Extranet för slutkunden

(HS-IDA-EA-99-418)

Adam Rehbinder (a95adare@student.his.se)

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

Examensarbete på det dataekonomiska programmet under vårterminen 1999.

Handledare: Ingi Jonasson

Extranet för slutkunden

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

990611

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

Signerat: _____

Extranet för slutkunden

Adam Rehbinder (a95adare@student.his.se)

Sammanfattning

Detta arbete har för avsikt att belysa problem och möjligheter för företag att utnyttja IT och webbteknik för att kommunicera direkt med slutkunder. Avsikten är att ta tillvara kundernas kunskap om produkterna för att underlätta utveckling av nya produkter, förbättra befintliga, och därigenom öka värdeskapandet hos de produkter som företaget tillhandahåller. Genom givande och tagande av information bör således förutsättningar skapas för förbättringar av en produkts kvalitet och därmed värdeskapande i alla led och för samtliga intressenter.

För att göra detta menar jag att ett kundfokuserat extranet kan skapas. Detta är ett extranet som sammanknyter slutkunder med företag, kunder och leverantörer. Kopplingen dem emellan består i att dessa intressenter har en relation till en unik produkt förvärvad av slutkunden. Ett kundfokuserat extranet är således ett extranet för informationsspridning och insamling där information tillgängliggörs som en webbtjänst för slutkunder och utvalda aktörer om en unik produkt, förvärvad av kunden.

Nyckelord: Kundfokuserat extranet, extranet, säkerhet, nätverksarkitekturer

Innehållsförteckning

1 Inledning

Traditionellt sett betraktas företag som organisationer som på ett så rationellt och effektivt sätt som möjligt samordnar produktionsfaktorer för att skapa lönsamhet och därigenom överlevnad (Wikström m.fl., 1998).

Detta innebär att det företag eller den organisation, som effektivast och till lägst kostnad producerar en produkt och med denna produkt bäst uppfyller sina kunders önskningar och krav, dvs har rätt kvalitet, är det företag som har störst chanser till långsiktigt god lönsamhet (Sandholm, 1995). Således är lönsamhet förbundet med kvalitet.

Den kvalitet som jag, i denna bemärkelse, avser definieras enligt Sandholm (1995, s 10) som de ”sammantagna egenskaper hos en produkt som ger dess förmåga att tillfredsställa uttalade eller underförstådda behov”. Med kvalitet avses även en produkts lämplighet för användning i alla sammanhang där den förekommer, samt dess förmåga att tillföra nya egenskaper som kan vara outtalade av kunden men som upplevs som positiva (Sandholm, 1995).

Kvalitetsbegreppet innefattar enligt ovanstående påstående kvalitet i kärnprodukten och kvalitet i de kringtjänster, som har till syfte att öka värdeskapandet kring produkten hos berörda intressenter. Därmed inkluderas också kringtjänster, som kunden vanligtvis inte väntar sig vid köp av en produkt men som ökar kundens tillfredsställelse och eventuellt kan motivera ett högre pris på produkten. Jag avser att studera möjligheter och problem vid skapandet av en sådan kringtjänst. Denna kringtjänst baseras på givande och tagande av information där webbteknik skapar förutsättningar för en effektiv kommunikation. En kringtjänst av denna typ inbjuder till dialog mellan kunden och aktörer som har intresse i relationen mellan kunden och dennes produkt. En sådan tjänst syftar till att gagna alla inblandade och därmed öka produktens värdeskapande förmåga under dess livscykel.

Genom ökad kvalitet och attraktiva kringtjänster har företag också möjlighet att skapa och underhålla en lojal kundkrets som köper företagets produkter om och om igen (Wikström m.fl., 1998). Kringtjänster och kvalitetsmedvetande kan således öka en produkts värdeskapande och förbättra företagets anseende hos sina kunder.

Wikström m.fl. (1998) menar att företag i dagsläget ser kunden som ett objekt till vilket företagen säljer en produkt. I detta tankesätt hanterar vanligen företaget på egen hand hela den värdeskapande processen, dvs de aktiviteter som tillför en produkt värde. Den möjliga typ av kringtjänst jag undersöker baserar sig på ett nytt sätt att tänka. Det nya tankesättet innebär att företag ökar värdeskapandet kring sina produkter genom att slutkunder och leverantörer på ett tidigt stadium involveras i utvecklingsprocessen och att dessa ses som samarbetspartners i alla delar av en produkts livscykel. Företagen framstår därmed som organisatörer av den värdeskapande processen (Wikström m.fl., 1998).

Synen på kunder och leverantörer som samarbetspartners leder enligt Wikström m.fl. (1998) till en ökad vilja att dela information med dessa. Detta har fått genomslag bl.a. genom utvecklandet av extranet som med webbteknik knyter samman kunder och leverantörer med det egna nätverket (Pfaffenberger, 1998). Ett extranet är vidare enligt Loshin (1997) ett nätverk som korsar organisatoriska gränser och ger utomstående intressenter möjlighet att på ett kontrollerat sätt nå information i ett företags interna nätverk.

1 Inledning

I dagsläget sammanbinder ofta extranet ett företag med stora kunder och stora leverantörer för att minska kapitalbindning i lager, för att effektivisera företagens aktiviteter och inte minst för att ta fram bättre produkter med lägre pris och högre kvalitet (Pfaffenberger, 1998). Ett extranät torde även kunna användas för att på ett säkert sätt temporärt inbjuda även den enskilde slutkunden i dialog med företaget. Detta torde öka möjligheterna för företaget att på olika sätt kommunicera effektivt med varje enskild slutkund. En sådan direktkommunikation skulle kunna leda till att företaget kan ta del av den unika kundens erfarenheter och kunskap om en produkt. Detta kan t.ex. ske i utbyte mot att företaget delger kunden relevant information om produkten.

Jag avser undersöka möjligheter till stöd för direktkommunikation mellan ett företag och varje enskild kund. Vilka möjligheter och problem uppstår, då ett företag eller en grupp intressenter delar information med slutkunden i ett webbaserat extranet, där kunden enkelt kan hämta information och ge feedback om en unik produkt? Med unik produkt avses här vad kunden köpt och inte beteckningen på en tillverkningsserie.

Antag att en slutkund och övriga intressenter med skilda inloggnings- och autentifikationsmetoder får tillgång till eller kan uppdatera information om relationen mellan kunden och en unik produkt och därefter sammanställa för dem relevant information. Detta innebär att slutkunder och övriga intressenter har möjlighet att ge feedback om en unik produkt. Detta kan resultera i möjligheter för inblandade aktörer och för en slutkund att belysa kvalitetsrelaterade och produktrelaterade problem. Dessutom skulle kunden kunna ge feedback om möjligheter och erfarenheter och dessutom berätta om hur en produkt upplevs. Jag menar att detta kan skapa möjligheter att analysera information om varje produkt med avseende på dess funktion, beteende och lämplighet i den verkliga användningsmiljön. Sådan information är troligtvis intressant för företagens produktutveckling och marknadsföring. Denna feedback kan även komma från andra intressenter som har intresse i relationen mellan kund och produkt. Kunden kan genom att lämna information kanske få tillgång till uppdateringar, förbättringar och tillbehör som utvecklats och som ökar produktens lämplighet och kvalitet.

Att företaget får feedback om unika produkter innebär möjligheter till information om produktens verkliga funktion och användning. Detta kan t.ex. resultera i kunskap om feltyper i relation till specifik användningsmiljö. För kunden kan det medföra att istället för att produkten går sönder och kunden därmed uppfattar produkten som lågkvalitativ så kan företaget ta in produkten för service varvid kunden upplever detta som positivt med en känsla av ökad kvalitet som följd. Sålunda skulle produktens kvalitet kunna öka, både konstruktionsmässigt och i form av användartillfredsställelse. Detta skulle i sin tur eventuellt kunna motivera högre försäljningspris, lägre service- och reklamationskostnader och därmed nämnvärt öka en produkts kundvärde.

Det har på senare tid blivit allt vanligare att slutkunder har tillgång till Internetanslutna datorer (Loshin, 1997). Jag anser att detta medför nya möjligheter för webbaserade kringtjänster för direktkommunikation mellan slutkunder och företag på ett sätt som tidigare inte varit möjligt. Dessa möjligheter tillsammans med synen på kunder och leverantörer som samarbetspartners gör att dessa kan ses som källor för information. Detta medför också att företag får nya möjligheter att vara organisatörer av informationsflöden. Med nya möjligheter kommer också nya problem vilka jag avser att belysa.

Det är vidare intressant att belysa vilka förutsättningar som gäller för att ett företag skall kunna dra nytta av en webbaserad kringtjänst av denna typ. Det är också intressant att utröna vilka problem som uppstår om tjänsten skulle implementeras. Bland dessa problem finns t.ex. aspekter på hur den personliga integriteten hos företagets kunder skall hanteras. Detta innefattar frågor rörande säkerhet vid informationspridning och informationsförsörjning samt vilket genomslag detta får på personlig integritet. Hur många register vill vi som kunder hamna i och vem skall ha tillgång till dessa? Med andra ord, hur kan tekniken användas så att den inte äventyrar kundens personliga integritet.

En annan aspekt på detta är att om detaljerad information om kunden kan härledas, så får den inte hamna i orätta händer eller användas på ett otillbörligt sätt. Informationen syftar till att gagna alla intressenter för att därigenom skapa möjligheter att öka produktkvaliteten. Informationen är inte avsedd att användas för att utreda kunden. Kunden måste därmed få möjlighet att styra vem som kan få tillgång till informationen och hur den får användas vid t.ex. samkörning av databaser.

Jag tänker med detta arbete inrikta mig på att studera tekniska problem som finns vad avser stöd för en extranetbaserad kringtjänst som stöder tankar kring samarbete med slutkunder. Studien kommer att ske främst avseende säkerhet och nätverksarkitekturer. Jag kommer att ta upp detta i syfte att utröna huruvida en kringtjänst av detta slag är möjlig att skapa. Om så är fallet kommer jag dessutom undersöka hur detta möjligen kan påverka personlig integritet.

Förutom tekniska problem så uppstår även frågor om hur stora och vilka resurser som krävs. Om en webbaserad kringtjänst skall få genomslag så bör det inte kosta mer än det smakar. Kostnaden bör både vara mätbar och rimlig.

2 Bakgrund

I detta kapitel kommer jag att beskriva olika termer och begrepp som är relevanta för förståelsen av problemområdet. Då så är tillämpligt kommer jag även att ge en kort historik.

2.1 Internet

Internet är ett globalt plattformsoberoende datanätverk som består av ett stort antal autonoma nätverk som alla pratar samma språk (Loshin, 1994). Internet växte fram för ca 25 år sedan som en följd av det kalla kriget då den amerikanska regeringen insett att de telelänkar som styrde bland annat strategiska vapen kunde slås ut (Loshin, 1994). Telenätverken hade svaga punkter i de växlar som styrde trafiken och den amerikanska regeringen beslöt då att skapa ett robust nätverk som kunde stå emot attacker och sabotage (Loshin, 1994). Forskningen ledde enligt Loshin (1997) fram till skapande av en rad nya regelsystem (protokoll) för hur ett redundant nätverk där datatrafiken kunde dirigeras på flera möjliga vägar kunde byggas upp. Det protokoll som togs fram kallas TCP/IP och är ett regelsystem som styr adressering och transport av data på alla nätverk som ingår i Internet (Loshin, 1997).

De nätverk som byggdes upp ifrån det nya konceptet var i början förbehållna olika forskningscenter (Pfaffenberger, 1998). Till en början låg dessa i USA men sedermera kom även noder i andra länder och till slut började de befintliga nätverken kopplas ihop (Pfaffenberger, 1998). Detta blev, menar Pfaffenberger (1998) grunden för det internationella plattformsoberoende datanätverk, som kallas Internet. På senare tid har Internet blivit kommersiellt och Internet används ofta synonymt med en del av Internet som kallas WWW (world wide web) (Pfaffenberger, 1998). WWW är en del av Internet som använder grafiskt gränssnitt och det är således på olika WWW-adresser som de flesta Internetsidor finns.

2.2 Intranet

Ett intranet är ett företagsinternt TCP/IP-nätverk som använder webbteknik för att företagets anställda skall kunna kommunicera samt sprida och samla information rörande en verksamhet (Hills, 1997). Ett intranet har möjlighet att utnyttja alla de funktioner som förekommer på Internet och fungerar därmed som ett slags mini-Internet inom verksamheten (Hills, 1997). Vanligen innebär detta att ett intranet har en webbserver som endast de anställda kan komma åt (Casselberry m.fl., 1996). Företagets intranet är sedan i sin tur vanligen anslutet till Internet via en firewall som filtrerar information mellan de olika näten och därigenom håller obehöriga utanför (Hills, 1997).

Ett intranet behöver, om det är anslutet till Internet, inte vara beroende av en fysisk plats. Ett företag kanske har anläggningar i flera länder. Hills (1997) menar att varje plats kan ha sitt eget intranet men också att hela företaget kan ha ett gemensamt intranet. Detta kan sammanbindas via krypterade och ”säkra” kanaler över Internet (Hills, 1997).

2.3 Extranet

Ett extranet är enligt Loshin (1997) ett intranet som utnyttjar internetteknologi och har öppnats selektivt för att tillåta externa intressenter åtkomst via Internet. Ett extranet är således ett virtuellt nätverk som korsar organisatoriska gränser (Loshin, 1997). Vidare

är enligt Loshin (1997) alla extranet anslutna till Internet och har extra lager av säkerhetsfunktioner för att kunna stödja ett säkert informationsutbyte mellan organisationerna. Ett extranet kan således via Internet t.ex. koppla samman ett företags interna nätverk med dess leverantörers och med dess kunders för att möjliggöra selektiv delning och åtkomst av resurser och information (Loshin, 1997).

Baker (1997) menar att synen på ett extranet måste utökas från rent tekniska definitioner till att även innefatta de tjänster som ett extranet erbjuder. Ett extranet är således enligt Baker (1997) summan av hårdvara, mjukvara och de tjänster som extranätet erbjuder. Pfaffenberger (1998) menar i likhet med Baker (1997) att ett extranet även måste inbegripa de tjänster som erbjuds. Pfaffenberger (1998) går dock ett steg längre och menar att extranet är ett sätt att tänka som syftar till att omstöpa en organisation till en oumbärlig kunskapsresurs. Kunskapsresursen kan sedan, menar Pfaffenberger (1998), skapa ett extranet med kunder och leverantörer där alla inblandade vinner på den kunskapsprocess som kan bli följden.

2.4 Personlig integritet och etik vid databehandling

Då ett företag skall införa metoder för användning av Internet, intranet och extranet och med dessa medier hantera, för den enskilde, känslig information anser jag att det är viktigt att även etiska aspekter på informationshantering berörs. Utgångspunkten måste vara en definition på vad som menas med personlig integritet. Detta definieras enligt Markgren (1984) av Integritetsskyddskommittén (SOU, 1970) som:

”Den enskildes anspråk att informationer om hans privata angelägenheter inte skall vara tillgängliga för eller få begagnas av utomstående utan hans vilja.” (Markgren, 1984, sid 41 i SOU, 1970, sid 58)

För att den personliga integriteten inte skall äventyras måste någon form av principer för hur information får behandlas ställas upp.

Enligt en OECD-rapport bör en rad krav ställas för att insamlad information inte skall inkräkta på den enskildes integritet (OECD, 1980). Riktlinjerna antogs, då de lades fram, av samtliga OECD-länder men är enligt Forester och Morrison (1990) inte juridiskt bindande. Jag anser att dessa riktlinjer kan utgöra en god grund för vilka krav som bör ställas på ett extranet som behandlar känslig information om olika intressenter. Riktlinjerna består av en rad olika principer vilka Forester och Morrison (1990) tolkat nedan. (Med subjektet menar jag den person som informationen handlar om.)

- Insamlingsprincipen. Information bör insamlas lagligt och med medgivande från subjektet.
- Kvalitetsprincipen. Informationen bör vara korrekt, aktuell och komplett.
- Principen för syftesspecificering. Subjektet bör vid tiden för informationsinsamlandet meddelas syftet till varför informationen insamlas.
- Användningsprincipen. Informationen får inte förmedlas till utomstående utan laglig grund eller att subjektet medger detta.
- Säkerhetsprincipen. Den som insamlar informationen bör vidta rimliga förebyggande åtgärder för att skydda informationen mot förlust, otillåten användning, ändring och exponering.
- Öppenhetsprincipen. Subjektet skall kunna avgöra vem som har tillgång till informationen och hur den används.

- Delaktighetsprincipen. Subjektet skall ha rätt att inspektera informationen och därutöver kunna kräva ändring eller borttagning av felaktigheter.
- Ansvarsprincipen. Den som insamlar informationen ansvarar för att ovanstående riktlinjer följs.

Dessa principer kommer att vara centrala då jag kommer att undersöka anpassning av säkerhetslösningar med avseende på personlig integritet.

2.5 Säkerhet

Med säkerhet menas sekretess, integritet och tillgänglighet (Olovsson m.fl., 1999). Tillgänglighet är att hålla information och resurser åtkomliga för behöriga, medan sekretess innebär att information och resurser hålls otillgängliga för obehöriga (Olovsson m.fl., 1999). Med integritet menas förhindrande av oavsiktlig och otillåten modifiering av information och resurser (Olovsson m.fl., 1999). Denna definition inbegriper även skydd av systemets omgivning som kan vara olika former av användare och förhindrande av obehörig tillgång till information som kan exponera dessa (Olovsson m.fl., 1999).

Olovsson m.fl. (1999) menar att ett system är säkert om systemet i alla situationer beter sig som förväntat.

Loshin (1997) menar att säkerhetsbegreppet bör innefatta såväl intern och extern säkerhet som yttre och inre fysiska hot. Med extern och intern säkerhet menar Loshin (1997) hot om intrång och manipulation från yttre källor eller från anställda inom en organisation. Vidare menar Loshin (1997) med yttre och inre fysiska hot skadegörelse, brand, stölder, sabotage och naturkatastrofer som kan skada ett företags informationssystem. Säkerhet innefattar även skydd mot datavirus och programfel och alla andra hot som kan skada ett system eller dess information eller göra att ett system ”läcker” information (Loshin, 1997).

I min undersökning kommer jag att utesluta fysiska hot som brand, stöld och naturkatastrofer då detta är en form av säkerhet som måste tillses vid uppbyggnad av ett datanätverk och inte på begreppsmässig nivå.

2.6 Den nya affärslogiken

Jag kommer i min undersökning att utgå från ett relativt nytt sätt att tänka vad gäller företagens syn på sina kunder. Jag kommer i detta delkapitel att förklara grundtankarna kring detta.

Wikström m.fl. (1998) menar att företag traditionellt ser kunden som ett objekt till vilket företaget säljer en produkt. Wikström m.fl. (1998) menar vidare att de viktigaste faktorerna i detta tankesätt som kallas transaktionsmarknadsföring, är produkten, priset och företagets image.

Värdeskapande dvs produktens förmåga att generera monetära värden sker enligt en traditionell princip kallad värdekedjan i vilken värdeskapandet är uppbyggt som en sekvens av aktiviteter (Wikström m.fl., 1998). Detta linjära tankesätt medför att varje aktivitet eller avdelning i kedjan interagerar endast med föregående och efterkommande aktivitet och att varje aktivitet i sin tur tillför produkten värde efterhand (Wikström m.fl., 1998).

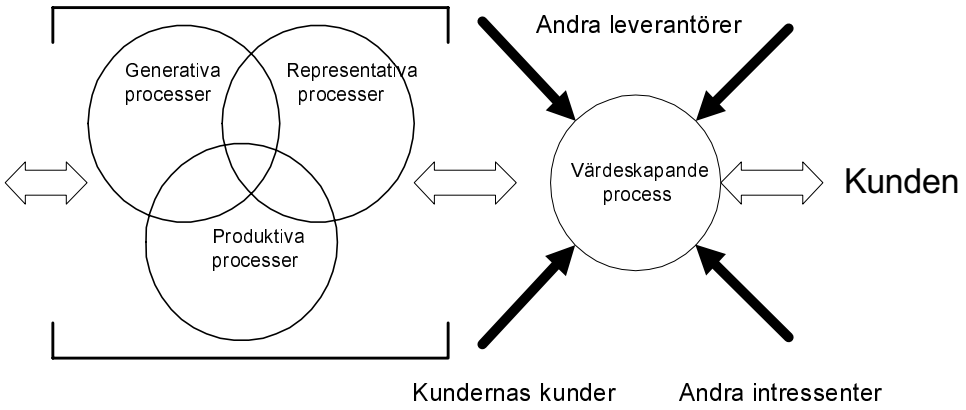
Utveckling och marknadsföring av komplexa produkter kostar företagen stora summor. Antag att ett företag utvecklar en ny bil. Denna utvecklingsprocess kostar

vanligen flera miljarder kronor och kräver att utvecklings-, produktions- samt marknadsföringsprocesserna är effektiva så att investeringen snabbt kan betala sig och bidra till vinst och värdeskapande för företaget både i ett kortsiktigt och i ett långsiktigt perspektiv.

För att detta skall möjliggöras måste produkterna ha rätt kvalitet när de marknadsförs, inte när de utvecklades. Detta ställer krav på snabba produktcykler där företagen i allt större utsträckning behöver ta till vara olika intressenters kunskaper och erfarenheter. För att detta skall vara möjligt måste enligt Wikström m.fl. (1998) företaget ha en lärande inställning till olika intressenter. Först då, menar Wikström m.fl. (1998), kan företaget lära sig nya saker och skapa värde för kunden på samma gång.

Behovet av effektivisering av den traditionella värdekedjan har medfört ett tankesätt vad avser utveckling av och värdeskapande kring produkter. Det nya tankesättet innebär att företagen ökar sin integration och sitt samarbete med kunder och andra intressenter för att underlätta fortlöpande innovationer och förbättringar av sina produkter (Wikström m.fl., 1998).

