TEKNISKA HÖGSKOLAN

HÖGSKOLAN I JÖNKÖPING

# KONTINUITETSPLANERING

# FÖR

# Saab Training Systems AB

Ulf Andersson

EXAMENSARBETE 2008

TEKNISKA HÖGSKOLAN

HÖGSKOLAN I JÖNKÖPING

# KONTINUITETSPLANERING FÖR SAAB TRAINING SYSTEMS
Continuity Planning for SAAB TRAINING SYSTEMS

Ulf Andersson

Detta examensarbete är utfört vid Tekniska Högskolan i Jönköping. Arbetet är ett led i den treåriga högskoleingenjörsutbildningen. Författaren svarar själv för framförda åsikter, slutsatser och resultat.


| | |
|---|---|
| Examinator: | Inger Palmgren |
| Författare: | Ulf Andersson |
| Handledare: | Anna Karin Carstensen |
| Utskriftsdatum: | 2009-05-27 |

## Sammanfattning

Katastrofer uppstår med ohämmad frekvens. Allt från enkel felhantering av människor till riktigt stora katastrofer, händelser som kan ha allvarliga konsekvenser för en affärsverksamhet.

Efter attacken på World Trade Center har man sett alldeles för omfattande förluster. Förutom stora förluster av människoliv så förstördes mängder av värdefull information som lagrades i olika datorsystem. Stora företag har gjort relativt stora framsteg i arbetet att uppdatera sina katastrofplaner. Utan att ha haft så kallade ”off-site backups” av legala dokument och konfidentiella datafiler, har många företag förlorat stora mängder av kritiska dokument. Många företag har spenderat miljontals dollar på kontinuitetsplaner som ska mildra risken för att bli utsatta för en katastrof. Dessa enorma spenderingar är investeringar för att garantera säkerheten av verksamheten och försäkra värdet av verksamhetens tillgångar.

Informationssäkerhet involverar många aspekter både när det gäller externa och interna hot. Det kan handla om enskilda användare som överskrider sina rättigheter och därmed kan komma över konfidentiell information. Det kan även vara brist på kunskap om vad informationssäkerhet är för något och vad som gör att medarbetarna lagrar känsligt material på bärbara datorer eller öppet diskuterar affärer i offentliga sammanhang. För att öka säkerheten behöver det formuleras skriftliga rutiner och anvisningar för de anställda.

Kontinuitetsplaneringen inleds normalt med att man börjar med att identifiera de områden som skall skyddas. De mest kritiska processerna inom organisationen och de tjänster de levererar analyseras. Inarbetade processer och rutiner och på det sätt de används av medarbetarna uppdateras i takt med att man identifierar eventuella hot.

Planen rekommenderar att man anskaffar ett Intrusion Detection System (IDS) som hanterar inloggning, larm och eventuella motattacker. Planen hanterar även virusskydd och hur olika virus kan skada datasystemet. Det är viktigt att förstå hur olika typer av antivirusprogram hanterar hot och att man installerar dem på bäst sätt för att erhålla bästa skydd.

Det är extremt betydelsefullt att ha en god strategi för att bevara data på en plats som inte är direkt kopplad till datorhallen. Det är också viktigt att återvinna data på ett korrekt sätt vi ett eventuellt datorhaveri.

Målet med kontinuitetsplanen har varit att motverka datastörningar inom en affärsenhet och att skydda kritiska processer för att minimera datorfel samt att nå en skälig återställningstid efter ett datorhaveri.


## Nyckelord

- Kontinuitetsplanering
- Saab Training Systems AB
- IT Infrastructure Library
- Brandvägg
- Intrusion Detection System
- Anti-Virus
- Backup


## ABSTRACT


Disasters occur often with unrestrained frequencies, from basic misunderstanding by humans to immense disasters, events that can have serious consequences for a business unit.

After the attack on the World Trade Center we have seen extensive losses, which gave us a new realization on how vulnerable our societies are. Except for the loss of human beings, also valuable information vanished in different computer systems. Large companies have made some progress in updating their catastrophe plans. Large companies have invested in millions of dollar on continuity plans to lower the catastrophic risks. These huge investments guarantee the security and ensure the value of the companies assesses.

Continuity planning is an instrument to increase the competence and preparedness inside an organization and to be able to reduce interruptions in the business. The plan promotes the reduction of damage caused by one or several severe interruptions. A continuity plan establish processes and prepares an organization to coordinate the work, create and implement the plan, review and test the plans and to handle a continuity adaptation of the plan to validate new risks, threats and changes in the business.

A condition to develop and document a continuity plan is by implementing a thorough risk analysis. The goal is to identify interruption events that are related to the business infrastructure.

These events should be reviewed through a risk perspective, where the probability and consequence of an interruption is analyzed.

The work with continuity planning starts with the task to identify the areas that need to be protected. It includes identifying the most critical processes within the organization and their delivered products/services which needs to be protected. Existing processes, routines and the way the employees handles the daily work can be changed by ensuring that the business operation receives proper IT-support. The continuity plan ensures that the company processes are followed properly and these processes shall be modified/updated if the plan so requires. Some applicable processes are described within the “IT Infrastructure Library” section.

The plan recommends acquiring an Intrusion Detection System (IDS) that deal with logging, alarming and counter attacking activities. Pros and cons are considered for positioning the IDS externally or internally of the firewall.

Data virus has always been a threat for computer users. The plan defines various virus threats and how these affect the computer systems. It is important to understand how various anti virus SW deals with the threat and to install and execute them properly to get the most beneficial use of them.

It is extremely important to have a good backup strategy to save data at a remote location in the case of a computer breakdown. It is also important to restore the data in a correct manner after a computer breakdown. The plan deals with these activities and gives proper recommendations.

The goal of the task has been to reach new levels of preventing interruptions within a business unit and to protect the critical processes within the organization to minimize errors within the computer system and to reach a reasonable restore time after a computer breakdown.

## INNEHÅLLSFÖRTECKNING

# Table of Figures

# 1 INLEDNING

Kontinuitetsplanering är ett medel för att öka skickligheten och beredskapen inom en organisation för att kunna hantera avbrott i verksamheten. Den ska främja till att reducera skador som härrör sig från ett eller flera avbrott. Kontinuitetsplaneringen ska även säkerställa att organisationens kritiska processer skyddas på en acceptabel nivå som kan garantera en finansiell och konkurrenskraftig position. Kontinuitetsplanering kan även kallas katastrofplan, avbrottsplan eller beredskapsplan.

En kontinuitetsplan innefattar bland annat etablering av processer, och en organisation som kan koordinera arbetet med att utarbeta och införa planen, genomföra granskningar och tester av planen samt hantering av kontinuerlig anpassning av planen för nya risker, hot och förändringar i verksamheten. Ett bra förslag på dessa tester är ITIL[2] som kommer att beskrivas längre ner i rapporten. Kontinuitetsplanen ska utgå ifrån organisationens övergripande säkerhetspolicy, om sådan finns, och inte vara begränsad till dess informationssäkerhetspolicy.

Arbetet med kontinuitetsplanering bör inledas med att identifiera de områden som behöver skyddas. Detta inkluderar att identifiera verksamhetens mest kritiska processer och de produkter/tjänster dessa levererar och som måste skyddas. I Core infrastrukturen ska det finnas en välplanerad och strategisk metod som involverar skydd av kritiska processer, nätverk, datorer och lokaler. Hur kontinuitetsplanering sammanfogar detta är omlokalisering av kontor, redundanta datorhallar, dubblerade nätverk osv.

