad arkitektur räcker det med att endast säkra upp servern. Detta gör det enklare att hantera säkerheten eftersom allt är på ett och samma ställe, nämligen servern. Mainframe och dumma terminaler gjorde det enklarae att hantera säkerhetsproblem, det räckte att säkra dessa två punkter vid ett klockslag till exempel vid kl. 08.00.

Enligt respondent C uppgavs att defintionen av Biztalk som integrationsplattform är missvisande och att detta kan få problem för säkerheten Det är snarare ett säkerhets problem ur arkitekts synvinkel. Integrationsplattformen berör mer området som hanterar routing av kommunikationen och processorkestrerings funktion. Varje system har separata säkerhetsdomäner där eget ansvar inom funktionsområde råder. Det som funktionsmässigt skall skötas av en integrationsplattform är att det inte skall finnas hårda kopplingar mellan system, detta för att inte skapa kaos inom integrationen.

Det är viktigt att de applikationer som skall integreras delar ut ansvar för säkerhet i den mån det är möjligt till integrationsplattformen eller mellanliggande komponenter. Detta när det gäller pålitligheten hos informationen, mapning mellan teknologiska API'er som .NET och Java, Mappning av datatyper och schema (skillnader inom datarepresentationen) och sist vidarebefordring till andra system (vilka system som skall påverkas vid olika events).

Processorkestrering och integrationsteknik är två skilda funktioner. Ett problem som uppstår när processlogik läggs i integrationsplattformen är att denna inte längre är *"stateless"* då det sker beräkningar inom själva integrationsplattformen. Det skall inte finnas ansvar för processlogik som prisberäkningar hos integrationsplattformen. En rekommendation från respondenten är att processorkestering och hantering av meddelande byggs i separata applikationer. Något som nämndes under intervjun var att det ofta finns hopp mellan olika operativsystem vilket utgör ett problem

Det finns ett sekventiellt beroende mellan datan som skickas vilket kan leda till problem då integrationsplattformar är flertrådiga applikationer som bearbetar ett antal meddelande parallellt samtidigt. Affärsprocesshantering tar bort denna *"statelessness"*. Det kommer då att hända incidenter vilket måste belysas. Har man tagit ansvar för transaktioner får man högre krav att kunna ansvara för säkerheten. Det är en dålig ide att lägga dessa på samma applikation.

Under intervjun kom det fram ett antal påståenden kring säkerhet som är värda att belysas:

-"Tycker att det som står i akademisk litteratur till 50 % inte stämmer överens med verkligheten eftersom det finns problem som inte belyses. Inom detta verksamhetsområde arbetar man med program som är upp till 20 år gamla. Det finns ofta upp till 10-tal olika tekniker i en verkligt integrerat IS vilket i sig är ett tydligt problem".

-"Bara för att teknik som FTP används i riklig omfattning betyder inte att det är en bra teknik. Utan snarare är det dyrare eftersom man måste bygga om systemet. Ofta måste man handskas med inneboende problem hos äldre teknologier som filbaserad integration".

-"FTP-protokollet används för 80 % av all den data som flyttas runt integrationsmässigt, inte för att den är bra men för att den stöds av industrin och är väl spridd. Det hävdas även att uppskattningsvis 65 % av all automatisering av affärstransaktioner sker via EDI".

Applikationer speglar ett företags processer men de behöver inte spegla hela verksamheten. Därför är det nödvändigt att bygga ut eller modifiera systemet. IS effektiviserar företags befintliga organisation. EAI får alltid denna effekt generellt. När någon slags förändring sker t.ex. genom nyförvärv eller förändringar inom den egna affärsverksamheten då speglar inte denna IT-infrastruktur hela verksamheten. Föråldrade applikationer kan inte slängas på grund av att utvecklingskostnaderna skulle skena iväg om allt nyutvecklades med den senaste tekniken. Företag förändras snabbare än sina applikationer, detta eftersom förväntningarna på affärstjänsterna ändras och integration handlar ofta om återanvändning

eller uppgradering av äldre system. Resultatet blir att befintliga applikationer klistras ihop till ett större s.k. metasystem som skall spegla företagets nuvarande affärsverksamhet.

Själva applikationerna som integreras är oftast säkra men det viktigaste är avseende deras tillgänglighet samt deras integritet i att datan inte ändras vid kommunikation. Det är vanligt att företag väljer att släta över säkerhetsrisker. Ett exempel är att det kan vara problematiskt att säkra upp gammal IT-infrastruktur som t.ex. Unix och PC-system.