Det nya tankesättet innebär att företagen skapar mervärde genom att utnyttja en värdestjärna, se figur 1 (Wikström m.fl., 1998). Kunder och leverantörer involveras på ett tidigt stadium i utvecklingsprocessen och dessa ses som samarbetspartners medan företaget framstår som en organisatör av den värdeskapande processen, se figur 1 (Wikström m.fl., 1998).



Figur 1: Värdestjärnan representerar utsuddandet av gränser mellan organisatoriska aktiviteter eller avdelningar samt visar hur övriga intressenter bidrar till ökat värdeskapande i en lärprocess med företaget som organisatör (fritt efter Wikström m.fl., 1998, sid 49). (Generativa processer behandlar planering och utveckling av produkter, produktiva processer hanterar tillverkning och representativa processer inbegriper marknadsföring och försäljning (Wikström m.fl., 1998).)

I värdestjärnan samordnas idéskapande, produktion, marknadsföring och försäljning för att främja interaktivitet och göra gränser mellan både interna och externa/interna aktiviteter mer diffus (Wikström m.fl., 1998). Intressenternas erfarenheter, förslag och kunskap tas till vara och organisationen transformeras från produktionsinriktad till att vara en lärande organisation (Wikström m.fl., 1998). För att kunna skapa en värdestjärna eller värdekonstellation som Pfaffenberger (1998) väljer att kalla det, är det enligt Pfaffenberger (1998) nödvändigt att dela information med strategiska bundsförvanter för att på så sätt få tillgång till ny kunskap utifrån.

3 Problem

I detta kapitel kommer jag ta upp problemställningar i samband med problemområdet. Jag kommer även redogöra för min avgränsning och det resultat jag förväntar mig.

3.1 Problemområde

Mot den bakgrund jag tidigare presenterat vill jag främst peka på varför det är av intresse att inbegripa slutkunder i ett samarbete med producerande företag och leverantörer. Mer precist vill jag undersöka hur en satsning på ett extranet kan vinklas mot enskilda slutkunder. Jag anser att detta är intressant då extranetstödda kringtjänster troligtvis kan tillföra produkter ökad kvalitet och därigenom förbättra lönsamheten.

Antag att ett extranet, vinklat mot enskilda slutkunder, stöder webbtjänster som kan öka produktkvaliteten. Hur kan då detta extranet byggas upp och vilka problem och möjligheter uppstår? Ett extranet gentemot enskilda slutkunder kommer sannolikt att hantera information om dessa. Detta ställer krav på säkerhet och på hur känslig information får hanteras och användas så att inte den enskildes personliga integritet äventyras. Om ett extranet dessutom innehåller information både om en slutkund och om dennes relation till en unik produkt blir dessa krav än mer påtagliga. Detta kräver att organisationer, som hanterar information om kunder och av dem köpta produkter, måste ta ställning till möjliga etiska intressekonflikter vad avser informationen och dess användning. Därefter måste organisationen tillsammans med kunden avgöra hur informationen får hanteras och av vem. Kunderna bör därmed ha möjlighet att bestämma vilken information som får finnas tillgänglig om dem och hur denna får spridas och användas.

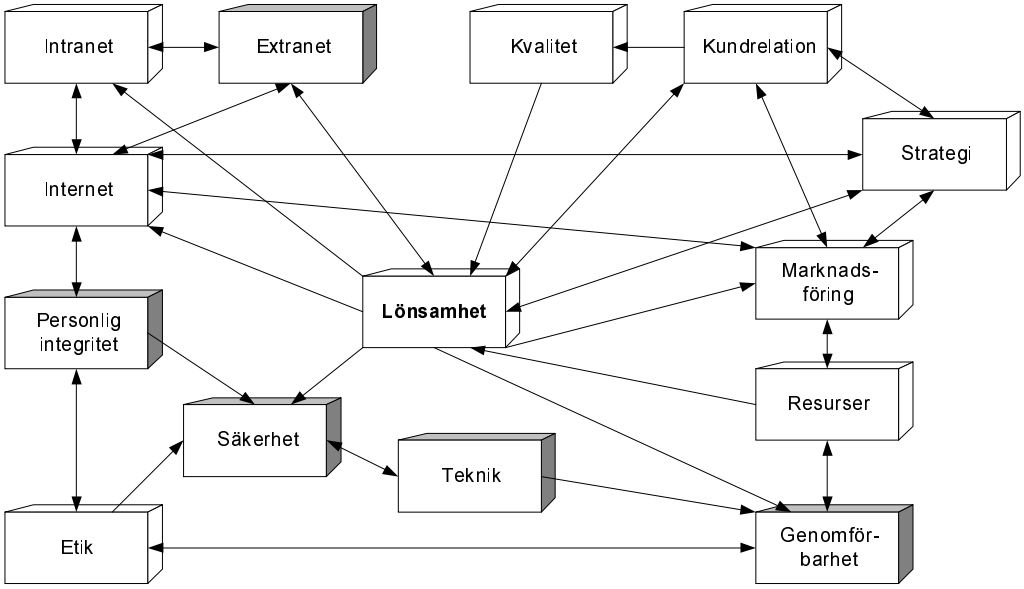
Frågor rörande personlig integritet och säkerhetslösningar är centralt när begreppet extranet hanteras. Ett extranet är ett virtuellt nät som byggs upp mer eller mindre med hjälp av säkerhetslösningar. Olika former av säkerhetslösningar hänger således intimt samman med nätverksarkitekturer och teknik för uppbyggnad av ett extranet. Anpassning av dessa måste kunna ske för att kunna tillgodose olika intressenters krav vad avser tillgänglighet, sekretess och personlig integritet.

Att skapa ett extranet där såväl slutkunder som andra kunder, leverantörer och organisationer ingår ställer inte bara tekniska krav. Jag menar att en organisation även bör ha en viss syn på sina kunder. En organisation som inte ser sina kunder som informationsresurser har heller ingen anledning att skapa ett extranet för att dela information med dessa. Jag menar därför att kunder och övriga intressenter, av organisationen, bör ses som viktiga partners och informationskällor, dvs som resurser i en värdestjärna (se kapitel 2.6). I samband med detta bör organisationen också ha en strategi för hur kvalitet, både på produkter och på kundrelationer skall hanteras. Även organisationens syn på Internet vad avser användning och marknadsföringskanal bör sammanfalla med denna samarbetssyn.

3.2 Avgränsning

Problemområdet är ganska brett. Detta ställer krav på en skarp avgränsning vilket möjliggör en genomtänkt struktur och en uttalad ”röd tråd”. Avgränsningen syftar dessutom till att möjliggöra ett djup i undersökningen och för att den skall vara genomförbar med avseende på planerad tidsåtgång. Nedan följer figur 2 som är en

illustration av problemområdet med dess olika delområden. Figur 2 visar vidare delområdenas inbördes relationer och deras relation till vald avgränsning.



Figur 2: Avgränsningens relation till problemområdet. (Skuggade boxar är de begrepp som inom problempreciseringen kommer att undersökas ingående. Helvita boxar syftar till att främja förståelsen av problemområdet.)

Problemområdet som illustreras i figur 2 består huvudsakligen av två olika områden. Det ena området har att göra med bland annat synen på kunder och kvalitet samt synen på delning av information, dvs olika frågor som huvudsakligen rör företagskultur och ledningstrategier. Det andra området innefattar frågor av mer teknisk och säkerhetsmässig karaktär som genom informationshanteringsaspekter senare får genomslag på t.ex. personlig integritet. Jag kommer främst att inrikta mig på detta område och därmed behandla extranet med avseende på frågor rörande teknik, säkerhet, och personlig integritet. Inriktningen kommer vidare medföra undersökning av hur dessa aspekter påverkar förutsättningar för en möjlig realisering.

Jag har valt dessa aspekter på grund av att utan möjlighet att realisera ett extranet så kan övriga frågor inom problemområdet endast diskuteras hypotetiskt. Jag menar att det krävs kunskap om och i så fall hur ett extranet kan byggas upp, med avseende på föreslagna aspekter, för att andra frågor inom problemområdet skall vara intressanta. Med detta menar jag att diskussion om t.ex. resursåtgång, påverkan på kvalitet och på kundrelationer inte är intressant innan det är klarlagt om ett extranet av detta slag kan byggas upp.

Min avgränsning skall således inriktas mot undersökning av möjliga extranetlösningar. Dessa kan sedan utgöra en reell grund för diskussion om hur ett extranet kan stödja kvalitetshöjande kringtjänster. Diskussionen kan då förankras i möjliga scenarion som sedan eventuellt kan undersökas och i slutändan implementeras. För att ytterligare underlätta diskussion har jag valt att upprätta en sammanhållande definition på ett extranet med den funktionalitet som problemområdet påvisar.

Tidigare har jag i nämnt att ett extranet fokuserat mot slutkunder kan komma att innehålla information om relationen mellan en slutkund och dennes unika förvärvade produkt. Antag att ett extranet innehåller sådan information och att denna information med slutkundens medgivande exponeras och kan användas av utvalda intressenter. Detta menar jag är en utökning av det som vanligen kallas extranet (se kapitel 2.3). I

fortsättningen kommer jag därför att kalla ett extranet med dessa egenskaper för ett kundfokuserat extranet.

Ett *kundfokuserat* extranet är således ett extranet för informationsspridning och insamling där information tillgängliggörs för slutkunder och utvalda aktörer om en enskild unik produkt, köpt av kunden.

Skillnaden mellan ett kundfokuserat extranet och ett extranet är att ett extranet vanligen inbegriper endast storkunder och stora leverantörer. Detta skiljer sig från ett kundfokuserat extranet som även inbegriper enskilda slutkunder, och hanterar information som berör dem. Således är ett kundfokuserat extranet ett extranet med utökad funktionalitet för att även kunna inbegripa enskilda slutkunder.

3.3 Problemprecisering

Är det med avseende på teknik, säkerhet och personlig integritet genomförbart att skapa ett kundfokuserat extranet?

För att belysa denna frågeställning har jag valt att formulera tre delfrågor.

- Finns teknik finns tillgänglig och kan denna utnyttjas med avseende på uppbyggnad av nätverksarkitekturer för ett kundfokuserat extranet?
- Finns det säkerhetslösningar som kan hantera problem av säkerhetskaraktär?
- Påverkas personlig integritet av ett kundfokuserat extranet som hanterar känslig information och kan säkerhetslösningar anpassas för att hantera detta?

Ett kundfokuserat extranet är ett virtuellt nätverk som sammankopplar nätverk över organisatoriska gränser med enskilda slutkunder. Om uppbyggnad av ett sådant skall vara genomförbart bör nätverksarkitekturer och teknik för implementering utredas.

Alla former av extranet byggs till stor del upp av säkerhetslösningar (Pfaffenberger, 1998). Därför anser jag att det är viktigt att undersöka om säkerhetslösningar som hanterar möjliga säkerhetsproblem finns och om dessa stöder uppbyggnad av ett kundfokuserat extranet. Om ett kundfokuserat extranet hanterar känslig information är det dessutom relevant att undersöka påverkan på personlig integritet. Frågor rörande personlig integritet bör hanteras med vissa etiska ställningstaganden och det är därför av vikt att utreda om säkerhetslösningar kan anpassas för att hantera dessa.

3.4 Förväntat resultat

Ett kundfokuserat extranet är en, av mig, vidareutvecklad definition på ett extranet med fokus på enskilda kunder. Jag vill med detta arbete undersöka om ett sådant utifrån valda aspekter är möjligt att skapa. Denna undersökning hoppas jag därför skall resultera i att det med avseende på teknik, säkerhet och personlig integritet visar sig teoretiskt möjligt att skapa ett kundfokuserat extranet.

Det är min uppfattning att detta förmodligen är möjligt men att det kommer att ställa stora krav på främst teknik, säkerhet och anpassning av säkerhetslösningar. Detta dels för att kunna bygga upp en lämplig nätverksarkitektur, dels för att hantera personlig integritet och för att verifiera användare. Anpassningarna kommer förmodligen att kunna göras men jag vill med arbetet försöka säkerställa att detta verkligen *är* möjligt.

4 Metoder och metodval

Det ämnesområde och den problemprecisering som jag valt är vägledande för vilka metoder som kan komma att vara aktuella. Problempreciseringen anger vad som skall undersökas och metoderna hur detta skall göras. Detta arbete är huvudsakligen teoretiskt då det mig veterligen inte finns någon som implementerat ett kundfokuserat extranet. Således bygger frågeställningarna på en teori om vad ett kundfokuserat extranet är och hur ett sådant kan implementeras. Detta, menar jag, ställer speciella krav på vilka metoder som kan användas och på hur dessa skall anpassas för att så bra som möjligt besvara de frågeställningar jag valt. Frågeställningarna utgör en betydande del i den teori om ett kundfokuserat extranet som framkommer i detta arbete. Metoderna blir således även ett medel för att validera delar av denna teori. Jag kommer inledningsvis att presentera varje metod separat och därtill ge min motivering till varför, respektive varför inte, jag valt att utnyttja föreslagna metoder.

4.1 Metodalternativ

De metoder och undersökningsfaser som kan vara intressanta för genomförandet är:

- Teoribildning
- Experiment
- Intervju & enkät
- Modellbildning & scenarier
- Litteraturstudie
- Fallstudie
- Prototyping

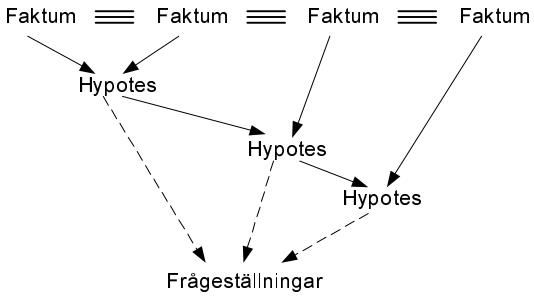
Dessa metoder kan huvudsakligen delas in i två olika kategorier: dels teoretiska metoder för hur teorier och hypoteser kan byggas upp och testas, dels praktiska metoder som används för att illustrera och förtydliga dessa. Praktiska metoder kan således användas för att påvisa möjliga angreppssätt för implementation av teorier och hypoteser. Därmed blir metoderna till viss del validerande.

4.1.1 Teoribildning

Teoribildning innebär enligt Ejvegård (1993) att vi bygger en teori för hur någonting är tänkt att fungera. En teori säger således inte hur ett enskilt undersökningsobjekt som t.ex. ett kundfokuserat extranet verkligen fungerar utan endast hur det är tänkt att fungera. En teori utgör vidare enligt Ejvegård (1993) en förenklad bild av hur delar av en verklighet eller en tänkt verklighet hänger ihop och fungerar.

Teoribildning går enligt Ejvegård (1993) till på så sätt att utifrån en mängd givna faktum kan nya hypoteser härledas. Med ett faktum menas ett säkert konstaterat sakförhållande om hur någonting hänger ihop eller fungerar (Svenska Akademien, 1986). Härledningen av de nya hypoteserna drivs fram av att det finns någonting som är meningsfullt att ta reda på (Ejvegård, 1993). Härledda hypoteser kan sedan ställas i relation till både gamla och nya ännu ej tillämpade faktum för att forma ytterligare hypoteser (Ejvegård, 1993). Om hypoteserna inte motsäger varandra, formar hypoteserna tillsammans med faktumen ett nät som hålls samman av härledningarna

(Ejvegård, 1993). Detta nät av hypoteser, fakta och härledningar menar Ejvegård (1993) utgör teorin.



Figur 3: Teoribildning. Utifrån en mängd faktum härleds icke motstridiga hypoteser som försöker besvara givna frågeställningar. Nya hypoteser tillsammans med nya eller tidigare använda faktum kan sedan i sin tur härleda ytterligare hypoteser. Det nätverk av hypoteser, faktum och härledningar som uppstår utgör den nya teorin. (Ifyllda pilar innebär härledning, streckade pilar innebär försök till förklaring, trippelstreck medför icke motsägelsefullt dvs överensstämmande (Fritt efter Ejvegård, 1993, sid 37).

Detta arbete syftar till att bilda och validera eller falsifiera min teori om ett kundfokuserat extranet. Teoribildning kommer därmed att utgöra grunden för den undersökningsmetod jag valt. Teoribildningen kommer därmed att genomsyra rapporten i den mening att jag kommer att utgå från helhetshypoteser. Dessa kommer jag sedan att sätta i samband med en rad faktum för att kunna härleda nya helhetshypoteser som sedan kan verifieras alternativt falsifieras.

4.1.2 Experiment

Experiment är en kvantitativ metod som innebär att en eller ett fåtal enskilda variabler studeras i en mer eller mindre sluten miljö (Patel och Davidson, 1994). Detta innebär kontroll av den omgivning som på ett eller annat sätt påverkar de studerade variablerna (Patel och Davidson, 1994). Arbetssättet bygger på att studera hur beroende variabler, påverkas av kontrollerade variabler (Patel och Davidson, 1994). För att kunna se hur den beroende variabeln påverkas används oftast en experimentgrupp och en kontrollgrupp (Patel och Davidson, 1994). I experimentgruppen manipuleras de oberoende variablerna vilket påverkar de beroende variablerna (Patel och Davidson, 1994). Kontrollgruppen fungerar enligt Patel och Davidson (1994) som en referens till hur de beroende variablerna beter sig om dessa inte påverkas av de oberoende variablerna. Syftet med experiment är att undersöka relationer mellan de beroende och de oberoende variablerna (Patel och Davidson, 1994).

Eftersom, mig veterligen, ingen tidigare byggt upp eller fört fram tanken på ett kundfokuserat extranet, finns det inte någon grunddata att experimentera med. Således kommer jag i min undersökning att utelämna experiment som metod då arbetet främst kommer att inrikta sig på att ta fram variabler att undersöka.

4.1.3 Intervju & enkät

Patel och Davidson (1994) menar att intervjuer och enkäter bygger på att material insamlas genom att frågor ställs till respondenter. Syftet med en intervju eller en enkätundersökning är att besvara en given frågeställning utifrån de svar som undersökningen ger (Patel och Davidson, 1994). En intervju innebär vanligen att intervjuaren träffar respondenten men intervjuer kan också genomföras telefonledes (Patel och Davidson, 1994). Vid en intervju kommer intervjuaren väl förberedd med

frågor som antingen kan vara nedtecknade eller som intervjuaren kommer på och ställer efterhand (Patel och Davidson, 1994). En enkätundersökning innebär att istället för att intervjuare och respondent träffas personligen så skickas ett frågeformulär, en enkät, ut med brev (Patel och Davidson, 1994).

Innan en intervju genomförs eller en enkät skickas ut så måste en rad val göras om hur frågorna skall ställas och vilka svar som dessa kan tänkas ge (Patel och Davidson, 1994). Patel och Davidson (1994) menar, att frågornas standardisering och hur strukturerade dessa skall vara, medvetet måste avgöras. Grad av standardisering innebär enligt Patel och Davidson (1994) hur mycket ansvar som läggs på intervjuaren med avseende på frågornas inbördes ordning och deras utformning. Enkäter är alltid fullständigt standardiserade då frågor och svarsalternativ vanligen är fasta (Patel och Davidson, 1994). Grad av strukturering behandlar på liknande sätt respondentens möjligheter till svarsalternativ (Patel och Davidson, 1994). En i hög grad ostrukturerad enkät eller intervju ger respondenten möjligheter att svara fritt medan strukturerade frågor ofta har förutsett möjliga svarsalternativ på någon form av skala (Patel och Davidson, 1994).

En enkät eller en intervjuundersökning är enligt Patel och Davidson (1994) beroende på respondenternas villighet att svara på de frågor som ställs. Detta menar Patel och Davidson (1994) medför att de frågor som ställs måste vara neutrala och sakna eventuell känsloladdning som annars kan störa svaren eller svarsvilligheten. För att garantera en hög svarsfrekvens är det också, enligt Patel och Davidson (1994), viktigt att respondenterna är införstådda med undersökningens syfte varför dessa då kan motiveras till att ta sig tid att svara. Patel och Davidson (1994) menar vidare att respondenterna måste informeras om hur inhämtad information skall användas och huruvida deras svar är konfidentiella och anonyma eller ej.

Intervjuer och enkäter skulle kunna vara ett möjligt sätt att gå tillväga. Undersökningens karaktär är emellertid normativ då det huvudsakligen är grunddata som eftersöks. Det är därför tveksamt att skicka ut enkäter eller göra intervjuer om någonting som för respondenterna skulle vara helt nytt. Visserligen skulle det förmodligen gå att samla in information om olika ingående ämnesområden och även om problemställningarna i sig. Problemet med en undersökning av detta slag torde vara att undersökningen inte skulle ha någon direkt koppling till ett kundfokuserat extranet utan behandla olika ämnesområden var för sig. Detta anser jag skulle leda till att ämnesområdenas sammanhang och relation till teorin om ett kundfokuserat extranet möjligen skulle gå förlorad varför jag valt att inte tillämpa denna metod.

4.1.4 Modellbildning & scenarier

Genom att vidareutveckla teorier och hypoteser kan en modell av verkligheten eller av en tänkt verklighet skapas (Ejvegård, 1993). Ejvegård (1993) menar att denna modell syftar dels till att ge förklaring men även till att illustrera den verklighet som den försöker avspegla. Den verklighet eller tänkta verklighet som modellen avspeglar kan i många fall innehålla en hög grad av komplexitet. Det är dock inte nödvändigt att modellen har samma komplexitet som den verklighet den avbildar utan den kan med fördel vara en förenkling (Ejvegård, 1993).

