IT-SÄKERHET

- en fråga för ledningen
**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 utsätts 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** ............................................................................................................................... 5  
   1.1 Bakgrund ................................................................................................................................. 5  
   1.2 Problemdiskussion .................................................................................................................. 6  
   1.3 Syfte, målgrupp och avgränsning ......................................................................................... 7  
   1.4 Disposition av arbetet ........................................................................................................... 8  
   1.5 Definitioner ............................................................................................................................ 8  

2. **METOD** ...................................................................................................................................... 10  
   2.1 Val av ansatser ....................................................................................................................... 10  
      2.1.1 Positivistisk och hermeneutisk vetenskapsuppfattning ................................................... 10  
      2.1.2 Kvalitativa och kvantitativa metoder ............................................................................. 10  
      2.1.3 Induktiv och deduktiv forskningsansats ....................................................................... 11  
   2.2 Metoder i undersökningsprocessen .................................................................................... 11  
      2.2.1 Datainsamlingsmetoder ................................................................................................. 11  
      2.2.2 Teoretiska perspektiv .................................................................................................... 11  
      2.2.3 Datasammanfattningsmetoder ..................................................................................... 12  
      2.2.4 Urvalsmetoder .............................................................................................................. 13  
   2.3 Genomförande ...................................................................................................................... 13

3. **FÖRETAGSLEDNINGENS ANSVAR I IT-SÄKERHETSPROCESSEN** ........................................... 14  
   3.1 Strategier och regelverk ........................................................................................................ 14  
      3.1.1 Strategisk styrning av företag ........................................................................................ 14  
      3.1.2 Beslutsprocessen ............................................................................................................. 14  
      3.1.3 Delaktighet i besluten ..................................................................................................... 15  
      3.1.4 Ledarens personlighet .................................................................................................. 15  
      3.1.5 IT-säkerhetssystemet ...................................................................................................... 16  
      3.1.6 IT-strategi och IT-policy ............................................................................................... 16  
      3.1.7 Säkerhetsmanualen ....................................................................................................... 16  
      3.1.8 Nackdelar med pappersbaserade säkerhetsmanualer ..................................................... 17  
      3.1.9 Faran med alltför strikta regler ...................................................................................... 17  
      3.1.10 Lagar och regler .......................................................................................................... 18  
      3.1.11 Internationella skillnader i säkerhetsarbetet ............................................................... 18  
      3.1.12 Kvalitet på säkerheten .............................................................................................. 18  
   3.2 Ekonomiska aspekter på säkerheten .................................................................................. 19  
      3.2.1 Bristande rutiner ............................................................................................................ 20  
      3.2.2 Kostnader för IT .......................................................................................................... 20  
      3.2.3 Relationen till kunden ................................................................................................ 20  
      3.2.4 Risk- och sårbarhetsanalys ......................................................................................... 21  
      3.2.5 Bedömning av riskerna ............................................................................................... 21  
      3.2.6 Modeller som hjälper med i säkerhetsarbetet ........................................................... 22  
      3.2.7 Brister i säkerheten ..................................................................................................... 22  
      3.2.8 Försäkringsvillkor ........................................................................................................ 23  

4. **IT-SÄKERHET** .......................................................................................................................... 24  
   4.1 Hot mot den interna säkerheten ........................................................................................ 24  
      4.1.1 Intern säkerhet ............................................................................................................... 24  
      4.1.2 Faror eller risker för företagets information ................................................................ 24  
      4.1.3 Lönsamt att attackera IT-system .................................................................................. 24  
      4.1.4 Ethiska attityder ............................................................................................................ 25  
      4.1.5 Insiderbrott .................................................................................................................. 25  
      4.1.6 Personal och ansvarstugande ..................................................................................... 25  
   4.2 Avsiktliga attacker mot företags IT-system ........................................................................ 26  
      4.2.1 Kapningsattacker ......................................................................................................... 27  
      4.2.2 Olika sätt att attackera ett skiftersystem .................................................................... 27  
      4.2.3 Spoofing och scanning efter portar .......................................................................... 28
5.2 F

4.3 OAVSIKTLIGT ORSAKADE INCIDENTER .............................................................................................................. 35

5.1 Ö VERGRIPANDE ÅTGÄRDER FÖR INTERN SÄKERHET .............................................................................................................. 38

5.4.3 Loggning................................................................................................................. .................................. 52

5.3 A CCESSKONTROLL ............................................................................................................................... ............. 44

5.3.2 Kommunikationsaccesskontroll ............................................................................................. ................... 45

5.3.3.1 Accessrestriktioner .................................................................................................... ...........................................47

