STATSKONTORET 1997:29 b

Handbok i IT-säkerhet

Del II

Policy, ansvar och organisation

STATSKONTORET 1997:29 b

Handbok i IT-säkerhet

Del II

Policy, ansvar och organisation

STATSKONTORET
Box 2280, 103 17 Stockholm

Beställningar:
Publikationsservice
Tel 08-454 46 43 · Fax 08-454 46 45
E-post: publikations.service@statskontoret.se
http://www.statskontoret.se

Original och tryck CM Gruppen AB, 1998
ISBN 91-7220-298-X

Förord

Dagens elektroniska informationshantering ställer höga krav på säkerheten. Då många organisationer strävar efter att göra sin information tillgänglig över nätverk uppkommer många nya hot speciellt då man ansluter organisationens nät till publika nät.

För att säkra informationen, så att t.ex. obehöriga inte manipulerar den, krävs en helhetssyn på informationssäkerheten. Det räcker ofta inte med enskilda tekniska säkerhetslösningar utan det behövs även olika administrativa rutiner såsom katastrofplanering, plan för utbildning av användare m.m.

Som ett led i Statskontorets rådgivning till myndigheter har vi under åren 1989–1994 givit ut en rapportserie i elva delar som heter Vägledning i ADB-säkerhet. På grund av den snabba teknikutvecklingen och delvis nya hotbilder har rapportserien nu reviderats.

Handboken består av tre delar med utgångspunkt från olika ansvarsområden. Även om delarna vänder sig till delvis olika målgrupper kan de med fördel läsas av alla som önskar en djupare orientering inom området informationssäkerhet.

Del 1. Introduktion
Vänder sig till alla som behöver en överblick i informationssäkerhetsfrågor. Denna del är en sammanfattning av de två följande delarna. Syftet är att läsaren snabbt ska kunna orientera sig inom ämnesområdet. Här finns även en ordlista som förklarar vissa av de begrepp som förekommer.

Del 2. Policy, ansvar och organisation
Vänder sig till främst verksamhets- och linjeansvariga. Syftet är att öka medvetenheten om organisatoriska skyddsåtgärder som en förutsättning för fungerande tekniska lösningar.

Del 3. Skyddsåtgärder

Vänder sig främst till IT- och IT-säkerhetspersonal. Syftet är att öka medvetenheten om de tekniska skyddsåtgärder med tillhörande administrativa åtgärder som kan tillämpas i olika driftmiljöer för att höja informationssäkerheten.

Innehållet i denna handbok bygger på omarbetat material från Vägledning i ADB-säkerhet men stora delar av materialet är nyskrivet. Arbetet har utförts inom ramen för Statskontorets verksamhetsområde Tekniska plattformar och informationssäkerhet. Projektledare vid Statskontoret har varit Henrik Tollin (till september 1997) och Anton Granlund.

Anne-Marie Eklund Löwinder
e-post: anne-marie.eklund-lowinder@statskontoret.se

Innehållsförteckning – Del 2

1 Inledning

Denna del av handboken syftar till att informera om olika krav som ställs på IT-säkerheten i en organisation. Dessa krav består av interna krav som t.ex. användare ställer men även externa krav som lagstiftningen och andra organisationer ställer.

Vidare behandlas olika administrativa åtgärder som bör vidtas för att höja IT-säkerheten. Det kan vara framtagande av policies, ansvarsfördelning inom organisationen, risk- och sårbarhetsanalyser, utbildning m.m.

2 Grundläggande säkerhetskrav

2.1 Generella krav

De krav olika intressenter ställer varierar givetvis, men generellt gäller att ett IT-system ska

- producera information, program och tjänster som har den **riktighet** som intressenterna förväntar sig, d.v.s. är **korrekt, aktuell och begriplig**
- ha en hög **tillgänglighet**, d.v.s. vara tillgängligt för behöriga användare i beslutad omfattning på definierade tider
- kunna tillhandahålla **sekretess**, d.v.s. skydda information och program så att de inte avsiktligt eller oavsiktligt görs tillgänglig eller avslöjas för obehöriga eller utnyttjas på ett otillåtet sätt
- kunna tillhandahålla funktioner som gör det möjligt att härleda alla utförda operationer till enskilda individer/program, d.v.s. **spårbarhet.**

I det följande beskrivs närmare innebörden i de olika kravområdena liksom en del av de konsekvenser som kan uppstå om IT-systemet har sådana brister att kraven inte uppfylls.

2.1.1 Riktighet

För den som är beroende av IT-stöd i sitt arbete krävs att den information som systemet tillhandahåller är korrekt, aktuell och fullständig samt presenteras på ett sådant sätt att den direkt går att använda för det avsedda ändamålet.

Kravet på aktuell information innebär att den senast inträffade händelsen i en informationsbehandlingskedja ska finnas med. De utdata som produceras ska inte heller innehålla inaktuell eller felaktig information.

Dålig kvalitet på informationen kan exempelvis medföra att:

- felaktig information sprids internt och externt
- beslut fattas på grundval av felaktiga underlag
- personalen drabbas av extraarbete
- företag kan förlora kunder och myndigheterna kan bli föremål för negativ publicitet i massmedier.

2.1.2 Tillgänglighet

I takt med att allt mer verksamhet förs över till IT, och därmed att de flesta anställda arbetar direkt med ett eller flera IT-system, ökar också kraven på att systemen ska ha en hög tillgänglighet, d.v.s. att IT-stödet ska fungera utan störningar.

Olika verksamheter ställer givetvis skilda krav på tillgängligheten i IT-systemen. En viss funktion kanske bara behöver information ur ett system några gånger per vecka medan en annan funktion, t.ex. en frågeverksamhet, behöver ständig tillgång till systemet under arbetstid. Extra höga krav på tillgänglighet ställs inom områden där man är beroende av IT-stöd dygnet runt, t.ex. polis, bevakningsföretag, vissa industrier m.fl.

Dålig tillgänglighet kan exempelvis medföra att:

- ett visst arbete inte kan utföras i tid
- underlag för beslut kan försenas
- svar inte kan lämnas till externa intressenter som förväntar sig viss service, vilket gör att personalen tvingas ta emot klagomål
- omvärlden känner misstro mot myndighetens/företagets förmåga att sköta sin verksamhet.

En annan och ofta förbisedd aspekt när man talar om krav på ett IT-system är att det ska vara väl utformat från arbetsmässig synpunkt, dels gentemot användarna, dels gentemot den IT-personal som ansvarar för drift av systemet. Samtliga har rätt att kräva bl.a. att systemet är lätt att arbeta med och att riskerna för att göra fel är minimerade.

För användarna är det dessutom viktigt att svarstiderna inte är för långa eller alltför varierande. Inom IT-organisationen finns krav på att systemet är utformat så, att det dels är väl anpassat till den tekniska miljön, dels har en sådan teknisk utformning att driftstörningar inte inträffar på grund av allvarliga systemfel.

Om IT-systemet fungerar illa kan det medföra att:

- systemet är svårt att lära sig och därför inte används på rätt sätt
- ojämna svarstider förorsakar stress och irritation hos personalen, vilket kan bidra till att fel uppstår
- satsvisa bearbetningar genomförs på ett felaktigt sätt vilket, förutom stress och irritation för driftpersonalen, kan medföra försenade utdataleveranser och tillfälliga avbrott i IT-stödet.

2.1.3 Sekretess

Behovet att skydda information och program från att göras tillgängliga eller avslöjas för obehöriga under lagring, bearbetning och kommunikation finns hos såväl myndigheter som företag.

För myndigheternas del ställer sekretesslagstiftningen krav på att viss information skyddas. Datalagen kräver att såväl myndigheter som företag skyddar personuppgifter. Militära myndigheter, övriga totalförsvarsmyndigheter och företag som tillverkar försvarsmateriel har behov av att skydda en stor del av sina IT-system. Information som är knuten till produktutveckling, marknadsföringsplaner, planerade organisationsförändringar är andra exempel på information som kan behöva skyddas.

Om information och program inte skyddas kan det medföra att:

- enskilda personers integritet skadas
- företagshemligheter sprids till obehöriga
- uppgifter som berör rikets säkerhet kommer i orätta händer
- systemet upphör att fungera på grund av att någon oavsiktligt eller avsiktligt förstört data eller program
- någon tillskansar sig pengar genom otillåten användning av systemet.

2.1.4 Spårbarhet

Spårbarhet erbjuder skydd och återställande från förluster och brott mot säkerheten. Kravet på spårbarhet innebär att användare ska kunna hållas ansvariga för sina handlingar i IT-systemet t.ex. förändringar av systeminställningar, mottagande eller sändande av en informationsmängd eller editering i olika dokument.

Dålig spårbarhet kan innebära att:

- obehöriga aktiviteter inte kan spåras
- upphovsmannen till en transaktion, t.ex. överföring av en stor summa pengar, förnekar att han/hon har utfört handlingen.

2.2 Intressenternas krav

För de flesta organisationer gäller att det finns många intressentgrupper att ta hänsyn till när IT-säkerhetsnivån ska fastställas för enskilda informationssystem och för organisationen som helhet.

2.2.1 Olika intressenter

Intressenterna finns såväl inom som utom den egna organisationen. Det är viktigt att ingen intressentgrupp blir bortglömd när olika säkerhetskrav ska fastställas. Visserligen sammanfaller olika intressenters krav i många avseenden, men det finns också fall där man kanske måste prioritera en extern intressentgrupps krav framför de interna intressena. Bland intressenter som de flesta organisationer måste beakta kan nämnas

- ”Externa” intressenter som:
  - andra myndigheter
  - fackliga organisationer
  - leverantörer och kunder/allmänheten
  - rättsliga instanser.
- ”Interna” intressenter som:
  - myndighets-/företagsledning

– verksamhetsansvariga chefer på olika nivåer
– administrativ personal som ofta arbetar direkt mot olika IT-system men som inte har ett direkt verksamhetsansvar
– IT- och driftpersonal.

Var och en av dessa intressentgrupper kan sedan delas in i olika undergrupper med sina speciella krav.

Det finns anledning att speciellt poängtera de höga krav på säkerhet i informationshanteringen som alla medborgare har rätt att ställa på **myndigheterna.**

Enskilda personer, företag och organisationer är i hög grad beroende av den verksamhet som statliga och andra myndigheter bedriver med hjälp av IT-teknik.

Allmänna krav på rättssäkerhet och god service innebär att allmänheten har rätt att fordra att säkerheten i dessa IT-system är hög. Särskilt viktigt är detta i system där uppgifter om medborgarna själva registreras. Skyddet av enskilda individers integritet är den fråga som mest uppmärksammas i debatten om myndigheternas IT-verksamhet. Debatten rör både integritetskrav i enskilda system och, kanske framför allt, vid samkörning mellan flera system.

Förutom att integritetskraven ska tillgodoses måste långtgående krav kunna ställas på att informationen i en myndighets IT-system är korrekt, så att varken enskilda eller företag åsamkas rättsförlust eller annan skada.

Integritetsfrågorna kompliceras av de bestämmelser som finns om allmänna handlingars offentlighet.

2.2.2 Krav på riktighet

Intressenterna ställer krav på att den information och de program som de använder ska vara korrekta och riktiga. Dessa två begrepp är starkt kopplade till begreppet kvalitet. Kvalitetsbegreppet är svårdefinierat och bedömningen av vad som är god eller dålig kvalitet på information är ibland en fråga om personliga värderingar. Det som för en intressent är tillräckligt aktuellt och lättolkat

kan av en annan intressent uppfattas som mindre aktuellt och svårtolkat.

Intressenterna skulle t.ex. kunna formulera sina krav på riktighet enligt följande:

- Felaktiga uppgifter bör inte kunna registreras i systemet.
- Uppgifter ska inte kunna försvinna under bearbetning och lagring i systemet.
- Uppgifter som inte längre är aktuella ska inte finnas kvar i systemet.
- Utdata, oberoende av medium, ska presenteras på ett sådant sätt att de inte kan misstolkas.
- Utdata ska utformas så att de är anpassade till de mottagare som ska använda dem.