Vidare menar Ejvegård (1993) att en modell skapas för ett bestämt syfte. Detta får enligt Ejvegård (1993) genomslag på vad modellen avbildar och vilken komplexitet som är relevant. Om vi t.ex. skulle planera att bygga en parkeringsplats så är bilarnas yta och svängradie intressant och vi kan bygga en modell av en parkeringsplats som tar hänsyn till detta. Bilarnas färg, märke och topphastighet kan visserligen vara del i

den verklighet som modellen avspeglar men är inte relevant för syftet och behöver därmed inte ingå.

Modeller används oftast för att försöka förklara hur olika delar i ett sammanhang hänger ihop (Ejvegård, 1993). Modellen blir därmed ett verktyg för förklaring av olika fenomen (Ejvegård, 1993). För att modellen skall kunna bli ett verktyg för förklaring måste olika fakta eller variabler kunna sättas in i modellen i någon form av simulering dvs modellen tillämpas teoretiskt i olika situationer (Ejvegård, 1993).

En annan möjlig tillämpning är att bygga scenarion som är en form av simulering (Ejvegård, 1993). Ett scenario är enligt Ejvegård (1993) en teoretisk förenklad tillämpning av en modell, som kan användas för att föra ett resonemang om ett möjligt händelseförlopp.

Jag kommer i detta arbete att använda mig av scenarier som ett viktigt medel för att föra fram och kunna resonera kring teorin om ett kundfokuserat extranet. Scenarierna kan i detta sammanhang vara ett hjälpmedel för att resonera kring möjligheter och problem som kan uppkomma i samband med ett kundfokuserat extranet.

4.1.5 Litteraturstudie

En litteraturstudie kan enligt Patel och Davidson (1994) innefatta information från alla möjliga källor där informationen finns tryckt, nedtecknad eller elektroniskt lagrad. Möjliga källor kan finnas både i privata och i statliga arkiv och kan, men behöver inte vara offentliga eller tillgängliga (Patel och Davidson, 1994). Detta, menar Patel och Davidson (1994), innebär att det vid planering av en undersökning tidigt bör undersökas huruvida de dokument som erfordras står till förfogande. Om detta inte föregår undersökningen finns det enligt Patel och Davidson (1994) stor risk att detta får genomslag på problemställningarna med eventuella krav på att dessa revideras löpande p.g.a. av att information är otillgänglig.

Litteraturstudier kan användas ”för att besvara frågeställningar kring faktiska förhållanden och faktiska skeenden.” (Patel och Davidson, 1994, sid 55). För att frågeställningarna skall kunna anses besvarade är det viktigt att de fakta som presenteras är sannolika och att de inte är motsägelsefulla (Patel och Davidson, 1994). Detta medför att en litteraturstudie ställer höga krav på att de fakta som frågeställningarna besvaras med är korrekta. Patel och Davidson (1994) menar att vi måste förhålla oss mycket kritiska till de källor vi använder. Detta innebär att källorna måste genomgå kritisk granskning vad avser var och när källan tillkommit, vem som skrivit den och i vilka syften samt om det förekommit yttre omständigheter som kan ha påverkat författaren (Patel och Davidson, 1994). Det är även intressant att ta reda på om författaren varit en lekman eller någon som haft djupa kunskaper inom ämnet samt om vi har att göra med en primär- eller en sekundärkälla (Patel och Davidson, 1994).

Mängden material som måste samlas in för att en frågeställning skall kunna anses besvarad varierar, dels beroende på frågeställningen i sig, dels beroende på den tidsram som föreligger (Patel och Davidson, 1994). Om denna tidsram inte kan hållas måste problemställningarna avgränsas ytterligare (Patel och Davidson, 1994). Ett problem i samband med detta kan vara att frågeställningarna kanske besvaras utifrån ett enda perspektiv vilket tar kortare tid. Patel och Davidson (1994) menar att för att en undersökning skall vara intressant så bör en frågeställning kunna besvaras utifrån flera olika perspektiv för att undvika skevhet. Detta menar Patel och Davidson (1994) beror på att det ofta går att välja ut fakta på ett sådant sätt att det går att bevisa nästan

vad som helst. En undersökning får således större relevans om det går att visa att någonting sannolikt förhåller sig på ett visst sätt oavsett vilket perspektiv som väljs. Patel och Davidson (1994) menar därmed att en frågeställning bör diskuteras även utifrån möjliga motsägande fakta.

Detta arbete bygger på teoribildning kring ett kundfokuserat extranet. Den teori som jag kommit fram till måste sedan valideras på lämpligt sätt. Jag har tidigare i kapitel 4.1.3 diskuterat svårigheter att få tag på relevant information som har direkt samband med ett kundfokuserat extranet. Det är min uppfattning att en litteraturstudie kan lösa detta då studien kan riktas mot att ta upp de punkter som i teorin framstår som relevanta. En litteraturstudie ger dessutom möjlighet att undersöka likheter mellan teorier utifrån, om så källorna medger, väl underbyggda resonemang. Detta ger möjlighet till att väga in tidigare resonemang med dem som är nya för att på så sätt ge en vetenskapligt hållbar grund till arbetet. Detta innebär att det finns stora möjligheter att föra in och jämka resonemang från olika källor för att se om dessa överensstämmer eller motsäger de resonemang som ligger till grund för kundfokuserade extranet. Litteraturstudien anser jag således vara en lämplig metod för att samla in data samtidigt som den kan ge arbetet och därmed teorin kring kundfokuserade extranet en ökad validitet.

4.1.6 Fallstudie

En fallstudie innebär enligt Patel och Davidson (1994) att en undersökning görs som rör en begränsad urvalsgrupp. Urvalsgruppen kan vara en eller ett fåtal personer, organisationer eller situationer som vi vill göra en omfattande undersökning om (Patel och Davidson, 1994). En fallstudie syftar till att ge en helhetsbild av det studerade urvalet och bidrar därför enligt Patel och Davidson (1994) till att generera så heltäckande och komplett information som möjligt. Patel och Davidson (1994) menar att fallstudier med fördel kan användas för att studera processer och förändringar. Fallstudier bör enligt Ejvegård (1993) ses som en kompletterande metod då slutledningarnas generaliserbara giltighet i många fall inte kan garanteras. Detta, menar Ejvegård (1993), beror på att en fallstudie utförligt undersöker en eller ett fåtal fall. Detta medför enligt Ejvegård (1993) att slutsatserna bör dras med försiktighet. Vidare menar Ejvegård (1993) att, förutsatt att det studerade fallet inte är särskilt representativt, så bör slutsatserna ses som mer eller mindre tydliga indicier hellre än som rena slutsatser.

Fallstudien är en metod som skulle kunna vara intressant förutsatt att det finns fall att undersöka. Det går rimligen att göra fallstudier inom olika ämnesområden som relaterar till kundfokuserade extranet. En fallstudie av t.ex. ett extranet skulle kunna generera data men i relation till tidsåtgång och relevans avseende kundfokuserade extranet skulle nyttan troligen bli liten och ta stora tidsanspråk.

4.1.7 Prototyping

Prototyping är en experimentell metod som innebär skapande av en förenklad och delvis genomförd tillämpning av en modell eller ett scenario (Andersen, 1994). En prototyp har därmed stora likheter med t.ex. ett scenario (Ejvegård, 1993).

Skillnaden är att ett scenario är en teoretisk beskrivning som lämpar sig för resonemang kring delar av en modell medan en prototyp är en implementering av ett scenario eller av en modell (Neelamkavil, 1987). En prototyp är således ingen färdig tillämpning utan syftar endast till att på ett mer eller mindre detaljerat sätt förevisa hur en modell eller ett scenario möjligen kan genomföras (Neelamkavil, 1987).

Prototyper kan användas för att vidareutveckla modeller och scenarion genom att t.ex. peka på problem och möjligheter som uppkommer i samband med framtagning av prototyperna (Andersen, 1994). Med detta menar Andersen (1994) att det i en modell eller i ett scenario kan framkomma möjliga problem som sedan eventuellt kan bekräftas vid utvecklandet av prototyper. Prototyper utgör således en koppling mellan teori och praktik som sedan kan diskuteras, utvecklas och undersökas.

Prototyping är en av de metoder som jag kommer att inbegripa i detta arbete då jag ser prototyping som en möjlig metod för att vidareutveckla de scenarier som resoneras fram. Således kommer prototyping att fungera som hjälpmedel för att kunna generera en, på papperet, delvis genomförd tillämpning. Att jag väljer metoden beror på att prototyping kan ske utifrån ett scenario och med hänsyn till de resonemang och den information som litteraturstudien ger. Således bör prototyping kunna medföra sammanslagning av teori och inhämtad information till en förenklad helhetsbild.

4.2 Tillvägagångssätt

Jag har tidigare i kapitel 4.1 redogjort för filosofin bakom de metoder som jag anser vara lämpliga för att försöka besvara givna frågeställningar. I detta avsnitt kommer jag att mer specifikt att beskriva hur valda metoder kommer att anpassas och hur de kommer att samverka för att besvara givna frågeställningar. Jag kommer även översiktligt beskriva undersökningens uppläggning.

4.2.1 Teoribildning som grund

Teoribildning är en central del i detta arbete då de frågeställningar som jag avser att försöka besvara bygger på en teoribildning om vad ett kundfokuserat extranet är. Denna teoribildning har jag delvis utvecklat i samband med kapitel 1 och 2, dvs inledning och bakgrund. Jag har så som metoden föreskriver utgått från olika faktum och försökt härleda hypoteser om hur olika förhållanden kan hänga ihop och fungera. Dessa hypoteser har sedan tillsammans med tidigare och nya faktum använts för att härleda nya hypoteser. Jag vill i sammanhanget poängtera att denna form av härledning är rent teoretisk och min ansats är att använda så sannolika fakta som överhuvudtaget är möjligt. I det resonemang som jag fört och som jag kommer att föra lägger jag stor vikt vid att inte bara ta upp fakta som tillskriver min teori validitet utan även fakta som kan tänkas falsifiera den.

Teoribildningen kommer jag i det fortsatta arbetet endast att beröra indirekt. Denna metod kan således för hela arbetets framskridande ses som en form av ”paraply”-metod vilken övriga metoder kommer att underställas. Jag kommer således att börja med att först föra ett resonemang om teorin och dess uppbyggnad i tre olika scenarier. Därefter kommer jag att i samband med en litteraturstudie kring problemställningen undersöka möjliga tekniker och metoder för uppbyggnad av ett kundfokuserat extranet. De fakta som framkommer i samband med denna litteraturstudie kommer sedan användas för att om möjligt ge förslag på en prototypmodell av hur ett kundfokuserat extranet kan byggas upp.

Om det finns en heltäckande lösning som möjliggör skapande av ett kundfokuserat extranet kommer jag att anse frågeställningarna positivt besvarade.

4.2.2 Modellbildning & scenarier för resonemang och exemplifiering

För att utveckla och resonera kring teorin om ett kundfokuserat extranets möjliga genomförande har jag valt att framställa tre olika scenarier. Dessa scenarier kommer, enligt min mening, att följa ett kronologiskt perspektiv om hur informationshantering med internetteknologi har och möjligen kommer att kunna utvecklas. Därför kommer de tre scenarierna att till viss del bygga på varandra.

I scenarierna kommer jag att föra fram både besläktade och fristående exempel på möjliga utvecklingstendenser i samband med teorin kring ett kundfokuserat extranet. Med hjälp av scenarierna kommer jag således att vidareutveckla och tydliggöra teorin om ett kundfokuserat extranet. Jag kommer dessutom att försöka peka ut möjliga problem och möjligheter både vad avser ett tekniskt perspektiv men också vad avser ett samhälleligt och socialt perspektiv t.ex. rörande personlig integritet.

Scenarierna bygger på en idé av Ingi Jonasson. Denna har jag och Ingi Jonasson sedan vidareutvecklat i form av tre scenarier uppbyggda kring ett resonemang om informationshantering.

4.2.3 Litteraturstudie för insikt i teknik och lösningsstrategier

För att belysa problem och möjligheter relaterat till den problemställning jag valt kommer jag att göra en riktad litteraturstudie. Denna litteraturstudie kommer att behandla olika former av lösningsförslag som kan uppkomma i samband med ett kundfokuserat extranet. Studien kommer att i enlighet med problemställningarna endast inrikta sig på frågor rörande teknik, säkerhet, personlig integritet med avsikt att besvara givna frågeställningar och validera teorin.

Litteraturstudien baserar sig huvudsakligen på två olika källor. Dessa källor är båda skrivna efter 1997 och är således relativt aktuella inom ett område som utvecklas snabbt. Extranet är en typ av virtuella nätverk som kommer i många olika skepnader utifrån en rad möjliga komponenter (Pfaffenberger, 1998; Loshin, 1997). Detta medför att oavsett vilken typ eller vilken funktion ett extranet har så finns det komponenter att utgå ifrån (Pfaffenberger, 1998). Därmed anser jag att använda källor är aktuella och relevanta med avseende på kundfokuserade extranet.

”Extranet design and implementation” av Loshin (1997) är en förhållandevis detaljerad bok som på ett bra sätt beskriver de tekniker som kan användas för att bygga ett extranet. Boken är ganska teknisk och går på djupet hellre än att ge ett bredare perspektiv. Detta gör att boken tar formen av en sakbeskrivning medan den översiktliga bilden av hur ett extranet kan byggas upp saknas. Detta beror förmodligen på att Loshin i grunden är nätverkstekniker (Loshin, 1998). För att få ett helhetsperspektiv har jag istället vänt mig till en annan källa.

”Building a strategic extranet” av Pfaffenberger (1998). Denna källa är en av de nyare böckerna inom området som jag anser på ett mycket bra sätt tar upp inte bara hur ett extranet skall byggas upp utan även varför. Boken förhåller sig mer översiktligt till enskilda tekniker medan användningsområden och abstraherade typlösningar behandlas i detalj. Detta medför att boken ger en mycket bra översikt kring vad ett extranet är, vad det kan användas till och vilka möjliga lösningar som står till buds.

Bryan Pfaffenberger är professor inom teknologi, kultur och kommunikation vid University of Virginia och har även fått pris för årets bästa bok av ”The American Society of Information Science”.

Jag anser att vare sig Loshin (1997) ”Extranet design and implementation eller Pfaffenberger (1998) ” Building a strategic extranet” på egen hand kan ge en heltäckande bild av ett extranet men att de mycket väl kompletterar varandra.

4.2.4 Prototyping, framtagning av en prototypmodell

Om det finns en möjlig lösning för hur ett kundfokuserat extranet kan byggas upp så kommer detta att redovisas i en schematisk prototypmodell, dvs en modell av en tänkbar prototyp. Denna prototypmodell skall fylla två olika syften. Dels skall den ge möjlighet att på ett lättillgängligt sätt visa viss funktionalitet och möjliga nätverksarkitekturer och topologier i ett kundfokuserat extranet. Dels kommer prototypmodellen även att användas för att om möjligt ge alternativ till lösningsförslag på olika säkerhetsrelaterade problem. Prototypmodellen skall således användas för att om möjligt skapa ett teoretiskt lösningsförslag för implementering av ett kundfokuserat extranet.

4.2.5 Undersökningens generella uppläggning

Genomförandet av detta arbete kommer att vara uppdelat i tre olika kapitel som följer det arbetssätt och de metoder för genomförande av undersökningen som jag valt. Jag kommer att börja med att redovisa tre olika scenarier i vilka jag försöker ge ett tidsperspektiv på hur jag ser på informationshantering med internetteknologi. Dessa scenarier kommer att leda till en ytterligare precisering och förhoppningsvis en förståelse för teorin om ett kundfokuserat extranet. Jag kommer därefter att göra en litteraturstudie där jag i enlighet med mina frågeställningar undersöker utvalda aspekter avseende ett kundfokuserat extranet mer ingående. Slutligen kommer jag att skissa på en prototypmodell för att, om möjligt, exemplifiera ett lösningsförslag som kan indikera att ett kundfokuserat extranet är möjligt att skapa.

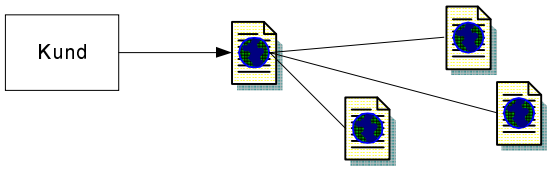
5 Typscenarier för informationshantering

För att illustrera hur utnyttjande av Internet kan användas för att öka värdeskapandet kring olika produkter följer nedan tre olika scenarion på hur tekniken kan utnyttjas på ett mer eller mindre avancerat sätt. Till varje scenario finns exempel som belyser möjligheter och problem. Dessa scenarier är framtagna i samarbete med Ingi Jonasson och bygger på en, av honom framtagen idé.

5.1 Scenario 1 – Kunden som aktiv part

Den första typen innebär att kunden är den aktiva parten. Kunden söker aktivt information om en produkt på Internet. Kunden har inget önskemål att ge eller få feedback utan letar självständigt upp den efterfrågade informationen och därefter finns ingen bestående relation mellan kund och leverantör. Detta förutsätter att det företag som tillhandahåller produkten publicerar information som är relevant för kunden och således kan skapa ett mervärde till produkten. Företaget är i den här situationen passivt och förmodas inte få någon direktkontakt med sina kunder då kunderna inte ger sig tillkänna.

Scenariot medger för kundens del information om en viss produkt där det är irrelevant att relatera informationen till en enskild unik produkt. I den här produktgruppen återfinns massproducerade produkter och konsumtionsvaror. Kunden ses som ett objekt till vilken företaget säljer en produkt och därefter är transaktionen huvudsakligen avslutad. De företag som tillverkar och säljer sina varor på detta sätt arbetar efter den traditionella värdekedjan och det finns inget större behov av att inleda en lärande relation med slutkunden. Genom att publicera information om tillverkning och hantering av kundens produkt hoppas företaget att kunden skall få en kvalitetskänsla för produkten och för det företag som tillverkar och/eller tillhandahåller den.



Figur 4: Informationsutbyte där kunden är aktiv part. Kunden surfar in på sidan och hittar länkar som pekar till andra sidor med information relevant för sammanhanget. Kunden ger sig inte tillkänna och skapar ingen direkt relation med tillverkaren.

Den relation som detta scenario skapar med kunden har en rad begränsningar. Kunden kan visserligen få information om en produkt vilket kan vara positivt för både kunden och för det säljande företaget. Företaget har dock endast begränsade möjligheter att få feedback från kunden om sidan saknar en ordentlig feedbackfunktion. Detta leder till att det är svårt att skapa en produktiv relation med kunden och denne kommer förmodligen också att titta på produkter från andra företag nästa gång kunden skall inhandla något. För företagets del så ligger det en begränsning i att kunden får information om en produkt medan företaget har små eller inga möjligheter att direkt påverka och tycka till om vad som kunde göra den bättre. Om många företag med liknande produkter marknadsför dessa på likartade sätt så kommer prisjämförelser att bli allt viktigare om inte något företag tillhandahåller en produkt eller tjänst som vida överträffar konkurrenternas.

Dessutom kan det, om företaget har många produkter, bli tidsödande och dyrt att underhålla en komplex webbplats. Om denna blir stor blir det dessutom svårare för kunden att hitta fram till informationen och risken finns att många kunder ger upp på vägen. Förhållandet mellan storleken på webbplatsen och lättheten att snabbt hitta det som söks kan därmed utradera några av fördelarna med att distribuera information på detta sätt.

Detta scenario belyser ett tankesätt som enligt min erfarenhet är aktuellt i dagsläget. Företagen låter sina kunder hämta information om produkterna för att, genom denna typ av kringtjänst, öka produkternas kvalitet och för att stärka varumärket.

5.2 Exempel på scenario 1 – Kunden som aktiv part

Ett exempel på den här typen av scenario kan vara ett mejeri. Kunden ser en Internetadress på ett mjölkpaket och surfar då på Internet för att få reda på mer information om produkten i fråga. Mejeriet publicerar på sina sidor information om företagets ”anrika” bakgrund och om de processer genom vilka mjölken hanteras och hur de olika produkterna produceras och hanteras. Förutom dessa sidor finns även sidor med information om bondgårdarna, bilder på kossor som strövar fritt och information om naturen i den kommun där mjölken produceras.

Meningen är att kunden allteftersom de olika sidorna gås igenom skall få en känsla av att mjölken har hög kvalitet. Med detta menar jag t.ex. att kunden kanske upplever det som extra positivt att mjölken är ekologisk och att kossorna som producerar den får ströva fritt. Detta ger en känsla av kvalitet och kan sedan leda till att kunden köper andra produkter från mejeriet och att dessa kanske efterfrågas i affärer som för närvarande inte säljer mejeriets produkter.

Detta scenario går även att utveckla till det förhållande som kan gälla då stora köpcentra vill ha mejeriprodukterna paketerade i eget namn, s.k. ”brandname”. Detta gör rimligen mejeriets varumärke svagare och mer osynligt. Om köpcentrat byter till ett annat mejeri så står det första mejeriet helt utelämnat.

Om vi förutsätter att mejeriet har en länk till en hemsida på sina produkter i enlighet med det sätt som diskuterades ovan så har mejeriet rimligen möjlighet att inte bara leverera en anonym produkt utan även en möjlighet att bygga upp ett varumärke som tillför värde utöver själva produkten. Skulle köpcentrat sedan byta leverantör kan mejeriet sälja till någon annan och fortfarande ha ett starkt varumärke.

Denna typ av scenario kan även gälla mer avancerade produkter. Antag t.ex. att en kund har köpt en ny tv, video och ljudanläggning och då fått tre olika fjärrkontroller och en massa sladdar som skall kopplas ihop på ett enda korrekt sätt. Detta vållar troligtvis mycket arbete och missnöje och leder förmodligen till att kunden initialt blir missnöjd då denne inte räknar med att det skall ta timmar att få anläggningen att fungera.

