


Handelshögskolan
VID GÖTEBORGS UNIVERSITET
Institutionen för informatik
2004-11-02

Uppdateringar
Påverkan på systemadministratörer och användare

Abstrakt

Den här uppsatsen syftar till att försöka få en bild av hur systemadministratörer och användare påverkas av att uppdateringar blir allt mer frekventa. Uppsatsen tar upp problemet med utgångspunkt från tre organisationer. Uppsatsen bygger på kvalitativa intervjuer av systemadministratörer och användare i dessa organisationer. En litteraturstudie genomfördes, främst har böcker från systemutvecklingens underhållsfas och artiklar från näringsliv studerats. Slutsatsen är att systemadministratörer påverkas av uppdateringar och de behöver en plan över hur de ska hantera detta för att säkerställa en bra systemmiljö på organisationen. Denna plan behövs också för få att kontroll över uppdateringarna. Användarna påverkas negativt, framför allt när de arbetar på distans, då de saknar kunskap och tid för att underhålla sin systemmiljö.

Nyckelord: Uppdatering, Patch, Systemunderhåll

Författare: Anders Adriansson, Gustav Flink
Handledare: Petersson, Lennart
Examensarbete 1 10poäng

Förord

Den här uppsatsen har vi genomfört under hösten 2004 på Institutionen för informatik, Handelshögskolan vid Göteborgs Universitet.
Ett stort tack till vår handledare Lennart Petersson för att han bistått oss med råd och stöd. Vi vill också tacka följande organisationer för att ha medverkat i vår respondentgrupp.

* Marin Mätteknik AB

* Mölndals Kommun, Barn och Ungdom Central- IT-grupp

* Göteborgs Universitet, Gemensamma förvaltningens dataservice

Göteborg 2004-10-20

Anders Adriansson
Gustav Flink

Innehållsförteckning

1.0 Inledning

Uppdateringar är en företeelse som har förändrats kraftigt under den senaste tiden. Förändringen märks främst på ökningen av säkerhetsuppdateringar. Cert CC är ett inrapporteringscenter för Internetsäkerhet och de har tydligt märkt av trenden. Till Cert rapporterades 1995 171 stycken säkerhetshål, medan det 2003 rapporterades 3784 stycken. Dessa säkerhetshål har tvingat fram uppdateringar för att åtgärda felen. Men ökningen gäller inte bara säkerhet. Ökningen av datorer och datasystem i samhället innebär också att antalet uppdateringar har stigit. I spåret av detta har många nyhetsartiklar rapporterat om konsekvenser, när uppdateringar inte har applicerats på olika system, vidare har man kunnat läsa om behovet att uppdatera för att skydda sig mot virusangrepp. Vi kan alltså konstatera att uppdateringar som helhet har ökat. Denna ökning kan bero på många faktorer. Sommerville (2001) menar att när de yttre faktorerna runt ett system ständigt förändras måste även systemet förändras, annars kommer det att förlora funktionalitet. Ett exempel på en yttre förändring är den ökningen av människor som arbetar från hemmet. Idag har 36 procent av företagen i Sverige personal sysselsatt som regelbundet arbetar utanför själva företaget och som använder sig av elektronisk kommunikation gentemot företaget (SCB 2003). Systemen måste då anpassas till den nya miljön medhjälp av uppdateringar. Christine Faulkner menar i *The essence of Human computer interaction* att det är ett krav att mjukvaran ska förändras för att bättre kunna stödja människan i dess arbete. Krav på förändringar beror på att vanliga användare hittar fel, kommer med förslag eller klagar på mjukvaran. Tillverkaren av mjukvaran svarar på detta genom att förändra systemet eller att strunta i användarnas önskemål. I takt med att uppdateringar ökar, ökar arbetet för systemadministratörer. Hur har systemadministratörer försökt att hantera denna utveckling? Vilka hjälpmedel har de till sitt förfogande och vilka hjälpmedel vill de ha till sitt förfogande? Finns det ett behov av att kunna automatisera uppdateringsprocessen eller förlorar då systemadministratörer kontrollen? Hur påverkas användarna av utvecklingen? Hur förhåller de sig till uppdateringar? Det finns många frågor men lite forskning på området ur detta perspektiv. Avsaknaden av forskning och relaterade arbeten gör att det är svårt att dra parallella jämförelser och slutsatser. Men denna uppsats är ett försök att besvara några av frågorna genom att djupintervjua ett antal systemadministratörer och användare av datasystem. Vilket föranleder oss till vår frågeställning:

1.1 Frågeställning

Hur hanterar systemadministratörer det ökade antalet uppdateringar av mjukvaror och vilka konsekvenser medför detta för användarna?

1.2 Avgränsning

För att kunna studera detta ämne krävs att man gör en avgränsning av problemet. Vi har valt att se på hur tre olika organisationer hanterar uppdateringar. Att undersöka ett större antal organisationer skulle ha blivit för omfattande. Intervjuobjekten avgränsades till en systemadministratör och en användare per organisation. Bara de olika system de intervjuade har angett att de använder och som uppdateras på organisationerna har diskuterats i uppsatsen.

1.3 Engelska termer

Vi har försökt att använda oss av svenska genom hela uppsatsen. Men då nästan all litteratur har varit på engelska och vissa ord inte haft någon korrekt översättning till svenska, har vi i detta fall valt att behålla den engelska termen.

2.0 Metod

Detta kapitel beskriver vår undersökningsmetod samt varför vi valt den.

2.1 Kvalitativ undersökningsmetod

Kvalitativ undersökning valdes för att få en bred helhetssyn. Undersökningen har ett litet urval. Den har heller inte en statistisk slumpmässighet och det finns därför en möjlighet att resultatet från urvalet inte motsvarar den totala populationen (Seymour, 1998). Intervjuerna har varit ett verktyg för att se det konkreta. Kriteriet för att medverka i undersökningen var att de använder datorsystem i verksamheten, vilket 97 % av alla företag gör i Sverige (SCB 2003).

Vi har i valet av organisationer försökt att se till eventuella organisatoriska skillnader, för att få en spridning. Vi har antagit att skillnader kan härledas till utformningen av organisationen (Mintzberg, 1993) likväl som till verksamhetsområdet. Också att en privat, en statlig och en kommunal organisation kan ha skillnader i sin inställning till uppdateringar. Detta innebär att vi får en ytterligare spridning i undersökningen. Vi ville också ha organisationer med skillnader i sin datorpark och även att användarna skulle skilja sig åt med tanke på ålder, utbildning och användarrättigheter i de olika systemen.

Vi försökte få en jämn genuspopulation men lyckades inte, endast en sjättedel av de intervjuade var kvinnor. Vi har valt att vända oss till både systemadministratörer och användare inom samma företag för att först få en klar inblick över hur uppdateringarna behandlas. Därefter undersöker vi vad uppdateringarna har för eventuella effekter på användarna och hur användarna upplever dessa. ”Vi börjar med konkreta observationer av verkligheten för att sedan bygga generella mönster, modeller och teorier” (Seymour, 1998). Vi har i vår undersökning en möjlighet att utveckla en förståelse för den situation som råder i djungeln av uppdateringar. Vår objektivitet ersätts av viljan att vara så nära det som studeras som möjligt (Seymour, 1998).

Vi valde att intervjua istället för att observera. Detta främst för att få reda på varför personerna gör på ett visst sätt, inte vad de gör. Bandspelare användes inte, istället fördes anteckningar av en av intervjuarna. Detta berodde på att eventuell känslig information kunde komma fram då vissa frågor kunde glida in på organisationernas säkerhet. En annan anledning är att många intervjuobjekt talar friare utan bandspelare (Trost, 1993). Just att de talar fritt om deras syn på uppdateringar inom organisationen är det som vi anser vara viktigt.

Vi begränsade oss till sex intervjuer då vi ansåg att detta skulle leda oss djupare ner i ämnet. Fler intervjuer skulle antagligen leda till en kvalitetshöjning vad det avser mängden av insamlad data, men vi var hämmade till att ha nio veckor till vårt förfogande.