Något som betonades av respondent C var att det är viktigt att tänka på vart data transaktionen exporteras, om den går över företagets egna nätverk eller över externa nätverk. Interna nätverk är oftast helt i sin ordning men vid externa nätverk blir man synlig och har inte längre direkt kontroller över hårdvaran och systemen som transporterar informationen. Man ska därför i synnerhet bekymra sig om kommunikationen sker bakom systemets brandvägg och inträffar det att den sker utanför ställs det då högre krav på säkerheten. Vid val av vilket protokoll som skall användas är detta då även viktigt att ta hänsyn till.

Applikationsintegration handlar om automatiserad kommunikation vilket ställer krav på säkerheten. Respondenten hävdar att integrationplattformen alltid är en säkerhetspunkt till exempel utifrån autentisering, *”För mig är den enormt stora mängden slutanvändare inget problem i sig, det är program som kommunicerar mellan integrationshubbar där hubben alltid är en säkerhetserver”.*

Vid god struktur i kommunikationen mellan applikationer är det lätt att använda kryptografiskt teknologi samt auktorisering för att säkra upp system. *”...det gäller att identifiera och eventuellt autentiserar alla inkommande kopplingar. Alltså datan som flyttas har en egen säkerhetskontext och om det blir typ alvarligt så vill man gärna kunna använda kryptgrafisk teknologi för att säkra på informationsnivå”*

Äldre varianter av API’er är dåliga ur säkerhetssynpunkt, ett exempel är vid en filbaserad integration som har inneboende problem. Eftersom säkerhetsproblem ärvs genom systemen som integreras kan systemet därför delas upp i nya säkerhetsdomäner efter hand som olika system integreras. Respondenten framhåller att integrationsplattformen är som en central punkt för att säkra upp informationssystem. Ett bra exempel är där 500 personnummer samlas i en gemensam fil för att utbytas med ett annat system och i ett annat fall där de sedan delas upp i 500 mindre objekt där varje nytt objekt representerar ett personnummer. Sannolikheten för fel när man klumpar ihop data är väldigt mycket högre då kontrollsummor inte har samma kontroll över att datan t.ex. behåller sin ursprungliga form.

Under intervjun så lyfts det fram att integrationplattformen utgör en stabil grund för att förbättra säkerheten i befintliga system. Den ökar möjligheten att kunna övervaka systemet och ger bättre kontroll av miljön i jämförelse med punkt till punkt integration. Säkerhet är större än integrationsplattformen, det handlar om domäner av säkerhet. Det betonas att man vid uppgradering av äldre teknologier till nyare system ska uppmärksamma att säkerhetsproblem ärvs över de system som är sammanknutna och att dessa måste säkras upp till den minsta nivå som skall gälla över alla system som integreras.

Det är därför viktigt att kunskap finns för att bedöma säkerheten på befintlig teknologi som skall integreras och hur mycket den måste säkras upp för att inte utgöra en risk till de system som den kopplas samman med.

5 Analys av respondenternas svar och kopplingen till säkerhetskoncepten

Inom detta kapitel kommer vi att koppla ihop referensramens koncept med respondenternas svar och på detta sätt skapa ett följsamt resultat som är kopplat till de olika koncepten.

De säkerhetsrisker som kan dykas upp vid användandet av integrationsplattformar i ett IS är flertal och väldigt beroende av hur integrationsplattformens miljö är sammansatt. Man måste även inom ett företag enas om en gemensam definition av en lämplig säkerhetsnivå. De måste ta ett beslut om vad begreppet innebär för just dem, i fråga om vad de tänker ha en säkerhetspolicy kring, men även vilken nivå de tänker lägga ribban på. Ett exempel på dessa variabler står att läsa om i kap 4.1 där SIG Security presenterar de viktigaste (SIG Security, 2005). Om förändringar av definitionen skulle inträffa i framtiden bör det även uppdateras inom policyn.

Utifrån empirin som samlats har utvärdering gentemot säkerhetskoncepten kunnat utföras.

5.1 Sekretess, integritet och tillgänglighet (CIA)

Integritet (Integrity) är ett viktigt men svårt koncept eftersom det krävs ett starkt förtroende mellan sändaren och mottagaren vid dataöverföringen. Vid integrationsplattformar krävs en säker kommunikation under överföringen. Genom att skapa ett konto med begränsade rättigheter uppnår man säkerhet. Beroende på vilken lösning man har släpper integrationen in och ut olika användare, detta för att förhindra att systemet kodas om för mycket.