2.2.3 Krav på tillgänglighet

Intressenternas varierande krav på tillgång till viss information vid en viss tidpunkt styr kraven på IT-systemets tillgänglighet. Det är till en del fråga om användarnas kortsiktiga krav på att informationen ska kunna nås när den behövs för en viss arbetsuppgift, d.v.s. att användarna inte accepterar ständiga avbrott under arbetstid. I kravet på tillgänglighet ligger också att organisationens hela verksamhet på längre sikt kan äventyras om den information som bearbetas i IT-system försvinner eller av andra anledningar blir oåtkomlig under en längre tid. För en organisation som i hög grad är beroende av den information som finns i IT-systemen kan intressenternas krav vara:

- Informationssystemet ska vara tillgängligt on-line 24 timmar per dygn och antalet korta avbrott (mindre än 10 minuter) får inte överstiga två per vecka i genomsnitt.
- IT-stödet kan inte avvaras mer än högst fyra timmar.

I en organisation där den information som bearbetas i IT-systemen inte är av vital betydelse för verksamheten kan intressenternas krav vara betydligt lindrigare, t.ex. följande:

- Informationssystemet bör vara tillgängligt on-line alla arbetsdagar mellan kl 8.00 och 17.00.
- IT-stödet kan avvaras utan större olägenheter i ca tre dagar. Efter fem dagar uppstår emellertid allvarliga problem för såväl interna som externa intressenter.

Hur ett IT-system är utformat och fungerar, sett ur användarens synvinkel, har stor betydelse för den totala säkerheten i informationsbehandlingen. System som är utformade på ett sätt som gör dem svåra att använda, och som dessutom kanske fungerar dåligt, kan medföra att den information som bearbetas i systemet inte används i tillräckligt hög grad eller används på fel sätt. Exempel på krav som intressenterna ställer på systemets funktionssätt:

- Systemet ska ha korta och jämna svarstider.
- Användardialogerna ska vara utformade så att risken för att göra fel minimeras.
- Information ska kunna hämtas ur systemet vid behov och/eller vid fastställda tider.

2.2.4 Krav på sekretess

Praktiskt taget alla som är intressenter i en organisations informationshantering kan i varierande omfattning ha krav på skydd av den information som hanteras i IT-systemen. Skydd av information är inte bara en fråga om att skydda sekretessbelagd eller integritetskänslig information från att spridas till obehöriga, utan är också i hög grad en fråga om att förhindra att information förvanskas eller förstörs på annat sätt. Intressenternas krav på sekretess kan formuleras på följande sätt:

- Personuppgifter som bearbetas i systemet ska bara vara tillgängliga för de personer som behöver uppgifterna för sitt arbete.
- Uppgifter som är eller kan tänkas bli sekretessbelagda ska inte kunna göras tillgängliga för obehöriga.
- Uppgifter som bearbetas i systemet ska inte kunna förändras på ett otillåtet och okontrollerbart sätt.

2.2.5 Krav på spårbarhet

Intressenternas krav på spårbarhet varierar. Detta är naturligt eftersom spårbarhet innebär att alla operationer som genomförs i IT-systemet ska kunna härledas till en viss individ eller visst program. Detta är nödvändigt för t.ex. driftpersonal för att kunna garantera en kontinuerlig och korrekt drift. Intressenternas krav på spårbarhet kan innebära följande:

- Obehöriga användare ska kunna spåras och göras ansvariga för sina handlingar.
- Alla händelser i IT-systemet ska registreras.

3 Rättsliga krav

Lagar och förordningar påverkar i stor utsträckning myndigheternas verksamhet och därmed också de säkerhetskrav som ställs, både på enskilda informationssystem och på den totala strukturen.

I en allmän handbok som denna är det inte meningsfullt att räkna upp alla de lagar som på olika sätt påverkar kraven på säkerhet i myndigheters och företags informationssystem. Vi hänvisar därför till Statskontorets rapport ”Offentlighet och IT” som på ett uttömmande sätt behandlar området.

4 Policy och riktlinjer

4.1 Vad är en IT-säkerhetspolicy

För att skapa medvetenhet och engagemang från personalens sida i frågor som rör IT-säkerhet måste ledningen på ett tydligt sätt uttala sin syn på IT-säkerhet. Det är lämpligt att göra detta i ett dokument som anger övergripande policy med tillhörande riktlinjer eller strategi i IT-säkerhetsfrågor. Vi talar här i fortsättningen om *Policy & Riktlinjer för IT-säkerhet.*

Policydokumentet ska ge ledningens syn på behovet av IT-säkerhet. Det ska ge en klar uppfattning om vilken inriktning IT-säkerhetsarbetet ska ha. En viktig del i policyn är också att fastställa hur ansvaret för IT-säkerheten är fördelat mellan olika funktioner inom organisationen.

Policyn uttrycker företagsledningens syn på **behovet av IT-säkerhet** och anger **målen för IT-säkerhetsarbetet**.

Avvägningen hur detaljerad policyn ska vara är en betydelsefull fråga. Enligt vår uppfattning bör den inte vara alltför detaljerad, men får heller inte vara så allmänt hållen att innehållet inte går att följa upp. Policyn ska vara relativt ”stabil” och väl förankrad i den verklighet som organisationen verkar i.

Både policy och riktlinjer är tvingande för hela organisationen. Avvikelse kräver dispens av den som utfärdat policyn eller riktlinjen.

Ett exempel på hur en IT-säkerhetspolicy kan utformas finns i avsnitt 4.4.

4.2 Hur uppfyller man en IT-säkerhetspolicy

Policyn är avsedd att visa anställda och omvärlden att företaget har ett uttalat mål vad gäller IT-säkerhet. Hur dessa mål ska uppfyllas måste i de flesta fall förtydligas i **riktlinjer**, som utgör praktiska anvisningar för hur policyn ska förverkligas.

En **policy** anger **målen.**
Riktlinjer anger **hur man uppnår** målen.

4.3 Riktlinjer

Riktlinjerna anger hur målen i policyn ska nås. De är ett stöd för säkerhetsansvarig och systemansvariga att **uppnå och vidmakthålla den säkerhetsnivå ledningen/lagarna har bestämt**. Riktlinjerna är förankrade i teknik, metoder och rutiner. De måste sammanställas av personer med goda kunskaper om IT-säkerhet. Ett sätt att gå tillväga vid framtagning av riktlinjer är att till lämpliga punkter i policyn skapa avsnitt som ger svar på frågorna:

- Vad?
- Varför?
- När?
- Vem?
- Hur?

Riktlinjerna kan beröra alla områden inom IT-säkerhet. De bör vara kortfattade, konkreta, begripliga och innehålla essensen av budskapet. Vid förändringar inom IT-området, t.ex. nya hotbilder, eller i verksamheten kan riktlinjerna behöva uppdateras. Behov av att uppdatera riktlinjerna kan även vara resultat av regelbundna **uppföljningar** av IT-säkerheten.

Ett viktigt komplement till *Policy & Riktlinjer* bör sammanställas i en *Handbok om IT-säkerhet,* där bakgrunden, teorierna, och andra längre förklaringar kring IT-säkerhet kan förtydligas. I handboken ska berörda personer kunna läsa och fördjupa sig i det aktuella området.

Dessutom bör varje systemdokumentation innehålla ett särskilt avsnitt som behandlar de säkerhetskrav som är specifika för den verksamhet systemet stöder, t.ex. de krav som viss lagstiftning ställer.

4.3.1 Vilka riktlinjer behöver vi

Riktlinjer behövs på alla områden där företaget vill att verksamheten ska följa **enhetliga** anvisningar. Det kan gälla:

- hur något ska göras
- vilken nivå som ska användas och gränsvärden för denna
- vem som ska göra något
- när det ska göras.

4.4 Exempel på IT-säkerhetspolicy

En IT-säkerhetspolicy måste ha anknytning både till den eventuella IT-policy som finns och till den egentliga verksamheten. Nedanstående exempel på innehåll i en policy måste således anpassas till varje enskild organisations verksamhet.

Exemplet innehåller förslag på rubriker i en policy. Under varje rubrik formulerar man kortfattat sina mål. Här bör man alltså inte gå in på hur saker ska genomföras.

Policy för IT-säkerhet

- **IT-säkerhetspolicy för** .....

  Denna policy uttrycker ledningens syn på behovet av IT-säkerhet. Den anger omfattning och ansvarsfördelning för hur IT-säkerhetsarbetet ska bedrivas.

- **Definitioner**
- **Avgränsningar**
- **Syfte**

- **Motiv för IT-säkerhet**

  Ett fungerande IT-stöd är en förutsättning för att vår verksamhet ska kunna bedrivas effektivt. Beroendet av IT-stöd ökar också i takt med att nya system utvecklas och fler och fler befattningshavare får tillgång till befintliga system.

  Även måttliga störningar i enskilda IT-system kan få betydande negativa konsekvenser, inte bara för den verksamhet som direkt berörs, utan även för andra delar av organisationen.

  Mer omfattande störningar i IT-verksamheten kan innebära allvarliga ekonomiska och andra negativa konsekvenser, inte bara för hela vår egen verksamhet, utan även för andra samhällssektorer.

  För att minimera riskerna av att IT-verksamheten ska drabbas av allvarliga störningar måste en viss IT-säkerhetsnivå uppnås och upprätthållas.

- **IT-säkerhetsnivå**

  IT-säkerheten ska ha en nivå som står i överensstämmelse med de övergripande målen för vår verksamhet. Detta innebär att hänsyn ska tas till bl.a.:

  – de övergripande säkerhetskrav som ställs på verksamheten

  – de lagar som direkt påverkar vår verksamhet samt sådana lagar som speciellt måste beaktas i samband med IT-verksamheten, t.ex. Datalagen

  – den årliga skadekostnad som kan accepteras i enskilda IT-system och totalt för IT-verksamheten

  – olika intressenters krav på korrekt information

  – personalens berättigade krav på en god social och fysisk arbetsmiljö.

- **Organisation och Ansvar**

  – Operativt ansvar

    Ansvaret för IT-säkerheten följer verksamhetsansvaret på olika nivåer inom organisationen. Detta innebär att:

    * **ledningen** har det yttersta ansvaret för IT-säkerheten
    * **de verksamhetsansvariga** har det operativa ansvaret för att de IT-system som utgör stöd för deras verksamhet, uppfyller de krav på IT-säkerhet som verksamheten ställer.

  – Samordningsansvar
    * Det praktiska IT-säkerhetsarbetet kan, bl.a. på grund av att specialkompetens krävs, inte utföras av de funktioner som har det juridiska och administrativa ansvaret.
    * Ansvarig för samordning av IT-säkerhetsarbetet är **IT-säkerhetschefen.**
      I alla frågor som rör IT-säkerhet, rapporterar IT-säkerhetschefen direkt till ledningen/säkerhetschefen.
    * IT-säkerhetschefen ska samordna allt IT-säkerhetsarbete och ansvara för att detaljerade riktlinjer finns för hur IT säkerhetsarbetet ska bedrivas.

- **Budget**
  Kostnader för IT-säkerhetsåtgärder ska ingå som en del av den budget som finns för varje verksamhetsområde.

4.5 Exempel på riktlinjer

Riktlinjerna anger hur vi ska nå målen i vår policy. Syftet är att **uppnå och vidmakthålla den säkerhetsnivå ledningen/lagarna har bestämt**. Innehållet i riktlinjerna ger vägledning vad gäller de frågor som rör IT-säkerhet. Riktlinjerna är både av administrativ och teknisk karaktär. Riktlinjerna bör delas in i olika områden, förslagsvis utifrån de olika driftmiljöerna man har. För varje IT-miljö beskrivs hot och svagheter som identifierats, liksom lämpliga skyddsåtgärder för olika nivåer av säkerhet. Nedan följer exempel på områden där riktlinjer måste definieras för de olika IT-miljöerna:

- Organisation och ansvar
  – Säkerhetsrevision

En viktig del i IT-säkerhetsarbetet är att göra erforderliga säkerhetsrevisioner och riskbedömningar för att därigenom få underlag för att bedöma behovet av skyddsåtgärder.