En förutsättning för att ta fram och dokumentera en kontinuitetsplan är att man har genomfört en riskanalys. Denna har som syfte att identifiera tänkbara händelser som är relaterade till såväl verksamhetens infrastruktur som dess affärsverksamhet och vilka som kan orsaka avbrott i verksamheten. Dessa händelser bör sedan bedömas utifrån ett riskperspektiv där sannolikheten och konsekvensen av ett avbrott, inklusive omfattning och tid för att återställa, analyseras. **[10] [13]**



[1] Se ordlistan

## 1.1 MÅL

Målet med problemställningen är att ta fram en kontinuitetsplan[1] och därefter anvisningar om hur planen ska uppnås för IS/IT-avdelningen på Saab Training Systems AB. Målet med detta examensarbete är att uppnå nya gränser för att förhindra avbrott i verksamheten och att skydda kritiska processer i verksamheten samt minimera fel i informationssystemen eller katastrofer och att åstadkomma rimlig tid för återstart av systemen. I uppdraget ingår även att ta reda på vilken information som är viktig och vilka hot det finns gentemot denna, samt att finna och identifiera de kritiska tillgångar som är önskvärda att skydda. En kontinuitetsplan på Saab Training Systems AB ska utarbetas som en version 1.0.

## 1.2 MÅLGRUPP

Denna uppsats riktar sig till högskolestudenter och intressenter med en förståelse av ämnet som berör kontinuitetsplanering. Uppsatsen riktar sig även till företagare som har som mål att implementera eller alternativt uppdatera sin kontinuitetsplan.

## 1.3 SAAB TRAINING SYSTEM – HUSKVARNA

Uppdraget för examensarbetet vid Jönköping Tekniska Högskola med företaget Saab Training Systems AB har varit att forma en utgåva av en kontinuitetsplan. Denna kontinuitetsplan innehåller omfattande åtgärder om vad som ska följas upp vid en incident.

## 1.4 FÖRETAGSBESKRIVNING

Saab Training Systems AB är ett världsledande högteknologiskt företag som grundades 1960 i Jönköping. Senare, i slutet av 60-talet flyttade verksamheten till Huskvarna.

Saab Training Systems AB har fokuserat sig inom försvar, flyg och rymdteknik. På Saab Training Systems AB arbetar cirka 13000 anställda och har en omsättning som ligger runt 16 miljarder kronor, varav cirka 65% exporteras.



[1] Se ordlistan

Saab Training Systems AB har sitt huvudkontor i Huskvarna med cirka 400 anställda. Av dessa är cirka 80% ingenjörer inom olika områden. Saab Training Systems har dotterbolag i USA, England, Frankrike, Finland, Tyskland, Holland och Norge

## 1.5 IS/IT

IS/IT avdelningen står för kärnan i infrastrukturen och bygger på ett antal fysiska och virtuella servrar. Datorutrustningen och dess nätverk är lokaliserade till två datorhallar, där det ena systemet ska replikera den andra, samt se till att systemet fungerar som det ska.

IS/IT-avdelningen hanterar sin backup veckovis ett systematiskt och kontinuerligt sätt. Fördelen med att företaget gör denna typ av backup med veckodagarna involverade innebär att företaget åtminstone kommer ha en veckas sparad data ifall en incident skulle uppstå. Nackdelen är om en brand skulle uppstå, kan i princip ingen av de anställda arbeta.

Rutiner för hur backup ska hanteras följs upp varje morgon. Däremot saknar IS/IT-avdelningen för närvarande en återställningsplan. Backupbanden återanvänds och policys finns för detta på Saab Training System.

Det finns detaljerade beskrivningar av vad som ska sparas på banden samt hur länge detta ska vara lagrat innan det får överskrivas av nytt material. IS/IT har valt backupmedier som diskbackup som första steg och sen föra över dessa på band. Detta kan ses som ett långsamt alternativ men fördelen med detta är att man får en snabbare backup.

IS/IT har valt att köra med månadsbackup som lagras i ett antal månader och denna backup får inte skrivas över. Först efter en specifik månad kan man skriva över informationen.

Säkerheten är hög. Det existerar system som skickar varning via SMS eller e-post, och man har klassat in olika system i prioritetsordning. System som klassas som prioritet 1 larmar dygnet runt. Skulle det hända något med dessa prioritetssystem vidtas åtgärder omedelbart. Det finns idag inga krav om detta för IS/IT.



[1] Se ordlistan

## 1.6 AVGRÄNSNINGAR

Avgränsningar kommer att göras på Saab Training System i Huskvarna inom områden som tilldelning av övningar som är rekommenderade att göra vid en konstruktion av kontinuitetsplan. Dessutom ska avgränsningar göras om hur konfigurationer ska sättas upp i hårdvara för att skyddet ska bli så effektivt som möjligt, vilket kommer att göras av företaget.

I kontinuitetsplanen kommer ord som ska väljas i första hand. Ord som bör, kan, kanske eller rekommenderat kommer att undvikas på grund av tonvalet av tveksamhet. Ordet *ska* är mer bestämt än de övriga orden och är ett mer bestämt krav om att man ska utföra något. Om företaget Saab Training System inte kan utföra de åtgärder som har skrivits i kontinuitetsplanen, ska man se över om det är en brist. Kontinuitetsplanen kommer inte att vara bifogad i denna examensrapport, då innehållet av denna ej får distribueras utanför Saab Training Systems AB.

Då en kontinuitetsplan kan bestå av små som stora katastrofer, har uppdragsgivaren valt att begränsa kontinuitetsplanen till att innefatta datorutrustningen hos Saab Training Systems, samt begränsa omfattningen till:

- Säkerhetskopiering & återläsning av data
- Prioritering av system efter avbrott
- Handlingsplan vid strömavbrott
- Brandskydd i datorhall
- Skydd mot virus
- Intrång i datorsystem
- Brandvägg
- Installation och konfiguration av datorsystem



[1] Se ordlistan

# 2 TEORETISK BAKGRUND

Det finns många olika incidenter som kan skada en organisation. Det kan exempelvis bestå av hårdvarufel, olika typer av oväder, bränder, fel som uppstår av människan etc. Detta går att motverka med hjälp av en kontinuitetsplan som verktyg där man noggrant följer upp med övningar, om det är möjligt att motverka en katastrof. Om det inte gör det är det rekommenderat att se över sin kontinuitsplan ytterligare.

Organisationer blir allt mer beroende av IT, delvis för att kunna följa upp sina affärsmål och delvis för att kunna nå affärsverksamhetens behov. Den växandet tillförliten till IT leder till allt större krav på kvalitativa IT-tjänster. Med kvalitet så refererar man till tjänster som passar in på organisationens behov och användarnas krav.

Begreppet informationssäkerhet innefattar många beståndsdelar såsom tillgänglighet, riktighet och sekretess.

- Tillgänglighet omfattar att endast behöriga användare har tillgång till vissa resurser.
- Med sekeretess menas att bara behöriga ska komma åt den givna informationen.
- Riktighet täcker områden såsom att information inte ändras utan tillsyn av en användare som har behörighet till detta.

Uppdelningen av säkerheten och ansvarsfördelningen i olika organisationer kan se olika ut. Variationen kan påverkas av ledningens engagemang. Allra vanligast är fel, misstag samt oavsiktliga underlåtelser som förorskas av brister i organisationen som exempelvis ansvarsfördelning, kompetens och kunskapsbrist. **[5] [7]**

## 2.1 RISKANALYS

I ett kontinuitetsplanearbete fokuserar man sig allt för mycket på själva planeringen som är relaterad till infrastrukturen. Till exempel;

- Vad händer om nätverket inte är tillgängligt längre?
- Vad händer om byggnaden brinner ner?