Säkerheten i Biztalk regleras mycket genom det operativsystem man använder för att köra integrationsplattformen på. I Biztalk's fall används Microsoft Windows, och detta operativsystem i sig har vi inte undersökt. Dock så finns det flera hot som kan uppstå vid användandet av detta operativsystem (virus, hacking och med mera). Säkerheten i Websphere använder sig av en kryptografisk teknologi.

När det handlar om transport av känslig data så kan ett behov av att öppna upp olika system uppstå. Detta medför att systemen i sig blir mer intoleranta mot angrepp och på så sätt även mer osäkra för angrepp såsom modifiering av meddelandet. Dock så sker en verifiering av riktighet, fullständighet och ursprung vid kommunikation och på detta sätt säkerställer integrationsplattformen att meddelandet kommer från rätt person (ursprung), ej är modifierat (riktighet) och att meddelandet är fullständigt.

För att uppnå *integritet* vid integrationsplattformar bör man sätta upp administrativa regler för inloggningssystemen. Enligt vår studie sker loggningen inom integrationsplattformar oftast både i mottagande och sändande applikation. Loggningen kan även stängas av under kontrollerade former för att sedan förlita sig på omgivande systems loggning. Eftersom man förlitar sig så starkt på integrationsplattformar kan det även leda till att man inte upptäcker de riskerna som ej uppenbarar sig omedelbart.

Integrerad data saknar oftast information om behörighet detta gör att man förlitar sig på att integrationsplattformen inte läcker ut känslig information och att mottagande system har en behörghetslösning. Genom att låta endast användaren med behörighet få tillgång till det den ska, uppnås *sekretess* (confidentially). Men för att uppnå hög säkerhet och full sekretess vid dataöverföring måste datan krypteras.

Vid design av integrationslösningar kan man utforma rättigheter till den information som användare ska ha tillgång till men det är viktigt att inte öppna upp mer konton än nödvändigt. Att lagra kompletta mottagna meddelanden för varje avsändande system och integration anses meningsfullt. Med hjälp av detta kan man kontrollera och spåra upp användarna och skapa en säkrare miljö för integrationsplattformen. Om ett avbrott skulle uppstå vid en integrationsplattform skulle detta förhindra kommunikationen och därför är det svårt att uppnå full *tillgänglighet (*availability).

Vid implementering av intergrationsplattformar kan man beroende på vilken säkerhetsnivå man väljer lägga till olika säkerhetsfunktioner. Företagen kan köpa delar av funktioner för att skapa en säkrare integrationsplattform. Vid integrationsplattformen Biztalk rekommenderas extra lager av funktioner såsom en brandvägg.

5.2 Ansvarsskyldighet, autentisering, auktorisering, kryptering och felhantering (AAA)

Vid användandet av Biztalk som integrationsplattform så finns funktioner som möjliggör att man kan spåra handlingar som är utförda. Detta sker till största delen genom loggning. Funktioner som gör det svårt eller omöjligt för en användare att avvisa eller förneka vissa handlingar finns även i systemet. Beroende på hur omfattande loggningen är kan dessa uppgifter syfta till att ansvarsskyldighet uppnås. Det finns även funktioner för behörighet till information. Dessa styrs av affärssystemet som integrationsplattformen är kopplad till.

Systemet för *autentisiering* är uppbyggd utifrån de grupper som finns i operativsystemet. I övrigt har varje användare en unik identitet då denna ska använda integrationsplattformen som meddelandehanterare. *Autentisieringen* beror även på hur den som designar plattformen har delat ut rättigheter för olika funktioner. Det finns dock vissa tjänster som användarna kan ha direktåtkomst till. I loggningen kan även användarnas identitet registreras för att sedan enkelt kunna spåra vem som har gjort vad.

Applikationsintegration handlar om automatiserad kommunikation vilket ställer krav på säkerheten. Respondenten hävdar att integrationplattformen alltid är en säkerhetspunkt till exempel utifrån autentisering, *" För mig är den enormt stora mängden slutanvändare inget problem, det är program som kommunicerar mellan integrationshubbar där hubben alltid är en säkerhetserver*

Då integrationsplattformen jobbar med kommunikation mot många system finns valet att använda *kryptering* vid denna. Men mycket beror även på omgivande system och vad dessa har för krypteringsalternativ. Då kommunikationen sker via ett antal olika protokoll finns även möjligheten att använda den inbyggda krypteringen i dessa.

