Datasäkerhet - metoder för säkerhetsanalys

(HS-IDA-EA-98-408)

Lars-Johan Furborg (a95larfu@ida.his.se)

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

Examensarbete på det dataekonomiska programmet under vårterminen 1998.

Handledare: Lennart Börjesson

Datasäkerhet - metoder för säkerhetsanalys

Examensrapport inlämnad av Lars-Johan Furborg till Högskolan i Skövde, för Kandidatexamen (BSc) vid Institutionen för Datavetenskap.

1998-06-08

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

Signerat: _____

Datasäkerhet - metoder för säkerhetsanalys

Lars-Johan Furborg (a95larfu@ida.his.se)

Key words: computer security, methods for analysing security

Abstract

Today most organisations have some sort of computer system. These systems are exposed to different threats which could be everything from unintended system disturbance to external attacks and sabotage from hackers. They could lead to loss of important information or stop in the production and cost the organisation a lot of money. To analyse the different threats the organisation can be exposed to is therefore very important. One way of avoiding this threats is to use a complete method for analysing the security. This methods is used for identifying the possible risk and to give support for taking further action.

This paper examines what methods can be used and their advantages and disadvantages. Furthermore a number of organisations has been investigated to see how they handle this issues.

Innehållsförteckning

Bilagor

Sammanfattning

Verksamheters datasystem är i dag utsatta för en mängd olika hot och risker. Dessa kan vara allt från oavsiktliga driftstörningar och slarv av personal till angrepp utifrån och sabotage. De kan leda till förlust av viktig information eller till stopp i produktionen och kan bli mycket kostsamma. Det är därför viktigt att ringa in vilka risker och hot som finns för verksamheter av olika slag

Ett sätt att förebygga risker och hot är att använda en färdig metod för analysera säkerheten. Metoder för att analysera säkerhet handlar om att identifiera de risker som kan uppstå. Därefter har man en handlingsplan för var de förebyggande insatserna bör sättas in.

I detta arbete har jag försökt att belysa de viktigaste metoderna för att analysera säkerhet. Det finns i rapporten också en genomgång vilka riskerna mot olika typer av verksamheter kan vara. Den viktigaste delen av rapporten är undersökningen som jag utfört på ett antal organisationer för att se hur säkerhetsarbetet bedrivs i praktiken.

Genom att studera litteratur, främst om metoder för att analysera säkerhet och sedan jämföra denna med min undersökning om hur ett antal organisationer bedriver sitt säkerhetsarbete, har jag bl.a. sökt besvara frågeställningen ”hur analyseras säkerheten i vissa verksamheter”. Resultatet och de slutsatser jag har kommit fram till finns redovisade i denna rapport.

1 Bakgrund

Det här examensarbetet kommer främst att behandla olika metoder för att analysera datorsäkerhet

Datorsäkerhet är en sektor inom databranschen som expanderar kraftigt. Det kommer ständigt nya produkter och verktyg som erbjuder skydd för datasystem. Paradoxalt nog ökar ändå intrången och metoderna blir mer sofistikerade anser Sjögren (1996). Även personer med begränsad datorkunskap kan på Internet hitta program som hjälper till att ”hacka” datorsystem.

Hoten mot företag och organisationer ökar allt eftersom informationsutbytet expanderar och datorer över hela världen blir mer och mer sammankopplade med varandra. Därför är det viktigt för företag och organisationer att ha ett fullgott och kontinuerligt skydd för kritisk information.

2 Inledning

2.1 Allmänt om inledningen

I detta kapitel kommer jag att definiera viktiga begrepp och klargöra väsentliga sammanhang för att ge läsaren förståelse för området som jag kommer att avhandla. Detta kapitel kan ses som en introduktion till ämnet datasäkerhet och kan hoppas över av personer med goda kunskaper om ämnet.

2.2 Information

2.2.1 Informationsbegreppet

Enligt Edlund m.fl. (1989) är definitionen på information:

> ”sammanställda och behandlade data som presenteras på ett sådant sätt att den får ett meningsfyllt innehåll.”,
>
> (Edlund m.fl., 1989 s. 103)

Andra definitioner finns om vad information är, men jag anser att denna tillhör de bättre, eftersom den också indirekt förklarar skillnaden mellan information och data. Gemensamt för de olika definitionerna är dock att information anses vara en vidareutveckling av data. Exempel på information kan vara t.ex. fakta om marknader, kunder, försäljning, bokföring, prognoser och konkurrenter.

Edlund m.fl. (1989) menar att information är en av företagens viktigaste resurser och bör därför skyddas likväl som de mer påtagliga av företagets tillgångar, exempelvis pengar och byggnader. Information kan för företaget vara ytterst väsentlig kunskap som t.ex. forskningsresultat och försäljningssiffror. Detta är kunskaper som konkurrenter skulle ha stor nytta att ta del av och därför är det ytterst viktigt att hindra utomstående att komma åt viktig information.

Informationsmängden i Sverige växer med 12 % årligen enligt Freese och Holmberg (1993). Samtidigt som mängden information växer ökar också kraven på att vara uppdaterad för att fatta viktiga beslut. Förvaltning av information har därför blivit en av de största uppgifterna för företag och myndigheter anser Freese och Holmberg (1993).

2.2.2 Intern och extern information

Intern information är framtagen för bruk inom den egna verksamheten. Denna information bör klassificeras efter hur känslig den är och bara göras tillgänglig till personalgrupper som har behov att ta del av den. Intern information bör bara i undantagsfall vara tillgänglig för personer utanför företaget. Exempel på intern information är bl.a. internredovisning, kundregister och forskningsresultat enligt Edlund m.fl. (1989).

Extern information är information speciellt framtagen för intressenter utanför företaget. Det handlar om information som inte är känslig för företaget utan fakta som presenteras, t.ex. kataloger annonser och intervjuer. Det kan också vara information som företaget är lagstadgad att dela med sig av t.ex. årsredovisning och uppgifter till myndigheter (Edlund m.fl., 1989).

2.2.3 Behov av informationsskydd

Olofson (1997) redovisar att en nyligen gjord undersökning i USA visar att 42 % av de tillfrågade företagen har haft intrång i sina system det senaste året. Detta tycker jag visar hur bristfälligt informationsskyddet många gånger är.

Eftersom det är svårt att ta reda på exakt vad som har gjorts vid ett intrång, kan det vara svårt att lita på systemets informationen efteråt. Freese och Holmberg (1993) anser att detta var fallet efter ett intrång i Vägverkets datasystem. Vägverket som anses ha en ganska hög säkerhet fick vid ett tillfälle intrång i ett par av sina datorer. Efteråt var det omöjlig att säga exakt vad inkräktarna hade gjort inne i systemet. Detta resulterade i att man tvingades tömma alla datorer på information för att därefter rekonstrueras den. Hela affären ledde till mycket höga kostnader för vägverket enligt Freese och Holmberg (1993).

Enligt en undersökning presenterad av Granlund (1997) åstadkommer ”hackaren” följande vid intrång i företags datasystem:

- Otillåten åtkomst till systemet 14,6%
- Åtkomst till e-post och andra dokument 12,6%
- Inplantering av olika virus 10,6%
- Åtkomst av affärshemligheter 9,8%
- Nedladdning av filer 8,1 %
- Ändrat information 6,8%
- Installerat lösenordssniffer (dvs ett program som letar efter lösenord) 6,6%
- Låst hela systemet 6,3%

Detta visar enligt min uppfattning att det ofta är allvarliga och kostsamma händelser som inträffar vid intrång och därför är det mycket viktigt med ett heltäckande säkerhetsarbete. Speciellt allvarligt anser jag det faktum att var tionde intrång leder till åtkomst av affärshemligheter. Detta borde vara en alarmklocka för de flesta säkerhetsansvariga.

2.2.4 Förvaltning av information

För att kunna förvalta information är det enligt Freese och Holmberg (1993) nödvändigt att klargöra följande:

- Vem äger informationen?
- Vilken information har vi behov att skydda?
- Vilken säkerhetsgrad krävs?

Det är ägaren av informationen som är ansvarig för att den skyddas på ett sådant sätt att trovärdighet och kvalité upprätthålls. Datalagen definierar vem som enligt lagens mening är ansvarig (ägare). En kritisk faktor i förvaltning av information är människorna som handhar informationen. Därför är det viktigt att definiera vilken information som ska vara fritt tillgänglig för alla och vilken som måste begränsas till vissa personalgrupper. Denna indelning är viktig för säkerhetsarbetet och graderingen av information bör därför formaliseras framhåller Freese och Holmberg (1993).

2.2.5 Lagstiftning

Datalagen är den lag som främst behandlar informationsfrågor för datasystem. Lagen reglerar hur dataregister skall hanteras och hur tillstånd till register erhålls. Lagen är bl.a. till för att skydda den personliga integriteten, tvinga registerägaren att ändra felaktiga uppgifter samt att ålägga registerägaren att hålla ordning i registren. Alla personregister måste anmälas till datainspektionen som hanterar lagens efterlevnad. Datalagen innehåller en dataintrångsparagraf. Denna reglerar hur register skall skötas ur säkerhetssynpunkt och kräver bl.a. att det finns en säkerhetsorganisation hos de registeransvariga, (Freese och Holmberg, 1993).

I Sverige finns enligt Elgemyr och Mattson (1992) en ny lag sedan 1990 som innebär att information som är företagshemlig måste märkas. Om detta inte görs kan brott mot lagen inte straffas. Därför är det viktigt att rutiner för märkning av företagshemlig information formaliseras så att arbetet med detta sker kontinuerligt.

För offentliga myndigheter gäller tryckfrihetsförordningen. Denna förordning reglerar medborgarnas rättighet att ta del av offentliga handlingar. Undantag gäller dock sekretessbelagda handlingar framhåller Elgemyr och Mattson (1992).

2.3 Säkerhet

2.3.1 Datasäkerhet

På samma sätt som ordning är frånvaro av kaos menar Elgemyr och Mattson (1992) att säkerhet är frånvaro av osäkerhet. Av detta påstående kan man dra slutsatsen att ett säkert datasystem är ett system som skyddas kontinuerligt och heltäckande. Naturligtvis är det omöjligt att ha ett hundraprocentigt skydd för all information och prioriteringar måste därför göras. Dessa prioriteringar är en del av vad som kommer att behandlas i denna uppsats.

Samma författare menar också att uppnå säkerhet har ett egenvärde i all verksamhet och att ett säkert företag aktivt satsar resurser på att minimera risker, förebygga skador och utforma organisationen ur ett säkerhetsperspektiv.

2.3.2 Säkerhetsansvar

Ansvar och styrning för säkerhet är mycket olika i olika verksamheter. Detta beror på en mängd faktorer, t.ex. organisationens storlek, ledningens intresse av säkerhetsfrågor, ansvarsfördelning inom organisationen och säkerhetspolicyn.

Arbetet med säkerhetsansvar bör enligt SIG Security (1997) börja med att man inrättar en organisation för säkerhet, eller på ett mindre företag en säkerhetsansvarig. Därefter bör man införa administrativa regler och rutiner för styrningen av säkerheten. Detta ger en bas för säkerhetsarbetet

SIG Security (1997) menar att det är ledningen som har det yttersta ansvaret för informationssäkerheten och detta ansvar försvinner inte vid delegering. De bör därför vara insatta i säkerhetsskyddets betydelse. De bör upprätta ett övergripande dokument, en säkerhetspolicy som beskriver inriktningen på företagets säkerhetsarbete.

De anställda bör aktivt vara med i säkerhetsarbetet och bör därför involveras på ett tidigt stadium av arbetet. De anställda ska vara väl informerade om säkerhetsbestämmelserna för att på så vis kunna följa dem.

2.3.3 Systemsäkerhet

Enligt SIG Security (1997) är det viktigt med god systemsäkerhet för att:

> ”säkerställa att data med en kvalitet som fastställts av verksamheten finns tillgänglig för behöriga användare enligt verksamhetens specificerade krav.”
>
> (SIG Security, 1997, s. 81)

Samma författare menar att detta uppnås genom att det finns en samverkan av företagets metoder och tekniker för kontroll av användare, t.ex. genom samordning av behörighetskontroller, spårbarhet och säkerhetsloggning. Men systemsäkerhet handlar också om att ha pålitliga operativsystem och databaser, samt att ha ett aktivt och heltäckande skydd för exempelvis obehöriga intrång och virus.

2.3.4 Kostnad för säkerhet

För att räkna ut hur mycket säkerhet får kosta måste man enligt Edlund m.fl. (1989) bedöma de risker en verksamhet är utsatt för och jämföra dem med de kostnader som uppstår om de inträffar.

Genom att bedöma sannolikheten för en händelse och analysera konsekvenserna som händelsen ger upphov till får man en riskbild.

Konsekvenserna av en händelse beräknar man med:

- Skadefrekvensen - Talar om hur ofta en negativ händelse beräknas inträffa.
- Skadekostnaden - Talar om vilka kostnader en negativ händelse medför.

Med hjälp av dessa begrepp kan man använda formeln:

Skadekostnad * Skadefrekvens = Riskkostnad

Genom att räkna ut riskkostnader får man siffror på hur olika hot mot företaget kan graderas. Detta kan vara till som hjälp vid beslut om vilka säkerhetsåtgärder som bör prioriteras.

2.4 Kommunikationer, nätverk och datasystem

2.4.1 Central databas och client server

2.4.1.1 Central databehandling

Enligt Roberts och Kane (1989) har en central dator eller mainframe ett antal terminaler uppkopplade mot sig. Antalet terminaler kan vara allt från några stycken till tusental. All bearbetning av data sker i centraldatorn och terminalerna är ”dumma”, dvs de behandlar ingen data själva. Terminalerna kan befinna sig i samma byggnad som centraldatorn eller finnas flera mil bort. Exempel på system som använder centraldatabehandling är UNIX och as/400.

Centraliserad databehandling innebär enligt Grate (1994)

Fördelar:

- god kontroll över informationen som bara behöver lagras och bearbetas i datacentralen.
- god kontroll över utskrifter och kopiering

Nackdelar:

- dyr maskinvara
- programvara som ofta är mycket komplex och dyrbar
- högt utnyttjande av telekommunikationer (kan bli mycket dyrbart)
- Extrem sårbarhet - om den centrala datorn slås ut stannar datoranvändningen.

2.4.1.2 Client server

Enligt Grate (1994) handlar client server om pc datorer som är uppkopplade i någon form av lokalt nätverk eller LAN (Lokal Area Network). Ett lokalt nätverk består av pc datorer som är sammankopplade mot varandra och har ett antal servrar där vissa applikationer och gemensamma databaser finns. Datorerna kan också dela på ett antal skrivare. I pc miljö utförs alla beräkningar av de enskilda datorerna.

Client server innebär enligt Grate (1994)

Fördelar

- minimal sårbarhet
- relativt billig maskinvara
- överskådlig och relativt billig maskinvara
- billiga kommunikationslösningar och minimalt utnyttjande av telelinjer

Nackdelar

- dålig kontroll över informationen som lagras och bearbetas på ett stort antal ställen i ett nät
- dålig kontroll över utskrifter och kopiering

2.4.2 Intranet

Intranet är enligt Hedemalm(1997):

> ”ett internt nätverk inom ett företag eller annan organisation som använder webfunktioner och annan Internetteknik i liten skala.”
>
> (Hedemalm, 1997, 143)

Ett intranet kan ha en anslutning till Internet men måste inte ha det. Eftersom intranet kan användas med ett det lättförståeliga gränssnitt som webbrowsers blir det relativt användarvänligt, vilket är bra för organisationer som snabbt och enkelt behöver sprida information till medarbetare. Användaren kan använda det enkla gränsnittet utan att förstå tekniken bakom det. Intranet behöver inga nya tillbyggnader på det befintliga nätverket, eller datastrukturen, det räcker med att nätverket klarar att hantera TCP/IP. Gamla system klarar dock inte alltid att hantera TCP/IP enligt Gunnarsson (1996).

2.4.3 Extranet

Definitionen på ett extranet är enligt Loshin (1997):

> ”Ett nät som korsar organisations gränser och ger därigenom utomstående tillgång till resurser och information, som är lagrat i organisationens interna nätverk”

(Loshin, 1997, s. 265):

Enligt Bort och Felix (1997) är det svårt att definiera exakt vad som ryms i begreppet extranet. Men de menar att det centrala i begreppet är att information utbyts mellan organisations gränser, t.ex. genom att kunder och leverantörer släpps in på det interna nätverket. Loshin(1997) anser i sina definitioner av extranet att det är ett krav att Internetteknik används för att det skall kunna kallas extranet.