Vi väljer att anta en halvstrukturerad intervjumetod som innebär att vi har en öppen intervjumall med ett antal föreslagna frågor. Frågorna var öppna och följdordningen oväsentlig. Intervjuerna började med en kort presentation av oss främst för att intervjuobjekten skulle känna sig säkra och avslappnade (Ejvegård, 1996).

När vi väljer en kvalitativ undersökningsmetod utgår vi från den undersöktes eget språk och symboler om vi däremot hade valt en kvantitativ undersökning skulle vi ha baserat undersökningen på svarsformulär med bundna svarsalternativ som vi skapat själva. Informationen vi vill få fram består av människors egna skrivna eller talade ord när de

definierar sin värld (Seymour, 1998) och vi anser att både systemadministratörens och användarens egna världar skall speglas.
Undersökningens tillvägagångssätt har varit att efter ha studerat in ämnet, djupintervjuade vi personer i tre olika organisationer: *Gemensamma förvaltningens dataservice* på Göteborgs Universitet, *Barn och Ungdom Central- IT-grupp* Mölndals Kommun och *Marin Mätteknik AB.* En systemadministratör och en användare intervjuas i varje organisation.

2.2 Validitet och reliabilitet

Vi har försökt lägga stor vikt vid hög validitet och reliabilitet i våra metoder. Vid valet av intervjupersoner anser vi oss ha hög validitet eftersom vi anser att har vi intervjuat rätt personer och har undersökt rätt fenomen. De personer som utgör vår respondentgrupp anser vi vara de mest relevanta och de besitter kunskap om den information vi behöver. Vi har försökt att anpassa vår intervjuteknik och har också härlett intervjufrågorna till uppsatsens frågeställning. Däremot kan reliabiliteten inte anses fri från slumpmässiga påverkningar. Vi har försökt att inte styra de intervjuade.

3.0 Teoretisk bakgrund

Detta kapitel beskriver vårt tillvägagångssätt för att finna information om uppdateringar och de svårigheter som framkom samt hur uppdateringar definieras. Den innehåller också en beskrivning av hur systemutvecklingen behandlar uppdateringar samt en plan hur man kan hantera uppdateringar.

3.1 Beskrivning av litteraturstudiens tillvägagångssätt

En litteraturstudie är en förutsättning för att få kunskap om ämnet. Man skaffar sig en bakgrund och en överblick av vad man vet inom ett givet problemfält (Backman, 1998). Vårt undersökningsområde utvecklas ständigt och det är därför viktigt att få aktuellt material. Litteraturstudien görs av böcker, främst böcker som behandlar systemutvecklingens underhållsfas men vi studerar även artiklar. En stor del information hämtas in från olika webbplatser. Vi studerar också delar av den information som finns tillgänglig hos tillverkarna av de system som uppsatsen handlar om. Begreppen som undersöks är uppdateringar och patchar. Vi inriktar oss på forskning om de problem och problemlösningar som förekommer vid uppdateringar.

Litteraturstudien omfattade vetenskapliga artiklar, dessa söktes i olika databaser såsom**:** HCI Bibliography (Human-Computer Interaction Resources Bibliography) och ACM (Association for Computing Machinery).

Detta resulterade i många träffar men vårt problemområde fanns inte upptaget i artiklarna.

Artiklar med *+problem +update*	
HCI	ACM
8	8000

Vidare utökades sökningen med flera olika termer. Exempel på dessa var patch, upgrade, reengineering och software management. Detta resulterade i fler träffar men problemområdet fanns fortfarande inte med. Ytterligare synonyma sökningar genomfördes med samma resultat.

Under litteraturstudien kom vi fram till att det fanns ett behov av att gå utanför de böcker som finns om software engineering och hitta artiklar som tar upp begreppet *att uppdatera sina system*. Detta ledde oss till olika organisationer vars uppgift är att informera om olika säkerhetsbrister i datasystem. Organisationerna har publicerat ett antal artiklar som riktar sig mot systemadministratörer och deras behov att planera och utarbeta en åtgärdsplan för hur de hanterar uppdateringar. Artiklarna tar inte upp begreppet uppdatering på samma sätt som i frågeställningen, men de utgår från att man skaffar sig en plan för hur uppdateringar skall gå tillväga. Information om hur man hanterar uppdateringar har också tagits upp av vissa programtillverkare. Denna information är mycket lik informationen som ges från säkerhetsorganisationerna.

3.2 Definition av uppdatering

För att kunna skapa sig en bild över vad en uppdatering är måste man försöka få en definition av vad uppdatering innebär.
Nationalencyklopedin beskriver uppdatera som:

upp`datera
SUBST.: **uppdaterande, uppdatering**
• komplettera genom att tillföra nya uppgifter till förteckning, register e.d.: *databasen ~s varje vecka*; *en ~d version av det nu tioåriga uppslagsverket*
HIST.: sedan 1960-talet; efter eng. *update* med samma bet.;

Med en uppdatering avser vi förnyelse av filer och/eller stycken av kod. Förnyelsen kan vara ett tillägg eller ersättning av den gamla koden eller filen. Syftet med att uppdatera är att förbättra ett system eller rätta till fel. När filen eller koden har lagts till i systemet blir det nya systemet en uppdaterad version av det gamla.

Sveriges IT Incidentcentrum (SITIC) är en organisation som ligger under Post och Telestyrelsen (PTS). Dess uppgift är att stödja samhället mot IT incidenter. Deras definitioner av uppdateringar av datasystem är följande:

Systemuppgradering – en ny version av produkten som tillför ny funktionalitet.
Systemuppdatering – åtgärdar ett stort antal fel i program eller operativsystem. En systemuppdatering består av flera programfixar.
Programfix – åtgärdar ett mindre antal fel i program eller operativsystem.(Sitic)

Microsoft har den största delen mjukvaror till både klientdatorer och servrar i materialet som vi har tittat på. Detta innebär att man måste se om de definierar uppdateringar på samma sätt. Microsoft beskriver uppdateringar som: ”En uppdatering är en fil eller en samling filer som kan installeras på datorn för att åtgärda ett specifikt problem.”(Microsoft Technet)
Microsoft har delat in uppdateringarna enligt ytterligare kategorier för att kunna skapa en ordning över hur olika rekommendationer och instruktioner skall fördelas (Microsoft Support). De beskriver också vart man hittar information om de olika uppdateringarna.

Update är en uppdatering som rättar till ett fel i programvaran. Den klassas inte som en säkerhetsrisk och är inte kritiskt viktig för systemet. Det följer alltid med information om vad uppdateringen gör i en artikel i Microsofts Knowledge base.

Critical Update är en uppdatering som hanterar ett allvarligt fel i programvaran, men som inte påverkar säkerheten. Information om uppdateringen finns i en artikel i Microsofts Knowledge base.

Security update gäller för säkerhetsrelaterat, produktspecifikt fel, det finns ett antal olika nivåer för hur viktig uppdatering är: kritisk, viktig, normal eller låg. Information om dessa uppdateringar och vad de innebär publiceras på två ställen, dels i Microsoft Knowledge base men också med en säkerhetskungörelse.

Hotfix är en uppdatering som påverkar ett problem som har hittats. Hotfix är gjorda för ett problem som har hittats hos en specifik kund, denna uppdatering är inte till för allmänheten och man får inte heller publicera den. Hotfixar distribueras av Microsofts product support services.

Service pack. När ett service pack publiceras är det en samling hotfixes, security updates, critical updates och updates. Den kan också innehålla rättningar för problem som inte är kända för allmänheten. Vidare kan vissa förändringar när det gäller utseende och funktioner finnas med. Även här finns det artiklar som beskriver vad ett servicepack gör.

