HANDELSHÖGSKOLAN VID GÖTEBORGS UNIVERSITET
Institutionen för Informatik

IT-SÄKERHET

- en fråga för ledningen

Examensarbete i informatik

Magisteruppsats 20 poäng
VT 1998

Handledare: Kjell Engberg

Författare: Wictoria Sahlén

Abstrakt

Avsikten med denna uppsats var att belysa de faktorer som har betydelse för god IT-säkerhet i ett svenskt företag ur ett företagsledarperspektiv.

I uppsatsen utreds de hot som finns mot företags IT-system, samt vilka skyddslager/lösningar som bör nyttjas för att skydda mot dessa hot. För att nå god IT-säkerhet krävs det av ledningen att den sätter sig in i problematiken gällande hoten som ett företags IT kan ställas inför.

Rapporten leder fram till vilket ansvar och skyldighet som åligger ledningen, samt vilka hot och skydd/lösningar som är aktuella för svenska företag. Nyckelaktiviteter i säkerhetsarbetet är att motivera, informera, utbilda, i viss mån kontrollera, agera och förebygga både tekniskt och på det mänskliga planet. De mjuka faktorerna är nödvändiga att ta hänsyn till i säkerhetsprocessen för att erhålla säker IT.

För att uppnå säker IT krävs det av företagsledningen att den inser att säkerheten behövs, att det kostar, samt att personalen måste vara med i arbetet. De attacker som företagets information kan utsättas för finns det en mängd olika åtgärder/redskap för att förhindra, men utan medarbetarnas medverkan i säkerhetsprocessen är det inte möjligt att uppnå säker IT.

Nyckelord: Informationsteknik, IT-säkerhet, företagsledning, hotbild, skydd

Innehållsförteckning

1. Inledning

1.1 Bakgrund

Dagens samhälle kommer med stor sannolikhet att betecknas informationssamhället i framtida historieböcker. Det finns redan idag de som, liksom framtidsforskaren Tomas Lönn (1996), benämner samtiden för informations- eller kunskapssamhället, eftersom produktionen av kunskap och beroendet av tillgång till information har en huvudroll, samtidigt som integrerade system för datorer och teleteknik blivit allt viktigare.

Företagsklimatet idag är mycket resultatinriktat och verksamheter effektiviseras för att möta de allt strängare kraven från konkurrenter och kunder. Företagen är ofta mycket beroende av snabb tillgänglighet och hög integritet av sin information. Många tidigare manuella rutiner sköts numera av datorer och kräver inte längre mänskliga kontroller eller avvägningar. Avsaknaden av mänskligt omdöme kan vara en säkerhetsrisk, särskilt om effektiviseringen av verksamheten resulterat i att tids- och kostnadsfaktorer pressats och säkerhetskontrollerna i systemen dragits ned. Oftast är det inte förrän efter en incident som säkerhetsaspekten blir aktuell.

Informationssystemen har blivit en essentiell del av många verksamheter. Då ett företag blivit beroende av att dess informationstekniska (informationsteknik kommer i fortsättningen förkortas till IT) system fungerar för att verksamheten skall flyta, ökar systemets värde för företaget. Ju mer beroende verksamheten är av IT-systemet, desto större konsekvenser medför en attack eller annan typ av avbrott.

Svenska företag har till stor del varit förskonade från organiserad IT-brottslighet, i alla fall som kommit allmänheten tillkänna. I en undersökning gjord av Riksrevisionsverket framkom att endast en tredjedel av alla IT-brott anmäls (Sundén, 1997). Anledningar som uppgavs var att företaget inte trodde att polisen skulle klara upp brottet och att en anmälan medför ”bad will” för företaget. I och med att brotten inte anmäls utan tystas ned i stället, når de heller inte media. Eftersom få konkreta exempel på IT-brottsligheten når allmänheten, uppfattas det inte som något större problem för företagen och därmed inte heller getts någon prioritet. Den ökande kommunikationen över Internet, som är känt som ett osäkert media, har dock satt säkerhetsaspekterna i fokus och därmed ökat även medvetandegraden över hoten (Wedberg, artikel 2, 1997). Utnyttjandet av world wide web och Internet samt den ökande elektroniska handeln, gör att risken ökar för att externa individer skall lyckas få tillgång till information de inte har rätt till på grund av den ökade exponeringen av den information som hanteras (Kommunikationsdepartementet, 1997). Därmed har också behovet av att skydda sin information från obehöriga ökat.

Skyddet av såväl informationen som den utrustningen som krävs för att överföra och använda informationen innefattas under begreppet IT-säkerhet. Den kontinuerliga utvecklingen på IT-området gör att även förutsättningarna för IT-säkerheten ständigt förändras och därmed bör även skyddsmekanismerna utvecklas för att det inte skall uppstå brister.

I och med att företagen blir allt mer beroende av information, ökar även vikten av informationstillgångarna och behovet av att skydda dem. Vissa företag hanterar numera sina överföringar av likvida medel elektronisk, vilket gör det absolut nödvändigt för sändarna och mottagarna att säkerheten för transaktionerna är säkrad.

Det är inte enbart den tekniska utvecklingen som är viktig i säkerhetsarbetet, de mjuka faktorerna såsom relationen mellan arbetsgivare och personalen som hanterar informationen får en alltmer framträdande roll. Till de mjuka faktorerna hör också företagets image eller rykte utåt, faktorer som är beroende av att företaget kan hantera sin information. Om företaget blir bestulet på information eller om ett svårare datoravbrott medför förseningar i t ex produktionen, kan det medföra att omvärlden förlorar förtroendet för företaget. Bristen på förtroende kan resultera i att kunder och leverantörer söker sig till ett annat företag där verksamheten är säkrad. Därför är det troligt att många organisationer inte anmäler informationstekniskt relaterade brott eftersom företagen är rädda för negativ publicitet och förlust av förtroende hos aktieägare, kunder m. fl.

1.2 Problemdiskussion

I dagsläget satsar svenska företag stora resurser på olika tekniska IT-säkerhetsmekanismer. De tekniska delarna av säkerheten är viktiga, men även den mänskliga faktorn bör vara av betydelse för den totala IT-säkerheten. Kan det kanske till och med vara så att den mänskliga faktorn är avgörande för företags IT-säkerhet?

IT-säkerhet är ett intressant och komplext fenomen som lockar till fördjupning. Ämnet är relativt nytt i jämförelse med andra organisatoriska delar av ett företag, vilket gör att många företagsledare inte är fullt insatta i problematiken (Lönn, 1996). Det är få svenska företag som har kommit så långt att de implementerat policys eller har beredskap för avbrott (Cardholm, 1997).

IT-systemen är olika i alla företag och därmed har de också olika behov av säkerhet. Svårigheter kring att bestämma vilken grad av IT-säkerhet företaget kräver beror på en mängd olika faktorer, såsom om det är frågan om ett stort eller litet företag, hur många anställda företaget har, vilken typ av verksamhet som bedrivs, eventuella internationella anknytningar osv.

Företag präglas av människorna som arbetar i företaget, och eftersom alla människor är olika är det också rimligt att anta att det finns en unik kultur på varje arbetsplats som behöver tas hänsyn till i säkerhetsarbetet. Vidare har varje företag har en unik ledarsammansättning, en egen historik som resulterat i erfarenheter som gäller just det speciella företaget, unika ekonomiska förutsättningar och personalkonstellation. Företagets lokalisering, utrymmesmässiga förutsättningar, det informella och formella kontaktnätet är andra faktorer som rimligtvis borde påverka IT-säkerhetssystemets utformning.

Ett grundläggande motiv till uppsatsen är att, eftersom säkerheten är eftersatt på så många svenska företag, studera vad svenska företagsledare kan göra för att erhålla säkra IT-system, samt vilken betydelse de mjuka faktorerna såsom medarbetarnas motivation, inställning och kunskap har för slutresultatet.

För att som företagsledare kunna fatta resonabla beslut i frågor rörande företagets IT-säkerhet är det rimligt att anta att denne bör vara på det klara med vilka hot som existerar mot verksamhetens IT-system. Likaså bör den ansvarskännande personen alternativt personerna i ledarställning vara initierade i formalia gällande IT-säkerhet, samt ha en preciserad strategi och policy för säkerhetsarbetet. Förutom tekniska lösningar på säkerhetsproblematiken bör med stor sannolikhet även en översyn av de mjuka faktorerna göras för att ha möjlighet att skydda IT-systemet.

Tidigare forskning i ämnet är till stor del koncentrerad kring tekniska lösningar. I min litteratursökning fann jag främst böcker om brandväggar och hur man kan skydda sig mot hoten från Internet (”Internet Security Secrets” av Vacca, ”Internet Firewalls & Network Security” av Siyan och Hare, ”Firewalls and Internet Security” av Cheswick och Bellowin, ”Web Security Sourcebook” av Rubin m fl, ”Web Security & Commerce” av Garfinkel och Spafford, osv.), men få som berörde IT-säkerheten ur ett mer holistiskt perspektiv. De mesta som finns att läsa om IT-säkerhet är anpassat efter amerikanska förhållanden och de flesta svenska böcker i ämnet är tyvärr flera år gamla. Den aktuella informationen fann jag främst i tidningsartiklar.

1.3 Syfte, målgrupp och avgränsning

Syftet med denna uppsats är att, ur en företagsledares perspektiv, belysa de faktorer som har betydelse för god IT-säkerhet i ett svenskt företag. För att åstadkomma detta måste först och främst företagsledningens ansvar och de ekonomiska aspekterna i processen klarläggas. Därefter skall anledningen till behovet av IT-säkerhet utredas, d.v.s. vilka de vanligaste hoten som förekommer mot IT-system är. När hotbilden framträtt ställs frågan hur IT-system skall kunna skyddas mot dessa hot, m.a.o. vilka skydd och lösningar som finns att tillgå. Då ansvaret, hotbilden och säkerhetslösningarna blottlagts bör även en närmare granskning av företagens kärna - människorna i organisationen, göras för att få fram en bild av hur god IT-säkerhet i ett svenskt företag kan se ut.

Uppsatsen riktar sig till svenska företagsledare och andra intresserade av säkerhetsfrågor ur ett företagsledarperspektiv. Av denna anledning kommer jag att koncentrera rapporten till det holistiska säkerhetsperspektivet och inte gå in närmare på de tekniska säkerhetslösningar som finns på marknaden idag.

1.4 Disposition av arbetet

Kapitel 1 Inledningen innehåller en bakgrund till uppsatsen, problemställning, syfte och avgränsningar.

Kapitel 2 Metodkapitlet består av de metoder som användes i förberedelserna inför studien och metoder vid genomförandet av undersökningen.

Kapitel 3 Här diskuteras företagsledningens roll och ansvar i IT-säkerhetsprocessen, samt de ekonomiska aspekterna på säkerheten.

Kapitel 4 I detta kapitel behandlas hoten mot den interna säkerheten i svenska företag såväl avsiktliga som oavsiktliga.

Kapitel 5 Detta kapitel behandlar de åtgärder ett företag kan vidta för att skydda sina informationstillgångar på det mer tekniska planet.

Kapitel 6 Diskussionen i detta kapitel kretsar kring medarbetarnas betydelse samt gynnsamma företagskulturella förhållanden för säker IT.

Kapitel 7 Först i slutdiskussionen tolkar jag den insamlade informationen och drar slutsatser av undersökningen.

1.5 Definitioner

Vissa begrepp som använd frekvent i studien förklaras här. Förklaringarna är hämtade ur Bonniers lexikon, om annat inte står angivet.

access	möjlighet till åtkomst
datasäkerhet	vetenskapen och studien av metoder för att skydda data i ett dator- och kommunikationssystem från icke auktoriserat avslöjande, överföring, försening, modifiering eller förstörelse antingen den är avsiktlig eller inte. (Caelli, Longley och Shain, 1989)
datorsäkerhet	att skydda datorer från oavsiktlig såväl som avsiktlig åverkan samt stöld
informationsteknologi	*IT*, all teknik för att samla in, lagra, bearbeta, återfinna, kommunicera och presentera text, bild och tal. Oftast avses tekniker som förutsätter digital databehandling samt sådan lagring och överföring.
IT-säkerhet	IT-säkerhet innebär både skydd av information och den utrustning som krävs för att överföra och använda informationen.

Internet	internationellt nätverk av datanät som bygger på ett gemensamt överföringsprotokoll och datapaketförmedling över telenäten
e-post	elektronisk post, är den nättjänst som har störst räckvidd. Internetadressen är uppbyggd ungefär som en vanlig adress med namn, underdomän och toppdomän. (anna.andersson@skolan.se)
säkerhet	tillstånd som inte innebär fara, kan även betyda visshet. (Norstedt, 1990)
world wide web	*www*. Det allmänna internationella nätverket av websidor som finns på Internet.

2. Metod

2.1 Val av ansatser

Det finns ett antal olika sätt att närma sig ett vetenskapligt problem, och beroende på karaktären hos det som skall undersökas används olika typer av metoder för att undersöka fenomenet. Oftast bestämmer sig forskaren redan i ett tidigt skede för vilken vetenskapsuppfattning, undersökningsmetod och tillvägagångssätt som skall användas för att utföra undersökningen. Jag kommer kort att beskriva vilka typer av ansatser som varit aktuella i min undersökning och motivera varför jag väljer att använda respektive metod.

2.1.1 Positivistisk och hermeneutisk vetenskapsuppfattning

De två vanligaste forskningssynsätten på hur kunskap skall produceras är positivismen och hermeneutiken. Positivism är uppfattningen att vetenskaperna bör använda sig av en gemensam metodik, som utifrån iakttagelser leder till kunskap om universella orsakssamband. Positivismen utvecklades ur empirismen och bygger på naturvetenskapliga ideal.

Den andra stora vetenskapsuppfattningen är hermeneutiken som också kallas för tolkningslära. Ursprungligen användes hermeneutiken främst för att tolka texter, men uppfattningen övergick senare till att gälla studier av mänskliga fenomen överhuvudtaget. Idén bygger på att människan är intentionell och alltså har en avsikt med det hon gör. Hermeneutiken söker efter rimliga skäl till den mänskliga handlingen.

Hermeneutiken betonar helheten i den meningen att den har en mening utöver enskildheterna. Den grundläggande idén är att om något ändras i en enskild del påverkar det helheten som i sin tur kan påverka andra delar[1]. Den används för att tolka utsagor och handlingar. Hermeneutiken används inom humanistiska och samhällsvetenskapliga ämnen.

Jag väljer att använda mig av den hermeneutiska vetenskapsuppfattningen, då min undersökning till stor del består av att tolka delar av säkerhetsproblematiken för att belysa IT-säkerheten ur företagsledningens perspektiv.

2.1.2 Kvalitativa och kvantitativa metoder

Undersökningsmetoder delas in i två grupper; de kvantitativa och de kvalitativa metoderna. Kvantitativa metoder är ofta positivistiska med naturvetenskapliga ideal. Det som skall studeras måste göras mätbart och resultatet skall presenteras numeriskt. Denna uppfattning av vetenskaplighet är inspirerad av den logiska positivismen med naturvetenskapligt forskningsideal. Den kvantitativa metodens dilemma är att välja ut vilken/vilka kvaliteter som är relevanta att mäta, nästa problem är hur det skall mätas, valideras och slutligen presenteras. ”Den kvantitativa metoden söker en verklighet för att pröva ett givet begrepp på.” (Eneroth, 1984)

Kvalitativa metoder är svårare att definiera än de kvantitativa. Dessa metoder är ofta fenomenologiska med ideal ur humanioran och bygger på att allt inte går att göras mätbart. En

[1] Lind, ur föreläsningsanteckningar från VTM-kursen 1996

kvalitativ undersökningsmetod används för att nå en förståelse både av delar och helhet och att alla fenomen består av ett antal unika kvalitetskombinationer.

Kvalitativa metoder utgår från att varje undersökt företeelse är unik, till motsats från kvantitativa metoder som utgår från att alla fenomen har exakt likadana kvaliteter och alltså är mätbara. Syftet med en kvalitativ metod är att beskriva en företeelses kvaliteter, alltså vilka egenskaper en företeelse har och vilka som karaktäriserar företeelsen.

Som framgår av kapitel ett är IT-säkerhet ett kvalitativt problemområde och kräver därmed en kvalitativ undersökningsmetod. Den kvantitativa metoden är utesluten eftersom det inte är möjligt att mäta de fenomen jag avser att undersöka i siffror.

2.1.3 Induktiv och deduktiv forskningsansats

Induktion används för att göra enskilda observationer som sedan skall leda till en slutsats av allmän giltighet. Detta tillvägagångssätt är det som oftast används i kvalitativa metoder. Induktivt tillvägagångssätt innebär att forskaren närmar sig en verklighet förutsättningslöst, utan några klara hypoteser och med en ganska vag och oprecis problemställning.[2] Detta medger en flexibel uppläggning av undersökningen. Induktion innebär att låta de funna kvaliteterna som hittas i studier av ett litet urval ingå i generella begrepp.

Deduktion utgår från premisser och kommer med hjälp av regler fram till en slutsats. Ansatsen är utgångspunkten ur vilken forskaren söker klargöra vad som sker under vissa förutsättningar. Deduktion förknippas med kvantitativa metoder.

Jag kommer att studera hoten mot och skydden för företags IT-system, hur människorna i organisationen påverkar IT-säkerheten samt företagsledningens ansvar i säkerhetsprocessen. Med dessa observationer avser jag att dra en generell slutsats som gäller flertalet svenska företag. Därmed väljer jag att till större delen använda mig av den induktiva forskningsansatsen, men med vissa inslag av deduktion då jag även avser att klargöra vad som händer under vissa förutsättningar.

2.2 Metoder i undersökningsprocessen

Som det framgår av problemställning och syfte är uppsatsen inte inriktad på att lösa något kvantitativt problem utan på att göra en kvalitativ undersökning. Jag avser att göra en deskriptiv uppsats och har utifrån ovanstående valt ut passande metoder för undersökningsprocessen.

2.2.1 Datainsamlingsmetoder

Undersökningsmetoder för datainsamling består av innebördsstruktur (för att få fram förståelsedata) och materiella aspekter (för att erhålla sinnesdata). Jag använder mig till huvudsak av sekundärdata i undersökningsprocessen.

2.2.2 Teoretiska perspektiv

När datamassan om företeelsen tagits fram måste en ”varseblivningsmetod”, eller ett teoretiskt perspektiv väljas, det vill säga bestämma vilken information som är relevant för perspektivet. När jag bestämt mig för ett perspektiv kommer det att fungera som en ram för min förståelse

[2] Grundén, ur föreläsningsanteckningar från VTM-kurs 1996

och mina sinnen. Ramen styr uppmärksamheten mot viss information och förbi annan information.

Det finns tre olika perspektiv som kan antas: det statiska, det dynamiska och det teleologiska perspektivet. Det statiska perspektivet innebär att ta fasta på det relativt bestående och stabila hos en företeelse. Företeelsen kan observeras oförändrat vid olika tillfällen. Det dynamiska perspektivet är ämnat för det instabila som forskaren försöker tydliggöra hos en företeelse och koncentrerar sig på förändringar. Exempel på förändringar kan vara hur en statisk aspekt förändras eller flöden genom det statiska. Det tredje perspektivet som Eneroth (1984) tar upp är det teleologiska perspektivet som är målrelaterat. Detta perspektiv grundar sig på att en företeelses statiska och dynamiska aspekter är bara intressanta utifrån hur de förhåller sig till vissa grundläggande mål. Perspektivet kallas också för ”ändamålsperspektivet”.

Jag använder det statiska perspektivet, trots att IT-säkerhet kan tyckas vara en dynamisk företeelse, eftersom ett företag ofta förändras långsamt och kan ses som en relativt stabil företeelse.

2.2.3 Datasammanfattningsmetoder

En datasammanfattningsmetod sammanfattar information till begrepp om den undersökta företeelsen, därför kallas metoden också för begreppsbildning. För att kunna lyfta upp den insamlade informationen från olika individer till en allmängiltig nivå måste den syntetiseras.

När informationen skall sammanfattas grupperas den under olika kvaliteter. Statiska aspekterna hos företeelsen kräver statiska begrepp som kan sammanfatta och framhäva det bestående, dynamiska aspekter kräver dynamiska begrepp och teleologiska aspekter kan använda båda aspekterna beroende på deras karaktär.

För de statiska aspekterna nämner Eneroth tre viktiga sammanfattningsmetoder som syftar till att beskriva tillstånd; grounded theory-, idealtyps- och väsentypsmetoden.

Grounded theory metoden, eller kartläggningsmetoden som den också kallas, syftar till en kartläggning av företeelsens kvaliteter. Datasammanfattningsmetoden utformades av Glaser och Strauss. När en forskare står inför en mängd tydliggjord data, försöker han/hon systematiskt gruppera och omgruppera dem till en så fullständig kartläggning av företeelsen som möjligt utifrån dessa givna data. Begrepp delas in i kategorier, som har olika dimensioner, som i sin tur har flera olika kvaliteter. Denna metod är avsedd för det statiska perspektivet.

Idealtypsmetoden, eller karikatyrmetoden, syftar till att forma en karikatyr av de olika sorters fall som exemplifierar företeelsen. Metoden avser att gruppera data till en slags konstruerande idealtyp av olika sorters ”exemplar” av företeelsen. Detta är den mest fantasirika och förmodligen den mest använda metoden till vardags (t ex Svensson, lantis, fikus). Ingen har *alla* de egenskaper som ingår i en idealtyp, metoden söker fånga det centrala eller det ideala hos företeelsen.

I väsentypsmetoden försöker man finna det kännetecknande och det eventuellt gemensamma för alla fall av företeelsen ifråga. Metoden är anpassad till en företeelses statiska aspekter. Metoden försöker fånga det kännetecknande, dvs de gemensamma kvaliteterna för *alla* fall av

företeelsen och fastställa de *verkligt* gemensamma kvaliteterna för en grupp fall samt belysa likheter och skillnader.

Av de dynamiska aspekternas sammanfattningsmetoder tas det upp två metoder; processmetoden och den dialektiska metoden. Dessa båda metoder beskriver ett förlopp och var alltså inte aktuella för min del.

Eftersom jag redan valt en statiskt synvinkel på problemet kunde jag välja någon av de därför avsedda datasammanfattningsmetoderna. Jag väljer att använda mig av grounded theory metoden eftersom den passar bäst in på IT-säkerhetsproblemet.

2.2.4 Urvalsmetoder

Kvalitativa urvalsmetoder syftar till att göra ett urval som innehåller så många olika slags kvaliteter som möjligt för att informationen skall resultera i ett begrepp om företeelsen.

Innan en urvalsmetod kan väljas måste datasammanfattningsmetoden vara vald, kanske bör även datainsamlingsmetoden och det teoretiska perspektivet vara valda. Anledningen till det är att forskaren måste veta vad som skall hända med materialet innan det går att bestämma hur urvalet skall gå till.

Kvalitativa undersökningar kräver endast ett litet urval, främst för att det skall vara möjligt att överblicka datamängden. Urvalet måste därför väljas ut med omsorg för att ge maximalt antal kvaliteter.

2.3 Genomförande

Jag samlade kontinuerligt in information kring problemområdet under arbetets gång. Efter den formade strukturen sammanfattades informationen begreppsvis i enlighet med grounded theory. För att få en bättre förståelse för de fysiska säkerhetshjälpmedlen, som finns och krävs på marknaden, tog jag kontakt med ett försäkringsbolag. Med de rättsliga aspekterna fick jag god hjälp av advokat Woodstocks föredrag i Borås i slutet av oktober. Slutligen drogs slutsatser av det insamlade materialet.

3. Företagsledningens ansvar i IT-säkerhetsprocessen

3.1 Strategier och regelverk

Det yttersta ansvaret för IT-säkerheten innehas av företagets ledning och säkerhetsarbetet grundläggs i företagets informationssäkerhetspolicy. (Wedberg, artikel 2, 1997) I denna policy framgår företagets mål med säkerhetsarbetet, vilken inriktning företaget antagit, samt ansvarsfördelningen med avseende på säkerheten. Då policyn omsätts i praktiken sätts utförliga ramar upp för vad som skall göras, hur det skall utföras och vem som skall utföra det. Policys och ramverk för säkerheten måste, för att fylla sin funktion, föras ut i hela organisationen.

3.1.1 Strategisk styrning av företag

Ett företag är uppbyggt kring en affärsidé. Denna idé kan utvecklas med tiden i och med att företaget förändras, men grundidén förblir ändå densamma. För att förverkliga idén ställer ledningen upp vissa mål och försöker styra utvecklingen i företaget mot dessa mål. Efterhand behövs någon form av kontroll för att kontrollera att utvecklingen sker på så sätt som det är tänkt och i annat fall sätta in korrigerande åtgärder.

Begreppet styrning kan användas som ett sammanfattande begrepp för samordning och kontroll, dvs alla de åtgärder som vidtages för att påverka beteendet i organisationen. Chandler (1962) preciserade styrbegreppet till att innefatta den information och ordergivning som strömmar i de kommunikationskanaler som bildas i strukturen (ur Holmström, 1995). Kanalerna kan vara av både formell och informell natur.

Styrningen genomförs med hjälp av en uppsättning styrinstrument. Den övergripande styrningen kallas för strategisk styrning. I den strategiska styrningen ingår organisationen av företaget, strategisk planering, företagets kontakter med omvärlden m.m. Den strategiska eller den mer långsiktiga styrningen bestämmer företagets inriktning i stort vad gäller verksamhetsområden, marknader, IT-säkerhet osv. Detta sker oftast i form av diskussioner kring alternativa planer angående utvecklingen och olika yttre händelser. Ledningen formulerar därför flera olika strategier i form av avsedda åtgärder vid olika tänkbara framtida scenarier. I vissa fall preciseras strategierna i kvantitativa planer för ett visst antal år framöver, ibland görs även en viss investeringsbedömning (Frenckner och Samuelson, 1989).

3.1.2 Beslutsprocessen

Ett företags ledning har till uppgift att fatta de strategiska IT-besluten för organisationen. Det är ledningens ansvar att välja styrmedel och att fatta nödvändiga beslut. För att kunna fatta riktiga beslut krävs ett ordentligt beslutsunderlag.

Beslutsprocessen är inte över i och med att beslutet fattats, detta illustreras i Bäck och Halvarssons beslutscirkel (se bild 3.1). Innan det formella beslutet antas görs en noggrann plan och beredning av beslutet. Efter genomförandet görs en utvärdering som delges planering och beredning. Planerings- och beredningsfunktionen korrigerar därefter beslutsunderlaget till nästa beslut i frågan.

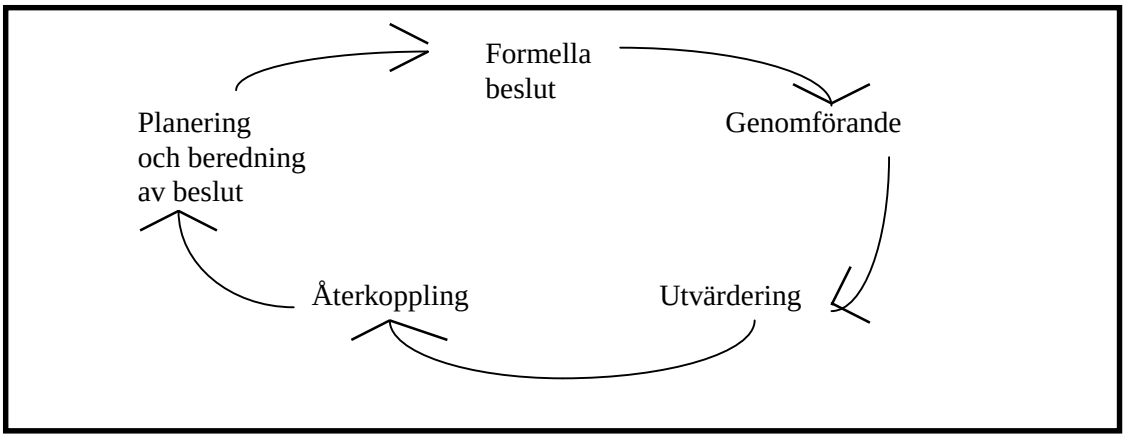

Bild 3.1 Beslutscirkeln[3]

3.1.3 Delaktighet i besluten

Ett företag bör ha en ledningsgrupp som speglar företagets olika delar. Den som är huvudansvarig för säkerheten bör därför sitta med i företagets ledning för att på så vis vara med och ge säkerhetsaspekten på de förändringar som planeras. (Caelli, Longley och Shain, 1989)

För att en enhetschef skall göra ett bra arbete bör hon/han känna ansvar för sin enhet. Delaktighet i de beslut som fattas vad gäller den egna enheten såväl som hela organisationen är faktorer som ger ansvarskänsla hos enhetschefen. Delaktigheten i företagets utveckling och styrning skapar lojalitet, vilket i sin tur genererar bättre genomtänkta beslut. Det är viktigt att överlåta till varje enhetschef att prägla sin enhet för bästa resultat och att tänka på att var och en är expert på sitt område. (Bäck och Halvarsson, 1992)

För att information skall ge avsedd effekt bör den vara utformad så att den är lätt att förstå och överskåda. All berörd personal skall kunna ta till sig innehållet för att själva kunna göra riktiga bedömningar. Självklart är det viktigt *att* de tar del av materialet.