Det finns betydligt värre saker man borde ställa frågor emot. Exempelvis kan det vara

- Vad händer om en leverantör inte kan leverera?
- Vilka är de kritiska produkter och tjänster som kan tänkas påverka ett huvudkontor och de anställda om dessa blir otillgängliga?

Det finns många organisationer som har kundomsorg som framgång. Kontinuitetsplanering bör vara en del av de strategiska målen för ett lyckat kundfokuserat företag.

# 3 IT INFRASTRUCTURE LIBRARY

Under det senaste årtiondet så har IT-utvecklingen haft en stor påverkan på företagens affärsprocesser. Introduktionen av PC, LAN, klient/server-teknologin och Internet har möjliggjort att organisationer har kunnat ta fram produkter väsentligt snabbare än tidigare. Denna utveckling har ledsagat en övergång från den traditionella industriella till en mer IT-baserad uppbyggnad. Under den IT-baserade uppbyggnaden så har alla företagsprocesser blivit snabbare och mer dynamiska. Traditionella hierarkiska verksamheter har oftast haft det svårt att svara på den snabba förändringsmarknaden, vilket har lett till en trend som rör sig i riktningen mot mindre hierarkiska och allt fler flexibla företag. Likadan betoning med verksamheter har skiftat från vertikala funktioner eller avdelningar till horisontella processer som rör sig inom organisationen och som styr anseendet, är påtagligen stigande.

ITIL ger en detaljerad guide som involverar processbeskrivning av flera viktiga IT-övningar med omfattande checklistor, uppgifter och processer med ansvarsområden som kan bli skräddarsydda till vilken IT-verksamhet som helst. Detta har möjliggjorts genom att definiera delmomenten som processer, vilka täcker stora delar av IT-tjänstens handhavande. **[3]**

Slutsatsen är att man kan förändra existerande rutiner, processer och sina anställdas sätt att hantera sina dagliga arbetsuppgifter genom att säkerställa att verksamheten får ett godtyckligt IT-stöd **[2]**

Kontinuitetsplanen bör säkerställa att företagsprocesser fungerar på ett tillfredställande sätt, dvs processerna bör omarbetas om kontinuitetsplanen så kräver. Detta kan innefatta följande kvalitetsprocesser såsom, (vilka var och en behandlas i följande underparagrafer);

- SERVICES AND QUALITY
- SERVICE LEVEL MANAGEMENT
- SERVICE CATALOGUE
- INCIDENT MANAGEMENT
- PROBLEM MANAGEMENT
- CONFIGURATION MANAGEMENT
- CHANGE MANAGEMENT
- RELEASE MANAGEMENT
- FINANCIAL MANAGEMENT FOR IT SERVICES
- CAPACITY MANAGEMENT
- AVAILABILITY MANAGEMENT
- SECURITY MANAGEMENT
- IT SERVICE CONTINUITY MANAGEMENT

Figuren nedan visar en förenklad modell över hur en förbättringsprocess kan se ut,

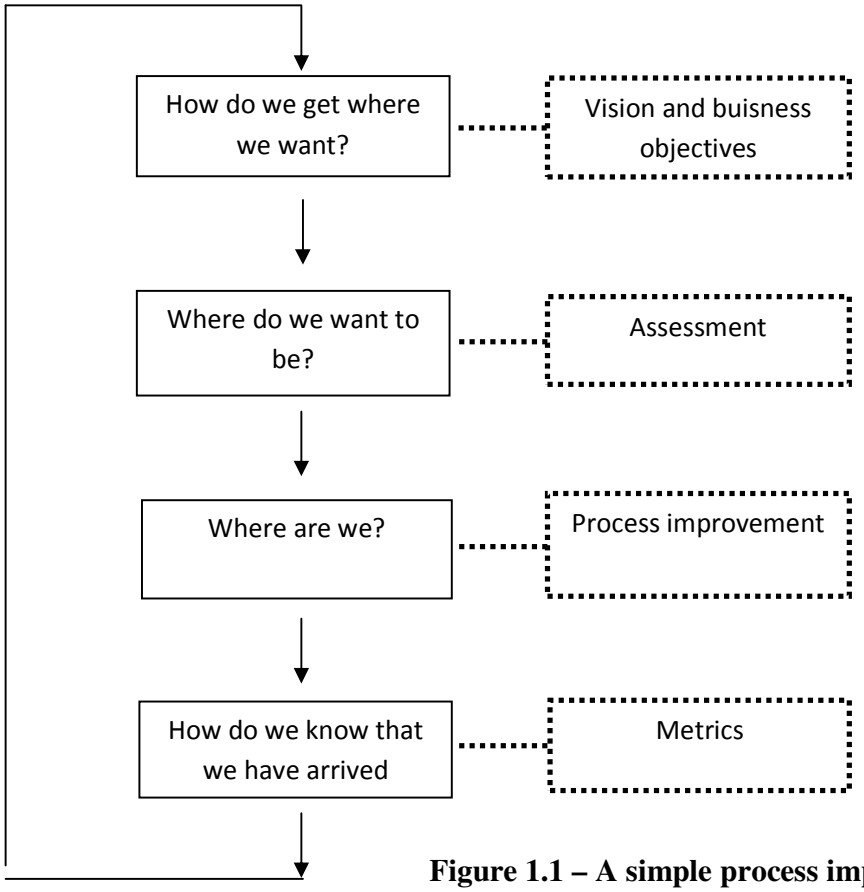


**Figure 1.1 – A simple process improvement model**.

## 3.1 SERVICES AND QUALITY

Verksamheter är ofta beroende av sitt IT-stöd men förutom att tillhandahålla kvalitativ support krävs även möjlighet att presentera och ta fram nya tjänster som kan implementeras i organisationen. Leverantörer av IT-tjänster kan inte längre ha råd med vidareutveckling av deras egen teknologi och deras interna organisation. De måste nu istället betrakta element som kvalitativa tjänster som kan framhållas och fokuseras på deras kundrelation. **[3]**

## 3.2 SERVICE LEVEL MANAGEMENT

Service Level Management är processen för att kunna förhandla, definiera, värdera, verkställa och förbättra kvaliteten av IT-tjänster inom en rimlig summa. Detta måste kunna äga rum med en snabb förändringstakt baserat på affärsbehov och snabba teknologiförändringar. Service Level Management har som målsättning att finna den rätta balansen mellan kvalité och kostnader av IT-tjänster. Det är viktigt att både förhandlaren och kunden förstår att en tjänst upprätthålls. Service Level Management inkluderar design, samtyckning och underhållning av följande:

- Service Level Agreements (SLA's)
- Operational Level Agreements (OLA's)
- Underpinning Contracts (UC's)
- Service Quality Plans

**[3]**

## 3.3 SERVICE CATALOGUE

Syftet med denna process är att åstadkomma tydliga överenskommelser med kunden om vad IT-tjänsterna ska innehålla. Processen ger ett strukturerat sätt för kund och tjänsteleverantör att diskutera och mäta kvaliteten i tjänsterna. Tjänsterna presenteras för kunden i en tjänsteportfölj (Service Catalog). När kunden köper en tjänst beskrivs hur tjänsten ska levereras i dokumentet "Service Level Requirements". Detta dokument beskriver kundens generella krav. Detaljerade överenskommelser om t.ex. antal användare och tillgänglighet beskrivs i dokumentet "Service Level Agreement" (SLA).