3.3 Uppdatering enligt systemutvecklinglitteraturen

I den litteratur som behandlar systemutvecklings underhållsfas finns några kapitel som tar upp uppdateringar. Dessa kapitel handlar i stor utsträckning om att man måste uppdatera och hur man uppdaterar samt vilka sorters uppdateringar det finns, perspektivet är dock ett annat. Den eventuella påverkan uppdateringar har på systemadministratörer och användare saknas. Sommerville (2001) menar att system som är i drift är i behov av förändringar. Han anser vidare att systemen måste förändras för att kunna fortsätta vara till hjälp för organisationen och stödja dess funktioner. Det finns en del olika strategier för mjukvaruförändringar. Sommerville pekar på tre olika former av uppdateringar:

- *Underhåll* av systemet görs som svar på förändringar som skett i systemets miljö. Dock finns den fundamentala strukturen av mjukvaran kvar.
- *Arkitektuell omvandling* är en radikalare form av mjukvaruförändringar. Den gör större förändringar i mjukvarans arkitektur.
- *Software re-engineering* den här strategin skiljer sig från ovanstående då ingen ny funktionalitet läggs till systemet. Systemet modifieras för att lättare kunna hantera förändringar. Software re-engineering kan innebära strukturella förändringar men gör sällan några större förändringar i arkitekturen. (The Renaissance)

Pressman och Swanson skiljer sig lite från Sommerville i sin definition av vad för sorts uppdateringar det finns; Swanson (1990) delar in underhållet i fyra aktiviteter. Underhåll där man gör korrektioner i mjukvaran, underhåll där man anpassar mjukvaran, underhåll där man förbättrar mjukvaran och slutligen de preventiva underhållet reengineering.
Pressman (2001) menar att underhållet av existerande mjukvaror uppgår till mer än 60 procent av mjukvarutillverkarnas tid och resurser. Den här siffran fortsätter öka ju fler mjukvaror som tillverkas. (Manna 1993). Pressman refererar till Osborne och Chikofsky som menar att det läggs ner så mycket pengar och resurser på detta beroende på att mycket av mjukvaran är 10 till 15 år gammal. Den skrevs när programstorlek och lagringsutrymme spelade en viktig roll, då sådant var begränsat. Design och kodningsteknik har förändrats mycket sedan dessa mjukvaror gjordes. I dagens mått mätt menar Osborne och Chikofsky att äldre mjukvarors struktur är dålig, att de har dålig kod, dålig logik och dålig dokumentation[1]. Dessa system måste ändå underhållas. Pressman menar att då förändringar är ett krav när man utvecklar mjukvaror måste man utveckla mekanismer för förändring, kontroll och för att kunna göra modifieringar.

Pressman menar vidare att bara 20 procent av allt underhåll är att rätta till fel i mjukvaran. De resterande 80 procent av underhållet är till exempel att anpassa mjukvaran till en ny miljö, lägga till nya funktioner som efterfrågas av användarna och att med hjälp av reengineering förbereda mjukvaran för kommande underhåll. Man kan då förstå varför det krävs så stora resurser vid underhållet.

[1] Detta skrevs 1990, nu idag hörs istället röster om att komplexiteten i systemen ökar och försvårar. Då exempelvis Windows NT har 3 miljoner rader kod och Windows XP har 45 miljoner rader kod (Patch and pray 2003, http://www.csoonline.com/read/080103/patc)

3.4 Åtgärdsplan för uppdatering

Bland annat Sitic och Cert beskriver en åtgärdsplan där informationen om hanteringen av uppdateringar tas upp. Sitic och Cert tycker att organisationer skall ha en strategi för hur uppdateringar hanteras. Strategin bör innehålla utvärdering av systemnivåer, dokumentation, riskanalyser säkerhetstester, installationsförfarande, uppföljning av installerade programrättningar, säkerhetsuppdatering - hantering och katastrofplanering (Sitic).

3.4.1 Information om uppdateringar

Första steget i en åtgärdsplan är att införskaffa information om uppdateringar. Organisationer är i behov av detta då uppdateringar blir fler och fler. Att sammanställa en lista över alla program som finns inom organisationen är nödvändigt. Vid respektive program skall det finnas en lista över källor till den information som behandlar uppdateringar. E-postlistor och webbsidor dyker upp, försvinner och förändras hela tiden. Därför är det viktigt att hålla sin lista över källor uppdaterad. E-postlistor är bra då man får information om förändringar så snart de är tillgängliga. Webbplatser kan variera mycket i hur uppdaterad den information som presenteras på dem är. Informationen från Microsoft kommer oftast snabbt efter det att en bugg har hittats. I vissa program finns det inbyggda funktioner som informerar om när uppdateringar finns tillgängliga (Sitic)

3.4.2 Dokumentation av systemmiljön

För att skapa ordning i allt mer komplexa systemmiljöer, där system kräver uppdateringar med jämna mellanrum och allt oftare också akuta uppdateringar, rekommenderar säkerhetsorganisationer att man skapar en omfattande dokumentation över sina system, även Pressman (2001) uttrycker ett behov av en sådan dokumentation. Dokumentationen bör innehålla information om vilka typer av system organisationen äger, och vilka versioner som finns. Viktigt är att man dokumenterar de eventuella beroenden som finns mellan olika system. När kartläggningen av systemen är klar, grupperar man systemen. Grupperingen sker genom en klassificering av de olika systemen och vidare en indelning där man delar upp systemen i olika kritiska nivåer (Pressman, 2001). I dokumentationen beskriver man sedan vilka typer av uppdateringar man skall göra och vilken tidpunkt detta skall göras, beroende av systemets kritiska gruppering till exempel om skall man göra detta under dagtid eller efter ordinarie arbetstid (Sitic). I dokumentationen bör det finnas en förteckning över de personalresurser som finns inom företaget och vilken kompetens de har. Komplettering av dokumentationen efter en förändring är viktig, speciellt om många personer inom organisationen delar på ansvaret. I dokumentationen över systemet bör även en katastrofplan finnas. I denna skall åtgärder i händelse av dataförlust beskrivas, vem som skall kontaktas och vem är ansvarig. Om det har inträffat en katastrof bör dokumentationen även innehålla information om hur man undviker det i framtiden (Sitic).

3.4.3 Utvärderingar

Nästa steg i åtgärdsplanen enligt branschorganisationerna Sitic och Cert är att uppdateringar bör utvärderas. När en uppdatering publiceras av en mjukvarutillverkare, bör man ha en frågeställning gentemot uppdateringen.

Hur kommer denna uppdatering att påverka organisationen?
Kommer uppdateringen att påverka organisationens system och kommer det innebära problem?
Vilka är konsekvenserna om uppdateringen inte installeras?

När frågeställningarna är besvarade får organisationen väga fördelar mot nackdelar och ta ett beslut. Om beslutet innebär att man skall installera uppdateringen på systemet, är det viktigt att organisationen är medveten om att en uppdatering som är gjord för att åtgärda ett problem kan orsaka ett nytt (Sitic).

När en uppdatering har publicerats från tillverkaren och man skall göra en utvärdering rekommenderar tillverkare (Microsoft) att man följer ett antal steg:

1. Utse en ansvarig för uppdateringen,

2. Läs igenom all information som finns om uppdateringen. När informationen gås igenom bör fler än en person läsa den för att minimera risken att missa någon punkt som är kritisk för systemen.
När man läser igenom dokumentationen bör man tänka på om uppdateringen är relevant för organisationen. Kommer det att innebära problem om man installerar denna uppdatering? Hur kommer den att påverka systemen, finns det beroenden som följer denna uppdatering, t.ex. behöver vissa tjänster vara på eller stängas av för att uppdateringen skall fungera?

3. Bestäm vilken kategori uppdateringen kommer att hamna under när det gäller patchar.
När man har läst all information som tillhör en uppdatering bör man söka på tillverkarens hemsida för att se om ytterligare information har tillkommit. (Microsoft Technet)

3.4.4 Tester

Beroende på vilken kategori uppdateringen hamnar i kan man utvärdera i vilken utsträckning tester skall genomföras. Nedanstående tabell visar på hur bedömningen kan tillämpas enligt Microsoft.