3.1.4 Ledarens personlighet

Macintosch (1985) hävdar att olika chefer har olika sätt att bearbeta information och fatta beslut. Chefen sätter sin egen personliga prägel på arbetssättet i organisationen såväl som beslutsfattandet. Macintosch menar att skillnaderna är så stora att informations- och redovisningssystem egentligen borde skräddarsys efter chefens personlighet.

Av ledares arbetsuppgifter är det informationshanteringen som tar mest tid i anspråk. Mintzberg (1972) ansåg att en effektiv ledare skall fungera som nervcenter i en organisation. Ledaren skall fungera som informationsspridare, talesman och strateg för företaget.

Organisationssociologin fokuserar på den sociala interaktionen och beslutsfattandet i organisationen med avseende på faktorer som osäkerhet, oberoende mellan organisationens komponenter, speciella och integrerade mekanismer, samt teknologi (Macintosch, 1985). Strukturen av de nämnda faktorerna influerar organisationsstrukturen och dess beteendemönster.

[3] idé från Bäck och Halvarsson, 1992

3.1.5 IT-säkerhetssystemet

Bra IT-säkerhet är alltså beroende av bra ledarskap, det finns inga teknikaliteter som kan uppväga bristen på gott ledarskap. Brister i IT-systemet är det som utnyttjas i första hand av personer som avser att skada det. IT-säkerhet kan enbart uppnås i system som är väldesignade och väl hanterade. (Caelli, Longley och Shain, 1989) Det är dock först när ledningen funnit att informationen är värd att skyddas och att informationsbehandlings/kommunikationssystemet är möjligt att skydda kan företagsledningen rikta sin uppmärksamhet mot att formulera en säkerhetspolicy och fördela ansvaret för IT-säkerheten. Ledningen utgår då ofta ifrån en riskanalys av de existerande systemen i företaget och finner procedurer för modifiering av de existerande systemen, samt design och implementering av nya system. Därefter förs den framarbetade säkerhetspolicyn ut i verksamheten och en beredskapsplan tas fram. Det gäller dock att inse att det inte räcker med att ha vidtagit åtgärderna en gång, då systemet hela tiden förändras.

3.1.6 IT-strategi och IT-policy

En konstruktivt formulerad IT-strategi med tillhörande IT-policy där säkerhetsarbetet är klart formulerat ger företaget en bra förutsättning för att skydda sin information. Caelli, Longley och Shain (1989) förespråkar en omfattande och detaljrik säkerhetspolicy som syftar till att täcka hela IT-säkerhetsområdet. En sådan policy innehåller:

- den organisatoriska strukturen och tillhörande ansvar i säkerhetsfrågor. En högre chef kan tilldelas den övergripande kontrollen och rapporteringen till högsta ledningen.
- risk management
- personal policy
- informationstillhörighetspolicy och informationshanteringsansvar
- access- och krypteringsreglering
- informationsflödeskontroll
- säkerhet av lagrad data
- övervakningsfunktioner och spårbarhet
- bedrägerikontroll
- regler för design och modifieringsprocedurer av IT-systemet
- standarder, fortlöpande utvärderingar och rapporteringsprocedurer
- beredskapsplan

Cardholm (1997) däremot anser att en sådan omfattande policy gör säkerhetsarbetet tungrott och ineffektivt, han förespråkar därför ett tunt häfte med regler för att de skall vara lätta att ta till sig för de anställda. Ett annat förslag är att sammanfatta minnesregler i maximalt 10 punkter som placeras där alla kan se dem. De vanligaste reglerna är:

- att inte använda enkla lösenord
- att aldrig lämna ut sitt lösenord
- att alltid göra en backup
- att använda aktiva virusskydd
- att överträdelse av reglerna kan straffas enligt lag

3.1.7 Säkerhetsmanualen

Ansvarig för datasäkerheten på arbetsplatsen använder sig av en mängd olika tekniker för att informera de anställda om säkerhetsproblem och dess lösningar i organisationen. De använder

sig av broschyrer, affischer, samtal samt säkerhetsmanualer i sin kamp för ett säkert IT-system. Manualen kan innehålla allt från några sidor till tjocka pärmar med vad som är tillåtet och inte, beroende på vilken filosofi säkerhetsansvarig är anhängare av. Vanligtvis finns det bifogat checklistor för de anställda att gå efter, telefonnummer till personer att ringa i nödsituationer och ibland även vad som kan hända om inte manualens säkerhetsföreskrifter följs. Följder av överträdelse av reglerna kan vara böter, åtal, avsked mm. I och med att säkerhetsmanualerna växer i omfång, då användandet av datorer blir allt viktigare i det dagliga arbetet och nödvändigheten av att datorerna används och sköts på ett riktigt sätt, blir de lätt oöverskådliga och upplevda som ett hinder i arbetet.

Highland[4] (1992) menar att de flesta organisationer har inkorrekta och förlegade manualer. I och med att tekniken utvecklas med en hög hastighet har företagen inte haft möjlighet att hålla sig med uppdaterade säkerhetsmanualer. VanMeter[5] (1991) pekar i sin studie på att även när manualer är omfattande och korrekt hanterade utgör själva volymen av policys och procedurer ett hot mot effektiviteten. Oftast, menar han, är det få - om någon, som egentligen känner till att manualen existerar.

I en svensk undersökning, av Rabenius, Tsagalidis och Wester 1990, över användares förståelse av säkerhetslösningar i organisationer visade på att det finns stora avvikelser mellan säkerhetsdirektiven i en organisation och användarens förmåga att förstå och koppla dem till det vardagliga arbetet.

3.1.8 Nackdelar med pappersbaserade säkerhetsmanualer

Kowalskis studie visade att den pappersbaserade säkerhetsmanualen inte fungerade av flera olika anledningar. Han fann att de oftast hade ett icke-pedagogiskt upplägg med antingen för mycket information eller också hade de inte tillräckligt med information. Om en manual skall fylla någon funktion alls måste personen som läser den förstå och vara kapabel att ta till sig den information som ges. Därför är det förkastligt att använda speciell terminologi och en linjär uppbyggnad av manualen.

Det skrivna ordet uppfattas som gällande även om det, i och med att systemet förändrats, hittas felaktigheter i manualen. Säkerhetsmanualer är ofta förlegade eftersom uppdateringar innebär att det måste tryckas nya, vilket också innebär en kostnad för företaget. Andra nackdelar med tryckta handlingar är att de ofta innehåller redundant information och att de inte ger någon möjlighet till feed-back.

3.1.9 Faran med alltför strikta regler

Vissa företag har mycket strikta policyregler och kräver att de anställda skriver på särskilda säkerhetskontrakt. Underskrifterna intygar att den anställde är införstådd med vad som gäller och vilka straff som föreligger vid en överträdelse. Denna metod används främst i USA, men också av amerikanska företag i Sverige. I Sverige finns ett självständigt tänkande och en viss misstro till auktoriteter, vilket gör att en sådan tvångsåtgärd kan få motsatt effekt. Westman (1997) hävdar att svensken i allmänhet inte har mycket respekt för regler och att det snarare uppfattas som kreativt att finna sin egen väg. Givetvis förväntas ”kreativiteten” ske inom lagens ramar.

[4] ur Kowalski, 1994
[5] ur Kowalski, 1994

3.1.10 Lagar och regler

Cardholm (1997) menar att en väl formulerad säkerhetshandbok ger företaget möjligheten att på laglig väg kunna hävda att information spridits mot företagets vilja. Den som lämnar ut information till obehöriga riskerar då åtal med påföljd upp till sex års fängelse och den som mottagit informationen riskerar upp till fyra års fängelse. I datalagen finns regler som ger företaget full frihet att bestämma vilka delar av datasystemet som skall vara öppet för interna och externa medarbetare samt kunder. Överträdelser kan medföra upp till två års fängelse. Arbetsgivarna är ofta inte särskilt intresserade av att föra ett mål mot en av sina anställda till domstol, men genom att de har lagens stöd understryks vikten av fungerande säkerhetsrutiner, och säkerhetstänkandet inom företaget ökar.

Det finns flera svenska lagar som syftar till integritetsskydd, exempelvis brottsbalken, rättegångsbalken och sekretesslagen. Integritetsskydd i förhållande till datoranvändning återfinns främst i datalagen från 1973. Då var den lagen ett föredöme, men nu är den mycket föråldrad.

Enligt advokat Eric Woodstock (1997) kan det rent generellt sägas att den föråldrade lagstiftningen ger få svar på frågorna kring IT-säkerhet. Inte heller i framtiden kan företagen räkna med att få bättre vägledning då de nya lagarna också kommer att vara av generell karaktär. Det bästa rådet Woodstock kunde ge var att tänka till innan något händer och bygga system med funktionella behörighetssystem, backup, rutiner och spårbarhet. Advokaten ansåg att det viktiga var att systemen gör det möjligt att presentera ett förlopp i domstol. Det är vidare möjligt att skriva avtal med de aktörer som företaget har elektronisk kommunikation med, där det beskrivs vad som gäller om något går galet.

3.1.11 Internationella skillnader i säkerhetsarbetet

Det finns skillnader länder emellan hur långt företaget kan dra sina riktlinjer i säkerhetsarbetet. Westman (1997) påvisar att det i Tyskland finns en stor respekt för auktoriteter, vid tilltal används titlar och ”Ni” till de som står över i hierarkin inom företaget. Detta medför att det finns en större acceptans för strikta säkerhetsregler. Amerikanerna har även de ett striktare förhållningssätt mellan arbetsgivare och arbetstagare än vad vi har i Sverige, därmed kan detaljerade säkerhetsrutiner som fungerar bra i USA ha liten eller ingen effekt i Sverige. I vissa andra länder finns det även annorlunda hot såsom terrorism, detta hot har Sverige till stor del varit förskonat ifrån. Olikheter som dessa bör tas med i beräkningarna då ett företag har internationella ägarintressen.

3.1.12 Kvalitet på säkerheten

Implementeringen av en effektiv säkerhetspolicy är i allra högsta grad en fråga för ledningen. Bakom implementering av säkerhetspolicy bör det finnas en väl genomtänkt strategi. Den största delen av god IT-säkerhet inkluderar utvecklingen av organisatoriska kontroller och motivation hos personalen som utför kontrollerna. Detta arbete bör vara av hög kvalitet.

Begreppet kvalitet har varit populärt under många års tid och förknippas med positiva egenskaper. (Vedin, 1993) Hög kvalitet anses som ett mycket gott betyg, oavsett vad det syftar till. Begreppet används ofta om produkter, men kan lika väl användas vid syftning på inre egenskaper i organisationen såsom IT-säkerhet. Kvalitetsbegreppet innebär olika för olika personer, men brukar användas då något skall tillfredsställa både uttalade och underförstådda behov.

Säkerhetstänkandet bör vara med från början i en planeringsprocess och utvärderas kontinuerligt. Även kvaliteten på säkerheten bör revideras regelbundet. Systemet ackrediteras av en antingen intern eller extern person som går igenom systemet och granskar det. Denna revision används senare som ett underlag för ett driftsgodkännande av systemet (Wedberg, artikel 2, 1997).

ISO9001 är en av fem standards i ISO9000-serien som har funnits som ISO standard sedan 1987 (Sandholm, 1995). ISO står för International Organisation for Standardisation och är det internationella organet för standardiseringar. ISO är norm för kvalitetsarbete både i Sverige och utomlands. I Sverige liksom i många andra länder har den antagits som nationell standard.

ISO innehåller krav på en kvalitetspolicy och på kvalitetsuppföljningen. Kvalitetspolicyn visar riktlinjer för kvalitetsarbetet. Det finns olika skäl till att utföra ett kvalitetsarbete enligt ISO9000, det kan vara på grund av egna behov, krav från kunder, för att hävda sig i konkurrensen, krav från myndigheter i vissa branscher mm. Det har blivit allt viktigare för leverantörer att visa att de har ett kvalitetssystem som uppfyller kraven i ISO9000. En certifiering underlättar marknadsföringen och kan leda till att kunder gör beställningar utan att göra en leverantörsbedömning först.

Wedberg (1997) uttrycker kritik mot kvalitetsrevisorerna som certifierar företag i enlighet med ISO 9001-standarden. Han menar att denna vedertagna standard inte tar tillräcklig hänsyn till betydelsen av IT i företagen. ISO 9001 - standarden kräver mycket lite av IT-avdelningen, ett backup-system är mer eller mindre tillräckligt för att bli certifierad. Det förebyggande arbetet tas inte upp i standarden överhuvudtaget.

3.2 Ekonomiska aspekter på säkerheten

Det är uppenbart att systemet måste återställas efter ett intrång eller annat haveri på ett företags IT-system, samt att detta kostar att utföra. Wedberg (1997) menar att vid en kostnadsmässig översyn på säkerheten finner många företag att det inte är en hackerattack som de skulle förlora mest pengar på, utan ett IT-avbrott. Det är lätt att förbise att ett avbrott i datasystemet även medför konsekvenser för den övriga verksamheten såsom att tillgängligheten störs, att de anställda inte kan utföra sina arbetsuppgifter mm. Det är de sistnämnda konsekvenserna som måste analyseras för att få en rättvisande bild av vad ett avbrott skulle innebära. Olika företag kan ha olika tidpunkter på året då de är särskilt sårbara för ett IT-haveri, t ex då bokslutet skall sammanställas.

IT-brottsligheten ökar och därmed även ”reparationskostnaderna”. Det finns ett stort mörkertal kring denna typ av brott med anledningar som tidigare nämnts. Det görs dock vissa beräkningar på området. Under 1996 uppgick kostnader som kan härledas till databrott och effekter av databrott i USA till en summa på fem miljarder dollar (Ottoson, 1997).

I Sverige genomfördes under mars 1996 en telefonundersökning av Rinfo Research på uppdrag av Cap Programator (Nilsson, 1996). Resultatet av undersökningen visade att personal på företagen i genomsnitt spenderade 2 timmar och 2 minuter varje vecka på att hantera problem med sina datorer. Under den tiden kostar den anställde företaget i såväl lön som utebliven produktivitet. För ett företag med 1000 användare medför detta en kostnad på 23 miljoner kronor per år, motsvarande ca 60 heltidstjänster. Problem med datorer kostar

totalt svenska företag 35 miljarder kronor per år. Detta kan jämföras med att företagens totala IT-investeringar under 1996 uppgick till 80 miljarder kr.

3.2.1 Bristande rutiner

Wedberg (1997) uppger att hälften av alla incidenter beror på bristande rutiner. Enligt Stefan Lithén, som är säkerhetschef på ABB Infosystems, finns det många företag som inte uppdaterar sina backup-rutiner. Många företag har inte heller någon översikt över de ekonomiska konsekvenserna som en störning i systemet skulle medföra. Det måste finnas en viss ordning och reda i rutinerna, annars kostar det menar han - förr eller senare.

3.2.2 Kostnader för IT

Företagets kostnader för IT består av direkta och indirekta kostnader. Problemet är att de indirekta kostnaderna sällan kommer med i några kalkyler för IT-investeringar, vilka då i sin tur inte blir rättvisande.

IT-investeringar delas vanligtvis in i tre huvudgrupper av kostnader. Den första är den rena kapitalkostnaden som uppstår vid inköp av dator, mjukvara och kringutrustning. Den andra är supportkostnaden som vanligtvis mest består av telefonsupport. Den tredje kostnadsgruppen är den administrativa för t ex utredningar och uppföljningar. Förutom dessa kostnader tillkommer de indirekta kostnaderna som mestadels består av användarkostnader. Exempel på de indirekta kostnaderna är timmar spenderade vid datorn, introduktion, utbildningar, att ringa support, att läsa manualer och att hjälpa kollegor. De indirekta kostnaderna utgör över hälften av datorinvesteringarnas totala kostnad, enligt en Garther Groups undersökning (Nilsson, 1996).

Att skydda sina informationstillgångar kostar pengar, men med bakgrund av ovanstående bör säkerheten tillåtas att kosta, ta tid och plats i organisationen. Givetvis i rimlig relation till det som säkerhetsåtgärderna skall skydda. Kostnaderna för säkerhetsinsatserna bör inte överstiga värdet på informationen som säkerhetsinsatserna skall skydda. Det gäller att finna en balans mellan värde och kostnad.

Det finns, menar Caelli, Longley och Shain (1989), vanligtvis ett motstånd i organisationen mot kostnader som inte ger något påtagligt tillbaka. Kostnader kring förebyggande åtgärder såsom säkerhet är exempel på sådana kostnader. Men det finns troligen inte någon som är så säkerhetsmotiverad som den som just drabbats av förlust av information. Cardholm (1997) påtalar att det kan bli en mycket kostsam metod att vänta med säkerhetsrutinerna till en incident, t ex ett IT-avbrott, redan inträffat.

I IT-kommissionens rapport 6/97 fastställs det att om inte säkerheten är beaktad då ett företag bygger upp sitt IT-system, medför det att säkerheten kostar ännu mer pengar då den måste implementeras i efterhand.

3.2.3 Relationen till kunden

Kundens förtroende för företaget, företagets image och den personliga relationen mellan säljaren och kunden kan vara ett avgörande konkurrensmedel.

Det är väsentligt att tala samma språk inom en organisation. Om någon i en organisation skulle bete sig drastiskt annorlunda eller ”sämre” än den/de som skapat förtroendet är risken stor att kunden vänder sig till en annan organisation. Tjänster och relationer bör fungera väl

mellan enskilda individer, dvs alla i organisationen måste tala samma språk och bete sig konsekvent utåt. ”Det måste finnas en i många avseenden ensartad och konsekvent företagskultur.” (Vedin, 1993)

Samhället befinner sig i en ständig förändringsprocess. Olika branscher förändras olika fort, teknologiskt beroende företag förändras t ex ofta mycket snabbare än andra. Kunder ställer högre krav och förväntar sig snabba besked och leveranser. I denna miljö, menar Vedin (1993), att det är viktigt att företagen har en god anpassningsförmåga och en hög grad av flexibilitet, för att stå sig i konkurrensen.

3.2.4 Risk- och sårbarhetsanalys

Det kan vara svårt för en säkerhetsansvarig att komma till ledningen för företaget och begära en större summa pengar till säkerhetsinvesteringar för att inget skall hända. I ett sådant läge kan det vara bra att kunna redovisa hur mycket ett dataavbrott, alternativt ett intrång, skulle kosta företaget. Eftersom IT-säkerheten berör hela verksamheten är det viktigt att bedöma vad som händer om ett avbrott skulle inträffa. Wedberg (1997) hävdar att genom att göra en risk- och sårbarhetsanalys kan företaget lättare se konsekvenserna av en driftsstörning.

3.2.5 Bedömning av riskerna

För att kunna beräkna kostnaderna av ett dataintrång eller ett diskhaveri måste riskerna utredas. Utredningen går ut på att bedöma konsekvenserna för varje händelse och vilka kostnader det för med sig. För att upptäcka brister i rutinerna kan checklistor och liknande användas. Det viktigaste är att det är ordning och reda i systemet. Det mest effektiva sättet, att bedöma risken för förlust av data och kostnaden för att skydda den, är att göra en sårbarhetsanalys. Cardholm (1997) menar att enbart genom att genomföra en sårbarhetsanalys och diskutera säkerheten på arbetsplatsen ökas informationsskyddet i företaget på ett effektivt sätt.

Det första som bör göras är att tänka efter vad det är som behöver skyddas, vad någon kan tänkas vilja komma åt eller förstöra, vad som kan gå sönder eller försvinna och vilken betydelse detta skulle få för företagets driftsäkerhet. När detta är gjort har företaget en ganska klar hotbild. Hotbilden bör även innehålla de eventuella hot som uppkommer via informella vägar i företaget (Westman, 1997). För att få en så total bild som möjligt bör representanter från flera olika personalgrupper finnas med i arbetet.

Riskanalys är numera ett vanligt mätinstrument i organisationer. En riskanalys över säkerheten innebär att företaget söker svaren på frågor som:

- Hur stor risk föreligger?
- Hur osäker är miljön/omgivningen?
- Hur mycket är rimligt att betala för säkerheten?
- Vilken säkerhetsgrad kan uppnås för en given summa?
- När blir det kostnadsineffektivt att spendera mer på säkerheten?
- Hur trovärdiga är de valda säkerhetsmåtten?
- Var bör säkerhetsinsatserna sättas in?

3.2.6 Modeller som hjälpmedel i säkerhetsarbetet

Det är viktigt att förankra säkerhetspolicys och att på ett acceptabelt och realistiskt sätt väga åtgärderna mot kostnaderna. Modeller kan användas som ett hjälpmedel i säkerhetsarbetet. Den första säkerhetsmodellen - SBC (Security by Consensus) modellen presenterades 1990 på IEEEs[6] Computer Society Symposium on Security and Privacy (Kowalski, 1994). Modellen kallades då för ”the Information System Secure Interconnection Model” eller ISSI modellen och lades fram som ett ramverk för utvecklingen av säkra protokoll mellan olika informationssystem. Modellen utvecklades sedan till att även innefatta ramverk för jämförelser mellan nationella datorsäkerhetspolicies.

SBC modellen är en utveckling av den svenska sårbarhetsanalysen. SBC modellen delar upp sociala och tekniska system och därmed även säkerhetsaspekterna i sociala och tekniska kategorier. Dessa två huvudkategorier delas i sin tur upp i sex underklasser, som i sin tur delas upp i två säkerhetsgrupper, en daglig och en akut.

Sårbarhetskommittén upprättade 1983 ”Säkerhet genom analys metoden”. De flesta analysverktygen är designade för riskanalys på mikronivå, dvs de används av individuella system användare för att analysera deras specifika systems risker och hotbilder. Det finns enligt Kowalski (1994) inga modeller som analyserar risker och hot från ett makroperspektiv.

Dataföreningen i Sverige marknadsför fortfarande SBA-modellen, som skapar scenarier för vad som kan hända och vad detta skulle kosta (Cardholm, 1997). Modellen uppskattar dessutom risken för hur ofta det kan inträffa och bedömer risken mot vad motåtgärden skulle kosta att installera och underhålla.

I arbetet med modeller kan det vara av vikt att minnas att abstrakta modeller som har syftet att förenkla en komplex verklighet kan dock i själva verket samtidigt kan inge en falsk trygghet.

3.2.7 Brister i säkerheten

Ofta beror säkerhetsluckor på distribuerade system. Problem uppstår då ansvaret har fördelats ut i företaget, utan att det vid varje ny fördelning tagits hänsyn till säkerhetsaspekterna. Ett annat säkerhetsproblem i företag är att det inte finns några rutiner för att ta bort behörigheten för medarbetare som slutar sin anställning. Eftersom företagsmiljön hela tiden förändras är det av yttersta vikt att säkerhetsrutinerna kontinuerligt omprövas. Därför bör även riskanalysen vara en fortgående aktivitet eftersom förutsättningarna ständigt förändras. Caelli, Longley och Shain (1989) skriver att riskanalysen ingår som ett första steg i risk management som främst

[6] the Institute of Electrical and Electronics Engineers, Inc.

används av försäkringsbolag. Mest kostnadseffektivt är det att göra riskanalysen i inledningsskedet av designprocessen av ett nytt system.

3.2.8 Försäkringsvillkor

Ett mål med riskanalysen är att bestämma vilket försäkringsskydd företaget behöver. Försäkringsbolaget Folksam anser att företagsförsäkringar bör skräddarsys för företaget beroende på företagets placering, storlek, ägarförhållanden och personal. Ett försäkringsskydd skall skydda vid händelser som skadar näringsverksamheten som vid t ex brand, stöld, inbrott och avbrott. Eftersom alla företag är olika finns det ingen generell försäkringslösning som passar alla. Ett grundskydd bör bestå av försäkring för egendom, avbrott, ansvar och rättsskydd. Därefter är det företagets verksamhet som styr hur försäkringen skall se ut. Företaget bör sträva efter såväl ett optimalt som ett kostnadseffektivt försäkringsskydd.

I försäkringsbolaget Folksams försäkring för tillverkande företag, ingår en egendomsförsäkring som skyddar företagets byggnader, maskiner, inventarier och varor. Denna försäkring täcker skador till följd av brand, vatten, inbrott, utbrott, rån och skadegörelse samt glas- transport och allriskskador. En allriskförsäkring ingår för maskiner, inventarier, varor och kunders egendom. Även plötsliga och oförutsedda skador liksom förlust av säkerhetskopierad information ersätts av allriskförsäkringen. Ett tillverkande företag är särskilt sårbart för avbrott i produktionen och bör därför ha någon form av avbrottsförsäkring som ersätter uteblivna intäkter mm vid stillestånd i verksamheten. Det finns allriskavbrottsförsäkringar som ersätter vid bortfall av täckningsbidrag mm, om företaget måste stå stilla under en period på grund av allriskskada på exempelvis en dator eller annan utrustning.

Företag kan tilläggsförsäkra för diverse kostnader som kan uppstå såsom extrakostnader vid avbrott, oförutsedd skada på maskin, rättsskydd, fasta kostnader i rörelsen i samband med nyckelpersons sjukdom, åtkomstkostnader som uppkommer i samband med avhjälpande av fel i arbeten, förlustkostnader som uppstår genom att en anställd i sin tjänst gentemot arbetsgivare begår vissa typer av brott såsom IT-brott. Även skador på eller förlust av föremål som medförs utanför det ordinarie försäkringsstället, t ex IT-utrustning, kan försäkras.

För att få full ersättning vid ett inbrott måste inbrottsskyddskraven i försäkringsvillkoren och försäkringsbrev vara uppfyllda. Skulle det finnas brister kan företaget gå miste om ersättningen vid ett inbrott. Ju högre värde på företagets egendom, desto högre krav på inbrottsskyddet.

4. IT-säkerhet

4.1 Hot mot den interna säkerheten

Det finns en anekdot om hur den amerikanska generalen Norman Schwarzkopf glömde sin bärbara dator i en taxi, mitt under Gulfkriget. I datorn fanns hela strategin över hur Irak skulle besegras (Westman, 1997). Oavsett om denna anekdot är sann eller inte så är det uppenbart att det inte spelar någon som helst roll hur bra skyddet är mot yttre hot och spioner om inte den interna säkerheten fungerar.

4.1.1 Intern säkerhet

Med intern säkerhet avses skyddet av systemen mot allt från slarv till kriminella handlingar (Westman, 1997). I detta ingår faktorer som säkerhetspolicys, säkerhetskopiering, utbildning och motivering av medarbetarna.

De interna hoten mot företagets information kan delas upp i avsiktliga och oavsiktliga hot. Exempel på avsiktliga IT-brott kan vara att stjäla information eller datorutrustning, att utföra någon form av sabotage mot företagets system, att smitta företagets system med t ex virus eller att illegalt komma över ekonomiska medel genom företagets IT-system.

Det är inte alltid som hoten mot IT-systemet är medvetna handlingar. De oavsiktliga hoten kan bero på okunskap från användarens sida, slarv eller att företagskänslig fakta yppas för obehöriga personer (att prata bredvid mun). Enligt Cardholm (1997) är de vanligaste orsakerna till förlust av information användarens vardagsslentrian och missuppfattningar kring hur informationen bör skyddas och lagras.

4.1.2 Faror eller risker för företagets information

Företagets tillgångar i IT-systemet består av hårdvara, mjukvara och information. (Pfleeger, 1989) Dessa IT-tillgångar kan råka ut för en mängd olika incidenter. Brand, översvämning (eller annan vattenskada), maskinhaveri, strömavbrott, blixtnedslag, telekommunikationsavbrott eller skadedjur (som kan skada datorernas innanmäten eller gnaga av sladdar och kablar) är exempel på faktorer som kan skada systemets hårdvara. Operatören kan hantera datorn fel och därmed orsaka oavsiktlig skada. Det händer att datorer hanteras ovarsamt och åsamkas skada genom fall, eller att drycker eller mat hamnar i tangentbordet och därmed gör det obrukbart.