Kostnaderna för olika skyddsåtgärder måste alltid ställas i relation till den skada som kan uppstå om en viss händelse inträffar och den sannolikhet som finns för denna händelse.

- Handlingsplan

  Säkerhetsrevisioner och riskbedömningar utgör underlag för den handlingsplan som IT-säkerhetschefen varje år ska upprätta. Av handlingsplanen ska framgå om andra faktorer än interna brister kräver speciella IT-säkerhetsåtgärder. Sådana faktorer kan vara verksamhetsanknuten eller annan lagstiftning samt förändringar i externa intressenters krav.

- Uppföljning och kontroll

  Uppföljning av IT-säkerhetsstatus i enskilda IT-system och tillhörande manuella rutiner är en viktig del i IT-säkerhetsarbetet. Denna uppföljning ska ske fortlöpande och inom alla delar av organisationen.

  IT-säkerhetschefen ska en gång per år lämna en skriftlig redogörelse över genomförda IT-säkerhetsåtgärder. Av redovisningen ska framgå om åtgärderna har medfört att förväntade effekter har uppnåtts.

- Riktlinjer för Informationsklassificering.
  - Riktlinjer för hur information om IT-säkerhet får spridas.
  - Information på papper/listor.
  - O.s.v.
- Riktlinjer för risk- och sårbarhetsanalyser samt IT-säkerhetsrevision.
- Riktlinjer för avbrotts- och katastrofplanering.
- Riktlinjer för drift och driftplanering.
- Riktlinjer för utbildning.
- Riktlinjer för fysiskt skydd.

- Riktlinjer för arbetsplatser.
- Riktlinjer för lokala nätverk.
- Riktlinjer för fjärrnät.
  - Riktlinjer för anslutning.
  - Riktlinjer för kommunikation.
  - Riktlinjer för distansarbetsplats.
- Riktlinjer för anslutning till Internet.
  - Riktlinjer för informationsspridning via Internet.
- Riktlinjer för systemutveckling och förvaltning.

Generella riktlinjer för vissa områden kan finnas, t.ex:

- Riktlinjer för användning av BKS.
- Riktlinjer för användning av kryptering.
- Riktlinjer för användning av aktiva kort och läsare.
- Riktlinjer för brandväggar.
- Riktlinjer för säkerhetskopiering.
- Riktlinjer för virusskydd.

5 Säkerhetsorganisation och ansvar

5.1 Ansvar och IT-säkerhetsarbete

Det är viktigt att skilja mellan generellt ansvar för IT-säkerheten och det särskilda ansvar för IT-säkerhetsfrågor som ankommer på en för detta ändamål tillskapad funktion.

Det **generella ansvaret för IT-säkerheten** är knutet till verksamhetsansvaret på alla nivåer inom organisationen. Ledningen har alltid det övergripande ansvaret.

Det **särskilda ansvaret för IT-säkerhetsarbetet** bör ligga på en rådgivande och samordnande funktion, som har den specialkompetens som krävs för att kunna omsätta verksamhetens krav på IT-säkerhet i lämpliga säkerhetsåtgärder. Det bör alltid finnas en ”IT-säkerhetschef” e.d., som representerar denna funktion.

När frågor om IT-organisation och IT-säkerhet diskuteras används också ett antal andra ansvarsbegrepp, som inte alltid är vedertagna och väldefinierade. Ett undantag är ”registeransvarig” som finns definierat i Datalagen. Innebörden av följande ansvarsbegrepp kommer i korthet att behandlas i texten:

- verksamhetsansvar
- systemägaransvar
- informationsägaransvar
- systemansvar
- egenansvar/användaransvar
- registeransvarig och offentlighetsansvarig
- IT-säkerhetsansvariga.

På grund av de stora variationer som finns i olika organisationers storlek och struktur samt i IT-verksamhetens utformning och omfattning går det inte att generellt knyta ett visst ansvar till en speciell tjänstenivå eller befattning, t.ex. avdelningschef. Av samma skäl går det inte heller att fastställa en viss ”IT-säkerhetsorganisation” som kan gälla för alla organisationer.

5.2 Verksamhetsansvar

Ledningen har alltid det övergripande ansvaret för verksamheten och de IT-system som används som stöd. Eftersom IT-säkerhet ska ingå som en naturlig del i ett IT-system ligger därmed också det **generella ansvaret** för IT-säkerheten hos ledningen.

Delegering av ansvaret för IT-säkerhet sker normalt enligt samma principer som gäller för delegering av verksamhetsansvaret inom organisationen. Under ledningen är alltså var och en, som är ansvarig för någon del av verksamheten, ansvarig också för IT-säkerheten inom sitt område. Detta generella ansvar sträcker sig i princip ner till den enskilde användaren. Se avsnittet Egenansvar/Användaransvar.

Lika litet som delegering av verksamhetsansvar befriar ledningen från det yttersta ansvaret för verksamheten, kan delegering av IT-säkerhetsansvaret befria ledningen från det övergripande ansvaret för IT-säkerheten. Ledningen måste fortlöpande orientera sig om tillståndet när det gäller IT-säkerhet och ingripa vid behov. Vissa beslut som rör IT-säkerheten bör inte delegeras till lägre beslutsnivåer utan tas på ledningsnivå. Hit hör bl.a. att:

- fastställa organisationens IT-säkerhetspolicy
- utse den som ska samordna IT-säkerhetsarbetet inom organisationen (”IT-säkerhetschef”)
- fastställa hur IT-säkerhetsarbetet i stort ska organiseras och genomföras
- fatta beslut i sådana IT-säkerhetsfrågor som berör hela organisationen
- fastställa vilka resurser som totalt ska anslås till IT-säkerhetsarbetet.

Till de uppgifter som kan delegeras till lägre nivåer hör bl.a. att:

- ansvara för att av ledningen beslutade IT-säkerhetsåtgärder genomförs inom respektive del av verksamheten
- ansvara för att den information som bearbetas i de IT-system som stöder den egna verksamheten är klassificerad med avseende på sekretess och tillgänglighet samt fastställa hur behörigheter till olika typer av information ska fördelas

- fastställa vilken skyddsnivå som ska gälla inom den egna verksamheten med hänsyn till såväl verksamhetens som lagstiftningens krav, d.v.s. säkerhetsnivån
- fortlöpande kontrollera tillståndet när det gäller IT
- ansvara för att personalen får tillräcklig utbildning och information om IT-säkerhet
- genomföra uppföljning av IT-säkerheten.

5.3 Systemägaransvar

Begreppen ”systemägare” och ”systemägaransvar” hör till dem som saknar en allmänt vedertagen definition. De används i samband med IT-säkerhet och systemförvaltning, främst för att göra verksamhetsansvariga chefer medvetna om att det övergripande formella ansvaret för de IT-system som stöder verksamheten också ingår i verksamhetsansvaret. I ansvaret ingår även yttersta ansvaret för IT-säkerhet.

Ytterst är alltså ledningen ägare till organisationens samtliga IT-system. Delegering av systemägaransvaret följer delegering av verksamhetsansvaret, men det ska betonas att systemägare bör utpekas på nivån närmast under ledningen. I systemägarens ansvar bör bl.a. ingå att fastställa resursramar för IT-stödet, liksom att besluta vilken IT-säkerhetsnivå som ska gälla.

Av det som sagts framgår att en verksamhetsansvarig chef kan ha systemägaransvar för ett antal IT-system och i denna egenskap ha ett övergripande ansvar för bl.a. säkerhetsnivån i dessa system. Det operativa ansvaret för att IT-systemen uppfyller verksamhetens krav delegeras oftast till lägre nivå, där någon ”systemansvarig” utses för varje enskilt system.

5.4 Informationsägaransvar

Formellt är informationsägaransvar och systemägaransvar samma sak. Enligt datalagen ska den som innehar ett register med personuppgifter ha någon som är **registeransvarig** (eller persondata-

ansvarig enl. nytt förslag). Ansvaret i detta fallet handlar om att sekretess och integritet ska hanteras på rätt sätt.

Hantering av information som inte omfattas av datalagens krav har alltid andra krav, lagar eller verksamhetskrav, som ska uppfyllas. Ytterst ansvarig för denna informationshantering är informationsägaren vilken vanligtvis sammanfaller med systemägaren.

I den praktiska tillvaron uppstår numera ofta situationen att samma information faktiskt hanteras i flera olika ”system”. Moderna klient/server-lösningar t.ex. arbetar ofta parallellt med en databas och sidoordnade system utväxlar regelbunden uppdateringsinformation sinsemellan. I dessa lägen kan det vara svårt att göra en tydlig koppling mellan informationsägande och systemägande. Istället bör här informationsägandet lyftas upp till en systemoberoende nivå, där man i första hand fokuserar och fastställer vem som ansvarsmässigt äger informationen, snarare än på vilket sätt detta ägande faktiskt utövas.

5.5 Systemansvar

Systemansvaret är direkt knutet till ett **visst IT-system** och innebär oftast ett verksamhetsansvar för systemet ifråga. Systemansvaret innefattar då bl.a. ansvar för att systemet fyller kraven på IT-säkerhet. Som tidigare har sagts bör dock systemägaren inte delegera alla frågor till den systemansvarige. Systemansvar ska skiljas från det systemtekniska ansvaret, som innebär ansvar för att systemet rent tekniskt fungerar väl ur tillgänglighetssynpunkt.

5.6 Egenansvar/Användaransvar

Varje användare av IT-system ska vid något tillfälle få utbildning och information vad gäller IT-säkerhet för den egna miljön. Det är sedan varje användares skyldighet att följa de säkerhetsföreskrifter som gäller, dels generella, dels de som är specifika för de egna arbetsuppgifterna. Varje användare ska också veta på vilket sätt konstaterade brister ska rapporteras.

5.7 IT-funktionens ansvar

Inom större organisationer finns i allmänhet en IT-avdelning, som dels har ansvar för drift av IT-system, dels har personal för systemutveckling och teknisk förvaltning av IT-system. I mindre organisationer med enbart lokalt placerade datorer finns kanske bara en driftansvarig för varje dator, medan utvecklingsarbete och förvaltning av befintliga system sker i omedelbar anslutning till den egentliga verksamheten.

En IT-avdelning har ansvar för att verkställa och upprätthålla IT-säkerheten inom de IT-system de är ansvariga för.

På samma sätt kan en IT-samordnare ha ansvar för att verkställa och upprätthålla IT-säkerheten inom sin avdelning eller i vissa fall för en hel organisation.

Gemensamt för båda är att säkerhetsnivån bestäms av de krav som ställs av linjefunktionerna.

5.8 Registeransvarig och offentlighetsansvarig

Enligt datalagen är den som är registeransvarig för ett personregister skyldig att se till att IT-säkerheten är tillfredsställande. Registeransvarig är normalt den myndighet, det företag eller den organisation, för vars verksamhet personregistret förs. **Det straffrättsliga ansvaret åvilar respektive organisations ledning**. Även när det gäller datalagens krav bör det följa med verksamhetsansvaret på olika nivåer att se till att erforderliga säkerhetsåtgärder vidtas.

När det gäller myndigheternas användning av IT anges i sekretesslagen att den ska ordnas med beaktande av offentlighetsprincipens krav. Vissa mer preciserade bestämmelser finns också. Det bör vid varje myndighet finnas en särskild offentlighetsanvarig tjänsteman. Denne har till uppgift att samordna de krav som offentlighets- och sekretesslagstiftningen ställer på utformningen av och säkerheten i myndighetens IT-system.

5.9 IT-säkerhetschef

Det generella IT-säkerhetsansvaret är oftast knutet till verksamhetsansvaret på olika nivåer i organisationen. Det behövs emellertid en särskild stödfunktion som svarar för samordning av IT-säkerhetsarbetet inom organisationen. Detta är nödvändigt eftersom IT-säkerhetsarbetet kräver specialkompetens som mestadels saknas inom såväl linje- som IT-avdelningarna.