Antag att kunden kan hitta Internetadresser t.ex. på baksidan av fjärrkontrollerna. Om kundens produkter alla är av samma märke så kan det på denna webbsida finnas information om hur kundens produkter skall kopplas ihop. Kunden får kanske välja just vilka produkter denne har med någon form av valfunktion och sedan genereras en steginstruktion precis hur dessa produkter skall kopplas samman. Dessutom kan det på sidan finnas tips och råd för att få det så bra som möjligt i kundens miljö.

Jag menar att denna typ av kringtjänst troligtvis skulle tillföra produkterna ökad kvalitet då tjänsten behandlar produkternas lämplighet för användning.

Hopkopplingar av denna typ är oftast relativt enkla men blir ofta komplicerade och tidsödande om inte kunden vare sig har tillräckliga kunskaper eller kan få en exakt stegbeskrivning.

En webbtjänst av denna typ skulle även kunna hjälpa kunden att få tillgång till och kanske skriva ut en komplett manual för hur de inköpta produkterna används tillsammans.

Jag vill peka på den utsuddning av gränserna mellan fysisk vara och tjänst som sammansmälter i ett resonemang av detta slag. Den fysiska hemmabioanläggningen som levereras får i detta resonemang formen av både en vara och en tjänst vilket troligtvis ökar kvalitén och värdeskapandet av produkten sett som en helhet.

Nästa steg för kunden är att få alla produkter att skötas av en enda fjärrkontroll. För detta ändamål måste en av fjärrkontrollerna, vanligen den till TV-n programmeras. Även en utförlig manual eller en instruktion för ett visst programmeringsschema samt användarmanual för detta och bilder på layout skulle kunna laddas hem från webbsidan.

I ett inte allt för avlägset perspektiv kan TV-n användas för att surfa på Internet. Speciellt gäller detta i samband med införandet av digital-TV. Alla produkter i kundens hemmabioutrustning kanske kommunicerar med hjälp av t.ex. Suns Jini som låter olika enheter kommunicera och på ett enkelt sätt själv ansluta sig till ett nätverk. Detta skulle kunna leda till att kunden med TV-n surfar in på en webbsida där denne får hjälp med hopkoppling av fysiska sladdar och sedan får kunden välja hur fjärrkontrollen och interaktionen mellan de olika enheterna skall fungera. Detta sparas sedan i TV-n som konfigurerar upp de andra enheterna varvid kunden slipper göra detta tidskrävande arbete manuellt. Detta skulle då även kunna fungera trots att de olika enheterna är av olika märken. En tjänst av denna typ där enheter interagerar med varandra i ett nätverk skulle även möjliggöra uppdateringar av programprodukt i de olika komponenterna som gör att kundens produkt löpande håller sig i frontlinjen.

En kund som på detta sätt får hjälp med att få sina nya produkter att fungera som det är tänkt på ett snabbt och enkelt sätt kommer förmodligen att tillskriva produkterna ökad kvalitet. Kunden skulle rekommendera dessa för andra samtidigt som supportavdelningar kan minskas i omfattning.

5.3 Scenario 2 – Kunden och företaget som aktiva parter

I ett scenario av denna typ ökas kundfokus och kunden får status som subjekt i förhållande till företaget. Detta gör att rollen mellan företaget och kunden förändras på så sätt att företaget aktivt tar reda på information om vem kunden är och först därefter försörjer kunden med information. I denna nya roll är både kunden och företaget aktiva parter men det är kunden som står för initiativet till upprättandet av den mer eller mindre varaktiga relation som följer. Med detta menar jag att den händelse som initierat relationen antingen kan vara webbtjänsten i sig eller att kunden köpt en produkt.

Tillvägagångssättet bygger på en bestående relation mellan kunden och företaget där informationsutbyte sker åt båda hållen. Detta informationsutbyte kan bestå i att kunden loggar in dvs lämnar information om sin identitet och begär därefter information från företaget som företaget då i sin tur tillhandahåller.

De produkter som i första hand är aktuella här är sådana som är massproducerade men trots det relativt avancerade och konfigurerbara, dvs kunden får välja en kombination

av alternativ. Dessutom finns det vanligtvis någon form av garantivillkor som skapar en relation mellan kunden och företaget under en period av ett eller ett par år. Eventuellt kan kunden vid köpet, eller när denne vill, registrera sig på webbtjänsten och får därmed tillgång till support och service. Vid registrering av denna typ är det vanligt att det finns både frivilliga och obligatoriska uppgifter som kunden måste fylla i. Detta är en möjlighet för företaget att få information om nya kunder.

När sedan informationen finns registrerad så kan kunden begära information, support och service från företaget. Således är denna relation i högre grad kundfokuserad och bygger på ett informationsutbyte mellan företaget och kunden inom givna ramar. Fortfarande så är kunden inte på samma nivå som tillverkaren. Med detta menar jag att företaget fortfarande inte på ett strukturerat sätt tar tillvara den enskilda kundens kunskap om en produkt. Detta sätt att hantera en webbplats handlar ofta om att använda det som ett verktyg för marknadsundersökningar. Kunden blir aldrig direkt involverad i produktutvecklingen, dvs står utanför den egentliga värdekedjan.

Figur 5: Kunden och företaget som aktiva parter. Företaget fokuserar hårdare på kunden och erbjuder personliga sidor som handlar om just denna kund. Kunden begär information från en webbsida och detta efterföljs av inloggningsinformation där kunden ger sig tillkänna (streckad pil). Kunden får då fram en sida innehållande mer eller mindre specifik information om det som kunden är intresserad av.

När information hanteras på detta sätt så har företaget möjlighet att samla information i databaser om kunder, som registrerat sig. Denna information kan sedan sammanställas och användas i olika syften. Informationen kan t.ex. säljas eller komma ut till företag som sysslar med direktmarknadsföring via Internet eller till andra intressenter som kan ha intresse i relationen mellan en kund ett företag och/eller en produkt. Då detta troligtvis skulle uppfattas som negativt av många kunder finns naturligtvis krav på att informationen inte får delges andra hur som helst.

Detta gör att företaget måste ha ett säkerhetstänkande vad avser integritet för den enskilde kunden. Detta innebär att information utan kundens medgivande inte får distribueras vidare då detta förmodligen skulle skapa ett stort missnöje hos kunden i fråga. Dessutom måste företaget se till säkerheten i den hårdvara och mjukvara som administrerar webbplatsen är tillfyllest. Detta gäller då inte bara säkerhet i allmänhet utan särskilt åtkomst och inloggningsförfaranden samt hur kundunik information och lösenord lagras.

5.4 Exempel på scenario 2 – Kunden och företaget som aktiva parter

Exempel på denna typ av scenario kan vara ett elektronikföretag som säljer en PDA (personal digital assistant, liten handhållen datakalender). Då denna typ av produkt är under ständig utveckling och p.g.a. att den är så pass avancerad medför detta att företaget behöver ge service och support, dvs inkludera detta som en tjänst i sin produkt. Dessutom kan företaget kontinuerligt släppa uppdateringar av programvara som främjar kompatibilitet med andra produkter och ökar användbarheten. Detta är exempel på kringtjänster som tillför kärnprodukten ökad kvalitet och kanske kan motivera ett högre försäljningspris och resultera i nöjdare kunder. I och med att kunden är känd så finns det möjligheter att ta kontakt med denne när uppdateringar finns tillgängliga eller för att informera om nya produkter. Speciella tillbehör och

programvaror, som kunden måste betala för, kan erbjudas och således beställas direkt över Internet.

För att företaget skall få ett relevant underlag för produktförbättring är det önskvärt att få information om vilka kundgrupper som väljer företagets produkt. Enligt min egen erfarenhet är ett vanligt sätt för att göra detta att starta en webbplats och förutom vanlig service erbjuda FAQ, programuppdateringar och onlinehjälp mot att kunden registrerar sig och loggar in specifikt.

Den information som kan härledas ur detta kan öka företagets möjligheter att anpassa produkten efter marknaden. När kunden har loggat in kan denne dra fördel av de tjänster som erbjuds på hemsidan och företaget å sin sida får information om vilken typ av tjänster som kunden utnyttjar. Att kunden loggar in unikt innebär även möjligheter för företaget att erbjuda anpassade sidor för varje specifik kund.

Antag att en kund köpt en ny bil. Att öka kundens känsla av kvalitet och värde genom kringtjänster kan i första hand ske på två olika sätt. Företaget kan i enlighet med scenario 1 tillhandahålla kunden en webbplats där denne kan gå in och leta information och manualer för sin speciella bil. Detta kan kunden göra genom att förflytta sig i en struktur med webbsidor. Kunden får, när denne navigerar på webbplatsen, göra vissa val på vägen för att komma åt den specifika information som kunden är intresserad av. De val som kan göras kan t.ex. vara bilmodell, beteckning, färg, årsmodell och inredningsfärg.

Ett annat sätt att underlätta för kunden är att första gången denne går in på företagets webbsida, så görs vissa val avseende bl.a. bilmodell. Nästa gång kunden loggar in så presenteras relevanta sidor utifrån dessa val. Kunden måste i detta fall identifiera sig och får då direkt fram information om sin bilmodell med en viss beteckning, färg, årsmodell och inredning.

Fördelen med denna typ av webbsida är att kunden får en ökad känsla av att sidan handlar om kundens specifika bil med de egenskaper som den har. Detta kan tyckas banalt men det kan t.ex. finnas särskild information om hur lack med en viss färg bör skötas. Den information som delges handlar således mer eller mindre om just kundens bil.

När kunden loggar in unikt så kan företaget följa upp vilken information som kunden söker och vilka fel som kunden söker information om. Detta kan ge en informationsbas om bilens funktion i användningsmiljön utifrån vilken företaget kanske kan förbättra sina produkter. Företaget får dessutom möjlighet att presentera specifika manualer och handböcker för alla olika varianter av bilar. Dessa manualer kan även löpande uppdateras och felkorrigeras. Dessutom kan aktuell information till bilverkstäder och återförsäljare på ett enkelt sätt göras tillgänglig. Det kan gälla servicehandböcker och kopplingsscheman som förenklar för olika intressenter och därmed ökar kvaliteten hos företagets produkter.

Observera att kunden i denna typ av scenario har möjlighet att få information om exakt sin variant av bil utifrån de val som gjorts när kunden köpte bilen. Men webbsidan handlar inte om kundens unika bil och möjligheterna till mer specifik information om den unika bilens aktuella status begränsas därmed. Hur ett företag kan implementera en tjänst för att tillgodose kunden och andra intressenter med information om kundens unika bil är vad detta arbete i fortsättningen kommer att behandla.

5.5 Scenario 3 – Kunden som strategisk partner

Detta scenario innebär en kund omdefinieras från att ensidigt vara köpare av en vara till att ses som en ”strategisk” partner från vilken företaget hämtar lärdomar och interagerar med. Detta förändrar inte synen på att kunden är den som i slutändan betalar varan men innebär en förändrad syn på kundens roll i de processer vid vilka en produkt utvecklas, produceras och marknadsförs.

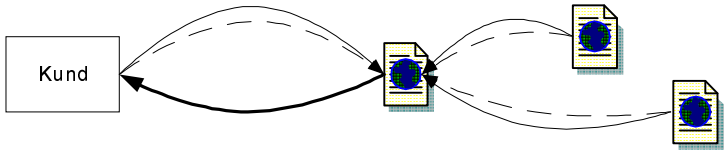
Kunden intar i detta fall en förhållandevis aktiv roll och får nya möjligheter att ”tycka till” och direkt påverka utvecklingen av nya produkter. Produkterna är huvudsakligen konfigurerbara, massproducerade produkter där det finns intresse för olika intressenter att förmedla och ta del av information om en kunds relation till en fysiskt unik produkt.

Detta bygger på att det vid en köptransaktion genereras information om vem som har köpt exakt vad, dvs vilken unik produkt som en enskild kund införskaffat. Kunden får tillgång till en webbsida som kunden med ett inloggningsförfarande kan komma åt. Denna sida behandlar kundens unika produkt som denne inhandlat. Meningen är att kunden genom att gå in på sidan kan komma åt manualer, servicetips och aktuell statusinformation på sin produkt. Denna information behöver inte bara komma från det enskilda företaget utan kan komma från alla de intressenter som har ett intresse i relationen mellan kunden och produkten. Således skall sidan i kundens ögon vara ett medium för att få tillgång till information och service men även för att kunna lämna synpunkter och förslag till de olika intressenterna. Därmed bör sidan ha implementerade feedbackfunktioner. En tjänst av detta slag torde rimligen kunna öka en produkts kvalitet och värdeskapande förmåga i en kunds ögon.

Sett ur företagets och övriga intressenters perspektiv kan den specifika relationen mellan kund och produkt vara mer eller mindre intressant. För dem är huvudsaken att relationen mellan en kund och dennas unika produkt möjliggör förutsättningar för skapande av information om antingen kunden eller om produkten. För att detta skall kunna gå att genomföra så måste det gå att unikt identifiera såväl en unik produkt som den enskilde kunden.

I ett IT-perspektiv innebär detta att kunden får tillgång till och har möjlighet att ge feedback och information om sin unika produkt till företaget som har tillverkat den och även till övriga intressenter. Detta scenario är en utökning av exemplet i scenario 2 och innebär att kunden inte bara kommer åt information om sin variant av bil, utan istället kommer åt en sida som verkligen handlar om kundens unika bil. Skillnaden är att informationen inte handlar om en instans av en unik produktvariant utan om den unika produkten i sig. Webbsidan kan utnyttja samma teknik för att sammanställa generell information om en viss biltyp men sidan kommer, till skillnad från scenario 2, att handla om en unik bil.

Kunden får på motsvarande sätt som i scenario 2 logga in på en sida för att få tillgång till information. När kunden gör detta så länkas relevant information in till sidan och denna skickas explicit till kunden. Informationen är av sådan typ att den hämtas på ett säkert sätt och därefter sammanställs till en central webbsida ”on the fly”, dvs när kunden beställer den. Informationen hämtas inte bara från en webbservrar utan länkas till viss del in från olika databaser innehållande information om kunden och dennes relation till produkten. Kunden ger sig således till känna varvid kunden blir försedd med information.



Figur 6: Kunden som strategisk partner. Företaget fokuserar på varje enskild slutkund och erbjuder vid inloggning tillgång till information om kundens unika produkt. Information relevant för relationen hämtas även från övriga aktörer på ett säkert sätt. Dessa aktörer är lämpligen strategiska partners som ingår i företagets extranet.

5.6 Exempel på scenario 3 - Kunden som strategisk partner

För att exemplifiera detta scenario antar jag att den biltillverkare som i scenario 2 erbjöd sina kunder information om en viss bilmodell nu i realiteten ger kunderna information om deras unika bilar. För att detta skall vara möjligt måste varje bil vara märkt med en unik identifierare. Varje bil har tre unika identifierare, chassinummer, motornummer och registreringsnummer. Antag att vi väljer registreringsnumret som identifierare på bilen. Antag vidare att en kund vill komma åt en webbsida för att hitta information om hur bakluckans belysning skall bytas.

Kunden loggar in på biltillverkarens sidor med användarnamn och lösenord. Biltillverkaren har information i sin databas om att kunden köpt en bil med registreringsnummer ABC 123. I bilregistret ser de vilket chassinummer som detta är kopplat till och kunden länkas direkt till en sida dit information länkas, ”on the fly”, om kundens aktuella bil. På denna sida finns bilder på bilen, användarmanualer, videosnuttar om hur olika servicemoment görs och information om hur bilens speciella lack och klädsel skall skötas. Dessutom finns information om aktuellt försäkringsläge och information om vilken service som är utförd samt data om bilens och däckens kondition. Denna information kommer inte bara från det enskilda tillverkande företaget utan länkas in från olika databaser i försäkringsbolag, bilverkstäder och kanske låneinstitut och finansbolag, om bilen är leasad.

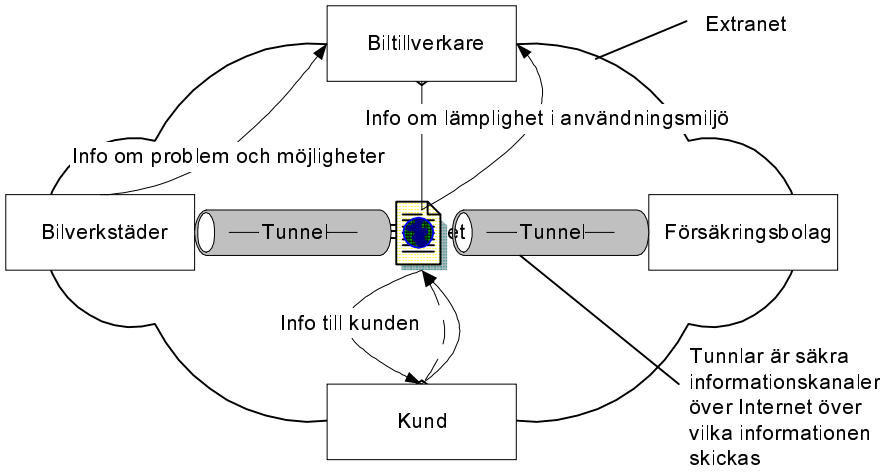
På webbsidan kan kunden göra kostnadsberäkningar och få erbjudanden om nya däck när de gamla börjar bli slitna eller erbjudanden om olika tillbehör som kunden kan tänkas vilja ha. Information om kunden gör det möjligt att skräddarsy information och erbjudanden efter kundens önskningar och beteende. En bilförare som kör 5000 mil på ett par däck är förmodligen inte intresserad av en ny spoiler medan en annan som bara kommer 2000 mil på ett par däck kanske absolut vill ha en. Däremot är båda intresserade av nya däck när de gamla är utslitna.

I och med att informationen länkas in från de olika aktörer som har intresse i relationen mellan en kund och dennes unika produkt finns det stora möjligheter att utvinna information ur de data som lagras. Exempel på information som möjligen kan lagras följer nedan.

När kunden lämnar in bilen för service på en bilverkstad så lagras förmodligen detta i bilverkstadens databas. Det är t.ex. information om vilken service som utförts, mätarställningar och däcksdjup samt information om bilens tillstånd som har laddats ner från elektronikbox och färddator. Dessutom tar bilverkstaden till vara kundens kommentarer och vad som upplevs som bra eller dåligt med produkten. Denna informationsmängd görs sedan tillgänglig för kunden genom att denne begär webbsidan och då kommer åt informationen som länkas in från bilverkstadens databas.

Försäkringsbolaget lägger vidare upp information om bilens historia i olyckssammanhang och presenterar premier, bonuserbjudanden och annan finansiell information om bilen. Biltillverkaren står för generell information om kundens exakta bilkonfiguration och presenterar bilder och manualer samt annan information som är generell för bilar av den speciella typen.

Viktigt i detta sammanhang är att informationen inte skall skickas in till en central databas. En sådan skulle bli ohållbar då en biltillverkare normalt säljer hundratusentals bilar. Informationsmängden skulle då rimligen bli för stor. Istället lagras informationen lokalt där den genereras eller mer centralt i den genererande aktörens databas. Informationen kanske inte lagras i den lokala bilverkstadens databas utan kan läggas i en för kedjan av bilverkstäder central databas. Därefter länkas den in ”on the fly” till en central webbsida som det tillverkande bilföretaget, eller generalagenten, står för. Detta innebär att redundant information inte genereras utan att webbsidan utnyttjar information som redan finns och sammanställer denna på begäran.



Figur 7: Exempel på ett scenario där ett extranet finns mellan olika aktörer och där kunden loggar in och då får information genererad ”on the fly” om sin unika produkt. Figuren visar även exempel på vilken typ av information som kan resultera när kunden ses som en strategisk partner. Information skickas säkert i tunnlar mellan olika aktörer till den centrala webbservern som tillhandahålls av företaget. Den information som skickas handlar om kundens relation till sin produkt. I detta fall är alltså bilen huvudsakligen det objekt som informationen behandlar.

Detta möjliggör för de olika aktörerna att hämta data från detta virtuella informationslager för att på så sätt få en grund för produktutveckling och produktanpassning.

Antag att en kund köper en bil. Varje bil måste enligt lag ha en trafikförsäkring och köpet medför dessutom att företaget svarar för vissa garantier och servicevillkor sedan köpet gjorts. Detta innebär att det vid köpet skapas information om relationen mellan kunden, säljaren och bilen.

Antag vidare att bilföretaget, eller dess generalagent, i samband med köpet skapar en webbsida som kunden, ett försäkringsbolag och en kedja med ”rekommenderade” bilverkstäder får tillgång till. Information om bilens försäkringsläge samt övrig information om bilen från det tillverkande företaget länkas nu in. Webbsidan i sig kan möjligen vara en standardiserad mall som specificerar de länkar och det utseende som sidan skall ha. Sidan kan därmed, i sig, vara begränsad då den uteslutande innehåller en struktur och länkar till information. När sidan sedan begärs av kunden, sammanställs informationen som länkarna pekar på till en komplett sida.

När kunden efter en viss tids körning lämnar in bilen på service hos en av de ”rekommenderade” verkstäderna, skapas information som sedan tillgängliggörs på webbsidan. Därmed finns informationen tillgänglig nästa gång kunden loggar in. Bilverkstaden kan dessutom få tillgång till sidan för att kolla bilens nuvarande status och hur det borde se ut. Det tillverkande företaget kan sedan titta på sidorna och sammanställa information om bilarnas verkliga beteende i den miljö där de används. Denna information kan t.ex. leda biltillverkaren till en upptäckt att bilar som kör i områden där det ofta är kallt på vintern har en försämrad bränsleekonomi och att vissa saker p.g.a. kylan slits hårdare. Biltillverkaren kan sedan utreda detta och kanske på sidan föreslå en annan tändningsinställning som får bilen att gå bränslesnålare tillsammans med ett erbjudande om ändring av detta gratis eller till en låg kostnad.