Vid avbrottshantering har analyser gjorts, men dock så finns risken att samtliga processer i företaget stannar. Analysen är relevant att utföra då integrationsplattformen tenderar till att vara en länk som hela företaget är beroende av. Det är därför viktigt att uppnå tillräcklig driftsäkerhet i systemet. Det finns även planer för hur man skall fortgå efter ett avbrott eller fel som har uppstått i samband med integrationsplattformen. Redundans skulle kunna vara en åtgärd för detta. Det finns dock ändå en möjlighet att systemet blir ett objekt för olagliga intrång och förstörelse, ett sådant problem löses genom åtskilliga andra säkerhetslösningar.

Biztalk anses vara mindre krävande och har inte all funktionalitet som finns i Websphere. För att skapa en enkel bild av Biztalk och Wepshere kan man för egen uppfattning jämföra Biztalk med wordpad och Websphere med MS Office Word 2003. Biztalk har sämre

funktionalitet för att koppla upp sig mot andra plattformar än Websphere. Vilket medför att det inte går att likställa produkterna då olika plattformar skiljer sig åt funktionsmässigt.

Det är viktigt att kunskap finns för att bedöma säkerheten av befintlig teknologi som skall integreras och hur mycket den måste säkras upp för att inte utgöra en risk till de system som den kopplas samman med.

Säkerhetskoncept	**BizTalk**	Websphere
Sekretess	Ja, sekretess sker genom kryptering	Ja, sekretess uppstår via en kryptografisk teknologi då rätt information ska nå rätt mottagare
Integritet	Ja, om administrativa regler för inloggningssystem utförs	Ja, dataintegritet
Tillgänglighet	Nej, systemet är ej till 100 % tillgängligt. Men genom plan för avbrott i systemet kan man uppnå mer tillgänglighet i systemet	Ja, om verksamheten utfört en god plan för avbrott i systemet.
Ansvarsskyldighet	Ja, om verksamheten tar ett sådant beslut	Ja, tilldelning av ansvar utförs för att säkra upp kommande risker. Viktigt att applikationer som integreras delar ut ansvar för säkerhet
Autentisering	Ja, via SSL.	Ja, via SSL.
Auktorisering	Ingen uppgift om detta	Ja, genom att identifiera alla inkommande kopplingar
Kryptering	Ja, möjlighet till kryptering finns	Ja, med en kryptografisk teknologi för att säkra upp system.
Felhantering	Ja, genom att skapa riskanalyser vid implementering	Ja, för att undvika avbrottshantering görs redundans av databasen

Tabell 3 Tabell på säkerhetskoncepten på Biztalk och Websphere.

Utifrån respondenternas svar har vi fått information om hur integrationsplattformar fungerar och hur säkerheten är runt dessa. Utifrån litteraturstudien och empirin har vi lyckats få djupare förståelse på hur integratiosnplattformen fungerar och vilka säkerhetsåtgärder som påverkar dess fullständiga säkerhet. Det är nämligen så att det finns inbyggda funktioner hos integrationsplattformar som måste anpassas till omgivande systems säkerhetsfunktioner. Men dock har ingen av respondenterna uttalat att de känt sig begränsade av de ramar som integrationsplattformarna sätter för säkerheten.

5.3 Jämförelse av Biztalk och Websphere

De två integrationsplattformarna som vi utgått från är Microsoft´s Biztalk och IBM´s Websphere. Dessa integrationsplattformar har olika designupplägg och systemarkitektur men har likadan funktionalitet. Biztalk har sämre funktionalitet för att koppla upp sig mot andra plattformar än Websphere.

Det finns olika produkter inom Websphere familjen som kan ses likvärdiga med Biztalk men eftersom Websphere är en stor familj finns det olika produkter som överglänser Biztalk på flera olika punkter. Websphere kan även delas in i olika kategorier beroende på vilken funktionalitet man vill ha på systemet. Detta gjorde det svårare för oss att utvärdera säkerheten hos denna teknik.

Biztalk är kopplat till Microsoft Windows och därför styrs säkerheten mycket av operativsystemet (Respondent A, 2006). Websphere styrs också till stor del av operativsystemet, men varför anses denna produkt mer säkrare än Biztalk?

Vi är medvetna om att komplexitet råder vid stora system till exempel vid flera sammankopplade system. Vid komplexa system blir det oftast dyrt att säkra upp sig, detta eftersom många system är sammankopplade. Därför är det viktigt att hantera säkerheten på ett enkelt sätt som möjligt till exempel genom att följa olika riktlinjer samt rekommendationer. Att tilldela ansvar inom varje system gör det även enklare att hantera säkerheten. Man bör då ta hänsyn till de andra systemen man integrerar sig med.