Minsta nivå på tester:

Nivå på uppdateringen	Testfaser
Kritisk	Bedöm uppdateringen Utvärdera serverpåverkan (Begränsad)
Moderat	Bedöm uppdateringen Installera uppdateringen i en testmiljö Utvärdera påverkan på servern Kontrollera att avinstallation fungerar
Låg	Bedöm uppdateringen Installera uppdateringen i en testmiljö Utvärdera serverpåverkan Utvärdera påverkan på applikationerna Kontrollera att avinstallation fungerar

När en patch har utvärderats, med hjälp av informationen som finns att tillgå, bör patchen testas. Det optimala är om ett test sker på ett isolerat testsystem, då finns möjlighet att se hur den kommer att påverka organisationen utan att den gör någon skada för produktionen. Även möjligheten att genomföra prestandatest och kunna utvärdera materialet från en sådan körning är viktig att göra innan den installeras sin skarpa miljö (Sitic).
När testerna på testsystemet är avklarat är det vikigt att kontrollera att borttagandet av patchen fungerar. Efter avinstallationen testas systemet igen för att försäkra sig om att allt fungerar (Microsoft Technet).

3.4.5 Installationen
När organisationen tar steget att installera en uppdatering rekommenderar Sitic att man informerar de som berörs av uppdateringen. Man bör också ha en klar ordning i vilken följd uppdateringarna skall appliceras, samt kontrollera att uppdatering lyckats. Sommerville (2001) anser att en ångrafunktion bör finnas, för att kunna återställa system efter att en systemkritisk åtgärd, såsom en uppdatering har gjorts.

3.5 Säkerställandet av data inom organisationen
3.5.1 Säkerhetskopia
När man installerar en uppdatering är det viktigt att man har säkerhetskopierat systemet innan detta påbörjas. 47 procent av alla företag med mer än 10 anställda använder sig av databackup på annan plats än driftmiljön för att skydda sina data. (SCB 2003)

3.5.2 Skapa en rollbackplan
När testerna på en patch är avklarade och inga fel har upptäckts är det fortfarande viktigt att ha en plan för att kunna återställa systemen i det stadium de befann sig innan uppdateringen. Även om man har gjort omfattande tester kan fel hittas när uppdateringen appliceras i organisationen (Microsoft security, 2004).

3.6 Automatisk uppdatering
Automatiska uppdateringar är ett sätt att minimera det administrativa arbetet. Uppdateringar laddas ner med automatik, utan att involvera systemadministratören, möjlighet att även låta uppdateringar installeras kan finnas (Dunn). Nackdelen med detta är att administratören kan förlora kontrollen på vad som installeras på systemen.(Sitic). Vanligast förkommande varianten är en kombination mellan automatiska och manuella uppdateringar (Sitic).

Det finns ett antal program från tredjepartstillverkare som hanterar den automatiska uppdateringen när det gäller system. Alla är olika och har skilda funktioner. Det de har gemensamt är att försöka skapa ett lättare sätt att hantera uppdateringar.
Fördelen när man använder ett program som är avsett för denna uppgift är att inte bara Microsofts produkter stöds. Här kan man få program som uppdaterar Windows, Linux, Solaris, Aix, Netware och som dessutom stödjer en mängd olika applikationer. Problemet med dessa program är att de inte stödjer svenska operativsystem. (Nätverk och kommunikation nr.6 2004).

Till Linux finns det ett verktyg för att underlätta hanteringen av uppdateringar som heter YUM, Yellow dog Updater, Modified.

3.7 Vikten av att uppdatera

De flesta tillverkare arbetar aktivt för att förbättra mjukvaran. Antingen genom att rätta till fel eller anpassa mjukvaran till en annorlunda miljö, samt tillägg av funktioner eller modifiering av befintliga sådana (Sommerville, 2001). Problemet är att det tar tid från det att felet upptäcks och programtillverkare skapar en uppdatering till dess att användarna installerar uppdateringen. Det är denna tid då företag är mest sårbara gentemot personer som utnyttjar dessa svagheter i programmen. (ComputerSweden 2003-10-22 s.2)

Många mjukvaruföretag tar upp till sex månader från det att brister upptäcks i programmen till dess att de publicerar en patch. Lehmans tredje lag bekräftar detta då den säger att stora system har en egen dynamik, där resultatet beror på fundamentala strukturella och organisationella faktorer (Lehman 1985). Efter det att en uppdatering har kommit ut kan det dröja länge innan en organisation applicerar den på sitt system. Exempel på vad som kan hända om detta sker är den globalt kända masken sql slammer. Information lades ut på tillverkarens hemsida om sårbarheten och beskrivning över hur den/det påverkade systemen. En hacker, medveten om att företag inte applicerar patchar, lyckades skriva masken slammer. Den beräknas ha kostat samhället en miljard dollar (ComputerSweden2003-10-22 s.2).

Enligt Statistiska centralbyrån i *Företagens användning av datorer och Internet 2003* har uppskattningsvis 27 procent av företagen med 10–19 anställda, under de senaste tolv månaderna utsatts för datavirus som resulterat i förlorad information eller förlorad arbetstid medan 48 procent av företagen med 500 anställda eller fler utsatts för detta säkerhetsproblem. Detta visar på att virus är ett problem som företagen måste ta hänsyn till. De tvingas att uppdatera för att säkerställa sig mot dataförlust.

Systemutvecklingen har gått från linjärutveckling till att bli evolutionär, detta innebär att användaren har hamnat i systemutvecklingsfasen, där utvecklarna låter användare testa systemen. Dessa system är inte färdigutvecklade vilket leder till att användarna får uppdatera sina system med jämna mellanrum (Pressman, 2001). Detta kan leda till att användarna blir mer involverade i utvecklingen av mjukvaran, vilket i sin tur kan leda till ett bättre program som tillfredställer användaren i slutändan (Pressman, 2001). En annan aspekt på detta sätt att utveckla program är att mjukvarutillverkare släpper halvfärdiga program som kräver att man uppdaterar med jämna mellanrum. De släpper också ut system på marknaden som innehåller buggar[2]. Vi ser en trend att så är fallet, ett exempel är en produkt som en av organisationerna använder, där uppdateringar inte ingår om man inte tecknar ett dyrt avtal.

Vad detta innebär är att det är upp till användaren att hålla sina system uppdaterade och om detta inte sker finns det heller inga garantier att programmen fungerar.

[2] ”…komplexa program från marknadsledande företag är knökfulla med fel och det förväntas vi acceptera.” Anna-Marie Eklund Löwinder, Säkerhetsansvarig NIC-se (ComptuerSweden 2004 0917, s.21)

4.0 Resultat

I det här kapitlet finns en kort beskrivning av de intervjuade organisationerna och deras systemmiljö. Vidare redogörs en sammanställning av intervjusvaren från systemadministratörerna och användarna

4.1 Presentation av organisationer

4.1.1 Marin Mätteknik

Marin Mätteknik är ett mätföretag som har specialiserat sig på högupplöst sjömätning. De kartlägger med hög detaljrikedom hav och sjömiljö. De sysslar också med navigation, marin geologi och mjukvaruintegration av sin mätutrustning. Marin Mätteknik gör navigation, batymetriska, geofysiska och geologiska undersökningar. Deras mål är att kartera havsbotten och geologiska lager. De har även stor erfarenhet av sökuppdrag efter föremål på havsbottnen samt den utrustning som behövs för det. Marin Mätteknik använder sig främst av fyra fartyg vid sjömätning. Det arbetar sexton personer på Marin mätteknik men ofta många fler under de större projekten (MMT AB).

Systemmiljöbeskrivning

Företaget har klienter med Windows och Solaris. Windowsklienterna använder olika versioner av systemet, till exempel NT, XP och 2000. De använder sig av Linux, Solaris och Windowsservrar. Systemadministratören ansvarar för uppdatering av klienter och servrar, antivirus mm. Exempel på andra mjukvaror som används är Isis Triton, Autocad2000 och Office.

4.1.2 BoU Central- IT-grupp

Vid BoU Central- IT-grupp I Mölndal arbetar sju personer. De ansvarar för driften av cirka 1200 PC-datorer och servrar, samt ansvarar tillsammans med andra avdelningar för IT-utbildning av ca 8 000 till 10 000 personal och elever. Organisationens mål är att utbilda elever och personal inom IT samt tillhandahålla en bra systemmiljö (BoU).