Vidare kanske företaget kan upptäcka att en komponent på bilen vanligen går sönder i vissa miljöer och då erbjuda kunden att fritt byta denna komponent. Detta istället för att kundens bil går sönder under garantitiden och kunden blir stående arg på en vinterväg och får kalla på bärgning. Eftersom garantin för denna typ av fel kan hålla biltillverkaren skyldigt att kostnadsfritt byta komponenten så medför detta samma kostnad om komponenten byts före eller efter att den har gått sönder. Dock så kommer kunden om komponenten byts i förebyggande syfte kommer kunden att känna sig omhändertagen och förknippa biltillverkaren och produkten med kvalitet.

Distribution av information på detta sätt skulle alltså kunna leda till att företaget kan erhålla en informationsbas om verkliga förhållanden vid utvecklingsarbete. Detta skulle ytterst kunna bidra till ökad kvalitet. God kvalitet kan, enligt Sandholm (1995), medge högre försäljningspriser, högre vinster, och därigenom bättre chanser för överlevnad i en konkurrensutsatt marknad.

6 Säkerhet för kundfokuserade extranet

Ett kundfokuserat extranet bör kunna erbjuda selektiv extern åtkomst via Internet. Detta medför att olika former av säkerhetsfrågor är centrala. När det kundfokuserade extranetet planeras måste det sålunda avgöras vem eller vilka som skall ha tillgång till vilken information och vilka säkerhetslösningar som skall hantera detta. Åtkomst kan innefatta både känslig information som användarnamn och lösenord samt resurser som i vissa fall kan vara känsliga. Hantering av detta kan låta förhållandevis okomplicerat men betänk problem som kan uppstå när det kundfokuserade extranetet inbegriper olika geografiskt skilda aktörer och slutkunder som arbetar från olika plattformar. Lägg därtill det faktum att informationen transporteras via Internet som överhuvudtaget inte har några inbyggda säkerhetsfunktioner. Varje företag som överväger att satsa på ett kundfokuserat extranet måste därför i enlighet med sin strategi överväga de säkerhetsrisker som finns och planera lösningar som kan möta dessa.

Jag kommer i detta kapitel att redovisa första delen i den litteraturstudie som jag har valt att göra. Denna del kommer att behandla dels möjliga hot vid införande av ett kundfokuserat extranet dels vilka möjliga tekniker och metoder som finns för att avvärja dessa. För att bilda sig en uppfattning av vilka hot och säkerhetskrav som föreligger kommer jag att inleda med att presentera ett antal kriterier för datasäkerhet i samband med extranet.

6.1 Säkerhetsmässiga hotbilder och försvarsstrategier

Bort och Felix (1997) identifierar sex olika mål för datasäkerhet i samband med extranet. De säkerhetskriterier som presenteras är i huvudsak inriktade på extranet men jag anser att kundfokuserade extranet bör vara föremål för dessa kriterier. Kriterierna har stor betydelse i samband med kundfokuserade extranet då detta är en typ av extranet som i hög grad är exponerade mot Internet. Målen eller säkerhetskriterierna är enligt Bort och Felix (1997):

- Konfidentialitet. Detta mål skall enligt Bort och Felix (1997) eftersträva att informationen hålls privat och att den därmed uteslutande är åtkomlig för personer, organisationer eller datorer som har behörighet.
- Autentifikation. Detta mål skall garantera att användare, vare sig de är datorer eller människor, är de som de säger sig vara. (Bort och Felix, 1997)
- Ickedesavouering. Detta mål syftar till att garantera att meddelanden och transaktioner inte skall gå att förneka (Bort och Felix, 1997). Om jag t.ex. lämnar ett meddelande på en telefonsvarare så kan jag inte förneka detta då jag lämnar bevisliga spår i form av mitt unika röstmönster. Jag kan således inte ta tillbaka mitt meddelande.
- Integritet. Med integritet menas således enligt Bort och Felix (1997) att det skall gå att verifiera att inga förändringar har skett mellan en sändare och en mottagare, dvs att meddelanden går fram intakta.
- Åtkomstkontroll. Öppenheten i ett extranet ställer stora krav på att resurser och information skyddas från obehörigt intrång eller användande. Bort och Felix (1997) definierar åtkomstkontroll som att resurser och information är under exklusiv kontroll av auktoriserade användare.

- Tillgänglighet. Detta mål avser datasystemets förmåga att i alla lägen förbli operativt och att eventuell nedtid inte beror på säkerhetsrelaterade problem (Bort och Felix, 1997).

Dessa kriterier är en utökning och förgrening av de översiktliga säkerhetsdefinitioner som jag tagit upp i kapitel 2.5.

Loshin (1997) och Baker (1998) identifierar ytterligare ett säkerhetsproblem som endast indirekt inkluderas av ovanstående definitioner. Detta är ett extranets förmåga att säkra öppna kanaler över Internet (Loshin, 1997; Baker, 1998). En genomgång av relevant litteratur visar att de definitioner som givits ovan huvudsakligen täcker de säkerhetsaspekter som finns även om dessa inte alltid ges samma namn.

En orsak till de många säkerhetsproblem som finns är det protokoll (TCP/IP) dvs det regelsystem för kommunikation och transport av data som finns på Internet (Pfaffenberger, 1998). Då detta är en central del i förståelsen av flera av de säkerhetsproblem som finns kommer jag att ge en kortfattad definition av TCP/IP med fokus på hur detta får genomslag på säkerhet.

6.1.1 TCP/IP och säkerhet

TCP/IP står för ”Transmission Control Protocol / Internet Protocol” och består av två olika protokoll (Bort och Felix, 1997). Dessa protokoll hanterar all dataöverföring på Internet och i de flesta extranet (Loshin, 1997). Systemet fungerar som ett postkontor. Antag att vi vill skicka en produkt som inte får plats i ett paket. Detta medför att produkten måste delas upp och packas i flera paket. På dessa paket skrivs destination och avsändare och posttjänsten tar sedan hand om leveransen. När paketen anländer vid destinationen öppnas de och produkten sätts samman igen. Denna funktionalitet är liknande den som TCP/IP medger. TCP hanterar nerpackning och uppackning medan IP hanterar transport mellan avsändare och destination. Paket som skickas med TCP/IP över Internet kan anlända i fel ordning och vid oregelbundna tidpunkter då vägvalet är dynamiskt med flera möjliga vägval (Loshin, 1997).

TCP/IP medför en rad säkerhetsproblem. TCP/IP-s brist på inbyggda säkerhetsfunktioner medför att det är möjligt att undersöka alla paket som har en viss avsändare och en viss destination för att på så sätt få tillgång till informationen. Varje paket innehåller dessutom information om innehåll i paketet (Loshin, 1997). Detta medför att information som skickas över Internet är lätt att stjäla. Denna typ av informationsstölder kallas ”IP-sniffing” och är enligt Pfaffenberger (1998) och Loshin (1997) fullt genomförbart med datoriserade verktyg. TCP/IP har vidare enligt Pfaffenberger (1998) överhuvudtaget inga inbyggda funktioner eller inbyggt stöd för att kontrollera att paketen kommer från den avsändare som anges. Detta medför att avsändare, innehåll och destination kan förfalskas precis som vi kan skriva vad som helst på avsändaren när vi skickar ett brev. Detta kallas ”IP-spoofing” och är ett vanligt sätt att försöka lura datasystem att släppa in obehöriga (Pfaffenberger, 1998).

TCP/IP medför alltså säkerhetsproblem men är det protokoll som används på Internet (Pfaffenberger, 1998). Detta medför att TCP/IP ändå bör användas i ett kundfokuserat extranet för att kunna tillåta Internetåtkomst. Avsaknaden av säkerhetsfunktioner i TCP/IP-protokollet medför krav på att säkerheten implementeras på fler sätt än att endast titta på paketens utsida.

6.1.2 Allmän hotbild för ett kundfokuserat extranet

Ett kundfokuserat extranet är ett öppet extranet. Öppet i den bemärkelsen att ett kundfokuserat extranet måste tillåta direktåtkomst från Internet. Eftersom de presumtiva kunderna kan sitta vid olika datorer från gång till gång går det heller inte att endast tillåta åtkomst endast från vissa datorer. Detta begränsar vilka säkerhetstekniker som kan komma att vara aktuella och förstärker på så sätt hotbilden. Samtidigt är det viktigt att poängtera att om ett företag inte är berett att kommunicera öppet så får företaget förmodligen inte reda på så mycket heller. Således kan risktagandet sägas vara en förutsättning för att överhuvudtaget kunna göra affärer.

Jag anser att de hotbilder som föreligger främst har att göra med personlig integritet för företagets slutkunder. När dessa loggar in på det kundfokuserade extranetet och kommer åt sina personliga hemsidor som innehåller eller länkar in känslig information är det viktigt att denna information inte kommer obehöriga tillhanda. Detta kan dels skada kunderna men också indirekt det kundfokuserade extranetets huvudaktörer som kan dra på sig negativ publicitet och därmed en ovilja bland kunderna att tillhandahålla information om sig själva (Pfaffenberger, 1998). Detta innebär att ett kundfokuserat extranet måste stödjas av säkerhetslösningar som hanterar problem avseende åtkomstkontroll och konfidentialitet enligt de definitioner som Bort och Felix (1997) givit. Förtroendet bland kunder anser jag vara en viktig förutsättning för ett möjligt genomförande av ett kundfokuserat extranet varför även säkerhetsmålen avseende tillgänglighet, integritet och auktorisation är viktiga. Kunderna kan tappa förtroende för extranettjänsterna om det kundfokuserade extranetet ofta är nere och om de känner att det finns risk för att information om dem själva kan läcka ut eller mixtras med av någon annan (Pfaffenberger, 1998).

Pfaffenberger (1998) identifierar en rad hot som kan uppkomma i samband med ett extranet. Dessa hot gäller i oförminskad grad även ett kundfokuserat extranet. Detta beror på att det kundfokuserade extranetet är exponerat mot Internet och att detta är öppet för externa attacker. Detta har att göra med att den adressrymd (möjliga Internetadresser) från vilken åtkomstförfrågningar alternativt attacker kan göras inte kan begränsas, då slutkunder bör få möjlighet att ansluta från valfria platser. Pfaffenberger (1998) identifierar de främsta hoten som:

- Nedtider eller ”denial of service” dvs väntetider och tider då extranetet helt eller delvis sätts ur funktion som ett resultat av att någon obehörig gör intrång, försöker göra intrång, eller avsiktligt försöker störa ut extranetet så att detta temporärt slutar fungera (Pfaffenberger, 1998).
- Bedrägerier och industrispionage kan vara en orsak till att obehöriga försöker bryta sig in för att t.ex. få tillgång till personuppgifter eller annat känsligt material som t.ex. företagshemligheter. Äventyrandet av känsliga och värdefulla uppgifter kan enligt Pfaffenberger (1998) allvarligt skada ett företags rykte och förtroende bland både kunder och bland andra aktörer som är delaktiga i extranetet. Detta menar Pfaffenberger (1998) kan på sikt få kunder och övriga intressenter att sluta att använda ett extranet. Jag menar att äventyrandet av information är lika mycket ett hot mot den personliga integriteten som ett hot mot företaget och för det kundfokuserade extranetet i sig.
- Olika former av intrång och sabotage. Det finns vissa personer som ser det som en intellektuell utmaning eller har det som ett jobb att försöka bryta sig in i datasystem för att där ändra, kopiera och/eller förstöra data. Detta menar

Pfaffenberger (1998) kan få allvarliga konsekvenser för den eller det extranet som drabbas.

Ett kundfokuserat extranet bör som tidigare nämnts använda TCP/IP och Internet för att kunna kommunicera effektivt med ett stort antal användare vilka kan vara spridda i ett globalt samhälle. TCP/IP har som tidigare nämndes inte några säkerhetsfunktioner och även detta måste enligt Loshin (1997) vägas in i den möjliga hotbilden.

6.2 Firewalls

För att hantera de säkerhetskriterier och bemöta den hotbild som tidigare i kapitel 6.1 nämnts kommer jag att undersöka olika säkerhetslösningar. Pfaffenberger (1998) menar att säkerhetslösningar i olika former av datanätverk, som t.ex. ett extranet eller ett kundfokuserat extranet, vanligen byggs upp av en eller flera firewalls.

En firewall är enligt Pfaffenberger (1998) en datorbaserad hård- och mjukvarulösning som används för att förhindra obehörig åtkomst till ett företags intranet. En firewall kan samtidigt användas för att tillåta selektiv åtkomst av externa resurser (Pfaffenberger, 1998). Denna funktionalitet medför att en firewall vanligen ligger i gränssnittet mellan ett intranet och Internet och är en vanligt förekommande lösning för de flesta typer av zonuppdelningar i och mellan nätverk (Olovsson m.fl., 1999). Firewalls har således ett brett schema av möjliga tillämpningar.

En firewall är ingen burk som går att köpa i detaljhandeln under namnet ”Firewall” utan istället en sammansatt lösning som kan bestå av en eller flera komponenter (Pfaffenberger, 1998). En firewall kan därmed bestå av en eller flera routers, proxies, certifieringsservrar, autentifikationsservrar och eventuellt programvara för att analysera och spåra data (Pfaffenberger, 1998). Vilken lösning och vilka tekniker som kan komma att bli aktuella beror på den säkerhetsstrategi och de hot som ett föreslaget extranet lämpligen bör kunna adressera (Pfaffenberger, 1998). Pfaffenberger (1998) menar att implementerande av effektiva firewalls är centralt vid införande av ett extranet. Jag vill återigen peka på den mycket nära släktskapet mellan extranet och kundfokuserade extranet. Detta släktskap medför att firewalls och säkerhetslösningar för extranet också är applicerbara på kundfokuserade extranet.

Att skapa en mycket säker firewall är svårt då det enligt Pfaffenberger (1998) finns ett samband mellan säkerhet, kostnad och användbarhet. Det går, menar Pfaffenberger (1998), att skapa en i stort sett ”säker” firewall men kostnaden för denna skulle bli mycket stor samtidigt som rigorös säkerhet troligen skulle göra extranetet oanvändbart. För att hantera detta skapas vanligen någon form av kompromisslösning som ger tillräcklig säkerhet (Pfaffenberger, 1998). En rätt konfigurerad firewall kan, enligt Pfaffenberger (1998) få bukt med en rad olika säkerhetsproblem och även användas för att styra resursanvändning. Firewallen kan, menar Pfaffenberger (1998) användas för att t.ex.:

- Tillåta eller förhindra åtkomst av externa resurser och därigenom styra vilka resurser som av ett företag anses acceptabla eller oacceptabla.
- Dölja interna adresser från omvärlden för att på så sätt förhindra bland annat attacker med IP-spoofing.
- Logga och presentera information om externa åtkomstförfrågningar för att kunna följa upp eventuella attacker.
- Logga och presentera statistik för att hitta mönster som kan visa på ”onormalt” beteende.

- Varna vid starten av en attack eller upptäcka en pågående attack.

Pfaffenberger (1998) menar vidare att det är viktigt att poängtera att en firewall som hanterar gränssnittet mellan intranet/Internet dvs ett extranet, inte svarar mot interna attacker.

Målet med en firewall är att skydda resurser och data. För att göra detta finns det enligt Loshin (1997) ett antal komponenter och strategier som kan användas. Jag kommer nedan att redogöra för dessa olika komponenter och tekniker.

6.2.1 Routers

Routers finns i de flesta former av firewallösningar och utgör i många fall den grund som andra säkerhetslösningar bygger ut och kompletterar (Pfaffenberger, 1998). En router är en hårdvaruenhet som vanligen installeras vid gränssnittet mellan ett intranet och Internet eller mellan två eller flera olika nätverk (Pfaffenberger, 1998). Huvudfunktionen för en router är att styra leverans av datagram (TCP/IP-paket med data) till nästa router som ligger närmare den angivna destinationen eller direkt till destinationen. För användning av routers inom ramen av en firewall kan de flesta routers implementera ”packet filtering” (Loshin, 1997).

Packet filtering

Packet filtering innebär att alla datagram som passerar routern filtreras och endast släpps igenom om datagrammet har en godkänd destination och avsändare samt ett godkänt innehåll (Pfaffenberger, 1998). Loshin (1997) menar att TCP/IP-protokollets datagram på grund av sin uppbyggnad är okomplicerat att filtrera då destinationsadress och avsändare och innehåll finns lättillgängligt i alla datagram. Alla datagram passerar dessutom enligt Loshin (1997) vanligen en enda punkt mellan det interna och det externa nätverket. Detta gör det möjligt att på ett relativt okomplicerat sätt applicera regler för vilken trafik som skall släppas igenom åt det ena eller andra hållet (Loshin, 1997). Loshin (1997) menar att packet filtering inte på egen hand kan användas för att säkra interaktionen mellan två nätverk. Däremot är metoden användbar som en dellösning för att huvudsakligen hindra banala attacker och för att sakta ner en mer avancerad attack (Loshin, 1997).

Packet filtering finns så gott som alltid implementerad i en firewall (Loshin, 1997). Det finns dock, enligt Loshin (1997), en rad problem som begränsar användbarheten och metodens förmåga att skydda ett nätverk. Dels så är det komplicerat att använda packet filtering som ett heltäckande skydd då detta skulle kräva ett stort antal regler och då även begränsa nätets användbarhet (Loshin, 1997). Dels går det att förfalska adresser och innehållstyper i datagrammen, något som packet filtering vanligen inte kan hantera (Loshin, 1997). Packet filtering kan dessutom inte hantera trafiken efter att den släppts igenom. Detta medför enligt Loshin (1997) att en obehörig användare som kommit åt en resurs på det interna nätet kan utnyttja säkerhetshål i denna för att komma vidare. Det innebär i praktiken att när en kanal igenom routern väl öppnats så kommer den att förbli öppen. Detta ökar sårbarheten. Mot bakgrunden av att packet filtering inte medger kontroll av användaridentitet utan förlitar sig på säkerheten i det system från vilket ett paket härstammar kan metoden endast ses som en delkomponent i en firewall (Loshin, 1997).

6.2.2 Circuit gateway

”Circuit gateway” är en teknik i vilken all datatrafik måste gå via en ”circuit gateway firewall” som vidarebefordrar godkänd trafik (Loshin, 1997). På detta sätt får externa

och interna servrar aldrig direktkontakt med varandra utan de ansluter enbart till firewallen som sedan förmedlar kontakten dem emellan. Metoden kan användas tillsammans med andra metoder som t.ex. packet filtering och är liksom den senare metoden ännu en komponent som kan användas för att höja säkerheten i gränssnitten mellan två nätverk (Loshin, 1997). En circuit gateway firewall kan dessutom i viss mån användas för att förhöja den interna säkerheten inom ett intranet. Detta menar Loshin (1997) blir en följd av att även intern datatrafik måste ansluta till firewallen först för att kunna ta kontakt med interna servrar.

Jag menar att implementerandet av en circuit gateway är en fråga om avvägning mellan olika krav. Sannolikt så kommer det interna nätverkets prestanda att sänkas samtidigt som kommunikation med externa resurser görs säkrare. Jag menar dock att denna säkerhet måste ställas mot bakgrunden av att en circuit gateway också ger sårbarhet i intranätet om den skulle gå sönder eller slås ut av en elakartad attack.

6.2.3 Proxies

En ”proxy” är en mer avancerad och säkrare vidareutveckling av en circuit gateway (Loshin, 1997). En proxy kallas ibland även för ”application gateway” och förmedlar en transparent kommunikation mellan kommunicerande applikationer snarare än mellan kommunicerande datorer (Loshin, 1997). Detta innebär i praktiken att proxyn ger illusionen av att två kommunicerande applikationer är direktanslutna mot varandra. (Loshin, 1997). För att göra detta håller proxyn kontinuerligt statusinformation om datalänken och de kommunicerande applikationerna vet således inte och behöver heller inte veta var den applikation de pratar med befinner sig (Loshin, 1997). Då en proxy huvudsakligen verkar på applikationsnivå finns det enligt Loshin (1997) stora möjligheter att logga information. Detta möjliggör detaljerad information om lyckade anslutningar, möjliga intrångsförsök eller misslyckade anslutningar som gjorts (Loshin, 1997).

En proxy är enligt Loshin (1997) den säkraste formen av komponent i en firewall. En proxy har emellertid vissa negativa sidor. En proxy undersöker och håller statusinformation om all kommunikation som sker i en session inbegripande två applikationer (Loshin, 1997). Detta är mycket processorkrävande och om många sessioner hålls samtidigt kan proxyn bli en flaskhals som begränsar nätverkets prestanda (Loshin, 1997).

6.2.4 Hardened operating systems

En firewallösning byggs upp av olika hårdvarukonfigurationer som kompletteras med mjukvara, t.ex. en proxyservermjukvara som körs en eller flera servrar. En server har normalt operativsystem och detta är vanligen tänkt att användas t.ex. i ett fleranvändarsystem (Loshin, 1997). När servern skall användas i en firewallösning med en för detta ändamål anpassad mjukvara och en bestämd och avgränsad uppgift är det menar Loshin (1997) viktigt stänga av onödiga tjänster. En bred funktionalitet medför fler möjliga säkerhetshål som går att utnyttja (Loshin, 1997). För att komma till rätta med detta kan alla tjänster och alla funktioner som inte är absolut nödvändiga för uppgiften tas bort eller stängas av (Loshin, 1997). Detta kallas enligt Loshin (1997) för att operativsystemet härdas och resultatet blir ett ”hardened operating system” som bibehåller endast kritiska funktioner.

Genom att tillämpa denna metod accepterar systemadministratören att det finns möjliga buggar och säkerhetshål. Istället för att försöka leta efter varje möjlig sådan

kombination i olika tjänster tas dessa istället bort vilket ger mindre, mer överskådliga och framförallt säkrare system (Loshin, 1997).

6.2.5 Network adress translation (NAT)

”Network adress translation” (NAT) är en annan vanlig metod som används för att skydda ett intranet från obehörig åtkomst från Internet. NAT innebär att alla interna adresser endast fungerar internt och att dessa sedan översätts till nya adresser när kommunikation skall ske med externa resurser (Loshin, 1997).