Beroende på vilka rättigheter som är konfigurerade på integrationsplattformen, har både Biztalk och Websphere stöd för autentisering via SSL, vilket framgår ur tab. Därför kan både Biztalk och Websphere likställas vid autentiseringen.

En annan anledning till att Websphere anses säkrare kan vara att Biztalk är en ny produkt som ännu inte är fullt utvecklad. *”Biztalk ses dock som en stor utmanare gentemot andra olika integrations plattformar på grund av att Biztalk är i nuläget liten och billig”* (Respondent C). Mer kunskap och erfarenhet kring produkten är i behov. Ett förslag är dokumentera och sammanställa någon form av ”Best practices” så att man kan ta lärdom av de misstag som uppstått hos integrationsplattformen.

Integrationsplattformens omgivning har en viktig betydelse för hur säkert systemet är. Anledningen till att Websphere anses vara säkrare, kan vara för att man vid stora och komplexa system blir tvungen att införa hårdare kontroll och övervakning.

Något som är värd att belysas är att man inte behöver ha ett säkert system bara för att man följer alla säkerhetskoncept eller utför dyra säkerhets investeringar. Man måste även vara medveten och ha kunskap om sitt system. Detta genom att analysera fram verksamhetens innan man implementerar någon integrationsplattform. Innan en implementation av en integrationsplattform bör en analys utformas på säkerheten som företaget kräver genomföras och eventuellt måste även säkerhetspolicyn uppdateras så att dessa stämmer överens. Om inte en fullständig genomgång av säkerheten genomförs kan det leda till stora konsekvenser för ett företag, till exempel när man sänder ut känslig information genom integrationsplattformen.

Säkerhetsrisker som uppkommer i samband med användandet av integrationsplattformar är sådant som har följt med ifrån den gamla tekniken. Exempel på detta kan vara, transport av

känslig data och system som behöver öppna sig för att möjliggöra åtkomst av data. *"I en automatiserad process där integrations-plattformen ska göra många saker samtidigt, så krävs det stor tillåtelse för integrationsplattformen att göra saker i många olika system och detta kan ses som en säkerhetsrisk"*. Detta löses dock genom att skapa ett konto med mycket funktionalitet men nödvändigtvis inte mycket rättigheter.

Var går egentligen gränsen för säkerheten vid ihopkoppling mellan olika säkerhets-domäner, så att inga glapp kan uppstå som äventyrar säkerheten?

För att ett företag ska undvika säkerhetsrisker av integrationsplattformar bör man till exempel implementera säkerhetskonfiguration. Säkerhetsriskerna kan vara många om man inte tar hänsyn till vad för slags data som skickas till och från integrationsplattformen. Man bör även ta hänsyn till om plattformen används inom det egna företagets nät eller om det är sammankopplat med andra system utanför ens verksamhet. Om detta sker måste en högre säkerhet implementeras. Detta innebär att säkerheten är behovsstyrd, vilket beror på olika resurser och hur säkert företagets information behöver vara.

Vi bör även ta hänsyn till att många företag idag outsourcar sin IT verksamhet, vilket medför ytterligare risker för integrationsplattformen. Men beroende på företagets ekonomi, kunskap och prioritering av säkerhet kan man utforma den önskade säkerhetsnivån. Det är genom kunskap och erfarenhet som man undviker säkerhetsrisker hos integrationsplattformen

Vid applikationsintegration är säkerheten beroende av att man har kunskap om de system och integrationstekniker som binds samman då säkerhetsproblem ärvs. Genom till exempel kryptering och autentisiering mot databasen skapar man en säkrare miljö för integrationsplattformen. Kedjan är inte starkare än den svagaste länken.

Integrationsplattformar kan även ha en bristfällig säkerhet på grund av den mänskliga faktorn och kontrollen av behörighet. Vid auktorisering är det viktigt att ha ett säkert lösenord och dessutom byta detta med jämna mellanrum i enlighet med företagets säkerhetspolicy. Vid vissa fall av integrationen skapas ett konto med större rättigheter för styrning av hela, eller vissa delar av systemet, än vad som krävs. Detta konto kan ha ett starkt lösenord, men problem som kan uppstå är om flera användare och applikationer delar detta gemensamma konto. Då bör lösenordsbyte ske, vilket man ofta bortser ifrån för att göra. Detta eftersom det är smidigt för varje individ som arbetar med integrationsplattformen. Detta borde regleras i säkerhetspolicyn på företaget och även kontrolleras att denna åtföljs och är aktuell efter införandet av en integrationsplattform i IS'et.