2.4.4 Extern kommunikation

Extern information definieras av Dataföreningen i Sverige (1997) som

> ”datorkommunikation som sker över ett eller flera nät där den egna verksamheten saknar kontroll/styrning över nätets användning.”
>
> (Dataföreningen i Sverige, 1997 s.107)

Extern datorkommunikation kan genomföras genom en kopplad förbindelse vid varje kommunikationstillfälle t.ex. via telefonnätet, via fast förbindelse eller genom trådlös förbindelse t.ex. radioförbindelse eller laserlänk.

Dataföreningen i Sverige (1997) menar att det finns en rad risker förenade med extern datorkommunikation. Obehörig avlyssning går till så att någon kopplar in utrustning för att kunna avlyssna datorkommunikationen någonstans på nätet. En annan risk är obehöriga intrång. Risken för obehöriga intrång ökar naturligtvis när de kan göras på stora avstånd och därför blir svårare att upptäcka.

2.4.5 Internet

2.4.5.1 Historik

Enligt Gunnarsson (1997) började Internet som ett militärt forskningsprojekt. Myndigheten som hade hand om denna forskning döptes till ARPA (Advanced Research Projects Agency). Nätverket konstruerades för att fungera även om delar av det slogs ut. Därför har Internet inte någon central punkt och varje paket kan välja sin egen väg utifrån givna förutsättningar.

Grunden till det som idag kallas Internet uppkom när forskare och studenter vid några stora universitet i USA kopplades till nätverket. 1988 kopplades sju länder utanför USA till Internet däribland Sverige. Under de följande åren anslöt sig allt fler till nätverket. Antal datorer på Internet har i stort sett fördubblats varje år sedan 1982 och i juni 1996 fanns det nästan 13 miljoner värddatorer (Gunnarsson, 1997).

2.4.5.2 Användningsområden

Internets huvudsakliga användningsområden är enligt Dataföreningen i Sverige (1997) att:

- göra information tillgängliga för andra
- inhämta information
- utbyta information genom exempelvis elektronisk post eller diskussionsgrupper

Dessa funktioner är användbara för de flesta företag, offentliga myndigheter och organisationer då ett effektivt informationsutbyte blir allt viktigare i dagens samhälle.

2.4.5.3 Anslutning till Internet

Vid anslutning till Internet via en operatör kan man välja vilka tjänster som man vill ha tillgång till, exempelvis elektronisk post, tjänster för newsgroups och WWW (World Wide Web). Uppkopplingen till Internet sker via antingen modem (analogt eller ISDN) eller via fast uppkoppling, (Dataföreningen i Sverige, 1997).

För att behålla en grundläggande säkerhetsnivå vid Internetuppkopplingar bör man ha en sk brandvägg (firewall). Brandväggar reglerar trafiken in och ut från det lokala nätverket till Internet, (Dataföreningen i Sverige, 1997).

2.4.5.4 Säkerhet på Internet

En Internetuppkoppling innebär alltid en viss säkerhetsrisk. Detta eftersom Internet inte har någon ansvarig kontrollfunktion men också p.g.a. hot från hackers.

Riskerna med en fast anslutning till Internet är enligt Dataföreningen i Sverige (1997):

- att ett stort antal kontaktvägar kommer in i systemet som inte finns någon kontroll över, om inte speciella skyddsåtgärder vidtas
- en stor risk att få in datavirus. Denna risk har ökat då datavirus även har börjat uppkomma i nya former, t.ex. som bilagor till epost och som makrovirus.
- risk för att det oavsiktligt uppstår oskyddade möjligheter till s.k. bakvägsuppkopplingar som kan vara svårt att förhindra.

2.5 Hot mot företag och andra organisationer

2.5.1 Inre angrepp

Elgemyr och Mattson (1992) definerar inre angrepp som:

> ”Brott riktat mot företag eller organisation till vilken gärningsmannen har en naturlig tillhörighet eller behörighet.”
>
> (Elgemyr och Mattson, 1992 s. 140)

Samma författare menar att inre angrepp inte ofta syns i statistik eftersom de sällan blir offentliga. Företag vill inte skylta med att de blivit utsatta av denna typ av angrepp eftersom det kan skada deras anseende. Av samma orsak leder det sällan till polisanmälan. Ofta kan angreppen vara en kombination av inre och yttre angrepp, t.ex. stölder med både medarbetare och utomstående inblandade.

Ser man till värdena som försvinner är det främst trolöshet mot huvudman, bedrägeri och förskingring, som ger de största ekonomiska kostnaderna. Stölder begås ofta av yngre anställda som inte varit i tjänst längre än ett år, medan ekonomiska brott ofta begås av personer med förtroendeuppdrag som varit anställda en längre tid, (Elgemyr och Mattson1992).

2.5.2 Databrottslighet

Databrottslighet kännetecknas enligt Freese och Holmberg (1993) av

> ”Olovliga handlingar där kunskap om och bruket av datorer är nödvändiga för att kunna genomföra handlingen”
>
> (Freese och Holmberg, 1993, s. 36)

Samma författare delar in databrott i två huvudkategorier:

- Handlingar där datorer används för att begå den straffbara handlingen: t.ex. bedrägeri, svindel och stöld.
- Handlingar där datorn eller datamediet är objektet: t.ex. vid ändring av data i skadesyfte, spridning av virus eller spionage.

Att få ett riktigt grepp om hur utbredningen av databrottslighet är svårt eftersom mörkertalet är stort och företag i många fall inte vill anmäla denna typ av brottslighet.

En annan svårighet med denna brottslighet är hur lagstiftning ska tillämpas. Schwatau (1994) menar att ett stort problem är vilken lagstiftning som ska gälla vid brott som utspelas på stora internationella datornät, t.ex. Internet. Ett datainbrott som sker i en delstat (i USA) och som utförs via det nationella nätverket av kommunikationsförbindelser kan ha tagit sig genom sex olika delstater. Svårigheter ligger också i om federal eller delstatlig rätt ska gälla.

Sätter man in detta resonemang i ett internationellt perspektiv uppenbarar sig ett gigantiskt problem. Om det är svårt att inom ett land att avgöra hur lagar ska tillämpas, hur är det då inte när datornät och kommunikationer knyter samman länder över hela världen. Problem som kan uppstå är t.ex. att de nationella lagarna står i konflikt med varandra, det kan vara svårigheter att fastställa var brottet ägt rum och brister på lagar om denna typ av brottslighet.

2.5.3 Industrispionage

Schwatau (1994) menar att industrispionage mellan företag är svårt att upptäcka och ännu svårare att bevisa, eftersom de i praktiken ofta är mycket svåra att spåra. Många företag har dåligt skydd mot denna typ av attacker, eftersom de ofta anses som ganska osannolika. Att få reda på hur stora förlusterna är för företag drabbade av spionage är svårt.

Spionage kan förekommer med hjälp av datorer. Detta p.g.a. att företagsinformation i allt större grad lagras på datorer, samt att datorer blir mer sammankopplade till varandra. Ett inbrott med hjälp av dator är dessutom svårupptäckt. Kostnaderna om resultaten från ett dyrt forskningsprojekt kommer på avvägar kan bli höga och helt eliminera fördelarna ett projekt var tänkt att ge. Drivkraften bakom industrispionage är alltså att få tag i värdefull information, anser Schwatau (1994).

Industrispionage förekommer på både nationell och internationell nivå. På internationell nivå handlar det om storföretag som spionerar på varandra men också om hur länder spionerar på varandra, t.ex. för att få reda på försvarshemligheter.

2.5.4 Sabotage

Gali (1992) menar att det finns många sätt att skapa oreda och förstöra i ett datasystem. Allt från EMP (elekromagnetisk puls), till logiska bomber, inplantering av virus och fysisk skadegörelse. Detta är vad som vanligtvis räknas in i begreppet sabotage.

Samma författare menar att motiven till att ställa till skadegörelse är många. Det kan vara allt från ekonomiska orsaker till missnöje bland anställda. Orsaker till varför sabotage förekommer har det forskats kring. Formeln MICE kan ses som ett verktyg att analysera vilka personer i en organisation som kommer att utföra sabotage.

M	Money	I	Ideology
C	Compromise	E	Ego

Nyckelorden ger en fingervisning till skälen för en individ att svika en lojalitet. Skälen är pengar, ideologi, kompromitterande uppgifter samt av egoistiska orsaker, anser Gali (1992).

2.5.5 ”Hacking”

Personer som i hemlighet och med hjälp av datorer försöker ta sig in i datorsystem de inte har behörighet till kallas ”hackers”. Enligt Grate (1994) använder sig hackers nästan alltid av telenätet över stora avstånd.

Hackers använder ofta smarta program som hjälper till att knäcka behörighetskontrollen. Det är troligt att de allra flesta hackers skulle misslyckas om lösenordssystemet var säkrare. Lösenord går ofta att lista ut p.g.a. att de byts för sällan och är för enkla, (Grate (1994)).

Elgemyr och Mattson (1992) framhåller att hackare ofta är unga dataentusiaster som av nyfikenhet och intresse försöker ta sig in i datasystem, läsa filer och eventuellt lämna meddelanden.

2.5.6 Virus

Med virus menas enligt Gali (1992) ett program som kopierar sig själv utan användarens godkännande. Virus överförs mellan datorsystem på olika sätt, ofta genom att gömma sig i andra program.

Grate (1994) menar att det i första hand är persondatorer som drabbas av virus. Ett datavirus som tillverkats för persondatorer kan inte överföras till andra plattformar. Ett virus kan spridas via diskett eller nätverk. För att undvika virus ska man bara använda program från erkända leverantörer eller program som man vet är fria från virus. Piratkopiering är en vanlig källa till spridning av virus. Det finns speciella virusprogram som har till uppgift att hitta och bekämpa virus.

2.6 Problem för olika intressenter

2.6.1 Privata företag

Företag har enligt Freese och Holmberg (1993) fått ett stort beroende av IT. Detta beroende gör många företag sårbara, eftersom mycket få verksamheter skulle klara att bedriva sin dagliga verksamhet helt utan datorer och annan kommunikationsutrustning. Informationsmängderna växer och fler och fler människor får tillgång till alltmer data. Detta gör det allt svårare att rätt klassificera vem som ska få ha tillgång till vilken data. Man måste dela upp information i olika säkerhetsklasser och bara ge dem som har behörighet tillgång till respektive klass.

Freese och Holmberg (1993) anser att dagens informationssituation inte kännetecknas av brist på information, utan av överskott på information. Därför tror jag att det finns behov av verktyg och metoder för skilja ut relevanta information från mindre relevant.

2.6.2 Offentliga sektorn

Regeringens IT proposition 1995/96:125 säger bl.a. att:

> ”… Den offentliga förvaltningen skall utnyttja IT för att effektivisera verksamheterna och ge en god service till företag och medborgare. Mer rationella arbetsrutiner, effektivare organisations- och samarbetsformer i den offentliga förvaltningen skall förbättra servicen och samtidigt minska kostnaderna…”

Propositionen beskriver enligt Toppledarforum och Statistiska centralbyrån (1996) hur offentlig sektor ska använda IT för att göra kontakter med myndigheter effektivare och lättare, samt att information ska bli enklare att ta del av.

Den stora information och säkerhetsaspekten så som jag ser det är att avgränsa vilken information som ska vara offentlig i olika typer av datornät och vilken som ska vara säkerhetsklassad. Känsliga personuppgifter, t.ex. inom vården och socialtjänst är relativt lätt att klassificera, medan uppgifter i myndighetsprotokoll, t.ex. från kommunfullmäktige sammanträden kan vara svårare att klassificera. Datalagen begränsar enligt Toppledarforum och Statistiska centralbyrån (1996) möjligheten att lägga ut offentliga dokument, då information med personuppgifter ej får publiceras på offentliga datornät utan tillstånd,

Jag anser att det finns en konflikt mellan regeringens ambitioner för ökad demokratisering med hjälp av IT och en lagstiftning som förhindrar att detta kan ske i praktiken.

2.6.3 Föreningar

Med föreningar avses organisationer och liknande som inte är företag och inte heller offentliga myndigheter. Exempel på föreningar kan vara religiösa föreningar som svenska kyrkan, politiska partier, intressegrupper som veganer, bostadsrättsföreningar och idrottsföreningar. Mitt antagande är att de flesta föreningar inte har så stora behov av skyddsåtgärder. Denna tes bygger jag på att de flesta inte är så stora att de behöver skräddarsydda lösningar för datorsäkerhet, utan kan hyra in sig på ett webbhotell för kommunikationer med omvärlden.

Detta gäller naturligtvis inte riktigt stora organisationer som t.ex. FN (Förenta Nationerna) och Röda korset. För dessa bedrivs säkerhetsarbetet troligtvis i en form som liknar företagens.

Jag kommer inte ha med några organisationer i min undersökning eftersom deras problemområde vad gäller säkerhet är mer begränsad än offentliga myndigheters och privata företags.

3 Metoder för att analysera säkerhet

3.1 Allmänt om metoder

Allt arbete med informationssäkerhet utgår enligt Ledell (1993) från att man vill begränsa riskerna för att informationen påverkas på ett icke önskvärt sätt och att det därför uppstår negativa konsekvenser. Metoder för att analysera säkerhet handlar om att identifiera de risker som kan uppstå.

De olika metoderna skiljer sig mycket från varandra, bl.a. har de olika utgångspunkter, omfattning och komplexitet. Därför är de lämpliga i olika situationer. De metoder som jag redovisar här nedan är de som jag efter mina litteraturstudier anser som de bästa och mest omfattande.

3.2 Informationsklassificering

Informationsklassificering innebär enligt Ledell (1993)

> ".. att man värderar informationen med utgångspunkt från de negativa konsekvenser som inträffar om något händer."

Vid denna metod tas ingen hänsyn till hur sannolik händelsen är eller vilka skyddsåtgärder som vidtagits för att förhindra eller begränsa verkningarna av händelsen. Bedömningen görs med utgångspunkt från alla tänkbara händelser som kan ge upphov till den aktuella konsekvensen."

Några av skälen till att använda informationsklassificering är enligt samma författare:

- medvetandegöra verksamheten om informationens värde för verksamheten.
- önskemål om en enhetlig bedömning i hela verksamheten
- lika skydd för datoriserad information som för pappersbaserad
- minimera skyddskostnaden genom en enhetlig och systematisk analys

Modellen för informationsklassificering som Ledell (1993) beskriver består av två delar, en analysdel och ett förslag till kravspecifikation.

Analysdelen har som funktion att klassificera systemet med hänsyn till fem hotområden enligt Ledell (1993):

- felaktig spridning av informationen
- felaktig förändring av informationen
- förlust av informationen
- dålig tillgänglighet till informationen
- bristfällig riktighet (kvalitet) hos informationen

Efter detta kommer man till kravspecifikationen. Första steget är att vart och ett av systemets hotområden delas in i fyra skyddsnivåer där ett är den lägsta klassen, dvs information som inte behöver något planerat skydd och fyra är den mest skyddade klassen, dvs företagshemlig.

Därefter sker ytterligare indelning efter påverkan av verksamhetsområde, där bl.a. arbetsplatsen, datorkommunikationen och den generella datormiljön räknas in. Därefter

sker ytterligare ett steg där man preciserar åtgärderna på 8 områden, bl.a. indata, utdata. åtkomst och bearbetning. Därefter kan man precisera var skydden ska installeras.

Jag anser att Ledells metod för informationsklassificering är onödigt komplicerad och invecklad. Det medger också författaren själv till viss del i bokens inledning. Jag tror dock, till skillnad från Ledell inte att metoden är effektiv och rationell, eftersom dess användbarhet begränsas av hur svår den är att överblicka. Men det ska också poängteras att denna metod av informationsklassificering inte är den enda som kan användas och att det därför går att använda andra metoder eller skräddarsy sin egen.

3.3 Riskanalys

Om informationsklassificering har utgångspunkt från negativa konsekvenser av alla tänkbara händelser så har riskanalys utgångspunkt från en given händelse, enligt Ledell (1993).

Freese och Holmbeg (1993) anser att målet med en riskanalys är att förse verksamheten med information om:

- vilka hot man är utsatt för
- hur ofta de inträffar
- omfattningen av den aktuella skadekostnaden

Samma författare definierar riskanalys som en systematisk analys av hotet mot ett objekt (t.ex. en verksamhet, ett datasystem, en dator osv) och den risk dessa hot representerar.