Detta innebär att en firewall som implementerar NAT visserligen skickar vidare åtkomstförfrågningar till interna resurser men att dessas interna adresserna aldrig visas upp (Loshin, 1997). NAT kan i vissa fall öka säkerheten i ett intranet från externa attacker men skapar också en rad problem när information från t.ex. en webbserver skall göras tillgänglig utifrån (Loshin, 1997). För att information skall vara tillgänglig utifrån, måste adressen till denna resurs finnas tillgänglig (Loshin, 1997). Det går att anropa firewallen med en begäran om åtkomst av en webbsida. Firewallens NAT kommer då att behandla detta utifrån vilken typ av begäran som kommer in och ge åtkomst därefter (Loshin, 1997). Problem uppkommer då företaget vill ha flera olika webbservrar. NAT-tjänsten vet då inte vilken av dem som den skall välja och begäran avslås (Loshin, 1997).

6.2.6 Vanliga firewallösningar

En firewall går inte att köpa rakt av då det oftast är frågan om en sammansatt lösning. En vanlig lösning kan t.ex. innebära en firewall bestående av en fristående router som skickar alla datagram vidare till en proxyserver (Pfaffenberger, 1998). Denna sammansatta firewallösning installeras sedan vid gränssnittet mellan t.ex. intranätet och Internet, och blir en form av gateway. Det finns menar Pfaffenberger (1998) och Loshin (1997) ett flertal olika tekniker för att skapa en effektiv och samtidigt användbar firewallösning. Författarna menar att dessa lösningar ofta är varianter av ett och samma tema. Jag kommer därför att ta upp en form av översiktlig och anpassningsbar lösning som författarna anser vara den viktigaste. Jag väljer att i enlighet med Pfaffenberger (1998) kalla den för ”demilitarized zone” (DMZ).

Demilitarized zone (DMZ)

DMZ är en form av firewallarkitektur i vilken två packet-filtering routers och en proxyserver samverkar för att skapa en stabil och säker firewallösning (Pfaffenberger, 1998). I praktiken innebär detta att ett avskilt mellannätverk i gränssnittet mellan intranätet och Internet skapas. Detta fungerar på så sätt att den router som har kontakt med Internet skickar all trafik vidare till en proxyserver (Pfaffenberger, 1998). Bakom denna proxyserver skapas ett mellannätverk där vissa applikationer t.ex. en webbserver kan läggas (Pfaffenberger, 1998). Detta mellannätverk är sedan i sin tur anslutet till intranätet via en extra packet-filtering router som endast släpper igenom trafik adresserad specifikt till interna adresser av proxyn (Pfaffenberger, 1998). Genom att använda en DMZ kan ett företag erbjuda tjänster och anslutningsmöjligheter till avgränsad information utan att öppna hela intranätet (Pfaffenberger, 1998). Denna typ av arkitekturlösning kan dessutom användas för att skydda särskilt känslig information även internt genom att dela upp intranätet med hjälp av kontrollerade DMZ (Pfaffenberger, 1998).

Tekniker för att begränsa och dela upp ett intranet i zoner och kunna erbjuda säker åtkomst till utvalda resurser med hjälp av ett DMZ-system är särskilt intressant vid

skapande av ett kundfokuserat extranet. Jag menar i likhet med Pfaffenberger (1998) att detta kan vara ett tillförlitligt sätt att tillåta åtkomst av extranetresurser från Internet. Detta kan dessutom, menar Pfaffenberger (1998), göras utan att för den sakens skull exponera hela intranätet med de risker som då följer.

6.3 Kryptering av data

Kryptering är en metod för att skicka meddelanden över en osäker kanal som om de avlyssnas är oläsliga för alla utom den avsedda mottagaren (Pfaffenberger, 1998). Kryptering innebär att ett meddelande i klartext (okrypterat) krypteras med en i förväg bestämd algoritm som kallas nyckel (Pfaffenberger, 1998). Det krypterade meddelandet kan sedan endast dekrypteras med en passande nyckel, dvs en passande dekrypteringsalgoritm (Pfaffenberger, 1998).

Kryptering är en mycket effektiv metod för att möjliggöra säker kommunikation mellan två intressenter och detta är således en central metod för säkerhet i samband med extranet. Jag kommer inledningsvis att diskutera kryptering i samband med ett kundfokuserat extranet. Därefter går jag vidare till olika tekniker.

6.3.1 Krypteringsmetoder för kundfokuserade extranet

Jag menar att ett kundfokuserat extranet sätter stor vikt vid att inbegripa även slutkunden. Detta, menar jag, ställer hårda säkerhetskrav på de metoder som kan användas för att göra kommunikation inom det kundfokuserade extranetet säker. Det beror på att informationen måste skickas över Internet som är ett osäkert medium och på att den information som skickas kan vara värdefull och därmed av intresse för obehöriga.

Det finns, anser jag, huvudsakligen två krav på de metoder som måste till för att informationsutbyte skall kunna ske på ett säkert sätt. För det första använder slutkunderna Internet för åtkomst vilket medför att inga specialnätverk kan införas i gränssnittet gentemot kunden. För det andra så kan inga krav ställas på att kunderna måste installera särskilda programvaror eller på andra sätt drabbas av icke standardiserade lösningar för åtkomst. Detta innebär t.ex. att vanliga nätbläddrare som Microsoft Internet Explorer eller Netscape Navigator måste gå att använda. De metoder som då ligger närmast till hands är metoder för säker kommunikation genom kryptering. Jag kommer nedan att ge en introduktion till några olika former av krypteringsmetoder och även ta upp standardiserade tekniker för kryptering mellan vanliga nätbläddrare och resurser i kundfokuserade extranet.

6.3.2 Symmetrisk kryptering

Den enklaste formen av kryptering är enligt Bort och Felix (1997) symmetrisk kryptering. Detta innebär att meddelanden krypteras med en hemlig nyckel som både sändaren och mottagaren känner till (Bort och Felix, 1997). Den nyckel (algoritm) som används kan vara av olika komplexitet och därmed kan säkerheten i de meddelanden som används variera (Bort och Felix, 1997).

För att skapa en starkare kryptering väljs därför matematiska algoritmer som genererar ett ansenligt antal möjliga kombinationer (Pfaffenberger, 1998). Dessa kombineras sedan med val av en lång nyckel, ju längre desto säkrare (Pfaffenberger, 1998).

Kryptering med symmetriska nycklar fungerar enligt Bort och Felix (1997) bra sånär som på en fatal svaghet. Om kryptering och dekryptering sker med samma nyckel

måste kommunicerande parter få tillgång till nyckeln (Bort och Felix, 1997). Detta kan skapa problem om obehöriga får tillgång till nyckeln när denna skall transporteras till parterna (Bort och Felix, 1997). Transportproblemet har på senare tid drivit fram utveckling av vad som kallas asymmetrisk kryptering (Bort och Felix, 1997).

6.3.3 Asymmetrisk kryptering

Vid asymmetrisk kryptering används ett nyckelpar bestående av en publik och en privat nyckel (Bort och Felix, 1997). Den publika nyckeln och den privata nyckeln har en matematisk länk som baserar sig på en icke reversibel envägsfunktion som härleder den publika nyckeln från den privata (Bort och Felix, 1997). För att skicka ett asymmetriskt krypterat meddelande till en mottagare krypterar sändaren meddelandet med mottagarens fritt åtkomliga publika nyckel (Bort och Felix, 1997). Meddelandet kan sedan endast dekrypteras med hjälp av mottagarens privata nyckel (Pfaffenberger, 1998). Detta innebär att publika nycklar används för kryptering och privata nycklar för dekryptering (Pfaffenberger, 1998). Resultatet är att den privata nyckeln aldrig behöver sändas över mediet och således hålls hemlig varför riskerna för avlyssning minskas (Pfaffenberger, 1998).

Kryptering med privata och publika nycklar innebär enligt Bort och Felix (1997) att den publika nyckeln kan spridas fritt medan den privata hålls hemlig. Detta medför att två parter som aldrig tidigare haft kontakt kan skicka krypterade meddelanden till varandra (Bort och Felix, 1997). Detta kan göras så fort respektive parts publika nyckel är känd (Bort och Felix, 1997).

Asymmetrisk kryptering eliminerar transportproblemet men kräver stor datakraft för kryptering och dekryptering vilket kan leda till flaskhalsar och prestandaproblem (Bort och Felix, 1997). För att komma runt detta används ofta en kombination av symmetrisk och asymmetrisk kryptering.

6.3.4 Kombinationer av symmetrisk och asymmetrisk kryptering

Prestandafördelar vid användande av symmetrisk kryptering sammantaget med transportproblem av nycklar har medfört att en kombination av asymmetrisk och symmetrisk kryptering ofta används (Bort och Felix, 1997). I dessa kombinationer används ofta asymmetrisk kryptering för att initiera kommunikationen. Detta fungerar enligt Bort och Felix (1997) på så sätt att en slumpmässig symmetrisk algoritm genereras. Denna algoritm krypteras sedan med mottagarens publika nyckel varefter den skickas till mottagaren (Bort och Felix, 1997). Mottagaren dekrypterar den symmetriska algoritmen med sin privata nyckel och sedan används istället den symmetriska algoritmen för kommunikation (Bort och Felix, 1997). Således används asymmetrisk kryptering endast för att hantera transport av en symmetrisk nyckel.

Bort och Felix (1997) identifierar två olika standarder som kan vara av intresse vid användning gentemot slutkunder i ett kundfokuserat extranet. Dessa båda standarder har fullt ut eller delvis stöd i både Internet Explorer och i Netscape Navigator (Baker, 1997).

Secure sockets layer (SSL)

SSL är enligt Bort och Felix (1997) ett säkerhetsprotokoll som syftar till att erbjuda en säker och avskärmad kommunikation mellan två parter. SSL är utvecklat av Netscape Communications Corporation och finns implementerat både i Internet Explorer och i Netscape Navigator (Baker, 1997).

SSL implementerar både symmetrisk och asymmetrisk kryptering för att säkra en virtuell anslutning mellan två kommunicerande parter (Bort och Felix, 1997). Detta innebär att SSL går utöver kryptering av autonoma meddelanden till att även säkra sessionsanslutningar (Bort och Felix, 1997). SSL är vidare oberoende av vilken typ av meddelanden som skickas (Bort och Felix, 1997). Detta innebär t.ex. att både HTTP-meddelanden med åtkomstförfrågningar till webbsidor eller FTP-förfrågningar till filresurser på ett nätverk kan säkras med SSL.

För att skapa en säker länk mellan två parter är det viktigt att dessa kan identifiera sig. För att uppnå denna funktion kan SSL tillämpa certifikat och digitala signaturer (Baker, 1997). Jag kommer i kapitel 6.4 nedan att beskriva olika former av certifikat och digitala signaturer närmare.

Private Communication Technology (PCT)

PCT är Microsofts svar på SSL och utvecklades i samarbete med Visa International (Bort och Felix, 1997). PCT är i grunden en bakåtkompatibel och utökad variant av SSL vilket skall leda till att PCT-implementerade servrar skall kunna prata med både PCT- och SSL-klienter (Bort och Felix, 1997). Dock kan inte alla funktion hos PCT utnyttjas av en SSL-klient (Bort och Felix, 1997).

PCT stöder längre nycklar och kan därför göras något säkrare än SSL men till följd av att SSL släppts i en ny och förbättrad version är det tveksamt om PCT kommer att få ett genombrott (Baker, 1997). Som exempel på detta kan nämnas att endast SSL finns omnämnt i manualen till Internet Explorer 4.0.

6.4 Certifiering och digitala signaturer

Förutom att ha möjlighet att kunna kryptera meddelanden och därigenom föra en säker kommunikation mellan två parter är det även viktigt att parterna säkert kan identifiera varandra. Som exempel kan nämnas att om en obehörig får tillgång till en användares privata nyckel kan kommunikation etableras på ett säkert sätt men av fel användare. Detta är inte särskilt lyckat och medför att metoder för att verifiera att kommunicerande parter är de, som de utger sig för att vara, måste tillämpas (Pfaffenberger, 1998). Dessutom är det lämpligt att även använda metoder för att upptäcka manipulering av meddelanden och för att avsända meddelanden inte skall kunna förnekas. För att komma till rätta med dessa aspekter som innefattar säkerhetsmålen åtkomstkontroll, integritet och ickedesavouering kan digitala signaturer och certifiering i samarbete med någon form av ”certificate authority” (CA) användas (Loshin, 1997).

6.4.1 Certificate Authorities (CA) och förtroendenätverk

CA-s bygger enligt Loshin (1997) på en form av förtroendenätverk. Problemet är att förhindra att obehöriga kan skicka krypterade meddelanden i någon annans namn (Loshin, 1997). För att lösa detta byggs ett förtroendenätverk upp. Detta byggs upp av ett hierarkiskt system av förtroenden som fungerar så att om t.ex. X litar på A och på B så bör A också kunna lita på B (Loshin, 1997). X har förtroende hos både A och B och får med detta förtroende tillgång till deras publika nycklar. A och B kan därmed ta kontakt med X för att X skall skriva på och styrka A:s och B:s identitet (Loshin, 1997). Detta fungerar så att A och B har var sina certifikat i vilka deras publika nycklar finns krypterade av X. X kan sedan jämföra A:s och B:s publika nycklar med den publika nyckel som finns i certifikatet. Eftersom det endast är X som kan dekryptera detta så kan X styrka respektive parts identitet. Således byggs vad Loshin

(1997) kallar ett förtroendenätverk upp. Kommunicerande parter som vill bli betrodda, t.ex. för webbhandel, registrerar således sin servers publika nyckel hos en CA (Loshin, 1997). CA-n fungerar sedan som en tredje betrodd part som är villig att garantera två kommunicerande parters identitet. Detta sker genom att CA-n undersöker att den publika nyckeln överensstämmer med den som finns i det utfärdade certifikatet som endast CA-n kan dekryptera (Loshin, 1997). Certifiering, dvs utfärdande av certifikat bygger på att en part som önskar kommunicera kan producera någon form av identitetshandling eller någon form av betalning för tjänsten (Loshin, 1997). Många CA-s har anpassats för att stödja SSL vilket även medfört ökad spridning av detta säkerhetsprotokoll (Loshin, 1997).

6.4.2 Certifikat

CA-s baserar sina tjänster på certifikat. Ett certifikat är en fil som skickas ut av en CA till en godkänd part som kan styrka sin identitet (Pfaffenberger, 1998). Den fil som skickas ut innehåller information om certifikatets utfärdare och innehavare samt om innehavarens publika nyckel och information om hur denna skall användas (Loshin, 1997). Certifikatet är när det skickas ut krypterat med CA-s publika nyckel (Pfaffenberger, 1998). När kommunikation sedan skall upprättas mellan två parter så frågar dessa CA efter motpartens publika nyckel och skickar med sitt certifikat och sin publika nyckel. Om certifikatet kan valideras genom dekryptering med CA-s privata nyckel så kan CA skicka tillbaka ett meddelande krypterat med sändarens publika nyckel som finns tillgänglig för CA i certifikatet (Loshin, 1997). I detta meddelande kan även den önskade kommunikationspartnerns nyckel följa med och därefter är ett förtroende mellan de två parter som i första hand ville kommunicera upprättat (Loshin, 1997). CA har i detta fall fungerat som en tredje part och genom krypteringen på certifikaten intygat att alla inblandade parter är de som de säger.

Att använda en CA som förtroendepart ger enligt Pfaffenberger (1998) påtagligt ökad säkerhet men alla lösningar har sina baksidor. Det blir visserligen svårare att komma åt och förfalska data men samtidigt kan CA-n bli utsatt för attacker vilket kan drabba alla dem som använder denna (Pfaffenberger, 1998). För att undvika detta finns det enligt Pfaffenberger (1998) tre olika sätt att så långt detta är möjligt garantera CA-n integritet.

- De som vill få certifikat måste kunna uppvisa erforderliga identifikationshandlingar så att inte certifikatet kommer i fel händer.
- De nycklar som CA använder för kryptering och dekryptering av certifikaten måste vara så pass långa att dessa inte kan äventyras då detta skulle leda till att vem som helst kan göra egna certifikat.
- Ingen anställd inom en CA bör ha tillgång till vare sig den privata eller den publika nyckeln i sin helhet utan kunskapen om dessa bör vara utspridd så att varje anställd bara vet en liten del av en nyckel.

Pfaffenberger (1998) menar att om dessa regler följs så kan användande av CA ge mycket goda säkerhetseffekter. Det är värt att notera att en CA inte alltid behöver vara en extern tredje part. En CA-server även kan upprättas av ett företag i t.ex. en DMZ och således förmedla certifikat till godkända extranetanvändare (Pfaffenberger, 1998). Detta, menar jag, skulle kunna vara en lämplig lösning i t.ex. ett kundfokuserat extranet.

6.4.3 Digitala signaturer

Pfaffenberger (1998) menar att användande av CA och olika former av certifikat visserligen med stor sannolikhet kan garantera att ett meddelandes innehåll bara är känt av behöriga parter. Det finns dock, menar Pfaffenberger (1998), ingen kontroll av om ett meddelande blivit manipulerat på vägen. För att lösa detta kan digitala signaturer användas (Pfaffenberger, 1998).

En digital signatur innebär att meddelandets innehåll plus eventuella certifikat körs genom en hashfunktion som genererar ett värde inom ett bestämt intervall (Pfaffenberger, 1998). Detta värde läggs sedan med i meddelandet som därefter krypteras med mottagarens publika nyckel och sänds iväg (Pfaffenberger, 1998). Pfaffenberger (1998) menar att det är osannolikt att mottagaren utifrån meddelandet genererar samma värde om meddelandet har ändrats på vägen och således ger den digitala signaturen en indikation till om meddelandet gått fram intakt.

7 Nätverksarkitekturer och applikationshantering

För att komma fram till vilka lösningar som kan implementeras för att skapa en bra arkitektur för ett kundfokuserat extranet anser jag att det är det viktigt att syftet och eventuella krav reds ut. Jag menar att ett kundfokuserat extranet skall tillfredsställa främst tre olika krav. Dessa krav är även anpassade i samklang med scenario 3 som finns i kapitel 5.5 Detta ger en mer allmän överblick av vad jag menar med ett kundfokuserat extranet. Jag anser att följande krav kan ställas:

- Information om unika produkter skall kunna presenteras för slutkunder och för andra utvalda aktörer. Inga andra skall komma åt informationen.
- Aktörerna skall, undantaget slutkunden, kunna leverera information begärd av kunden till en central webbserver varifrån den skickas säkert till kunden.
- Kunden skall ha möjlighet att bestämma vilken information som finns tillgänglig för extern åtkomst. Därtill skall kunden även ha möjlighet att bestämma om och i så fall hur de olika aktörernas databaser får samköras.

Dessa krav anser jag utgör grundkrav för en arkitektur som kan stödja syftet med ett kundfokuserat extranet. I begreppet arkitektur innefattar jag begreppsbyggnad om hur nätverk, säkerhetslösningar och applikationslösningar bör utformas.

7.1 Arkitekturaspekter i samband med ett kundfokuserat extranet

För att kunna skapa ett kundfokuserat extranet finns det vissa aspekter som är viktiga vad avser funktion och användbarhet. Slutkunder måste kunna erbjudas en krypterad och säker kanal in till det kundfokuserade extranetet då viss information kan vara av för kunden känslig karaktär.

Ett kundfokuserat extranet går att dela upp i olika säkerhetszoner (se kapitel 7.2.2). Detta ger möjlighet för det kundfokuserade extranet som skapas mellan övriga aktörer att utformas med större frihet. Fortfarande måste dock möjliga arkitekturer följa de krav som ställts upp ovan. Med anledning av detta kommer jag att i detta avsnitt ta upp stödjande nätverksarkitekturer. Jag kommer därefter även att behandla kraven på informationsförsörjning i samband med objektorienterade extranetapplikationer. Jag anser dessutom att föreslagna lösningar bör ha stöd för säkerhetsfunktioner då kundfokuserade extranet kan komma att behandla känsliga data och således inte bara användas för att ge åtkomst till webbroschyrer.

7.2 Möjliga nätverksarkitekturer

För att kunna ge en god redogörelse för vilka nätverksarkitekturer som står till förfogande kommer jag i detta kapitel att presentera dellösningar som jag anser är av särskilt intresse för ett kundfokuserat extranet. Dessa dellösningar kommer att ha två olika perspektiv. Det gäller gränsnittet mot slutkunder och mot övriga aktörer.

7.2.1 Virtual private network (VPN)

För att hantera kommunikation i gränssnittet mellan olika organisationer anser jag att ett ”virtual private network” (VPN) kan vara en lämplig lösning. Med ett VPN menas säkra datalänkar mellan två eller flera organisationer genom virtuella avskärmade tunnlar där krypterad information färdas (Pfaffenberger, 1998). Pfaffenberger (1998) menar att användning av tunnlar och VPN ger en förhållandevis hög säkerhet men att detta är en lösning som endast passar för informationsutbyte mellan eller inom ett

fåtal organisationer. Därmed passar detta inte för kommunikation med slutkunder då bland annat särskild programvara krävs (Pfaffenberger, 1998). Det är min uppfattning att tekniken med att bygga upp VPN mellan olika organisationer skulle kunna vara ett användbart alternativ i ett kundfokuserat extranet då det går att skilja mellan gränssnitt mot kunder och gränssnitt mot organisationer. Detta skulle således möjliggöra att organisationerna sinsemellan kan utbyta information på ett mycket säkert sätt och sedan i ett annat gränssnitt erbjuda slutkunden information.