Till de avsiktligt orsakade incidenterna hör spionage, stöld av hårdvara, mjukvara och information, illasinnad attack av hackers, databedrägeri, m. fl. Pleeger (1989) delar upp hoten mot informationens säkerhet i fyra olika sorters hot; avbrott, avlyssning, modifiering och fabricering. Förutom dessa fyra bör alltid den okända faktorn tas med i beräkningen.

4.1.3 Lönsamt att attackera IT-system

Företagssystemen blir allt attraktivare för kriminellt sinnade personer eller grupper, som ser möjligheten till stora belöningar för liten ansträngning. Dessutom menar Caelli, Longley och Shain (1989) att risken för att bli upptäckt innan attacken eller sabotaget är slutfört är väldigt liten. Ett lättforcerat system kan leda till förlust av företagshemligheter (industrispionage)

eller elektronisk överföring av likvida medel (bedrägeri). Industrispionage innebar förr att bryta sig in på ett företag och spränga deras kassaskåp för att komma åt företagshemligheter. Numera innebär begreppet oftast att en person bryter sig in i organisationens allra heligaste via företagets IT-system.

4.1.4 Etiska attityder

1986 gjordes en studie om etiska attityder och datoröverträdelser bland 135 kanadensiska och 158 svenska universitetsstuderande (ur Kowalski, 1994). Det visade sig att 32% av kanadensarna och 22% av svenskarna hade försökt komma in på en dator de inte hade rätt till. 10% av kanadensarna och 12% av svenskarna lyckades. 6 av 13 kanadensiska studenter blev upptäckta, men bara 3 av 19 svenskar upptäcktes. (Om dessa siffror betyder att svenskarna i undersökningen var smartare än kanadensarna, eller om svenska säkerhetssystem var sämre än de kanadensiska, förblir obesvarat.) 56% av kanadensarna hade använt piratkopierade mjukvaror, men endast 19% av svenskarna hade gjort detsamma. 56% av kanadensarna som ägde modem hade försökt att ta sig in illegalt i ett datasystem och 42% av svenskarna.

Siffrorna visar att det är relativt vanligt förekommande att försöka komma över information som man inte har rätt till. Det är därför rimligt att anta att det inom hackarkulturen inte ses som ett allvarligare brott att utnyttja en dator för att komma in på områden som inte tillhör en själv. (Se även sista stycket i 3.2.5 the Internet Worm.)

Datasäkerhetsforskare såsom Parker (1976) och Carroll (1980) har påpekat hur viktigt det är med den etiska aspekten i datasäkerhetsproblematiken, men det är först på senare år som ämnet har vunnit någon riktig uppmärksamhet.

4.1.5 Insiderbrott

Av de kriminella hoten mot företagets information är insiderbrott ett av de absolut största problemen. Tidigare utgjordes 80-95% av säkerhetsriskerna av insiderbrottslingar, men enligt Engholm (1997) har Internet ändrat på detta. Riksrevisionsverket rapporterade under 1997 att utomstående numera står för de flesta databrotten. Det är dock mycket svårt att få fram uppgifter som stämmer överens med verkligheten eftersom mörkertalet är stort.

Säkerhetskonsulten Roger Gustafsson, på företaget Atremo Datasäkerhet, menar att Internet visserligen har inneburit en ökning av de yttre hoten, men att insiderbrotten fortfarande står för den största delen (Westman, 1997). De kontakter som han har haft med försäkringsbolag och banker visar att anställda som medvetet stjäl information eller på annat sätt missbrukar systemet är ett betydligt större problem än hackers och andra hot. Anledningen till att det inte förekommer i media är att incidenterna oftast tystas ned.

Den genomsnittlige insiderbrottslingen är enligt Gustafsson en medelålders anställd som känner sig åsidosatt av yngre medarbetare. Han rättfärdigar sitt handlande genom att resonera att ”Jag har minsann jobbat hårt för företaget och förtjänar därför en bonus”. Han utnyttjar sedan sin erfarenhet, snarare än sin tekniska kunskap, för att utföra den kriminella handlingen.

4.1.6 Personal och ansvarstagande

Företag som har datoriserat stora delar av sin verksamhet är beroende av skickligheten, engagemanget och integriteten hos företagets IT-personal. (Caelli, Longley och Shain, 1989) Personalen kan dock genom sin kunskap innebära en riskfaktor för företagen. Sårbarhet kan uppstå då en medlem ur personalen har avsevärd tillgång till att experimentera med

säkerhetskontrollerna i ett system eller att någon i nyckelposition får monopol på kunskapen om systemets egenheter. Personer som arbetar som operatörer, programmerare och systemerare kan också utvecklas till sådana maktfaktorer då de har möjlighet att utveckla en överlägsen kunskap om systemet och kan utnyttja detta i eget intresse om de så skulle önska. Om en eller ett fåtal personer utvecklar en sådan maktposition blir organisationen beroende av personen/personerna och dennes/dessas fortsatta anställning, tillgänglighet samt integritet och lojalitet.

Personer som är anställda av företaget, kan av olika anledningar besluta sig för att avsiktlig modifiera information i ont syfte, avslöja företagskänslig information eller lämna ut känsliga uppgifter till obehöriga. Särskilt allvarligt är detta om denna typ av aktivitet utförs av IT-personal med särskilda accessprevilegier. Gary Lynch på Gartner Group (Computer Sweden, nr. 63, 1996) menar att det finns indikationer som tyder på att utpressningsfallen ökar, det vill säga anställda som sparkats hotar att avslöja hål i företagets säkerhetssystem om de inte får tillbaka sitt arbete.

Under överföring av information, särskilt över allmänna kommunikationskanaler såsom Internet, händer det att data går förlorad, modifieras, fördröjs eller avslöjas av illasinnade externa individer eller organisationer. Detta gäller även information som är lagrad och behandlad i företagets system. (Pfleeger, 1989)

Personal kan utsättas för moraliska påtryckningar om de är mottagliga för utpressning, eller liknande, att begå illegala handlingar. Medarbetare kan vidare utsättas för frestelser om de tillåts utföra uppgifter som de vet inte kommer att granskas av andra. Om personal dessutom kan implementera privata rutiner, som varken är väldokumenterade eller begripliga av andra, så befinner sig företaget i beroendeställning gentemot denne. Även nyanställda kan innebära en säkerhetsrisk om de tillåts att använda systemet utan handledare, innan de är insatta i såväl systemet som säkerhetsfrågorna, eftersom de då kan göra fel. (Caelli, Longley och Shain, 1989)

En medarbetare som planerar att sluta sin anställning kan medföra en riskfaktor. Han eller hon kan ha anställts av en konkurrent och kan då använda kunskapen om företaget till konkurrentens fördel. En person som avslutar sin anställning på företagets begäran innebär en mycket stor säkerhetsrisk eftersom det kan innebära att personen går i hämndtankar och vill skada företaget så som det har sårat eller förorättat honom eller henne.

4.2 Avsiktliga attacker mot företags IT-system

Från 1967 till 1977 rapporterades 30 fall till polisen (Solarz, 1985). I en uppföljande undersökning som gjordes 1983 fick man fram att mellan 1977 och 1983 hade 400 databrott rapporterats till myndigheterna (Angerfeldt 1992, ur Kowalski, 1994). 1989 gjordes en annan undersökning, den visade att under perioden 1 januari 1987 till 31 augusti 1989 rapporterades 47 fall (Kronqvist och Ståhl 1991, ur Kowalski, 1994). I denna undersökning fördelades brotten enligt följande:

datorer eller program användes som verktyg i brottet Varav tre personifieringar, två bakdörrar (trapdoors)[7], en lösenordsattack, tio falsk datainförsel, en denial of service samt två genomsökningar	19 st
datorer eller program angreps i kriminellt syfte Varav en trojansk häst[8] och en denial of service	2 st
program kopierades, maskerades eller ändrades på ett kriminellt sätt Varav nio avsiktliga överträdelser av befogenheter, en denial of service och fyra som gjorde det omöjligt att använda tangentbordet	14 st
datorer eller nätverk av datorer besöktes eller användes av obehöriga Varav sex avsiktliga överträdelser av befogenheter, en genomsökning och fem med otillräckliga data	12 st
totalt	47 st

Alla fallen höll inte för rättegång.

Nästan alla de rapporterade kriminella angreppen riktades mot svagheter i applikationssystemen såsom redovisningssystem och elektroniska överföringssystem för likvida medel. Endast två av de rapporterade fallen berodde på att operativsystemets säkerhet var bristfällig då det utsattes för attacken. I ett av de två fallen hade en före detta anställd använt sig av en bakdörr för att få tillgång till systemet och ha ”super-user” previlegier genom ett allmänt konto. I det andra fallet var det studenter som genom en lösenordsattack kom åt skolans PC system eftersom systemet tillät upprepade inloggningsförsök.

4.2.1 Kapningsattacker

En ”öppen” terminal eller ”login session” kan kidnappas från en användare av systemet. När väl inkräktaren har root access[9] till ett system använder han/hon ett redskap som låter modifiera systemets innersta. (Russel och Zwicky, 1997) Då kan de terminalförbindelserna tas över efter det att identifieringsprocedurerna avklarats. Engångslösenord hjälper inte i detta fallet eftersom attacken sker först efter en lyckad inloggning. Det enklaste sätten att kidnappa eller kapa en terminal är att vänta tills någon reser sig för att hämta en kopp kaffe och då passa på. Sabotören kan annars skapa windowssystem som t ex ser ut som inloggningsfönster och lurar användaren att skriva in användare och lösenord i tron att allt är som det skall. Kapningsattacker utförs även mot företags servrar, av så kallade hackers, via internationella nätverk.

4.2.2 Olika sätt att attackera ett skiffersystem

Kryptering av meddelanden, lösenord eller kontonamn anses som relativt säkert, men det finns flera sätt att komma över den kodade informationen. Ett sätt är att göra en så kallad meddelandeutmattning. Genom att koda en mängd textfiler och sedan jämföra dem med ett kodat meddelande kan sabotören lista ut vad texten innehåller. Ett annat sätt är att skicka ett kodat meddelande ytterligare en gång till mottagaren, så kallad repetition, och sedan kontrollera vad effekten av meddelandet blir och genom det lista ut vad meddelandet innehöll.

[7] en dold accesspunkt till ett program
[8] ett till synes legitimt program som avser att utföra en uppgift, men utför även en annan dold aktivitet
[9] högsta behörighet i systemet

En tredje möjlighet att komma över kodad information är att uppträda maskerad. Detta utförs genom att angriparen identifierar sig korrekt och hämtar nycklar eller dekodad data. Ett fjärde angreppssätt kallas spoofning. Angriparen skär då av kommunikationen mellan två parter och agerar mellanled utan deras vetskap och får på så vis reda på all information. (Pfleeger, 1989)

4.2.3 Spoofning och scanning efter portar

Spoofning innebär, enligt Skalin (1997), att leta efter tillgängliga IP-adresser och används ofta av hackers för att de skall kunna ta sig vidare och försvåra för eventuella offer att spåra dem efter tillslaget.

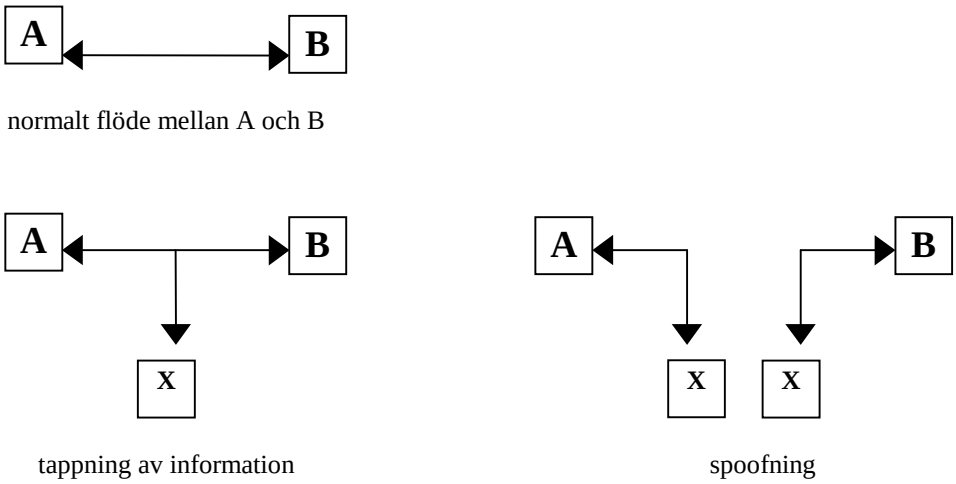

Bild 4.1 Illustrering av skillnaden mellan tappning och spoofing

Kullmar (1997) menar att spoofning än så länge inte är någon vanligt förekommande företeelse. Däremot skriver han att det är relativt lätt att avlyssna kommunikation, eller tappa information, i ett nätverk av typen Token Ring eller Ethernet. Anledningen är att det i nätverk är enkelt att tolka starten av vissa protokoll och på så sätt få fram lösenord. I denna typ av nätverk är det inte nödvändigt med något fysiskt ingrepp för att kunna avlyssna kommunikationen, det räcker med att ha rätt programvara. I datasystem som NT och UNIX behövs bara rätt behörighet.

4.2.4 Internet

För bara några år sedan ansågs inte Internetsäkerhet som ett behov. Grundtanken med Internet var ju att uppmuntra användarna att dela med sig av information och idéer. Ursprungligen utnyttjades Internet av de som skapade nätet, men i och med att användarantalet har ökat är det inte ett tryggt och säkert media längre. Trots att det redan tidigt i Internets utveckling inträffade incidenter, togs det inte på fullt allvar eftersom säkerhetsproblemen ansågs vara tonåringar som på kul bröt sig in i banker via sina modem hemma (Russel och Zwicky, 1997).

Internet är idag en global sammanslutning av privata nätverk som är sammankopplade genom allmänna länkar. Nätet ger de som är anslutna till nätet tillgång till kommunikationsredskap som e-post, informationssökning, filöverföring samt on-lineförbindelser, IRC (Internet Relay Chat). Den snabbast växande tjänsten för informationssökning är world wide web.

I mitten av 1995 förband Internet mellan 2 och 3 miljoner datorer över alla kontinenter, varav merparten i USA. En uppskattning av det totala användarantalet hamnade då runt 30-40 miljoner. I december 1996 uppskattades användarantalet i USA till 35 miljoner och i Europa till ca 6 miljoner (Barron, 1997). Detta ger en vink om hur explosionsartat tillväxten på Internet sker.

Kommunikationen med omvärlden via Internet är flitigt utnyttjad och innebär ofta ett säkerhetsproblem. Elektronisk post, e-post, är den nättjänst som har störst räckvidd, men det är ett relativt oskyddat kommunikationsmedel. En annan fara med Internet menar Westman (1997) att Usenet är. Usenet är ett system av över 2000 diskussionsgrupper och newsgroups för diverse intresseinriktningar. På dessa diskussionsforum och nyhetsgrupper loggar användare in sig utan att riktigt veta var de hamnar. Ofta är dessa typer av möten helt öppna, att i ett sådant möte diskutera företagskänsliga angelägenheter måste ses som direkt olämpligt.

Hoten från Internet målas ofta upp som skräckscenarier, men enligt Sam Sethi som är marknadsansvarig på Netscape i England, är 99% av det som passerar över Internet vanliga affärstransaktioner. Detta lämnar endast en procent för illegal verksamhet, men med avseende på hur många som är uppkopplade är 1% relativt mycket. Företag är dessutom troligare mål för en attack än vad en privat uppkopplad person är, vilket ökar sannolikheten för en attack mot företag (Time, sept. 8, 1997).

I IT-kommissionens rapport nr 6 1997 fastslås att konkurrenter måste kunna hemlighålla sina kunskaper och avsikter från varandra för att fri konkurrens skall kunna råda. Mycket av de stora företagens hemligaste trafik är till och från andra länder. Av den anledningen bör det inte förekomma några handelshinder och andra regelverk som begränsar den elektroniska överföringen, anser IT-kommissionen. I rapporten framgår även att mindre företag är omedvetna om hur dåligt skydd deras budskap har.

Wedberg (1997) menar att i och med att kommunikationen över Internet fortfarande ökar, är det troligt att denna typ av affärskommunikation kommer att innebära ett stort hot mot säkerheten i framtiden. Det är dock inte bara den externa kommunikationen som behöver ses över i säkerhetssyfte, den interna säkerheten får inte förbises bara för att det dyker upp nya intressanta tekniska lösningar på säkerhetsrisker på Internet.

Anne-Marie Eklund Löwinder, avdelningsdirektör på Statskontoret[10], menar att det finns ingenting som gjort så mycket för IT-säkerheten som Internet (Wedberg, artikel 2, 1997). Hon varnar dock för övertron på att brandväggar skulle lösa alla säkerhetsproblem i samband med Internetanvändningen.

4.2.5 ”The Internet Worm”

Enligt Russel och Zwicky (1997) förändrades grundinställningen till säkerheten på Internet november 1988, i och med ”The Internet Worm”. 1988 var ungefär 60.000 datorer uppkopplade mot Internet och de flesta av dem befann sig plötsligt under virusattack. Även de som inte attackerades var tvungna att försäkra sig gång på gång att inte de också hade blivit smittade. Kostnaden för incidenten uppgick till flera hundra miljoner dollar. ”The Internet Worm” uppmärksammades i tidningar och på TV och över en natt förändrades attityden om

[10] Statskontoret är en stabsmyndighet under Finansdepartementet. Statskontoret har till uppgift att samordna arbetet med den fredstida IT-säkerheten vad gäller den civila statsförvaltningen.

säkerheten på nätet. Frågan var inte längre om det fanns ett behov av säkerhetsåtgärder utan *hur* man skulle skydda sig från incidenter. Efter ”The Internet Worm” har Internetanvändarna ökat än mer och attackerna mot nätet likaså.

Russel och Zwicky beskriver ett uppmärksammat exempel på användning av Internet i syfte att skada. Incidenten drabbade datorsäkerhetsforskaren Tsutomu Shimomura, på San Diego Supercomputer Center. Han har under sina år som forskare samlat ihop ett ovärderligt arkiv av säkerhetshjälpmedel och dokumentation över systems säkerhetsluckor. På juldagen 1994 kopierade en inkräktare alla hans filer i arkivet. Två dagar senare fick Shimomura ett röstmeddelande (voice mail message) där någon skröt över inbrottet och hotade honom till livet. Shimomura reagerade med att installera stealth-övervakning[11] över sina poster och spårade inkräktarens vidare inbrott i andra företag. Till slut fann han att inkräktaren var datorbrottslingen Kevin Mitnick som sökts i flera år av myndigheterna. Mitnick spårades till Raleigh i North Carolina. Han greps i februari 1995 och anklagades för att under fyra år ha försökt tränga in i datorsystem hos bl a Nokia, Motorola och Fujitsu. Rättegången är planerad till april 1999.

4.2.6 Hackers

Attacker som utförs på illegalt sätt för att ta sig in i företags IT-system, t ex genom Internet, görs av så kallade hackers. Dessa är personer med stort intresse för datorer och dess möjligheter. De söker ta reda på koder och lösenord till andras datorsystem för att olagligt ta sig in i dem. Vissa hackers utövar även sabotage och konstruerar t ex datavirus. Hemsidor är ett populärt mål för hackers då det är en synlig attack som ofta väcker uppmärksamhet. Ofta ändras texten och eventuella bilder på hemsidan till obscena eller förlöjligande meddelanden och bilder.

Den femte mars 1997 hackades NASAs hemsida av hackergruppen H4G1S där de protesterar mot bl a ovan nämnda Mitnicks fängelsedom för att han varit, som de uttrycker det, nyfiken och velat lära sig. (Flashback Hackers Archive, 1997) De anser inte att han har begått något som helst brott. Andra anhängare till den fängslade Mitnick hotade i december 1997 att släppa loss ett virus i datorsystem världen över om han inte släpps (TT-AFP, ur BT 3 januari 1998). Hoten som fanns att läsa på Internet löd bl a ”Viruset kan stoppas - men inte av dödliga”. Attacken skall enligt hotelsen utföras den 25:e december 1998.

Sveriges första riktigt stora hack utfördes den 17:e mars 1996 mot Telia. Incidenten uppmärksammades ordentligt i media. Efter det att Telia gått ut i radio och meddelat att säkerhetsluckorna var tätade hackades hemsidan ytterligare en gång, denna gång av ”the Kevin Mitnick Liberation Front”. Senare samma år hackades företaget igen då inkräktarna bl a hotade med att sprida privata brev från Telias ledning. Även hackerattacken mot Livets Ords hemsida uppmärksammades i media. Efter den 3:e lyckade hackerattacken på mindre än två veckor gav Livets Ord upp och tog bort sin hemsida från Internet. Under 1997 har Aftonbladet, Kvällsposten, div. skolor och universitet, kristna grupper, NASA, nazistsidan Arisk Kamp m fl blivit utsatta för hackerattacker. (Flashback Hackers Archive, 1996 och 1997)

Världens troligen mest ”ansedda” hackerattack utfördes den 29:e september 1996 av svenska hackers, ”Power through Resistance”, mot CIAs hemsida. Attacken, som hade rubriken ”Sluta

[11] ung. gömd eller dold övervakning

ljug Bo Skarinder", uppmärksammades bl a av CNN. Statsåklagaren Skarinder hade tidigare under samma vecka inlett en rättegång mot fem personer för dataintrång.

4.2.7 Industrispionage med hjälp av datorer

Donald Delaney, avdelningschef för databrott vid polisen i New York State, säger att polisen är inte så bekymrad över okynneshackers som de är över de växande skaran hackers som ägnar sig åt rent industrispionage (Olander, 1997). De sistnämnda är extremt välutbildade dataexperter, ofta från före detta östblocket. De arbetar enligt Delaney för stora företag, organiserade brottslingar och till och med andra länders underrättelsetjänster. Eftersom de är så avancerade lämnar de inga spår efter sig och företaget som blivit utsatt för industrispionaget kanske inte ens upptäcker det. Ett känt exempel på denna typ av industrispionage är då franska säkerhetsagenter hackade sig in i ett system i Indien som innehöll offerter för köp av stridsflygplan till den indiska försvarsmakten. Aktionen resulterade i att Frankrike fick ett rejält övertag i förhandlingarna och fick mångmiljonkontraktet. Särskilt hotade för denna typ av attack är företag som bedriver avancerad forskning och utveckling, såsom läkemedelsföretag och IT-företag.

4.2.8 Virus

Ett datorvirus är ett program som kan kopiera sig själv på andra program. Viruset behöver ett "värdprogram" för att kunna kopiera sig själv. När "värdprogrammet" körs aktiveras viruset. Avsikten med virus är att de skall göra skada.

Det finns en mängd olika virustyper. *Boot sektor virus* är det vanligaste viruset. Det ändrar eller byter ut boot sektorn på en hårddisk, diskett eller CD-ROM. Exempel på denna typ av virus är Stoned och Michelangelo. *Filvirus* infekterar exekverbara filer och körs varje gång som den infekterade filen körs. Exempel på filvirus är Fredag den 13:e. *Multi-delnings virus* infekterar både exekverbara filer och bootsektorer. Namnet kommer från att det sprider sig så snabbt och lätt. Ett exempel på ett sådant virus är Tequila. *Polymorfa virus* krypterar eller förvanskar sin programkod varje gång det infekterar ett nytt objekt. Ingen kopia av viruset ser likadant ut. Viruskoden krypteras med en annan nyckel varje gång och lägger till en liten dekrypteringsrutin som exekveras då den körs. Virus av denna typ är svår att upptäcka. Exempel på detta virus är Whale. *Systemvirus,* som t ex Number of the Beast, fokuserar på systemfiler som är nödvändiga för DOS, kommandofiler är typiska mål för detta virus. *Stealthvirus* undgår upptäckt och eliminering genom att ta till sig en eller flera mekanismer i systemet eller programmet som det har infekterat. Ibland komprimeras den infekterade filen till sin ursprungliga storlek. Stealthvirus som t ex Blah.3385 och Hundered Years är mycket svåra att upptäcka. *Makrovirus* är ett multiplattform virus skrivet i applikationens språk. Detta virus sprids vanligen via Word-dokument. Viruset kopierar sig själv och infekterar data hellre än exekverbara filer. Ett automatiskt exekverbart makro körs som respons på en händelse som t ex öppnande av en fil. Ökända exempel på makrovirus är Atom, Color, Concept, Nuclear och Hot. (Fakta hämtad ur eget specialarbete på kursen Computer Security, 1996)

4.2.9 Makrovirus

Joel McNamara publicerade sin studie 1994 där han visade hur ett makrovirus som han själv skapat fungerade (Sundström, 1997). Sundström menar därmed att McNamara bidrog till att sprida konsten att skriva makrovirus och inspirera andra att försöka göra sina egna. Makrovirusen skapas och sprids med hög hastighet. I början av hösten 1997 påstod det finska företaget bakom F-Prot att det fanns ca 1000 makrovirus i cirkulation.

Användare bör vara medvetna om att när de startar en bat-fil eller ett basic-program så startas ett program som kan utföra flera olika saker i datorn. Vid ett par situationer kan dock användaren vara omedveten om vad för slags program hon/han egentligen startar. En situation är då en textfil matas till bildskärmen via en console driver som reagerar på ANSI-styrkoder. Detta kan utlösa en ANSI-bomb, något som Sundström inte anser är speciellt vanligt längre. En annan situation som är betydligt vanligare numera är då användaren tar in ett dokument i ett ordbehandlings- eller kalkylprogram. Dokumentet kan då innehålla makroprogram som går igång utan att användaren är medveten om det och sedan smittar andra program. Dessa makrovirus är på stark frammarsch. Att makrovirus har fått en sådan utbredning kan bero på att de är plattformsoberoende virus och därför lättare att implementera. Anledningen till att denna typ av virus blivit ”populära” är den utbredning de kan få genom Internet och www.

Tillgången till ett kraftfullt makrospråk innebär vissa säkerhetsrisker. Det går att jämföras med det senaste årets mest populära programmeringsspråk - Java. Java har många fördelar, men då det används som applets på websidor bör dess möjligheter starkt begränsas av säkerhetsskäl.

ShareFun-viruset är exempel på ett wordbaserat makrovirus. Detta virus kontrollerar om användaren har MS-Mail i datorn och är uppkopplad mot Internet. Om dessa villkor är uppfyllda kontrollerar viruset om det finns e-postadresser i adresslistan till Mail och skickar meddelandet: ”You have to see this! Share the fun!” till tre slumpmässigt valda personer i adresslistan. Till meddelandet bifogas ett attachment med det smittade dokument som användaren jobbar med i Word. Då mottagaren öppnar dokumentet i Word smittas även dennes Word-installation. Datorn smittas alltså inte förrän mottagaren öppnar det smittade dokumentet i Word. (Fakta hämtad ur eget specialarbete på kursen Computer Security, 1996)

Ett av de senaste tricken vad gäller makrovirus är att utnyttja den inbyggda krypteringsmöjligheterna som finns i Word och på så sätt låsa dokument för användaren. (Sundström, 1997) Det finns program för att låsa upp Word-krypterade program, men det ställer till med onödigt besvär. Kryptering innebär svårigheter för scanningprogram som måste kunna läsa inuti de krypterade dokumenten för att upptäcka makrovirusen.

4.2.10 Lösenordsattacker

Det finns olika program som gissar lösenord med hjälp av ordlistor. För att utföra attacken behöver hackern administratörsrättigheter och möjlighet att köra ett program som t ex PWDUMP eller komma åt företagets lösenordsdatabas. (Gustafsson, 1997) Hackern erhåller då lösenorden i klartext. Det finns även andra program som läser lösenordsdatabaser och knäcker MD4-algoritmen som ofta används vid krypteringen av databasen. Resultatet kan bli att hackern tar sig in i ett system med hjälp av ett krypterat lösenord.

Russel och Zwicky (1997) beskriver en annan typ av lösenordsattack, som utförs genom att sabotören kör ett program som drar nytta av möjligheten att lyssna av nätet efter IP (Internet Protocol) trafiken på nätverket, en så kallad lösenordssniffare. Genom att t ex fånga upp de första 128 byten för varje FTP eller Telnet sektion som passerar kan lösenordssniffaren lätt plocka ut användarnamn och lösenord när någon skriver in dem. Under 1994 blev ca 100.000 websidor attackerade av lösenordssniffare enligt CERT (Computer Emergency Response Team). Särskilt känsliga för denna typ av attack är nätverk som t ex Ethernet som anses lätt att avlyssna.

4.2.11 Informationsserviceattacker

Ett antal olika servicefunktioner gör att datorer kan dela med sig av information till andra och tillåta användare att lätt förflytta sig mellan datorer. Dessa servicefunktioner utnyttjas för attacker mot systemet genom att få dem att dela med sig av mer information än vad som var avsett eller genom att dela med sig av informationen till andra än det var meningen.