5.3.3.3.5 Kryptering ............................................................................................................. ...............................................49

5.3.3.3.2 Verifiera identitet .................................................................................................... .............................................48

5.3.3.1 Accessrestriktioner .................................................................................................... ...........................................47

5.3.3.3.2 Verifiera identitet .................................................................................................... .............................................48

5.3.3.4 Lösenordspolicy ........................................................................................................ ...........................................49

5.3.3.3.1 Accessrestriktioner .................................................................................................... ...........................................47

5.3.3.3.4 Lösenordspolicy ........................................................................................................ ...........................................49

5.3.3.6 Smarta kort ............................................................................................................................. 50

5.4 ADMINISTRATIVA KONTROLLER OCH PROCEDURER ......................................................................................... 51

5.4.2 Övervakning................................................................................................................................. 51

5.4.2.1 Fysisk övervakning........................................................................................................ .................................... 51

5.4.2.2 Logisk övervakning........................................................................................................ .................................... 51

5.4.3 Loggning ........................................................................................................................................... 52

4.2.4 Internet.......................................................................................................................................................... 28

4.2.5 "The Internet Worm" .................................................................................................................................. 29

4.2.6 Hackers ..................................................................................................................................................... 30

4.2.7 Industriisponjage med hjälp av datorer ................................................................................................. 31

4.2.8 Virus....................................................................................................................................................... 31

4.2.9 Makroprogram........................................................................................................................................ 31

4.2.10 Lösenordsattacker .................................................................................................................................. 32

4.2.11 Informationsserviceattacker .................................................................................................................. 33

4.2.12 Denial of Service attacker .................................................................................................................... 33

4.2.13 IP attacker .............................................................................................................................................. 33

4.2.14 Cookies .................................................................................................................................................. 34

4.2.15 Dödspringet ......................................................................................................................................... 34

4.2.16 Anonym inloggning ............................................................................................................................. 34

4.3 OAVSIKTLIGT ORSAKADE INCIDENTER .............................................................................................................. 35

4.3.1 Hemlighålla information .................................................................................................................................. 35

4.3.2 Vanligaste orsaken till utebliven produktivitet .......................................................................................... 35

4.3.3 Svenska företags beredskap .................................................................................................................... 35

4.3.4 Avbrott ..................................................................................................................................................... 35

4.3.5 Installationsproblem .................................................................................................................................. 36

4.3.6 Milleniumbomben .................................................................................................................................. 36

4.3.7 Förlust av filer ......................................................................................................................................... 36

4.3.8 Kompatibilitetsproblem .......................................................................................................................... 37

4.3.9 Minskad kontroll över systemen .......................................................................................................... 37

5. SKYDD OCH LÖSNINGAR PÅ IT-SÄKERHETSPROBLEM ................................................................................................. 38

5.1 ÖVERGRIPANDE ÅTGÄRDER FÖR INTERN SÄKERHET .............................................................................................................. 38

5.1.1 Begränsning av tillgängligheten.......................................................................................... ..................... 38

5.1.2 Ansvar för informationstillgångarna ........................................................................................................ 38

5.1.3 Säkerhetsmatriser och zonindelning ................................................................................................. 38

5.1.4 Elementen i ett säkert operativsystem ............................................................................................... 40

5.1.5 Pya grundläggande osäkerhetstyper ................................................................................................. 40

5.1.6 Skyddsdiagram kring informationstillgångarna .................................................................................. 41

5.2 FAKTÖRER FÖR DEN FYSiska SÄKERHeten .............................................................................................................. 42

5.2.1 Säkra byggnader .................................................................................................................................. 42

5.2.2 Brand ..................................................................................................................................................... 43

5.2.3 Placering av datorcentralen .................................................................................................................. 43

5.2.4 Avlyssning ............................................................................................................................................ 43

5.2.5 Intrång .................................................................................................................................................. 43

5.2.6 Godtagbart inbrottskydd .................................................................................................................... 44

5.3 ACCESSKONTROLL ................................................................................................................................. 44

5.3.1 Fysisk accesskontroll .......................................................................................................................... 45

5.3.2 Kommunikationsaccesskontroll ........................................................................................................ 45

5.3.2.1 Säkerhetslösningar för Internet .......................................................................................... 45

5.3.2.2 Hemsidor .................................................................................................................................. 45

5.3.2.3 Motringning ............................................................................................................................. 45

5.3.2.4 Brandväggar ............................................................................................................................. 46

5.3.3 Logisk kontroll .................................................................................................................................. 47

5.3.3.1 Accessrestriktioner ............................................................................................................................. 47

5.3.3.2 Verifiera identitet ............................................................................................................................. 48