Då integrationsplattformen är en central funktion och även en central punkt för kommunikationshantering i företaget får detta ett antal olika följder (detta kallas för single-point-of-failure). Detta innebär att om integrationsplattformen slutar fungera kan hela påverka företaget och leda till oönskade konsekvenser. Det är därför viktigt att ta hänsyn till detta vid implementering så att redundans skapas i systemet.

Genom att tilldela säkerhets ansvar kan man lättare hantera kommande framtida förändringar. Det finns även positiva följder av centraliseringen eftersom all kommunikation sker genom denna del av systemet. Det blir då lättare att övervaka systemet ur en administrativ synvinkel och man får även en centralisering av ansvaret.

Vi nämnde under den empiriska studien att *"applikationer speglar ett företags processer men att de inte alltid behöver spegla hela verksamheten"*. I detta fall innebär det att integrationsplattformen

Websphere skapar en säkrare miljö. Detta genom att informationen inte modifieras på ett obehörigt sätt. Detta täcker även säkerhetskonceptet *riklighet* som anser att känslig information inte ska avslöjas för obehöriga eller andra användare utanför säkerhetsnivån.

"För mig är den enormt stora mängden slutanvändare inget problem, det är program som kommunicerar mellan integrationshubbar där hubben alltid är en säkerhetserver" (Respondent C).

Den nya tekniken för applikationsintegrations kan få konsekvenser för säkerheten. Då integrationsplattformar kopplas samman med många andra system är det möjligt att det uppstår säkerhets risker. Men genom att bygga ut tekniken med extra funktioner kan man skapa en säkrare miljö kring integrationsplattformen.

6 Slutsatser

Syftet med vår uppsats är att undersöka om det finns säkerhetsrisker med användandet av integrationsplattformar vid applikationsintegration. Följande slutsatser har framställas för att ge svar på vår undran.

– Vi har dragit slutsatsen av att Biztalk och Websphere kan endast likställas i fråga om autentiseringen men inte i allmänhet. Detta eftersom de har olika design upplägg och systemarkitektur, men de har dock likadan funktionalitet. Biztalk har sämre funktionalitet för att koppla upp sig mot andra plattformar än Websphere.

– Vid koppling mellan ny och gammal teknik kan konsekvenser för integritet i systemet uppstå. Detta för att om det finns brister i den gamla tekniken där säkerhetsproblem fortfarande existerar, medför detta att säkerhetsrisken blir den svagaste länken i integrationen. Informationssystemet i helhet ärver säkerhetsproblem via system. Därför har vi dragit slutsatsen att det finns säkerhets risker hos integrationsplattformar.

– För att ett företag skall undvika säkerhetsrisker hos integrationsplattformar bör man till exempel implementera korrekt säkerhetskonfiguration. Beroende på företagets ekonomi, kunskap, och prioritering av säkerhet kan man utforma den önskade säkerhetsnivån. Genom kunskap och erfarenhet kan man undvika säkerhetsrisker hos intergrationsplattformen.

7 Slutdiskussion

Inom detta kapitel kommer vi att ge ett förslag på reflektioner och idéer kring fortsatt forskning kring hur vår uppsats kan följas upp.

7.1 Egna reflektioner

Det är en viktig insikt att explorativ studie i kombination med en metod av kvalitativ karaktär i väldigt hög grad bestäms av dem som sedan skall analysera svaren och försöka skapa ett logiskt sammanhang vid tolkningen av forskningsunderlaget. Vi har fått svar på väldigt mycket kring vår frågeställning och om ämnet integrationsplattformar i sen helhet, men vi hade så här i efterhand önskat en djupare litteraturstudie kring de två integrationsplattformarna *Biztalk*, *Webspshere* i kombination med egen praktisk erfarenhet av att ha arbetat med dessa. Vi hade då kunna bilda en egen uppfattning om det olika abstraktionsnivåerna som behandlas under säkerhetsavsnittet och då kunna ställa mer konkreta frågor och ifrågasätta svaren vi fått under intervjun på ett mer tillfredställande sätt.

För att skapa kvalitet på intervju svaren och uppnå hög reliabilitet skickade vi ut frågorna i förväg via e-post. Detta för att kontrollera och undvika misstolkningar vid intervjun. Men vår metod för undersökningen var tidskrävande eftersom hög svårighetsgrad rekommenderades vid studie av säkerhetsfrågor vid nya produkter. Detta på en marknad i ständig förändring, såsom i detta fall integrationsplattformar.