Freese och Holmberg (1993) menar också att följande uppgifter kan ingå i en riskanalys:

- Identifiera väsentlig interna och externa hot som verksamheten kan bli utsatt för som ett resultat av
  - avbrott i eller skada på fysiska enheter
  - konsekvenser i form av förlorade intäkter
  - ansvar inför kunder eller samarbetspartners till följd av förstörd eller skadad produktionsutrustning
  - skada, sjukdom etc hos egna medarbetare
- Värdera sannolikheten och skadekostnaderna för sådana händelser
- Värdera kostnaderna och fördelarna med att reducera eller eliminera risken
- Undersöka existerande reserv- och katastrofplaner och värdera i vilken omfattning dessa täcker de händelser företaget kan bli utsatt för
- Utarbeta ett program eller handlingsplan som siktar till att skydda företagets värden till en rimlig ekonomisk insats

En riskanalys har fyra steg:

1. Kartlägga status
2. Värdera riskerna

3. Utarbeta förslag till åtgärder
4. Upprätta handlings- och införandeplan

Om man studerar litteratur om riskanalys kan man se att den kan utföras på mer än ett sätt. SIG Security (1997) beskriver att riskanalysen kan utföras med metoder som bygger på checklistor, datoriserade analyser, scenarioanalyser, trädanalyser samt processanalyser. Riskanalysen är alltså ett flexibelt verktyg som jag anser på ett enkelt och lättöverskådligt sätt åskådliggör riskerna som ett företag är utsatt för.

3.4 Övriga metoder

3.4.1 Allmänt om övriga metoder

Riskanalys och informationsklassificering är de metoder som anses vara mest användbara enligt genomgången litteratur. Men det finns också ett antal andra metoder som kortfattat beskrivas här nedan. Metoderna likar i några fall varandra så mycket att det om vissa kan antas att de är samma metod, men med olika namn.

3.4.2 Sårbarhetsanalys

Enligt Edlund m.fl. (1989) används sårbarhetsanalys för att förebygga avbrott och andra oförutsedda händelser som stör informationsbehandlingen. Det finns en rad olika metoder för att genomföra sårbarhetsanalys, av vilka många innefattar mycket detaljerade beräkningar för att kvantifiera den totala säkerheten

De fem stegen som analysen innehåller är enligt Edlund m.fl. (1989):

1. Kartlägga status
2. Värdera riskerna
3. Utarbeta förslag till åtgärder
4. Upprätta handlings- och införandeplan
5. Följa upp införda åtgärder och utvärdera resultatet

3.4.3 Katastrofplan

Syftet med en katastrofplan är enligt Freese och Holmberg (1993):

> ".. att hålla företaget igång, även i en katastrofsituation."

Katastrofplanering handlar om att planera för att undvika oförutsedda driftavbrott, men också om att förkorta avbrottstiderna och minska skadeverkningarna när avbrott väl inträffar. Arbetet med katastrofplanering bör ledas av företagsledningen. Under detta arbete får företaget goda möjligheter att dämpa och minimera problem som kan stoppa informationsflödet. Alla kritiska funktioner ska identifieras och dokumenteras, samtidigt som ansvariga för de olika funktionerna kartläggs, (Freese och Holmberg (1993))

3.4.4 Krisplan

Utgångspunkten i en krisplan är enligt Elgemyr och Mattson (1992) att en katastrof plötsligt inträffar, utan förvarning och har ett snabbt förlopp. För att inte katastrofen ska få långtgående skadeverkningar för företaget måste den snabbt begränsas.

Krisplanering handlar om att bygga upp en god bas utifrån vilken åtgärder snabbt kan vidtas. Enligt Elgemyr och Mattson (1992) måste följande punkter förberedas i förväg:

- Utse ett kristeam
- Studera hotbild och skydd
- Arbeta fram en krisplan
- Genomföra krisövningar

Kristeamet lägger upp riktlinjer för det fortsatta arbetet och sammansätter en krisledning. Detta team bör ha högsta ledningens stöd och förtroende.

3.4.5 Säkerhetsdeklaration och Konsekvenskalkyl

Säkerhetsdeklaration och Konsekvenskalkyl är två förenklade metoder baserade på riskanalys. De gör en analys av företagets databeroende baserat på kostnader för olika skadeeffekter. Stegen i analysen är enligt Dataföreningen i Sverige (1997) beräkning av skadeeffekt för:

1. Förlust av information
2. Spridning av information till obehöriga
3. Obehörig förändring av information

Dessa steg leder till en slutsats om företagets databeroende. Nackdelen med metoden är att den inte tar hänsyn till vilka hot systemet utsätts för i verkligheten och hur ofta hoten blir verkliga.

4 Problembeskrivning

4.1 Allmänt om problemområdet

Enligt Olofson (1997) är det omöjligt att ha en hög säkerhetsnivå överallt i en verksamhet och prioriteringar måste därför göras. Prioriteringarna kan ske med hjälp av olika metoder och analyser. Vilken metod eller analys som ska användas beror på vilken slags verksamhet det handlar om och vad skyddet ska vara mot.

Metoder och analyser är grunden för säkerhetsarbetet. För att effektivt kunna skydda sig måste det finnas ett underlag för beslut angående säkerhet. Det är detta arbetet som är problemområdets kärnpunkt.

4.2 Frågeställning

Frågeställning är:

- Hur analyseras datasäkerheten i vissa verksamheter och vilka faktorer är de viktigaste?
- I vilka sammanhang är de olika säkerhetsmetoderna lämpliga och använder de undersökta verksamheterna dem på ett lämpligt sätt, ur säkerhetssynpunkt?

4.3 Avgränsning

Eftersom problemområdet fokuserar på metoder för att analysera säkerhet har följande avgränsningar gjorts:

Tonvikten kommer att vara vilka metoder verksamheter av vissa slag använder sig av och hur det påverkar deras säkerhetsarbete.

Tänkbara lösningar för att klassificera information kommer att beskrivas på ett allmänt sätt. Tekniska resonemang är mindre relevanta (exempelvis hur man på bästa sätt konfigurerar en brandvägg), istället är det processen som leder fram till lösningar som är det väsentliga.

Verksamheter som kommer att undersökas är två konsulter inom databranschen (hur de bedriver arbetet för sina klienter), två tillverkande företag samt två kommuner. Orsaken till denna indelning är att se skillnader och likheter mellan de olika verksamheternas säkerhetsarbete, men också att se hur driftmiljön och typen av verksamhet påverkar metodvalet.

4.4 Förväntat resultat

Det förväntade resultatet är att hitta vilka metoder för analys av säkerhet som kan appliceras på problemområdet. Dessa metoder kommer att undersökas och förhoppningsvis kan det leda till en slutsats om när de bör användas och deras lämplighet.

Metoder som används i vissa verksamheter kommer att undersökas men också om de används på ett riktigt sätt.

Ett delområde av undersökningen är att hitta skillnader mellan konsulters, företags och kommuners sätt att lösa dessa problem, att det finns skillnader byggs på antagandet att konsulter ofta har personer som bara arbetar med säkerhetsfrågor och följaktligen

borde vara mycket insatta i dessa frågor. Mindre företag och kommuner däremot har ofta inte denna kompetens inom verksamheten. Därför ingår det också i frågeställningen att ta reda på vem som har ansvaret, det kan t.ex. vara intressant att se om mindre verksamheter lägger ut arbetet på utomstående experter och i så fall hur arbetet och säkerhetsansvaret påverkas av detta.

Skillnader förväntas finnas på hur säkerhet hanteras i vissa datormiljöer och vid olika typer av extern kommunikation, t.ex. vid en Internetuppkoppling.

Ett antagande är att svenska företag inte alltid tar säkerhetsarbetet på tillräckligt stort allvar eftersom de litar på sin omgivnings goda avsikter och har svårt att tro att inbrott drabbar dem.

5 Behov av information

5.1 Allmänt om informationsbehovet

För att få svar på de frågeställningar som ställts i problembeskrivningen behövs information. Detta kapitel beskriver den information som behövs. Informationen delar jag in i bakrundsinformation och information som undersökningen ska ge. Problembeskrivningen innehåller fem frågor som skall besvaras. Dessa är:

1. Hur analyseras datasäkerheten i vissa verksamheter?
2. Vilka faktorer är de viktigaste i arbetet med datasäkerhet?
3. I vilka sammanhang är de olika metoderna lämpliga?
4. Använder de undersökta verksamheterna metoderna på ett lämpligt sätt?
5. Vem har ansvaret för säkerhetsarbete?

Det är att hitta svaren på dessa frågor som är målet med detta arbete. Information som behövs för att besvara dessa frågor kommer främst från undersökningen men också från litteraturstudien.

5.2 Bakgrundsinformation

Bakgrundsinformationen innefattar dels information som ger en inblick i ämnet datasäkerhet och dels information om de olika metoder som senare ska vara en del av undersökningen.

Information som ger inblick i ämnet är viktigt eftersom detta ligger till grund för kapitlets inledning samt min förståelse för ämnet datasäkerhet. Kravet som jag ställer på denna information är att den är aktuell och relevant. Det är också viktigt att information kan verifieras från flera källor för att kunna kontrollera informationen.

Information om de olika metoderna som kan användas för att analysera säkerhet är väsentlig för undersökningen. Detta för att det är dessa metoder som ska ligga till grund för jämförelsen med metoderna som de undersökta verksamheterna använder sig av. Denna information ska vara relevant, ge en god bild av den beskrivna metoden samt beskriva när metoden är lämplig.

Det är främst i fråga tre och fyra som bakgrundsinformationen behövs för att besvara frågorna. Bakgrundsinformationen är dock inte den primära informationen som behövs för att besvara dessa frågor, utan fungerar mer som en kunskapsbas att relatera undersökningen emot.

5.3 Information från undersökning

Frågeställningen handlar om hur säkerhetsarbetet utförs i vissa verksamheter. Eftersom jag inte har hittat någon större mängd information i min litteratur som berör detta krävs det att jag utför en egen undersökning. Denna undersökning ska syfta till att finna den information som frågeställningen kräver. Informationen som behövs är bl.a. vilka metoder olika verksamheter använder, hur de använder metoderna samt faktorer som påverkar deras säkerhetsarbete och val av metod. Det är alla frågor (ett till fem) som behöver information från undersökningen för att kunna besvaras. Undersökningen är

det primära i detta arbete eftersom huvuddelen av all information som behövs kommer från denna fas.

Kraven jag ställer på information från undersökningen är att den ger god inblick om de olika verksamheternas arbete med metoder, är saklig samt att den går att jämföra med andra verksamheters arbete.

6 Möjliga metoder och val av metod

6.1 Allmänt om metoder

Detta kapitel beskriver kortfattat de olika metoder som kan användas för att ta fram information samt vilka metoder som valts. Information kan insamlas på flera olika sätt. För att uppnå önskat resultat räcker det inte alltid att använda bara en metod, utan ibland måste en kombination av flera användas.

De metoder som finns har olika egenskaper som gör dem mer eller mindre lämpade att besvara en viss frågeställning. Det viktigaste är att hitta en kombination som på bästa sätt löser den aktuella frågeställningen. Fördelar och nackdelar med respektive metod samt när de är lämpliga att använda kommer att diskuteras. Detta arbete kommer förhoppningsvis att leda fram till en slutsats om vilka metoder som är mest lämpade att applicera på problemområdet.

Som tidigare har nämnts räcker det inte alltid med bara använda en metod. Metoderna måste inte heller alltid följas till punkt och pricka. Kriterierna för de metoder som kan användas är att de ska fungera som stöd för undersökningen samt att problemområdet kan angripas med hjälp av dem. I bilaga ett finns längre allmänna beskrivningar av de olika metoderna. Där beskrivs också indelningen metoderna i klasserna fältundersökning och skrivbordsundersökning. Där finns också en beskrivning av de olika urvalsmetoderna samt en förklaring av skillnaderna mellan kvalitativ- och kvantitativ undersökning. Här nedan beskrivs hur de olika metoderna kan användas för min undersökning samt motiveringar varför vissa valts och andra valts bort.

6.2 Fältundersökning

6.2.1 Metoder som valts bort

6.2.1.1 Brevformulär

Undersökning med brevformulär går till så att ett formulär skickas till respondanten med brev. Respondanten får sedan returnera formuläret. Att Brevformulär inte har använts beror på naturen av undersökningen. Denna typ av undersökning kunde ha används för att skicka ut stora mängder enkäter och få mycket information att analysera. Detta skulle kunna med fördel ha stött kvantitativ undersökning där jag matematiskt skulle kunnat stödja mina påståenden. Nackdelen med detta som jag ser det är att denna typ av formulär inte ger någon större djup i frågorna, bl.a. eftersom det inte går att ha en dialog med respondanten om frågor anses oklara och det därför är svårt att ha några längre frågor med. En annan nackdel är att det inte säkert går att veta vem i organisationen som verkligen svarat på frågorna samt att det kan vara svårt att få hög svarsfrekvens eftersom denna typ av undersökning är lätt för respondanten att ignorera.

6.2.1.2 Observationsundersökning

Observationsundersökning går till så att man övervakar en eller flera personer och dokumenterar vad de gör. För att utföra en observationsundersökning hade det krävts stora mängder tid. En undersökning av detta slag kunde ha gått till så att man följt en organisations arbete med metoder för säkerhet. Detta hade gett en god insikt om hur de använde sin metod, men hade inte get någon allmän insikt om vilka metoder som

kan användas och när de är lämpliga att använda. Jag har velat ha en något större spektrum i min undersökning och att bara undersöka en organisation hade inte gett någon material att undersöka olika organisationer som efterlyses i problembeskrivningen.

6.2.1.3 Telefonintervju

En telefonintervju utförs så att respondanten blir intervjuad över telefon. När undersökningen påbörjades tänkte jag på något sätt använda telefonintervju. Men innan jag påbörjade genomförandefasen valde jag bort denna typ av intervju. Detta främst eftersom min undersökning är av en kvalitativ natur och jag ansåg inte att telefonintervju hade gett den djup på intervjuerna som jag eftersträvade, bl.a. p.g.a. att visuella hjälpmedel inte kan användas. Fördelen med telefonintervju är att jag antagligen skulle ha hunnit med fler intervjuer och därför haft mer material att bearbeta. Jag ansåg dock att nackdelarna var större än fördelarna.

6.2.2 Metod som valts

6.2.2.1 Besöksintervju

Besöksintervju går till så att respondanten intervjuas på sin arbetsplats. För att uppnå önskat resultat tror jag att besöksintervju är lämpligast att använda. Orsaken till detta är att denna metod ger möjlighet att genomföra en djupintervju med personer som arbetar med säkerhet inom valda organisationer och jag tror att detta leder till material med hög kvalitet. Detta arbetssätt kommer att leda till ett material som är främst kvalitativt.

Ett ostrukturerat frågeformulär kommer att användas eftersom det är svårt att konstruera ett frågeformulär som är utformat för att ta hänsyn till alla tänkbara eventualiteter. En ostrukturerad intervju har den fördelen att följdfrågor kan ställas och diskussioner kring problem genomföras.

Den största nackdelen med detta intervjuförfarande är att det tar mycket tid. Det innebär att jag inte kommer att hinna utföra en omfattande undersökning. Att undersökningen inte blir så omfattande tror jag uppvägs av att kvaliteten på denna typ av undersökning blir relativt hög.

6.3 Skrivbordsundersökning

6.3.1 Metoder som valts bort

6.3.1.1 Intern företagsinformation

Intern företagsinformation är information som företag lagrar för internt bruk, t.ex. kundstatistik och tidigare utförda undersökningar. Det är alltid svårt för personer utanför en organisation att få ta del av intern företagsinformation. Det är antagligen ännu svårare att få använda denna information för ett akademiskt arbete som av sin natur är offentligt. Därför har denna metod inte använts för denna undersökning. Hade jag fått ta del av sådan information, t.ex. interna säkerhetsrapporter och resultat av genomförda metoder hade jag haft mycket bra information att jobba med och hade antagligen kunnat presentera ett mycket gott resultat.

6.3.1.2 Officiell statistik

Officiell statistik är information som är insamlad av myndigheter och andra organisationer. Jag använder mig indirekt av officiell statistik i min undersökning. Jag har inte gått till källorna (t.ex. SCB), men jag har presenterat viss statistik som har funnits i den litteratur som jag har använt mig av. Denna information har visat förhållanden, t.ex. vad en ”hacker” åstadkommer vid ett intrång. Information av detta slag är inte oumbärlig för min undersökning och har bara använts till att ge en bakgrund till ämnet.