5.3.3.4 Lösenordspolicy ............................................................................................................................. 49

5.3.3.5 Kryptering .................................................................................................................................. 49

5.3.3.6 Smarta kort ............................................................................................................................. 50

5.3.4 Falsk attack ........................................................................................................................................... 50

5.4 ADMINISTRATIVA KONTROLLER OCH PROCEDURER ......................................................................................... 51

5.4.1 Informationssödeskontroll ............................................................................................................... 51

5.4.2 Övervakning ........................................................................................................................................... 51

5.4.2.1 Fysisk övervakning ............................................................................................................................. 51

5.4.2.2 Logisk övervakning ............................................................................................................................. 51

5.4.3 Loggning ............................................................................................................................................. 52
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.


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 all IT-brott anmäls (Sundén, 1997). Anledningar som uppgavs var att företaget inte trodde att polisen skulle klara upp brotten och att en anmälan medför ”bad will” för företaget. I och med att brotten inte anmäls utan tystas ned i stället, när de heller inte media. Eftersom få konkreta exempel på IT-brottsligheten när 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 svårar 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 anmäljer informationstekniskt relaterade brott eftersom företaget 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 en unik ledarsammansättning, en egen historik som resulterat i erfarenheter som gäller just det speciella företaget, unika ekonomiska förutsättningar och personalkonstellation. Företagets lokaliserering, 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.

Uppsatsern 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.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet</td>
<td>internationellt nätverk av datanät som bygger på ett gemensamt överföringsprotokoll och datapaketförmedling över telenäten</td>
</tr>
<tr>
<td>e-post</td>
<td>elektronisk post, är den nätjäst som har störst räckvidd. Internetadressen är uppbyggd ungefär som en vanlig adress med namn, underdomän och toppdomän. (<a href="mailto:anna.andersson@skolan.se">anna.andersson@skolan.se</a>)</td>
</tr>
<tr>
<td>säkerhet</td>
<td>tillstånd som inte innebär fara, kan även betyda visshet. (Norstedt, 1990)</td>
</tr>
<tr>
<td>world wide web</td>
<td><a href="http://www">www</a>. Det allmänna internationella nätverket av websidor som finns på Internet.</td>
</tr>
</tbody>
</table>
2. Metod

2.1 Val av ansatser


2.1.1 Positivistisk och hermeneutisk vetenskapsuppfattning


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.


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


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
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 företeelhes 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


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 sekunderdata 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 bestämde mig för ett perspektiv kommer det att fungera som en ram för min förståelse

2 Grundén, ur föreläsninganteckningar från VTM-kurs 1996
och mina sinnen. Ramen styr uppmärksamheten mot viss information och förbi annan information.


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


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


Idealtypsmetoden, eller karikatymetoden, syftar till att forma en karikatyf 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 företeelsera statiska aspekter. Metoden försöker fånga det kännetecknande, dvs de gemensamma kvaliteterna för alla fall av
företeelserna och fastställa de **verkliga** 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

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 tänt och i annat fall sätta in korrigérande åtgärder.


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-beslutet 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 beslutskirkel (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.
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 berörda personal skall kunna ta till sig innehållet för att själva kunna göra riktiga bedömningar. Självlärdt är det viktigt att de tar del av materialet.

3.1.4 Ledarens 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


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 detaljerad 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 tungt och ineffektivt, han förespråkar därför ett tunt häfte med regler för att de skall vara lätt 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 checkclistor för de anställda att gå efter, telefonnummer till personer att ringa i
nödsituationer och ibland även vad som kan hänvisa 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
överskådliga 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 anställda 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 tvängsåtgärd kan få motsatt effekt. Westman
(1997) hävdar att svensken i allmänhet inte har mycket respect 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


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


3.1.12 Kvalitet på säkerheten


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).


### 3.2 Ekonomiska aspekter på säkerheten


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


### 3.2.2 Kostnader för IT

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


### 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)


3.2.4 Risk- och sårbarhetsanalys

3.2.5 Bedömning av riskerna

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


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 underkategorier, som i sin tur delas upp i två säkerhetsgrupper, en daglig och en akut.


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


---

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


I försäkringsbolaget Folksam fortsätter 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 säkerhetskopiaerad information ersätts av allriskförsäkringen. Ett tillverkande företag är särskilt särskilt sårbar 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 tilläggsförsäkrar för diverse kostnader som kan uppstå såsom extrakostnader vid avbrott, oförutsedda skada på maskin, rättskrydd, fasta kostnader i samband med nyckelpersons sjukdom, åtkomstskador med uppkommer i samband med avhjälpande av fel i arbeten, förlustskostnader som uppstår genom att en anställd i sin tjänst gentemot arbetsgivare begär 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 inbrottskyddskraven 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


4.1.1 Intern säkerhet


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.