Systemmiljöbeskrivning

IT-Miljön är centraliserad och använder sig av en teknik, som baseras på Windows 2000/XP och Citrix MetaFrame X. Servrarna står centralt placerade, men de har även en del klienter som använder sig av exempelvis äldre Windows versioner såsom 95, 98, ME, 2000. Man har använt sig till viss del av tunna klienter och Windows terminal server.

Andra mjukvaror som används är till exempel Office, Adobe photoshop, F-Secure.

BoU Central- IT-grupps strävan är att skapa olika standardmaskiner med identiskt innehåll. En standardisering av skrivarmiljön har införts.

4.1.3 Gemensamma förvaltningens dataservice

Inom Avdelningen för IT på Göteborgs universitet finns den Gemensamma förvaltningens dataservice (GFDS) som svarar på frågor och ger stöd åt datoranvändarna på Gemensamma förvaltningen när det gäller dator-, skrivar- och serverproblem. Den gemensamma förvaltningen ansvarar för ca 350 datorer och servrar (GFDS).

Systemmiljöbeskrivning

(Denna information gäller för denna avdelning inom Göteborgs universitet andra avdelningar på Göteborgs universitet har andra lösningar). Gemensamma förvaltningens dataservice

använder Windows till största delen i sin organisation. Windows Server 2003 används på deras servrar och på klienterna kör man Windows XP. Anledningen är att man vill skapa en enkel miljö som är lätt att underhålla och konfigurera.
De använder Citrix som en terminal-server lösning där man kör personalsystem och ekonomi på distans, även Ladok körs genom Citrix.

4.2 Intervjuer

Intervjuerna presenteras under tre rubriker, det är administratören allmäna syn på uppdateringar och hur de hanterar detta. Sedan följer *Information till användare om uppdateringar från administratören* och därefter *Användarna om uppdateringar*.
När vi nedan presenterar resultatet av intervjuerna har vi valt att inte skriva vilket företag som säger vad. Orsaken till detta är att vi inte vill ge ut vilket företag som säger vad med tanke på att det kan vara dåligt ur säkerhetstänkande att göra detta.

4.2.1 Administratören om uppdateringar

Det framkom i intervjuerna med organisationerna att de har upplevt ett antal problem med uppdateringar. Problem som omtalades under intervjuerna var av ganska olik karaktär. Någon gång hade alla tre organisationerna upplevt problem efter det att en uppdatering installerats. De som tillsynes skulle avhjälpa ett problem hade istället skapat ett nytt. En administratör berättade om en uppdatering som ledde till en instabil miljö med svårigheter att logga in, slöhet i systemen och krascher som innebar omstarter. Detta hände efter det att ett service-pack installerats. Det tog två veckor innan en ny uppdatering kom som kunde åtgärda detta. Då ett återställande med hjälp av säkerhetskopia fortfarande skulle låta ett säkerhetshål vara öppet fick de förlita sig på en instabil datormiljö. En annan administratör berättade om en uppdatering på sitt gamla jobb som ledde till att ingen kunde logga in på systemet. En tredje berättade generellt att uppdateringar ibland gör att program slutar fungera eller beter sig underligt. Alla tre intervjuade ansåg att servicepack ställde till problem och de väntade alla med att installera sådana.
Nästan alltid upptäcktes problem som en uppdatering skapat, med en gång. Sommerville (2001) menar att ju tidigare fel upptäcks, desto bättre är det, men givetvis skall detta ske under utveckling eller testningen av uppdateringen, inte efter det att uppdateringen lanserats. En av administratörerna hade tidigare upplevt det vanligt, att uppdatering ofta ledde till hårdvaruproblem. Han menade att äldre hårdvara inte klarade av de nya drivrutinerna, den var inte tillräckligt snabb att hantera nya versioner. Administratören ansåg att detta problem nästan inte existerade längre då hårdvara uppgradering blivit både billigare och enklare, samt att de numera gör uppdateringar bakåtkompatibla och antagligen testas bättre innan de släpps. Samtliga administratörer sa att när en uppdatering inte fungerade som den skulle och kanske orsakar problem kommer det en snabbt en rättelse, det dröjer sällan mer än några dagar.

Trots de brister som de intervjuade anser de ändå att uppdateringarna av systemen var ett måste, främst för att säkra sig mot virus och angrepp. De ansåg alla att uppdateringar har blivit bättre och mer lättåtkomliga. En av de intervjuade ansåg att dennes problem med uppdateringar minskat avsevärt under de senaste åren, trots att säkerhetsriskerna blivit fler.

4.2.2 Information till användare om uppdateringar från administratören

I samtliga organisationer var det administratörerna som hade rollen att informera sig om uppdateringar, samt att vidarebefordra den information de ansåg att användarna var i behov av. Någon information till användaren om säkerhetsuppdateringar av operativsystem gavs inte, det ansåg ingen av administratörerna att de var i behov av. Däremot informerades de ibland om andra uppdateringar. En administratör informerade när större uppdateringar av program gjordes. På en annan av organisationerna anordnades ibland kurser där de förändringar som tillkommit gicks igenom. På en tredje fanns det ofta egen gjorda interaktiva kurser som går igenom nyheter och förändringar som var resultat av uppdateringarna. Till två av administratörerna kom användare när de behövde hjälp med uppdateringar som hade krånglat. Administratören tog sig då tid att åtgärda problemet. På den tredje organisation fanns support dit användare kunde vända sig.

4.2.3 Användare om uppdateringar

Användarna som vi intervjuade har upplevt både negativa och positiva konsekvenser när det gäller uppdateringar. Det är också en avvikelse på hur det upplevs på arbetsplatsen och i hemmet. Vi har valt att ta med upplevelserna från hemmet då de djupintervjuade användarna inte skiljde dessa från upplevelserna från arbetsplatsen. Användarna arbetade till viss del hemifrån och behövde då en väl fungerande datormiljö. Skillnaden mellan problem som upplevdes i hemmet och på arbetsplatsen var att de problem som uppkom i hemmet upplevdes som mycket värre och fler.

En av användarna var missnöjd med hur policyn var utarbetad på arbetsplatsen, användaren tyckte att organisationerna saknade en struktur för hanteringen av uppdateringar. Åtgärderna verkade vara att ”installera allt som kommer för att vara på den säkra sidan”. En användare berättar om buggar som finns i en programvara, det finns uppdateringar som åtgärdar dessa buggar men de är bara tillgängliga om man tecknar ett serviceavtal med tillverkaren. De stora kostnaderna som är relaterade till serviceavtalet kan inte motiveras så buggarna får vara kvar. Ett tydligt exempel på när en uppdatering inte har installerats är problem med webbläsaren där sidor inte visas korrekt och att användaren därför inte kunde logga in på exempelvis sin bank

Information om uppdateringen som kunde läsas i samband med uppdateringen ansågs inte vara tillräcklig. Informationen som ges är alltför teknisk, användarna ville istället veta hur lång tid uppdateringen kommer att ta? Kommer datorn att sluta svara på instruktioner? Kommer det att krävas en omstart av datorn? Ingen av användarna tycker att denna information finns lättillgänglig. De anser sig inte ha tid att leta reda på vad som kommer att hända för varje uppdatering. Frustration upplevs när en uppdatering tar lång tid, användarna saknar också information om vad som händer under installationen. Användarna anser inte att avinstallation av en uppdatering var något som de kunde göra. När frågor om man vill uppdatera program kommer direkt efter start av datorn upplevs det som stressande, ofta har användaren bråttom och vill bara utföra sitt arbete. Efter att en uppdatering blivit installerad, märkte användaren sällan någon skillnad, varken i gränssnittet eller i funktionerna.

Några problem som upplevts efter en uppdatering var att alla personliga inställningar i programmet försvann och det tog lång tid att återställa. Att program automatiskt kopplar upp sig mot Internet och utan att fråga letar efter uppdateringar upplevdes av en av användarna som påfrestande. Positiva upplevelser efter en uppdatering är känslan av att uppdateringar gör datorn säkrare, och man känner sig tryggare. Någon gång har det tillkommit funktioner i ett

program som användaren inte hade saknat, dessa funktioner visade sig underlätta oerhört i användandet av programmet.