- Förbättrad kundrelation och kundnöjdhet
- Tydligare överenskommelser och åtaganden som sätter rätt förväntansnivå hos kunden genom leverans av IT-tjänster med Service Level Requirements
- IT fokuserar på det som verksamheten efterfrågar och levererar tjänster där kunden kan balansera mellan kvalitet (QoS) och kostnad
- Uppföljning av servicenivåer, vilket möjliggör förstärkning inom svaga leveransområden
- Ökad kontroll av tjänster och dess delkomponenter ger på lång sikt reducerade kostnader för resurskontroll

**[3]**

## 3.4 INCIDENT MANAGEMENT

Incident management är en reaktiv uppgift, dvs. minska eller utesluta effekterna av aktiva eller potentiella störningar inom IT-verksamheten, och därigenom säkerställa att användarna kan återgå till verksamheten så fort som möjligt. Detta åstadkommes genom att;

- registrera störningen
- klassificera störningen
- utse lämplig person, (specialist) för åtgärd,
- bevaka framsteg av åtgärd(erna)
- när störningen är eliminerad stängs uppgiften

Eftersom detta kräver nära kontakt med användaren, så sker informationsutbytet mellan användare och IT-avdelning vanligtvis via en serviceenhet inom IT-avdelningen, (service desk). ”Incident Management” är väsentlig för de övriga processerna inom ITIL eftersom den förmedlar värdefull information om infrastrukturella problem och fel.

- Reducera verksamhetspåverkan genom snabba lösningar, såsom vilket ökar effektiviteten
- Förebyggande identifiering av fördelaktiga systemförbättrande åtgärder och regeländringar
- Förbättrad övervakning som medger korrekt uppföljning mot SLA
- Förbättrad kontroll och styrning av levererad kvalitet
- Bättre utnyttjande av personal och därigenom höjd effektivitet
- Reducera borttappad eller felaktig information om anmälda incidenter och kundförfrågningar
- Ökad kontroll och bättre kvalitet på konfigurationsinformation
- Ökad användare- och kundtillfredsställelse

**[3]**

## 3.5 PROBLEM MANAGEMENT

Som tidigare nämnts så aktiveras ”Incident Management” om en störning inom IT-verksamheten inträffar och ”Incident Management” upphör då störningen åtgärdats. Detta betyder inte att åtgärden har åtgärdat grundproblemet utan problemet kan dyka upp igen.

Problem management undersöker infrastrukturen och all tillgänglig information, inklusive störningsdatabasen, för att identifiera roten av aktuella/potentiella fel/störningar. Dessa undersökningar behövs för att infrastrukturen kan vara komplex och länkarna mellan störningarna är inte alltid tydliga. Till exempel, ett flertal fel kan vara orsak till ett problem, och flera problem kan vara associerade till samma fel. Som första steg bör man identifiera orsaken till en störning. När väl bakomliggande orsak har identifierats och en acceptabel lösning tagits fram så kan problemet identifieras som ett känt fel. Därefter när väl en varaktig lösning tagits fram så kan en begäran om ändring, Request for change, utfärdas för att eliminera det kända felet. Även efter detta förfarande, så fortsätter ”Problem Management” att kontinuerligt spåra kända fel i infrastrukturen. Därför lagras informationen över alla identifierade fel, deras symptom och tillgängliga lösningar. **[3]**

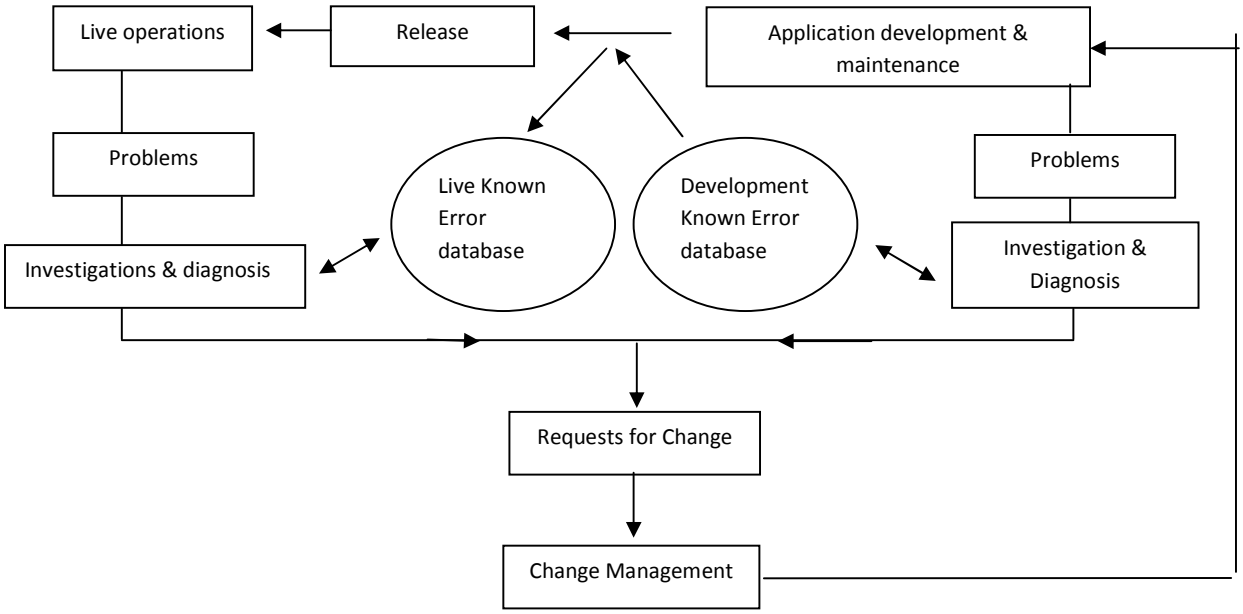


**Figure 2.2 – Errors in the Live and Development Life-cycles**

## 3.6 CONFIGURATION MANAGEMENT

Varje IT-organisation har information om dess infrastruktur. Sannolikheten för att denna information finns tillgänglig äger i regel rum efter att ett större projekt genomförts. Konsten att bevara denna information består snarast i att hålla den kontinuerligt uppdaterad. Målet med ”Configuration Management” är att säkerställa tillförlitliga och uppdaterade detaljer om infrastrukturen. Viktigast är att inte bara upprätthålla information om specifika detaljer i infrastrukturen, utan snarast hur detaljerna eller elementen inom infrastrukturen relaterar till varandra.

Konfigurationsstyrning kontrollerar om ändringar i infrastrukturen har lagrats på ett riktigt sätt, inklusive sambandet mellan alla element, samt kontrollerar status på komponenterna för att säkerställa att de har en riktig bild av versionerna av elementen som används inom infrastrukturen.

Exempel på andra komponenter i infrastrukturen som kan dokumenteras är: hårdvara, mjukvara (applikationer), nätverkskomponenter, servrar, dokumentation och processbeskrivningar. Även versionskontroll av källkod för mjukvara ingår i denna process.