6.3.2 Metoder som valts

6.3.2.1 Litteraturstudier och Internet

Litteraturstudier är grunden till detta arbete. Det är genom dessa de generella metoderna för att analysera säkerhet står att finna. Därför har litteraturstudier använts som underlag för undersökningen men också för att ge en god kunskap om ämnet datasäkerhet.

På Internet finns en stor mängd information som berör datasäkerhet. Eftersom Internet har vissa nackdelar bl.a. att det är svårt att kontrollera kvalitet på informationen så används denna källa inte i någon större omfattning. Det som har använts är generell information om säkerhet från kända organisationer och myndigheter.

Litteratur- och Internetstudier är också användbara för, att i ett senare skede av undersökningen kunna ha en kunskapsbank att relatera till och för att kunna analysera de framkomna resultaten mot denna.

Nackdelen med båda dessa medier är att det kan vara svårt att veta vilken information som är av forskningsvärlden accepterad fakta och vilken som är författarens egna subjektiva åsikter. Jag har försökt att minska denna risk genom att försöka ha flera källor som verifierar påståenden.

6.4 Urvalsmetoder

6.4.1 Metoder som valts bort

Att få fram en lista över organisationer som jobbar med säkerhet skulle gå att ordna. Man kan på gulasidornas hemsida på Internet (http://www.gulasidorna.se) få fram en lista över t.ex. datakonsulter som finns i Sverige. Antas att denna lista är komplett skulle någon av metoderna som använder stickprovsmetod (t.ex. obundet slumpmässigt urval eller stratifierat urval) kunna användas för att få fram ett urval. De företag som kommit med i detta skulle sedan undersökas med någon av de tidigare beskrivna metoderna.

Problemet som jag ser med detta är att begränsa bortfallet. Med bortfall menar jag de företag som väljer att inte medverka i undersökningen. Vid ett för stort bortfall skulle den statistiska säkerhet som denna typ av undersökning ger gå förlorad och därmed skulle fördelarna med statistiskt urval dramatiskt minskas. Vidare skulle undersökningen kräva ett större urval än jag har möjlighet att undersöka p.g.a. de tidsramar som finns för arbetet.

6.4.2 Metod som valts

Metoden tillgänglig grupp innebär att undersökningen kan hållas på en lagom nivå och inte påverkas av bortfall på samma sätt som vid stickprovsundersökningar. Detta eftersom undersökningen ändå inte kommer att ha någon statistisk säkerhet.

Den tillgängliga gruppen är främst företag, konsulter och kommuner som uppfyller två kriterier. Det första kriteriet är att organisationen går med på att låta sig intervjuas om sin datasäkerhet. Det kommer antagligen att bli ett visst bortfall p.g.a. att vissa organisationer inte vill diskutera dessa kritiska frågor med personer utanför organisationen. Det andra kriteriet är att organisationen har ett datanätverk och någon som är ansvarig för detta. Det är främst personer med ansvar för datorverksamheten som jag kommer att intervjua.

7. Genomförande

7.1 Allmänt om genomförandet

I detta kapitel kommer att beskrivs hur jag genomfört min undersökning, vilket är en fortsättning på alla de tidigare faserna i arbetet. Denna del av arbetet är också den som gett störst utrymme för egen bearbetning då den ska besvara de problemområden som skissats inledningsvis. I avsnittet behandlas mitt tillvägagångssätt vid skapandet av frågeformulär mm och till sist genomförande av intervjuer.

7.2 Skapandet av frågeformuläret

Utgångspunkten vid konstruktionen av frågeformuläret var att få fram den information som krävs för att svara på frågeställningen i problembeskrivningen. Eftersom jag anser det svårt att få fram all information utan att använda följdfrågor användes ett frågeformulär med låg grad av standardisering. Detta innebär att jag inte slaviskt måste följa frågeformuläret, utan kan vid behov byta ordning på frågorna, be respondanten om förtydligande samt ställa följdfrågor. Detta passar bra eftersom mitt ämne är relativt komplext och det annars kan vara svårt att få tillfredsställande svar.

Jag insåg på ett tidigt stadium att det inte går att ställa samma frågor till de olika organisationerna. Därför är frågeformulären något modifierade efter huruvida respondanterna är företag, kommuner eller konsulter. Det är främst svaret på de första frågorna i formuläret som kommer att ge en allmän bild av organisationen, vilken skiljer sig beroende på organisationens typ.

Frågeformuläret omarbetades ett flertal gånger innan jag var nöjd med resultatet. Ett antal försökspersoner (främst studenter vid datainstitutionen vid högskolan i Skövde samt min handledare) har fått läsa igenom frågeformulären. Jag gjorde antagandet att om de förstod frågorna skulle också de tilltänkta respondenterna göra det. Deras tolkningar av frågorna har sedan legat som grund till omarbetningar, både av vilka frågor som skulle vara med samt hur frågorna skulle vara formulerade.

Frågeformulären (bilaga 1, 4 och 7) är indelade i tre delar. Den första delen behandlar organisationens storlek, arbetsuppgifter och datamiljö. Den ger material till att relatera informationen om datasäkerhet mot.

Den andra delen, huvuddelen av frågeformuläret går mer specifikt in på frågor om vilka metoder organisationer använder sig av i sitt säkerhetsarbete. Denna del kommer att ge den mest väsentliga informationen, eftersom det är den som främst besvarar frågeställningen.

Den tredje delen innehåller mera preciserade frågor om hur organisationer bedriver sitt säkerhetsarbete. Den del är en uppföljning och precisering av frågorna i del två. Dessa frågor finns med för att på ett detaljerat sätt få information om organisationernas säkerhetsarbete.

På det hela taget anser jag att formuläret i sin helhet tjänar sitt syfte med att besvara frågeställningen, framför allt med tanke på att den ska tjäna som en mall för en intervju med låg grad av standardisering och därmed ge möjlighet till korrigeringar,.

7.3 Förberedelser inför Intervjuer

Mina första förberedelser var att hitta företag att intervjua. Jag använde mig av gula sidorna på Internet (http://www.gulasidorna.se) för att hitta företag som verkade intressanta. Därefter gick jag till deras hemsidor på Internet för att se om företaget kunde passa för min undersökning. Därefter gjorde jag mitt val över vilka företag som skulle ingå i undersökningen.

Jag kontaktade sedan de aktuella företag via telefon. Det var främst personer insatta i frågor om datasäkerhet och med en hög position i företaget jag sökte. Orsaken till det sistnämnda beror på att jag ville utföra mina intervjuer med personer som har en helhetssyn över organisationen och inte bara över säkerhetsarbetet. De flesta som intervjuades var därför IT-chefer eller chefer på motsvarande nivå, insatta i datorsystemet.

I mitt inledande telefonsamtal med personerna jag ämnade intervjua beskrev jag kortfattat syftet med min intervju samt vilka frågor jag skulle komma att beröra. Det var väldigt få personer som tackade nej till att medverka i min undersökning. Inför mitt besök på organisationerna informerade jag mig om deras verksamhet för att vara väl förberedd.

Jag erbjöd alla organisationer att vara anonyma i undersökningen, eftersom viss känslig information skulle kunna beröras. De flesta ville vara anonyma och därför kommer undersökningen inte att innehålla några företagsnamn i klartext. Detta är en avvägning som sannolikt inte kommer att påverka resultatet av undersökningen.

7.4 Genomförande av intervjuer

Alla intervjuer gick till så att jag träffade tilltalade personerna på deras arbetsplatser. Jag använde mig av en bandspelare vid intervjuerna för att i efterhand kunna gå tillbaka till det som sagts och få en god bild av den information som givits.

I den första intervjun var respondanten datoransvarig för en kommun. Jag känner denna person sedan tidigare och såg därför ett tillfälle att på honom testa mitt frågeformulär. Denna intervju tjänade således som en test av hur väl frågorna i formuläret fungerade. Efter denna intervju gjordes ett par mindre korrigeringar i frågeformuläret.

7.5 Litteraturstudier

Den framtagna litteraturen användes till viss del i genomförandet. I frågeformuläret finns med frågor om de olika metoderna för datasäkerhet som står beskrivna i litteraturen. Jag använde också dessa metoder som referens när jag i mina intervjuer diskuterade hur de tillfrågade organisationerna använde sina metoder för analys av säkerhet.

Jag har i denna fas av undersökningen inte tagit fram någon ny information, utan den information som finns beskriven i kapitel 3 har använts.

7.6 Erfarenheter från genomförandet

Genomförandets uppläggning har varit en process som hela tiden har utvecklats. De första utkasten av frågeformuläret var till viss del oklara. För att i senare versioner bli mer konkreta och ge ett bättre underlag för att få fram den information som efterfrågas

i problembeskrivningen. Samma sak gäller för intervjuerna, då de första intervjuerna var trevande och något ogenomtänkta. Efterhand som jag blev mer insatt i ämnet blev intervjuerna emellertid bättre och det var mycket enklare att få fram den information som var relevant.

En annan erfarenhet som jag gjorde var att frågeformuläret inte fungerade så bra som det borde på alla organisationer. Det var främst vid intervjun med konsult två (det rikstäckande företaget) som frågorna var för specifika. Deras verksamhet var så omfattande och komplex att mina frågor som är ganska specifika inte gav önskat resultat. Därför var jag tvungen att omformulera vissa frågor och byta ordning på dem. Med denna korrektion gav dock intervjun önskat resultat. Därför tror jag att det var ett riktigt val att använda ostrukturerade intervjuer eftersom dessa är mer flexibla och därför går att anpassa till uppkomna situationer.

Jag anser att jag i denna fas, som beskrivs i bilagorna 1 till 9, har tagit fram det mesta av den information som behövs för undersökningen. Om jag skulle göra om genomförandefasen idag skulle jag i stort sätt göra allting likadant.

8. Analys

8.1 Allmänt om analysen

Analysen kommer att göras med utgångspunkt av problemställningen. Det är främst de fem frågorna som problembeskrivningen innehåller som kommer att behandlas. Dessa frågor är:

1. Hur analyseras datasäkerheten i vissa verksamheter
2. Vilka faktorer är det viktigaste i arbetet med datasäkerhet
3. I vilka sammanhang är de olika metoderna lämpliga
4. Använder de undersökta verksamheterna metoderna på ett lämpligt sätt
5. Vem har ansvaret för säkerhetsarbetet

För varje organisation görs en genomgång av samtliga frågor utom nr tre. Denna analyseras istället mot metoderna i litteraturen under kapitel 8.3. Följande analys bygger på intervjuerna med organisationer som presenteras i bilaga två till tio.

8.2 Analys av undersökta organisationer

8.2.1 Företag ett

Företag ett använder sig av katastrofplan för att analysera sin säkerhet. Denna metod använder de främst för att gardera sig mot oförutsedda driftavbrott. Ingen systematisk analys har gjorts för att gardera sig mot några andra säkerhetsrisker som t.ex. intrång utifrån eller sabotage. Jag anser att den krisplan de använder sig av är i stort sett identisk med den som beskrivits i kapitel 3.4.4. Grunden för denna analys är alltså att begränsa skadeverkningarna vid en oförutsedd katastrof. Detta är naturligtvis något som är mycket väsentligt för ett tillverkande företag vars existens i mångt och mycket beror på att produktionen fungerar. Min reflektion är dock om företaget borde analysera sin säkerhet utifrån andra perspektiv också, t.ex. se över skyddet mot inre- och yttreangrepp. Detta kan göras med en metod som är mer komplett och kan användas för att täcka in dessa händelser också, t.ex. riskanalys. Att inte mer gjorts av säkerhetsarbetet kan delvis förklaras med att företaget inte har några fasta uppkopplingar och att inga inre angrepp tidigare har förekommit. Detta är dock ingen orsak att inte systematiskt se över dessa områden för att försäkra sig om att företaget har en hög säkerhetsnivå.

Huruvida verksamheten använder metoden katastrofplan på ett lämpligt sätt är svårt att avgöra. Eftersom det var hela tre år sedan den större genomgången av datasäkerheten gjordes kan man hävda att säkerhetsarbetet borde utföras mer frekvent, då mycket har hänt på dataområdet sedan dess. Själva tillvägagångssättet vid utförandet fick jag inte någon större insyn i, eftersom det var länge sedan den utfördes och p.g.a. att det var en konsult som ledde arbetet. Baserat på den information som finns anser jag dock att katastrofplanen utfördes som kapitel 3.4.4 beskriver.

Företaget anser att planering mot driftstopp och skydd mot virus är särskilt viktiga i säkerhetsarbetet. Faktorer som påverkar säkerhetsarbetet är brist på tid och till viss del datorbudgeten. Att planering mot driftstopp och skydd mot virus anses som viktigt tycker jag är naturligt, eftersom båda dessa faktorer stör verksamheten och minskar

produktiviteten. Ett intryck jag har är dock att företaget kanske borde ha en mer övergripande syn på säkerhetsarbetet.

En säkerhetsansvarig har det övergripande säkerhetsansvaret, vilket även inkluderar den fysiska säkerheten. Eftersom företaget är litet är det naturligt att de inte har någon större säkerhetsorganisation.

8.2.2 Företag två

Företag två använder sig av sårbarhetsanalys för att analysera sin säkerhet. Denna metod används främst för att räkna ut hur kostsamma driftstopp skulle bli, samt se hur länge verksamheten klarar sig utan datorstöd. Denna analys används för att få en säkerhetsnivå som står i proportion till kostnaden. Verksamheten anser sig ha ett omfattande skydd för intrång utifrån, men har inte använt någon analys för att analysera hoten. Sårbarhetsanalys används för att förebygga avbrott och andra oförutsedda händelser som stör informationsbehandlingen (metoden beskrivs närmare i kapitel 3.4.2). Jag anser att säkerhetsarbete i företag två är relativt likt de i företag ett. Företag två använder sig av sårbarhetsanalys som är relativt lik den katastrofplan som företag ett använder sig av, eftersom båda har som främsta syfte att förebygga oförutsedda avbrott i verksamheten. Företag två är liksom företag ett en tillverkande industri och därför är det naturligt att deras säkerhetsarbete är har likheter. Hur arbetet med att analysera den externa säkerheten var upplagt var datorchefen relativt förtegen om. Enligt honom utförde företaget arbete med detta men hade inte använt någon metod för systematiska analyser. Detta anser jag vara något underligt med tanke på företagets storlek och de omfattande uppkopplingarna mot omvärlden. Men eftersom jag inte fick någon detaljerad insyn i företagets externa säkerhetsarbete är det svårt att dra några slutsatser om detta.

Enligt Edlund m.fl. (1989) finns det en rad olika metoder för att utföra sårbarhetsanalys. Metoden som företag två använder sig av är en relativt enkel variant med färdiga blanketter som grund. Det företaget främst ville ha fram av analysen var hur länge företaget klarar sig utan datorstöd samt hur kostsamma driftstopp skulle bli. Eftersom sårbarhetsanalys som den beskrivs av Edlund m.fl. (1989), sammanfattad i kapitel 3.4.2 har just denna inriktning så antar jag att företaget använde en variant som är relativt lik denna. Med de uppgifter de ville ha fram anser jag detta vara ett bra val.

Datorchefen anser att det mest kritiska i säkerhetsarbetet är att få tid från de dagliga rutinerna till säkerhetsarbetet. Att få en säkerhetsnivå som står i proportion till kostnaden anses viktigt. Jag anser att detta är ett sunt resonemang. Naturligtvis ska kostnaderna för säkerhetsarbetet inte skena iväg och bli orimliga, men samtidigt är det svårt att i förväg veta vilka kostnader som är väl investerade pengar. Det är just det som mer omfattande analyser skulle kunna hjälpa till att ta reda på.

Företaget har en dataavdelning som har ansvar för säkerheten. Det finns också en central IT-stab som ger riktlinjer för säkerhetsarbetet. Säkerhetsansvaret verkar vara logiskt uppdelat med en den lokala IT-enheten som har ansvar för divisionens datasystem och en IT-stab som har ett övergripande ansvar.

8.2.3 Kommun ett

Kommun ett har aldrig gjort någon analys av sin säkerhet. Det har inte heller skett något strategiskt arbete med datasäkerhet. Jag anser att kommunens säkerhetsarbete är mycket bristfälligt. Även om det är en mindre organisation med få kopplingar mot

omvärlden så borde säkerheten ses över. Det finns 120 datorer i nätverket och kopplingar mot omvärlden i form av modem för distansarbete. Detta innebär att det finns en potentiell risk för intrång utifrån. Att kommunen även varit utsatt för interna angrepp borde mana till ökad förståelse av behovet för ökade åtgärder. Jag anser att en omfattande analys för att få ett samlat begrepp om säkerhetsläget och planera för olika åtgärder borde göras. Metoder som jag anser som lämpliga är de som täcker flera aspekter av säkerhetsarbetet, t.ex. informationsklassificering och riskanalys.