4.2.12 Denial of Service attacker

Det finns två klassiska typer av Denial of Service (ung. nekande till service) attacker, båda är lika förödande när de används på ett nätverk. Den ena typen används för att överskölja systemet eller nätverket med meddelanden, processer, eller nätverksförfrågningar så att inte systemet klarar av att göra något annat än att försöka ta emot det som sänds eller utföra det som begärs. Resultatet blir att inget kan utföras alls. Den andra typen av attack slår ut eller stänger av all utrustning eller service. Attacken utförs genom att sabotören skickar ett ICMP meddelande till en värd eller router och säger åt den att upphöra att sända paket till alla delar av nätverket. Tyvärr är det så att så länge företaget vill kunna ta emot e-post, paket eller telefonsamtal är det möjligt att arrangera en ”översvämning” på systemet eller nätverket. Dessa typer av attacker är dock, enligt Russel och Zwicky, oftast lätta att spåra vilket gör det riskfyllt för den som utför attacken.

Ett exempel på en Denial Of Service-attack (DNS-attack) var då de två författarna, Josh Quittner och Michelle Slatalla, utsattes för en ”e-post-bomb” hösten 1994. Aktionen var, skriver Russel och Zwicky, en hämnd för en artikel de skrivit i tidningen Wired om hackarkulturen. Någon bröt sig in på IBM, Sprint, och författarnas nätverksanslutning och ändrade program så att författarnas e-post och telefonkommunikation avbröts. En störtvåg av e-post sköljde över deras nätverk så att andra meddelanden inte kunde komma fram. Till slut bröt deras Internetanslutning samman fullständigt. Även telefonlinjerna omprogrammerades så att de som försökte ringa författarna istället hamnade utanför delstatsgränsområdet och fick lyssna till obscena inspelningar.

Det finns flera olika varianter av DNS-attacker som tidigare har varit vanliga i UNIX-miljö på Internet, men nu även i NT-miljö. Attacken går ofta ut på att hänga en maskin genom att via Internet sända ett ”Out-of-Band-paket”[12] till maskinen. Maskinen blir då obrukbar tills den startas om, men hackern får inte tag på någon information. Hackern använder program som har spridits via Internet. Programmen utför automatiskt attacken och kräver ingen större kunskap för att användas. Allt som krävs är att hackern kompilerar källkoden, kopplar upp sig via Internet på den maskin som skall attackeras och sedan köra programmet. Programmet skickar t ex en sträng till port 139 och påverkar efter mottagandet en drivrutin för TCP/IP-stacken med resultatet att maskinen hänger sig. (Gustafsson, 1997)

4.2.13 IP attacker

Varje gång en användare kopplar upp sig mot Internet tilldelas denna en tillfällig IP-adress för sejouren. Det är till den adressen som information skickas. Servern behöver dessutom veta vilka typer av filer som användarens browser kan hantera, vilket abonnemang som utnyttjas, användarens e-postadress, vilket operativsystem användarens dator har, hårddiskens namn, vilka filer användaren söker och tar osv. Uppgifterna sparas i loggfiler på de olika serverdatorerna som användaren besökt. Vid ytterligare besök tillfogas de nya uppgifterna till de gamla.

[12] ung. för stora paket

Sabotörer drar ibland nytta av denna sällan använda möjlighet - ”the source routing option” - i IP huvudet av paket som sänds över Internet. Även system som skyddas av brandväggar har fallit offer för denna typ av attacker. En annan typ av IP attack är då sabotören skapar paket med falsk IP-adress (Shimomura, ur Russel och Zwicky, 1997). Denna typ av attack är tekniskt mer avancerad eftersom sabotören måste gissa sekvensnummer associerade med nätverksförbindelser mm. Sabotören får ingen respons på att attacken fungerade, men gör den det kan den ställa till med stor skada.

4.2.14 Cookies

När en användare kontaktar vissa servrar skickas en liten loggfil med från servern till användarens browser. Loggfilerna kallas för cookies (kakor) och används för att övervaka användarens aktiviteter, t ex vilka websidor som besöks och vilka filer som användaren hämtar hem. En cookie lagras på den egna datorn till skillnad från loggfilen. Denna möjlighet kan missbrukas på ungefär samma sätt som IP-adressen. (Internetguiden, nr.6, 1997)

4.2.15 Dödspinget

Vissa system är känsliga för det så kallade dödspinget (Kullmar, 1997). Detta är ett ping som kan skickas från en dator med Windows 95 och som är större än det får vara. Dödspinget resulterar i att datorn kraschar eller hänger sig.

4.2.16 Anonym inloggning

Ett serverprogram som släpper in utomstående på företagets IT-system medför en mycket stor säkerhetsrisk. För att demonstrera hur farligt det är med anonym inloggning utvecklades programmet ”Red button”. (Gustafsson, 1997) Programmet används numera av hackers. Hackern startar programmet på sin dator och attackerar servarna i det lokala nätverket eller via Internet. Det enda programmet frågar efter är namn och IP-adress på måldatorn, resten sköts automatiskt. Programmet skriver ut information, bl a namnet på administratörens konto, som det hämtat från den attackerade servern.

Det finns många fler exempel på attacker mot IT-system, det är egentligen bara sabotörens kunskap och fantasi som sätter stopp om han eller hon är ute efter att skada ett företag.

4.3 Oavsiktligt orsakade incidenter

Det är inte enbart illasinnade personer som åstadkommer förödande effekter på företags IT-system och information. Enligt Caelli, Longley och Shain (1989) beror 80% av säkerhetsbrotten på misstag eller försummelse och inte avsiktligt bedrägeri.

4.3.1 Hemlighålla information

Utvecklingen inom IT sker mycket snabbt och det är inte alltid dokumentation och säkerhetsaspekter hänger med. Det händer att information förloras, modifieras eller avslöjas helt oavsiktligt i samband med PC-användning. Information kan exempelvis gå förlorad om backup-rutinerna inte fungerar som de skall. Det är vidare lätt hänt att t ex ett finger slinter på tangentbordet och inkorrekt data därmed förs in i systemet. Systemet kan innehålla gammal, vilseledande eller motstridande information eftersom det ibland inte finns några regler eller rutiner för att undvika detta. Det kan skapa stor förvirring då uppgifter strider mot varandra. Utlämnande av information inom organisationen eller nedsmittande av lagrad data kan drabba företaget då det inte finns tillräckliga accesskontroller. Otillräcklig kommunikationssäkerhet kan vara orsaken till att information utlämnas under överföring. (Pfleeger, 1989)

Säkerhet förknippas ibland med sekretess och hemlighetsmakeri. Att hemlighålla sekretessbelagd information har lite av James Bond-känsla över sig och anses som spännande. Men det hjälper föga att hemlighålla informationen om den inte är korrekt eller tillgänglig för den som behöver den. Om inte datan som förs in i systemet är korrekt så är den ju inte värd att skydda inne i systemet. Den mesta informationen i företag är dock inte hemlig, däremot kan den vara väldigt viktig för företagets verksamhet. Skulle sådan information försvinna eller modifieras på något sätt, kan det innebära att verksamheten hindras.

4.3.2 Vanligaste orsaken till utebliven produktivitet

Enligt en svensk undersökning av Rinfo Research på uppdrag av Cap Programator var den vanligaste orsaken till utebliven produktiviteten, bland personer som använder datorer i sitt yrke, att hjälpa sina kollegor då de fått problem med sina datorer (Nilsson, 1996). Näst vanligaste orsaken var att vänta på utskrifter från skrivare som inte fungerade som de skulle, sedan följde orsaker som att vänta på hjälp och hantera problem med den externa kommunikationen. Övriga problem som framträdde i undersökningen var vid konvertering mellan olika program och programversioner, svårighet att nå information i de centrala registren, problem med e-post, virus och uppkoppling till arbetsplatsen.

4.3.3 Svenska företags beredskap

Cardholm (1997) skriver i en artikel om en undersökning, utförd av IMU/Testologen, av de börsnoterade bolagen i Sverige under hösten 1996. Undersökningen visade att 49% av de börsnoterade företagen i Sverige saknade en skriven policy för IT-säkerhet. Detta trots att 43% hade varit med om minst ett avbrott under de senaste två åren. 52% av de undersökta företagen saknade helt en avbrottsplan och 39% av företagen hade inte bedömt följderna av en katastrof.

4.3.4 Avbrott

Ett IT-avbrott eller datorkrasch betyder att datorn avbryter alla pågående aktiviteter och stänger användaren ute. Andra uttryck för samma sak är att datorn ”låser sig” eller ”hänger

sig". Detta är exempel på interna krascher, dvs utan yttre påverkan. En sådan krasch uppstår då ett fel inträffar på en server eller servern helt "går ned". Wedberg (1997) påpekar att ett avbrott i IT-systemet medför konsekvenser i verksamheten såsom att tillgängligheten störs, att de anställda inte kan utföra sina arbetsuppgifter osv. Ett längre IT-avbrott kan orsaka stora produktionsstörningar och ett allvarligt ekonomiskt avbräck för företaget.

4.3.5 Installeringsproblem

Misstag kan ske redan vid installeringen av hård- och mjukvara. Felen kan bero på flera faktorer såsom att instruktionerna upplevs som svåra, anvisningar är otydliga eller att installatören får problem med språket i installationsanvisningarna. Om installationsanvisningarna är svåra eller otydliga att förstå kan den person som installerar göra feltolkningar eller bli så frustrerad att hon/han helt enkelt struntar i anvisningarna och gör som hon/han anser är det logiska sättet att fullgöra uppgiften på. Många mjuk- och hårdvaror som säljs idag har manualer och anvisningar på engelska. De flesta svenskar är utmärkta på det engelska språket, men tekniska anvisningar som innehåller engelska facktermer kan vara svåra att förstå och därmed följa.

4.3.6 Milleniumbomben

Under systemutvecklingsfasen kan också misstag ske. Ett uppmärksammat designfel är den så kallade Milleniumbomben. Med Milleniumbomben avses den relativt vanliga företeelsen att årtal skrivs med två siffror istället för fyra, vilket ställer till problem vid det förestående milleniumskiftet då 00 inte logiskt följer på 99. (Gustafsson, 1998) Anledningen till att systemutvecklare har valt att skriva årtal på detta vis är dels för att underlätta för användaren av programmet, dvs att bara behöva skriva in två siffror istället för fyra, dels för att spara utrymme på skärmen.

Såväl statliga myndigheter som företag i Sverige är dåligt förberedda inför skiftet till 2000-talet menar Jan Freese, före detta chef för bl a datainspektionen. Allt med en klockfunktion som innehåller datum måste anpassas för att inte bryta samman den 1 januari år 2000. (Gustafsson, 1998) Det råder stor aktivitet med att ändra i alla program som innehåller någon form av datumfunktion. Förutom datorer gäller anpassningen inbäddade system i kortläsare, hissar, vatten- och värmepumpar m fl. Trots att det nu är mindre än två år kvar till år 2000 finns det fortfarande företag som inte har anpassat sina system.

Riksförsäkringsverkets generaldirektör, Anna Hedberg, krävde i början av januari 1997 att alla riksdagsbeslut som avser förändringar i socialförsäkringarna före år 2000 skulle stoppas för att verket skall ha en möjlighet att anpassa systemet. (Gustafsson, 1998) Om inte full omställning sker kan det innebära att nyfödda får pension och pensionärer barnbidrag. Freese har varnat för problemet i över 10 år, utan att bli uppmärksammad. Omställningskostnaderna beräknas kosta närmare 200 miljarder kronor.

4.3.7 Förlust av filer

Användare spenderar en hel del tid med att hantera problem med sina datorer. Filer som försvinner är ett vanligt problem som grundar sig i att användaren inte har klart för sig hur datorn är uppbyggd och hur nätverkets struktur ser ut. Felet ligger ofta i att de sparar utan att veta var filerna hamnar. Nästa gång kanske användaren öppnar i en annan katalog eller enhet och hittar då inte den/de filer som de söker. Vissa namn är skyddade och då användaren sparar en fil med felaktigt namn kan den filtreras bort av programmet användaren använder.

Även om de flesta program blivit mer toleranta vad gäller filändelser är det möjligt att spara filer med felaktiga eller utan filändelser. Detta kan medföra att de inte syns i ett annat program med normal inställning. Det kan även bli problem med åtkomsten om filen sparats i en senare version av programmet än den som användaren försöker öppna filen i. Det händer till och med att filer oavsiktligt raderas av användaren själv. (Westman,1997)

Det går oftast att hitta eller återskapa försvunna eller raderade filer, men de tar tid att hitta och är en källa till irritation och kostar dessutom företaget pengar i utebliven arbetsinsats och medför stopp i verksamhetsflödet.

4.3.8 Kompatibilitetsproblem

Det kan vara ett problem att få programvara att fungera tillsammans i olika datorer (t ex mellan en IBM och en Macintosh). Sveriges nya transaktionssystem för kortbetalning via Internet kan endast användas av PC som har programvaran Windows 95. (Wickberg, 1997) Detta ställer givetvis till problem för de företag som har Macintosh-datorer och önskar utnyttja tjänsten. Likaså kan det vara ett problem med olika versioner av program som då kräver konverteringar. Att konvertera från en äldre version till en nyare är oftast inga problem, men äldre versioner klarar inte alltid att ta emot en ny version.

4.3.9 Minskad kontroll över systemen

Då persondatorn slog igenom, förlorade datoravdelningen mycket av sin kontroll i och med decentraliseringen som följde. (Westman, 1997) De lokala näten har medfört att det blivit en vana att lagra viktig information på servrar och ta backup från dem. Decentraliseringen har dock utökats än mer i och med distansarbetare, bärbara datorer, e-post och Internet. Datoravdelningen har därmed i mångt och mycket förlorat kontrollen över systemen.

Bärbara datorer är ett stort problem enligt säkerhetskonsulten Roger Gustafsson (Westman, 1997). När de är kopplade till företagets dator kan de uppdateras och kontrolleras, men säkerhetskopieringen blir ofta lidande. Ett annat problem med bärbara datorer är, liksom i anekdoten om general Schwarzkopf (se sidan 24), att personalen tar med sig information ut från företagets skyddande väggar. Det händer att personal tar med datorerna hem och låter barn och anhöriga använda dem. En person med nyckelposition i företaget kan ha riktigt känslig information i sin dator såsom företagets strategier, offerter, kunder, konkurrenter osv. Om sådan information finns på en bärbar dator är den naturligtvis mycket svårare att skydda.

5. Skydd och lösningar på IT-säkerhetsproblem

5.1 Övergripande åtgärder för intern säkerhet

Det finns egentligen inga helt säkra skydd mot förlust av information. Luckorna i systemet finns där, det är enligt Cardholm (1997) bara en fråga om tid innan någon upptäcker dem och utnyttjar dem. Företagen har ett visst skydd av lagen, men viktigast är ändå att försöka ligga i fas med utvecklingen. Cardholm menar att svenska företag är dåligt medvetna om de hot som finns mot deras information. Ett steg i utvecklingen för säkrare svenska företag är därmed att öka medvetenheten om IT-säkerhet.

5.1.1 Begränsning av tillgängligheten

Det finns en hel del företaget kan göra för att skydda sin information mot hackers, industrispionage och ohederliga medarbetare. Hans Skalin (1997) anser att företaget bör utgå ifrån att inga användare skall få komma åt någon resurs överhuvudtaget, först därefter lättas säkerheten så långt som krävs för att användarna skall ha nödvändigt stöd för att kunna utföra sina arbetsuppgifter. Givetvis bör de säkerhetsfunktioner som finns i nätverksoperativsystemet och applikationer användas, därefter kan säkerheten byggas på och användarnas möjligheter begränsas genom exempelvis en brandvägg mellan nätet och ingångarna.

5.1.2 Ansvar för informationstillgångarna

Information är en tillgång och bör behandlas som en sådan. Tillgångar har alltid ett visst värde som företag ofta förbiser. I budgetar tilldelas de olika ansvarsenheterna en viss summa, ofta ned till en mycket detaljerad nivå. Enligt Caelli, Longley och Shain (1989) bör ett liknande system göras över informationen, dvs. bestämma vem viss information tillhör. Detta sker på ett praktiskt plan genom att tilldela ansvar för information, klassificera data, samt upprätta regler för skapande, dubblering, överföring, förvaring och radering av data.

5.1.3 Säkerhetsmatriser och zonindelning

Wedberg (artikel 2, 1997) skriver att för att undvika att information blir som en stor massa, kan olika typer av information ges olika status, betydelse- och sekretessgrad. För att kunna dela upp informationen måste man veta vad som är värt att skydda och vad som är mindre viktigt.

För att hindra personalen från att ta sig friheter bör det finnas goda designprocedurer och rutiner som förhindrar lokala systemegenheter och som främjar bra dokumentation. Detta, tillsammans med goda personalrutiner, både vad gäller att skapa en positiv attityd till företaget och säkerhetsarbetet som att begränsa tillfällen för brottslig aktivitet, bidrar till att göra IT-systemet säkrare. Caelli, Longley och Shain, (1989) anser att företaget bör hålla operativ och expertispersonal åtskilda och att en ”need-to-know”-förhållning bör hållas strikt vad gäller säkerhetsrutiner. Detta förfarande kan dock orsaka merkostnader, mindre flexibilitet och självständighet på IT-avdelningen.

IT-området är mycket omfattande och därmed även säkerhetsaspekterna på IT. Säkerhetsarbetet går främst ut på att säkra företags integritet och försvara eller förhindra attacker mot företagets information och utrustning. Kluwer har gjort en schematisk bild över

datasäkerheten, där han delat in försvaret av företagets integritet i olika försvarszoner och hoten i professionella och ”deltidsarbetande” bedragare.

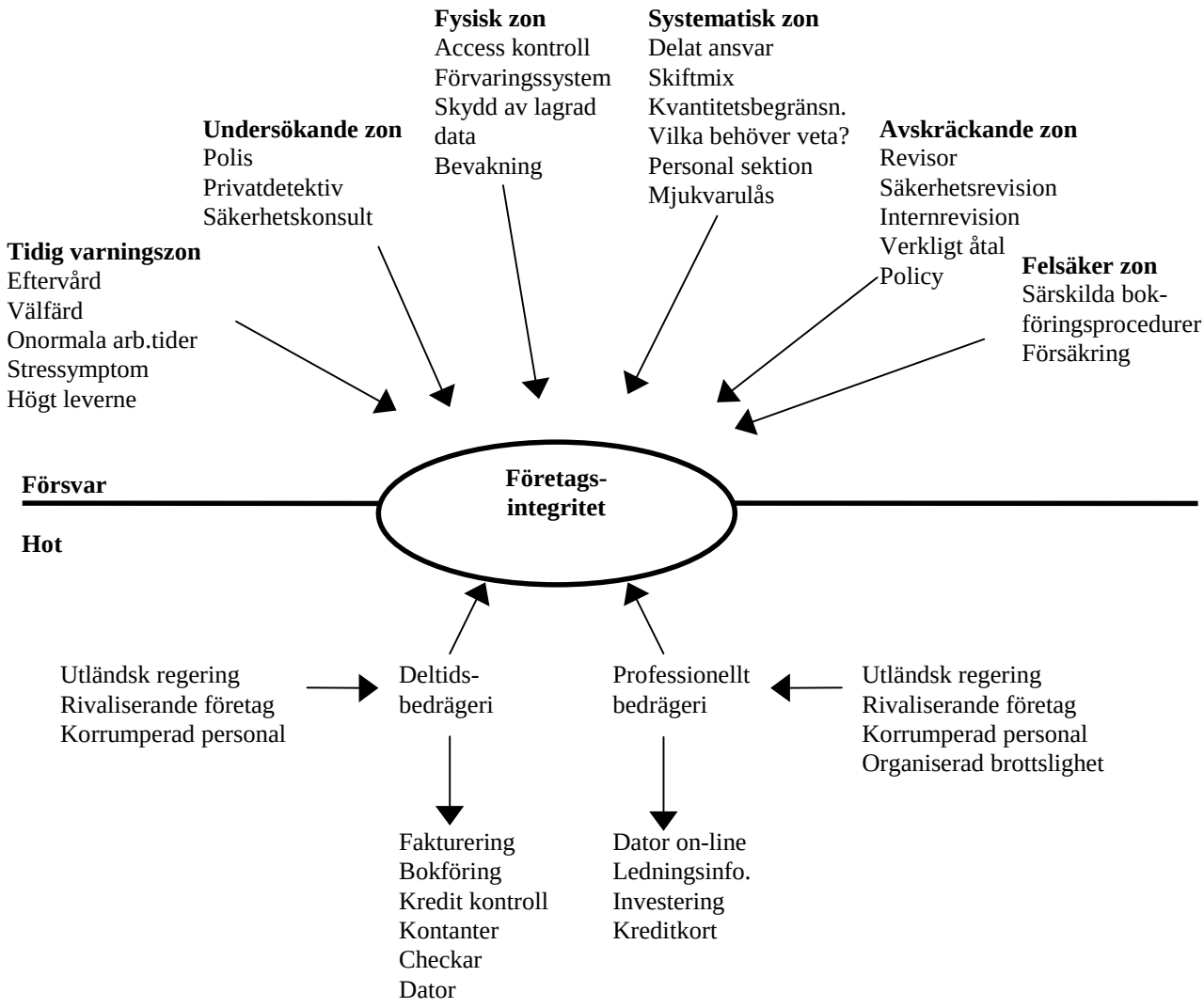

Bild 5.1 Schematisk översikt av datasäkerhet (Handbook of Security, Kluwer)[13]

För att erhålla god säkerhet bör det finnas en viss ordning i systemet. För att få bättre ordning i systemet kan en överskådlig säkerhetsmatris upprättas. En säkerhetsmatris har olika typer av information längs ena axeln och personal på den andra. Exempel på olika informationstyper kan vara kundregister, löneregister, strategiska planer, offerter mm., personalkategorier kan vara ekonomiavdelning, ledning, säljare osv. Chefen över säkerheten och eventuellt några andra bör finnas med på personalaxeln som enstaka individer. Därefter bestäms vilken information som respektive personalkategori/person skall ha rättigheter till. Rättigheterna delas ofta upp i läsa, skriva, radera och ändra. Det underlättar om matrisen överensstämmer relativt väl med filrättigheterna i operativsystemet.

För att göra det hela enklare kan personalkategorierna och informationstyperna delas in i olika zoner. Med zonindelning menas att olika delar av datorsystemet och personalen är separerade.

[13] sid 2, Caelli, Longley och Shain, 1989, (egen översättning)

Denna matris kan sedan fungera som ett stöd för såväl teknisk som annan personal. Hur säkerhetsmatrisen och zonindelningen ser ut beror naturligtvis på företagets verksamhet, storlek mm. Matrisen fungerar även som en dokumentation över företagets säkerhetstänkande.

Zonindelningen kan med fördel användas även för information i databaser, filer på servrar och arbetsstationer, samt websidor. Riktigt viktig information kanske inte skall gå att nås via nätverket alls utan finnas på en fristående dator på en säker plats.

5.1.4 Elementen i ett säkert operativsystem

I kontruktionen av ett säkert operativsystem ingår åtgärder både för att förhindra och upptäcka incidenter som kan skada företagets integritet. I de förhindrande åtgärderna ingår kontroll av access, isolering och identifiering. I den upptäckande delen ingår övervakningsfunktioner.

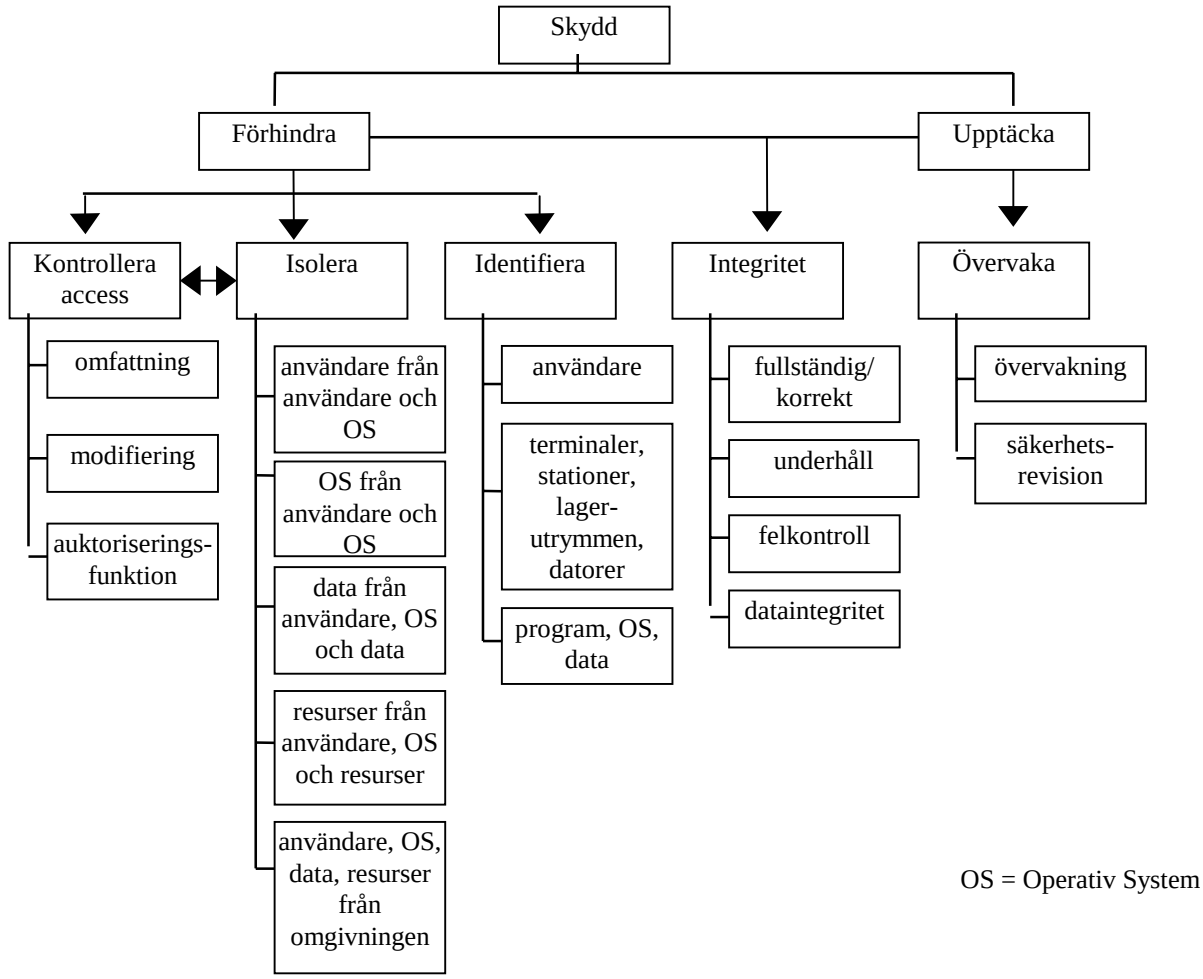

Bild 5.2 Elementen i ett säkert operativ system.[14]

5.1.5 Fyra grundläggande osäkerhetstyper

Enligt Kowalski finns det fyra grundläggande osäkerhetstyper: naturlig, social, teknisk och övernaturlig osäkerhet. Naturlig osäkerhet kan vara osäkerhetsfaktorer som jordbävning,

[14] sid. 80 i Caelli, Longley och Shain, 1989 (egen översättning)

översvämning, och andra naturkrafter. Social osäkerhet syftar till osäkerhet i samband med kontakt med andra människor, dessa människor kan ha goda eller onda avsikter. Teknisk osäkerhet innebär att vi är beroende i många fall av ting som kan bryta samman vid oväntade tillfällen. Övernaturlig osäkerhet är det ogripbara som endast är med för den holistiska bilden.

Tägil (1977)[15] poängterar att det viktigaste i kombinationen av sociala och tekniska förändringar är att båda elementen skall ges lika uppmärksamhet. Teknologin eller samhället bör inte studeras var för sig, istället bör relationen mellan dem och deras dynamik vara föremål för studierna.

5.1.6 Skyddslagren kring informationstillgångarna

Säkerhetsarbetet bör inkludera såväl det fysiska som det logiska skyddet av IT-systemet. Det är inte svårt att förstå betydelsen av att skydda datorer och dess innehåll mot rent fysiska hot såsom stöld, brand eller annan åverkan, men att dessutom skydda informationen logiskt är inte lika självklart. (föreläsningsanteckningar, Computer Security, 1996)

IT-säkerhet involverar både skydd av information och den utrustning som krävs för att överföra och använda informationen. Det finns fem grundläggande faktorer som bör tas hänsyn till i upprättandet och underhållet av säker information. Dessa faktorer kan illustreras som ringar på vattnet kring informationstillgången som skall skyddas.