- Tillhandahåller uppdaterad information om våra Configuration Items (CI's) och deras dokumentation.
- Lagrar historisk information om infrastrukturen
- Ger kontroll på värdefulla CI's
- Upprätthålla juridiska skyldigheter
- Hjälper till vid ekonomisk och inköpsplanering
- Synliggöra programvaruförändringar
- Hjälper och förbättrar Release-hantering
- Möjliggör påverkansanalys och förändringsplanering på ett säkert och optimalt sätt
- Förbättrar säkerheten genom att tillhandahålla versionsinformation om våra CI's
- Hjälper till att eliminera otillåten programvara
- Ger kontroll och information om affärsmässiga effekter av incidenter, problem och förändringar **[3]**

## 3.7 CHANGE MANAGEMENT

Den snabba utvecklingen inom IT-teknologin och affärsmarknaden innebär att förändringar är en självklarhet. Affärsverksamheten behöver ständigt förändras för att förbättra servicen och minska dess kostnader och man behöver IT-stödet för att hinna vara med i den kontinuerliga förändringsprocessen.

Erfarenhet visar att IT-störningar som påverkar affärsverksamheten ofta är relaterade till förändringar. Orsaken till dessa störningar är flera, de kan vara orsakade av;

- slarv
- brist på resurser
- otillräckliga förberedelser
- otillräckliga analyser
- otillräckliga tester **[3]**

Om störningar som är relaterade till att ändringar inte tas om hand på ett kontrollerat sätt så kan IT-leverantören och följaktligen företaget i fråga få eskalerande problem. Antalet störningar kommer att öka där varje störning kan förorsaka en brandutryckning vilket oftast leder till att nya störningar genereras. Den dagliga planeringen av förändringar underskattar oftast mängden av arbetsinsatser som krävs varvid förändringar i allmänhet sköts på ett dåligt sätt. **[3]**

”Change Management” syftar till att hantera förändringsprocesser och därmed begränsa uppkomsten av fel och störningar som är orsakade av förändringar. **[3]**

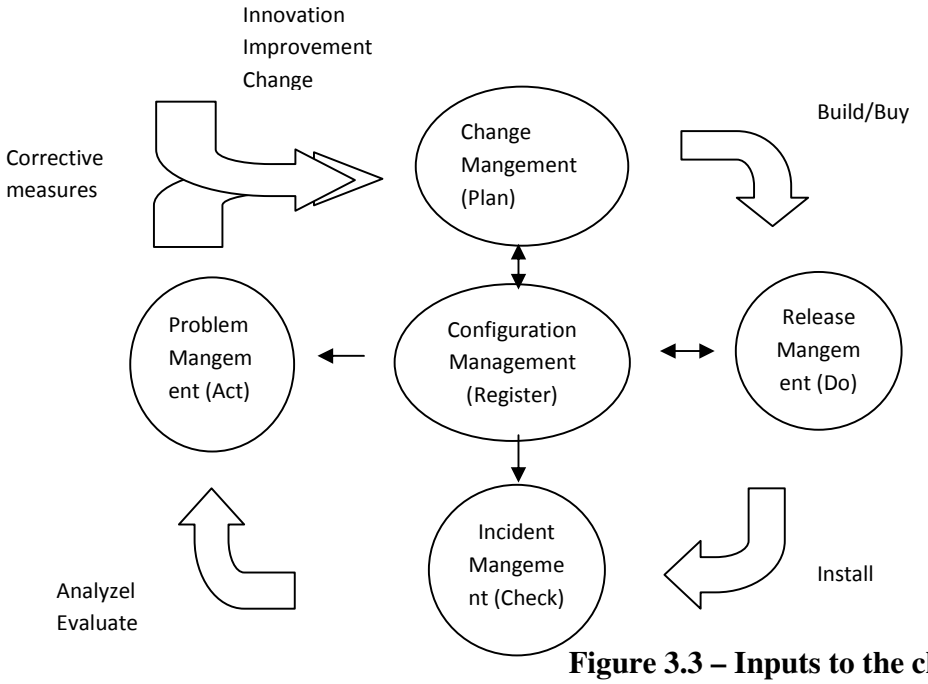


**Figure 3.3 – Inputs to the change process**

Det är inte ovanligt att problem uppstår när ändringar ska göras i IT-infrastrukturen. Därför behövs en process, Change Management, för att begränsa ”skadorna” som uppstår när ändringar ska genomföras. Alla ändringsförslag (Request for Change, RFC) skickas till denna process som antingen godkänner eller förkastar förslaget. Change Manager kan ensam godkänna enklare ändringsförslag. Mer kvalificerade förslag måste godkännas av Change Advisory Board (CAB). En rutin för att införa ”nödrättningar” måste finnas för de fall när en ändring måste införas omedelbart, t.ex. p.g.a. lagstiftning eller stora intäktsbortfall, (produktionsstopp).

Processen samlar sedan ett eller flera ändringsförslag till en ny version som implementeras av processen Release Management. När ändringen är implementerad ska Change Management följa upp den och verifiera att målet med ändringen uppfylldes. Först då kan också berörda ändringsförslag stängas.

Exempel på vem som kan initiera en RFC: processen Problem Management, kunder, utvecklingsprojekt samt anställda på IT-avdelningen (tjänsteleverantören).

- Förbättrad syn på IT genom förbättrad servicekvalité och professionellt genomförande
- Förbättrad risk och kostnadshantering för föreslagna förändringar
- Färre förändringar som kräver återställande och bättre genomförande av eventuella återställanden
- Ökad användarproduktivitet genom minskad förekomst av problem vid förändringar i egna infrastrukturen
- Ökad förmåga att genomföra mer frekventa förändringar utan att få en instabil IT-miljö

**[3]**

## 3.8 RELEASE MANAGEMENT

Allt eftersom organisationer blir mer och mer beroende av IT-processer så blir även övervakningen och skydd av dessa processer mer viktig. Allt eftersom takten av förändringar fortsätter att öka uppstår även ett växande behov av att kontrollera förändringsprocessen.

Release Management syftar till att bibehålla en hög kvalitet i produktionsmiljön vid installation av nya versioner. Processen arbetar med att planera, koordinera och genomföra installation av mjukvara och hårdvara. Processen startar när Change Management initierar en ändring bestående av en eller flera ändringsförslag (RFC). Processen genererar en mängd fördelar såsom; **[3]**

- Ökad framgång vid utrullning av hårdvara och mjukvara, därigenom förbättrad servicekvalitet på levererade tjänster
- Optimerar antalet driftstörningar på grund av förändringar i infrastrukturen
- Försäkran om att hårdvara och programvara som används uppnår känd kvalitet
- Stabilare produktionsmiljö
- Minskat antal incidenter
- Planerade förändringar
- Minskade kostnader för licens- och serviceavtal som inte nyttjas
- Minskar sannolikheten till olaglig programvara
- Lättare identifiering av otillåten och fel version av programvara

## 3.9 FINANCIAL MANAGEMENT FOR IT SERVICES

Financial Management handlar om att hantera pris och prestanda för IT-tjänsterna. Det ger medvetenhet om kostnader och gör att förändringar kan diskuteras i termer av kostnader och nivå av kvalitet. Exempel: vi ska dra ner IT-kostnaderna med 10%. Vad innebär det för kvaliteten på de IT-tjänster vi levererar? **[3]**

- Tydliggöra de egentliga IT-kostnaderna för tjänster genom god kostnadsuppföljning
- Effektivare nyttjande av IT-resurser genom att t.ex. införa högre taxor vid nyttjandetoppar
- Ökad kostnadsmedvetenhet inom organisationen genom bättre kostnadskontroll och direkt koppling mellan nyttjande av tjänst & kostnad
- Medger mer affärsmässiga IT-beslut och styrning av IT-organisationen som en affärsenhet