4.1.2 Faror eller risker för företagets information


Till de avsiktligt orsakade incidenterna hör spionage, stöld av hårdvara, mjukvara och information, illasinnad attack av hackers, databräderi, 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


4.1.4 Etiska attityder
1986 gjordes en studie om etiska attityder och datoröverträdelser bland 135 kanadensiska och 158 svenska universitets studerande (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 svenska upptäcktes. (Om dessa siffror betyder att svenskarna i undersökningen var smartare än kanadensarna, eller om svenska säkerhetssystem var sämre än de kanadensiska, förblir iberesvarat.) 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.)


4.1.5 Insiderbrott

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 stjal 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 genomsnittliga 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 här för företaget och fortjänar 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 företagsskänslig 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 använda systemet utan handledar, 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 hämnadtankar och vill skada företaget så som det har sårat eller förörättat honom eller henne.

4.2 Avsiktliga attacker mot företags IT-system

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” privilegier genom ett allmänt konto. I det andra fallet var det studenter som genom en lösenordsattack kom åt skolans PC system eftersom systemet tillåtit upprepade inloggning. 

4.2.1 Kapningsattacker


4.2.2 Olika sätt att attackera ett skiffer system


\(^7\) 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

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


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).

IT-SÄKERHET - en fråga för ledningen

I mitten av 1995 förband Internet mellan 2 och 3 miljoner datorer över alla kontinenter, varav merparten i USA. En uppskattning av det totala användaraantalet hamnade då runt 30-40 miljoner. I december 1996 uppskattades användaraantalet 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.


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, 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.


4.2.6 Hackers


Världens troligen mest ”ansedda” hackerattack utfördes den 29:e september 1996 av svenska hackers, ”Power through Resistance”, mot CIA:s 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 rättstånd 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 dataexpertner, ofta från före detta östblocket. De arbetar enligt Delaney för stora företag, organiserade brottslingar och till och med andra länder underrättelsestjänster. Eftersom de är så avancerade lämnar de inga spår efter sig och företaget som blivit utsatt för industrispionage 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 mångmiljonkontrakten. 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 ska skada skada.


4.2.9 Makrovirus


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)


4.2.10 Lösenordsattacker

Det finns olika program som gissar lösenord med hjälp av ordlistor. För att utföra attacken behöver hackern administratörssättigheter 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 knackar 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.

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


4.2.13 IP attacker


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

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

4.3.1 Hemlighålla information


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 kolleger 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 ”läser sig” eller ”hänger
IT-SÄKERHET - en fråga för ledningen


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 fackterminer kan vara svåra att förstå och därmed följa.

4.3.6 Milleniumbomben


4.3.7 Förlust av filer

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

4.3.9 Minskad kontroll över systemen

5. Skydd och lösningar på IT-säkerhetsproblem

5.1 Övergripande åtgärder för intern säkerhet


5.1.1 Begränsning av tillgängligheten


5.1.2 Ansvar för informationstillgångarna


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 viktigt och vad som är mindre viktigt.


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 försvar av företagets integritet i olika försvarszoner och hoten i professionella och ”deltidsarbetande” bedragare.

**Bild 5.1** Schematisk översikt av datasäkerhet (Handbook of Security, Kluwer)\(^\text{13}\)


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 konstruktionen 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.

![Diagram](bild5.2)

**Bild 5.2 Elementen i ett säkert operativ system.**

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,

\[sid. 80 i Caelli, Longley och Shain, 1989 (egen översättning)\]
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) 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. (föreläsninganteckningar, 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 illusteras som ringar på vattnet kring informationstillgången som skall skyddas.

Ytterst finns det rent fysiska skydet 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 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 kommunikationskablar 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 byggnaterialet bör även inredning väljas i brandsäkra material. Givetvis bör det finnas brandlärm 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 regnovänder, 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 marknivån, att ha vattendetektorer under golvet, att inte ha vattensprinklers mm.


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 radera 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


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. Ställdörrar, 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 lästa 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 läshuset har spärranordningar som tillhållarlås eller dubbelcylinder (nyckel använts från både in- och utsida) och nödvändiga tillbehör. Dessutom måste det finnas slutbleck och godkända dörrförstärkningsbehör. För läsning med hänglås och beslag skall även de vara godkända av försäkringsbolaget. (Folksam, 1997)

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

5.3 Accesskontroll

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 informationsprocesssystem och dess lagrade data som nås via kommunikationslänkar. Kommunikationslänkarna är särbara för hackers som vanligtvis arbetar över modem via telenätet. (Skalin, 1997)


5.3.2.1 Säkerhetslösningar för Internet

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.