Den första åtgärden för en organisation som inte påbörjat ett aktivt IT-säkerhetsarbete är att utse den person, ”IT-säkerhetschef” e.d., som ska ha huvudansvaret för samordning av IT-säkerhetsarbetet. IT-säkerhetschefen ska gentemot linjeavdelningarna ha en enbart rådgivande och inte en beslutande funktion.

IT-säkerhetsfunktionens betydelse motiverar att den är placerad direkt under organisationens ledning. I överensstämmelse med vad som har sagts tidigare om behovet av samordning mellan IT-säkerhet och övrig säkerhet är det lämpligt, i de fall det redan finns en säkerhetschef, att IT-säkerhetschefen är underställd denne.

Till IT-säkerhetschefens uppgifter hör bl.a. att:

- samordna IT-säkerhetsarbetet inom organisationen
- medverka i utarbetandet av övergripande planer, policy och riktlinjer för hur IT-säkerhetsarbetet ska bedrivas
- ge råd i IT-säkerhetsfrågor
- medverka i genomförandet av säkerhetsåtgärder
- följa utvecklingen inom IT-säkerhetsområdet för att kunna anvisa de lämpligaste metoderna och teknikerna i IT-säkerhetsarbetet
- övervaka att regler och anvisningar för IT-säkerheten följs och vid behov föreslå åtgärder
- kontrollera att befintliga säkerhetsanordningar fungerar väl och vid behov föreslå förbättringar
- medverka vid genomförande av säkerhetsanalyser.

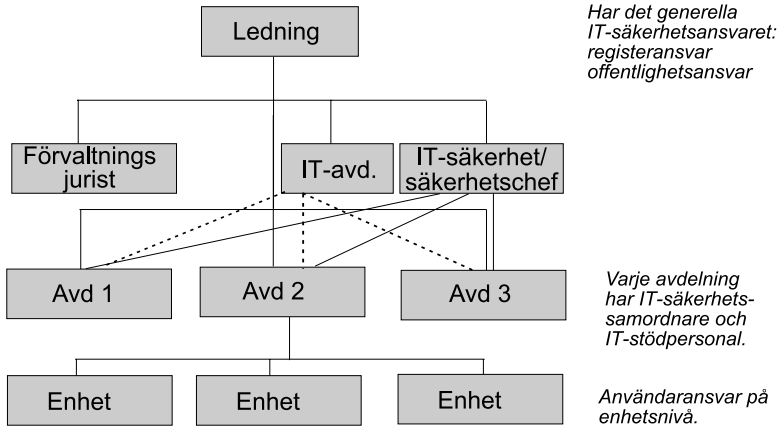
Ett exempel på en befattningsbeskrivning för IT-säkerhetschefen finns i avsnitt 5.12.

5.10 IT-säkerhetsorganisation

Som tidigare sagts är det ett minimikrav att varje organisation som utnyttjar IT-stöd i sin verksamhet utser en funktion som är särskilt ansvarig för IT-säkerhetsfrågor. Hur organisationen av IT-säkerhetsarbetet sedan ska utformas beror på många faktorer, bl.a. organisationens storlek och geografiska spridning, IT-stödets omfattning, IT-systemens komplexitet och känslighet m.m. IT-säkerhetsorganisationen kan exempelvis utformas på följande sätt. En IT-säkerhetschef har ansvaret för att samordna IT-säkerhetsarbetet inom hela organisationen. Är organisationen stor och har en omfattande IT-verksamhet kan IT-säkerhetschefen behöva medhjälpare i det centralt bedrivna IT-säkerhetsarbete som avser hela organisationen.

Inom varje linjeavdelning, liksom inom IT-avdelningen, är respektive chef ytterst ansvarig för säkerhetsfrågorna inom sin avdelning. IT-säkerhetschefen har en rådgivande roll. Till sin hjälp kan cheferna för avdelningarna ha särskilt utsedda IT-säkerhetsansvariga, som ska samordna IT-säkerhetsinsatserna inom respektive avdelning.

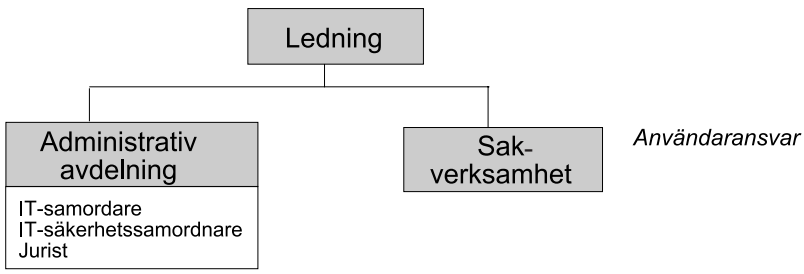
De IT-säkerhetsansvariga är underställda de verksamhetsansvariga cheferna men samverkar direkt med IT-säkerhetschefen och får anvisningar för sitt arbete från denne. Det kan gälla såväl kontroll av rådande säkerhetsnivå som genomförandet av beslutade skyddsåtgärder. De säkerhetsansvariga ska också fortlöpande rapportera iakttagelser och synpunkter angående IT-säkerhetsläget, inte bara till sin verksamhetsansvarige chef, utan också till IT-säkerhetschefen.



Figur 5. Stor säkerhetsorganisation.

Figuren illustrerar en relativt stor organisation. De heldragna linjerna mellan befattningsrutorna anger ordinarie ”ordervägar” i IT-säkerhetsfrågor. De streckade linjerna mellan rutorna anger kanaler för rådgivning och samordning. Även IT-säkerhetschefens anvisningar till den IT-säkerhetsansvarige inom en avdelning är ytterst att se som råd, t.ex. när det gäller hur en viss säkerhetsåtgärd ska genomföras inom avdelningen. Om IT-säkerhetschefen och den IT-säkerhetsansvarige är oense om hur frågan ska lösas, kan IT-säker-hetschefen inte fatta beslut i den, såvida inte ledningen uttryckligen har delegerat beslutanderätten i denna typ av frågor till denne. Vid behov får IT-säkerhetschefen vända sig till den verksamhetsansvarige avdelningschefen, som alltid har det yttersta ansvaret för IT-säkerheten inom sin avdelning.

Där det finns IT-säkerhetsansvariga spridda i organisationen kan det finnas anledning att bilda någon form av samarbetsorgan, t.ex. en IT-säkerhetskommitté, som utgör ett forum för information och erfarenhetsutbyte. IT-säkerhetschefen kan också använda kommittén för att snabbt få ut information om t.ex. nya IT-säkerhetsregler.



Figur 6. Liten säkerhetsorganisation.

I figuren åskådliggörs ett exempel på en liten IT-säkerhetsorganisation. I en mindre eller decentraliserad organisation kan IT-säkerhetschefen vara den ende företrädaren för IT-säkerhetsfunktionen. Arbetet med IT-säkerhet kanske bara upptar en mindre del av hans tid.

Oberoende av hur IT-säkerhetsarbetet är organiserat är det viktigt att det finns dokumenterat hur ansvar och befogenheter i IT-säkerhetsfrågor är fördelade inom organisationen. Förutom att detta ska beskrivas översiktligt i policydokumentet ska det i IT-säkerhetshandboken finnas en detaljerad beskrivning av hur IT-säkerhetsorganisationen är uppbyggd och fungerar.

5.10.1 IT-säkerhetsansvariga

En verksamhetsansvarig avdelningschef behöver i regel någon medhjälpare som ägnar åtminstone en del av sin tid åt att arbeta särskilt med IT-säkerhetsfrågor inom avdelningen. En sådan IT-säkerhetsansvarig får sina arbetsuppgifter och sitt ansvarsområde genom delegering från den verksamhetsansvarige chefen. På motsvarande sätt behövs någon inom en IT-avdelning som särskilt tar sig an IT-säkerhetsfrågorna inom avdelningen. Förslag till befattningsbeskrivningar för IT-säkerhetsansvariga finns i avsnitten 5.12 och 5.13.

5.11 Ansvar inom organisation som saknar egen IT-enhet

Många organisationer utnyttjar servicebyråtjänster för sin IT-verksamhet. Detta innebär inte att man kan överlåta ansvaret för IT-säkerheten till servicebyrån.

I de här fallen är det viktigt att de avtal, som upprättas mellan den organisation vars verksamhet det gäller och servicebyrån, reglerar ansvaret även för IT-säkerheten. Den organisation som har verksamhetsansvaret måste klart specificera sina krav på säkerhet i de IT-system, för vilka servicebyrån övertar driftansvaret. Om något av de krav som ställts inte kan uppfyllas fullt ut, t.ex. krav på behörighetskontrollsystem, och ett driftavtal ändå upprättas, ska det klart framgå av avtalet vilka krav som inte är uppfyllda.

Även den organisation som anlitar servicebyrå måste ha en IT-säkerhetsfunktion som i princip har samma arbetsuppgifter som IT-säkerhetsfunktionen inom en organisation med egen IT-verksamhet. Även systemägarskap och systemansvar är lika viktiga funktioner vid extern som vid egen datordrift. Skillnaden är i princip endast att det är svårare att påverka den datatekniska säkerheten om driften ligger utanför den egna organisationen.

TÄNK PÅ

- Ledningens primära uppgift är att skapa ett allmänt IT-säkerhetsmedvetande.
- Organisationens/verksamhetens arbete kring IT-säkerhet ska beskrivas i en policy med tillhörande riktlinjer.
- Riktlinjerna för IT-säkerhet ska motsvara olika krav och tekniker och behöver därför fortlöpande omprövas.
- På varje nivå inom organisationen ingår i det allmänna verksamhetsansvaret också ett allmänt ansvar för IT-säkerheten.
- En IT-säkerhetsfunktion, IT-säkerhetschef, ska finnas som svarar för den särskilda kompetens i IT-säkerhetsfrågor som behövs.
- IT-säkerhetschefen ska ha en rådgivande och samordnande funktion gentemot de verksamhetsansvariga.
- Inom olika delar av en organisation kan det finnas IT-säkerhetsansvariga som är underställda respektive verksamhetsansvarig chef, men som i IT-säkerhetsarbetet samverkar med IT-säkerhetschefen.
- I en organisation med omfattande IT-verksamhet kan den centrala IT-säkerhetsfunktionen behöva personal utöver IT-säkerhetschefen.
- Samordning av IT-säkerhetsarbetet kan underlättas genom t.ex. en IT-säkerhetskommitté, i vilken IT-säkerhetschefen och IT-säkerhetsansvariga från organisationens olika delar ingår.
- Den som anlitar servicebyrå eller annan extern organisation för sitt IT-stöd får inte överlåta ansvaret för IT-säkerheten till den utomstående.

5.12 Exempel på befattningsbeskrivning för IT-säkerhetsansvarig

Inom varje avdelning ska det finnas minst en person utsedd att vara IT-säkerhetsansvarig. Följande uppgifter kan delegeras till den eller de som är IT-säkerhetsansvariga. (För IT-säkerhetsansvarig inom IT-avdelning gäller särskild befattningsbeskrivning.)

IT-säkerhetsansvarig ska:

- ansvara för att enheten följer de regler och instruktioner för IT-säkerhet som är fastställda av ledningen
- göra erforderliga anpassningar av de generella instruktionerna så att de överensstämmer med enhetens verksamhet i övrigt
- ansvara för att all personal som berörs av IT-system informeras om de IT-säkerhetsregler som gäller för olika verksamhetsområden
- ansvara för att beslutade IT-säkerhetsåtgärder genomförs
- kontrollera efterlevnaden av IT-säkerhetsreglerna och omedelbart underrätta verksamhetsansvarig chef eller IT-säkerhetschefen om händelser som tyder på bristande IT-säkerhet i något system
- ansvara för att reglerna för behörighetstilldelning följs
- företräda enheten vid de tillfällen då IT-säkerhetschefen har anledning att sammankalla de IT-säkerhetsansvariga
- bevaka att IT-säkerhetskrav beaktas i nyutvecklingsprojekt och i förvaltningen av IT-system
- se till att systemägare och systemansvariga är medvetna om behovet av återkommande översyn av IT-systemens säkerhetsstatus
- lämna underlag till IT-säkerhetschefen för dels den årliga sammanställningen över IT-säkerhetsläget, dels planeringen av IT-säkerhetsaktiviteter för det närmaste året.