4.3 Åtgärdsplan

När administratörerna intervjuades försökte vi få en bild över om de använde någon form av plan för hanteringen av uppdateringar. Vi delar upp svaren från intervjuerna efter den så kallade åtgärdsplanen, viss information kan komma att upprepas från kapitlet ”Administratören om uppdateringar” men detta är för att skapa en tydligare bild över hanteringen av uppdateringar.

4.3.1 Information om uppdateringar

De intervjuade organisationerna hämtar information från olika källor. Information från Microsoft hämtas till största del ifrån deras hemsida. Man läser vilka uppdateringar som finns tillgängliga och avgör om de skall tillämpas på organisationen. Informationen från Microsoft kommer oftast snart efter det att en bugg har hittats. I vissa program finns det inbyggda funktioner som informerar om när uppdateringar finns tillgängliga (Sitic). Automatiska system för att hämta och informera om uppdateringar fanns till Windows operativsystem och de används i viss utsträckning i alla intervjuade organisationer. Ytterligare källor till information är forum där man framförallt läser om problem som olika uppdateringar tros orsaka. Muntlig information inhämtas också från andra personer med liknande yrken. Samtliga intervjuade systemadministratörer tycker att informationen som fås från tryckt press är för inaktuell för att vara intressant.

4.3.2 Dokumentation av systemmiljön

En av de intervjuade organisationerna sade sig ha en icke fullständig dokumentation av sina system. Denna plan var inte indelad efter några kritiska nivåer och ansågs inte heller vara helt aktuell. En annan av organisationerna hade en katastrofplan som hade kommit till användning vid ett serverhaveri. Ingen av de intervjuade organisationerna sade sig ha någon komplett sammanställd dokumentation över sina system utöver detta.

4.3.3 Utvärderingar

De intervjuade organisationerna har skillnader i ansvarsförhållanden över systemen. I en av organisationerna finns flera ansvariga för uppdateringar av sina respektive system. I en annan organisation finns en ensam ansvarig och i den tredje organisationen finns en grupp ansvariga över uppdateringarna. I de organisationer där användaren själv kan installera program, ansvarar de även för programmets uppdatering. Genomgång av information om vad uppdateringen gör och vilka eventuella konsekvenser den för med sig skiljer sig också mellan olika organisationer. Säkerhetsuppdateringar installeras på två organisationer utan att man utvärderar dem. Den tredje organisationen installerar dem först efter det att information har lästs igenom och behovet bedömts vara nödvändigt för verksamheten. En organisation säger att när de läser informationen om en Microsoft produkt måste de hela tiden bedöma om uppdateringen innehåller mer åtgärder än vad som står beskrivet i dokumentationen. Det kan till exempel vara rättelser till buggar som inte är kända för allmänheten mm. Däremot får man veta exakt vad som ändrats i sina Linuxsystem genom att läsa en såkallade *change log* uppgav en av de intervjuade.

4.3.4 Tester

Test av uppdateringar sker på olika sätt i alla organisationer och det beror på vilken typ av uppdatering det är. Säkerhetsuppdateringar installeras utan tester i två av organisationerna. Stora uppdateringar testas i en av organisationerna på ett antal datorer som finns under

administratörens kontroll och om dessa fungerar släpper man uppdateringen till resten av organisationen. När ett nytt service pack blir tillgängligt testas det av alla organisationer. Servicepack brukar först testas på några datorer för att se hur påverkan på systemen blir. Samtliga organisationer sade sig avvakta en stund innan man installerar dessa då erfarenhet visar att dessa ofta orsakar olika problem. En av organisationerna installerade inte servicepack förrän de kom på cd-skiva. Ingen av de intervjuade organisationerna kunde motivera en testmiljö ur kostnadspunkt. En hade gjort den bedömningen att tester av uppdateringar förutom servicepack kostar mer än vad man kan acceptera då de anser att kostnader för hårdvara och personal blev för höga.

4.4 Säkerställandet av data inom organisationen

4.4.1 Säkerhetskopia

När det gäller data på servrar sade sig alla kunna återställa sina data upp till flera månader tillbaka i tiden och frekvensen på kopieringen var minst en gång om dagen. En av organisationerna har även säkerhetskopiering på sina arbetsstationer. Säkerhetskopiering är en avvägning mellan behov och kostnader och är anpassad efter de olika verksamheterna.

4.4.2 Skapa en rollbackplan

Hur organisationerna återställer systemen till ursprungligt skick varierar. En av organisationerna använder verktyg för att ta en ögonblicksbild av systemet som man sedan använder för återställandet. Frekvensen på bilderna av systemet varierade mellan dagligen och veckovis beroende på vilket system man använde. Detta innebär att man tar en ögonblicksbild av hur systemet ser ut och om uppdateringen misslyckas återställs systemet enligt denna bild. Systemet fungerar bra men används sällan. En av organisationerna skaffar ghostkopior (ytterligare ett verktyg för att ta en avbild av system) när man hade en bra konfiguration av ett system och kunde utifrån denna återställa system. Den tredje organisationen använder inte något av dess verktyg utan förlitade sig på sina säkerhetskopior.

4.5 Automatisk uppdatering

Alla de intervjuade organisationerna använder sig av Windows update, en tjänst från Microsoft som ingår när man köper en vanlig licens. Två av organisationerna använde sig av den automatiska funktionen när det gäller säkerhetsuppdateringar, båda var nöjda med den funktionen. Den tredje organisationen anser, som tidigare beskrivet, inte detta tillräckligt säkert, istället utvärderar de uppdateringarna först. Andra verktyg som en organisation använt för att underlätta är Microsoft Software Update Services (SUS) som är Microsofts första försök att strukturera uppdateringsprocessen för företag. SUS är konstruerat för Windows serverlösningar. Organisation som har testat SUS ansåg det vara för komplext och svårkonfigurerat för att passa in i systemmiljön. De väntar istället på Windows Update Services (WUS) som är andra generationens uppdateringsverktyg från Microsoft och som skall vara mer anpassad för komplexa miljöer.

5.0 Diskussion

Detta kapitel innehåller vår slutsats utifrån den teoretiska bakgrunden och intervjuerna. Även en kortare metodutvärdering samt våra personliga reflektioner över hur organisationer bör hantera uppdateringar för att undvika problem.

5.1 Slutsats

Huvudfrågan i denna uppsats har berört frågan om uppdateringar upplevs som ett problem av systemadministratörer och användare, d.v.s. vi har ställt frågan "Hur hanterar systemadministratörer det ökade antalet uppdateringar av mjukvaror och vilka konsekvenser medför detta för användarna?" Vi sammanställer våra slutsatser nedan:

Mjukvaror har gått ifrån att vara statiska till att bli allt mer dynamiska, en utveckling man inte själv kan påverka. Denna utveckling både påverkar och resulterar i konsekvenser för organisationer. Systemadministratörerna hanterar detta på ett sätt som ligger i linje med utvecklingen. Dock skiljer sig hanteringen mellan de olika organisationerna. Konsekvenserna för användarna är varierande. Dock märktes den ökade uppdateringsfrekvensen i deras arbete.

Frågeställningen verifieras men inte i den utsträckning vi trodde. Anledning till detta tycks vara att systemadministratörerna som stödjer systemen gör ett bra arbete för att minska det problem som uppdateringar kan komma att föra med sig. De har accepterat uppdateringar som en del i vardagsunderhållet.