Ytterst finns det rent fysiska skyddet som placeras kring byggnader och datorer. Skyddslagret innanför det fysiska lagret är accesskontroller som hindrar obehöriga från att ta sig in i företagets system. Innanför det andra lagret återfinns administrativa kontroller och procedurer som hindrar dem som redan är inne i systemet från att missbruka det. Därefter kommer beredskapsplanen ifall att något ändå skulle hända. Förutom de fyra skyddslagren bör ett fullgott försäkringsskydd finnas för att företaget skall ha ett ekonomiskt skyddsnät ifall alla de andra skyddslagren skulle misslyckas.

[15] ur Kowalski, 1994

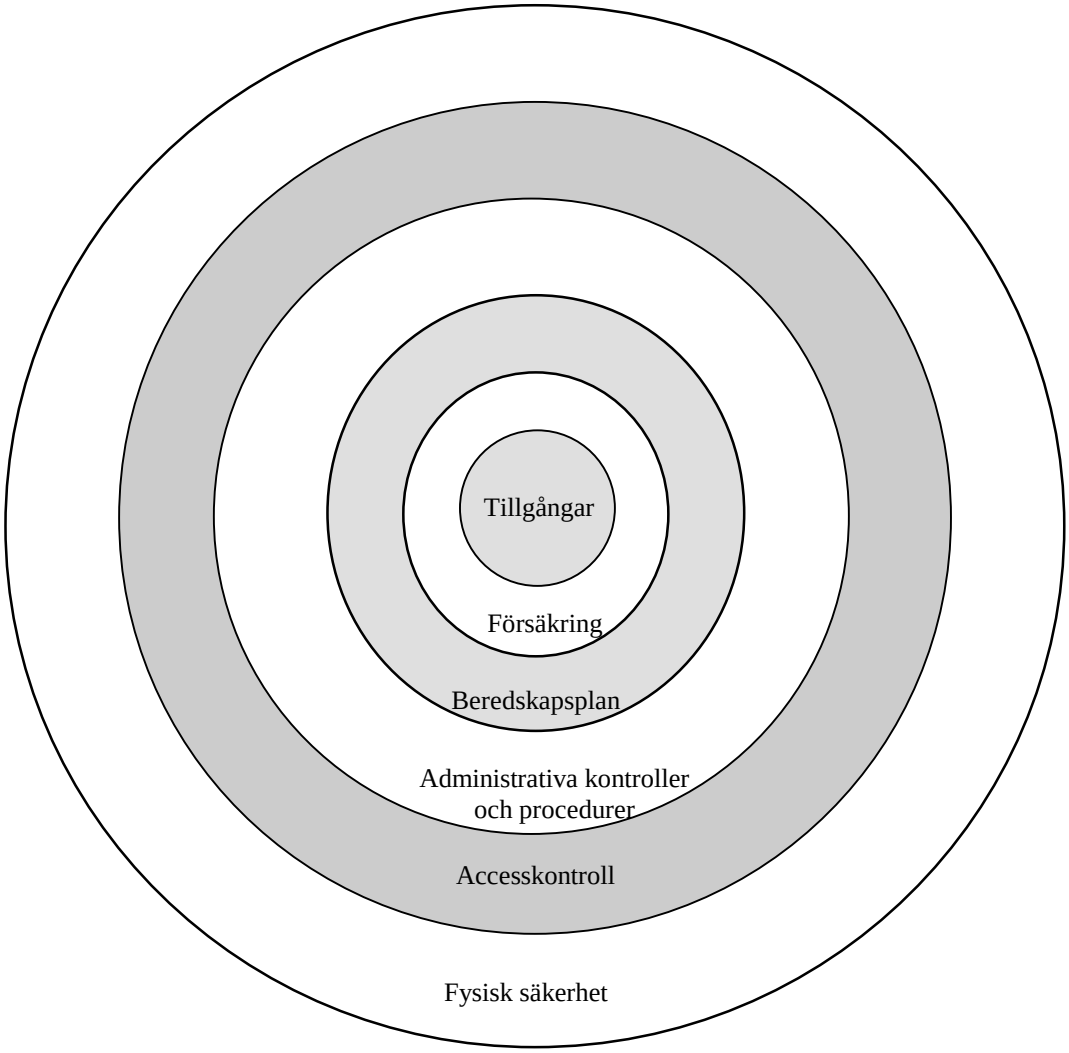

Bild 5.3 Skyddslagren kring informationstillgångarna.

5.2 Faktorer för den fysiska säkerheten

De grundläggande faktorerna i fysisk säkerhet kretsar kring byggnaden, placering av datorcentralens placering, brand, vattenskada, intrång i fastigheten och avlyssning av elektromagnetiska signaler.

5.2.1 Säkra byggnader

Det finns en hel del att ta med i beräkningarna vid nybyggnation eller ombyggnad av företagets fastigheter. Vid nybyggnation bör hänsyn tas till brandsäkerheten, det finns brandsäkra byggnadsmaterial att tillgå för de flesta byggnadssyften. Vid en brand kan det bildas gaser såsom den giftiga gasen PCB från brinnande elektrisk utrustning och detta bör personalen uppmärksammas på anser Caelli, Longley och Shain (1989). För att varna vid fara bör övervakning och alarm installeras för brand, inkräktare, vatten mm. Det bör finnas någon form av evakueringsplan samt skyltning om vad som skall göras i olika nödsituationer. Personalen måste lätt kunna komma ut ur byggnaden ifall en olycka skulle inträffa, därför skall nödutgångar, in- och utgångar vara klart markerade.

Det bör finnas någon form av yttre skydd runt företagets faciliteter såsom en mur eller inhägnad för att hålla ute obehöriga. Ibland behöver företag ha serviceenheter utanför de egna faciliteterna för exempelvis nedkylnings- och luftkonditioneringsanläggningar eller dra el- och kommunikationkablar genom delade utrymmen. Givetvis bör dessa också ges någon form av skydd.

5.2.2 Brand

En brand kan vara förödande för vilket företag som helst, därför är det viktigt att beredskapen för en brand är hög. Förutom i byggmaterialet bör även inredning väljas i brandsäkra material. Givetvis bör det finnas brandlarm och brandsläckare utplacerade i byggnaderna. (Folksam, 1997) Dessutom bör all personal ges utbildning och klara instruktioner i händelse av brand.

5.2.3 Placering av datorcentralen

Vattenskada är det vanligaste försäkringsanspråket för datorcentraler. (Folksam, 1997) Orsaker till vattenskador kan vara brustna vattenledningar, blockerade avlopp, översvämning efter t ex regnoväder, höjda nivåer på närliggande vattendrag, brandbekämpning med vatten, läckande tak, utlösta vattensprinklers mm. (Caelli, Longley och Shain, 1989) För att förhindra denna typ av skada bör företaget tänka på att placera datorcentralen ovan marknivå, att ha vattendetektorer under golvet, att inte ha vattensprinklers mm.

Det finns en mängd faktorer att ta hänsyn till vid placeringen av datorcentralen för att det skall vara så skyddat som möjligt. Förutom att undvika att placera datorcentralen under marknivån, bör företaget inte peka ut placeringen av datorcentralen, t ex genom att sätta upp skyltar. Företaget bör vidare tänka på tillgänglighet till datorcentralen, dvs vem som skall ha tillträde och hur obehöriga skall hållas borta. Vid planeringen för placeringen av datorcentralen bör även tillgången till telekommunikationskanaler och kraftkällor tas hänsyn till, samt reservkällor vid t ex ett strömavbrott. (Caelli, Longley och Shain, 1989)

5.2.4 Avlyssning

Det är fullt möjligt att med hjälp av modern teknik få tag på ett företags hemliga information utan att kliva in genom dörren eller hacka sig in i företagets IT-system. De elektromagnetiska signaler som bildskärmar och tangentbord sänder ut vid användning kan plockas upp och projekteras på en bildskärm långt därifrån. (Olander, 1997) Bästa skyddet för sådan avlyssning är att ha isolerade rum där IT-behandlingen sker och absolut inte placera datorer i närheten av fönster.

Dessutom bör inte magnetiska eller elektriska fält tillåtas komma i närheten av disketter eller magnetband eftersom de kan raderas om de befinner sig tillräckligt nära källan. Även om det magnetiska eller elektriska fältet befinner sig några decimeter bort kan det orsaka att informationen blir oläsbar. (Pfleeger, 1989)

5.2.5 Intrång

Möjligheterna för obehöriga att ta sig in i företagets faciliteter bör begränsas så långt det går. Byggnaderna kan bevakas med t ex övervakningskameror, infraröda strålar, sensorer för rörelse, ljud, värme eller vibrationer. (Caelli, Longley och Shain, 1989) Även ledningar och kablar till såväl övervakningsenheter som datorer bör också skyddas. För att skydda företaget mot intrång bör alla öppningar, dvs dörrar och fönster, vara av robust material liksom dess karmar samt naturligtvis vara säkrade genom lås och liknande. (Folksam, 1997)

Försäkringsbolagen har ofta detaljerade anvisningar för hur företaget skall vara utrustat för att försäkringen skall gälla.

5.2.6 Godtagbart inbrottsskydd

Försäkringsbolagen sätter upp kriterier för vad som räknas som ett godtagbart inbrottsskydd. Det finns vissa kriterier som gäller för de flesta bolag. Försäkringslokalens omslutningsytor skall i sin helhet ge ett, efter förhållandena, godtagbart skydd mot inbrott och göra det svårt att föra bort stöldgods. Med omslutningsytor menas väggar, golv, tak, dörr- och fönsterenheter samt lås- och reglingsanordningar. (Folksam, 1997)

Golv, tak och väggar måste uppfylla vissa kvalitetskrav för att vara godtagbara. Vad som inte är godtagbart är svaga eller tunna konstruktioner av träpanel, korrugerad plåt, plast eller byggskivor, detta gäller även för innerväggar som utgör en del av omslutningsytan.

Dörrar, portar och luckor måste också vara av stabil konstruktion och i bra skick. De måste vara utförda så att varken hela partier, delar och fästdon utan avsevärd svårighet kan demonteras från utsidan. De måste också vara väl förankrade i väggkonstruktionen så att det inte uppstår någon svikt mellan väggen och karmen. De säkraste dörrarna är de inbrottsskyddande dörrar som är märkta enligt svensk standard. Ståldörrar, brand- och arkivdörrar samt massiva trädörrar med stålförstärkning, ger också ett bra skydd. Glasdörrar bör undvikas, särskilt på undanskymda platser. (Folksam, 1997)

Fönster och glasväggar måste vara i bra skick och vara utförda samt monterade så att de inte utan avsevärd svårighet kan demonteras från utsidan. Öppningsbara fönster skall vara stängda och invändigt reglade. Då fönster är belägna nära marknivå bör de dessutom vara låsta med godkända fönsterlås. Fönster till stöldbegärlig egendom, såsom IT-utrustning, skall särskilt skyddas med inkrypningsskydd för att undvika att ersättningen reduceras vid en så kallad smash-and-grab. Även ventilationsfönster, brandventilatorer och andra öppningar skall skyddas.

Låsenheter för dörrar, portar och luckor måste vara godkända. Med godkänd låsenhet menas att låshuset har spärranordningar som tillhållarlås eller dubbelcylinder (nyckel används från både in- och utsida) och nödvändiga tillbehör. Dessutom måste det finnas slutbleck och godkända dörrförstärkningsbehör. För låsning med hänglås och beslag skall även de vara godkända av försäkringsbolaget. (Folksam, 1997)

Företaget bör även samråda med räddningstjänsten när det gäller låsning av utrymningsvägar så att personsäkerheten inte äventyras.

5.3 Accesskontroll

Accesskontroller förhindrar att personer inom företaget får information de inte har rätt till eller att lagrad data smittas ned. Westman (1997) menar att de automatiska accesskontrollerna är att föredra, eftersom de ger företaget en garanti för att kontroll sker varje gång till skillnad från de manuella som kräver åtgärder av användarna. Caelli, Longley och Shain (1989) delar upp accesskontrollerna i tre olika typer; fysisk, kommunikations- och logisk kontroll.

5.3.1 Fysisk accesskontroll

Den fysiska accesskontrollen syftar till att skydda fysiska komponenter av informationsprocessen eller lagringsmedia. Rum med datorer eller datorutrustning såsom magnetiska band, disketter, CD-ROM mm bör skyddas med vakt eller lås.

5.3.2 Kommunikationsaccesskontroll

Accesskontroll med avseende på kommunikation syftar till att skydda informationsprocessystem och dess lagrade data som nås via kommunikationslänkar. Kommunikationslänkarna är sårbara för hackers som vanligtvis arbetar över modem via telenätet. (Skalin, 1997)

I den finansiella världen är pengar och information nästan synonyma. Utbytet av finansiella tillgångar utförs genom utbyte av meddelanden över datakommunikationslänkar. Denna typ av utbyte gör att de som utför transaktionerna måste vara absolut säkra på att transaktionerna är helt skyddade. (Caelli, Longley och Shain, 1989) Kommunikationssäkerheten bör vara så hög att det inte sker någon form av utlämning av information under överföring.

5.3.2.1 Säkerhetslösningar för Internet

Det finns ingen universallösning på säkerhetshoten från Internet, så för att uppnå god säkerhet krävs en rad strategier och tekniker. (Russel coh Zwicky, 1997) Varje dator bör säkras var och en för sig. De ansvariga bör hålla sig á jour med nyheter om såväl eventuella säkerhetsluckor som försvar mot dem. Det viktiga är att försöka få systemet så säkert som det är möjligt.

5.3.2.2 Hemsidor

Företagets hemsida bör kontrolleras regelbundet efter modifikationer, eftersom just hemsidor är tacksamma och populära måltavlor för hackers. (Flashback Hackers Archive, 1997) Finner man att en attack kan ha ägt rum mot hemsidan bör hela systemet, som kan nås via yttre kommunikationslänkar, genomsökas och all aktivitet spåras eftersom hackern kan ha kommit vidare in i systemet.

Websidan kan skyddas mot anonymt tillträde genom installation av t ex Platform for Privacy Preferences (eller P3). P3 fungerar som ett handslag mellan browsern och websidan för att användaren skall ges tillträde (Personal Computer World, sept. 1997). Det kräver att användaren fyller i ett elektroniskt formulär med personlig information och preferenser som browsern automatiskt skickar till websidan vid förfrågan. Det kan vara bra ur säkerhetssynpunkt för företaget att veta vem som söker tillträde till hemsidan, men att fylla i formulär är inte alltid så populärt ur användarens synvinkel.

5.3.2.3 Motringning

Då någon ringer utifrån för att ansluta sig till nätverket bör det finnas vissa säkerhetsnivåer att passera. Först och främst skall användaren vara godkänd att ringa till systemet och eventuellt utförs en motringning. En motringning verifierar varifrån användaren kopplar upp (Höijer, 1997). Bibliotek som skall kunna nås av Internetanvändare bör också tilldelas olika säkerhetsnivåer.

Lösningen på problemet med anonym inloggning kan vara att installera ett IP-filter eller brandvägg som kan stänga ute all trafik från Internet till portarna UDP 137, 138 och TCP 139 (Gustafsson, 1997).

5.3.2.4 Brandväggar

Det har talats mycket om brandväggar under de senaste åren och tilltron till brandväggens förmåga att stå emot attacker framstår som stor. Visst är det bra att ha en brandvägg, och visst ökar brandväggen säkerheten, i alla fall om den satts upp och installerats på ett genomtänkt sätt, men helt säkert kan man aldrig känna sig. (Skalin, 1997)

En brandvägg används främst för att begränsa accessen mellan det interna nätverket och Internet. Den kan också användas för att separera två eller flera delar av det lokala nätverket, t ex mellan ekonomi och forskning. (Russel och Zwicky, 1997)

En brandvägg är helt enkelt en dator med programvara och kan beskrivas som ett hål in i ett nätverk, varigenom data passerar mellan företagets omvärld och det interna nätverket. Ibland har brandväggen även ett tredje gränssnitt mot andra resurser som FTP-, www-, eller mailservrar. Detta tredje gränssnitt kallas för den demilitariserade zonen (Skalin, artikel 2, 1997). Denna demilitariserade zon är ett extra lokalt nät som enbart kan nås via brandväggen. Anledningen för en sådan är att undvika belastning av trafik utifrån på det interna nätet. Genom det tredje gränssnittet kan företaget även erhålla bättre säkerhet på det interna nätet samtidigt som det blir enklare att till exempel ge utomstående tillgång till en webserver.

Brandväggen kan placeras på olika ställen i systemet. För att även surfarnas aktiviteter på det interna nätet skall kunna övervakas, placeras www-servern innanför brandväggen. Brandväggen kan också placeras i en demilitariserad zon, för att på ett enklare sätt lösa säkerheten och på så vis slippa onödig trafik på det egna nätet.

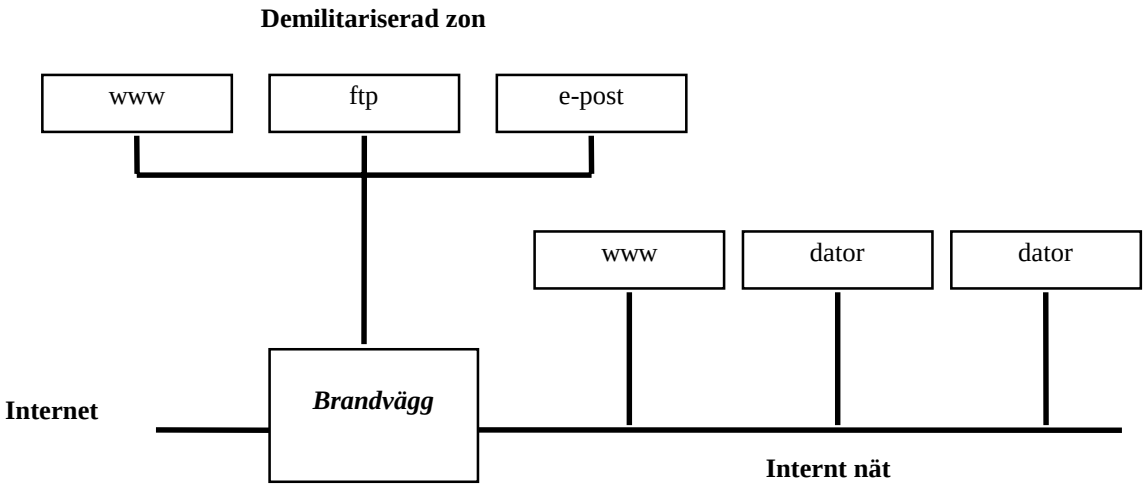

Bild 5.4 Brandväggens placering

Brandväggar har en mängd positiva egenskaper. De är lätta att installera och därmed även snabba att byta ut, vilket minskar risken för långa driftstopp då ett fel inträffat på brandväggen. Då brandväggen går ned bryts kontakten med omvärlden vilket gör den både stabil och driftsäker. Det finns enkla och bra övervaknings- och statistikfunktioner liksom funktioner för test av säkerheten efter installationen.

De viktigaste funktionerna i en brandvägg är enligt Skalin (1997) övervakning, rapportering och statistik. Med brandväggar ökar möjligheten att kontrollera vad som händer på nätet. Brandväggen upptäcker såväl externa som interna överträdelser och rapporterar vad som gjorts. Därför kan en skadas omfattning lättare bedömas och åtgärdas. Även om en extern inkräktare tar sig in i systemet via modem eller annan anslutning, utan att gå via brandväggen, kan det upptäckas genom att inkräktaren uppträder på ett misstänkt sätt.

En brandvägg kan användas för flera olika funktioner. Vanliga uppgifter är att filtrera filer från oönskade ting såsom ”cookies”, Java- eller Activex-program från websidor som inte anses betrodda. De används också för att dölja IP-adresser, resultatet av denna handling blir att alla paket som skickas ut uppfattas som om de har samma adress (Skalin, 1997). Samtliga användare utanför brandväggen har adresser som inte finns på Internet. Denna funktion kallas för NAT (Network Address Translation). Brandväggar har även funktioner för kryptering.

Skalin (artikel 2, 1997) beskriver två alternativa metoder för brandväggar. Den ena är paketfiltrering som kontrollerar alla in- och utgående paket efter skadligt eller oönskat innehåll samt kontrollerar IP-protokollet efter varifrån paketet kommer och vart det skall. Detta ger hög prestanda och bättre skalbarhet. Den andra är proxy som fungerar som en applikationsserver som användaren ställer frågor till och som i sin tur arbetar mot den egentliga applikationsservern. Detta ger en högre säkerhet och är vanligtvis enklare att sätta upp, men den kräver mycket processorkraft. Det finns även hybrider som fungerar som både filter och proxy samtidigt.

Liksom i övrig säkerhetsutrustning är det viktigt att brandväggens programvara är enkel att använda. I annat fall kan inställningarna bli fel och säkerheten påverkas negativt. Det är också viktigt att det klart framgår hur analysen vid ett eventuellt larm skall gå till och att det i säkerhetspolicyn är lätt att hitta de åtgärder som skall sättas in om ett intrång skett.

5.3.3 Logisk kontroll

Den logiska accesskontrollen är till för dem som redan är inne i systemet. Denna kontroll syftar till att begränsa tillgången till viss data eller mjukvara.

Det finns olika aspekter på logisk kontroll (Caelli, Longley och Shain, 1989). Logisk kontroll kan innebära att identifiera och verifiera användaren (autenticering), men kan även innebära en begränsning av användarnas accessprivilegier till ett minimum för det som krävs för att användaren skall kunna utföra sina tilldelade uppgifter. Logisk kontroll innebär också övervakning av all användning av systemet.

5.3.3.1 Accessrestriktioner

Det bör finnas mer än en kontrollnivå. Bara för att någon har klarat att komma in i systemet skall det inte betyda obegränsad tillgång till allt som finns i systemet.

Det finns flera sätt att begränsa access logiskt. Ett sätt är att använda tidsrestriktioner för användaren, som t ex användarens arbetstid plus minus någon timme. En sådan åtgärd skulle hindra en hacker från att använda ett överkommet lösenord på kvällstid eller helger. Filer kan skyddas så att endast de som skall använda dem får använda dem. På filer kan även skrivrestriktioner sättas så att filen går att läsa, men inte ändras i.

5.3.3.2 Verifiera identitet

En undersökning av Gartner Group visade att 65% av summan, som läggs på datasäkerheten i företag, kommer år 2001 att läggas på att lösa problem med identifiering av användare och administration av säkerhetssystemet.

Det finns flera sätt att verifiera användares identitet. Till de vanligaste hör att verifiera med hjälp av ett särskilt attribut, en tillhörighet eller någon specifik kunskap hos användaren. Attribut kan mätas med hjälp av biometriska[16] sensorer såsom fingeravtrycks-, signatur-, ögonnäthinnemönster-, handflate-, och röstanalysinstrument. Sensorerna identifierar då användaren genom något unikt biologiskt attribut. Troligen kommer denna typ av identifiering bli vanligare i framtiden. Fördelen med biometriska sensorer är att det är betydligt svårare att imitera biologiska attribut än att använda ett stulet id-kort, passerkort, nyckel, smart-card eller liknande. Av den anledningen bör en tillhörighet, som t ex ett magnetkort, kombineras med någon form av kunskap hos användaren, såsom en pinkod eller lösenord, vid verifieringen av identiteten för att försvåra för en tjuv som stjäl ett sådant kort.

5.3.3.3 Lösenord

Lösenord är enligt Caelli, Longley och Shain (1989) den vanligaste access identifieringen. Ett lösenord kan antingen vara självvalt eller slumpmässigt utvalt. Ett självvalt lösenord är oftast lätt för användaren att komma ihåg och lätt för någon annan att komma på. Ett slumpmässigt valt lösenord är vanligtvis svårare att komma ihåg och skrivs därför gärna på en minneslapp, men det är också betydligt svårare för någon obehörig att komma på såvida de inte finner minneslappen.

Lösenord och koder bör bytas ofta, särskilt i system som används av många medarbetare såsom gruppkonton, dörrkoder m. fl. Vid stor personalomsättning är byte av koder naturligtvis av extra stor vikt. Det finns särskilda program för att knäcka lösenord som kan användas i proceduren med att ta fram ”säkra” lösenord. (Kullmar, 1997)

Då en medarbetare slutar sin anställning bör givetvis dennes konton plockas bort ur systemet med omedelbar verkan, koder bör bytas ut och passerkort krävas tillbaka. Westman (1997) påpekar att det samtidigt bör kontrolleras att rättigheter för gästkonton och lösenorden för systemets standardkonton (som skapas vid installationen) är utbytta.

Lösenord bör inte skickas i klartext över nätverk och definitivt inte över Internet. Helst bör en alternativ väg än nätverk användas när lösenord skall skickas till någon annan. Det finns idag system på marknaden (som Kerberos och Ssh) som kan skydda från avlyssning (Kullmar, 1997).

För att skydda system från lösenordsattacker anser Gustafsson (1997) att administratören först och främst bör ändra namn på sitt konto, välja lösenord med omsorg, undvika osäkra program och datorer som kan innehålla denna typ av fällor. Säkerhetsansvarig bör även tänka på att även säkerhetskopian av SAM innehåller känslig information. Det bästa sättet att skydda sig mot ”lösenordssniffar”-attacker, och fortfarande ha tillgång till nätverk och Internet, är att använda engångslösenord. Vid användning av engångslösenord har användaren en dosa som genererar ett nytt lösenord vid varje inloggningstillfälle. Detta är säkrare än vanliga lösenord så länge dosan är säkrad från stöld.

[16] Biometri är den vetenskapsgren som studerar biologiska problem med statiska metoder (Nordstedt, 1990)

5.3.3.4 Lösenordspolicy

För att skydda lösenorden är det viktigt att ha en bra lösenordspolicy. Ett bra eller ”starkt” lösenord bör innehålla minst åtta tecken och bör inte gå att hitta i en ordlista. (Gustafsson, 1997) Det bör inte gå att göra mer än ett par misslyckade inloggningsförsök innan användaren stängs ute, detta för att förhindra att någon gissar lösenordet genom att försöka logga in ett stort antal gånger. Även om lösenorden är krypterade kan de gå att gissa med hjälp av olika program. (Kullmar, 1997)

Företaget bör markera vikten av att inte använda enkla lösenord. Enkla lösenord är egennamn, personnummer, registreringsnummer på bilen, barnens, partners eller husdjurs namn. (Cardholm, 1997) Vidare bör det ingå i en lösenordspolicy att aldrig lämna ut sitt lösenord. Skulle det ändå göras så bör lösenordet snarast bytas ut.

5.3.3.5 Kryptering

Kryptering är det mest kraftfulla redskapet för IT-säkerhet och sörjer för bibehållande av både integritet och sekretess. (Pfleeger, 1989) Kryptering är en viktig komponent i accesskontroll. Kryptering ”ser till” att data, som en angripare har skaffat sig fysisk och logisk access till, inte går att nyttja. Angriparen kan då varken läsa datan eller modifiera den utan att det märks på ett tydligt sätt.

Idag är det tillåtet att kryptera kommunikation inom Sverige och föra in krypteringssystem. IT-kommissionen utreder om det så skall förbli, samt hur den nationella policyn skall kunna anpassas till internationella regler. Användningen av kryptering i Sverige är idag omfattande, den mest kända är autentisering i betalsystem. Säkerhetspolisen och andra intressenter vill ha tillgång till viss krypterad information. Anledningen till att IT-kommissionen vill ha fri kryptering även i fortsättningen är att ”Människor och företag måste vara trygga i samhället och kunna kontrollera själva att ingen gått in och förändrat innehållet i meddelandena.” (Ottoson, 1997)

Enligt Sveriges IT-kommission (rapport 6/97) bidrar krypteringstekniken till att kommunikation över nätverk kan göras mer säker. En mer allmän användning av krypteringstekniken berör många olika samhällsintressen. Det kan röra näringslivets behov av säker kommunikation för företagskänslig information, enskildas integritetsskydd, men även rättsväsendets möjligheter att vidta formella åtgärder mot brott. IT-kommissionens rapport visar att de olika intressena kan stå i motsatsförhållande till varandra.