5.3.2.3 Motringning

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)


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.

![Diagram av demilitariserad zon](bild_5.4)

Brandväggens placering


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 säkerhetspolicyen 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.

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.


5.3.3.3 Lösenord


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).


---

16 Biometri är den vetenskapsgren som studerar biologiska problem med statistiska 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 förhålla 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)


5.3.3.5 Kryptering


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 på sig 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.


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 särskilt 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).


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 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.


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 överträdja 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 korrigerar 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, rödkontroller, vattensensorer mm. Accesskontroll som registrerar vem som t ex ännu lokaler med datautrustning, 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 tex en brandvägg. (Pfleeger, 1989)


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.


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
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


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


6.1.1 Brister i säkerheten beror på organisatoriska problem


6.1.2 Positiv attityd till säkerheten


6.1.3 Betydelsen av information

Soll 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 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. Soll 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

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.


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 vardagslentrian och missuppfattningar kring hur informationen skall skyddas och lagras. (Cardholm, 1997) Det är därför viktigt att den anställda 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.


56
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 ständig 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 missstag 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.


6.1.7 Revirtänkande

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 ansvarsämnelse 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,
techniska 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 försening 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


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


6.2.2 Kommunikation och interpersonella relationer


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.


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


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.


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, entreprenörialiteten och för viljan till kvalitetsarbete.


6.2.5 Företags informella struktur


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.


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.


Kultur är en kollektiv företeelse, som handlar om gemenskap. ”Det pragmatska perspektivet” innebär att mänskliga handlingar och handlingsvanor är primära. 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 företags värderingar och hjältemytyologi.

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

6.2.8 Företagskultur som styrmedel


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 pollicys.

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.


7. Slutdiskussion
Syftet med denna uppsats har varit att ur ett företagsledarspektiv 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 beskrivs 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 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-säkerhetsprocessen
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.

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 framarbetad 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, självlärande 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 avvikningar 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.


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 förändrade 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 fäst 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 Analyser av hotbild

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.


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, modifering 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.


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-inbrott 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 omvärlen av att han / hon lyckats ta sig in i systemet. Andra typer av hackers är de som, i vinstsyfte, använder sin expertis för industriionage. Dessa lämnar sällan några spår efter sig och företaget som blivit utsatt för bedrägeri vid monetära överföringar eller industriionage 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 insiderbrotsslingar, andelen insiderbrott har dock minskat i och med det ökade utnyttjandet av Internet. Under 1997 rapporterade Riksrevisionsverket att över hälften av databrott 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.


Eftersom det inte endast är illasinnade personer som ästadkommer 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 dokumerter och säkerhetsaspekter helt enkelt inte hänger med i den snabba utvecklingen. Misstag kan göras redan vid installation 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 fär 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 inneburi 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 försvaret mot dessa hot, men eftersom företagets IT
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 skyddsmechanismer 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 avbrottplan,
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,
kostar företaget stora pengar i återställningskostnader och utebliven produktivitet. Det är
ekonomiskt kännbart med tekniska säkerhetsanordningar som accesssystem 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-brotningsligheten ökar och därmed även återställningskostnaderna. Då personalen ägnar sin
tid åt att hantera problem med datorer kostar den anställda 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 slutsedning 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 kostta, 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 hotbilderna 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

can enbart uppnås i system som är väldesignade och väl hanterade. I konstruktionen 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 säkerhetsstänkande. För att strukturera upp

informationstillgångarna ytterligare kan personalen tillsdelas ansvar för information, datan kan

klassificeras och regler för skapande, dubblering, överföring, förvaring samt radering av data

can 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 skydds slager 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 skydds slagen bör ett

fullgott försäkrings skydd finnas, för att företaget skall ha ett ekonomiskt skydds nät ifall alla

de andra skydds slagen 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 skydds Lager.

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 utlämnning 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 å 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 svårimmerade 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 mjukvarudekalog 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 samtliga 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.

7.1.5 Den mänskliga faktorn i säkerhetssystemet


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.


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 loyaltyt 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 konflikt situationen 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.


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 skyddsmechaniser 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 skyddsstigar kring informationen. Ytterst återfinns det fysiska skyddsstiget 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 skyddsmechanismerna 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.

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 överkomlig 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 självtclarheter, 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.
Litteratursförteckning


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


IT-SÄKERHET - en fråga för ledningen


Periodika


”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 säkerhetskullorna!”, 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


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

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

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 säkerhetsrutinererna 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


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