Användarna sade sig vara ganska nöjda med hanteringen av uppdateringar på sina arbetsplatser. Pressman (2001) skriver att om ett system tillhandahåller det användaren vill ha, är användarna också beredda att tolerera vissa problem med systemet. Användarna upplever de största problemen med uppdateringar på sina hemdatorer. Detta leder till frustration då de arbetar till viss del hemifrån. Framför allt den tid som uppdateringarna tar i anspråk anses vara källan till frustration. Utifrån intervjuerna kan vi se att uppdateringar påverkar hela organisationen på olika sätt. Det är en ständigt pågående process där tid och resurser tas i anspråk. Negativa konsekvenser upplevs när uppdateringar orsakar problem i systemmiljön. Positiv påverkan är att uppdaterade system ofta upplevs som tryggare Användares åsikter när det gäller uppdateringar skiljer sig mycket från administratörens. Här kan man se att uppdateringar orsakar fler problem än vad systemadministratörer säger, dock händer dessa problem oftast på deras hemdatorer. Begreppet uppdateringar är något som alla användare känner till och förstår innebörden av. Viljan att uppdatera sina system finns och känslan av att datorn blir säkrare var det som mest sporrade användaren att uppdatera. När problemen diskuteras är det framför allt osäkerheten kring vad som kommer att hända om man installerar uppdateringen som framträder. Största oron är att data skall förloras och att system inte skall vara tillgängliga under en tid. Dessa svar stämmer med vad vi trodde existerade innan vi började skriva uppsatsen. Dock trodde vi att dessa problem även skulle förekomma på arbetsplatserna, men det framkommer inte i någon större utsträckning.

5.2 Metodutvärdering

Vi har genomfört undersökningen med förhoppning om att kunna fastslå om uppdateringar är ett problem för användare av datorsystem. Genomförandet av undersökningen gick, enligt vårt eget tycke bra. Vi fick en spridning på organisationer när det gäller storlek och vilken typ av organisation det var. Här skulle man om det funnits mer tid tittat på ett mycket större antal organisationer för att få en bättre överblicksbild över hur uppdateringar uppfattas. Under intervjuerna med användarna har de besvarat frågorna om uppdateringar på ett mycket uttömmande sätt**.** Vi upplever den information om problemen som vi fick, beskiver hur en

användare känner sig i förhållande till uppdateringar. Det var svårt att få användaren att skilja mellan hur de upplevde uppdateringar hemma och hur det var på jobbet. Här önskar vi att vi hade haft tid att intervjua fler användare. Om vi hade haft möjlighet att intervjua ett större antal användare skulle vi ha fått en mer nyanserad bild över hur uppdateringar upplevs. Vi anser dock att vi med den tiden som fanns till vårat förfogande har fått en ganska tydlig bild över hur organisationer hanterar sina uppdateringar.

Litteraturen innebar vissa svårigheter, det finns ganska mycket information som tar upp underhållsfasen av systemutveckling men det passar inte riktigt in på problemet. Det krävde att vi sökte efter andra källor. Vi har hittat och använt ett antal källor som är organisationer med uppgift att informera om säkerhetsbrister. Dessa organisationer har skrivit ett antal guider som vi har kunnat applicera utifrån vår problemställning. Dessa guider kan ifrågasättas, de är dock opartiska. För att få en inblick om uppdateringar var ett problem, gjordes en genomgång av tidskrifter, denna kan om tid finns göras mer omfattade och statistisk kartlagd, men genomgången fyller sitt syfte i denna uppsats.

Andra arbeten med liknade frågeställning har vi inte kunnat hitta. Detta innebär att vi har mycket svårt att dra parallella slutsatser. Istället har vi fått luta oss mot branschorganisationers rekommendationer och utredningar. Närmast tillhands fanns systemutvecklingens underhållsfas men här speglas inte perspektivet från rätt håll.

5.3 Personliga reflektioner

Vår personliga tanke var att uppdateringar orsakar problem. Efter våra intervjuer bekräftades inte detta fullt ut. Problem finns, men inte i den utsträckning vi hade trott. Administratörerna tog uppdateringar som en del av sitt jobb och användarna upplevde att uppdateringar orsakar vissa problem men inte i någon större omfattning. Vår intervjugrupp är förstås för liten för att man skall kunna dra slutsatser men med tanke på spridningen ger det ändå en fingervisning om hur problemställningen upplevs. Då alla av de intervjuade ansåg att uppdateringar var ett måste kan en av orsakerna till detta vara den publicitet som viruslarm orsakat. Ett problem tycks dock vara att utvärderingen av uppdateringar inte fungerar, en hel del av uppdateringarna som installerades hos de intervjuade organisationerna hade inget med den viruslarm att göra.

För att organisationer skall kunna hantera uppdateringar, har olika säkerhetsorganisationer utarbetat åtgärdsplaner för hur hanteringen bäst struktureras och tillämpas i en organisation. Dessa planer innehåller steg från att dokumentera fram till att applicera uppdateringen i organisationens skarpa systemmiljö. Åtgärdsplaner är gällande för alla uppdateringar som publiceras för organisationernas behov.

När man saknar åtgärdsplan finns det risk att man installerar även sådana uppdateringar som det inte finns något behov av. Detta ökar risken för konflikter i systemmiljön och andra negativa konsekvenser.

Vi är förvånade över avsaknaden av kompletta åtgärdsplaner. Även om delar av åtgärdsplaner fanns inom några av de intervjuade organisationerna, så anser inte vi det tillräckligt. Vi tror att en utarbetad och efterlevd plan, som är anpassad efter organisationens behov, skulle kunna innebära underlättande av den dagliga hanteringen av uppdateringar. Denna plan skall innehålla uppgifter om olika kritiska nivåer som de olika systemen innehar samt alla de kopplingar som finns mellan dem.

Den tid man lägger ner på att hålla en sådan plan aktuell med den senaste informationen får organisationen tillbaka genom ökad kontroll och trygghet om ett problem skulle uppstå. En

annan positiv konsekvens är att då små och medelstora företag ofta bara har en person som ansvarar för uppdateringar, kan en åtgärdsplan underlätta vid eventuellt manbortfall**.**
Vi tror att organisationerna skulle tjäna på att strukturera hanteringen av uppdateringar. Denna åtgärdsplan tillsammans med ett automatiserat programverktyg som håller reda på samtliga datorer, system och systemversioner. Ett sådant verktyg håller också reda på vilka uppdateringar som är relevanta för de olika systemen. Med hjälp av detta underlättar man bedömningen avsevärt. Beslutet om en uppdatering behövs, kan göras med minimal arbetsinsats. Detta innebär också att man slipper osäkerheten vid problem om vad som egentligen har uppdaterats.
Problem som kan uppstå är att uppdateringar öppnar gamla åtgärder, detta innebär att det är viktigt att kunna återställa systemen.(Guninski)
Även information från den systemadministrativa avdelningen behöver förbättras, inte på en teknisk men på en informativ nivå till användarna.

Behovet av tester kan tyckas minska i takt med att uppdateringar blir allt bättre och innehåller färre fel[3] detta har samtliga av de intervjuade systemadministratörerna märkt. Men detta är en farlig väg att ta när konsekvenserna om det händer något med systemen kan bli allvarliga Behovet att testa och utvärdera uppdateringar kan aldrig underskattas, testandet kan underlättas om en vedertagen strategi följs.

Likriktade systemmiljöer förenklar men har begränsningar i utnyttjande av användarna och organisationen. Möjligheten för en organisation med en likriktad systemmiljö att använda sig av funktioner som underlättar hanteringen av uppdateringar är större än för en komplex systemmiljö. Blandade systemmiljöer försvårar det administrativa arbetet med uppdateringar men uppfyller användarnas och organisationens behov.

Nätverken blir mer komplexa och kommer att innehålla fler delar, till exempel handdator, mobiltelefoner osv. Allt måste uppgraderas och uppdateras när de ansluts till nätverken. Merarbetet som detta medför kan underlättas med ett 3:e partsprogram, då inte bara strukturen utan även behovet kan tillgodoses. För en organisation med en likriktad systemmiljö behöver inte användandet av ett 3:e partsystem för uppdatering fylla en sådan funktion att de kan anses motivera att köpas in.

Vi tror att det finns ett behov av att standardisera uppdateringar, en standardisering skulle underlätta bedömningen av hur kritisk uppdateringen är, är det en säkerhetsuppdatering eller är den till för en mobiltelefon?