Det mest kritiska i kommunen är ledningens brist på intresse för dessa frågor. Det finns också brist på tid att utföra säkerhetsarbete samt brist på pengar. Det allvarligaste hotet anses vara intrång utifrån. Jag tror det är kommunledningens brist på intresse som är den bakomliggande orsaken till det bristfälliga säkerhetsläget. Utan engagemang från ledningen är det troligtvis omöjligt att uppnå en god säkerhet.

Det finns ingen säkerhetsansvarig inom kommunen. De olika nämnderna har dock ansvaret för sina register. Jag tror att det är farligt att inte ha en klar ansvarsfördelning av säkerhetsarbetet. För att bedriva ett effektivt säkerhetsarbete behövs det någon som har det övergripande ansvaret, samt resurser och befogenheter att kunna bedriva arbetet.

8.2.4 Kommun två

Kommunen har aldrig använt någon metod eller analysmetod för att analysera sin datasäkerhet. Däremot anser IT-chefen att han använder vissa av tankarna från litteraturen om metoder för att analysera säkerheten eftersom han är insatt i de olika metoderna. Jag anser att det är bättre att bedriva säkerhetsarbetet med dessa metoder i bakhuvudet än att bedriva arbetet utan någon insikt i dem. Det hade naturligtvis varit ännu bättre om arbetet hade bedrivits med systematiska analyser. Jag tror att risken är relativt stor att man missar viktiga delar när man inte utför en systematisk analys. En av fördelarna med metoderna är att man kan få en helhetsbild av verksamheten ur ett säkerhetsperspektiv, vilket kommunen nu går miste om.

Det mest kritiska för kommunens säkerhetsarbete är skyddet utåt, eftersom de har en fast uppkoppling mot Internet. Fysisk förstörelse av datasystemet eller delar av det (t.ex. genom brand) anses vara det största hotet mot verksamheten. Bristen på kompetent IT personal påverkar också säkerhetsarbete negativt, eftersom det inte finns tid att utföra allt som borde utföras.

IT-chefen har det övergripande ansvaret för datasystemet, medan de olika förvaltningarna har egna datoransvariga med ansvar för sin del av datasystemet.

8.2.5 Konsult ett

Konsult ett använder sig inte av någon metod eller systematisk analys av datasäkerhet. Det säkerhetsarbete han har utfört är mindre analyser av vad som händer när systemet får driftstopp, liknande katastrofplan men betydligt mindre omfattande. Han anser dock att dessa analyser mycket sällan leder till några åtgärder. Konsult ett har en verksamhet som skiljer sig mot tidigare beskrivna. Han tar främst fram specifikationerna vid systemutveckling, låter ett annat företag sköta programmeringen för att själv sköta inplementeringen. Detta betyder att det är han som i grunden avgör hur säkert ett system kommer att bli. Jag tycker det är något underligt att han inte tittar på hot och risker som företagen är utsatta för, t.ex. med hjälp av en metod för att analysera säkerhet, vid specifikationen av systemet. Då skulle man redan på ett tidigt stadium

kunna fastställa vilken säkerhetsnivå systemet bör ha. Jag antar att orsaken till att detta inte utförs är att han jobbar med mindre företagen som troligen inte vill spendera för stora belopp på säkerhet samt att han har jobbat med att utveckla denna typ av system en längre tid och troligen därmed skaffat sig en god uppfattning om vilka risker som föreligger.

Konsulten menar att säkerhetsarbetet mycket handlar om att lägga upp rutiner som verksamheterna sedan själva kan sköta, t.ex. rutiner för backuper. Jag anser att denna typ av förebyggande säkerhetsarbete uteslutande bedrivs för att få en tillfredsställande driftsäkerhet och inte skyddar mot något annat.

Konsulten har efter att han är klar med arbetet i ett system inget säkerhets eller driftansvar. Verksamheterna han jobbar mot tar över driftansvaret när han är färdig med sitt arbete.

8.2.6 Konsult två

Konsulten har för både riskanalys och sårbarhetsanalys egna mallar som specificerar hur arbetet ska utföras. Dessa analysmetoder kommer ofta in på ett mycket tidigt skede i utvecklingsprocessen och handlar om att analysera verksamhetsstödet. Med detta menas att funktionerna och verksamhetsprocesserna analyseras efter olika fel som kan uppkomma och hur systemet skall klara av dessa. Eftersom konsult två är en stort företag med många olika kunder och typer av uppdrag är det svårt att komma till generella slutsatser angående deras arbete med metoder. Hur säkerhetsarbetet utförs varierar från tillfälle till tillfälle beroende på kundens önskemål och hur mycket kunden själv har möjlighet och kunskap att utföra.

Det är mycket svårt att komma till några slutsatser om konsult två använder metoderna på ett riktigt sätt. Verksamheten är mycket omfattande, kunderna av olika karaktär och uppdragen mycket skiftande. Därför nöjer jag mig med att konstatera att deras arbete med metoderna verkar gediget samt att sättet som de anpassar arbetet efter, kundens behov och önskemål, är ett bra sätt att arbeta på.

Konsulten anser det viktigt att tillsammans med sina kunder resonera sig fram till en säkerhetsnivå som står i proportion till kostnaderna för implementeringen av åtgärden.

Konsulten har inga löpande driftansvar för sina kunder. Därför har de inget ansvar för sina kunders datasystem eller säkerhetsarbete.

8.3 Analys av metoderna

8.3.1 Allmänt om metoderna

De olika metoderna har olika användningsområden. I följande avsnitt skall jag behandla de olika metodernas användningsområden samt för- och nackdelar utifrån min problemställning. Analysen kommer både att göras utifrån litteraturstudien och materialet från undersökningen. Det jag främst kommer att beskriva är när de olika metoderna är lämpliga.

8.3.2 Informationsklassificering

Det är ingen av de undersökta organisationerna som har använt sig av metoden informationsklassificering. Jag tror det kan bero på att metoden är onödigt komplicerad och svåröverblickbar, vilket jag tidigare beskrivit (i kapitel 3.2). Ledell (1993) beskriver att informationsklassificering kan användas vid analys av komplexa

informationsmiljöer. Jag tror dock att det är få verksamheter som har tid och ork att göra en såhär omfattande och avancerad analys. Brist på kvalificerad personal och svårigheter att få tid med säkerhetsarbete upplevdes som problem i så gott som samtliga av de undersökta organisationerna. Därför tror jag att det är mycket få organisationer som har nytta av denna metod. De som kan använda den tror jag främst är verksamheter med stora resurser för säkerhetsarbete, mycket tid, omfattande uppkopplingar mot omvärlden och avancerade informationssystem. Organisationer som faller inom denna ram kan bl.a. vara försvarsmakten, Internet banker, och forskningsintensiva kunskapsföretag.

8.3.3 Riskanalys

I min undersökning är det bara konsult två som använder sig av riskanalys. Freese och Holmbeg (1993) beskriver riskanalys som en systematisk analys av hotbilder och den risk dessa hot representerar. Jag anser att riskanalys är en metod som kan användas till att analysera alla typer av hotbilder ett företag kan utsättas för. Riskanalysen har också den fördelen att den är anpassbar och kan göras relativt enkel. Jag anser att riskanalys kan användas av de flesta organisationer och i det flesta situationer. Denna metod är användbar för de verksamheter som vill analysera sin säkerhet, oavsett hur omfattande analysen de vill göra. Jag tror dock att denna metod passar dåligt för de allra största organisationerna eftersom jag tror att den blir oöverskådlig vid stora informationsmängder.

8.3.4 Sårbarhetsanalys

Sårbarhetsanalys var den mest använda metoden hos de undersökta företagen, både konsult två och företag två använde den. Enligt Edlund m.fl. (1989) används sårbarhetsanalys för att förebygga avbrott och andra oförutsedda händelser som stör informatiosbehandlingen. Detta gör att metoden främst är användbar för analyser som syftar till att förebygga driftavbrott. De verksamheter som har den största ekonomiska vinsten i att använda denna metod är de som bygger sin verksamhet på produktionen av varor, dvs främst tillverkande företag. Jag tror att detta är bör vara en del i alla tillverkande företags säkerhetsarbete oavsett storlek.

8.3.5 Katastrofplan

I undersökningen var det bara företag ett som använde sig av katastrofplan. Syftet med en katastrofplan är enligt Freese och Holmberg (1993) att kunna hålla företaget igång i en katastrofsituation. Denna metod är inte en komplett säkerhetsanalys, utan har som främsta syfte att planera för att minska riskerna för driftavbrott och när de ändå uppstår minska skadeverkningarna. Denna målsättning är relativt lik den som sårbarhetsanalys har och jag tror att min analys om när den bör användas också gäller för katastrofplan.

8.3.6 Krisplan

En krisplan har enligt Elgemyr och Mattson (1992) syftet att när en katastrof väl inträffat ha en god kunskapsbas om hur skadeverkningarna kan begränsas. Denna metod är alltså smalare än de tidigare eftersom den enbart analyserar en faktor. Detta tycker jag ger den en begränsad användbarhet. Jag tror att det är bättre att använda en analys som också tar upp hur katastrofer förebyggs, som t.ex. katastrofplan och sårbarhetsanalys.

8.3.7 Övriga metoder

Säkerhetsdeklaration och Konsekvenskalkyl är metoder som bygger på riskanalys men är förenklade. Dessa metoder tror jag är lämpliga för mindre företag som inte har någon större IT-kompetens men ändå vill kunna göra en översiktlig analys av sin säkerhet. Det är främst kostnaderna för förlust av information som räknas ut.

8.4 Analys av insamlat material

När det insamlade materialet analyseras bör det värderas efter hur tillförlitligt och trovärdigt det är. Jag anser att det material som har samlats in håller en relativt bra kvalitet men att det också har några brister. Den metoden som jag använt mig av för att samla in material, ostrukturerad intervju, har den fördelen att rena missförstånd kan undvikas eftersom den syftar till att intervjun ska bli en form av diskussion, där följdfrågor kan ställas och oklarheter redas upp. Detta ger en bra grund för att samla in material med god kvalitet.

De personer jag intervjuat är genomgående chefer för dataavdelningar, vilket innebär att de har god insikt i organisationens säkerhetsarbete. I de flesta fall var dessa chefer också säkerhetsansvariga. Detta är faktorer som ger grunden för ett material med bra kvalitet. Vad som däremot är svårare att bedöma är hur tillförlitlig informationen respondanterna givit om sina verksamheters säkerhetsarbete är. Det faktum att undersökningen genomförts anonymt tror jag har bidragit till att materialets tillförlitlighet ökat, eftersom det inte kommer att presenteras vilken organisation det handlar om. Dock tror jag ändå att det inte går att undvika att en viss del av den inhämtade informationen är färgad av de intervjuade personernas åsikter och deras lojalitet mot sin organisation.

Det var främst när jag kom in på frågor om hur verksamhets skydd utåt var upplagt som jag fick undvikande svar. Eftersom detta inte tillhör mitt primära undersökningsområde så påverkar det inte arbetet i någon större utsträckning. För övrigt fick jag av respondanterna svar på de frågor jag ställde. Det är mycket svårt att bedöma till vilken grad de intervjuade personerna har påverkat materialets tillförlitlighet, men jag tror att trovärdigheten i materialet som jag samlat in är relativt god.

Materialet ger inte någon stor inblick i hur svenska företag bedriver sitt säkerhetsarbete, eftersom antalet intervjuer är starkt begränsade. Detta gör att undersökningen inte ger ett resultat som kan appliceras på hela landet. Jag inser att detta är en svaghet i arbetet, men p.g.a. tidsbegränsningar , samt det faktum att jag ville besöka alla företag själv gjorde något annat tillvägagångssätt omöjligt.

9. Slutsatser

9.1 Allmänt om slutsatser

I detta avsnitt kommer de generella slutsatser som jag kommit fram till att beskrivas. Jag behandlar ämnet på en allmän nivå och går inte in på detaljer om enskilda organisationer. Det är istället området som helhet som kommer att behandlas.

9.2 Organisationers säkerhet

Om man tittar på de undersökta företagens säkerhetsarbete så framkommer ett antal intressanta aspekter. Det generella som kan sägas om arbetet med säkerhet är att det är betydligt sämre och mindre omfattande än vad jag hade väntat. Det jag saknade i många fall var en helhetssyn på säkerhetsarbetet samt större prioriteringar i form av resurser i tid och pengar.

Säkerhetsarbetet anpassas efter organisationens prioriteringar och vad de anser viktigt att skydda eller gardera sig mot. Generellt kan sägas att tillverkande företag analyserar mot driftstopp, eftersom detta anses vara det som leder de största ekonomiska förlusterna. Kommuner anser att skyddet utåt är viktigt eftersom det finns en hel del känslig information i kommuners datanät. Konsulter baserar säkerhetsarbetet efter kundernas önskemål och vad de är beredda att betala för säkerheten. Andra faktorer som har betydelse för säkerhetsarbetet är organisationens storlek, kompetensen hos personalen samt ledningens engagemang. Naturligtvis finns det fler faktorer som spelar in, men dessa är de som främst framkommit i min undersökning.

Det är svårt att svara på om de undersökta organisationerna använder metoderna på ett lämpligt sätt. Främst beror detta på att bara hälften av de undersökta organisationerna använder sig av metoder i sitt säkerhetsarbete. Till stor del kan detta förklaras av att de personer jag intervjuade var chefer som i de flesta fall inte var direkt involverade i arbetet med att analysera verksamheten m.h.a. säkerhetsmetoder. Detta ledde till att jag inte fick tillräcklig information för att göra en ordentlig bedömning. Baserat på befintlig information bedömer jag att organisationerna använder metoderna på det sätt som de är tänkta att användas och att de använder metoderna som ett stöd för fortsatta åtgärder. Jag ifrågasätter dock om det är rimligt att som tre av de undersökta organisationerna inte göra några analyser över huvud taget. Detta kan enligt min uppfattning leda till en mycket bristfällig säkerhetsnivå, där säkerhetsarbetet karakteriseras av brandkårsutryckningar och inte ett kontinuerligt och heltäckande arbete.

Granlund (1997) visar i sin artikel hur mycket intrången i datasystem generellt sätt har ökat och att angreppen blir allt allvarligare. Jag anser att en bakomliggande faktor till att intrång kan förekomma i så hög utsträckning är att många företag inte gör någon systematisk analys av sin säkerhet, t.ex. med hjälp av någon av metoderna som jag tidigare beskrivit i denna rapport. Att detta inte görs kan leda till att organisationer inte upptäcker sina svaga sidor och därmed lämnar öppningar som hackers kan utnyttja. Ett ökande användande av metoder i säkerhetsarbetet skulle ge är en ökad helhetssyn på vilka risker som verksamheter är utsatta för. Naturligtvis löser inte metoderna alla problem, men de kan vara ett bra hjälpmedel för att ta reda på vad som bör göras och var resurserna bör satsas.

9.3 Metoders lämplighet

Jag anser att metoderna är lämpliga i olika sammanhang. Vissa metoder lämpar sig främst till att undersöka driftsäkerheten, medan andra lämpar sig för att göra en heltäckande översyn över hela säkerhetsområdet. Det är svårt att generellt säga vilka eller vilken metod en viss organisation skall använda sig av. Faktorer som jag anser vara viktiga i detta sammanhang är:

- vilka risker organisationen utsatt för (ett företag med en fast Internetuppkoppling är mer utsatt än ett företag med ett slutet system),
- vad har organisationen som måste skyddas (t.ex. om organisationen har företagshemligheter som måste skyddas)
- vad är organisationen beredda att betala (beroende på organisationens finansiella situation mm)

En organisation som är utsatt för stora risker och har betydande affärshemligheter bör använda en heltäckande metod (t.ex. riskanalys), medan en mindre utsatt organisation kan använda sig av en mer begränsad metod (t.ex. sårbarhetsanalys eller katastrofplan). Jag anser dock att alla organisationer på lång sikt kan tjäna på att göra en heltäckande analys av verksamhetens säkerhetssituation om tid och pengar finns. Det kan vara viktigt att innan själva säkerhetsarbetet påbörjas göra en utvärdering av möjliga metoder samt jämföra vad de har för fördelar för att sedan välja den metod som är lämpligast. Görs detta får man ut det mesta möjliga av arbetet.