Säker elektronisk kommunikation är en angelägen fråga som ökar i betydelse för var dag. Det är viktigt att uppnå en balans mellan brottsbekämpning och förtroende för systemet. Sveriges regering har lagt ut ett uppdrag att ta fram en svensk policy för att kunna göra en rimlig avvägning mellan olika intressen. Företagsintegritet och personlig integritet skall balanseras mot samhällets behov av skydd. En svensk lösning bör vara internationellt anpassad och nyckeldeponeringssystem skall vara av global karaktär. Skulle inte ett nyckeldeponeringssystem vinna förtroende anser IT-kommissionen (nr 6/97) inte att det är troligt att potentialen i den elektroniska kommunikationen realiseras.

Med god kryptering kommer en inkräktare inte att kunna förstå filer och meddelanden även om han får tag på dem. Det finns många olika krypteringsprogram, vad som krävs är en med ett stark krypteringsalgoritm. I krypteringsalgoritmer med privat nyckel använder både krypteraren och dekrypteraren sig av samma nyckel. Data Encryption Standard (DES) är

fortfarande en bra privat nyckelkrypteringsalgoritm, särskilt varianter som Triple-DES. IDEA, Blowfish, RC2 och RC4 är andra bra privata nyckelalgoritmer. En annan privat nyckel krypteringsalgoritm är Clipper, men man bör vara medveten om att NSA kan läsa det som skrivs med denna algoritm. Problemet med privata nycklar är att de måste hållas hemliga och att de måste distribueras mellan parter som skall kommunicera med krypterade meddelanden. (ur föreläsningsanteckningar, Computer Security, 1996)

Diffie och Hellman kom på systemet med allmän krypteringsalgoritm 1976. Med en sådan algoritm kan parterna använda sig av olika nycklar för att kryptera och dekryptera meddelanden. I det här systemet har varje användare två nycklar, en allmän och en privat. På det sättet undviks problemet med distribution av nycklarna och hemlighållandet blir betydligt enklare. RSA (Rivest-Shamir-Adleman) algoritmen är en bra allmän nyckelalgoritm, andra exempel är Merkle-Hellman knapsack och PGP (Pretty Good Privacy). PGP är gjord av Phil Zimmerman och är ett program som implementerar RSA-algoritmen. PGP är den mest använda krypteringsalgoritmen för e-post. (ur föreläsningsanteckningar, Computer Security, 1996)

Kryptering bör användas för både e-post och på bärbara datorer. Det är viktigt att se till att nycklarna alltid är i säkra händer, att de skickas på ett säkert sätt och att de byts ut regelbundet samt vid behov. (Pfleeger, 1989)

SUN har arbetat fram en ny teknik för kryptering som kallas SKIP, Simple Key management for Internet Protocols. SKIP är en standard för nyckelbyte där vilken krypteringsmetod som helst skall kunna användas. Den ligger som förslag som standard för nyckelbyte även på Internet (Kullmar, 1997).

De amerikanska exportrestriktionerna för kryptering har enligt Ericsson (1997) lättat något. Andra banker än de amerikanska tillåts nu att köpa serverprogramvara med 128 bitars kryptering, mot tidigare tillåtna 56. Detta innebär betydligt säkrare transaktioner över Internet.

5.3.3.6 Smarta kort

Det senaste inom krypteringen är kryptering via smarta kort (smart cards). Det är dock viktigt att skyddet som sätts in är rätt för just den personen eller datorn och att inte sätta in samma lösning överallt. Mjukvarukryptering kan inskaffas för ca 500-600 kronor per dator, smarta kort däremot behöver en läsare för några tusen kronor och en administrativ apparat för att hantera korten (Westman, 1997).

IT-kommissionen anser att det bör tas fram de facto[17] standarder inom de områden som stödjer elektronisk kommunikation. Dessutom bör en standard kring smarta kort skapas för att användas som bas för elektronisk identifiering och för att kunna signera och skydda dokument.

5.3.4 Falsk attack

Bästa sättet att kontrollera sin accesskontroll anses vara att utsätta systemet för en falsk attack. Det finns före detta hackers som numera arbetar som säkerhetskonsulter. De iscensätter attacker mot företag och kontrollerar då hur säker företagets brandvägg är, om systemet loggar

[17] på grund av verkliga omständigheter (Bonniers, 1994)

aktiviteten, samt vilken information som kan nås genom en attack. De letar med andra ord hål i företagets säkerhet. (Harne, 1998)

5.4 Administrativa kontroller och procedurer

I det förra avsnittet behandlades accesskontroller som förhindrar att personer når information som de inte har rätt till eller att lagrad data smittas ned. Men det räcker inte med fysisk säkerhet och accesskontroller för att ha ett säkert system, det bör även finnas administrativa kontroller och procedurer som hindrar dem som redan är inne i systemet från att begå misstag eller missbruka systemet.

5.4.1 Informationsflödeskontroll

Med informationsflödeskontroll avses kontrollen av information som förs in i systemet, informationen som flödar i systemet och informationen som lämnar systemet till användarna.

För att undvika rena skrivfel och andra felinmatningar bör det finnas olika in-data-kontroller. Kontrollen av data som förs in i systemet kan bestå av felrutiner för inmatningar och möjlighet att kunna gå tillbaka och ändra vid senare tillfälle. (Caelli, Longley och Shain, 1989)

Designen av skärmbilder bör vara logisk och uppbyggd för den som sköter inmatningen och det får inte finnas utrymme för missförstånd om vad det är som skall matas in. Dessa åtgärder och kontroller minskar risken för felinmatningar i systemet. Det bör även finnas någon form av ”ägarkontroll” för all information i systemet så att problemet med gammal, vilseledande och motstridig information undviks.

5.4.2 Övervakning

Avsikten med övervakning är att verka avskräckande och övervakningsutrustning bör därför vara väl synlig. Förutom att verka avskräckande ger övervakningen företaget en tidig varning om personal verkar överträda sina befogenheter och befinner sig där de inte har någon anledning att vara eller hanterar icke arbetsuppgiftsrelaterade material. Övervakningsmaterialet kan användas för diagnos av en misstänkt angripare och som bevismaterial mot sabotörer. Övervakningen kan även hjälpa till att upptäcka luckor och korrigera dem. Det finns både fysisk och logisk övervakning att tillgå.

5.4.2.1 Fysisk övervakning

Den fysiska övervakningen bevakar den fysiska miljön runt hårdvarorna genom brandlarm, rökdetektorer, vattensensorer mm. Accesskontroll som registrerar vem som t ex äntrar lokaler med datorutrustning, hör också till den fysiska övervakningen liksom övervakning av personal. Den sistnämnda övervakningen består i att övervaka beteendemönster, förändringar inom personalstyrkan etc.

5.4.2.2 Logisk övervakning

Den logiska övervakningen bevakar externa inloggningsförsök på företagets system genom det allmänna telenätet. Genom säkerhetsregister över tillgänglighet till datorsystemet kontrolleras även de interna användarnas användning av systemet såsom t ex tid för användning av systemet, filstorlek, CPU tidsanvändning på applikationsprogram, minnesutnyttjande och överföringshastighet. Den logiska övervakningen innefattar även

registrering av de transaktioner som görs. Övervakningen kan ske av t ex en brandvägg. (Pfleeger, 1989)

Flera funktioner i nätverk är centraliserade till en viss server, såsom e-post och Internetkontakter, därmed kan trafiken övervakas utan användarens vetskap. Aktiviteter som övervakas kan vara inloggningstid eller program som används. För e-post finns det särskilda program som används för att läsa personalens korrespondens. Det finns även system som övervakar personalens effektivitet vid datorn. Dessa system är ofta kopplade till någon standard över hur lång tid en uppgift bör ta att utföra och jämför hur lång tid användaren behöver för att lösa uppgiften. System som dessa används vid rutingöromål. Övervakningen kan sträckas så långt som att bevaka varje tangentnedtryckning som användaren utför och kontrollera allt som sker på skärmen och spara dessa uppgifter för framtiden. En viss etisk konsideration bör göras vid användning av system som nämns i detta stycke.

Det finns även program som kan bevaka system utifrån och som är osynlig för en hacker. Varje tangentnedslag som görs sparas och programmet kan även stänga ned systemet om en förprogrammerad förbjuden åtgärd utförs, samt ringa upp systemadministratören och meddela vad som sker. (Olander, 1997)

5.4.3 Loggning

I ett internt nätverk går det oftast att styra hur användare får logga in, vem som får sätta sig vid servern och arbeta, vem som får ansluta sig via nätverket, samt vilka behörigheter de får. Åtkomsten till resurser såsom filer och skrivare kan också styras. Nätverket kan enligt Höijer (1997) oftast registrera både vem som lyckas och misslyckas med att logga in i systemet, samt kontrollera vem som ansluter via inringning.

Det finns möjlighet för företaget att bevaka vilka websidor som personalen besöker över Internet. En undersökning gjord av Techwire visade att 12 % av nätanvändare surfar till porrwebsidor på arbetet (Ericsson, 1997). Under hösten 1997 uppmärksammades flera fall i USA där personal hade fått sluta efter att ha surfat till sexwebsidor på företagets datorer, trots att det skett efter arbetstid. Det är möjligt att även svenska företag kommer att vidta åtgärder för oetiskt surfande på företagets datorer.

5.4.4 Dokument i pärmar

Det är inte enbart information inom datorsystemet som bör skyddas. Dokument i pärmar, lösa papper och noteringar kan också innehålla känslig information. En dokumentförstörare kan vara en investering för att kopior och utskrifter med företagskänslig information inte skall hamna i papperskorgen där vem som helst kan läsa dem.

Det är ingen vits att förse en dator med lösenord och andra säkerhetsfunktioner om man samtidigt förvarar en pärm bredvid datorn med samma känsliga information. (Pfleeger, 1989)

5.4.5 Säkerhetskontroll av personal

Caelli, Longley och Shain (1989) anser att samtlig personal bör genomgå någon form av säkerhetskontroll - även städare, beroende på vad de skall ha tillgång till. Vissa organisationer har ju medicinska (exempelvis hur vi hanterar stress) och psykologiska (t ex attityder, politisk läggning, stabilitet) tester, så då borde säkerhetsundersökning göras vid anställning av person som skall hantera känslig information. För att undvika oklarheter om vad som gäller för vem bör säkerhetsrutinerna skrivas in i arbetsbeskrivningarna.

5.5 Beredskapsåtgärder

Alla företag bör ha någon form av beredskapsplan ifall att något skulle hända trots de skyddslager som företaget satt upp. Det mest grundläggande i beredskapen är att det alltid finns en färsk backup. Personalen måste veta vad de förväntas göra ifall något händer och vem som skall göra vad och hur i olika situationer. I beredskapsplanen har företaget också tagit hänsyn till om de behöver t ex en extra server eller annan reservkraft i händelse av en nödsituation. Företaget kan förlora mycket på exempelvis ett avbrott och det är därför viktigt att allt är förberett så att personalen kan agera snabbt.

5.5.1 Backup

Backup garanterar inte avbrottsfri tillgång till information vid ett fel, men den garanterar att informationen inte går förlorad. Då en dator alternativt server kraschar måste felet åtgärdas för att komma vidare, men då ett fel bara uppstår ibland kan det vara svårt att bevisa och därmed också att åtgärda. I vissa system, såsom UNIX, finns en syslog som dokumenterar tillfälliga fel. Ett fel som kan komma smygande är överhettning (Öhman, 1997). En stor hårddisk kan bli väldigt varm, upp till ca 80 grader innan överhettning inträffar och datorn kraschar.

Ett sätt att slippa långa driftstopp då servern går ned är att ha en extra server. Med tanke på kostnaderna ett eller flera dygns databortfall innebär ett sådant stort ekonomiskt bakslag att ett system med spegling av datasystemet snabbt borde löna sig.

Säkerhetskopieringen bör inte slarvas med. Om inte backupfunktionerna fungerar som de skall kan det övriga säkerhetsarbetet vara förgäves. Westman (1997) ser helst att backupbanden och servern är placerade på helt skilda platser, gärna olika byggnader. Banden bör dessutom vara placerade i brandsäkert skåp ifall att olyckan skulle vara framme.

Problemet med säkerhetskopiering till bandstationer är att det ofta tar lång tid (Mikrodatorn nr 10, 1997). Informationen skrivs först på bandet och spolas sedan tillbaka för läsning och verifiering av informationen mot hårddisken. Det finns nya produkter på marknaden som halverar tiden genom att skriva och verifiera informationen samtidigt.

5.5.2 Virusskydd

Virus kan ställa till med stor skada, det bör därför vara en självklarhet idag att ha ett virusscanningsprogram som körs igång då datorn startas eller då en fil från en diskett eller CD-ROM öppnas. Virusmakarna hittar hela tiden på nya trick och är väl framme i utvecklingen av nya metoder därför bör även virusscanningsprogrammen uppdateras regelbundet.

5.5.2.1 Skydd mot makrovirus

Datorn smittas oftast inte förrän mottagaren öppnat ett smittat dokumentet. För att skydda sig mot denna typ av virus bör det inte finnas någon automatisk öppning av ett program bara för att det finns en attachment till ett mail. Dokument som erhålles via e-post bör därför först sparas ned och därefter kontrolleras med ett scanningprogram om det innehåller virus innan filen öppnas.

För att skydda sig mot makrovirus tycker Sundström (1997) att man bör skapa ett eget makro som hindrar att makros exekveras automatiskt. För att göra ett eget makro väljes ”Makro” under ”Verktyg” och sedan anges namnet ”AutoExec”. Därefter väljs ”Skapa makro” och följande kod skrivs in:

```
Sub MAIN
DisableAutoMacros
MsgBox   ”AutoMacros är avstängda”,”Virusskydd”, 64
EndSub
```

Därefter stängs fönstret och sparas. När Word startas i fortsättningen sätts detta makro igång och ger användaren ett visst skydd mot makrovirus.

6. De mänskliga faktorernas roll i IT-säkerheten

6.1 Mjuka faktorer av vikt i IT-säkerhetsprocessen

Fysiska säkerhetshjälpmedel kan invagga företagets ledning i falsk trygghet. För ett fungerande säkerhetssystem bör hänsyn även tas till den mänskliga faktorn. Det är främst genom att kontinuerligt utveckla kompetensen på området och anpassa systemen som säkerheten kan upprätthållas. Säkerhetstänkandet bör finnas med hela tiden i allt företaget tar sig för. Utvecklingen får inte stanna av, regelbundna kontroller och genomgångar av brandväggarnas och andra systems loggar, för att finna avvikelser från det normala beteendemönstret, är en nödvändighet för att säkerheten bibehålls.

Det är viktigt att inte bli alltför produktinriktad i säkerhetsarbetet, varken i det interna eller externa arbetet. God säkerhet är resultatet av kontinuerligt arbete och en djupare förståelse för hur systemen och människorna i organisationen fungerar. Det krävs en stor portion kreativitet för att finna de bästa lösningarna på säkerhetsproblemen. Det är inte den maximala säkerheten som skall eftersträvas utan den optimala säkerheten. Risken blir annars att säkerhetssystemet blir för krångligt och därmed en risk i sig självt eftersom medarbetare då söker sig runt det. Ett exempel på att för mycket säkerhetsåtgärder utan rätt motivation av personalen får motsatt effekt är då dörrar med kodlås ställs upp för att det är för krångligt att hålla på att leta rätt på sitt passerkort och komma ihåg koder.

6.1.1 Brister i säkerheten beror på organisatoriska problem

Enligt svenska Överstyrelsen för Civil Beredskap kan 75% av alla brister i datasäkerheten härröras till organisatoriska problem medan de övriga är av teknisk natur (Engholm, 1997). Louise Yngström konstaterar i sin doktorsavhandling (1997) att för att uppnå datasäkerhet krävs kontinuerligt arbete och underhåll, samt kunskap om både teknik och organisation. Hon anser att det är särskilt viktig med personalvården för att uppnå datasäkerhet.

6.1.2 Positiv attityd till säkerheten

Begreppet säkerhet upplevs ofta som något negativt. Det innebär ju speciella arbetsrutiner, kostnader osv. utan att egentligen producera något positivt. Personalen instrueras att följa rutiner och regler och stå ut med olägenheter och ändå vara precis lika effektiva och produktiva som vanligt. Det är därför viktigt för ledningen att uppmuntra en positiv attityd, uppmuntra säkerhetstänkandet, belöna funna säkerhetsluckor eller uppmärksammade incidenter osv.

6.1.3 Betydelsen av information

Solli och Westins studier (Polesie och Johansson, 1992) har visat att den informativa bilden för att se sina prestationer och deras konsekvenser sällan stämmer överens med den givna situationen. Förklaringen kan ligga i att styrinformation konstruerats av och för ledning och tjänstemän, inte för dem som utför det dagliga arbetet. Arbetstagarna har då inte haft möjlighet att få en bra bild av vad de gör och har gjort genom det existerande centrala informationssystemet. Solli och Westins studier visar vidare att en konfliktsituation kan uppstå när det finns motsättningar mellan att göra, förstå och att kunna påverka. Följden av att

inte ha möjlighet att påverka kan bli att anställda inte bryr sig om att göra något de ser och förstår borde bli gjort, eftersom de inte känner att de får något för det.

6.1.4 Motivation och kunskap

Basen för det mer långsiktiga arbetet med säkerheten rör sig kring mjuka faktorer som utbildning och motivering av personalen. Motivationen kan uppnås genom en känsla av lojalitet för företaget och samhörighet med övrig personal. (Södergren, 1987) En annan grundförutsättning för motivation är delaktighet. (Vedin, 1993) Medarbetarna bör alltså beredas plats i arbetet kring de säkerhetsproblem som rör just deras arbete, vilket medför att de blir införstådda i problematiken och får en djupare förståelse för hur säkerheten bäst bevaras och varför det är viktigt att skydda informationen.

Det är inte säkert att en extern konsult kan lösa företagets problem med avseende på säkerheten. För att nå den optimala lösningen i säkerhetsarbetet krävs att det ingår personal i arbetsgruppen som känner företaget, de informella kanalerna, olika grader av betydelse för olika information, praktiska förutsättningar, de anställdas kapacitet osv. Därför krävs det att säkerhetsproblematiken behandlas internt.

Motiveringen av medarbetarna till att deltaga i säkerhetsarbetet är en av grundförutsättningarna för att satsningen skall lyckas. Motivering kan ske på en mängd olika plan. Exempelvis kan företaget hyra in någon intressant talare, göra något annorlunda och gärna spektakulärt för att höja graden av intresse. Att sätta upp plakat med vad de anställda inte får göra kan verka som ett lätt sätt att få alla medvetna om reglerna, men Westman (1997) menar att denna åtgärd kan ge motsatt effekt på en svensk som inte tycker om att få pekpinnar i ansiktet.

En viktig motivator är känslan av gemenskap och lojalitet för företaget och andra anställda. Företaget bör ha informella möten där hotbilden och lämpliga åtgärder diskuteras över personalgrupperna. Samarbete över personalgränserna skapar förståelse för andras problem och ger en helhetssyn på säkerheten. Endast det som bör skyddas skall skyddas.

Förtrolighet mellan personer i ledarställning och de övriga anställda ger, menar Molander (1993) en atmosfär av samhörighet och trygghet på arbetsplatsen. Detta ger is in tur en stabil grund för säkerhetsarbetet. Medarbetare som arbetar både för och med företaget i en positiv anda och med ett engagemang för det de gör, är både effektivare och säkrare ur företagets synvinkel.

6.1.5 Vanligaste orsakerna till förlust av information

Som tidigare nämnt är de vanligaste orsakerna till förlust av information användarens vardagsslentrian och missuppfattningar kring hur informationen skall skyddas och lagras. (Cardholm, 1997) Det är därför viktigt att den anställde förstår anledningen till de olika säkerhetsåtgärderna som företaget har, såsom att regelbundet byta ut sitt lösenord, för att motiveras till att agera i enlighet med säkerhetsföreskrifter.

Lösningen på problemet med filer som försvinner för användarna är utbildning i hur systemet och katalogerna är uppbyggda och hur filer sparas på rätt sätt. För att hitta ”försvunna” filer själv kan användaren instrueras att använda sökverktygen som finns tillgängliga. Då program inte använts på ett tag kan det vara på sin plats att uppdatera kunskaperna med en repetitionskurs. Tiden det tar borde uppvägas av den tid som tas igen på uteblivna problem.

Förutom att utbilda personalen bör designen av katalogstrukturen ses över så att den är logiskt uppbyggd ur användarnas synvinkel. För att detta skall fungera krävs en uttalad företagspolicy och särskilda rutiner för ny personal. Även om det oftast går att hitta eller återskapa försvunna eller raderade filer tar de tid att hitta och är en källa till irritation och kostar företaget pengar i utebliven arbetsinsats och medför stopp i verksamhetsflödet.

Det räcker inte att informera om säkerhetsarbetet och dess betydelse för organisationen vid ett tillfälle, utan det krävs regelbundet återkommande säkerhetsdagar eller internutbildningar för att ständigt hålla en hög medvetenhet om säkerheten bland de anställda.

6.1.6 Personalen

I och med att personalen kan innebära en sårbarhetsfaktor för företagen är det viktigt att ha med sig medarbetarna i säkerhetsarbetet. Det finns flera sätt att minska sårbarheten med avseende på personalen.

Medarbetare bör exempelvis inte tillåtas att utföra uppgifter som inte kommer att granskas av annan personal, eftersom de dels kan utsättas för frestelse och dels tar det längre tid innan ett misstag upptäcks. Om personal kan implementera privata rutiner som varken är väldokumenterade eller begripliga av andra finner sig företaget i beroendeställning. Även nyanställd personal kan innebära en säkerhetsrisk om de tillåts att använda systemet utan handledare innan de är insatta i såväl systemet som säkerhetsfrågorna, eftersom de då kan göra fel. Ingen i personalen får heller upplevas som oumbärlig och det bör alltid finnas personer som kan ersätta annan personal utan varken tids- eller kostnadsförluster.

Då en medarbetare planerar att sluta sin anställning bör dennes säkerhetsstatus ändras till att vara en riskfaktor. (Wedberg, 1997) Så fort det blir känt att en medarbetare skall sluta bör alla id-brickor, nycklar, kort och andra tillgänglighetsfaktorer dras in och koder samt lösenord bör bytas ut. Alla som arbetar med säkerhet bör informeras om vem som avser att sluta. Det bör även ske en kontroll över att allt arbete, som den som skall sluta har arbetat med, är väl dokumenterat.

6.1.7 Revirtänkande

Ibland kan det uppstå revirtänkande på en arbetsplats eller ”inte mitt bord”-effekten (Södergren, 1987). Ett starkt revirtänkande kan uppstå om statusbetonade uppgifter, särskilt om dessa uppgifter inte kan generera mer resurser. Typiska sådana uppgifter är rutinarbete. Det kan också uppstå om djupare kunnande inom det egna området genom att en medarbetare t ex göra sig oumbärlig för organisationen. Revir kan sättas mellan individer, men även mellan grupper eller avdelningar inom ett företag.

Reviret ger trygghet, identitet och anseende, därför bör det skyddas mot förändring. Då reviret hotas kommer den revirbeskyddande med bortförklaringar eller kanske hemlighåller han/hon ogynnsam information. Då signalerna blir alltför starka, skär man helt enkelt av kommunikationen, slutar gå på möten och undviker ”farliga” personer. Det finns även en positiv sida av revirtänkandet då det istället resulterar i att motivationen och ansvarskänslan för den egna enheten ökar.

6.1.8 Två svenska företags lösning på den interna säkerheten

Skandinaviska Enskilda banken har skrivit regler och satt upp riktlinjer för den interna säkerheten, som följs upp av en revisionsavdelning. Banken har ett samspel mellan revision,

tekniska hjälpmedel, instruktioner och utbildning för att skapa en rimlig situation. De försöker skydda sig från insiderbrott genom att ha mycket begränsade rättigheter i systemet. De är inte oroliga för att personalen skall stjäla pengar från dem, eftersom det skulle vara oerhört svårt enligt IT-chefen Lars Landin, däremot kan det vara svårare att skydda känslig information inom värdepappershandeln (Westman, 1997).

SE-banken har en brandvägg som skydd mot Internet och systemet loggar all verksamhet. Det sista vet personalen om och därmed fungerar det även i preventivt syfte. De bärbara datorerna kommer att skyddas med kryptering via smarta kort. På ett mer långsiktigt plan är det kontinuerlig utbildning för personalen som gäller.

Volvo Data i Göteborg skyddar sig internt genom olika behörighetsnivåer, dessa nivåer är utformade per datasystem. Samtliga anställda har skrivit på en sekretessförbindelse och det finns även bestämmelser över hur säkerheten skall tillgodoses. Volvo Data har regler för hur företagshemlig information skall behandlas. Om det är nödvändigt att sända sådan information över Internet eller om den finns på en bärbar dator skall en godkänd krypteringsmetod användas. Internetanvändningen övervakas och resultaten av övervakningen analyseras regelbundet. På ett långsiktigt plan sker kontinuerliga utbildningar och motivation av nyanställda, ledande personal och andra personalgrupper. Holger Lissvall, informationschef på företaget, anser att det största hotet är förlust av data som innebär förseningar i verksamheten samt tekniska driftstopp (Westman, 1997).

6.2 Företagskulturens betydelse för säkerheten

Företagets ledning kan inte uppnå säker IT om inte medarbetarna i företaget vill, med andra ord bör företagskulturen vara positivt inställd till säkerheten.

6.2.1 Kultur

Begreppet kultur spänner över ett mycket brett område och är därför svårt att få grepp om. Jag skall dock göra ett försök att med hjälp av Simcha Ronen (1986) reda ut begreppet något.

Generellt sett är kultur benämningen på människors sätt att leva, deras livsstil. Kultur definierar och uttrycker både attityder och beteende. Det står även för kontinuitet både geografiskt och över tiden. Folk har alltid följt särskilda traditionella beteenden som ger deras liv ett speciellt mönster, regelbundenhet och mening. Olika samhällen har utvecklat skilda kulturella mönster, ingen kultur är exakt lik en annan. Eftersom kulturer är olika överallt och alla anser just sin kultur som den mest riktiga, är det oundvikligt med kulturella missförstånd och motsättningar. Som bäst kan kulturella skillnader visa på en fantastisk variation i hur folk väljer att leva. Som sämst kan dessa olikheter ge upphov till enorma konflikter.

Kultur innefattar det sätt som människor uppfattar världen, både med avseende på attityd och beteende. Ronen menar att kulturer representerar ett delat sätt att leva, vilka värderingar och sätt att agera som överförs från en generation till nästa. Alla mänskliga samhällen har en kultur som inkluderar åtminstone de delade uppfattningar som gör det möjligt att leva tillsammans. Det är inte nödvändigt att alla medlemmar delar alla uppfattningar, men några människor måste dela några uppfattningar.

Kultur inbegriper även moral och är det som avgör för varje grupp vad som är ”rätt och riktigt”, och hur saker och ting ”borde” utföras. Kulturen delas av alla medlemmar i en

speciell grupp och formar därmed basen för allt socialt och kollektivt liv. Fenomenet kultur utvecklas och förändras över tiden. Det sociala livet beror till stor del på individuella anpassning till de tidigare delade uppfattningarna som bildar en given kultur, men dessa delade uppfattningar befinner sig i en ständig förändringsprocess.

Barbara Czarniawska-Joerges (1993) beskriver den praktiska dimensionen i en organisation som kretsar kring förhållandet mellan människorna och teknologin i organisationen. Hotet om att bli ersatt med en maskin existerar än idag i vissa industrier och bidrar till rädsla och aversion mot teknologi. Faktum kvarstår dock att teknologin har hjälpt oss på många områden och att t ex datorer har blivit oumbärliga på de allra flesta arbetsplatser.

6.2.2 Kommunikation och interpersonella relationer

Kultur och kommunikation är nära förknippade med varandra. Kommunikationen kan ske verbalt, skriftligt eller intuitivt. Kulturen föreskriver vem som talar med vem om vad och hur kommunikationen fortskrider. Ronen (1986) studier visar också att kulturen avgör hur personer kodar meddelanden, vilka betydelser meddelandena har och under vilka förutsättningar eller omständigheter olika meddelanden sänds respektive inte sänds, uppmärksammas, eller tolkas.

Med kommunikation avses oftast den verbala kommunikationen, men den icke-verbala kommunikationen är minst lika viktig. Den icke-verbala kommunikationen kan bestå av t ex ansiktsuttryck, gester och mottaglighet för meddelandet.

Kommunikationen inom en organisation är i grund och botten påverkad av olika aspekter i den aktuella organisationen. Faktorer såsom den sociala sammansättningen, målorientering, arbetsfördelning, koordinationssystem, och kontinuitet över tiden är kraftfulla influenser.

6.2.3 Ledarskap

För att realisera mål som effektivitet, kvalitet och IT-säkerhet, måste ledningen betona dessa funktioner. Effektiviteten beror på hur bra organisationen kan uppnå sina satta mål.