5.13 Exempel på befattningsbeskrivning för IT-säkerhetsansvarig inom IT-avdelning

Inom IT-avdelningen ska det finnas minst en person utsedd att vara IT-säkerhetsansvarig. Följande arbetsuppgifter kan delegeras till den eller de IT-säkerhetsansvariga.

IT-säkerhetsansvarig inom IT-avdelningen ska:

- ansvara för att IT-personalen följer gällande regler för IT-säkerhet
- anpassa övergripande instruktioner till IT-avdelningens arbetsområden
- ansvara för att personalen inom IT-avdelningen får den utbildning och information som krävs inom IT-säkerhetsområdet
- kontrollera efterlevnaden av IT-säkerhetsreglerna inom avdelningen och rapportera till IT-chefen, IT-säkerhetschefen eller berörd verksamhetsansvarig chef om händelser som tyder på bristande IT-säkerhet i något system
- ansvara för att hanteringen av datorutrustning inklusive alla lagringsmedier sker enligt fastställda regler
- ansvara för att utvärdering görs av de tekniska hjälpmedel som finns för att höja säkerheten i IT-verksamheten och föreslå alternativa tekniska lösningar
- kontrollera att gällande avtal finns för all teknisk service som kan bli aktuell för olika typer av datorutrustningar
- kontrollera att juridiskt godtagbara avtal finns med transportfirmor och andra datordriftställen i de fall någon form av transport eller kommunikation förekommer till eller från externa datoranläggningar
- medverka till att en fullgod uppföljning kan ske av datordriften
- ansvara för att de regler som är fastställda för säkerhet i systemutveckling och systemförvaltning följs
- följa den tekniska utvecklingen för att successivt kunna höja säkerheten i olika tekniska miljöer

- ansvara för att säkerhetsanalyser av den tekniska miljön görs med jämna intervall
- ingå i den katastroforganisation som ska träda i funktion vid en allvarlig störning i IT-driften
- lämna underlag till IT-säkerhetschefens årliga sammanställning avseende IT-säkerhetsarbetet.

6 Informationsklassificering

6.1 Informationsklassificeringens betydelse

Många brister i den nuvarande IT-verksamheten beror på att den information som bearbetas inte har klassificerats. Man har helt enkelt inte fastställt vilken **säkerhetsnivå** som är nödvändig för att olika intressenters krav ska kunna tillgodoses.

Syftet med informationsklassificering är att fastställa i **vilken omfattning informationen** behöver skyddas, d.v.s. fastställa säkerhetskraven.

Informationsklassificering ska ge **underlag** för att fastställa vilka skydd som behövs, d.v.s. **skyddsnivå.**

Informationsklassificering är en delprocess i arbetet med IT-säkerhet. Skälet till att informationen behöver skyddas kommer från olika krav:

- lagar, t.ex. datalagen, sekretesslagen
- säkerhetskrav, t.ex. föreskrifter från försvarsmakten eller myndigheter
- övriga krav, t.ex. ekonomiska krav inom företag eller medborgare som ska ha tillgång till information.

6.2 Vad ska klassificeras och av vem

Information, vars behandling kräver tillstånd från Datainspektionen (DI), ska ha en person som är *ansvarig för behandlingen (registeransvarig, Datalagen (1973:289)).* Den ansvarige har även ansvar för att informationen skyddas enligt DI:s krav, vilket innebär att även ansvaret för att genomföra informationsklassificering ligger hos personen i fråga.

Ansvaret för all annan typ av information brukar innehas av verksamhetsansvariga som då är system- eller informationsägare. Det vanligaste är att ansvaret för informationsklassificering ligger på system/informationsägaren eftersom det är av avgörande betydelse för verksamheten.

I nyutvecklingsprojekt ska informationsklassificeringen ingå som en naturlig del i projektarbetet. Det är projektledarens uppgift att se till att den genomförs på ett så tidigt stadium som möjligt för att undvika att viktiga krav på säkerhet förbises. I annat fall kan det hända att viktiga skyddsåtgärder måste införas efter det att systemet är klart. I värsta fall beaktas inte kraven på relevanta skyddsåtgärder över huvud taget och svagheter har då introducerats i systemet.

I de flesta organisationer finns klara avgränsningar mellan olika verksamhetsområden och det är viktigt att i första hand klassificera den information, som rör de mest vitala områdena samt områden där känslig information hanteras.

En generell rekommendation är att **all** information inom en organisation bör klassificeras.

6.3 Hur går det till

I följande sammanfattning beskrivs klassificeringsprocessen. Ord med **fetstil** är begrepp som används inom IT-säkerhetsområdet.

Klassificera betyder att man systematiskt indelar något i klasser. För att kunna avgöra vilken **klass (säkerhetsnivå)** informationen ska åsättas kan man genomföra en **konsekvensanalys**, vilket innebär att **konsekvenser analyseras** och **graderas** inom fyra **bedömningsområden**. Vid bedömningen används lagar, riktlinjer, ekonomiska gränsvärden och sunt förnuft. **Ansvarig** för klassificeringen är **informationsägare/ verksamhetsansvarig**.

När klassificeringen är klar ska **säkerhetsnivån** vara definierad för informationen.

Med utgångspunkt från säkerhetsnivån, hotbilder och **riskbedömning** kommer **säkerhetsåtgärder** att vidtas. Informationen kommer då att få en viss **skyddsnivå.**

Vid informationsklassificeringen ska utgångspunkten vara att olika informationsslag ska relateras till lagstiftningens, olika intressentgruppers och den berörda verksamhetens krav.

Tillvägagångssättet vid klassificering är att informationen bedöms utifrån krav inom följande fyra områden:

- **riktighet** som intressenterna förväntar sig, d.v.s. informationen ska vara **korrekt**, **aktuell** och **begriplig**
- **tillgänglighet**, d.v.s. informationen ska vara tillgänglig för behöriga användare i beslutad omfattning på definierade tider
- **sekretess**, d.v.s. information och program ska vara skyddade så att de inte avsiktligt eller oavsiktligt görs tillgängliga eller avslöjas för obehöriga eller utnyttjas på ett otillåtet sätt
- **spårbarhet**, d.v.s. funktioner som gör det möjligt att härleda utförda operationer till enskilda individer/program.

Det är informationsägarens uppgift att utse personer med lämplig kompetens för att utföra informationsklassificeringen. I många fall är det lämpligt att genomföra den här typen av aktiviteter i ett eller, i stora organisationer, flera projekt.

Ett viktigt krav när det gäller projektgruppens sammansättning är att den måste bestå av personer som är väl insatta i de verksamhetsområden som berörs.

De kunskaper som krävs är bl.a.:

- vilken lagstiftning som berör den information som ska klassificeras
- på vilket sätt olika intressenter är beroende av viss information
- vad det innebär för enskilda intressentgrupper om det inträffar händelser som stör informationsförsörjningen på ett eller annat sätt

- vad det innebär för organisationen som helhet vid olika typer av störningar
- informationens beskaffenhet
- hur man med lämplig metod genomför en informationsklassificering.

Ett exempel på klassificering finns i datainspektionens skrift ”Allmänna råd om ADB-säkerhet för personregister”. Den är avsedd att kunna användas för alla typer av personregister. Råden bör emellertid anpassas till den egna verksamheten, eftersom kravet på skydd, t.ex. när det gäller personaladministrativ information, kan vara mer eller mindre starkt, beroende på inom vilken verksamhet klassificeringen görs.

Informationsklassificering ingår som en normalrutin inom t.ex. försvarsmyndigheter och andra myndigheter, där man hanterar information som omfattas av sekretesslagstiftningen. Detaljerade regler finns för hur olika typer av handlingar ska hanteras och vanligtvis finns det motsvarande regler för hur elektronisk information ska hanteras.

6.4 Förslag till metod

Genomför informationsklassificeringen genom konsekvensanalys, d.v.s bedöm storleken på konsekvenserna om informationen blir föremål för:

- bristande riktighet
- bristande tillgänglighet
- bristande sekretess
- bristande spårbarhet.

För vart och ett av ovanstående områden graderas konsekvenserna av oönskade händelser i fyra nivåer:

1 försumbara

2 lindriga

3 allvarliga

4 mycket allvarliga

Datainspektionen har i sin klassificering av personregister, vilken enbart tar hänsyn till integritetsfrågor, valt tre olika nivåer för att bedöma erforderlig säkerhetsnivå. I de flesta fall brukar man använda sig av fyra nivåer för att beskriva hur allvarliga konsekvenserna blir vid olika typer av oönskade händelser.

Med fyra nivåer visar följande exempel hur säkerhetsnivåer kan skapas:

Konsekvens	Säkerhetsnivå exempel 1	Säkerhetsnivå Datainspektionen
Försumbara	Öppen	
Lindriga	Intern	Grundnivå
Allvarliga	Företagshemlig	Hög nivå
Mycket allvarliga	Kvalificerat företagshemlig	Mycket hög nivå

Exempel 1 överensstämmer med den gradering som används i samband med säkerhetsanalyser enligt SBA-metoden.

Beskrivningen i det följande är ett exempel på vad en informationsklassificering bör omfatta och hur den kan genomföras. Principerna för indelning av de faktorer som ska bedömas och för nivåindelning av konsekvenserna överensstämmer i stor utsträckning med vissa företagsutvecklade metoder för klassificering av information i IT-verksamhet.

6.5 Fyra steg

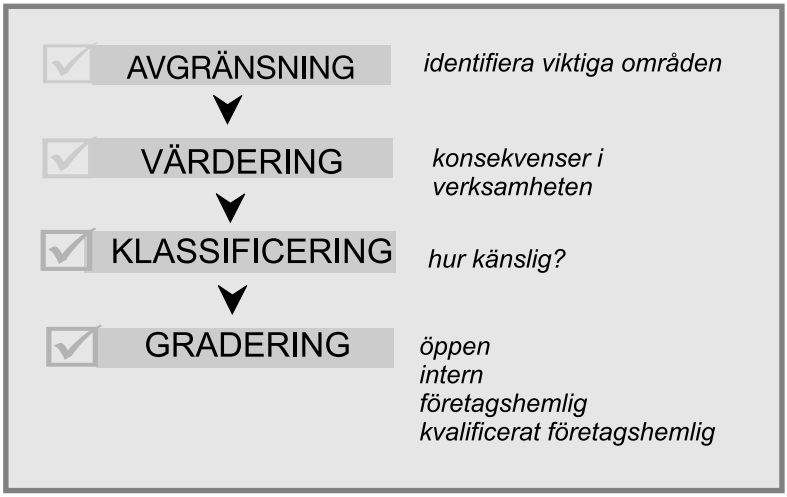
Efter det att man beslutat att genomföra en informationsklassificering och utsett den/de personer som ska ansvara för arbetet, genomförs själva klassificeringen normalt i fyra steg:

1 **Avgränsning** – Fastställande av hur omfattande klassificeringen ska vara, vilket bl.a. innefattar att avgöra vilka av de fyra bedömningsområdena riktighet, tillgänglighet, sekretess och spårbarhet som ska ingå.

2 **Konsekvenser** – Anpassning till den egna organisationen av konsekvensbeskrivningarna för de olika nivåerna inom varje bedömningsområde.

3 **Klassificering –** Genomförande av själva klassificeringen för det eller de informationsområden som ingår i bedömningen.

4 **Gradering –** Sammanställning av resultaten från klassificeringen och fastställande av önskvärd säkerhetsnivå.



Figur 7. Informationsklassificering.

6.5.1 Steg 1, Avgränsning

Fastställ vilka avgränsningar som ska göras, d.v.s. vilka olika informationsområden som ska omfattas, t.ex. personaladministrativ information och affärsinformation.