Att finna lämpliga respondenter var krävande eftersom studien kräver kunskap från experter inom både säkerhets område och integrationsplattformar. Området har tidigare inte utforskats vilket resulterade till en långvarig förstudie inom säkerhet och integrationsplattformar.

7.2 Framtida forskningsfrågor

Området kring integrationsplattformar är idag nytt och det skulle ha varit intressant att se ytterligare studier kring säkerhet och integrationsplattformar i framtiden. Det verkar inte finnas så mycket objektiv litteratur kring just integrationsplattformar ur en konceptuell vy. Eftersom vi ser brist på detaljerad kunskap kring säkerhet hos integrationsplattformar är ett förslag att forska vidare. Fler riktlinjer eller dokumentation på integrationsplattformar är en önskan från oss. Vi hoppas att ett intresse väckts hos er och kanske blir ni de kommande forskarna.

8 Författarnas tack

Vi vill tacka alla företag och deras respektive anställda som har ställt upp på våra intervjuer, de ville att svaren skulle behandlas konfidentiellt men ni vet vilka ni är. Dessutom vill vi rikta ett särskilt tack till Carl Thyberg från WM-data som fungerat som vår vägledare då funderingar kring området dykt upp. Vi vill även tacka vår handledare Jörgen Lindh på Internationella Handelshögskolan i Jönköping som har sporrat oss att fortsätta prestera när modet varit lågt och hindren känts svåra att överstiga.

Referenslista

Berglund. J., Bjelkemyr. M., & Håmås. J (2002*). Bankernas olika tekniker för säkerhetslösningar på Internet. Hämtad från,*
http://jibsnet.hj.se/documents/files/download/502414382/5139619303093608081/Bankernas % 20olika % 20tekniker%20f % F6r%20s%E4kerhetsl%F6sningar%20p%E5%20internet.doc

Bishop, M. (2004). *Introduction to computer security*. Boston: Pearson education.

Chappell, D.A, Chopra, V., Dubray, JJ., Van der Eijk, P., Evans, C., Harvey, B., McGrath, T., Nickull, D., Noordzij, M., Peat, B., Vegt, J. (2001). *Professional EbXML Foundations*. Storbritanien: Wrox press ltd.

Dataföreningen (2006). *SBA Check*. Hämtad 2006-04-23 från,
http://www.dfs.se/products/sba/check/

Davies, S., Broadhurst, P. (2005). *WebSphere MQ V6 Fundamentals*. IBM Redbooks

Goldkuhl, G., (1998). *Kunskapande*. Internationella Handelshögskolan i Jönköping & Centrum för studier av Människan, Teknik och Organisation (CMTO) Linköpings universitet

Gunnarsson, R. (2002). *Valliditet och Reliabilitet*. Hämtad 2006-03-05 från,
http://www.infovoice.se/fou/bok/10000035.htm

Linthicum, D.S. (1998). *Message brokers Rising*. Hämtad. 2006-02-08 från,
http://www.dbmsmag.com/9809d07.html

Linthicum, D.S. (1999). *Mastering Message Brokers*. Published: *Integration learning center*. Hämtad. (2006-02-08). http://microsites.cmp.com/print/

Linthicum, D.S (2004). *Next Generation Application Integration from simple information to web services*. Boston: Pearson education.

Microsoft, (2001). *Microsoft BizTalk Server 2000: Documented*. Washington: Microsoft Press

Middleware resource center. (2006) *Middleware resource center*. Hämtad 2006 03-02 från,
http://www.middelware.org/mom/broker.html

Milton, T. (2002). *BizTalk Server 2000 Developer's Guide for .NET*. Rockland:Syngress Publishing.

MSDN. (2006). *Message Broker*. Hämtad: 2006-04-24 från, http://msdn.microsoft.com/library/default.asp?url=/library/enus/dnpag/html/ArchMessageBroker.asp

MSDN. (2006). *Introducing BizTalk Server 2006* Hämtad 2006-05-09 från, http://msdn.microsoft.com/library/default.asp?url=/library/en-us/bts06gettingstarted/html/06a4a31a-eefe-4b1b-89ca-2cba2b6fa587.asp

Karlsson, H. G., Keisu, T., Lantz, M., Lundin Andersson, M., Osvald, T., Karlsson, J. (red.). (1997). *Riktlinjer för god informationssäkerhet SSR79ETT*. Lund: Studentlitteratur.

Sadtler, C., Coumo, G., Ganci, J., Haberkorn, M., Jones, C., Kovari, P., Griffith, K., Marhas D., Will, R. (2005). *Websphere product family overview and architecture*. North Carolina: IBM Redbooks.