Bass (1981) studier visade att karaktärsdrag hos den typiske ledaren är bl a envishet, självförtroende, en stark ansvarstagandedrift och att göra färdigt uppgifter, förmåga att influera andras beteende, samt originalitet (ur Ronen, 1986). Ronen menar att ledaren dessutom skall bry sig om hur gruppmedlemmarna mår, höja underordnades självkänsla, acceptera deras förslag och råd, samt prisa dem för väl utfört arbete. De underordnade ser hellre en omtänksam ledare, men betydelsen av ledarens effektivitet varierar med situationen. (Se bild 6.1)

En ledares beteendestil kan vara direktiv, stödjande, deltagande och prestationsorienterad.

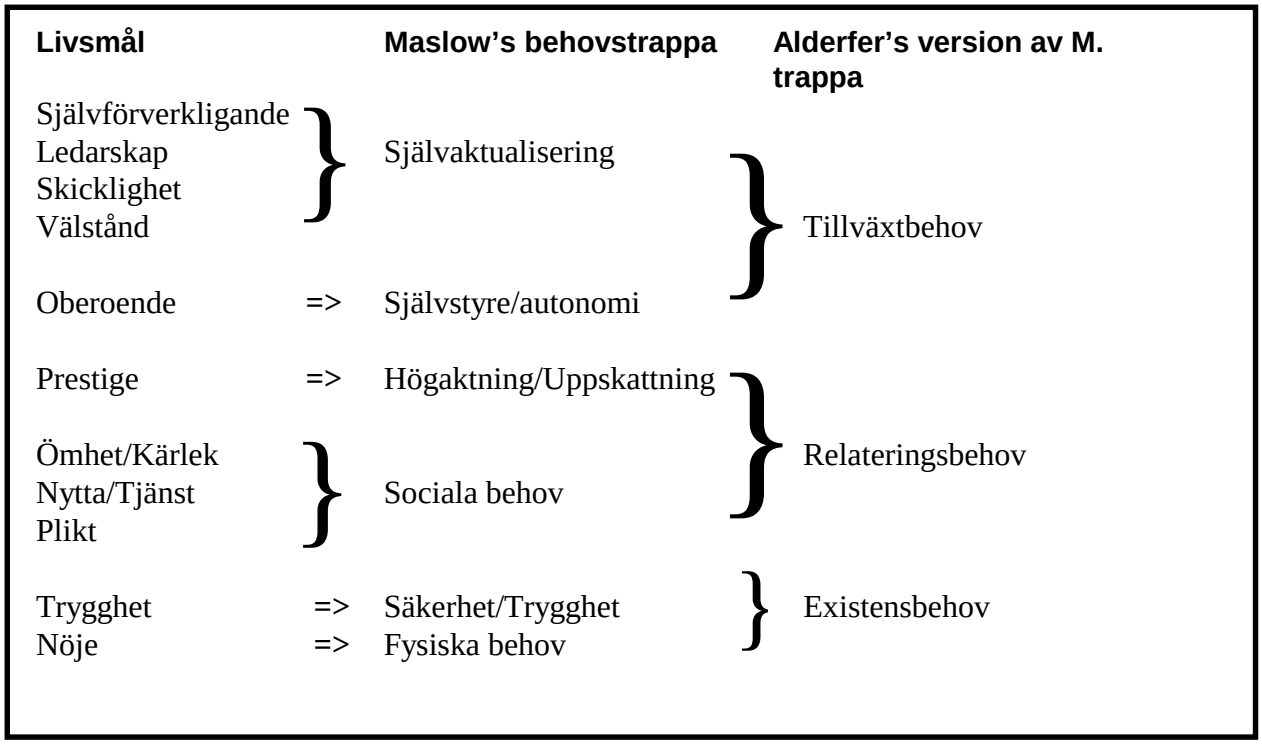

Bild 6.1 Relationer mellan livsmål och behovstrappan[18]

6.2.4 Medarbetarnas attityder och motivation

Social sammansättning existerar på olika nivåer inom företaget, dels på individnivå dels som en del av organisationen och även inom olika sociala grupper inom organisationen. Gruppernas normer och värderingar avgör form och innehåll av den information som överförs eller förmedlas, respektive tas emot och tolkas (Ronen, 1986).

I alla samhällen uppfostras vi att lyda lagar och ha respekt för auktoriteter. Ofta är det så att vi ser det vi vill se eller blivit uppmanade att se. Så är det även inom organisationer. Det är vetskapen om möjligheten att få ut något fördelaktigt av sin prestation som motiverar en individ att agera.

Macintosch (1985) beskriver den grundläggande teorin i Human Relations som tron på att de anställdas deltagande i budgetarbetet många gånger löser de organisatoriska problemen som finns. Genom att skapa kreativitet bland de anställda kan produktionen ökas. I detta fall blir ledarens roll att skapa ett arbetsklimat där alla organisationens medlemmar deltar i processen. Det i sin tur ökar arbetsmoralen och motivationen bland de anställda.

Hofstede (ur Macintosch, 1985) har i sina undersökningar, på bland annat stora organisationer i Holland, funnit att inställningen till planeringsarbete är mycket negativ. (Hofstede tittade främst på budgetarbetet, men paralleller går att dra till förberedande säkerhetsarbete.) Vare sig de anställda eller ledarna inom organisationen verkade bry sig om planeringsarbetet. Hofstede

[18] ur Ronan, 1986, tolkad bild sid. 203

fann att nyckeln, till att få människor engagerade, var deltagande. Det gäller dock att lägga sig på rätt nivå inom organisationen och hitta den rätta spelandan för att nå framgången.

Det gäller att motivera de anställda på alla nivåer för att få en laganda. Det gäller att utmana och motivera medarbetarna för att kunna nå den lojalitet och den effektivitet som eftersträvas.

Basen för en företagskultur är gemensamma värderingar, även om det kan finnas lokala subkulturer i stora och mångfacetterade strukturer. Värderingar spelar en stor roll för personalens motivationskraft. Motivationen är avgörande för idékraften, entreprenöriialiteten och för viljan till kvalitetsarbete.

Att få ta större ansvar för sin verksamhet är ofta förknippat med något positivt hos personalen, även om det kan innebära en större arbetsinsats. Vedin (1993) menar att förtroendet skapar stimulans och människor som känner sig stimulerade gör vanligtvis ett bättre jobb i form av förbättrade prestationer. Stimulans kan ges genom t ex företagsutbildning. ”De som tas ut till utbildning växer ofta i sitt arbete bara genom att känna sig utvalda och uppmärksammade.” (Södergren, 1987)

Den mänskliga aktiviteten är teleologisk. Jansson (1993) beskriver teleologin som en central föreställning i filosofisk handlingsteori, som dessutom ligger till grund för många samhällsvetenskapliga förklaringsmodeller. Detta innebär att människor handlar i syftet att åstadkomma ett av dem eftersträvat tillstånd. I slutändan innebär motivering av de anställda att de ses som kapabla individer som är mogna att fatta sina egna beslut.

6.2.5 Företags informella struktur

Det är den direkta kontakten mellan personer och enheter i ett företag som skapar den informella strukturen. Mintzberg (1983) menar att de formella och informella strukturerna i ett företag är sammanflätade och därför omöjliga att separera (se Holmström, 1995). De direkta informella kontakterna i ett företag är svåra att studera, men det är viktigt att veta att de finns och utgör en viktig samordningsfunktion.

6.2.6 Kulturell gemenskap

Thomas Kuhns paradigm-teori innebär att kulturen finns i tingen man arbetar med, i sätten att ställa frågor, i kriterierna för att bedöma svar, i normer för handlingar och handlingsvanor, samt i olika typer av praxis. Dessa faktorer är olika aspekter av kulturell gemenskap.

För att finna mening i det man gör i sitt arbete krävs en viss förståelse. Den hermeneutiska traditionen pekar på att förståelse bygger på förförståelse och omdömen bygger på föromdömen. Förståelse kan aldrig utgå ifrån *tabula rasa*, dvs ”oskrivna blad”. Förförståelse upprätthålls bl a genom en gemensam (för)förståelse av frågorna. Svar och motfrågor bidrar bl a till att stämma av, modifiera och ibland fördjupa vår förståelse av vad andra och vi själva gör. Molander (1993) påpekar dock att frågor och svar också kan skapa missförstånd och bidra till att bryta upp gemenskaper.

Molander ifrågasätter om vi verkligen alltid vet vad vi gör. Vad händer t ex bakom eller under det som vi betraktar som handlande? Det finns grundläggande samband och mekanismer som förklarar varför människor gör som de gör. Vi vill se människan i och genom de olika sociala och kulturella sammanhang som hon är del av och i vissa avseenden aktivt deltar i. Vi kan

även välja att avsiktligt avstå från att göra något. En avsiktlig handling bestäms i hög grad av hur den handlande själv uppfattar den, förmedlat genom beskrivningar, frågor och svar.

Becker och Green (1962) menar att hög målacceptans och stark gruppsammanhållning är receptet för framgång, medan låg målacceptans och stark gruppsammanhållning garanterat ger problem i organisationen (ur Macintosh, 1985). De anser att det senare alternativet är det sämsta tänkbar alternativet i professionella organisationer.

Kultur är en kollektiv företeelse, som handlar om gemenskap. ”Det pragmatiska perspektivet” innebär att mänskliga handlingar och handlingsvanor är primärt. Det innefattar inte åsikter, övertygelser och teorier. Rutiner och traditioner gör uppmärksamhet möjlig genom att ta över just det som kallas ”rutingöra” och ”rutintänkande”. Det ger en säkerhet i handlandet och varandet. Säkerhet är en förutsättning för att lära av misslyckanden och att kunna gå vidare. Molander anser att det gäller att ha mod att använda sig av sitt eget förstånd!

6.2.7 Företagets kultur

Den informella definitionen av företagskultur är: ”hur vi gör saker och ting på vårt företag”. En svag företagskultur innebär att de anställda endast arbetar för att tjäna pengar, men i en stark kultur är alla införstådda med mål och värderingar samt arbetar för att nå dem.

Det finns en rad element som tillsammans bildar kulturen. Affärskulturen styrs av marknadsförutsättningar, värderingar eller de grundläggande idéer och normer som gäller i företaget, människorna som personifierar de värderingar som finns i kulturen, riter och ritualer är systematiska och programmerade rutiner, särskilt i starka kulturer, samt det kulturella nätverket. Det huvudsakliga, men informella, kommunikationsmedlet i en organisation fungerar i det kulturella nätverket som ”budbärare” av företagets värderingar och hjältemytologi.

Kännetecken för företagskulturen kan vara lokalisering av företaget, lokalerna, placering av anställda och avdelningar. Ett annat kännetecken för kulturen i företaget är hur de behandlar sina besökare. Personalens planering av sin tid, karriärsutveckling och anställningstid, tillsammans med ledarens beteende, ger tydliga signaler om företagets kultur. Samma faktorer är betydelsefulla att ta hänsyn till i säkerhetsarbetet.

6.2.8 Företagskultur som styrmedel

Företagskultur kan delvis vara ett uttryck för hur ett företag fungerar, men även företagskulturen kan påverkas och användas som ett styrmedel i ett företag. Socialisering är exempel på ett indirekt styrmedel. I vissa företag försöker företagsledningen medvetet och aktivt styra verksamheten genom att påverka värderingar och kultur. Genom socialisering kan företagsledningen påverka inställningen till säkerhetsarbetet på företaget.

Enligt Anthony m fl (1992) sker styrning både formellt och informellt i ett företag. De ser företagskulturen som den mest betydelsefulla informella faktorn. Företagskulturen formas av värderingar och attityder som delas av organisationens medlemmar och kan enligt Anthony påverkas av företagsledningens personlighet och policys.

Saffold (1988) skiljer mellan starka och svaga företagskulturer. I den starka kulturen vet alla i företaget vilka mål, värderingar och normer som gäller. I en svag kultur kan företagsledning

och anställda ha olika uppfattningar om mål och värderingar, samt betydelsen av dessa. En svag företagskultur gör säkerhetsarbetet svårt att förankra i verksamheten.

Ray (1986) anser att företagskultur är en form av styrning där företagsledningen genom indoktrineringsprocesser försöker få personalen att dela ledningens mål och värderingar (ur Holmström 1995). Det är meningen att företagskulturen skall locka fram en känsla av tillhörighet som underlättar målkongruens och minskar behovet av övervakning.

Holmströms undersökningar visar att samtliga företagsledningar i hans studie mer eller mindre aktivt försöker påverka personalens värderingar och normer. De som lyckas bäst med detta har en utpräglad ledarhierarki som bildar en stark kulturell kärna. I de starka kulturerna hade enhetscheferna samma uppfattning som företagsledningen och på så sätt spreds värderingarna i företagen. En stark företagskultur kan skapas genom påverkan av rekrytering, utbildning och socialiseringsprocesser. Studien visar också att företagsledningarna krävde en omfattande självstyrning.

7. Slutdiskussion

Syftet med denna uppsats har varit att ur ett företagsledarperspektiv belysa de faktorer som har betydelse för god IT-säkerhet i ett svenskt företag. I det följande avsnittet drar jag slutsatserna av min undersökning och gör tolkningar utifrån den fakta jag samlat in.

7.1 Intern IT-säkerhet

Intern säkerhet innebär, som beskrevs i kapitel 4, att skydda företagets system mot allt från slarv till kriminella handlingar. För att kunna skydda företaget måste hotbilden först vara klarlagd. Man måste alltså veta vad eller vem som kan utgöra ett hot för företagets IT, för att kunna bygga upp ett adekvat försvar mot dessa hot.

Det första steget som en företagsledning bör vidta för att uppnå säker IT är en risk- och sårbarhetsanalys, som inkluderar de ekonomiska verkningarna av exempelvis en hackerattack eller ett IT-avbrott. Företagsledningens strategi bör därefter anpassas till företagets förutsättningar. Med förutsättningar avses företagets kultur, ekonomiska resurser, personalens kompetens osv.

Det mest grundläggande i ett säkerhetssystem är den fysiska säkerheten liksom accesskontroller för att undvika yttre påverkan, eller att obehöriga kan ta sig in i såväl byggnad som IT-system. För att undvika slarv, så långt det är möjligt, samt missbruk av systemet upprättas administrativa kontroller. Ett företag bör även ha en beredskapsplan över hur medarbetarna skall agera då något inträffar. Förutom dessa faktorer bör företaget även ha ett försäkringsskydd så att det finns ett ekonomiskt skydd om något ändå skulle inträffa.

Något som ofta faller bort, då ett säkerhetssystem planeras eller revideras, är det faktum att utan medarbetarnas medverkan i säkerhetsprocessen är det mycket svårt för ett företag att uppnå säker IT. Ingen av ovanstående säkerhetsåtgärder gör någon större nytta om inte medarbetarna vill skydda företagets IT eller vet hur de skall bära sig åt. Det räcker inte med de senaste tekniska hjälpmedlen om inte människorna i företaget är positivt inställda till säkerhet. En av de grundläggande förutsättningarna för att få med medarbetarna i säkerhetsprocessen är motivation.

7.1.1 Ledningens uppgift i IT-säkerhetssprocessen

Eftersom det yttersta ansvaret för IT-säkerheten innehas av företagets ledning bör medlemmarna i ledningen vara någorlunda insatta i säkerhetsfrågorna. IT-säkerheten bör ingå i den strategiska styrningen i ett företag och liksom andra strategiska planer utvecklas IT-säkerhetsstrategin med tiden, i och med att företaget förändras.

Säkerhetsarbetet grundläggs i företagets informationssäkerhetspolicy, där företagets mål för och inriktning på säkerhetsarbetet samt ansvarsfördelning framgår. Då policyn omsätts i praktiken bör utförliga ramar för vad som skall göras, hur det skall utföras och vem som skall utföra det sättas upp. Policys och ramverk för säkerheten måste, för att fylla sin funktion, föras ut i hela organisationen. Det är av vikt att alla känner till vad som gäller och även känner en delaktighet i säkerhetsarbetet.

Vid formuleringen av säkerhetspolicyn bör ledningen utgå ifrån en riskanalys av de befintliga systemen i företaget och finna procedurer för modifiering av de existerande systemen samt form för design och implementering av nya system. Därefter förs den framarbetade säkerhetspolicyn in i verksamheten och en beredskapsplan tas fram. Det gäller dock att inse att det inte räcker med att ha vidtagit åtgärderna en gång, då systemet och omvärlden hela tiden förändras. Av denna anledning krävs ständiga utvärderingar och uppdateringar av företagets säkerhet.

En konstruktivt formulerad IT-strategi, med tillhörande IT-policy där säkerhetsarbetet är klart formulerat, ger företaget en bra förutsättning för att skydda sin information. För att informationen i säkerhetspolicy och beredskapsplan skall ge avsedd effekt bör den vara utformad så att den är lätt att förstå och överskåda. All berörd personal skall kunna ta till sig innehållet för att själva kunna göra riktiga bedömningar, självklart är det viktigt *att* de tar del av materialet. Om materialet är alltför omfattande kan det i sig utgöra ett hot mot säkerheten, särskilt farligt är det om det finns stora avvikelser mellan säkerhetsdirektiven i en organisation och användarens förmåga att förstå och koppla dem till det vardagliga arbetet. Likaså kan allt för strikta policyregler få motsatt effekt, eftersom svensken i allmänhet, som Westman (1997) funnit, inte har mycket respekt för regler och att det snarare anses som kreativt att finna sin egen väg. Regler bör finnas för att erhålla en enhetlig syn på säkerhetsarbetet, men i vissa fall kan ett större personligt ansvar, som fungerar som motivator, för den enskilde individen ge ett bättre skydd för företagets information.

Det är, som Cardholm (1997) tidigare påvisat, viktigt hur säkerhetshandboken formuleras, eftersom en väl formulerad säkerhetshandbok idag ger företaget möjligheten att på laglig väg kunna hävda att information spridits mot företagets vilja. Det bör påvisas att information är något värdefullt. För att befästa allvaret med säkerhet bör personalen upplysas om att den som lämnar ut information till obehöriga riskerar åtal med påföljden på upp till sex års fängelse och den som mottagit informationen riskerar upp till fyra års fängelse. Säkerhetstänkandet ökar inom företaget i och med att de allvarliga konsekvenserna påvisas. Arbetsgivare är dock oftast inte särskilt intresserade av att föra ett mål mot en av sina anställda till domstol, men genom att de har lagens stöd understryks vikten av fungerande säkerhetsrutiner.

Ibland går företagsledningen en fin balansgång mellan att ge medarbetarna ansvar och information, för att skapa delaktighet och motivation i säkerhetsarbetet, och hota med vad som kan hända om de bryter förtroendet. Eftersom svensken i allmänhet har inte mycket respekt för regler, kan det i vissa fall vara bättre med tumregler än hot om straff.

Sveriges föråldrade lagstiftningen ger få svar på frågorna kring IT-säkerhet och de nya lagarna kommer även de att vara av generell karaktär. Det är därför desto viktigare att ligga i fas med utvecklingen och tänka till innan något händer. Systemen bör byggas med funktionella behörighetssystem, backup, rutiner och spårbarhet. Dessutom måste verksamheten skyddas ekonomiskt med försäkringar. I händelse av brott bör system ha förutsättningen att kunna presentera ett händelseförlopp i domstol.

7.1.2 Analys av hotbilden

Företagsledningen bör veta om att det finns luckor i systemet och att det bara är en tidsfråga innan någon upptäcker dem och utnyttjar dem. Det har dock konstaterats att svenska

företagsledare är dåligt medvetna om de hot som finns mot deras information. Ett steg i utvecklingen för säkrare svenska företag är alltså att öka medvetenheten om IT-säkerhet.

Först när en viss medvetandegrad är nådd kan ett IT-säkerhetssystem initieras. Eftersom IT-området är mycket omfattande är även säkerhetsaspekterna på IT många. Riskerna för företagets information bedöms i en sårbarhetsanalys. För att erhålla en så komplett hotbild som möjligt bör representanter från flera olika personalgrupper finnas med i analysarbetet. I sårbarhetsanalysen bedöms och utreds, ibland med hjälp av modeller som analysverktyg, konsekvenserna samt kostnaderna av varje tänkbar händelse. Eftersom IT-säkerheten berör hela verksamheten är det viktigt att bedöma vad som händer om t ex ett avbrott skulle inträffa. Genom att genomföra en sårbarhetsanalys och gå igenom säkerhetsriskerna ökas medvetenheten i säkerhetsfrågorna på arbetsplatsen och bidrar därmed till bättre säkerhet.

I riskanalysen bestäms även vilket försäkringsskydd verksamheten behöver. Detta försäkringsskydd skall skydda vid händelser som skadar näringsverksamheten. Företagsledningen bör sträva efter såväl ett optimalt som ett kostnadseffektivt försäkringsskydd.

De interna hoten mot företagets information kan delas upp i avsiktliga och oavsiktliga faktorer. Hoten mot informationens säkerhet brukar delas upp i fyra olika typer; avbrott, avlyssning, modifiering och fabricering. Till de avsiktligt orsakade incidenterna mot företags IT-system hör spionage, sabotage mot eller stöld av hårdvara, mjukvara och information, illasinnad attack av hackers, databedrägeri, m. fl. De oavsiktliga incidenterna orsakas bl a av okunskap, missförstånd, brist på uppmärksamhet, tekniska fel eller fel i systemdesignen.

Det finns en uppsjö av alternativ att välja bland om någon är ute efter att stjäla eller sabotera ett företags information. Ett relativt enkelt sätt att komma över information är att kapa en dator eller användararea, andra sätt är att spoofa eller scanna efter lediga portar i systemet alternativt att avlyssna aktiviteter på nätverk. Kryptering anses av många som ett fullgott skydd av information, men det är inte någon garanti för säker IT. Det krävs bara mer kunskap av den som utför attacken eller sabotaget. Den eller de som är ansvariga för säkerheten måste därför följa med i utvecklingen av hoten för att på så vis kunna sätta upp ett försvar mot dem.

Brotten mot IT-system ökar stadigt, även om många av olika anledningar inte rapporteras till polismyndigheterna. I och med det utvidgade utnyttjandet av internationella nätverk ökar även de kriminella IT-inbrotten från utomstående individer. Dessa kriminellt sinnade personer eller grupper ser möjligheter till stora belöningar för liten ansträngning. Risken för att bli upptäckt är dessutom väldigt liten.

Säkerhetsluckorna, i internationella nätverk som Internet, utnyttjas av hackers för att illegalt ta sig in i företags IT-system. Hackers kan utsätta IT-systemet för en rad olika typer av attacker. Till de vanligaste hör virus-, lösenords-, Denial of Service- och IP attacker. Hackers tar reda på koder och lösenord till andras datorsystem för att olagligt ta sig in i dem, vissa utövar även sabotage. Denna typ av hacker söker ofta uppmärksamhet och talar på något sätt om för såväl företaget som omvärlden att han / hon lyckats ta sig in i systemet. Andra typer av hackers är de som, i vinstsyfte, använder sin expertis för industrispionage. Dessa lämnar sällan några spår efter sig och företaget som blivit utsatt för bedrägeri vid monetära överföringar eller industrispionage kanske inte ens upptäcker det. Denna typ av agerande hotar den fria

konkurrensen eftersom konkurrenter måste kunna hemlighålla sina kunskaper och avsikter från varandra för att fri konkurrens skall råda.

I och med att kommunikationen över Internet stadigt ökar är det troligt att denna typ av affärskommunikation kommer att innebära ett stort hot mot säkerheten även i framtiden (Wedberg, 1997). Eftersom riskerna med Internet är relativt välkända har det medfört en ökad kännedom om försvar mot dessa risker, därmed kan det sägas att Internet har bidragit till ett ökat säkerhetstänkande i företagen. Vetskapen om en fara betyder inte att man vet vad som bör göras för att undvika den.

Studier har visat att det är relativt vanligt förekommande att försöka få tillgång till information som inte tillhör en själv. Tidigare utgjordes 80-95% de kriminella hoten mot företags IT-system av insiderbrottslingar, andelen insiderbrott har dock minskat i och med det ökade utnyttjandet av Internet. Under 1997 rapporterade Riksrevisionsverket att över hälften av databrotten utförts av utomstående, men uppgifter strider mot varandra och mörkerantalet anses vara stort. Det bör noteras att även om andelen insiderbrott minskar betyder inte detta att antalet minskar.

De interna hoten har länge varit ett problem. Organisationer som har datoriserat stora delar av sin verksamhet är beroende av skickligheten, engagemanget och integriteten hos IT-personalen, därför bör företagsledningen, alternativt säkerhetsansvarig eller enhetschef, vara uppmärksam på drastiska förändringar i en medarbetares beteende. Det bör uppfattas som varningstecken då någon medarbetare plötsligt visar tecken på ett högre leverne än tidigare. Likaså bör en medarbetares onormala arbetstider liksom stressymptom uppmärksammas och ifrågasättas, även om detta naturligtvis kan ha helt legitima orsaker. Den genomsnittlige insiderbrottslingen beskrivs som en medelålders anställd som känner sig åsidosatt av yngre medarbetare. Det har visat sig att det främst är genom missbruk av erfarenhet, inte teknisk kunskap, som den brottsliga handlingen utförs. Enligt ett känt talesätt är det tillfället som gör tjuven. Kan man i största möjliga mån försöker undvika att personalen utsätts för frestelse eller tillfälle, har man kommit en lång bit på vägen mot säker IT.

Eftersom det inte enbart är illasinnade personer som åstadkommer förödande effekter på företags IT-system, måste säkerhetssystemet även innefatta skydd mot att medarbetare helt oavsiktligt skadar IT-systemet. Undersökningar har visat att de vanligaste orsakerna till förlust av information är användarens vardagsslentrian och missuppfattningar kring hur information bör skyddas och lagras (Cardholm, 1997). Ibland kan det vara så att dokumentering och säkerhetsaspekter helt enkelt inte hänger med i den snabba utvecklingen. Misstag kan göras redan vid installering av hård- och mjukvara, felaktig information kan föras in i systemet, information kan förloras, modifieras eller avslöjas helt oavsiktligt i samband med PC-användning och det kan uppstå fel i backup-rutinerna. Att fela är mänskligt - därför får säkerhetsansvariga på olika sätt gardera IT-systemet mot tänkbara misstag. Artilleriet mot misstag heter information, utbildning, repetition och uppdatering.

Datoravdelningen har till stor del förlorat den kontroll den tidigare hade över systemen, i och med decentraliseringen i företagen som inneburit ett ökat utnyttjande av distansarbete, bärbara datorer, e-post och Internet. Teknikens utveckling kan innebära nya problem, som när personalen tar med sig sina bärbara datorer och därmed även information ut från företagets skyddande väggar. En person med nyckelposition i företaget kan ha riktigt känslig information

i sin dator såsom företagets strategier, offerter, kunder, konkurrenter osv. Om den informationen finns på en bärbar dator är den naturligtvis mycket svårare att skydda.

Då riskerna är klarlagda framträder hotbilden mot företagets IT, såväl externt som internt. Hotbilden bör då visa vad eller vem som kan utgöra ett hot mot företagets IT. Först då hoten är blottlagda kan företaget bygga upp ett försvar mot dessa hot, men eftersom företagsmiljön förändras hela tiden måste säkerhetsrutinerna omprövas kontinuerligt och riskanalysen bör vara en fortgående aktivitet.

Ur företagsledningens synvinkel är det av vikt att komma ihåg att den arbetstid, som medarbetarna använder till att hantera samt hjälpa varandra med olika datorrelaterade problem, skulle kunna användas till betydligt produktivare aktiviteter. Det är troligen omöjligt att gardera mot alla problem som kan uppkomma, men de vanligaste problemen bör i största möjliga mån minimeras. För att kunna minimera de datorrelaterade problemen måste de först och främst erkännas, för att sedan kunna lokaliseras och skyddsmekanismer av olika slag sättas in.

7.1.3 Ekonomiska aspekter

Ett avbrott i IT-systemet, oavsett anledning, medför konsekvenser i verksamheten såsom att tillgängligheten störs, att de anställda inte kan utföra sina arbetsuppgifter osv. Med tanke på att närmare hälften av de svenska börsnoterade företagen under 1995 och 1996 hade varit med om minst ett avbrott och över hälften av de undersökta företagen saknade en avbrottsplan, måste beredskapen hos svenska företag anses som dålig. 39% av företagen hade inte ens bedömt följderna av en katastrof. En policy som talar om hur medarbetare bör agera är ett gott hjälpmedel. Trots detta visade undersökningen att hälften av de börsnoterade företagen i Sverige saknade en skriven policy för IT-säkerhet. Dessa siffror tyder på stor okunskap eller möjligen nonchalans hos svenska företag vilket måste ses som oroande. Ytterligare ett exempel på att medvetenheten hos de svenska företagen är dålig är att det, trots att det nu mindre än två år kvar till år 2000, fortfarande finns företag som inte har anpassat sina system till skiftet.