Ett VPN fungerar enligt Pfaffenberger (1998) på så sätt att det mellan en firewall och ett intranet finns en tunnelserver som krypterar/dekrypterar all data som sänds eller tas emot. Firewallen är sedan i sin tur programmerad att bara släppa igenom och skicka data som kommer från den virtuella tunneln (Pfaffenberger, 1998). Motsvarande lösning finns sedan hos den organisation som ligger på andra sidan tunneln (Pfaffenberger, 1998). Ett enkelt exempel på hur en sådan lösning kan se ut ges i kapitel 5.5.

VPN bygger till viss del på zonindelning av det extranet som skapas (Pfaffenberger, 1998). Att indela extranetet i zoner med olika säkerhetsnivåer och åtkomstmekanismer ökar enligt Loshin (1997) möjligheterna att skydda information och resurser från olika former av säkerhetsproblem. Detta kallas enligt Loshin (1997) för att nätverket delas in i ”nested sequrity zones”.

7.2.2 Nested sequrity zones

Med nested sequrity zones menas att ett nätverk delas upp i olika delar, vart och ett med liknande eller egna säkerhetslösningar och åtkomstbehörigheter (Loshin, 1997). Zonindelningen fungerar på samma sätt som gränsdragningen mellan intranet/Internet. Det innebär att firewallösningar används för att dela av och styra den information som får passera mellan två zoner (Loshin, 1997). Säkerheten i de firewallösningar som används bör öka gradvis i takt med att nya hinder passeras och informationen blir känsligare (Loshin, 1997). Detta beror på att en inkräktare som knäckt det första hindret bör möta svårare och svårare hinder och inte tvärtom (Loshin, 1997). Detta beror enligt Loshin (1997) på att om den yttersta firewallen erbjuder den högsta säkerheten och en inkräktare tar sig igenom så är det rimligt att anta att denne också kan knäcka kommande hinder. Att använda zonindelning får även effekter på intern informationshantering inom en organisation då det är möjligt att effektivt skydda resurser och information även från interna hot (Loshin, 1997). Förutsatt att inte en circuit gateway (kapitel 6.2.2) används så erbjuder en firewall bara säkerhet i gränssnittet mellan två nätverk. Genom att dela upp nätverket i flera zoner skapas således möjligheter att applicera firewalls mellan dessa.

7.3 Extranetapplikationer och Distributed-Object Architectures

Att erbjuda möjligheter för slutkunder att komma åt information i databaser via Internet ställer stora krav. För att direkt dela ut en databas i en relativt osäker miljö måste det enligt Pfaffenberger (1998) finnas någon mekanism som kan styra åtkomst och distribution av information. Betydelsen av denna mekanism ökar om information skall sammanställas från flera databaser som dessutom kan vara geografiskt spridda (Pfaffenberger, 1998).

Tankesättet att försöka bortse från var resurserna finns och var databehandlingen sker är ganska nytt och kallas ”distributed-object architectures” (Loshin, 1997). Antag t.ex. att en slutkund loggar in på ett kundfokuserat extranet. Denne får då presenterat en webbsida som innehåller information från flera databaser vilka finns distribuerade hos

de i extranetet ingående organisationerna. Slutkunden behöver i detta fall inte explicit beställa information från varje databas. Dessutom behöver slutkunden inte veta något om var de olika resurserna finns någonstans. Jag anser att denna funktion är viktig för ett kundfokuserat extranet, då detta innebär att informationen inte behöver lagras permanent på en webbserver. Istället medger distributed-object architectures att den webbsida, som kunden kommer åt, genereras ”on the fly” och att informationen länkas in dynamiskt från relevanta databaser. Dessa förhållanden menar Pfaffenberger (1998) främjar både säkerhet och framförallt användbarhet.

Distributed-object architectures bygger på att istället för att programmera exakta gränssnitt mellan applikationer så byggs objekt upp (Loshin, 1997). Objekt kan skapas med ett bestämt gränsnitt och med egna data endast tillhörande objektet (Loshin, 1997). Detta innebär att objekt kan skapas med en viss funktion och ett väldefinierat gränssnitt (Loshin, 1997). Detta medför att objekt kan samverka oberoende av vilket programmeringsspråk eller plattform som används (Loshin, 1997). Detta kan medföra att en förfrågan till en webbserver resulterar i att denna skickar ett meddelande till ett objekt innehållande förfrågan om information från en databas (Loshin, 1997). Objektet kan sedan utifrån indata generera ett beteende (Loshin, 1997). Detta kan innebära att objektet först rådgör med ett annat objekt huruvida webbservern kan tillåtas att få åtkomst till databasen. Om detta tillåts, ställer objektet frågan till databasen, inväntar svaret, och skickar sedan detta vidare till webbservern (Loshin, 1997). I annat fall skickas ett felmeddelande (Loshin, 1997). Varje objekt kan ta hand om och innehålla data om endast en transaktion och samtidighet kan istället lösas genom att varje förfrågan genererar nya autonoma objekt (Loshin, 1997).

En viktig tanke bakom användande av objekt i samband med distributed-object architectures är att objektkod och även plattformen kan bytas ut utan att funktionaliteten påverkas (Loshin, 1997). Detta förutsätter dock att nya objekt får samma gränssnitt (Loshin, 1997).

7.4 Object request broker (ORB)

En möjlighet att utnyttja distributed-object architectures är att använda sig av ORB-teknik. Loshin (1997) menar att detta kan främja flexibilitet och effektivitet i olika extranetapplikationer. ORB-s är objekt vilka erbjuder tjänster i olika former av extranet. Dessa tjänster kan inkludera mekanismer för hantering av transaktioner, databasfrågor samt gränssnitt mot andra objekt eller andra ORB-s (Loshin, 1997). En ORB kan dessutom fungera som systembuss för mjukvara och för andra objekt. Detta kan närmast jämföras med en systembuss för hårdvara som tillåter inkoppling och identifiering av nya okända hårdvaruobjekt i en godtycklig kortplats (Loshin, 1997). Funktionalitet medger enligt Loshin (1997) att en ORB kan fungera som länk mellan olika objekt anslutna till ORB-en och därigenom möjliggöra effektiv och enkel kommunikation och meddelandehantering.

Den kanske allra viktigaste funktionaliteten vid användande av ORB-s är att dessa även kan utökas från att endast vara en isolerad komponent i ett intranet till att sammanbinda flera intranet till ett extranet (Loshin, 1997). Detta innebär i praktiken att en logisk objektorienterad systembuss för godtyckliga objekt kan utökas till att hantera transparent kommunikation i ett extranet (Loshin, 1997). Jag menar att denna funktionalitet ger ett mycket gott stöd för transparent informationsåtkomst även i ett kundfokuserat extranet. Detta beror på att den funktionalitet som användande av

ORB-s medför i praktiken ger möjligheter till implementering av ”distributed-object architectures” som jag tidigare i kapitel 7.3 argumenterat för.

De tjänster som en ORB vanligen erbjuder kan ses som en hel plattform för utveckling av allehanda applikationer (Pfaffenberger, 1998). Denna utvecklingsmiljö är dessutom på grund av det objektorienterade synsättet i stort sätt oberoende av vilka fysiska hårdvaruplattformar som används (Pfaffenberger, 1998).

Det har för implementering av ORB-s vuxit fram två olika standarder som helt eller delvis stöder filosofin (Loshin, 1997).

7.4.1 CORBA

CORBA är en standard som specificerar funktionalitet och beskriver hur objekt skall interagera oberoende av var i nätverket dessa befinner sig (Pfaffenberger, 1998). För att åstadkomma detta är CORBA fokuserat på användning av ORB-s både som kommunikationsplattform och som utvecklingsmiljö (Pfaffenberger, 1998). En annan funktionalitet med CORBA-s specifikationer på ORB-s är att dessa erbjuder en tjänst kallad ”dynamic invocation interface” (DII) genom vilken det går att ansluta objekt med okänt gränssnitt och lära sig mer om dessa (Pfaffenberger, 1998). När det nya objektet blivit känt läggs det till i klientens ”interface repository” och därefter kan objektet användas (Pfaffenberger, 1998). Detta medför enligt Pfaffenberger (1998) stora möjligheter att förändra och anpassa ett extranet efter nya krav. Detta beror på att CORBA dels möjliggör uppgradering till snabbare objekt och dels medger löpande transparenta förändringar av extranetets funktionalitet och beteende (Pfaffenberger, 1998). I CORBA-s arkitektur för hur ORB-s skall utnyttjas finns även uttalat att ORB-s oavsett plattform skall kunna kommunicera för att erbjuda helt transparenta tjänster över ett extranet (Pfaffenberger, 1998). För att göra detta har IIOP (Internet Inter-ORB Protocol) tagits fram (Pfaffenberger, 1998). Fullt utnyttjande av IIOP möjliggör transparent åtkomst av data från alla plattformar som implementerar protokollet förutsatt att den nätbläddrare som används även den har stöd för IIOP (Pfaffenberger, 1998). Således har IIOP och även CORBA som helhet kompatibilitetsproblem (Pfaffenberger, 1998). Dessa härrör från att CORBA utvecklas av datorvärlden förutom Microsoft som har sitt eget alternativ DCOM (Pfaffenberger, 1998).

7.4.2 DCOM

DCOM står för ”distributed component object model” och är Microsofts svar på CORBA (Pfaffenberger, 1998). DCOM lanserades först som en komponent i Windows NT 4.0 och är en del i Microsofts satsning på ActiveX (Pfaffenberger, 1998). DCOM bygger till stor del på ORB-tänkande men är också centrerat kring ActiveX varvid DCOM blivit dominerande på Windowsplattformen (Pfaffenberger, 1998). CORBA är huvudsakligen vinklat mot UNIX och specifikationen har enligt Pfaffenberger haft problem med höga införandekostnader och kompatibilitet. Microsoft har å sin sida svarar med att snabbt ta fram en användbar transaktionsserver och på grund av kompatibiliteten med ActiveX snabbt skapat stöd bland de flesta vanliga desktop-applikationer vilket allvarligt hotar CORBA (Pfaffenberger, 1998).

Jag menar att ett kundfokuserat extranet måste ta hänsyn till den miljö som slutkunden använder för att komma åt resurser. Bland hemanvändarna och även i de flesta organisationer är nog Windowsmiljön den vanligaste (Pfaffenberger, 1998; Loshin, 1997). Detta, menar jag, medför att DCOM får en särställning som det mest användbara alternativet i samband med ett kundfokuserat extranet då slutkunden troligen kommer att använda eller har tillgång till Windows i någon form.

8 Prototypmodellen

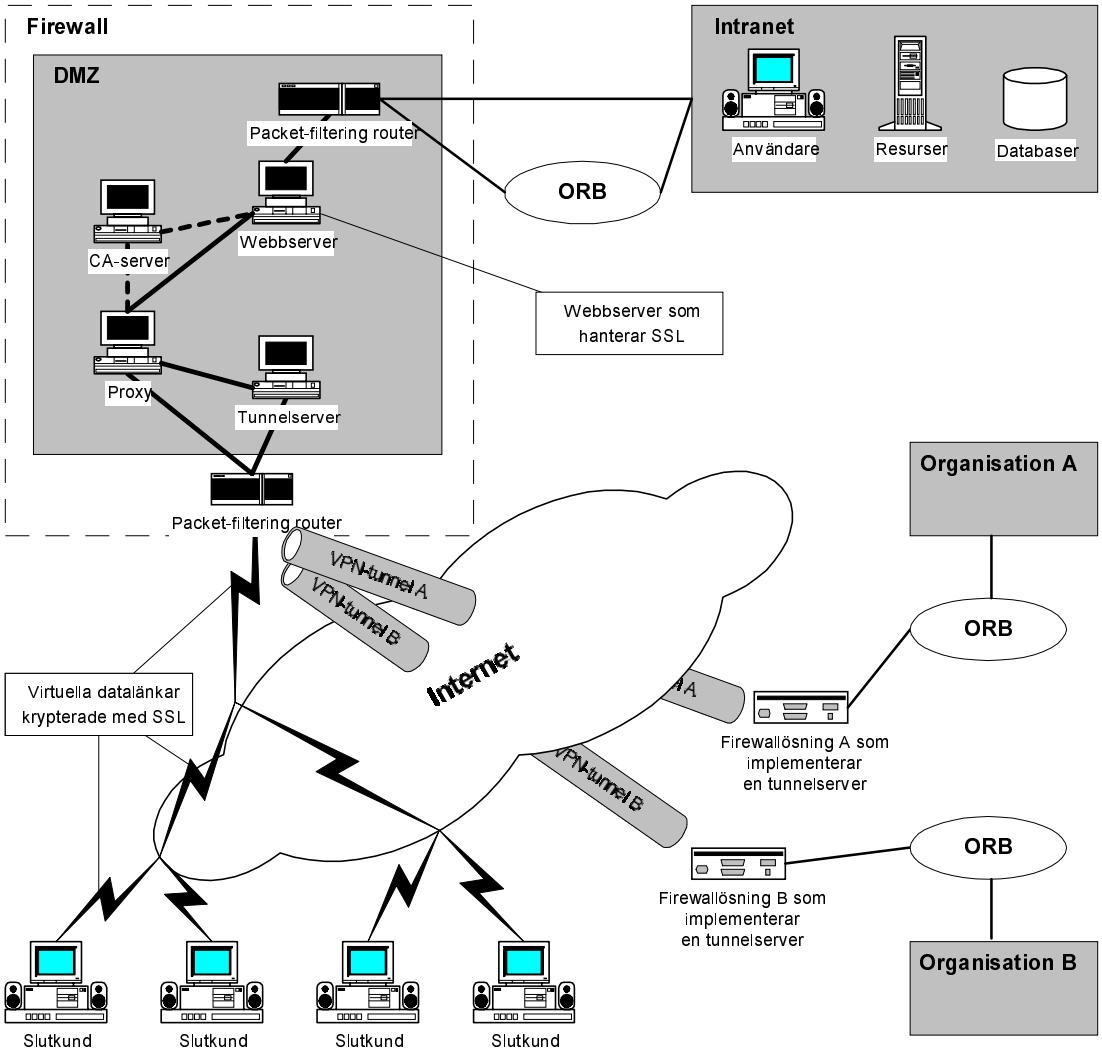
Med avsikt att illustrera hur en tänkbar uppbyggnad av ett kundfokuserat extranet kan se ut kommer jag i detta kapitel att föreslå en skiss av en övergripande prototypmodell. För att ta fram denna kommer jag att använda de olika komponenter och arkitekturer som jag redogjort för i kapitel 6 och 7. Prototypmodellen kommer därtill att vara en vidareutveckling av scenario 3 i kapitel 5.5. Min avsikt är inte att visa alla möjliga lösningar för hur ett extranet kan byggas upp utan jag kommer att inrikta mig på om det finns en lösning som stödjer ett kundfokuserat extranet. Detta medför att jag främst inriktar prototypmodellen mot kundgränssnitt och mot gränssnitt mot andra organisationer. Detta beror på att dessa aktörer är de som möjligen kan kopplas samman i ett kundfokuserat extranet. Perspektivet är vidare vinklat mot den organisation som initierar skapandet av det kundfokuserade extranetet. Detta medför att vissa beskrivningar är begränsade.

8.1 Översikt av prototypmodell

Ett kundfokuserat extranet bör erbjuda säker dataöverföring både mellan organisationer och mellan organisationer och slutkund. Samtidigt får säkerhetsmekanismerna inte vara så rigorösa att extranetet blir oanvändbart. Jag menar att säkerheten måste prioriteras efter hur många som skulle kunna drabbas eller hur stora skador obehöriga intrång skulle kunna orsaka. För att skapa en så fördelaktig lösning som möjligt anser jag att ett kundfokuserat extranet bör delas upp i olika zoner med någon form av ORB som kan hantera informationsspridning och insamling. Zonerna kan sedan skyddas med firewalls och olika metoder för kryptering, digitala signaturer och användarverifiering kan sedan användas för erbjuda erforderligt skydd.

8.2 Prototypmodell med kommentarer

Den prototyplösning jag har valt är tänkt att med ett undantag stödja samtliga säkerhetskriterier som redogjorts för i kapitel 6. Tillgänglighetskriteriet är undantaget då detta är ett resultat av att alla andra kriterier är uppfyllda (Bort och Felix, 1997). Säkerheten i kommunikationen mellan organisationer är särskilt kritisk varför jag valt att föreslå krypterade VPN-s som utnyttjar tunnlar för kommunikationen. Dessa tunnlar implementeras med både mjuk- och hårdvarustöd för alla anslutna parter. Vidare föreslår jag en heltäckande firewallösning inom en demilitarized zone som hanterar all inkommande och utgående kommunikation. Denna firewall skall sedan använda certifikat och SSL-kryptering mot slutkunderna. För att olika resurser inom det kundfokuserade extranetet skall vara åtkomliga för behöriga på ett transparent sätt, anser jag dessutom att någon form av ORB-lösning bör användas. För att sammanfatta mitt synsätt på en möjlig implementering av ett kundfokuserat extranet har jag valt att framställa en skiss av en prototypmodell.



Figur 8: Prototypmodell över möjlig nätverksarkitektur för ett kundfokuserat extranet. I gränssnittet mot slutkunder som ansluter ”on the fly” krypteras informationen med SSL och obehöriga stängs ute genom användande av certifikat och digitala signaturer. Gentemot andra organisationer fungerar det kundfokuserade extranetet med hjälp av hård- och mjukvaruimplementerade tunnelservrar som erbjuder en säker och krypterad kanal över Internet. De aktörer som vid ett givet tillfälle ingår i det kundfokuserade extranetet ansluter aldrig direkt utan detta görs via firewalls som kan låta aktörerna hämta information indirekt via ORB-s. Den firewallösning som finns visar schematiskt hur anslutningen går till. Routern gör för godkända adresser ett vägval beroende på om datan är krypterad i en tunnel eller inte. Proxyn förmedlar sedan, om innehållet är godkänt, en anslutning efter att CA-servern godkänt eventuella certifikat. Därefter skapas den virtuella anslutningen till webbservern som kan börja utföra de tjänster som begärs.

Den arkitektur för ett kundfokuserat extranet som föreslås i figur 6 är inte helt okomplicerad att genomföra och medför ett ganska allvarligt säkerhetsproblem som måste lösas. Antag att kunderna vill känna att ingen obehörig kan komma åt deras information genom att använda deras lösenord eller genom att agera med falsk identitet. Detta går att lösa genom att använda certifikat eller digitala signaturer. Digitala certifikat fungerar tillfredsställande så när som på en detalj. Jag anser att det är orimligt att en kund alltid kan ha tillgång till sitt digitala certifikat när kunden vill kunna komma åt sin information från olika platser. Antag t.ex. att kunden i likhet med scenario 3 har en bil och kunden vill komma åt information om den hemma eller från jobbet. Hur skall certifikatet transporteras? Jag anser att detta inte går att lösa på ett sätt som innebär att kunden både vet någonting och att den dator som används har certifikatet tillgängligt då detta kan vara svårt att flytta. För att lösa detta anser jag att

den certifiering och därigenom användarkontroll som skall användas måste byggas kring ett mobilt certifikat som kunden kan ha med sig. Jag vill anknyta till att de banker, som satsar på Internetkontor (en form av extranet), bygger sin säkerhet både på någonting mobilt, t.ex. smarta kort eller koddosor, och på någonting som kunden vet, t.ex. en Pinkod. Smarta kort innebär att kunden måste ha tillgång till en kortläsare varför detta inte är intressant. Att använda en koddosa med tillhörande Pinkod är däremot en intressant lösning då en sådan kan göras liten och fungera som nyckelring till bilnycklarna. Bilnyckeln är dessutom någonting som bilägaren ofta har med sig varför detta förmodligen inte skulle leda till att användaren glömmer koddosan, särskilt inte om bilen är med. Denna koddosa skulle dessutom kunna byggas in i larmdosan till de billarm som de flesta nya bilar har.

9 Analys

Detta kapitel syftar till att försöka koppla samman det faktiska genomförandet med hur detta besvarar givna frågeställningar. Jag kommer därför att sammanföra scenarier, litteraturstudie och prototypmodell kring ett resonemang huruvida detta besvarar mina frågeställningar.

Syftet med arbetet har varit att utifrån ett antal utvalda aspekter, undersöka om ett kundfokuserat extranet är möjligt att skapa. Det material som framkommit i undersökningen anser jag visar att ett kundfokuserat extranet är möjligt att skapa. För att belysa detta kommer jag nedan att ta upp de olika frågorna separat i en kort analys.

9.1 Genomförbarhet avseende teknik och nätverksarkitekturer

Den första frågan behandlar möjligheten att anpassa teknik och nätverksarkitekturer för ett kundfokuserat extranet. För att besvara detta har jag främst konsulterat litteratur. Bland de källor som jag använt märks här främst Bort och Felix (1997), Pfaffenberger (1998) och Loshin (1997). Författarna har liknande perspektiv på den teknik som finns tillgänglig och på hur den kan användas för att skapa extranetarkitekturer. Författarnas definitioner på ett extranet överensstämmer dock inte med definitionen på ett kundfokuserat extranet. Skillnaden ligger främst i kundfokus då dessa författare anser att extranet skapas främst med stora kunder och leverantörer medan ett kundfokuserat extranet även bör inbegripa slutkunder. Detta medför att jag vinklat materialet mot kundfokuserade extranet. Således har jag plockat bort delar som jag anser inte har haft tillräcklig koppling till kundfokuserade extranet.

Både Pfaffenberger (1998) och Loshin (1997) har snarlika lösningar på liknande problem och av dessa källor framgår klart att det finns lösningar både avseende teknik och nätverksarkitekturer som kan stödja ett kundfokuserat extranet. Jag har sammanfattat några av dessa i en prototypmodell som jag anser väl överensstämmer och stödjer ett kundfokuserat extranet. Detta tyder på att ett kundfokuserat extranet ur teknisk och arkitektursynpunkt är möjligt att skapa.