Vilka bedömningsområden som ska ingå i klassificeringen avgörs av en mängd faktorer, men generellt gäller att alla områden behandlas, särskilt i organisationer där man tidigare aldrig genomfört en informationsklassificering.

Det kan ändå finnas anledning att ibland utelämna något område, t.ex. när klassificeringen avser informationssystem där man redan har en hög säkerhetsnivå i vissa avseenden. I vissa lägen kan syftet med klassificeringen också vara att enbart fastställa vilka behov det finns av att skydda viss personrelaterad information, eller att fastställa vilken toleransnivå intressenterna har när det gäller avbrott i datordriften.

6.5.2 Steg 2, Värdering

Beskriv hur allvarliga konsekvenserna blir för olika intressenter inom vart och ett av bedömningsområden som bestämdes i steg 1. Gradera om konsekvensen är försumbar, lindrig o.s.v.

Här uppstår en svårighet, nämligen, vad ska bedömas som lindrigt, eller allvarligt. Eftersom olika organisationer har olika synsätt på vad som är en lindrig eller allvarlig skada måste det finnas klara interna anvisningar för hur sådana bedömningar ska göras.

Det är viktigt att observera att man i det här sammanhanget inte gör några sannolikhetsbedömningar avseende olika typer av händelser som kan inträffa inom ett bedömningsområde. Man utgår helt enkelt från **att något inträffar**, som medför t.ex. förlust av information. SBA-metodens scenariomodell, kan med fördel användas för att identifiera vad som kan inträffa med informationen.

Här följer exempel på hur man kan beskriva konsekvenserna inom varje nivå på den fyragradiga skalan försumbart, lindrigt, allvarligt resp. mycket allvarligt. Det görs för vart och ett av de områden som man i steg ett beslutat sig för att ha med i klassificeringen;

Bristande riktighet

För kvalitetsbegreppet brukar man ofta frångå den fyrgradiga skalan eftersom ”försumbart” anses irrelevant i sammanhanget. Det måste anses mindre rimligt att en organisation har elektroniskt lagrad information som är så beskaffad att skadan av en nedsättning av kvaliteten är försumbar.

För kvalitet kan man t.ex. använda följande beskrivning i en tregradig skala:

Lindrigt	Används för information där man ställer **normala** krav på kvalitet och när varken verksamheten eller olika intressenter störs i nämnvärd grad om det ibland finns brister i kvaliteten.
Allvarligt	Används när man ställer **höga** krav på kvalitet, d.v.s. att verksamheten störs, ekonomiska förluster kan uppstå och om enskilda intressenter kan skadas om kvalitetskraven inte uppfylls.

Mycket allvarligt Används om man ställer **mycket höga** krav på informationskvalitet, vilket innebär att kvalitetsbrister kan medföra mycket allvarliga störningar i verksamheten, allvarlig skada för många intressenter eller, i t.ex. ett företag, att en viss tillverkningsprocess störs allvarligt.

För system som, enligt datalagens definition, innehåller personuppgifter gäller att man måste ställa höga eller mycket höga krav på kvalitet. Exempelvis är den registeransvarige skyldig att omedelbart rätta felaktiga uppgifter i ett personregister.

Att dela in informationen efter krav på kvalitet förutsätter att man har definierat kvalitetsbegreppet. En vanlig definition på datakvalitet är att data ska vara:

Fullständiga Den information som produceras ska innehålla alla de uppgifter som användarna behöver för den verksamhet som systemet är avsett att stödja.

Tolkningsbara Den information som produceras ska ha en sådan form att innehållet är lätt att förstå och inte kan misstolkas.

Aktuella Informationen ska alltid vara så aktuell som användarna förväntar sig.

Korrekta Data ska så långt möjligt vara kontrollerade med avseende på ”objektiv” korrekthet.

Man kan givetvis göra kvalitetsklassificeringen mer sofistikerad genom att värdera de olika ”kvalitetsfaktorerna” var för sig. Detta kan var motiverat i vissa fall, men i allmänhet torde det inte vara nödvändigt med en sådan uppdelning.

Bristande tillgänglighet

Vid bristande tillgänglighet gäller det att få fram riktvärden för hur lång tid olika intressentgrupper kan avvara en viss typ av information. Här måste man ta hänsyn, inte bara till de interna intressenternas krav, som främst relateras till den egna verksamheten, utan

även externa intressenters krav på att få viss information inom en fastställd tidsram. Även viss lagstiftning kan påverka bedömningarna.

I första hand gäller det att beskriva innebörden i varje nivå på bedömningsskalan. Här bör man använda sig av värderingar och uttryck som är vedertagna inom organisationen. Allvarliga ekonomiska konsekvenser kan vara förlust av 500 000 kr eller 5 milj kr, beroende på organisationens storlek. Myndigheters bedömningar måste, förutom att ta hänsyn till de ekonomiska konsekvenserna, till stor del styras av de externa intressenternas intressen samt lagstiftningens krav (t.ex. att visst bidrag måste utbetalas vissa dagar). Viktigt är att samtliga konsekvenser beaktas när nivåerna beskrivs.

När det gäller avbrottssituationen är tidsaspekterna av stor betydelse, eftersom höga krav på tillgänglighet ställer speciella krav på skyddsåtgärder. I stället för att låta olika intressenter sätta egna tidsgränser för när man anser att situationen blir allvarlig eller mycket allvarlig, så brukar man fastställa en för organisationen eller visst verksamhetsområde gemensam gräns för respektive nivå.

Exempel på bristande tillgänglighet kan vara ett avbrott med varierande längd:

Försumbart	Avbrottet berör endast interna intressenter och de negativa konsekvenserna är mycket begränsade. Tidsgräns t.ex. < 1 dygn.
Lindrigt	Avbrottet berör interna intressenter och en mindre andel externa intressenter. Avbrottet förorsakar ett visst övertidsarbete när systemet kommer igång igen, men övriga negativa konsekvenser är måttliga (ca 50 000 kr). Tidsgräns t.ex. < 1 dygn.
Allvarligt	Avbrottet påverkar alla intressenter och verksamheten kommer att fungera mindre väl även några dagar efter det att informationen blir tillgänglig igen. De negativa ekonomiska konsekvenserna, utöver övertidsersättning, är relativt stora (50 000–500 000 kr). Tidsgräns t.ex. 3–7 dygn.

Mycket allvarligt Avbrottet medför omfattande störningar, inte bara för de verksamheter som är direkt beroende av informationen, utan för hela myndigheten/företaget. Vissa externa intressenter drabbas ekonomiskt och de egna ekonomiska förlusterna kan bli mycket stora (> 500 000 kr). Stora övertidsinsatser krävs och verksamheten kommer att störas även efter det att systemet fungerar igen. Tidsgräns t.ex. > 7 dygn.

Bristande sekretess

För offentlig förvaltning styrs klassificeringen av information vad avser sekretessområdet av **sekretesslagen.** För totalförsvaret finns också särskilda anvisningar för hur information som rör rikets säkerhet ska klassificeras och hanteras. Myndigheterna måste därför vid informationsklassificering i första hand beakta lagstiftning och andra fastställda regler för hur sekretessområdet ska behandlas.

För företag och andra organisationer än myndigheter är det en fråga för ledningen att ta ställning till hur olika informationsslag ska hanteras. Även om man redan har en dokumenterad indelning i olika sekretessklasser, finns det ibland anledning att komplettera reglerna när de ska användas för att fastställa säkerhetsnivån inom IT-området.

För att underlätta bedömningen kan företaget/myndigheten definiera ett belopp som skadan skulle kunna förorsaka och på så sätt kunna härleda den rätta konsekvensen. Exempel:

Försumbart Organisationen själv eller annan intressent kan inte på något sätt skadas om informationen sprids. För myndigheter gäller att vissa offentliga uppgifter återfinns här, t.ex. allmän information som beskriver myndighetens verksamhetsområde. Information som är allmän handling kan placeras på den här nivån under förutsättning att informationen inte i något sammanhang kan bli belagd med sekretess. För företag är det fråga om det man ibland kallar publika data/dokument.

Lindrigt För offentlig verksamhet kan det här vara fråga om arbetsmaterial som ännu inte blivit offentliga handlingar men kommer att bli det när arbetet är slutfört. Om det inte kan vålla någon skada att informationen sprids ”i förtid” kan den här graderingen gälla. En förutsättning är emellertid även här att informationen under inga omständigheter kan komma att beläggas med sekretess. För företag kan det vara information som är företagsintern men där skadan blir ringa om den sprids utanför företaget.

Allvarligt För alla personregister som innehåller känslig information, inte bara i datalagens mening, bedöms det normalt som allvarligt eller mycket allvarligt om informationen sprids till obehöriga. Till denna grupp hör också all information som enligt sekretesslagen är sekretessbelagd. För företag kan här återfinnas information som endast delges behörig personal och som, om den kommer i orätta händer, kan skada företaget, avtalsbunden part eller tredje man.

Mycket allvarligt Många myndigheter och företag har i sina IT-system sådan information som, om den kommer i orätta händer, mycket allvarligt skulle kunna skada såväl organisationen i dess helhet som enskilda intressenter. Här återfinns normalt sådan information som rör rikets säkerhet och som klassificerats som kvalificerat hemlig information enligt den nomenklatur som används inom offentlig förvaltning. **Finns inte fullgoda skydd installerade ska den här typen av information över huvud taget inte registreras i IT-system.**

Bristande spårbarhet

I dagens komplexa IT-system med kommunikation i öppna miljöer kan brist på spårbarhet få allvarliga konsekvenser i vissa tillämpningar, såsom e-post eller elektronisk handel.

Konsekvenser vid bristande spårbarhet är mycket beroende på vad handlingen innebär och i vilken typ av tillämpning det sker.

I exemplet är handlingen en otillåten ändring av data.

Försumbart Denna gradering innebär att den otillåtna ändringen inte skadar någon intressent eller verksamheten och inte heller kan leda till personlig vinning för den som utfört ändringen eller för någon annan. Den ändrade informationen är lätt att återställa.

Lindrigt Händelsen kan medföra en tillfällig störning i den berörda verksamheten, men det är relativt enkelt att återställa information/program till ursprungligt skick. Varken den som utför ändringen eller någon annan kan få personlig fördel av händelsen.

Allvarligt Den direkt berörda verksamheten störs allvarligt och även viss angränsande verksamhet störs i varierande omfattning. Alla otillåtna ändringar i system som hanterar ekonomiska transaktioner eller innehåller personuppgifter bör betraktas som allvarliga, även om ingen kan dra nytta av den gjorda ändringen och oavsett om det är lätt att återställa den manipulerade informationen.

Mycket allvarligt Otillåtna ändringar som kan hänföras till känsliga personuppgifter, sekretessbelagda uppgifter samt informationssystem som hanterar stora ekonomiska transaktioner måste alltid betraktas som mycket allvarliga oberoende av hur lätt eller svårt det är att återställa den ursprungliga informationen och oberoende av om någon kan dra fördel av den otillåtna ändringen.

6.5.3 Steg 3, Klassificering

Det tredje steget är att göra den egentliga klassificeringen (stämplingen) av informationen. Arbetet underlättas om man använder en matris, där man för varje informationsslag markerar graden av känslighet för en viss typ av störning.

Den första åtgärden är att besluta hur långt man ska sträcka sig när det gäller uppdelningen av informationen. Alltför stor ”hopklumpning” av informationen ger antagligen ett ofullständigt beslutsunderlag, medan en alltför långtgående finfördelning kräver så mycket arbete att klassificeringen aldrig blir klar.

För att förtydliga vad vi menar med uppdelning av information kan vi som exempel ta ett personaladministrativt system för en myndighet eller ett företag, där personalinformationen inte bara används för löneutbetalning och liknande, utan även för bemanningsplanering avseende vissa arbetsområden. Här finns flera olika intressentgrupper och många olika slag av information om varje person.