10 Diskussion

10.1 Allmänt om diskussion

Efter att ha genomfört detta examensarbete har jag erhållit erfarenhet i att genomföra omfattande projekt. Jag har lärt mig en mängd olika saker under arbetsprocessen, men har också efteråt upptäckt en del saker som kunde ha gjorts annorlunda.

10.2 Gjorda erfarenheter

10.2.1 Litteraturen

Ett av problemen med arbetet var att hitta lämplig litteratur. Det fanns mycket skrivet om området datasäkerhet och relativt mycket om metoder för att analysera säkerhet, däremot nästan inget om undersökningar som gjorts om organisationer verkligen använder dessa metoder och i så fall hur. Därför var det lämpligt att ha litteraturen som grund och undersökningen ta fram den information som inte täcktes i böckerna.

Ett problem är att många av böckerna som jag har som grund till arbetet är några år gamla, detta vägs dock upp av att säkerhetsmetoderna jag analyserat inte förändras så mycket över tiden, samt att resultatet till största delen bygger på undersökningen. En noggrannare genomgång av referenser till engelskspråkig litteratur hade möjligen gett fler aspekter som kunnat appliceras på mitt problemområde. Detta skulle kunna ha lett till ett resultat som var mer uppbyggt på litteratur, istället för som de är nu främst på undersökningen.

10.2.2 Intervjuundersökningen

En viktig bit av arbetet är undersökningen. Jag är till största delen nöjd med hur den genomfördes. Min undersökning hade givit ett säkrare underlag för slutsatser om den hade varit mer omfattande. Jag hade då kanske kunnat komma till ytterligare slutsatser och dessa hade varit säkrare. Det som hindrade mig till detta är främst tidsbegränsningarna och valet av undersökningsmetod. Men jag anser fortfarande att intervjuer är det bästa sättet att ta reda på informationen som behövdes. Jag anser också att en ostrukturerad intervju som jag använt har varit att föredra framför en strukturerad. Jag kunde dock ha gjort ett något modifierat frågeformulär till konsult 2, eftersom frågorna generellt sett är utformade att passa för mindre verksamheter med begränsade arbetsuppgifter.

Det jag inte fick fram så mycket information om som jag hade velat är hur företagen tillämpar metoderna för att analysera säkerhet. Detta beror på att jag pratade med högre chefer vilka hade mer övergripande överblick över säkerhetsarbetet, vilket var bra för andra delar av undersökningen, men inte gav så detaljerad inblick i tillämpningarna av metoden. Kanske detta skulle ha blivit ett bättre resultat på detta område om jag intervjuat fler tekniker som var direkt involverade i arbetet. Att de valda respondanterna var chefer gav dock bra resultat på de övriga frågorna.

Något jag kunde ha gjort annorlunda är att jag kanske borde ha påbörjat själva undersökningen tidigare. Då skulle jag haft mer tid att göra uppföljningar (t.ex. intervjuat några tekniker) och samtidigt haft mer tid över till analysen.

10.2.3 Rapportskrivningen

Jag anser att rapportskrivningen är en de svåraste bitarna i examensarbetet. Det är svårt att strukturera arbetet och bedöma vilken information som är viktig och bör tas med och vilken som är mindre viktig. Det är svårt att redan på ett tidigt stadium av rapportskrivningen när man inte är så insatt i ämnet bedöma författares trovärdighet och relevans. Jag anser dock att problemen minskat allt eftersom jag kommit in i arbetet och blivit insatt i ämnet.

10.3 Resultatet

Det resultat som jag uppnått med detta arbete tycker jag i stort sätt besvarar min frågeställning. Det är vissa delar jag velat tränga djupare in i, främst frågan om hur analysen går till i verksamheterna.

Jag tycker att resultatet som visar att relativt få verksamheter verkligen använder sig av analyser är intressant och det är en synpunkt som jag inte påträffat i någon av den litteratur som jag använt mig av. Därför anser jag mig ha hittat ett delområde i ämnet datasäkerhet som är relativt outforskat, dvs kopplingen mellan brist på analyser och det dåliga säkerhetsläge som råder i många verksamheter, (bl.a. visat av Granlund, 1997). Jag tycker också det är intressant att glappet mellan hur författare skriver att säkerhetsarbete bör bedrivas och vad som verkligen görs är så stort.

10.4 Vad som skulle kunna gjorts annorlunda

Jag anser att problembeskrivningen kunde ha varit något annorlunda. Det är främst avgränsningen som kanske är lite för bred och odefinierad. Att de skilda verksamheterna företag, kommuner och konsulter som har valts, kan ha givit arbetet en för bred karaktär, som påverkat kvaliteten negativt. Det är möjligt att resultatet skulle ha blivit bättre om jag hade koncentrerat mig på en typ av verksamhet. Å andra sidan anser jag att när man tittar på olika typer av verksamheter får man fram ganska intressanta skillnader och likheter. Men målgruppen kan trots allt vara lite för godtyckligt vald.

Jag tycker det skulle ha varit intressant att se hur informationsföretag (t.ex. banker) jobbar med att analysera sin säkerhet. Det hade varit en intressant jämförelse mot tillverkande företag. Analyserar t.ex. tillverkande företag mest för att förebygga driftstopp och analyserar då informationsföretag mer mot intrång utifrån? Denna vinkling på undersökningen tror jag skulle kunna ge ett intressant material att analysera.

10.5 Förslag till fortsatt arbete

Inom området datasäkerhet finns det mycket forskning, men det ämnesområde som jag valt, hur företag egentligen använder metoder i sitt säkerhetsarbete, har jag inte hittat mycket forskning kring. Därför tror jag att det finns mycket att göra inom detta område för vidare arbete.

En möjlig inriktning på fortsatt arbete skulle kunna vara att på djupet analysera hur företagen praktiskt använder de metoder som valts, den del av problembeskrivningen som jag funnit minst om. Detta skulle kunna leda fram till ett arbete som koncentrerar sig kring hur skillnaderna är mellan författares bilder av hur säkerhetsarbetet skall bedriva och hur organisationer i själva verket bedriver arbetet.

10 Diskussion

Min uppsats har mest gått in på djupet av ett fåtal verksamheters säkerhetsarbete. En tänkbar inriktning på fortsatt arbete är att göra en mer kvantitativ undersökning på en större målgrupp. Detta skulle leda till en mer heltäckande bild av företags arbete med metoder. Fördelen då är att man skulle kunna få resultat som statistiskt bevisar något.

Referenser

Böcker

Bort, J. och Felix, B. (1997) *Building an extranet*. Foster City, John Wiley & Sons Inc

Dahmström, K. (1991) *Från datainsamling till rapport*. Lund, Studentlitteratur

Dataföreningen i Sverige (1997) *Steg för steg mot bättre IT-säkerhet*. Sundsvall, DF Förlags AB

Edlund, L. Hedqvist, J. och Holmberg, S. (1989) *Affärssäkerhet.* Stockholm, Affärsinformation AB

Elgemyr, A. och Mattson, L. (1992) *Stora säkerhetsboken*, Stockholm, Publica

Freese, J. och Holmberg, S. (1993), *Datasäkerhet: Praktisk handbok för beslutsfattare*. Stockholm, Affärsinformation AB

Gali, P. (1992) *Informations säkerhet: hur du skyddar data, text, ljud och bild*. Stockholm, Affärslitteratur AB

Granlund, F. (1997) Datasäkerheten dålig under 1996, *Computer Sweden*, nr 2

Grate, I. (1994) *ADB-datasäkerhet*. Stockholm, Liber utbildning AB

Gunnarsson, G. (1997) *Internet boken*. Stockholm, Pagina Förlags AB

Hedemalm, G. (1997*) Intranät i praktiken*. Stockholm, Pagina AB

Ledel, G. 1993) *Att klassificera information -ett debattinlägg*. Lund, Studentlitteratur

Loshin, P. (1997) *Extranet design and implemention*. Alameda, Sybex inc

Olofson, K. (1997) Säkerhetsansvarig ett framtidsyrke, Försvara ditt nät, *Computer Sweden*, nr 18

Patel, R. och Davidson, B. (1996) *Forskningsmetodikens grunder: Att planera genomföra och rapportera en undersökning*. Lund, Studentlitteratur

Roberts, R. och Kane, P. (1989) *Computer security*. Greensboro, COMPUTE! Publications Inc

Schwatau, W. (1994) *Information warfare: chaos on the electronic superhighway*. Washington DC, Library of Congress Cataloguing-in-Publication Data

SIG Security (1997) *Riktlinjer för god informationssäkerhet*. Lund, Studentlitteratur

Sjögren, N. (1996) Datorsystemen hotas från alla håll, *Computer Sweden*, nr 67

Toppledarforum. och Statistiska centralbyrån (1996) *Det offentliga Sverige på Internet*. Solna, Design & Media

Trost, J. (1994) *Enkätboken*. Lund, Studentlitteratur

Åslund, B. (1998) *Hackare siktar in sig på företag*, Dagens Nyheter IT, 19 mars 1998

Internet

CERT (1998) *The CERT Coordination Center*

http://www.cert.org/ (As is: Mars 10 1998)

Referenser

ITSEC (1998) *The IT security scheme*
http://www.itsec.gov.uk/ (As is: Mars 05 1998)
Stein, L (1998) *The World Wide Web Security FAQ*
http://www.w3.org/Security/Faq/ (As is: Mars 10 1998)

Möjliga undersökningsmetoder

Fältundersökning

Allmänt om fältundersökning

Fältundersökning innebär att man gör en ny undersökning för att ta fram information för en specifik uppgift. Uppgiften kan t.ex. vara att utreda ett förhållande, ta reda på åsikter i en viss fråga eller ta reda på framtida eller tidigare beteende hos en viss målgrupp.

Fältundersökningar har den nackdelen att de oftast blir ganska dyra, kräver stor arbetsinsats och tar tid. Fördelen är dock att man kan få fram färsk och mycket relevant information. Här nedan beskrivs de metoder som oftast används inom fältundersökning.

Besöksintervju

Dahmström (1991) menar att en besöksintervju bör inledas med en första kontakt med personen som ska intervjuas där man ger information om undersökningen samt vad intervjun ska syfta till.

En besöksintervju kan ha hög eller låg grad av standardisering . I en intervju med hög standardisering sker intervjun efter ett strukturerat formulär. Detta förfarande innebär att formuläret måste följas till punkt och pricka för att få önskat resultat. En så strukturerad intervju underlättar redigering och behandling av det insamlade materialet.

Vid en låg grad av standardisering har intervjuaren ett antal generella frågor som respondenten uppmanas att svara på. Vid denna intervjuform har intervjuaren möjlighet att ställa följdfrågor och be respondenten att utveckla påståenden. Dessa mer ostrukturerade intervjuer är bra för att på djupet ta del av en expert- eller en annan kunnig persons kunskaper eftersom den ger möjlighet att styra intervjun. En intervju med låg grad av standardisering kan också användas som grund till en större undersökning med strukturerade intervjuer.

Dahmström (1991) menar att en besöksintervju är kostsam men ibland nödvändig för att få svar med hög kvalitet. Detta eftersom den tar mycket tid i anspråk i form av förberedelse, resa till respondenten samt själva intervjun.

Fördelar med besöksintervjuer:

- Oklarheter kan oftast enkelt redas ut genom diskussioner
- Många frågor kan ställas eftersom respondenten inte tröttnar lika fort som vid t.ex. ifyllande av formulär
- Ger möjlighet att använda visuella hjälpmedel och skisser

Nackdelar med besöksintervjuer:

- Dyrt och tar lång tid

Bilaga 1: Möjliga undersökningsmetoder

Telefonintervju

En telefonintervju liknar en besöksintervju. Skillnaden är den att intervjuaren och respondenten inte ser varandra. Detta kan resultera i att det blir svårare att förstå varandra, eftersom inga visuella hjälpmedel kan användas. En telefonintervju får inte heller ta för lång tid eftersom det är svårare att behålla respondentens intresse när han ej ser intervjuaren. Därför måste antalet frågor begränsas, (Dahmström, 1991)

En telefonintervju kan ha hög eller låg grad av standardisering. I en intervju med hög grad av standardisering används ett färdigt formulär, medan man vid låg grad av standardisering ställer generella frågor som styr ett samtal inom det aktuella ämnet.

Fördelar med telefonintervju:

- Oklarheter kan vanligen redas ut genom diskussion
- Snabbt och billigt

Nackdelar med telefonintervju:

- Intervjun kan ej vara alltför lång
- Krångliga och känsliga frågor bör undvikas
- Risk för mindre genomtänkta svar

Brevformulär

En undersökning via brevformulär går till så att ett frågeformulär skickas till respondenten. Denna har då tid att läsa igenom frågorna i egen takt för att sedan returnera dem. Ett frankerat svarskuvert bör medföljas till respondenten för att denne ska slippa kostnaden och besväret med att själv ordna detta. En stor nackdel med denna typen av undersökningar är att antalet personer som svarar ofta är lågt. Detta kan hjälpas genom att använda sig av ett väl utformat formulär som väcker intresse, samt att utlova någon slags belöning vid svar, (Dahmström, 1991)

Fördelar med postenkäter:

- Låg kostnad
- Ingen påverkan från intervjuaren
- Enkäten kan skickas till många personer

Nackdelar med postenkäter:

- Intervjuaren finns inte till hands vid oklara frågor
- Risk för bortfall

Observationer

En observationsundersökning innebär att man övervakar en försöksperson eller flera och dokumenterar hur de handlar i olika situationer. Försökspersonerna kan antingen vara införstådda med undersökningen eller så kan undersökningen genomföras utan deras vetskap.

Bilaga 1: Möjliga undersökningsmetoder

Undersökningar när försökspersoner är införstådda kan t.ex. vara vid observationer om hur användarvänligt ett nytt operativsystem är. Då observerar man en försöksperson och dokumenterar hur han kommunicerar med systemet och av detta kan man dra slutsatser om möjliga förbättringar. Ett exempel på registrering av försökspersoner utan deras vetskap ät t.ex. videofilmning av kundströmmar i livsmedelsbutiker. Utifrån denna information kan man sedan förbättra hyllornas placering i butiken.

Skrivbordsundersökning

Allmänt om skrivbordsundersökning

Skrivbordsundersökning handlar om att ta vara på lagrad information och eventuellt tolka eller anpassa den så att den passar för den aktuella situationen. Det kan vara en redan gjord undersökning som också är relevant för det område som undersöks. En skrivbordsundersökning kan vara interna uppgifter hos en organisation, t.ex. register över klagomål från kunder. Det kan också vara officiell statistik, t.ex. bransch statistik eller statlig statistik inom ett visst område. Skrivbordsundersökningar har den fördelen att de är billiga. Nackdelen är dock att det inte genom dessa alltid går att få fram relevant information.

Litteraturstudier

Litteraturstudier lämpar sig bra för att skaffa allmän kunskap om ett ämne. Detta bör göras på ett tidigt stadium i undersökningen så att man har kunskap om ämnet när skrivandet påbörjas. Till litteraturstudie räknas böcker, tidigare gjorda fallstudier, forskningsrapporter, artiklar osv. Det är viktigt att kritiskt granska den valda litteraturen eftersom man inte alltid vet hur forskningsvärlden accepterar författarens slutsatser. Därför kan det också vara bra att läsa flera författare och jämföra deras påståenden mot varandra.

Fördelar med litteraturstudie:

- Det finns mycket litteratur inom de flesta områden
- Information kan lätt åskådliggöras med hjälp av bilder
- Det ligger ofta mycket bakgrundsinsamling till litteraturen

Nackdelar med litteraturstudie:

- Det är lätt att ta författarens åsikter och synsätt som fakta
- Det finns inte alltid tillgång till litteratur inom nya områden

Internet

Internet är ett relativt nytt medium som bl.a. kan användas för att leta och finna information. Nackdelen med Internet ur ett informationssöknings perspektiv är att det kan vara svårt att bedöma hur tillförlitlig källan är. Vem som helst som har tillgång till Internet kan ha lagt ut information på nätet. Denna information kan i många fall vara partisk eller rent av felaktig. Därför är det viktigt, när man använder sig av Internet, att man kritiskt granskar informationen och gärna har två olika källor som stödjer

påståendena. Det kan också vara bra att hålla sig till kända källor, t.ex. regeringsorgan eller större fristående organisationer.