Undersökningen har även visat att det finns inkompatibilitetsproblem som gäller generellt för olika former av extranet. Pfaffenberger (1998) menar dock att objekttänkande inom extranetsektorn leder till plattformsoberoende som kan hantera de flesta av dessa problem. Vidare menar Pfaffenberger (1998) att färdigutvecklade program och standarder kan användas för att hantera applikationer i kundfokuserade extranet och då även att låta slutkunder vara delaktiga. Dessa applikationer tillsammans med hårdvara för uppbyggnad av nätverksarkitekturer ger således möjligheter att bygga ett kundfokuserat extranet.

9.2 Genomförbarhet avseende säkerhet

En hög säkerhetsnivå kräver enligt Loshin (1997), Bort och Felix (1997) och Pfaffenberger (1998) omfattande säkerhetsarbete och en rad implementerade säkerhetslösningar. Därtill menar författarna att ett extranet som exponeras mot Internet och tillåter Internetåtkomst måste kunna hantera åtkomstbehörighet och användarkontroll. Ett kundfokuserat extranet måste dessutom tillåta åtkomst från okända Internetanslutna datorer vilket medför att säkerhetsrelaterade aspekter rimligen ställs på sin spets. Pfaffenberger (1998) och Loshin (1997) menar att zonuppdelning av extranetet i säkerhetszoner med multipla firewalls kan vara en relevant lösning som kan hantera vissa säkerhetsproblem. Zonuppdelning kan enligt

Pfaffenberger (1998) och Loshin (1997) även göras gentemot webbservrar som tillhandahåller information till slutkunder. Pfaffenberger (1998) och Loshin (1997) menar att detta inte får innebära att kundernas säkerhet äventyras. Zonuppdelning skall enligt författarna ses som en dellösning som erbjuder kunderna högre säkerhet då informationen flyttas in bakom fler spärrar.

Jag anser att ett kundfokuserat extranet skulle få låg acceptans av slutkunder om känslig information inte förvaras säkert. För att hantera detta menar Pfaffenberger (1998) att certifiering och digitala signaturer måste tillämpas. I detta avseende har resultatet av min litteraturstudie överraskat mig. Säker användarcertifiering via Internet är inte möjlig om inte säkerhetsrutiner tillämpas som innebär att användaren både vet något och har någonting fysiskt, t.ex. ett certifikat i form av ett elektroniskt ID-kort, som kan styrka identiteten (Pfaffenberger, 1998 och Loshin, 1997). Detta kan medföra en begränsning av användningsområdet för kundfokuserade extranet och är därmed att betrakta som ett relevant problem som dock är lösligt med t.ex. en koddosa eller ett elektroniskt ID-kort som fungerar som certifieringslösning.

God säkerhet kan enligt Pfaffenberger (1998) och Loshin (1997) inte lösas enbart med certifiering utan är en funktion av en rad samverkande delkomponenter. Det finns enligt författarna en mängd olika alternativ för hur firewalls, intranet och extranetarkitekturer kan samverka för att skapa goda förutsättningar för säkerhet. Jag anser att dessa lösningar i hög utsträckning stöder kundfokuserade extranet varvid detta indikerar att ett sådant skulle vara möjligt att skapa.

9.3 Genomförbarhet avseende personlig integritet

Frågan om personlig integritet kan delas upp i två delfrågor. Den ena gäller hur säkerhetslösningar kan anpassas för användning i ett kundfokuserat extranet och den andra hur detta påverkar slutkunders personliga integritet. Dessa frågor har huvudsakligen behandlats indirekt. Detta beror på att om de säkerhetskriterier som ställts upp i kapitel 6.1 eftersträvas så ger detta kunden en tillräcklig bas för frågor rörande personlig integritet. Jag menar att om säkerhetslösningar i ett kundfokuserat extranet säkert kan identifiera en slutkund och endast ge denne tillgång till viss information så kan denna säkerhetslösning också hålla alla andra borta. Vidare måste implementering av användarkontroll och behörighet vara konfigurerbar. Detta medför möjligheter för kunden att själv, inom klart definierade ramar, få möjlighet att bestämma vem som får använda informationen och hur. De organisationer som möjligen skulle kunna sätta upp ett kundfokuserat extranet vill få tillbaka pengar på investeringen vilket kräver att extranetet måste få användare och därmed information som tillför värde.

Detta medför att ett lyckat genomförande bygger på förtroende från alla involverade parter. Detta innebär också att organisationer som har möjlighet att erbjuda tjänster i ett kundfokuserat extranet måste söka stöd för dessa tjänster dels internt men också hos de presumtiva slutkunderna. Jag anser att detta stöd rimligen uteblir om för kunderna känslig information exponeras utan att detta, inom vissa ramar, kan styras av slutkunderna själva. Det innebär att slutkunden bör få bestämma vilken information som finns tillgänglig och hur den får användas. Om slutkunderna själva kan välja anser jag att ett kundfokuserat extranets påverkan på personlig integritet blir minimal eller i alla fall ett resultat av självbestämmande.

Jag anser utifrån den undersökning som har gjorts att de säkerhetslösningar som kan erbjudas i ett kundfokuserat extranet stöder anpassning med avseende på personlig integritet. Dessa frågor måste dock till stor del avgöras på en organisatorisk nivå och i

samarbete med slutkunderna. Det medför att den undersökning som gjorts här endast klargjort att möjliga säkerhetslösningar är anpassningsbara men att undersökningens fokus inte förmår besvara frågor rörande påverkan på personlig integritet. Detta på grund av att vad som kan anses godtagbart måste bestämmas i samråd med slutkunder.

10 Resultat

I detta kapitel kommer jag att redogöra för de resultat jag erhållit och sätta dem i relation till de problemställningar och den teori som har initierat min undersökning.

10.1 Teknik och nätverksarkitekturer

Efter utförd litteraturstudie anser jag att det är fullt möjligt att med avseende på teknik och nätverksarkitekturer skapa ett kundfokuserat extranet. Jag menar att den undersökning jag utfört på ett klart sätt visar att såväl teknik som applicerbara nätverksarkitekturer finns tillgängliga.

Jag har till följd av detta kommit fram till en schematisk prototyp av en möjlig uppbyggnad av ett kundfokuserat extranet. Jag har tidigare i kapitel 4.2.1 nämnt att jag kommer att anse uppbyggnad av ett kundfokuserat extranet möjlig om det finns minst en komponentuppsättning som kan stödja detta. Då jag anser att såväl litteraturstudien som prototypförslaget stöder uppbyggnad av ett kundfokuserat extranet anser jag att ett sådant med avseende på teknik och nätverksarkitekturer är möjligt att skapa.

10.2 Säkerhet och säkerhetslösningar

Den undersökning jag har gjort visar att det med avseende på säkerhet och säkerhetslösningar finns tillgängliga tekniker som kan appliceras för uppbyggnad av ett kundfokuserat extranet. Dessa säkerhetslösningar kan vidare hantera möjliga säkerhetsproblem som kan uppstå.

Undersökningen behandlar säkerhetslösningar både med avseende på uppbyggnad av ett kundfokuserat extranet och med avseende på hot mot ett sådant. Undersökningen pekar på att en omfattande komponentlösning kan appliceras gentemot slutkunder medan säkerheten gentemot övriga aktörer kan lösas separat. Komponentlösningen gentemot slutkunden kan i så fall innefatta såväl en avancerad firewall som digital certifiering och digitala signaturer. Krypterade tunnlar i kombination med firewallen kan sedan användas gentemot övriga aktörer.

I samband med frågeställningen finns ett problem som visserligen går att lösa men som kan komma att kraftigt begränsa användningsområdet för ett kundfokuserat extranet. Undersökningen har visat att lösenord som enda användarkontroll är otillräckligt varvid någon form av komplement med digitala certifikat bör användas.

Problemet är att användare måste kunna logga in på det kundfokuserade extranetet från okända datorer. Detta medför att certifikatet måste vara mobilt och lätt för kunden att ta med sig. Ett mobilt certifikat kan t.ex. utgöras av en koddosa som eventuellt kan byggas in i en nyckelring, larmdosa eller dylikt.

10.3 Säkerhet och personlig integritet

Undersökningen visar att det är möjligt att anpassa säkerhetslösningar för att kunna hantera personlig integritet i ett kundfokuserat extranet. Undersökningen ger dock inga direkta svar på hur ett kundfokuserat extranet kan påverka personlig integritet. Istället pekar undersökningen på att påverkan av personlig integritet är något som intresserade aktörer, i samarbete med kunder, måste ta ställning till.

Säkerhet och personlig integritet är intimt förknippade med kundfokuserade extranet. Undersökningen visar att personlig integritet i ett kundfokuserat extranet är en

funktion av god och anpassningsbar säkerhet. Om känslig information om en slutkund är exklusivt åtkomlig för auktoriserade aktörer så är detta liktydigt med att informationen är oåtkomlig för alla andra. För garantera detta måste metoder tillämpas för att tillse att ingen kan avlyssna information eller utge sig för att vara någon annan. Ett resultat från undersökningen är därför att lösenord, certifikat, digitala signaturer och kryptering är betydelsefulla i ett kundfokuserat extranet.

Dessa tekniker är betydelsefulla då de stöder anpassning av generella säkerhetslösningar. Anpassning är därmed ett nyckelord för att kunna ta hand om säkerhetsproblem i samband med personlig integritet. Av detta följer att det bör vara möjligt, och även etiskt korrekt, att i extranetapplikationer ge slutkunder möjlighet att anpassa information om dem själva. Denna anpassning skulle t.ex. kunna avse vilken information som finns tillgänglig för vem och hur denna information får användas.

11 Slutsatser

I detta kapitel kommer jag att kortfattat presentera mina slutsatser utifrån genomförd undersökning. Med stöd av undersökningen är det min uppfattning att det avseende teknik, säkerhet och personlig integritet är möjligt att skapa ett kundfokuserat extranet då:

- Teknik och applicerbara nätverksarkitekturer för användning i ett kundfokuserat extranet finns tillgängliga.
- Det finns säkerhetsmetoder och tekniker implementerade i mjuk och hårdvara som kan lösa problem av säkerhetskaraktär.
- Krypteringsmetoder för att garantera användaridentitet och dataintegritet finns tillgängliga och är möjliga att implementera.
- Säkerhetslösningar i ett kundfokuserat extranet kan hantera personlig integritet då dessa kan anpassas för att tillåta explicit åtkomst av enskilda resurser. Anpassningsbarhet medför att slutkunder kan ges rättigheter att själva anpassa informationsspridning och informationsanvändning. Personlig integritet blir då en samarbetsfråga mellan enskilda slutkunder och övriga extranetaktörer.

12 Diskussion

Detta arbete har haft som syfte att framlägga teorin om ett kundfokuserat extranet och därtill undersöka dess validitet i vissa utvalda aspekter. Jag kommer i detta kapitel att reflektera och diskutera den undersökning och det arbete som jag utfört för att åstadkomma detta. Jag kommer således att diskutera vad som kunde ha gjorts bättre och vad som enligt min mening varit bra i samband med det arbete jag utfört. Därtill kommer jag även att redogöra för förslag till fortsatta arbeten inom problemområdet.

12.1 Undersökningens uppläggning

Detta arbete har inom sitt område försökt vara nyskapande. Detta har medfört att undersökningens uppläggning blivit normativ.

Innan jag påbörjade undersökningen sökte jag rätt på och kontrollerade om det fanns tillgänglig litteratur. Min uppfattning är att relevant litteratur finns men att denna inte i alla avseenden berör ett kundfokuserat extranet. Detta beror på att den litteratur som finns tillgänglig inom extranetområdet i stort sett uteslutande behandlar extranet gentemot storkunder och leverantörer.

Extranet har blivit ett modeord sedan det introducerades och då var det främst kunder och leverantörer som ville komma åt lager- och ordersystem för att skapa tidsvinster. På senare tid har många banker börjat erbjuda säkra banktjänster över Internet. Detta är en form av extranet som ligger närmare definitionen på ett kundfokuserat extranet. Ett kundfokuserat extranet går ett steg längre då detta skall kunna hantera relationen mellan en fysisk produkt och alla dem som handhar denna och erbjuda detta som en tjänst till kunden. Det kundfokuserade extranetet är således en ny företeelse som därmed begränsar möjliga uppläggningar av undersökningen.

Undersökningen inleddes med tre olika scenarier som förmedlar ett utvecklingsperspektiv. Dessa scenarier baserar sig på en idé av Ingi Jonasson. Denna idé har jag sedan i samarbete med Ingi Jonasson och utifrån egen erfarenhet och referenslitteratur utvecklat. I undersökningen och särskilt avseende prototypmodellen har det framkommit att scenarierna faktiskt speglar både användningsområde och översiktliga tekniska lösningar. Scenarierna har således, utöver förväntan, fyllt sin funktion och vidareutvecklat en begreppsmässig teori som varit stöd för fortsatt undersökning.

Litteraturstudien har haft två olika syften. För det första så ger den en teknisk orientering för uppbyggnad av ett extranet i allmänhet och ett kundfokuserat extranet i synnerhet. För det andra inriktar den sig på att specifikt ta reda på vilka tekniker, metoder och lösningar som kan vara tillämpliga för uppbyggnad av ett kundfokuserat extranet. Detta har medfört vissa tekniska djupdykningar som med avseende på problemställningen kan tyckas onödiga. Jag anser dock att dessa varit nödvändiga för att kunna föreslå specifika möjliggörande lösningar. Detta kunde kanske ha lösts på ett bättre sätt genom bättre förhandskunskaper och därmed bättre anpassning av den nivå som litteraturstudien förs på.

Nivåskillnaden i teknikaliteter är vidare stor mellan scenarier, litteraturstudie och prototypskissen. Denna nivåskillnad är som tidigare nämnts delvis ett resultat av alltför detaljerade djupdykningar men nivåskillnaden är också resultatet av ett medvetet arbetssätt. Scenarierna drar upp övergripande teoretiska ramar för ett kundfokuserat extranet medan litteraturstudien ger en teknisk beskrivning. Därefter följer en prototypmodell i vilken övergripande användning och sammansättning av i

litteraturstudien presenterade lösningar framförs. Min avsikt med detta har varit att börja med att ge en helhetsbild för att därefter undersöka detaljerna och sedan sätta samman dessa till en ny men mer detaljerad helhetsbild. Genom detta arbetssätt tycker jag att undersökningen på ett övertygande sätt gett resultat. Resultatet överensstämmer dessutom väl med det resultat som jag förväntade mig.

Ett specifikt resultat som överraskade mig var att säkerhetlösningar som endast bygger på lösenord inte kan garantera god informationssäkerhet i ett kundfokuserat extranet. Istället måste denna säkerhet bygga på både lösenord och på ett certifikat av något slag. Jag menar att detta visar varför de banker som tillämpar extranet för banktjänster alla bygger säkerhetslösningarna på både lösenord och certifikat. Min utgångspunkt när jag inledde undersökningen var att lösenord skulle räcka.

12.2 Erfarenheter kring arbetssätt

Detta arbete har på grund av sin teoretiska inriktning i hög grad utförts självständigt. Till en början har arbetet inletts med främst diskussion med handledare. Ur dessa diskussioner har en sammanhållande teori om ett kundfokuserat extranet framkommit. Dessa diskussioner sedan sammanställts till tre scenarier. Utifrån dessa har sedan en litteraturstudie och en prototypskiss utförts.

”Som man frågar får man svar” brukar det heta. Att ställa rätt frågor till handledaren kompliceras av att handledaren kanske inte har samma utgångspunkt eller samma referensram. Jag har under arbetet lärt mig att vikten av att komma väl förberedd till handledarmöten i den mening att det är på mina förberedelser och min kunskap som diskussioner måste ha sin grund. Handledaren kan då fungera som en katalysator för olika resonemang och för att göra bedömningar utifrån den kunniga läsarens perspektiv.

Att ställa rätt frågor för att få rätt svar har också medfört lärdomar i samband med litteraturstudien. För att få tag på rätt information är det viktigt att veta exakt vad som eftersöks. Den röda tråd som bör genomsyra en rapport går lätt förlorad om förhandskunskap och dispositioner saknas.

Jag insåg i samband med genomförandet av litteraturstudien att litteraturen inte kunde läsas parallellt som jag först hade tänkt. Detta medförde att jag först gick igenom all litteratur och därefter lade upp en disposition där alla kommande rubriker och kapitelindelningar strukturerades. Sedan kunde jag snabbt finna eftersökt material och samtidigt hålla ihop sammanhang och begrepp i vad jag anser vara en lämplig struktur. Denna struktur har visserligen korrigerats under undersökningens gång men dessa ändringar har inte varit särskilt omfattande. Detta är för mig ett nytt arbetssätt.

Genomförandet av litteraturstudien vållade inte några större problem. Ibland var det svårt att prioritera litteratur och veta vad som kunde utelämnas. Att läsa endast relevanta delar och utelämna resten anser jag kräver klart definierade problemställningar. Detta arbete har lärt mig vikten av att först skaffa bakgrundskunskaper för att sedan kunna formulera en klart definierad problemställning. Denna problemställning har sedan hjälpt mig att bevara den röda tråden genom arbetet och har därigenom hållit mig borta från stickspår.

12.3 Förslag till fortsatt arbete

Detta arbete täcker ett brett område varvid det finns en hel del intressanta uppslag till fortsatta arbeten. Några förslag på sådana skulle kunna vara:

- En undersökning som behandlar vilka preferenser som måste gälla inom områdena strategi, resurser, och kundpolicy för att ett kundfokuserat extranet skall gå att implementera. En undersökning behandlande dessa aspekter skulle kunna komplettera detta arbete och således validera teorin om ett kundfokuserat extranet ytterligare.
- En förstudie huruvida det inom en verksamhet finns förutsättningar för att kunna skapa ett kundfokuserat extranet. En studie av detta slag skulle kunna utröna vilka resurser och förutsättningar som krävs t.ex. med avseende på personal, kunskaper och på möjliga kostnader för införande, underhåll och eventuell nyrekrytering.
- En undersökning av hur en implementation kan genomföras. En undersökning av detta slag skulle kunna innefatta hur det kundfokuserade extranetet byggs upp och vilka problem och nya möjligheter som uppstår. Eventuellt skulle ett ramverk för implementation kunna fastställas.
- Undersökning av möjliga användarreaktioner på ett kundfokuserat extranet. Detta skulle t.ex. kunna ta formen av en enkät eller intervjustudie som utröner användarnas syn på de tjänster som kan erbjudas i samband med ett kundfokuserat extranet. Eventuellt skulle undersökningen kunna syfta till att ta reda ut användarnas reaktioner på ett antal möjliga tjänster relaterat till hur detta påverkar användarnas personliga integritet. Undersökningar av denna typ undersöker indirekt användarnas acceptans av en presumtiv tjänst vilket jag anser kan vara kritiskt för en lyckad satsning på ett kundfokuserat extranet.
- Praktisk implementation av ett kundfokuserat extranet. Detta skulle kunna innefatta framtagning och programmering av en praktiskt fungerande prototyp.

Referenser

Andersen, E.S. (1994), *Systemutveckling – principer, metoder och tekniker*. Andra upplagan. Lund: Studentlitteratur.

Baker, R.H. (1997), *Extranets the complete sourcebook*, New York, NY 10011: McGraw-Hill.

Bort, J. och Felix, B. (1997), *Building an extranet Connect your intranet with vendors and customers*. USA: John Wiley & Sons, Inc.

Casselberry, R, Baker, B, Benett, G, Calabria, C, Greene S, O´Donnel, J, Ramasubramanian, K, Rigg, J, Sankar, K, Schramm, D, Verschuren, I, Weber, J. (1996), *Running a perfect intranet*. Indianapolis, IN 46290: Que Corporation.

Ejvegård, R. (1993), *Vetenskaplig metod*. Lund: Studentlitteratur.

Forester, T. och Morrison, P. (1990), *Computer ethics Cautionary tales and ethical dilemmas in computing*. Oxford: Basil Blackwell Ltd.

Halsall, F. (1996), *Data communications, computer networks and open systems*. 4th ed. Harlow: Addison-Wesley Publishing Company.

Hills, M. (1997), *Intranet business strategies*. USA: John Wiley & Sons, Inc.

Loshin, P. (1997), *Extranet design and implementation*. Alameda, CA 94501: Sybex Inc.

Markgren, S. (1984), *Datainspektionen och skyddet av den personliga integriteten*. Lund: Studentlitteratur.

Neelamkavil, F. (1987), *Computer simulation and modelling*. Great Britain: John Wiley & Sons Ltd.

OECD (1980), *Guidelines on the protection and privacy of transborder flows of personal data*: OECD.

Patel, R. och Davidson, B. (1994), *Forskningsmetodikens grunder Att planera, genomföra och rapportera en undersökning*. Lund: Studentlitteratur.

Pfaffenberger, B. (1998), *Building a strategic extranet*. Foster City, CA 94404: IDG Books Worldwide, Inc.

Sandholm, L. (1995), *Kvalitetsstyrning med totalkvalitet*. Lund: Studentlitteratur.

Olovsson, T, Fredriksson, M, Johansson, M, Jonsson, E, Karlsson, A, Larsson, S, Laurén, C, Wiklund, J. (1999), *Säkerhetsarkitekturer*. Lund: Studentlitteratur

SOU. (1970), *Skydd mot avlyssning*. Integritetsskyddskommittén, nr 1970:47.

Ström, P. (1998), *Vinna eller försvinna i IT-åldern Internetsamhällets nya affärslogik*. Malmö: Liber Ekonomi.

Svenska Akademien. (1986), *Svenska Akademiens ordlista över svenska språket*. 11 upplagan, åttonde tryckningen. Stockholm: Norstedts Förlag.

Wikström, S., Lundkvist, A. och Beckérus, Å. (1998), *Det interaktiva företaget Med kunden som största resurs*. Stockholm: Svenska Förlaget Liv & Ledarskap.