SIG Security. (2005). *SIG Security*. Hämtad 2006-03 27 från, http://www.sigsecurity.se/web-content/

Svenning, C. (1996). *Metodboken*. Lorentz förlag.

Tanenbaum, A. (2003). *Computer Networks* (uppl. 4). New Jersey: Prentice Hall.

Tipton, F. H., Krause. M. (2001), *Information Security Management Handbook* (uppl. 4), Boca Raton: CRC Press

WM data. (2006). *WM data*. Hämtad 2006-04.03 från, http://www.wmdata.se/wmwebb/content.asp?

Statskontoret (2003). *Speficikation produkter och tjänster*. Hämtad från http://www.avropa.nu/upload/Bilagor/Aktuella/STK-6692-04-Ementor/Bilaga%204%20Specifikation%20av%20Produkter%20och%20tj%C3%A4nster.doc

Bilaga 1 Intervjufrågor

A. Generella inledande frågor

1. Hur länge har du jobbat inom IT-branschen?
2. Vilken bakgrund har du t.ex. utbildning, tidigare erfarenheter?
3. Har ni någon avdelning på företaget som enbart arbetar med säkerhet?
4. Har du erfarenhet av arbete med IT-säkerhet själv?
5. Vilka integrationsplattformar har ni erfarenhet av (VM-Data)?
6. Hur ser ni på utvecklingen för integrationsplattformar säkerhetsfunktioner?
7. Har ni upptäckt några nya säkerhetsrisker i samband med användandet av denna teknik (integrationsplattform)?
8. Har ni upplevt ökade krav så som mer kostnader för hantering av säkerheten i samband med användandet av integrationsplattformar?
9. Finns det någon säkerhetspolicy som ni följer vid implementation av integrationsplattformar hos kunder?
10. Vilken påverkan kan en implementation av integrationsplattform ha på ett företags interna säkerhetspolicy? Var och om dessa nu kommer i kontakt med varandra?
11. Finns det punkter inom säkerhetsområdet där de två marknadsledande produkterna (Websphere, Biztalk) skiljer sig åt både avseende tekniska lösningar och design för kund (nivå för anpassning)?
12. Finns det något avseende ovan nämnda frågor som du önskar tillägga till intervjun?

B. Användare och Inloggning

13. Finns det användarhantering för konsulter som anpassar applikationen?
14. Har varje användare en unik användaridentitet och ett personligt lösenord som bara han/hon kan ändra och känner till så att aktiviteter kan spåras till den ansvarige individen? samt är lösenordet minst sex tecken långt och tvingas alla användare att byta lösenord med ett intervall som systemet fastställt?
15. Har användarna direktåtkomst enbart till de tjänster som de särskilt har fått behörighet att använda?
16. Loggas, ur ett säkerhetsperspektiv, relevanta händelser och sparas dessa loggar under en fastställd tidsperiod?
17. Hur anser du att ovan nämnda funktioner hos integrationsplattformen påverkar säkerheten gentemot tidigare teknologi?
18. Finns det något avseende ovan nämnda frågor som du önskar tillägga till intervjun?

C. Säkerhet och avbrottshantering

19. Har det gjorts en analys av konsekvenserna för verksamheten vid olika typer av avbrott i integrationsplattformen/motorn?
20. Finns det planer för att organisations verksamhet där integrationsplattformen implementeras ska kunna fortgå eller återställas inom erforderlig tid efter ett avbrott eller fel i kritiska rutiner, finns det redundans i systemet?
21. Används funktioner som syftar till att göra det omöjligt för en användare att förneka eller avvisa att en viss handling är mottagen eller ej (oavvislighet)?
22. Beaktas behovet av verifiering av riktighet, fullständighet och ursprung för elektronisk överförd data vid kommunikation?
23. Finns begränsningar för uppkopplingstiden till integrationsplattformen?

24. Skiljer sig resursåtgången gentemot tidigare teknologier för att säkerställa att ovanstående punkter följs om det fall de efterlevs?
25. Finns det något avseende ovan nämnda frågor som du önskar tillägga till intervjun?

D. Dokumentation

26. Finns en fullständig dokumentation som omfattar system-, drift- samt användardokumentation?
27. Finns det någon driftdokumentation som bl.a. anger vilka säkerhetsåtgärder som administratören kan påverka?
28. Ingår säkerhetskonfigurationen vid installation eller levereras detta i samförstånd med kund som en separat tjänst?