Fördelar med Internet:

- Det finns ofta aktuell information att tillgå
- Det finns stora mängder information som berör många ämnen

Nackdelar med Internet:

- Tillförlitligheten hos funnen information kan vara bristfällig
- Det kan vara svårt att hitta rätt information p.g.a. Internets storlek

Intern företagsinformation

Intern företagsinformation är information som ett företag lagrar internt för eget bruk. Det kan vara internredovisningar, kundstatistik och tidigare utförda undersökningar. Denna information är företagets egna och det finns ingen utanför företaget, förutom myndigheter som i vissa fall har rätt att ta del av den. Denna information är därför svår att använda för utomstående och kan sällan användas i undersökningar annat än företagets egna.

Officiell statistik

Officiell statistik är information som samlas in av myndigheter, branschorganisationer och privata företag. Denna information är antingen gratis, som t.ex. vissa sifo undersökningar eller kostar, som t.ex. information insamlad av privata företag som gör marknadsundersökningar. Officiell statistik är ofta gammal och är inte alltid relevant eftersom den sällan är framtagen direkt för det ändamål som undersökningen har. Det är dock betydligt billigare än att på egen hand utföra en undersökning.

Urvalsmetoder

Viktigt för en undersökning är hur personerna som ska ingå i undersökningen väljs ut. Resultatet av undersökningen ska enligt Patel och Davidson (1996) vara så generellt som möjligt. Med det menas att resultaten som erhålls genom att undersöka en grupp människor ska gälla för andra personer som är jämförbara med den undersökta gruppen.

Den mest omfattande undersökningen som kan göras är en totalundersökning. I denna intervjuas hela målgruppen, i detta fall skulle det vara alla företag som på något sätt sysslar med säkerhet i Sverige. Eftersom det är praktiskt omöjlig att ensam undersöka denna stora grupp kommer ett urval att göras. Här nedan diskuteras de olika metoderna för urval som är möjliga.

Bilaga 1: Möjliga undersökningsmetoder

Obundet slumpmässigt urval

Enligt Patel och Davidson (1996) är obundet slumpmässig undersökning (OSU) den enklaste formen av urvalsmetod. Alla personerna i populationen har en lika stor slumpmässig chans att komma med i urvalet, dvs är hela målgruppen 100 personer kan en dator ordna att 10 personer slumpmässigt välj från målgruppen.

Fördelar med obundet slumpmässigt urval:

- Metoden är enkel och lättförståelig

Nackdelar med obundet slumpmässigt urval:

- Slumpen gör att viktiga grupper kanske inte alls kommer med i urvalet och andra mindre viktiga kan bli överrepresenterade

Stratifierat urval

Stratifierat urval går enligt Patel och Davidson (1996) till så att man delar in populationen i olika strata (delgrupper) beroende på egenskaper som man vill att de undersökta personerna ska ha. Därefter gör man ett slumpmässigt urval inom varje delgrupp.

Med hjälp av denna metod kan man reglera så att grupper med vissa egenskaper som man vill studera inte blir underrepresenterade. Variabler som är kan användas för att välja ut delgrupperna är exempelvis ålder och kön.

Fördelar med stratifierat urval:

- Ger rättvisare fördelning vid populationer som innehåller många delgrupper med olika egenskaper

Nackdelar med stratifierat urval:

- Det är arbeteskrävande att dela in populationen efter grupper

Systematiskt urval

Systematiskt urval är enligt Patel och Davidson (1996) liksom obundet slumpmässig undersökning en stickprovsmetod. Man väljer systematiskt ut individer i listan över individerna i populationen. Man kan t.ex. välja ut var 10:e individ, dvs först individ nummer 10, sedan individ nummer 20 osv.

Fördelar med systematiskt urval:

- Enkelt och kräver ej mycket tid
- Kan ge säkrare urval än obundet slumpmässig undersökning eftersom spridningen mellan de utvalda blir jämnare

Nackdelar med systematiskt urval:

- Om det finns någon variabel som uppträder med en viss periodicitet riskerar urvalet att inte bli en miniatyr av populationen

Tillgänglig grupp

När hela totalpopulationen av någon anledning inte är känd fungerar inte ovanstående urvalsmetoder, eftersom dessa kräver vetskap om totalpopulationen. De ekonomiska och tidsmässiga ramarna i en undersökning kan också hindra att en stickprovsundersökning görs. Urval enligt tillgänglig grupp medför dock att resultatet av undersökningen inte är överförbart på någon totalpopulation.

Fördelar med tillgänglig grupp:

- Metoden är snabb och mycket enkel
- Ger ekonomiska och tidsmässiga vinster

Nackdelar med tillgänglig grupp:

- Resultatet kan inte överföras på någon annan grupp än den undersökta

Kvantitativ eller kvalitativ undersökning

En undersökning kan enligt Trost (1994) vara antingen kvantitativt eller kvalitativt. Man kan något förenklat säga att en metod är kvantitativ när man använder sig av siffror eller jämförelser som: längre, fler och mer. En undersökning är däremot kvalitativ om man inte använder jämförelser, varelse i siffror eller jämförande ord.

Enligt Trost (1994) ska man använda en kvantitativ undersökning om man vill kunna ange frekvenser. Om frågeställningen däremot handlar om att få förståelse eller att hitta mönster i något skall en kvalitativ undersökning användas. Trost (1994) menar att det är syftet med projektet som avgör vilken metod man ska använda sig av.

Jag anser att besöksintervju och telefon intervju både kan användas till kvalitativ och kvantitativ eftersom det i dessa metoder inte finns något som begränsar frågornas struktur åt ena eller andra hållet. Brev undersökning tror jag främst stöder kvalitativ undersökning eftersom det är svårt att få en djupare förståelse i denna begränsade form av kommunikation. Observations undersökning däremot anser jag främst stödja kvalitativa undersökningar eftersom det ger en djup insyn i en verksamhet och följaktligen borde ge god kvalitet.

Frågeformulär företag

1) Hur stort är företaget i antal anställda och omsättning?
2) Vilka är era arbetsuppgifter?
3) Vilka är era kunder?
4) Vilken typ av datamiljö har ni?
   - Hur många datorer finns i ert nätverk?
5) Vilka typer av uppkopplingar har ni med omvärlden, t.ex. Internet, Extranet

6) Har ni någon generell metod för att analysera säkerheten? *(t.ex. Riskanalys, Informationsklassificering, Sårbarhetsanalys, Katastrofplan mm)*
   6a) Hur använder ni denna metod?
   6b) Fungerar denna metod tillfredsställande?
   6c) Vad upplever ni som sämst respektive bäst med denna metod?
   6d) Har ni övervägt att använda er av någon annan metod?

7) Hur påverkar följande faktorer säkerhetsarbetet och val av metod:
   - tillgänglig personal
   - budget
   - tidsramar
   - datormiljön

   Vilka övriga faktorer är avgörande för säkerhetsarbetet?

8) När utförs säkerhetsarbetet?
9) Hur sker uppföljningen?
10) Har ni någon säkerhetsorganisation eller säkerhetsansvarig?
11) Vad är det mest kritiska i ert säkerhetsarbete?
12) Vilka hot upplever ni som allvarligast mot er verksamhet?

12) Har du några övriga synpunkter eller kommentarer på ämnet?

Företag 1 (Intervju med Datorchefen)

Företag 1 är ett medelstort tillverkande företag i Mellansverige. Det har omkring 300 anställda och en omsättning ca 350 miljoner. De tillverkar förbrukningsmaterial för stora företagskunder, som främst finns i Sverige och USA.

Nätverket består huvudsakligen av PC-datorer med windows 95 på clienterna och Windows NT på servrarna. Det finns runt 150 PC maskiner i nätverkstoppologin tokenring. De program som används är främst de från Microsoft office paketet. Några få AS 400 används också för att sköta MPS systemet.

Företaget har en ISDN uppkoppling mot Internet och en mot sitt systerbolag i England. Datorchefen anser att företaget är ganska sent ute med uppkopplingar mot omvärlden, främst p.g.a. att de har ett dåligt geografiskt läge. Detta gjorde bl.a. att ISDN tills för ca ett år sedan var för dyrt för företaget att använda eftersom Telia tidigare hade höga anslutningsavgifter för glesbygd.

Metoder och säkerhetsarbete

En större genomgång av datorsäkerheten gjordes för ca tre år sedan av ett konsultföretag. Denne utförde en omfattande undersökning av främst systemets driftsäkerhet. Detta arbete har sedan legat som grund för företagets egna säkerhetsarbete. Datorchefen har också tagit fram en säkerhetspolicy för företaget efter riktlinjerna som bygger på resultaten från konsulten. Säkerhetspolicyn har som främsta uppgift att få hela organisationen att tänka på säkerhet. Ämnen som den behandlar är bl.a. hur skyddet mot virus skall genomföras samt de anställdas skyldigheter.

Den metod som företaget använder sig av är en katastrofplan, dvs planering för att minimera effekterna av oförutsedda avbrott (för mer information se kapitel 3.4.3). Företaget har inte blivit utsatt för några större incidenter och därför menar datachefen att säkerhetsarbetet kanske inte har tagits på så stort allvar som det förtjänar. Det geografiska läget samt att de inte har några fasta uppkopplingar anser datachefen också kan vara orsaken till att inte mer görs för säkerhetsarbetet.

Säkerhetsansvarige anser att bristen på personal med kompetens inom datorsäkerhet har påverkat företagets säkerhetsarbete negativt. Skall man anställa konsulter för att utföra säkerhetsarbete blir det dyrt och en räkning på 50 - 60 000 kr är inte ovanligt för att påbörja en kartläggning av säkerheten.

Företagsledningen vill inte lägga alltför stora pengar på datorsäkerhet. Datoransvarige anser att de löpande kostnaderna för en god datorsäkerhet är relativt höga eftersom arbetet hela tiden måste uppdateras för att vara aktuellt. Han upplever dock inte budgeten som något av företagets största hinder för en god datorsäkerhet.

Datorchefen anser att tidsbrist är en stor orsak till att säkerhetsarbetet inte är högprioriterat. Han upplever det svårt att få tid över från den dagliga verksamheten.

Företaget har en säkerhetsansvarig som har det övergripande ansvaret för säkerhetsarbetet. Han har inte bara ansvar för datasäkerheten utan för allt säkerhetsarbete, bl.a. anses den fysiska säkerheten vara relativt viktig. Den säkerhetsansvarige har inte säkerheten som sin enda uppgift utan jobbar också med andra frågor.

Det förekommer inget arbete med att skydda sig mot interna angrepp eftersom dessa inte anses som troliga. Det säkerhetsarbete som förekommer internt är främst arbete

med att skydda sig mot slarv, t.ex. att ta backuper för att undvika att viktiga filer går förlorade genom oavsiktlig radering.

Det som datorchefen anser vara det största hotet mot datorsäkerheten är virusangrepp. Hittills har angreppen varit begränsade till enstaka datorer, men han anser att ett mer omfattande angrepp skulle kunna få allvarliga konsekvenser.

Företag 2 (Intervju med Datorchefen)

Företaget har på den plats där jag besökte det i Mellansverige runt 700 anställda, men företaget är uppdelat i flera olika divisioner som finns på ett flertal platser i Sverige och övriga Europa. Divisionen som jag besökte arbetar främst med produktutveckling. Omsättningen är om man räknar in alla delar av företaget ett par miljarder. Företaget tillverkar produkter för en global marknad och köparna är främst andra företag och bolag.

Datormiljön är väldigt blandad med mycket stordatorer främst IBM 390 MVS datorer, men det finns också UNIX datorer främst för ekonomsystemet och CAD (Computer Aided Design). Det finns också en PC plattform som går under Windows NT i klienterna. Företaget har också ett antal bärbara datorer med Windows 95. Det totala antalet datorer (alla kategorier inräknade) tror datorchefen är runt 600 maskiner. Åtta personer är anställda på IT avdelningen.

Företaget har en mängd uppkopplingar mot omvärlden. De är uppkopplade tillsammans med alla andra divisioner i Sverige (7 st) i ett stort nätverk. De har via detta nätverk tillgång till ett Intranet, Extranet samt Internet. Kopplingen mot Internet utgår för alla divisionerna från en central punkt som finns i huvudkontoret.

Metoder och säkerhetsarbete

Varje division har en lokal datoravdelning som sköter om och har ansvar för sitt datornät. De olika enheterna kan sedan köpa tjänster från en central datorenhet som finns på huvudkontoret. Den centrala datorenheten tillhandahåller t.ex. förbindelsen mellan divisionerna och skydd utåt mot Internet med hjälp av en brandvägg.

Det finns också en central IT-stab som ger riktlinjer åt de olika divisionerna på en strategisk nivå. Riktlinjerna kan t.ex. vara att alla enheter måste använda samma ordbehandlingsprogram. Divisionerna kan sedan agera relativt fritt inom dessa riktlinjer. På IT-staben finns också en säkerhetschef som har ansvar för de strategiska säkerhetsbesluten. Det yttersta ansvaret för att en viss division får det IT-stöd som det behöver ligger på enhetschefen.

Den metod som företaget har använt sig av i sitt säkerhetsarbte är sårbarhetsanalys (se kap 3.4.2). Arbetet byggde på en variant av traditionell sårbarhetsanalys med färdiga blanketter som grund. Den främsta orsaken till att detta arbete genomfördes var att man ville se hur länge verksamheten kan klara sig utan datorstöd samt hur kostsamma driftstopp av olika typer skulle bli. Det svåraste som datorchefen såg var att med hjälp av denna analys få en säkerhetsnivå som står i proportion till kostanden. Mycket i arbetet handlade om vilka kritiska komponenter som borde dubbleras för att ha backup om en viss komponent fick driftstopp. Datorchefen ser arbetet med säkerhet som en försäkring mot stora oförutsedda utgifter. Det var dock två år sedan detta arbete utfördes senast. Arbetet med detta leds av den centrala IT-staben.

Datorchefen ville inte prata alltför ingående om hur företaget skyddade sig mot angrepp utifrån. Han medgav att företaget såg externa intrång som ett hot och att det arbetades med att skydda sig mot sådana angrepp. Säkerheten upprätthålls främst med hjälp av brandväggar, kryptering och logningsystem. Enligt datorchefen hade företaget dock inte använt sig av någon metod för att systematiskt analysera de externa hoten.

Bilaga 4: Intervju med företag 2

All information i företaget klassificeras. Nivåerna är: publikt, internt och företagshemligt.

Datorchefen anser att det i bland är svårt att få tid med säkerhetsarbete, mycket beroende att det måste ske parallellt med det dagliga arbetet. Det finns inom företaget ingen speciell budget för säkerhet. Istället tas pengar från IT avdelningens normala budget. Därför sker en bedömning om satsningar på säkerhet är lönsam, dvs om den återbetalar sig. Datorchefen anser att den blandade datormiljön gör säkerhetsarbetet svårare att administrera och mer kostsam en mer enhetlig datormiljö.

Företaget har också en omfattande IT policy som säger hur de anställda ska bete sig i datorsammanhang. Denna syftar främst till att förhindra att viktig information tappas bort eller förvanskas.

Datorchefen har svårt att se någon enskild del av säkerhetsarbetet som den mest kritiska. Han kan heller inte ange något hot mot verksamheten som det allvarligaste.

Frågeformulär kommuner

1) Hur många anställda finns i kommunen?
2) Vilken typ av datamiljö har ni?
   - Hur många datorer finns i ert nätverk?
3) Vilka typer av uppkopplingar har ni med omvärlden, t.ex. Internet, Extranet

4) Har ni någon generell metod för att analysera säkerheten? *(t.ex. Riskanalys, Informationsklassificering, Sårbarhetsanalys, Katastrofplan mm)*

   4a) Hur använder ni denna metod?

   4b) Fungerar denna metod tillfredsställande?

   4c) Vad upplever ni som sämst respektive bäst med denna metod?

   4d) Har ni övervägt att använda er av någon annan metod?

5) Hur påverkar följande faktorer säkerhetsarbetet och val av metod:

   - tillgänglig personal
   - budget
   - tidsramar
   - datormiljön

   Vilka övriga faktorer är avgörande för säkerhetsarbetet?

6) När utförs säkerhetsarbetet?
7) Hur sker uppföljningen?
8) Har ni någon säkerhetsorganisation eller säkerhetsansvarig?
9) Vad är det mest kritiska i ert säkerhetsarbete?
10) Vilka hot upplever ni som allvarligast mot er verksamhet?
11) Har du några övriga synpunkter eller kommentarer på ämnet?