När en organisation gör en utredning av hur de skall hantera uppdateringar av sina system, bör man överväga att hyra in en extern konsult, som har försäkringar mot dataförluster.

För att återställa system efter en misslyckad uppdatering används idag säkerhetskopiering. Det finns ett behov av att uppdateringar innehåller en funktion som tillåter ett enkelt återställande av systemet till dess tidigare läge istället för säkerhetskopiering. Om detta sker blir behovet av så kallade Rollback mindre. Vi anser att bättre tester av uppdateringar från tillverkarna och företagen minskar behovet ytterligare.

[3]]” *… Microsofts egna testar av patcharna blivit bättre. Han varnar dock för att det ändå är farligt att slarva med de egna testerna innan en patch tas i skarpt bruk. Analytikern Graham Titterington på Ovum”*
Microsoft blir allt bättre på att skriva bra uppdateringar,
(http://www.idg.se/ArticlePages/200404/02/20040402095337_NOK/20040402095337_NOK.dbp.asp)

6.0 Referenslista

6.1 Böcker

Backman, Jarl, **Rapporter och uppsatser**. Studentlitteratur, Lund, 1998

Ejvegård, Rolf, **Vetenskaplig metod**. Studentlitteratur, Lund, 1996.

Trost, Jan, **Kvalitativa intervjuer**. Studentlitteratur, Lund, 1993.

Seymour, Daniel T. **Marknadsundersökningar med kvalitativa metoder** , Högsbo Grafiska Göteborg 1992

Pressman, Roger S, **Sofware Engineering: a practitioner's approach**, McGrave-Hill New York, 2001

Sommerville, Ian, **Software Engineering**, Pearson Education Limited, Harlow 2001

Whiteley, David, **Introduction to Information systems**, Palgrave Mcmillan, New York 2004

Mintzberg, Henry, **Structure in fives designing effective organizations,** Englewood Cliffs, N.J, Prentice-Hall, 1993

Faulkner, Christine, **The essence of Human-computer Interaction,** Prentice hall, 1997

Osborne, W.M. E.J Chikofsky, **Fitting pieces to the maintenance puzzle,** IEEE Software, 1990.

6.2 Artiklar

Dunås, Elin. IT-Pro nr 4, 2004, Är ditt företag patchat och klart?

Jacobsson, Dick ComputerSweden 2003-10-22 s.2

Hanna, Mary, Maintenance Burden Begging for a remedy, April 1993 Software Magazine, (LV 2004-10-20)
(http://www.findarticles.com/p/articles/mi_m0SMG/is_n6_v13/ai_13732307)

Företagens användning av datorer och Internet 2003 SCB, januari 2004
Statistiska centralbyrån 2004-01-28, (LV 2004-10-20)
(http://www.scb.se/templates/publdb/publikation____2725.asp&plopnr=1899)

Berinato, Scott. Patch and pray, 2003, CSO, (LV 2004-10-22)
(http://www.csoonline.com/read/080103/patch.html)

Dunn, Kevin. Automatic updates risks: Can patching let a hacker in?, (LV 2004-10-20)
(http://www.insight.co.uk/downloads/presscoverage/PDA%20Security%20Concerns%20(Network%20Security).pdf)

The Renaissance of Legacy system (LV 2004-10-20)
Kapitel 1 och kapitel 2.
(http://www.comp.lancs.ac.uk/projects/RenaissanceWeb/project/Documents4.html)

Nazim H. Madhavji 2002, (LV 2004-10-20)
Lehman's Laws of Software Evolution,
(http://www.computer.org/proceedings/icsm/1819/18190066.pdf)

Osborne, W.M. E.J Chikofsky , Fitting pieces to the maintenance puzzle, IEEE Software, January 1990.

6.3 Webbplatser

Microsoft security guide Published: September 13, 2004, (LV 2004-10-20)
(http://www.microsoft.com/technet/security/guidance/legsgch6.mspx)

Georgi Guninski, (LV 2004-10-20)
(http://www.guninski.com/where_do_you_want_billg_to_go_today_1.html)

Swanson, E.B. The dimensions of maintenance 1990, (LV 2004-10-20)
(http://delivery.acm.org/10.1145/810000/807723/p492-swanson.pdf?key1=807723&key2=1247348901&coll=GUIDE&dl=GUIDE&CFID=29878480&CFTOKEN=46932885)

CERT, Coordination Center (LV 2004-10-22)
(http://www.cert.org/stats/cert_stats.html)

Mölndalskommun Barn och Ungdom IT-grupp, LV 2004-10-20
(http://www.skola.molndal.se/start/itinfo_filarkiv/filarkivet/IT-STR03.pdf)

Marin Mäteknik AB, (LV 2004-10-22)
(http://www.mmtab.se)

Göteborgs Universitet IT-enhet, (LV 2004-10-22)
(http://www.it.gu.se/org/default.html)

Sitic Sveriges IT incident centrum. (LV 2004-10-22)
(http://www.sitic.se/rad_och_rekommendationer/fr_uppdateringar.html)

Microsoft Technet, (LV 2004-10-22)
(http://www.microsoft.com/technet/prodtechnol/winxppro/sv/deploy/hfdeploy.mspx)

Microsoft Support, (LV 2004-10-22)
(http://support.microsoft.com/?kbid=824684)

7.0 Bilaga Intervjufrågor

Systemadministratör Del 1:

Vilka system används (olika former av servrar och klienter)?
Versioner av Operativ system? Office paket? Antivirus program? Några andra program?

Används ett system för patchhantering, vilket system i så fall? Om nej varför inte?

Hur ofta måste ni uppgradera eller uppdatera era system? (Exkludera virusprogram).

Hur ofta skedde detta när du började arbeta här? Hur länge har du jobbat med det detta?

Hur tror du att utvecklingen kommer att fortsätta?

Hur ofta uppkommer problem efter en uppdatering?

Vilken typ av problem är då vanligast? (Exempel: omstart, konflikter, instabilitet)

Har dessa problem förändrats under den perioden du har jobbat med detta?

Testas patchen innan den integreras i den skarpa miljön? Om ni testar patchen hur går ni tillväga?

Vem ansvarar för om eventuella problem uppkommer i samband med patchar?

Åtgärdsplan vid problem? Är ni försäkrade mot dessa eventualiteter?

Finns det någon uttalad policy för när/hur patchar skall appliceras i företaget? Skiljer sig denna för olika typer av system, typ applikationsservrar, användarmaksiner.

Skiljer sig en ev. policy för olika programtyper, OS kontra användarprogram t ex

Hur skiljer sig programvaruleverantörerna åt med avseende på patchar, t ex snabbhet att fixa fel osv.

Har ni råkat ut för något större problem på grund av att ni inte upgraderat eller uppdaterat era system?

Har ni råkat ut för något större problem på grund av att ni upgraderat eller uppdaterat era system?

Systemadministratörer Del 2:

Hur upplever ni uppdateringar?

Hur upplever ni patchhanteringen?

Vem skall ha rätt att patcha? Kan användare själv få göra detta?

Vilka är de vanligaste anledningarna till att medarbetare inte vill uppdatera sina system? (exempel Omstarter, förändringar i program, tidskrävande, att inte veta vad som kommer att hända)

Varför skall man patcha/uppgradera, är det alltid bäst med det senaste?

Hur upplever ni mediatrycket om säkerhets uppdateringar?
(viruslarm)

Hur ofta resulterar uppdateringar till användarproblem som upptäcks långt senare?

Utbildas användare vid större uppgraderingar av system?

Har du några förslag på en smidig lösning för hur uppdateringar ska lösas?

Frågor för användare
I vilka system arbetar du?
(Versioner av Operativ system? Office paket? Några andra program?)

Vad är en uppdatering för dig?

Hur ser du på uppdateringar?

Hur uppdaterar du dina system eller gör du inte det?

Brukar du få information om uppdateringar som har gjorts på dina system?

Hur upplever du uppdateringsprocessen av dina system?

Skulle man kunna göra på något annat sätt?

Upplever du några problem?
(Tidsåtgång, omstarter, konflikter, förluster, förändringar i gränssnittet ?)