Att bedöma varje deluppgift i den här typen av system skulle bli mycket tidsödande, men samtidigt är det uppenbart att viss uppdelning bör göras med tanke på att bemanningsplaneringen kan ha behov av mycket snabb tillgång till viss information, medan lönekassan kanske inte störs nämnvärt om man är utan datorstöd någon dag.

Man bör vid uppdelningen använda den kunskap man har om olika intressenters informationsbehov och olika informationsslags känslighet och med utgångspunkt därifrån göra lämpliga informationsgrupperingar.

Vid genomgången av de informationsgrupper som man har fastställt kan man ha problem med att för ett visst bedömningsområde avgöra vilken konsekvensnivå man ska välja. Man bör då välja den ”högsta”, d.v.s. den som representerar de mest långtgående konsekvenserna. I efterhand kan man sedan göra vissa justeringar, om t.ex. nya fakta tillkommer som underlättar avgörandet.

6.5.4 Steg 4, Gradering

I steg fyra ska resultatet av klassificeringen sammanställas.

Skilj ut de informationsslag som medför ”allvarliga” eller ”mycket allvarliga” konsekvenser om händelsen inträffar.

Komplettera sammanställningen med uppgifter om vilka tillämpningar som hanterar de olika informationsslagen.

Fastställ den önskvärda **säkerhetsnivån** med utgångspunkt från sammanställningen.

I kapitel 7, Risk- och sårbarhetsanalyser, kommer vi att gå närmare in på hur man med utgångspunkt från kraven på en viss säkerhetsnivå kan fastställa erforderlig **skyddsnivå.**

7 Risk- och sårbarhetsanalyser

7.1 Vad är risk- och sårbarhetsanalyser

Riskanalys, är en analys som:

- identifierar risk och hot
- bedömer konsekvenserna för en händelse för användarna, IT-verksamheten och organisationen som helhet.

Sårbarhetsanalys, är en analys som genom en studie:

- identifierar brister eller svagheter i kontrollrutiner eller installerade skyddsåtgärder
- rekommenderar skydds- och andra åtgärder.

Beroende på hur betydelsefullt informationssystemet är kan de olika analyserna göras mer eller mindre omfattande.

I fortsättningen använder vi begreppet **risk- och sårbarhetsanalys** som ett samlingsbegrepp för dessa analyser.

Alla analyser bör emellertid ta hänsyn till en eller flera möjliga händelser med anknytning till generella krav för säkerheten:

- **Riktighet**
- **Tillgänglighet**
- **Sekretess**
- **Spårbarhet**

När man genomför en risk- och sårbarhetsanalys är det viktigt att komma ihåg att det inte enbart är en fråga om att få kunskap om själva IT-systemets och datormiljöns säkerhetsstatus. Det väsentliga är att få en uppfattning om säkerheten i hela informationsbehandlingskedjan, d.v.s. såväl manuella som maskinella delar av informationssystemet.

En risk- och sårbarhetsanalys av enskilda IT-system ska föregås av någon form av verksamhetsanalys och/eller översiktlig informationsklassificering för att man ska kunna fastställa:

- vilken verksamhet som kräver ett kontinuerligt IT-stöd, d.v.s. där även kortare avbrott i IT-driften medför allvarliga negativa konsekvenser
- vilka informationssystem som innehåller känslig eller sekretessbelagd information
- vilka verksamhetsområden som ställer speciellt höga krav på informationskvalitet.

Det är system som uppfyller något av de här kriterierna som i första hand bör bli föremål för risk- och sårbarhetsanalyser. I stora organisationer med omfattande IT-verksamhet av den här arten kan det vara nödvändigt att göra en inbördes prioritering av i vilken ordning systemen ska analyseras. Det bör då redan i det här skedet göras försök att bedöma storleken på de negativa konsekvenserna vid en eventuell händelse.

7.2 När ska risk- och sårbarhetsanalys göras

Risk- och sårbarhetsanalys bör genomföras:

- vid utvecklingen av informationssystem. Det är viktigt att genomföra analyser redan i utvecklingsfasen. Ibland kan dessa bli relativt omfattande, t.ex. om det gäller att införa en helt ny IT-struktur med decentraliserad datordrift och väsentligt utbyggd datakommunikation
- i organisationer med existerande IT-verksamhet på samtliga system, som är av stor betydelse för verksamheten, om detta inte gjorts tidigare
- vid verksamhetsförändringar. De förändringar som sker i en verksamhet kan medföra att tidigare införda säkerhetskontroller inte längre fungerar och att sårbarheten därmed ökar
- ett tag efter genomförandet av omfattande risk- och sårbarhetsanalys för att kontrollera om åtgärderna fått avsedd effekt
- vid ändrad lagstiftning
- vid nya krav från interna och externa intressenter

- när andra faktorer påverkar behovet av förnyade analyser, t.ex. övergång till en ny teknisk miljö eller förändringar i hotbilden genom att nya hot tillkommer och andra blir inaktuella.

Det är svårt att ge exakta råd om hur ofta analyser bör genomföras. Som en tumregel kan man säga att förnyade analyser bör göras minst vartannat år på de viktigaste systemen inom en organisation. Dessutom ska analys alltid göras i samband med mer omfattande systemförändringar. I organisationer där initialanalyserna visat på många brister och ett stort beroende av IT-stödet kan det vara motiverat att genomföra en ny analys redan efter ett år, under förutsättning att IT-säkerhetshöjande åtgärder vidtagits. Varje organisation måste själv fastställa med vilka intervall olika typer av system bör analyseras.

Risk- och sårbarhetsanalyser är viktig del i IT-säkerhetsarbetet men räcker inte som instrument för att kontrollera effekterna av genomförda säkerhetshöjande åtgärder. En viktig uppgift för IT-säkerhets- och verksamhetsansvariga är att fortlöpande kontrollera att IT-säkerhetsregler efterlevs och att beslutade åtgärder genomförs. Detta kan göras med en säkerhetsrevision, se kapitel 11.

7.3 Behov av kompetens

Att genomföra risk- och sårbarhetsanalyser av komplexa informationssystem förutsätter att den som ska leda analysarbetet har goda kunskaper om IT-säkerhet och metodik vid sårbarhetsanalyser samt kännedom om vilka hjälpmedel som finns för att genomföra dem. En felaktigt genomförd sårbarhetsanalys kan göra mer skada än nytta i en organisation.

7.4 Behov av metodstöd

Risk- och sårbarhetsanalyser av ett IT-system kan genomföras på olika sätt. För att underlätta genomförandet av analysen är det lämpligt att använda något slag av formaliserade hjälpmedel, t.ex. blankettmallar, som kan styra arbetsgången.

- En analys som genomförs helt utan hjälpmedel riskerar att antingen bli ytlig, d.v.s. vissa brister i systemen upptäcks inte, eller alltför detaljerad, beroende på t.ex. att den som genomför analysen bäst känner till vissa avgränsade delar av verksamheten.

- Dokumentationen av analysen kan också bli ostrukturerad och svårbegriplig, vilket medför att den som ska besluta om erforderliga säkerhetsåtgärder får ett sämre beslutsunderlag.

Det är emellertid viktigt att ha klart för sig att en översiktlig analys av verksamheten och IT-stödet kan göras med relativt enkla hjälpmedel. Det viktiga är i första skedet att komma igång med ett analysarbete och därigenom tvingas tänka igenom vilken betydelse IT-stödet har för verksamheten.

I avsnitt 7.9 finns exempel på frågor som man kan använda för att bilda sig en uppfattning om behovet av en analys. Hur man sedan går vidare beror på verksamhetens och IT-stödets art och omfattning. För en organisation, som har en relativt begränsad IT-verksamhet finns det en del förenklade men ändå formaliserade metoder som kan användas.

Det är fullt möjligt att med utgångspunkt från någon av de metoder som beskrivs i det följande konstruera egna blankettmallar som är anpassade till den egna organisationens verksamhet. Det ska ännu en gång betonas att det viktiga är att komma igång med systematiserad analys av IT-säkerheten.

7.5 Hur väljer man analysmetod

Valet av metod är av betydelse när en analys ska genomföras. Många faktorer påverkar valet, t.ex:

- **analysobjektets omfattning**, t.ex. hela organisationens IT-verksamhet, ett visst verksamhetsområde med tillhörande informationssystem, ett enstaka IT-system, en viss datormiljö

- **organisationens storlek och struktur** (centrala, regionala och lokala enheter)

- **syftet med analysen**, som dels kan vara att initialt få kunskap om säkerheten i en viss IT-verksamhet, dels kan vara att göra en kontroll av att redan beslutade och genomförda IT-säkerhetsåtgärder haft önskad effekt
- **kompetensen** inom IT-säkerhetsområdet inom den egna organisationen.

Med utgångspunkt från olika styrande faktorer gäller det att välja en analysmetod som förväntas ge en uppfattning om befintlig säkerhetsnivå och hur stor sårbarheten är i organisationens IT-stödda informationssystem. Analysen bör också resultera i konkreta förslag till säkerhetshöjande åtgärder.

I detta avsnitt nämns ett antal olika analysmetoder och verktyg som kan användas i olika situationer, en närmare beskrivning av dessa finns att hitta i avsnitt 7.6.

7.5.1 Analysobjektets omfattning

Inom en myndighet eller ett företag som aldrig tidigare genomfört risk- och sårbarhetsanalyser av IT-verksamheten kan det vara nödvändigt att dela upp analysarbetet i etapper, där man i första steget identifierar de viktigaste och mest känsliga systemen, d.v.s. de som i första hand ska genomgå en mer detaljerad analys. Detsamma kan gälla organisationer med omfattande IT-verksamhet, som är svår att överblicka även om tidigare analyser gjorts.

Vad som är viktiga och känsliga system måste avgöras inom varje enskild organisation. För myndigheter är det mestadels personregister av olika slag som kan betraktas som känsliga system, medan det för företag ofta är system som innehåller produktutvecklingsinformation och marknadsföringsplaner, liksom sådana system som olika tillverkningsprocesser är beroende av. System som hanterar beloppsmässigt stora, eller stora mängder små men svårkontrollerade penningtransaktioner är viktiga system för alla organisationer.

För att avgöra vilka system som är de känsligaste och viktigaste för organisationen kan man t.ex. använda den urvalsmetod som beskrivs i Statskontorets metodhäfte **Att utveckla en handlingsplan.**

För analys av de utvalda IT-systemen kan SBA Scenario eller SBA Scenario för offentlig verksamhet användas. Om systemen inte är alltför stora kan man också tänka sig att använda Statskontorets förenklade metod Säkerhetsanalyser med Scenarioteknik.

Risk- och sårbarhetsanalyser med inriktning enbart mot vissa driftmiljöer kan genomföras på olika sätt. Ofta ger risk- och sårbarhetsanalyser av enskilda IT-system information även om säkerhet och sårbarhet i de berörda driftmiljöerna, men det kan i många fall vara motiverat att ändå göra speciella analyser.

7.5.2 Organisationens storlek och struktur

Hur stor en organisation är samt den geografiska spridningen och beslutsstrukturen kan påverka valet av analysmetod, liksom IT-strukturen inom organisationen. I stora organisationer med såväl gemensamma centrala IT-system som lokala system är det viktigt att den eller de metoder som väljs för att genomföra erforderliga analyser ger ett jämförbart resultat. Det är då önskvärt att samma eller likartade metoder används i t.ex. alla lokala och centrala analyser för att den centrala ledningen ska få en samlad bild av säkerhet och sårbarhet i hela organisationens IT-verksamhet.

Generellt kan sägas att ju större organisationen är och ju mer omfattande IT-verksamheten är desto starkare är skälen för att använda **SBA Scenario/SBA Scenario för offentlig verksamhet** vid analys av alla system som används gemensamt inom hela organisationen. Dessa metoddelar bör användas även för lokala system i de fall dessa samverkar med ett eller flera centrala system. I de fall de lokala systemen är isolerade driftmiljöer i form av persondatornät kan de av Statskontoret framtagna varianterna på scenarioteknik användas.

7.5.3 Syftet med analysen

För många organisationer innebär en risk- och sårbarhetsanalys med hjälp av t.ex. SBA Scenario att man för första gången på ett systematiskt sätt bygger upp kunskap om säkerhet och sårbarhet inom sin IT-verksamhet.