Kommun 1 (Intervju med dataansvarig)

Kommun 1 har runt 10 000 innevånare och ligger i Mellansverige. Det finns ca 700 anställda inom kommunen och datornätet har 120 användare. Datormiljön är enbart PC-datorer med till största delen Microsoft office program. Nätet administreras med hjälp av Novell.

Uppkopplingar mot omvärlden är en ISDN anslutning mot Internet som användarna på nätverket har tillgång till samt några få modem för att användas vid distansarbete och som går direkt in i nätverket.

Metoder och säkerhetsarbete

Kommunen har aldrig gjort någon typ av analys av sin säkerhet. Det har inte skett något strategiskt arbete med säkerhetsfrågor. Det finns inte heller någon säkerhetsansvarig inom kommunen. Det ansvar som finns är att de olika förvaltningarna inom kommunen själva ansvarar för sina register, t.ex. för att datan är korrekt och att licenser finns för programmen. Rent principiellt anser dock dataansvarige att det är kommunfullmäktige som har ansvaret för säkerheten.

Det arbete som skett med säkerhet är uppmaningar till regelbundna lösenordsbyten och spärrar för att folk inte ska kunna jobba hur sent som helst. Inom socialtjänsten krypteras information automatiskt av programmen så att bara behöriga kan få tillgång till klassificerad information, t.ex. uppgifter om socialbidrag. Enligt datoransvarige är det bara personer som handlägger de olika ärendena som har tillgång till dessa. Detta eftersom det finns reglerande lagstiftning på området.

Dataansvarige har haft uppe frågan med datorsäkerhet i datorgruppen, men något organiserat arbete har inte utförts. Detta beror till stor del på brist av personal samt en ganska snäv budget. Men datoransvarige anser inte att intrång utifrån är troligt eftersom det är svårt att ta sig in i systemet då det är relativt slutet. Han upplever dock ända intrång utifrån som det största hotet mot kommunens datorsäkerhet.

Det finns inga nedskrivna policys för användarna, men de uppmanas att logga ur eller använda skärmsläckare med lösenord när de lämnar sina datorer.

Kommunen har tidigare varit utsatt för ett internt angrepp. Det som inträffade var att en person med behörighet till ekonomisystemet bokade sina privata räknigar för kommunala tjänster som betalda. Detta uppdagades dock och personen blev avskedad. Datoransvarige upplever att det går att ”fiffla” med system som man har tillgång till men han anser att det förr eller senare upptäcks.

Kommun 2 (Intervju med IT-chefen)

Kommun 2 har omkring 60 000 innevånare och ligger i Västsverige. Antalet anställda är ca 3600 personer och det finns ungefär 500 datorer uppkopplade i nätverket (skolor borträknade).

Datormiljön är blandad. Huvuddelen består av Windows 95 datorer som clienter och Windows NT i servern. Men det finns också andra system bl.a. UNIX som främst används av socialförvaltningen.

Kommunen har två typer av uppkopplingar med omvärlden. De har en fast uppkoppling till Internet via en Internetleverantör samt X25 uppkoppling som främst används mot banker för att betala räkningar. Internetuppkopplingen går direkt in i nätverket via en brandvägg så att alla i kommunens datornät har tillgång till Internet.

Kommunens IT enhet är en fristående enhet och IT-chefen har budgetansvar. De olika förvaltningarna har egna datoransvariga med ansvar för sin del av datorsystemet. IT-chefen har det övergripande ansvaret och har hand om de strategiska frågorna.

Metoder och säkerhetsarbete

Kommunen har aldrig använt någon metod eller något analysverktyg för att analysera datorsäkerheten. IT-chefen anser sig vara insatt i de olika metoderna för att analysera säkerhet eftersom han har läst en mängd böcker i ämnet. Därför anser han sig ha använt en del av tankarna från dessa böcker i sitt arbete. Han menar att han har tittat extra noga på bitar som enligt litteraturen är särskilt kritiska i säkerhetsarbetet. Det han anger som mest kritiskt för kommunen är driftsäkerhet, (mer om det senare).

IT-chefen anser att skyddet utåt är viktigt eftersom kommunen har en fast uppkoppling mot Internet. Därför har man nyligen anlitat en konsult som har testat hur väl brandväggen fungerar, men resultatet från den undersökningen är ännu inte klar. Den interna säkerheten fungerar tillfredsställande med loginsystem som begränsar vilka som har tillgång till känslig information. Tidigare var det de olika förvaltningarna som hade hand om dessa aspekter och då fanns det stora skillnader i den interna säkerhetsnivån. Sedan IT enheten tog det övergripande ansvaret har säkerhetsnivån blivit bättre.

Kommunen har ingen nedskriven IT-policy. IT-chefen anser att det är viktigt att få ett helhetstänkande som innefattar alla anställda i säkerhetesfrågor. Arbete pågår med att bygga upp ett Intranet som bl.a ska användas för att få ut information till användarna.

IT-chefen anger att bristen på kompetent IT-personal påverkar säkerhetarbetet negativt, eftersom tiden inte alltid räcker till för att utföra det säkerhetsarbete som skulle behövas. Istället utförs arbetet med säkerhet när det finns tid för det. Att få pengar till säkerhetsarbetet ser han inte som något problem. Han upplever dock pressade tidsramar och den blandade datormiljön som faktorer som försvårar säkerhetsarbetet.

IT-chefen skulle önska att mer av arbetet med säkerhet dokumenterades. För närvarande finns det inte tillräckligt nedskrivet om säkerhetsarbetet. Han tycker att det är viktigt att utomstående personer tittar på arbetet och han ser det för närvarande som svårt, just på grund av bristen på dokumentation. Detta är dock ett område som kommunen ska bättra sig på. Tidigare har revisorerna givit viss feedback på säkerhetsarbetet, vilket han anser är bra.

Bilaga 7: Intervju med kommun 2

Enligt IT-chefen är det värsta som skulle kunna hända verksamheten ur datasäkerhetssynpunkt att systemet fysiskt skulle bli förstört eftersom man är beroende av ett fungerande system för den dagliga verksamheten. Han anger därför att en brand i datorrummet där servrar mm finns skulle vara förödande. På grund av detta anser han att driftsäkerheten är viktig. Han håller för närvarande på att analysera vad det skulle kosta att ha en extra backup för vissa viktiga system.

Frågeformulär konsulter

1) Hur stort är företaget antal i antal anställda och omsättning?
2) Vilka är era arbetsuppgifter?
3) Vilken typ av klienter har ni?

4) Vilka datamiljöer arbetar ni mest inom?

5) Har ni någon generell metod för att analysera säkerheten hos era klienter? *(t.ex. Riskanalys, Informationsklassificering, Sårbarhetsanalys, Katastrofplan mm)*

5a) Hur används denna metod?

5b) Fungerar denna metod tillfredsställande?

5c) Vad upplever ni som sämst respektive bäst med denna metod?

5d) Har ni övervägt att använda er av någon annan metod?

5e) Hur stor roll spelar externa kopplingar, t.ex. Internet, Extranet för säkerhetsarbetet?

6) Hur påverkar följande faktorer säkerhetsarbetet och val av metod:

- tillgänglig personal
- budget
- tidsramar
- krav från kunden
- datormiljön

Vilka övriga faktorer är avgörande för säkerhetsarbetet?

7) När utförs säkerhetsarbetet?
8) Hur sker uppföljningen?
9) Hur sker ansvarsfördelningen för säkerhetsarbetet mellan er och era klienter?
10) Vad är det mest kritiska i säkerhetsarbetet?
11) Vilka hot upplever ni som allvarligast mot era klienters verksamhet?
12) Har du några övriga synpunkter eller kommentarer på ämnet?

Konsult 1 (Intervju med ägaren)

Företaget är ett mindre konsultföretag i Västsverige. Verksamheten är ett enmansföretag dvs ägaren är också den enda som jobbar inom företaget. Omsättningen är runt 600 000 kr.

Han har två huvudsakliga verksamhetsområden, dels system för materialadministration och logistik för tillverkningsindustri och dels ett ADB-system för tryckerier som han har varit med om att ta fram och därför blivit kvar inom den nischen. Han samarbetar med ett finskt företag som utvecklar system för tryckerier. Han är också återförsäljare för ett svenskt administrationsprogram för mindre företag.

Hans kunder är för tryckerisystemen mindre eller medelstora företag med mellan 50-100 anställda och för materialadministrationssystemen något större företag med ca 200-300 anställda. Det administrativa programmet som riktar sig till småföretagare säljs företrädesvis till små företag med en eller ett par anställda. Kunderna finns främst inom närområdet.

Hans huvudsakliga arbetsuppgift är systemutveckling för tryckerier. Det är främst specifikationerna som han tar fram i samarbete med användarna. Han utför själv ingen programmering. Specifikationerna går i korthet till så att han gör en systemspecifikation utifrån hur verksamheten arbetar, vilka kunder de har och vilka krav de har. När konsulten har gjort specifikationen utför det finska företaget programmeringen. Konsulten utför sedan implimenteringen, hjälper till med att lägga upp rutiner samt utbildar personal.

Han arbetar mest inom PC-miljö, men har också vissa jobb i UNIX-miljö då systemet för tryckerier är UNIX baserat.

Metoder och säkerhetsarbete

Konsulten använder sig inte av någon metod eller någon annan systematisk analys av datorsäkerhet. Den enda analysen som han ibland genomför är en mindre analys av vad som händer när system får driftstopp, men detta brukar inte resultera i några åtgärder eftersom företagen räknar med att snabbt få hjälp genom sina serviceavtal. Han anser det vara ovanligt att systemen står stilla mer än några timmar och att den tiden det står stilla går det en kortare tid att sköta driften med hjälp av utskrifter som tidigare gjorts. Problemet är att informationen snabbt blir gammal.

Istället utförs praktiska säkerhetsåtgärder som, t.ex. att lägga in loginsystem och därmed begränsa att utomstående tar sig in i systemet och att användare kommer in i program som de inte har behörighet för. Andra delar av säkerhetsarbetet som han kommer i kontakt med är rutiner för backup, som han anser vara en viktig del. Han menar att säkerhetsarbete mycket handlar om att göra rutiner som företagen själva får utföra. Han använder modem med jämna mellanrum för att gå in och titta och kontrollera datasystemen hos företagen han jobbar mot.

Företagen han jobbar mot har först på senare år fått tillgång till externa uppkopplingar t.ex. Internet och då bara via modem. Detta gör att han inte jobbar något speciellt med den externa säkerheten, förutom det rutinmässiga som t.ex. loginsystem. Han medger dock att det finns risker utåt i och med att det går att ta sig in i de flesta företagen via modem. Dessa uppkopplingar har inte säkerhetsfunktionen återuppringning, vilket går dem sårbara för intrång.

Han har dock inte varit med om att företag har fått intrång utifrån. Han har inte heller varit med om företag som har varit utsatta för interna angrepp. De förluster som kommit sig av interna händelser har främst varit genom slarv eller oaktsamhet. Det mesta har gått att reda ut med hjälp av backuper. Det är få av företagen som han arbetar mot som har något heltäckande skydd mot virus. Han har inte varit med om virusangrepp i någon större omfattning och ser det därför inte heller som något stort problem.

Han medger att det inte förekommer speciellt mycket uppföljning av säkerhetsarbetet. Säkerhetsarbete utförs främst när systemet inplanteras i verksamheten, eftersom det är då login, grupper av användare och rutiner som läggs upp.

Företagen han jobbar mot är oftast för små att ha egna säkerhetsfunktioner, ofta ligger ansvaret på enstaka personer. Konsulten har efter att han är klar med arbetet i ett system inget säkerhets eller driftansvar. Han håller dock ett vakande öga på sina klienters system eftersom han anser att det ligger i hans egenintresse att allt fungerar tillfredsställande.

Konsult 2 (Intervju med chefen för ett regionalkontor)

Konsult 2 är ett större konsultföretag med verksamhet på ett flertal platser i Sverige och även utomlands. Jag har intervjuat chefen på ett lokalkontor på en mellanstor ort i Västsverige. Kontoret har ett tiotal anställda och omsättningen är för hela Sverige ca 3 miljarder.

Jag kommer i fortsättningen att beskriva arbetet som lokalkontoret utför och inte beskriva företaget ur ett helhetsperspektiv, dvs när jag beskriver konsultens arbete syftar jag på den lokala avdelningen. Kunderna i närområdet är främst större tillverkande industrier och distribuerande företag. Konsultföretaget arbetar med alla befintliga datormiljöer, dvs allt från PC till stordatorer och UNIX. Konsulten har inga kontrakt med några speciella leverantörer av hård- eller mjukvara. De har samarbetsavtal med alla större tillverkare för att på så vis kunna använda de produkter som är bäst för varje specifik klient.

Metoder och säkerhetsarbete

Konsulten har inga löpande driftavtal för sina klienter dvs det har inte ansvaret för ett företags hela datordrift (sk outscoring). Om någon kund i närområdet vill ha denna typ av tjänst blir det något av avdelningarna i övriga landet som arbetar med sådana uppgift som åtar sig jobbet. Detta gör att de inte bedriver något kontinuerligt säkerhetsarbete för sina klienter, utan istället är det främst inom systemutveckling som arbete med datorsäkerhet bedrivs.

Konsulten har för både riskanalys och sårbarhetsanalys egna mallar som specificerar hur arbetet ska utföras. Dessa analysmetoder kommer ofta in på ett mycket tidigt skede i utvecklingsprocessen och handlar om att analysera verksamhetsstödet. Med detta menas att funktionerna och verksamhetsprocesserna analyseras efter olika fel som kan uppkomma och hur systemet skall klara av dessa. Alltså systemets funktionalitet och risken att systemet inte klarar av att utföra de rutiner som krävs av det.

Arbetet går till så att man samlar inblandad personal i en sk ”workshop” där man har arbetsmöten efter en strukturerad metodik. Personer som närvarar på dessa ”workshops” är datafolk, verksamhetskunniga, ansvariga chefer och övriga berörda parter. De har sedan en mall på hur riskanalysen ska gå till som anpassas till den aktuella situationen. Själva analysen är en brainstorming där klassificerar de som känner till verksamheten de olika riskelementen i olika risk nivåer: 1,2 och 3. Sedan sammanställs informationen och en bedömning görs. Det finns sedan tumregler för vilka poäng som kräver någon typ av åtgärd.

Konsulten har flera medarbetare som har kunskap om dessa metoder för att analysera säkerhet. Detta krävs eftersom brist på personal inte ska få hindra att uppdrag utförs. Behövs det folk med en viss kompetens för ett visst projekt kan dessa hämtas in från något av de övriga lokal avdelningarna som finns runt om i landet. Organisationen är på så vis mycket flexibel.

I senare faser av systemutvecklingen, främst i inplementeringen utförs analys av hur datordriften ska kunna fungera på ett tillfredsställande sätt. Detta arbetet sker i samarbete med klientens dataavdelning och arbetet syftar till få systemet driftsäkert. Detta sker bl.a. genom att lägga upp rutiner för hur det dagliga arbetet skall bedrivas. Vilka faser som konsulten arbetar med är olika beroende på vad det är klienten

behöver hjälp med. Vissa av klienterna har intern kunskap av vissa av utvecklingsstegen och då hjälper konsulten bara till med de steg som behövs, andra har inte denna kunskap internt och konsulten får ta hela ansvaret.

På konsultföretaget finns en personalgrupp som de kallar för IT-arkitekter. De är experter på tekniska plattformar och datormiljöer. IT-arkitekterna är med i de delar av projektet där dessa kunskaper krävs. De kan t.ex. vara med i riskanalysen för att göra bedömningar om hur en viss datormiljö kommer att klarar av ett nytt och mera kapacitetskrävande system. Denna personalgrupp får inte några längre uppdrag för att på så sätt finnas tillgängliga för alla projekt där deras medverkan krävs.

Konsulten jobbar också med säkerhet mot intrång. Det som är ledstjärnan i detta arbetet är vad kunderna tycker är viktigt. Eftersom system med öppningar utåt t.ex. via Internet uppkoppling eller extranet, inte kan bli helt säkra så är det kunden som får avgöra säkerhetsnivån. Chefen anser att en avvägning måste göras eftersom man ibland måste ta en viss risk för att få systemen att fungera på ett vettigt sätt. Han menar att helt vattentäta system inte kan fungera på ett bra sätt. Det är främst när konsultföretaget jobbar med utveckling av system för Internet som denna problematik uppstår. Chefen anser att säkerhet berörs i alla faser av systemutvecklingen vid projekt av detta slag. IT-arkitekterna har det som ett av sina verksamhetsområden att vara insatta i tekniker för säkerhet inom detta område.