## 3.10 CAPACITY MANAGEMENT

Capacity Management innebär att planera, skala och kontrollera att kapaciteten för de levererade tjänsterna är tillräckliga. Huvudfaktorerna är tillräckliga server- och nätverksresurser, men även personella resurser ska vara tillräckliga, t.ex. att anställa fler personer till service-desk för att möta behovet av support. Fördelar med processen är följande;

- Skjuter upp inköp
- Kapacitet i takt med verksamhetsbehov
- Minskade kostnader genom planerade inköp och bättre nyttjande
- Minskar riskerna för befintliga program genom resurshantering och service hantering
- Förebygga felaktiga applikationsförvärv
- Minskat antal förändringar på grund av kapacitetsproblem **[3]**

## 3.11 AVAILABILITY MANAGEMENT

Målet med denna process är att säkra att levererade IT-tjänster är tillgängliga för användaren dygnet runt, 7 dagar i veckan och 52 veckor per år minus en viss överenskommen tid för oförutsedda störningar. Ett exempel är en e-handelssajt som förväntas vara uppe praktiskt taget jämt, där kanske tillgänglighetsgraden (hur många procent tjänsten är tillgänglig per tidsenhet)

kan vara 99,99%. Det innebär att e-handelssajten inte får vara nere mer än 4,5 minuter per månad. Processen medför bland annat följande fördelar;

- Säkerställer att tillgänglighetskraven på levererade tjänster uppfylls
- Kontinuerlig övervakning och förbättring av tillgänglighet
- Minskad tid då tjänster inte är tillgängliga motiverar givet tjänstepris
- Säkerställer att nya tjänster och produkter följer tillgänglighetsstandard överenskommen med kund

**[3]**

### 3.12 SECURITY MANAGEMENT

Security management omfattar bland annat följande;

- Upprätthålla en bra balans mellan säkerhet och tillgänglighet
- Öka verksamhetsnyttan genom att säkerställa att rätt och komplett information tillhandahålls när den erfordras
- Säkerställa att produkter och tjänster är tillgängliga för verksamheten

**[3]**

### 3.13 IT SERVICE CONTINUITY MANAGEMENT

Continuity Management hanterar planering och förberedelser för att kunna återställa överenskommen nivå för IT-tjänsterna även om ett plötsligt avbrott av större karaktär skulle inträffa. I denna process ingår även att utföra åtgärder för att förebygga dessa avbrott.

- Säkerställer återupprättande av tjänster efter inträffad katastrof
- Minimerar tid då tjänster inte är tillgängliga och ger bättre kontinuitet av tjänst till användare
- Minimerar avbrott i affärsmässiga aktiviteter

**[3]**

# 4 BRANDVÄGG

En brandvägg är en mekanism som förstärker behörigheten inom ett nätverk. Brandväggar är utvecklade för att hålla inkräktare utanför nätverket. Några brandväggar tillåter endast e-post meddelande, för att skydda nätverket mot alla tänkbara attacker och inte bara attacker som berör e-post tjänsterna. Andra brandväggar tillhandhåller mindre strikta skyddsåtgärder och blockerar endast de tjänster som är kända som problem.

Användandet av en brandvägg behöver inte inskränka på nätverks tjänster. Man kan använda en brandvägg för att skydda en enskild dator och inte regelbundet skydda tillgången till Internet. En brandvägg kan bestå av en fysisk enhet eller mjukvara. När man vill utveckla en fysisk brandvägg, så kan man använda en router som ansluter till det interna nätverket som vidarebefordrar informationen till Internet. Ett liknande tillvägagångssätt kan användas om man utvecklar en mjukvarubaserad brandvägg, där man kan använda sig av en Proxyserver. En Proxyserver har direkt tillgång till Internet och behandlar begäran från andra datorer på nätverket. **[4]**

## 4.1 FUNKTIONALITETEN HOS EN BRANDVÄGG

Oavsett vilken typ av brandvägg man använder så har alla brandväggar några basfunktioner, såsom autenticiering användare, säkra nätverket från nätverksskanningar, framställa NAT, samt filtreringstjänster. **[4]**

# 5 INTRUSION DETECTION SYSTEM

En rekommenderad åtgärd är att skaffa ett Intrusion Detection System[3], beroende på modell och hur den är konfigurerad kan den själv utföra motåtgärder. Dessa motåtgärder kan vara logga, larma eller utföra motattacker. En IDS ska logga onormala aktiviteter men även vanlig normaltrafik ska loggas. Loggningen är ett bra verktyg för att utföra en analys, så problemet är bara hur mycket av trafiken som ska loggas. Men om förutsättningarna finns så ska mycket som möjligt loggas.

Larm kan konfigureras på flera olika sätt. Ett bra exempel kan vara SMS eller personsökare vid akuta fall. För normala fall kan det räcka med att IDS larmar via ljud till där driftcentralen är placerad. Nackdelen är att en IDS ibland genererar för många falskalarm. Det är väldigt viktigt att inte hamna i en situation där användarna ignorerar larmen, vilket kan medföra att hackern kan utföra det han/hon vill.

Automatiserade motåtgärder rekommenderas inte även om det kan kännas frestande efter att ha blivit utsatt av en attack. Detta är på grund av att den information som avsändaren använder inte stämmer överens med den verkliga avsändaren. Det finns goda skäl att avsändaren kommer från en annan ursprungsplats för att kunna kamouflera det riktiga ursprunget. Om det skulle stämma överens är det högst olämpligt med en mottack. Förutom att det är olämpligt och kanske utgör en viss osäkerhet är det sannolikt olagligt att utföra dessa attacker. Det bästa alternativet är att informera administratören om vad som pågår. **[9] [14]**

## 5.1 INSTALLATION UTANFÖR BRANDVÄGGEN

Om man väljer att placera ett IDS utanför sin brandvägg kommer attacker att detekteras på ett tidigt stadium. Om en attack skulle uppstå, kommer den att detekteras, på grund av den brandväggspolicy som existerar. Även om man nu anser att sådant som inte berör systemet, inte behöver skyddas, så kan det i alla fall ha en stor betydelse för generell statistik, hotbildsbedömning och för att bekräfta att brandväggen fungerar. Man kan konfigurera sin IDS att endast logga intrångsaktiviteter och ignorera larm för att reducera att *”björnen kommer”-syndromet* uppstår. Om man har byggt upp sitt IDS-system utanför brandväggen kan man oftast



[4]Se ordlistan

avgöra vilken IP-adress attacken härstammar från. Dessvärre brukar denna information vara förfalskad via IPSpoof eller liknande. Denna typ av installation medger inte loggning av interna adresser om NAT[4]. **[12]**

## 5.2 INSTALLATION INNANFÖR BRANDVÄGGEN

Om man väljer att placera ett IDS innanför brandväggen kommer endast hot som riktar sig till de verkligt känsliga systemen att kunna granskas. Om larm förekommer här är det viktigt att vidare åtgärder tas i bruk med en gång eftersom brandväggen då kan ha blivit defekt. Den möjliga attacken är då att hackern sitter innanför företagets väggar med en otillåten modemuppkoppling. Fördelen med detta är att man kan se vem som bryter mot säkerhetspolicyn. Externa adresser som eskalerats från en NAT kan inte göra denna loggning och därför går man miste om denna information om attacken härstammar från utsidan. **[12]**

## 5.3 LOGGANALYS

En logganalys som finns i ett IDS kräver mer av analytikerna än vad traditionella loggfiler normalt gör. Nackdelen med loggfilerna är att de fort blir omfattande och svåra att överblicka. Fördelen är att ett IDS utnyttjar loggarna för att se ett större sammanhang än vad en människa kan göra. Ett väl konfigurerat IDS kan detektera nätverksskanningar under långa tidsperioder. En attack av sådan typ skulle inte det mänskliga ögat se eftersom det normalt rör sig om ett par anrop per dag från en viss IP-adress, vilket man normalt inte reflekterar över.