De ekonomiska aspekterna på säkerheten är inte obetydliga. Ett IT-avbrott, oavsett anledning, kan kosta företaget stora pengar i återställningskostnader och utebliven produktivitet. Det är ekonomiskt kännbart med tekniska säkerhetsanordningar som accessystem och firewalls, men goda investeringar om de medför att kostnader som kan härledas till databrott och effekter av databrott till stor del kan undvikas.

Det finns ett stort mörkertal kring IT-brott med anledningar som tidigare nämnts, men klart är att IT-brottsligheten ökar och därmed även återställningskostnaderna. Då personalen ägnar sin tid åt att hantera problem med datorer kostar den anställde företaget i såväl lön som utebliven produktivitet. Beräkningar har visat att problem med datorer kostar svenska företag totalt 35 miljarder kronor per år. Detta kan jämföras med att företagens totala IT-investeringar under 1996 uppgick till 80 miljarder kr. Även om det inte är möjligt att effektivisera bort alla datorrelaterade problem inom företag, borde dessa siffror ändå fungera som en tankeställare.

Då de indirekta kostnaderna utgör närmare hälften av den summa som svenska företag lägger på IT-investeringar, borde det vara en rimlig slutledning att företagsledningarna faktiskt inte är medvetna om problemen. Denna slutsats styrks av att det har visat sig att hälften av alla incidenter beror på bristande rutiner, men många företag har inte någon översikt över de

ekonomiska konsekvenserna som en störning i systemet skulle medföra. Bristande rutiner bör till stor del kunna undvikas om företaget satsar på förebyggande verksamhet som till exempel utbildning. Säkerheten bör tillåtas att kosta, ta tid och plats i organisationen, men kostnaderna skall givetvis stå i rimlig relation till det säkerhetsåtgärderna avser att skydda.

7.1.4 Säkerhetssystemets konstruktion

Det finns en mängd olika typer av skydd för företagets information och lösningar på IT-relaterade säkerhetsproblem. Oavsett vilka säkerhetsåtgärder företagsledningen vidtar, så kan de aldrig vara helt säkert.

Då hotbilden och de ekonomiska verkningarna är blottlagda kan själva konstruktionen av säkerhetssystemet sättas igång. Säkerhetsarbetet går främst ut på att säkra företags integritet och försvara eller förhindra attacker mot företagets information och utrustning. IT-säkerhet kan enbart uppnås i system som är väldesignade och väl hanterade. I kontruktionen av ett säkert IT-system ingår åtgärder både för att förhindra och upptäcka incidenter som kan skada företagets integritet. I de förhindrande åtgärderna ingår kontroll av access, isolering och identifiering, till detta kommer övervakningsfunktionerna som ingår i de upptäckande åtgärderna.

För att skydda ett mindre företags information mot hackers, industrispionage och ohederliga medarbetare, bör först och främst de säkerhetsfunktioner som finns i nätverksoperativsystemet och applikationer användas, därefter kan säkerheten byggas på och användarnas möjligheter begränsas genom exempelvis en brandvägg mellan nätet och ingångarna. I medelstora, större, samt i företag med hög riskfaktor krävs kraftigare säkerhetssatsningar.

Det är av betydelse att veta vilken information som är viktig att skydda. Olika typer av information kan därför, menar Wedberg (artikel 2, 1997), delas upp i olika status, betydelse- och sekretessgrad. En överskådlig säkerhetsmatris över olika typer av information och personal kan upprättas för att ge en bättre översikt över vem som har tillgång till vad i systemet. Denna matris kan sedan fungera som ett stöd för såväl teknisk som annan personal, samt som en dokumentation över företagets säkerhetstänkande. För att strukturera upp informationstillgångarna ytterligare kan personalen tilldelas ansvar för information, datan kan klassificeras och regler för skapande, dubblering, överföring, förvaring samt radering av data kan upprättas.

Säker IT inkluderar såväl fysiskt som logiskt skydd. Det finns fem grundläggande faktorer som bör tas hänsyn till i upprättandet och underhållet av ett säkert IT-system. Först och främst inrättas ett rent fysiskt skydd kring byggnader och datorer. Därefter installeras accesskontroller som skall hindra obehöriga från att ta sig in i företagets system. Innanför detta skyddslager återfinns de administrativa kontrollerna och procedurerna som avser att hindra dem som redan är inne i systemet från att missbruka det. Därefter kommer beredskapsplanen, ifall att något ändå skulle hända. Förutom de fyra skyddslagren bör ett fullgott försäkringsskydd finnas, för att företaget skall ha ett ekonomiskt skyddsnät ifall alla de andra skyddslagren skulle misslyckas.

7.1.4.1 Fysisk säkerhet

Det mest primära i ett säkerhetssystem är den fysiska säkerheten. Den syftar till att skydda företagets materiella tillgångar, från byggnader till datorer. De materiella tillgångarna skall skyddas från hot som brand, vattenskada, intrång i fastigheten och avlyssning av

elektromagnetiska signaler. Även åtgärder som placering av datorcentralen inkluderas i detta yttersta skyddslager.

7.1.4.2 Accesskontroller

Accesskontrollerna skall förhindra att personer får tag på information de inte har rätt till och att lagrad data från att smittas ned. Ibland kan det vara en fördel att använda automatiska accesskontroller som ger företaget en garanti för att kontroll sker varje gång, till skillnad från de manuella som kräver åtgärder av användarna.

Den fysiska accesskontrollen syftar till att skydda fysiska komponenter av informationsprocessen eller lagringsmedia genom exempelvis lås eller vakt.

Accesskontroll med avseende på kommunikation har blivit en stor del av accesskontrollen i och med den ökade användningen av kommunikationslänkar för bl a finansiella transaktioner. Kommunikationssäkerheten bör vara så hög att det inte sker någon form av utlämning av information under överföring. Eftersom det inte finns någon universallösning på säkerhetshoten från Internet, krävs en rad strategier och tekniker. En idag vanlig del av det kommunikativa säkerhetssystemet är brandväggen. Den används främst för att begränsa accessen mellan det interna nätverket och Internet, men kan också användas för att separera två eller flera delar av det lokala nätverket. Det är viktigt att de ansvariga håller sig á jour med nyheter om såväl eventuella säkerhetsluckor som försvar mot dem, för att försöka få systemet så säkert som det är möjligt.

Den logiska accesskontrollen är till för att skydda IT-systemet mot dem som redan är inne i systemet och syftar till att begränsa tillgången till viss data eller mjukvara. Detta kan innebära att identifiera och verifiera användaren, men även en begränsning av användarnas accessprivilegier. Logisk kontroll innebär också övervakning av all användning av systemet.

Den sistnämnda accesskontrollen är den som ökar mest. Beräkningar har visat att 65% av summan som läggs på datasäkerheten i företag år 2001 kommer att läggas på att lösa problem med identifiering av användare och administration av säkerhetssystemet. Idag är lösenord den vanligaste identifieringsmetoden, men de svårimiterade biometriska identitetskontrollerna har vunnit marknadsandelar och antas bli mycket vanligare.

Användningen av kryptering i Sverige är idag omfattande. Kryptering är en viktig komponent i all accesskontroll och är fortfarande det mest kraftfulla redskapet för IT-säkerhet då det sörjer för bibehållande av både integritet och sekretess. Tekniken tillgodoser till stor del såväl näringslivets behov av säker kommunikation för företagskänslig information som enskilda personers behov av integritetsskydd.

Säker elektronisk kommunikation är en angelägen fråga som ökar i betydelse för var dag. Det är viktigt att uppnå en balans mellan brottsbekämpning och förtroende för systemet. Företagsintegritet och personlig integritet bör dock balanseras mot samhällets behov av skydd.

Det bästa sättet att kontrollera sin accesskontroll anses vara att utsätta systemet för en falsk attack. Det kan vara en fördel att anlita före detta hackers som arbetar som säkerhetskonsulter. De kontrollerar hur säkert IT-systemet är genom att iscensätta attacker mot det och analysera resultatet. Fördelen med att anlita en före detta hacker är att de är familjära med hackers

tankesätt. Nackdelen med att släppa in en sådan person i sitt system framträder om personen i fråga inte har slutat tänka som en hacker.

7.1.4.3 Administrativa kontroller och procedurer

Administrativa kontroller och procedurer avser att hindra dem som redan är inne i systemet från att begå misstag eller missbruka systemet. Till denna typ av kontroll räknas informationsflödeskontroll, olika sorters övervakning, utbildning, loggning av användare, hur pappersdokument hanteras i företaget samt säkerhetskontroll av personal.

Informationsflödeskontrollen bör användas dels för att förhindra oavsiktliga misstag från användarnas sida och dels för att kunna vara relativt säker på att informationen i systemet är korrekt. Det finns flera anledningar även till övervakning eftersom den fungerar både i avskräckande syfte och som varningsklocka då något inte är som det skall. Ibland räknas även personalutbildning i systemet och användarvänlig mjukvarudesign till de administrativa procedurerna. Loggning är en viktig komponent i den administrativa kontrollen på flera sätt, dels som styrande och dels som dokumenterande och kontrollerande funktion. Utan loggning står sig företaget slätt i bevisföringen vid ett inbrott i datorsystemet.

Det är inte enbart information inom datorsystemet som bör skyddas. Dokument i pärmar, lösa papper och noteringar kan också innehålla känslig information och därför bör även den pappersbaserade informationen innefattas i de administrativa kontrollerna och procedurerna. Till de administrativa procedurerna hör även säkerhetskontrollen av samtlig personal. För att undvika oklarheter om vad som gäller för vem kan säkerhetsrutinerna skrivas in i arbetsbeskrivningarna.

7.1.4.4 Företagets beredskap

Ifall något ändå skulle hända, trots de skyddslager som företaget satt upp, bör företaget ha någon form av beredskapsplan. Personalen måste ha klara instruktioner om vad de förväntas göra då något händer, så att de kan agera snabbt. I beredskapsplanen bör företaget ha tagit hänsyn till om de t ex behöver en extra server eller annan reservkraft i händelse av en nödsituation. Nödvändigheten av sådana åtgärder framkommer i risk- och sårbarhetsanalysen, då en bedömning av kostnaderna görs.

Virus är idag en vanlig företeelse som kan ställa till med stor skada, av den anledningen bör det finnas ett virusscanningsprogram som körs igång då datorn startas eller då en fil öppnas. En uppdaterad backup är bland det mest grundläggande i beredskapen då den garanterar att information inte går förlorad vid exempelvis en virusinfektion. Backupband och servern bör vara placerade på helt skilda platser.

7.1.5 Den mänskliga faktorn i säkerhetssystemet

Det finns många bra tekniska säkerhetshjälpmedel på marknaden idag, men dessa kan invagga företagsledningen i en falsk trygghet. Det räcker inte att enbart ha de tekniska säkerhetsmekanismerna, den mänskliga faktorn är minst lika viktig för ett fungerande säkerhetssystem. Det gäller för företagsledningen att komma ihåg att det inte går att uppnå säker IT om inte medarbetarna i företaget vill det, dvs företagskulturen bör vara positivt inställd till säkerheten. För att realisera mål som effektivitet, kvalitet och IT-säkerhet, måste ledningen betona dessa funktioner. Säkerhetstänkandet bör därför finnas med i allt företaget tar sig för.

Kvalitet i säkerhetsfrågor har blivit konkurrensmedel likaväl som ett marknadsföringsargument. Kunder och leverantörer behöver känna trygghet med avseende på integriteten och konfidentiella uppgifter i exempelvis transaktioner med företaget. IT-säkerheten måste ha en viss kvalitet liksom allt annat i ett företag.

De flesta av alla brister i datasäkerheten kan härröras till organisatoriska problem. För att uppnå IT-säkerhet krävs kontinuerligt arbete och underhåll, samt kunskap om både teknik och organisation. God säkerhet är resultatet av kontinuerligt arbete och en djupare förståelse för hur systemen och människorna i organisationen fungerar. Det är den optimala säkerheten som skall eftersträvas, risken är annars att säkerhetssystemet blir för krångligt och därmed en risk i sig själv eftersom medarbetare då söker sig runt det.

Företagets ledningsgrupp bör vara sammansatt så att den speglar företagets olika delar. Det är lämpligt att huvudansvarig för säkerheten eller jämbördig person är med i företagets ledning för att kunna ge säkerhetsaspekten på de förändringar som planeras. Personalvård är en viktig faktor i företagets strävan efter säker IT. För att göra ett bra arbete krävs det att medarbetarna känner ett visst ansvar för och delaktighet i sin arbetssituation. Delaktigheten i företagets utveckling och styrning kan bidra till att skapa lojalitet. Det är viktigt att överlåta till varje medarbetare att prägla sin egen situation, i såväl ordinarie arbetsuppgifter som säkerhetsarbetet, för bästa resultat.

Det är en brist i fall den enskilda individen inte ser helheten av sitt arbete eller inser sin egen arbetsinsats betydelse i företaget. Då man inte förstår det egna arbetets syfte i organisationen och inte heller ser sig som en del av företaget som helhet kan revirtänkande uppstå. Dvs man arbetar för sig själv, sin grupp, alternativt avdelning, då man inte ser det strategiska syftet med det egna arbetet. Det är en nödvändighet att se det meningsfulla i sitt arbete, eftersom det finns en risk att det uppstår konflikter i företaget när det uppstår motsättningen mellan att göra, förstå och att kunna påverka. Följden av att inte ha möjlighet att påverka kan bli att personal inte bryr sig om att göra något de ser och förstår borde bli gjort, eftersom de inte känner att de får något för det.

Säkerheten medför ofta merarbete för medarbetarna, av den anledningen är det viktigt att ledningen uppmuntrar en positiv attityd till säkerhetstänkandet, belönar funna säkerhetsluckor eller uppmärksammade incidenter eller liknande. Den största delen av god IT-säkerhet inkluderar utvecklingen av organisatoriska kontroller och motivation hos personalen som utför kontrollerna.

7.1.5.1 Motivation och kunskap

Det är bara genom att kontinuerligt utveckla kompetensen på området och anpassa systemen som säkerheten kan upprätthållas. Basen för det mer långsiktiga arbetet med säkerheten rör sig därmed kring mjuka faktorer som utbildning och motivering av personalen.

Motiveringen av medarbetarna till att deltaga i säkerhetsarbetet är en av grundförutsättningarna för att satsningen skall lyckas. Viljan att arbeta för säkerheten på företaget uppnås då medarbetarna känner lojalitet för företaget och samhörighet med övrig personal. Samarbete över personalgränserna skapar förståelse för andras problem och ger en helhetssyn på säkerheten. Motivation ges även av delaktighet i arbetet kring de säkerhetsproblem som rör just deras arbete. I och med att de blir införstådda i problematiken och får en djupare förståelse för hur säkerheten bäst bevaras, samt varför det är viktigt att skydda informationen, undviks konfliktsituationen som kan uppstå när det finns motsättningar mellan att göra, förstå och att kunna påverka. Följden av att ges möjlighet att påverka gör att de anställda (i bästa fall) bryr sig om att göra något som de ser och inser borde bli gjort, eftersom de då känner att de får något för det.

En stabil grund för säkerhetsarbetet etableras då det finns en förtrolighet mellan företagsledare och övriga anställda, eftersom det ger en atmosfär av samhörighet och trygghet på arbetsplatsen. Medarbetare som arbetar både för och med företaget i en positiv anda och med ett engagemang för det de gör, är både effektivare och säkrare ur företagets synvinkel. Revirtänkande i företaget bör av denna anledning till varje pris undvikas.

Den sociala sammansättningen existerar på olika nivåer inom företaget, dels på individnivå dels som en del av organisationen och även inom olika sociala grupper inom organisationen. Gruppernas normer och värderingar avgör form och innehåll av den information som överförs eller förmedlas, respektive tas emot och tolkas (Ronen, 1986). För att uppnå den optimala lösningen på säkerheten krävs därför att personal som känner företaget, de informella kanalerna, olika grader av betydelse för olika information, praktiska förutsättningar, de anställdas kapacitet osv finns med från början i säkerhetsarbetet.

Gemensamma värderingar bildar basen i en företagskultur, även om det kan finnas lokala subkulturer i stora och mångfacetterade strukturer. Värderingar spelar en stor roll för personalens motivationskraft. Motivationen är i sin tur avgörande för idékraften, entreprenörialiteten och för viljan till kvalitetsarbete. Företagsledningen kan i viss mån påverka företagskulturen. En svag företagskultur kan ibland vara det mest fördelaktiga för företaget, men utvecklingen i svenska företag pekar på att företagen anser att en stark kultur är att föredra. Kanske särskilt då det gäller säkerhetsarbete. Ledningen bör finna vägar att motivera och inspirera sin personal att alltid tänka i termer av säkerhet.

Ett större ansvar innebär för de flesta något positivt, även om det kan innebära en större arbetsinsats. Förtroendet, som ett ökat ansvar innebär, skapar stimulans och leder i bästa fall till förbättrade arbetsprestationer enligt Vedin (1993). Det finns flera sätt att stimulera personalen, många innebär ett avbrott i det ordinära arbetet som t ex en företagsutbildning. Människor handlar i syftet att åstadkomma ett av dem eftersträvat tillstånd. Därför kan motivering av de anställda ses i ett större perspektiv, det att personalen består av kapabla individer som är mogna att fatta sina egna beslut.

7.1.6 I korta drag

Ledningens ansvar tillsammans med de ekonomiska aspekterna på säkerhet utgör grundpelaren i företagets IT-säkerhet. För att kunna bygga upp skyddsmekanismer kring informationen måste först en viss medvetandegrad i organisationen uppnås. Informationen måste ses som en värdefull tillgång för att kunna behandlas som en sådan, dessutom måste systemen byggas på ett sätt som gör dem möjliga att skydda och kontrollera.

För att gardera mot de olika osäkerhetsfaktorerna byggs skyddslager kring informationen. Ytterst återfinns det fysiska skyddslagret mot brand, intrång, avlyssning mm. Ledningen bör se till att bara den som har rätt till viss information har tillgång till den genom accesskontroller såsom lösenord, brandväggar och kryptering. För att skydda mot personer som har rätt att vara i systemet används administrativa kontroller och procedurer, exempelvis övervakning. Dessutom används beredskapsåtgärder som backup, virusskydd och försäkringar.

Det räcker dock inte med de tekniska skyddsmekanismerna eftersom hoten främst är av organisatorisk natur. Det krävs att medarbetarna känner sig delaktiga och är positivt inställda till säkerhetsarbetet. Detta uppnås genom motivering och utbildning om varför säkerheten är nödvändig. Kulturen har stor betydelse eftersom den återspeglar hur människorna i organisationen ser på omgivningen och hur de beter sig. Det finns vissa möjligheter för ledningen att påverka kulturen i positiv riktning för säker IT.

För att uppnå säker IT krävs det av företagsledningen att den inser att det behövs, att det kostar, samt att personalen måste vara med i arbetet. De attacker som företagets information kan utsättas för finns det en mängd olika åtgärder/redskap för att förhindra, men utan medarbetarnas medverkan i säkerhetsprocessen är det inte möjligt att uppnå säker IT.

7.2 Erfarenhet av metod

Litteraturstudierna för denna uppsats har varit mycket omfattande. Det har varit svårt att finna material som varit direkt knutet till syftet för rapporten. Genom att använda en kvalitativ undersökningsmetod har jag haft möjlighet att se problemet ur flera synvinklar och tolka informationen jag erhöll. Undersökningen har varit starkt hermeneutiskt präglad i det avseende att jag behövt tolka delar för att nå helheten. Detta har jag gjort induktivt.

Oavsett hur objektivt jag avsett att tolka det insamlade materialet, kvarstår det faktum att tolkningar alltid är subjektiva.

Det har varit viktigt att jag haft ramen för uppsatsen klar för mig och letat efter de statiska aspekterna hos företeelsen IT-säkerhet. Jag erhöll kvalitativ information i sådan mängd att det kändes som en oöverkomlig uppgift att sammanställa den. Med denna uppgift hade jag stor hjälp av den grounded theory baserade modellen.

7.3 Egna reflektioner

Det har under arbetets gång blivit min övertygelse att säkerhet måste behandlas ur ett holistiskt perspektiv. Förutom de tekniska delarna av IT-säkerheten måste såväl organisation

som sociala element ingå för att uppnå säker IT. IT-säkerhet varken börjar eller slutar med datorn.

Mycket av det som skrivits i den här rapporten kan tyckas vara självklarheter, men undersökningarna jag refererar till i texten visar att det är ett faktum att svenska företag idag har ett dåligt IT-skydd och företagsledarna är dåligt medvetna om problemet. För att uppnå ett bättre skydd av svenska företags IT måste medvetenheten hos företagsledarna först och främst höjas innan övriga åtgärder kan sättas in.

7.3.1 Fortsatt forskning

IT-säkerhet är ett vitt område och jag har täckt vissa valda delar med denna uppsats. Eventuell fortsatt forskning på det spår jag slagit in på skulle kunna inkludera ett eller flera studieobjekt i form av företag som avser att initiera ett IT-säkerhetssystem i verksamheten. Eftersom detta är en lång process skulle en sådan studie kräva mycket tid och resurser. Förutsättningen för ett lyckat resultat av en sådan undersökning skulle kräva ett nära samarbete och förtroende mellan företag och forskare.

Litteraturförteckning

Andersen H (redaktör) (1994) ”Vetenskapsteori och metodlära - En introduktion”, Studentlitteratur, Lund.

Backman J (1985) ”Att skriva och läsa vetenskapliga rapporter”, Studentlitteratur, Lund.

Bonniers Lexikon (1994 - 1997) Bonniers Lexikon AB, *tryckt i Ljubljana.*

Bäck H & Halvarsson A(1992) ”Metodbok; Projekt och utredningar”, SNS Förlag, Stockholm.

Caelli W, Longley D & Shain M (1989) ”Information Security for managers”, Macmillan Publishers Ltd., Great Britain.

Carroll J M (1996) ”Computer Security”, 3:e upplagan, Butterworths-Heinemann, Boston, USA.

Czarniawska-Joerges B (1993) ”The three-Dimensional Organization - A Constructionist View”, Studentlitteratur.

Eliasson G, Fries H, Jagrén L & Oxelheim L (1984) ”Hur styrs storföretag? - En studie av informationshantering och organisation”, Liber Förlag, Stockholm.

Eneroth B (1984) ”Hur mäter man ”vackert”? - Grundbok i kvalitativ metod”, Natur och Kultur, Göteborg.

Holmström M (1995) ”Styrning i storföretag - En studie av styrningens utformning och omfattning i tre svenska koncerner”, Universitetet i Linköping, Linköping.

Kowalski S (1994) ”IT Insecurity: A Multi-disciplinary Inquiry”, (Doctoral Thesis), Stockholm Universitet, Stockholm.

Lönn T (1996) ”Morgondagens arbetskraft - Hur du attraherar och behåller ung kompetens.”, Konsultförlaget i Uppsala AB, Uppsala.

Macintosch N (1985) ”The Social Software of accounting and Information Systems”, John Wiley and Sons, London, Storbritannien.

Meadows A J(edited) (1991) ”Knowledge and Communication - Essays on the information chain”, Library Association Publishing Ltd, London, Storbritannien.

Molander B (1993) ”Kunskap i handling”, Daidalos, Göteborg.

Norstedts svenska ordbok (1990) Norstedts förlag, Göteborg.

Pfleeger C P (1989) ”Security in Computing”, Prentice Hall P T R, Englewood Cliffs, New Jersey, U.S.A.

Polesie T & Johansson I-L (redaktörer) (1992) ”Kommunikation mellan människor och organisationer”, Studentlitteratur, Lund.

Ronen S (1986) ”Comparative and Multinational management”, John Wiley & Sons, U.S.A.

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

Solarz A (1985) Datorteknik och Brottslighet, Liber, Stockholm.

Södergren B (1987) ”När pyramiderna rivits. Decentralisering i praktiken”, Timbro/Affärsledaren, Stockholm.

Vedin B-A (1993) ”Nätverk för produktion och kunskap - En framtidsstudie kring logistik, informationsteknik och miljö.”, Liber-Hermods AB, Malmö.

Yngström L (1996) ”A Systemic-Holistic Approach to Academic Programmes in IT Security”, Stockholm Universitet, Stockholm.

Periodika

Barron A (dec. 1996) ”On-line business set to take off”, Doing business on-line, Financial Time guide, U.K. sid 74

”Virushot” (1998, 3 januari), Borås Tidning, sid 12

Cardholm L (1997) ”Lagar skyddar företagets information”, IT-nyheterna nr 7, sid 6

Engholm A (1997) ”Total datasäkerhet inget att eftersträva”, Computer Sweden, nr 62, sid 6

Ericsson M (1997) ”Täpp till säkerhetsluckorna!”, Internetguiden nr 6, sid 16-17

Gustafsson M (1998, 8 januari) ”Stoppa förändringar före år 2000”, Borås Tidning, sista sidan

Gustafsson R (1997) ”Fyra hot mot din NT-server”, Nätverk&Kommunikation nr 7, sid 83-85

Harne A (1998, 8 januari) ”Hacker att hyra - Ian Vitek har dataintrång till yrke”, Borås Tidning, del 2

Höijer S (1997) ”Windows NT Server blir inte säkrare än man gör det”, IT-nyheterna nr 7, sid 8

Kullmar B (1997) ”Med sannolikhet kan det mesta vara möjligt”, ABC-bladet, nr 3, sid 25

”Net.news” (sept. 1997) Personal Computer World, sid 196

Nilsson Å (1996) ”Datorstrulet kostar 35 miljarder om året”, Computer Sweden nr 35, sid 4

Olander J (1997) ”Spårlösa hack för miljarder”, Computer Sweden nr 33, Bilaga Persondatorn, sid 8-9

Ottoson M (1997) ”IT-kommissionen vill ha fri kryptering”, Nätverkskommunikation nr 7, sid 32 och 37

”Senaste nytt” (1997), Mikrodatorn nr 10, sid 17-18

Skalin H (1997) ”Bara en sak är säker Du kan aldrig vara säker”, IT-nyheterna nr 7, sid 9

Skalin H (artikel 2, 1997) ”Så fungerar brandväggar”, IT-nyheterna nr 7, sid 9

Sundström J (1997) ” ”, ABC-bladet, nr 3, sid 18, 26, 30 - 31

Wedberg H (1997) ”Uppdatera säkerhetsrutinerna annars blir det dyrt” och ”Organisera IT-säkerhetsarbetet”, IT-nyheterna nr 7, sid 10

Westman R (1997) ”Dålig intern säkerhet utgör ett större hot än hackare”, Nätverk& Kommunikation nr 7, sid 41 - 46

Wickberg S (1997) ”Riskera lite är sunt”, ABC-bladet, nr 3, sid 24

Öhman S (1997) ”Backup löser inte alla problem”, ABC-bladet nr 3, sid 22

Internet

Flashback Hackers Archive: 1996 och 1997 (http://www.flashback.se/hack/1996. html) + (1997.html), 17 december 1997

Howard J D ”An Analysis Of Security incidents On The Internet 1989-1995”, (http://www.cert.org/research/JHThesis/Start.html), 9 oktober 1997

IT-kommissionens rapport 6/97, ”Inför en svensk policy för säker elektronisk kommunikation”, (http://www.itkommissionen.se/itsite/pdf.krypte.pdf), 9 september 1997

Russel D och Zwicky E D ”Getting a Handle On Internet Security”, Internet, (http://www.geocities.com/CapeCanaveral/3498/inetsec.htm), 9 september 1997

Kommunikationsdepartementet ”Riktlinjer för uppdrag till Statskontoret”, bilaga till regeringsbeslut nr. 11, Internet, (http://194.251.183.23:81/itsaker.htm), 25 sept. 1997

Övriga källor

Sundén J. Sajber, november 1997

Tolfsson M. Folksam i Borås, dialog under december 1997

Woodstock E. Advokatfirman Delphi, föreläsare vid STIS-seminarie i Borås 20 oktober, 1997

Föreläsningsanteckningar från kursen Computer Security vid Otago University, Nya Zeeland våren 1996

Föreläsningsanteckningar från kursen Vetenskap, teori och metod med inriktning mot informationssystem, Högskolan i Borås, hösten 1996

Anteckningar från föreläsningar i Ekonomi och Styrning, Högskolan i Borås, januari 1997