[4]Se ordlistan

# 6 ANTI-VIRUS

Datavirus har alltid varit ett hot och är ett stortproblem för alla datoranvändare. De tidigare virusarna hade primära mål att infektera via disketter. Idag är det mer komplext då det kan sprida sig mobilt, vid användning av nätverksmiljöer och via Internet. Virus kan idag sprida sig runt vårt jordklot långt innan man ens har upptäckt och gett en diagnos till viruset. Antivirusmjukvara definieras oftast i tre huvudkategorier:

- Generic software
- Virus-specific software
- Hybrid software

”Generic software” studerar miljön i ett infekterat objekt som exempelvis en fil och letar efter förändringar i den. Det första som studeras är den totala filstorleken och andra integrerade parametrar, eller så kommer en studie att följa upp den process som ska presentera det karaktäristiska beteendet av ett virus.

”Virus-specific software” kontrollerar objekt mot en välkänd databas som har de olika värdena som ett virus kan klassas i. Denna mjukvara kan också känna igen viruskoden från det infekterade objektet eller ge den en ny rekommenderad plats. Virusspecifik mjukvara kan påverka ”*scanning on demand*” eller så kan skanningen göras transparent, dvs samtidigt när användaren har tillgång till dem.

Moderna ”Hybrid Software” är kompatibel med både generella och specifika tekniker. Sådan mjukvara används ofta teknik som heuristik analyser, där virusbeteendet övervakas på ett säkert och kontrollerat sätt.
**[6] [7]**

Ett virus är ett program som förökar sig eller replikerar sig av genom bifoga sig självt till ett annat program, som blir då infekterad, (se exempel i nedanstående tabell). Virus kan:

- Minimera funktionerna hos e-postservrar
- Korrumpera system och filer
- Stoppa operativsystemet
- Stoppa affärssystem

| Virus Effect | How It Is Caused |
|---|---|
| Attach to exacutable program | • Modify file directory<br>• Write to executable program file |
| Attach to data or control file | • Modify directory Rewrite data<br>• Append to data |
| Remain in memory | • Intercept interrupt by modifying interrupt handler address table<br>• Load self in nontransient memory area |
| Infect disks | • Intercept operating system call<br>• Modify system file<br>• Modify ordinary executable program |
| Conceal self | • Intercept system calls that would reveal self and falsify result<br>• Classify self as hidden file |
| Spread infection | • Infect boot sector<br>• Infect systems program<br>• Infect ordinary program<br>• Infect data ordinary program reads to control its execution |
| Prevent deactivation | • Activate before deactivating program and block deactivation<br>• Store copy to reinfect deactivation |

**Figure 4.4 – Virus effects and causes**

## 6.1 VIRUSKATEGORIER

Alla är vi medvetna om att virus är en skadlig kod som kan skada din dator. Förvirringen kommer först när man ska välja ett bra antivirus program. Antivirusprogram detekterar möjlig tillvaro av virus i din dator med att följa ett specifikt mönster som härstammar från de olika viruskategorierna. Nedan beskrivs tre olika typer av viruskategorier:

- Scriptvirus
- Mimetic-virus
- Worms

Scriptvirus har ökat påtagligt i Windows-miljön. HTML-script kan innehålla VBScript eller JavaScript-programmering. VBScript är särskilt framtagna av den anledning som framstår alla in/output som existerar, motsatt till en säkrare JavaScript.

Mimetic-virus är en intressant klass av virus. Mimetic-virus består inte av en exekveringskod, utan är betydligt intelligentare än så. Mottagare är ofta inte misstänksam, då det kan röra sig om ett skämt som de anställda skickar vidare runt i organisationen.

Worms är mer riskabla att bli utsatt för, än de övriga viruskategorierna, som ofta är förhärskande på Internet. Worms är en självreplikerade malware som snabbt sprider genom sig nätverk och de olika delsystem som finns. **[7]**

Nya viruskategorier hämmar frekvent, och det antivirusprogram som är installerad på din dator är endast effektiv om man har de senaste definitionsfilerna till antivirusprogrammet. Dessa filer är vanligast att hämta hem från Internet **[6] [4]**

## 6.2 INSTALLATION AV ANTI-VIRUS PROGRAM

Vid en installation av ett nytt Anti-virusprogram på din dator, kan det förekomma några bieffekter.

Virusskyddet kan ibland slöa ner system. Detta är mer sant för äldre maskiner som har ett begränsat minne, eller andra programfunktioner som motverkar skanning av filerna. För att motverka detta kan man stänga av funktionen autoprotect.

På äldre datorer bör man överväga att stänga av alla autoprotect-tillgångar, särskilt sådana som kör igång automatiskt så fort datorn startas om, eller som skannar igenom alla e-post med bifogat material. För att vara på den säkra sidan, att datorn kommer att fungera efteråt, bör man ha valt att köra igång autoprotect igen. Man bör även komma ihåg att om man har stängt av auto-protect så måste man med stor varsamhet köra regelbundna skanningar i systemet och kolla e-post som har bifogat material. **[7]**

# 7 BACKUP

Den mänskliga faktorn är den vanligaste orsaken till att fel uppstår. Dessvärre finns det inga bra motmedel mot dessa misstag, utan vi behöver medvetet vara beredda på att dessa typer av misstag kommer att uppstå. Till exempel:

- När man organiserar filstrukturen på hårddisken och inser att en hel mapp är borta med viktig data.

Lösningen till dessa problem kan vara i form av träning och backupstrategier som användaren själv kan hantera ifall en incident uppstår. Detta skulle spara tid både för användaren och för supportavdelningen då supportavdelningen inte behöver lägga tid på användaren. Dessutom behöver inte användaren belasta supportavdelningen. **[1]**

## 7.1 ÅTERSTÄLLNING

Återställning av data ska komma som en andra åtgärd för att skapa en god infrastruktur. Återställning ska göras på de mest kritiska systemen. Exempelvis:

- Produktdokumentation
- Kundkonton
- Affärskontakter
- Databaser

Denna typ av backup är en försiktighetsåtgärd i det fall hårdvaran skulle sluta att fungera. Återställningen skall i första hand vara utformad för användarnas behov, och vara initierad av användaren själv. Återläsning ska ske snabbt och enkelt. Om det gäller ett företag har man inte råd med långa avbrott eller att kalla på en IT-specialist för att kunna återfå de filer som av misstag raderats. Band som används som backupmedia är opraktiskt i detta sammanhang eftersom de lagrar data sekventiellt. Det kan ta timmar att hitta en enskild fil på ett stort band. **[1] [4]**

När det gäller online-lösningar så kan all data skickas till en off-site. Data kommer att bli krypterad om man väljer att använda sig av Internetteknik. Denna typ av lösning kan vara väldigt eftertraktad eftersom data i dessa fall ligger på ett säkert ställe, även om en brand skulle uppstå och om byggnaden blir totalförstörd så har man all backup på en annan plats. Denna teknik medför några frågeställningar, såsom:

- Kostnad för Internetanslutning
- Kostnad för lagring
- Begränsningar för att skicka ut data

**[4]**

Man kan överväga att skapa Redundant Array of Independent Disc (RAID). Speglingsfunktionen hos RAID kommer att ge ett hårdvaruskydd. Men RAID egenskaperna garanterar inte fel som uppstår av människan. Om man tar bort en fil, så är den borta från systemet på båda diskenheterna. Om man är oroad över fel som uppstår på grund av människan kan man enkelt partitionera disken i tre olika delar, en för operativsystem och två andra med samma storlek, en för användardata och en för backup. Detta är en lågkostnadslösning och man bör då ha i åtanke att datorn kan bli stulen eller förstörd. En lösning på detta är att man köper en extra extern hårddisk som är speglad mot de interna diskarna som man senare tar med dig hem och som man själv ser till att data går att läsa. **[1] [4]**

# 8 RESULTAT

Målet med detta examensarbete är att uppnå nya gränser för att förhindra avbrott i verksamheten och att skydda kritiska processer i verksamheten samt minimera fel i informationssystemen eller katastrofer och att åstadkomma rimlig tid för återstart av systemen

Kontinuitetsplaneringen har satt nya gränser för att förhindra avbrott i verksamheten genom att bidra med ett antal rekommenderade åtgärder. På grund av sekretess kommer inte kontinuitetsplanen att bli bifogat här. Nedanstående rubriker kan lämnas ut, utan att det kränker på företagets policy:

- Säkerhetskopiering & återläsning av data
- Prioritering av system efter ett avbrott
- Skydd mot datavirus
- Handlingsplan – strömavbrott
- Brandskydd i datahallarna
- Intrångsdetektering
- Brandvägg
- Installation & Konfiguration
- Kontaktlistor

Dessa rubriker innefattar även underrubriker och rekommenderade åtgärder beroende på vad det är för incident. Resultatet bygger även på ITIL strukturen, som handlar om processbeskrivningar men även om övningar. Övningarna har varit en avgränsning i detta arbete på grund av tidsbrist. Ett exempel kan vara Incident Management.

”Incident management är en reaktiv uppgift, dvs minska eller utesluta effekterna av aktiva eller potentiella störningar inom IT-verksamheten, och därigenom säkerställa att användarna kan återgå till verksamheten så fort som möjligt.” **[3]**

Analyser har gjorts på IS/IT avdelningen där placeringen av en del utrustning kan diskuteras till både för- och nackdelar. En intressant punkt att diskutera är om en brand skulle uppstå. Hur kommer användarna att kunna arbete vidare när den replikerade utrustning inte kan användas? Ett förslag finns om skarvningar från varje användarens kopplingspunkter. Men ett sånt förslag skulle i praktiken vara orealiserbart. Detta skulle man ha tänkt på innan byggnaden byggdes.

Resultatet i detta examensarbete har varit att utforma ett dokument till IS/IT avdelningen på SAAB Training Systems AB. Detta resultat är skilt från examensarbetet och kommer inte att bifogas.

Examensuppdraget har varit en utmaning då Saab Training System är att betrakta som ett högteknologiskt företag, vilket redan har ett högt säkerhetstänkande. Arbetet har lett till forskning inom all tänkbar information inom de rubriker som är nämnda ovan. Informationen har gett djupare kunskaper om olika åtgärder som bör sättas in mot olika typer av incidenter. Information om tänkbara åtgärder finns tillgängligt på både högskolans bibliotek och Internet där urvalet har varit omfattande.

Efter att ha genomfört detta examensarbete på SAAB Training Systems AB så var jag inställd på alla möjliga förändringar inom datorutrustningen, men insåg även att det inte bara handlar om säkerheten utan även om människors handlingar, vilket sedan kan leda till olika hot.

En slutsats som skulle kunna dras är att en kontinuitetsplan blir aldrig klar. Den måste ständigt uppdateras i den takt som nya hot och attacker dyker upp. Den plan som lämnats till Saab Training Systems bör ge ett gott grundskydd men bör repetitivt och omsorgsfullt granskas.

# 9 ORDLISTA

[1] Kontinuitetsplan – Kontinuitetsplan är ett dokument som ska uppdateras kontinuerligt och se till att säkerhetsåtgärderna är aktuella

[2] ITIL – IT Infrastructure Library, Detaljerad guide som involverar processbeskrivningar för IT avdelningar

[3] IDS – Intrusion Detection System är ett övervakningssystem

[4] NAT –Network Adress Translation eller med ett annat namn nätadressöversättning. Tekniken tillhandahåller Internetanslutning till flera datorer med en eller flera IP-adresser

# 10 REFERENSER


**[1]** Childs D, Dietrich S. *Contingency planning and disaster recovery*. Hoboken NJ, USA: John Wiley & Sons; 2002.

**[2]** Macfarlane I, Rudd C. *The IT service management forum*. Version 2.1.b. Reading, UK: itSMF; 2003.

**[3]** Office of Government Commerce. *Introduction to ITIL.* Norwich, UK: TSO; 2005

**[4]** Mitrovic P. *Handbok i IT-säkerhet*. Sundbyberg: Pagina; 2001.

**[5]** Wallace M, Webber L. *The disaster recovery handbook*. New York, USA: American Management Association; 2001.

**[6]** Sandu R. *Disaster recovery planning*. Cincinnati, USA: Premier Press; 2002.

**[7]** Pfleeger C, Pfleeger S. *Security in computing*. 3rd ed. Upper Saddle River N.J, USA: Prentice Hall; 2003

**[8]** Macfarlane I, Rudd C. *The IT service management forum*. Version 2.1.b. Reading, UK: itSMF; 2003.

**[9]** Mitrovic P. *Handbok i IT-säkerhet*. 4:e upplagan. Sundbyberg: Pagina; 2001.

**[10]** Syrén A. *På egen risk – en handbok om informationssäkerhet*. Stockholm: SIS förlag; 2005

**[12]** Stadskontoret. *Handbok i IT-säkerhet del 2 – policy, ansvar och organisation.* Stockholm: Statskontoret; 1998

**[13]** Maiwald E, Sieglein W. *Datasäkerhet i praktiken*. Sundbyberg : Pagina, 2002

**[14]** Northcutt S, Novak J. *Network intrusion detection*. 3rd ed. Indianapolis, USA: New Riders; 2002.

## 10.1 Figurreferenser

Figure 1.1 – A simple process improvement model. Office of Government Commerce. *Introduction to ITIL.* Norwich, UK: TSO; 2005. p.16

Figure 2.2 – Errors in the Live and Development Life-cycles *Introduction to ITIL.* Norwich, UK: TSO; 2005. p.46

Figure 3.3 – Inputs to the change process Office of Government Commerce. *Introduction to ITIL.* Norwich, UK: TSO; 2005. p.75

Figure 4.4 – Virus effects and causes Pfleeger C, Pfleeger S. *Security in computing*. 3rd ed. Upper Saddle River N.J, USA: Prentice Hall; 2003 p. 122

# 11 SÖKORD

# 12 TACK ORD

Tack till er på företaget SaabTraining System som har hjälpt mig med denna uppsats.

Jonas Florvik – IS/IT Manager
Tommy Englund - Network & System Manager
Patrick Ericsson – Servicedesk Manager
Björn Claesson – System Manager
Ronnie Andersson – Brandchef

Jag vill även passa på att tacka min handledare på JTH och min examinator.

Anna-Karin Carstensen

Inger Palmgren