Syftet med en riskanalys eller sårbarhetsanalys kan emellertid också vara att kontrollera att IT-säkerhetsåtgärder, som initierats genom en tidigare grundlig analys, verkligen haft avsedd effekt. Förutom att man givetvis kan genomföra en förnyad analys med t.ex. SBA Scenario kan man tänka sig ett något förenklat förfarande vid en förnyad analys. Statskontorets häfte **Säkerhetsanalyser med Scenarioteknik** är ett tänkbart alternativ till en komplett scenariostudie.

Vid kontroll av att vissa säkerhetsåtgärder haft önskad effekt kan det i vissa fall vara lämpligt att använda checklistor av olika slag. Checklistor kan vara bra att använda om det är ett begränsat område som ska kontrolleras, t.ex. en viss driftmiljö. Idag kan man använda sig av **SBA Check** för att identifiera de brister som kan uppstå i löpande verksamhet eller de brister som kan finnas i ett utvecklingsprojekt före driftsättning.

7.5.4 Kompetens

Kunskaperna inom den egna organisationen har betydelse för metodvalet, framför allt i den meningen att det krävs kunskap för att kunna välja den eller de analysmetoder som är lämpligast att använda i en viss situation.

Saknas denna grundläggande kunskap kan det ligga nära till hands att man överlåter problemet till en konsult. Metodvalet blir då helt beroende av vilken eller vilka metoder den utvalda konsulten arbetar med. Många IT-säkerhetskonsulter använder SBA-metoden som huvudsaklig analysmetod, ibland med vissa modifieringar i de olika metoddelarna. Sådana modifieringar innebär normalt inga nackdelar, utan är ofta ett tecken på att det gått att förbättra den ursprungliga metoden på vissa punkter.

Man måste emellertid här, som i andra sammanhang, kraftigt understryka vikten avatt man inte kan överlåta ansvaret för IT-säkerheten åt konsulten eller överlämna sådan kunskap och information som är olämplig att sprida utanför den egna organisationen. Det finns således all anledning att se till att åtminstone någon person inom organisationen har satt sig in tillräckligt väl i IT-säkerhetsfrågor för att dels kunna bedöma konsultens metodval, dels styra konsultens arbete samt bedöma resultat och förslag till

åtgärder. Konsultens roll ska vara att bistå med expertkunnande och att genomföra sådana arbetsmoment som den egna organisationen inte har resurser eller kompetens att själv utföra.

7.6 Analysmetoder och hjälpmedel

Utvecklingen av metodstöd på IT-säkerhetsområdet har tyvärr inte hållit jämna steg med utvecklingen inom IT-området i stort. IT-säkerhet/informationssäkerhet är också för många IT-beroende organisationer fortfarande ett eftersatt område, medan de senaste tekniska landvinningarna och systemutvecklingshjälpmedlen ofta är väl kända.

Det metodstöd som fanns att tillgå under tiden fram till början av 1980-talet var istor utsträckning inriktat mot de tekniska delarna av IT-verksamheten och i mindre utsträckning mot att analysera säkerhet och sårbarhet i ett komplext informationssystem med omfattande manuella rutiner vid sidan av det rent IT-tekniska stödet.

7.6.1 Metoder

Sedan början av 1980-talet pågår en utveckling på metodsidan inom IT-säkerhetsområdet och SBA-metoden. SBA-metoden är exempel på en svensk analysmetod som fått relativt stor spridning, sett i relation till att IT-säkerhetsmedvetandet hittills varit lågt inom såväl företag som myndigheter.

Vi ska i det följande beskriva den vidareutvecklade SBA-metoden och dessutom presentera en serie metoddelar som Statskontoret med utgångspunkt från SBA-metoden anpassat för myndigheternas räkning. Dessutom presenteras kortfattat några av de datorstödda svenskutvecklade analyshjälpmedel som finns på marknaden.

Anledningen till att vi i den här handboken valt att mer ingående presentera SBA-metoden och den av Statskontoret framtagna anpassningen för myndigheterna, är att de här metoderna på ett enkelt och tydligt sätt förklarar sårbarhetsanalysen. De möjliggör för alla med grundläggande kunskaper i IT-säkerhet och metodik att genomföra en analys.

7.6.1.1 SBA-metoden

SBA står för SårBarhetsAnalys och den ursprungliga metoden utvecklades i början av 1980-talet i samarbete mellan Riksdataförbundet (RDF) och sårbarhetsberedningen (SÅRB). I projektet deltog företrädare för offentlig förvaltning och näringsliv och metoden utformades för att kunna användas inom samtliga samhällssektorer.

Den nya SBA-metoden (SBA 2.0) består av en serie fristående metoder, tekniker och hjälpmedel för analys av sårbarheten i datoriserade verksamheter.

För varje metoddel finns ett särskilt metodhäfte med en utförlig beskrivning av arbetsgången, d.v.s. planering, genomförande och dokumentation av resultatet, samt även anvisningar om vilka personer som bör delta i analysarbetet. Till varje metoddel hör en blankett som dels utgör ett stöd för analysarbetet, dels underlättar arbetet med den efterföljande dokumentationen.

Vi ska här kortfattat beskriva några av de metoddelar som visat sig mest användbara i praktiskt IT-säkerhetsarbete.

SBA Scenario

SBA Scenario är en metod för att identifiera de risker som kan uppstå i samband med datoriserade informationssystem och för att hitta lösningar på dessa problem. Metoden bygger på att de anställda i verksamheten är de som bäst vet hur verksamheten fungerar. Metoden vänder sig framförallt till organisationer som satsar på informationssäkerhet och har en fungerande informationssäkerhetsstrategi. Den nya SBA Scenario bygger på svenska och utländska erfarenheter och kännetecknas av att:

- vara processinriktat
- ge ökat åtgärdsstöd
- skapa ett bättre ekonomiskt beslutsunderlag
- analysarbetet blir effektivare.

SBA Scenario som är avsedd att användas för analyser förutsätter att dessa genomförs av en grupp personer. Bäst resultat erhålls om

alla delar i verksamheten är representerade och deltagarna har varierande kompetens, anställningstid och verksamhetsansvar.

Följande funktioner ska vara representerade i analysgruppen:

- systemägare
- användare av systemet
- drift/utveckling
- systemförvaltning.

Om en scenariostudie på ett korrekt sätt ska analysera ett informationssystem ur total sårbarhetssynpunkt ska den innehålla 15 olika scenarier, minst 3 från var och en av följande sårbarhetsbegrepp:

- försening, avbrott, förlust av information
- obehörig användning
- bristande kvalitet
- datakommunikation.

Med scenario avses i detta sammanhang en teknik att utifrån vad som är känt, beskriva tänkbara händelser omkring ett IT-system.

Ett scenario kan beskrivas av en person eller av en grupp. I en studie enligt SBA Scenario är det i första hand meningen att beskrivningen sker inom en grupp. Det analyserade scenariot kommer att innehålla en mängd underlag för beslut eller för ett fortsatt mer detaljerat analyserande. SBA Scenario innehåller följande sex steg:

- Beskrivning i fri form av utvalda, tänkbara händelser, som ger negativa konsekvenser för den verksamhet som är beroende av det IT-system/informationssystem som ska analyseras. Det är dessa händelser och deras konsekvenser som ska detaljanalyseras.

- Beskrivning av de negativa konsekvenser som scenarierna får i och utanför de drabbade verksamheterna. Samtidigt görs ett försök till bedömning av hur sannolikt det beskrivna scenariot är.

- Beskrivning av brister eller svagheter i kontrollrutiner eller installerade skyddsåtgärder som möjliggjort scenariot och som påverkar scenariots utveckling.

- Förslag till åtgärder och beskrivning av åtgärdsförslagens effekt och påverkan på konsekvenserna.
- Val av åtgärder som kan genomföras direkt inom befintlig budget.
- Prioritering av återstående förslag till åtgärder som tagits fram.

I varje steg som genomförs dokumenteras utvalda scenarier och deras konsekvenser. Resultatet av SBA Scenario är ett underlag för att utarbeta en handlingsplan för åtgärder. Eftersom en scenariostudie endast speglar den kunskap och de erfarenheter som deltagarna i studien har, måste scenariostudien alltid kompletteras med den information och de förutsättningar som inte var kända av deltagarna innan scenariostudien.

En förutsättning för att SBA Scenario ska ge önskat resultat är att nedanstående fyra villkor är uppfyllda:

- ledningen är engagerad
- problemområdet är definierat
- rätt personer deltar i analysen
- analysdeltagarna är positiva till analysen.

I SBA Scenario används fyra blanketter samt sex konsekvensblad. En studie i full skala genomförs på två dagar.

7.6.1.2 Statskontorets metodhäften

SBA-metoden är, som tidigare nämnts, avsedd att kunna användas av såväl näringsliv som offentlig förvaltning. Eftersom den är avsedd att täcka de flesta behov av analyshjälpmedel inom IT-säkerhetsområdet uppfattas den emellertid av många som alltför omfångsrik. När det gäller den offentliga sektorn har det också visat sig önskvärt med en viss anpassning. Statskontoret har därför tagit fram ett antal metodhäften baserade på SBA Scenario.

De förändringar som gjorts hänför sig framför allt till de avsnitt som berör bedömning av konsekvenser och beräkning av skadekostnader. För offentlig förvaltning är det kanske i vissa situationer viktigare att bedöma ekonomiska och andra negativa konsekvenser för externa intressenter, t.ex. medborgarna, än att uppskatta myn-

dighetens egna förluster. Dessutom har vissa ord och uttryck förändrats för att bättre passa in i myndigheternas språkbruk.

SBA Scenario för offentlig verksamhet

Metodhäftet SBA Scenario för offentlig verksamhet är, bortsett från de ovan nämnda generella förändringarna, identiskt med SBA Scenario som beskrivits tidigare. Man använder således samma blanketter som i den ordinarie SBA-metoden och anvisningarna för genomförandet är också oförändrade. Detta är den metoddel som alla statliga myndigheter med mer omfattande IT-verksamhet och stora komplexa IT-system rekommenderas att använda vid sina sårbarhetsanalyser.

Komprimerade analyser med scenarioteknik

Som ett komplement till SBA Scenario för offentlig verksamhet har Statskontoret även tagit fram tre särskilda metodhäften för användning av scenarioteknik för mer begränsade analyser. Häftena som heter **Säkerhetsanalyser med scenarioteknik**, **Säkerhetsanalyser med scenarioteknik: PC** och **Säkerhetsanalyser med scenarioteknik: Terminal** innehåller beskrivningar över hur sådana analyser ska genomföras.

Dessa metoddelar kan sägas vara komprimerade versioner av SBA Scenario. Komprimerade så till vida att de genomförs på betydligt kortare tid, en dag i stället för två. Vidare är utrymmet för att beskriva händelseförlopp, konsekvenser och brister reducerat. Dessutom dokumenteras riskbedömningen på ett annat sätt. I stället för fyra olika blanketter används två blankettyper.

Att utveckla en handlingsplan

Statskontoret har i samma ”metodserie” tagit fram ett häfte, **Att utveckla en handlingsplan**, som bl.a. beskriver hur man kan initiera och planera IT-säkerhetsarbetet inom en myndighet. Dessutom innehåller detta metodhäfte beskrivning av en metod för att fastställa vilka IT-system som är de viktigaste och känsligaste inom en organisation och som därmed i första hand bör bli föremål för sårbarhetsanalyser.

Metoden är relativt detaljstyrd på systemnivå och är dessutom anpassad till myndigheternas organisation samt till den typ av system som finns inom statliga myndigheter. Den är främst inriktad mot att identifiera de system som innehåller personuppgifter eller sekretessbelagd information, system i vilka ekonomiska transaktioner hanteras, eller system där avbrott ger allvarliga negativa konsekvenser. Den är däremot inte utformad så, att man utgår från en översiktlig verksamhetsanalys för att välja vilka system som i första hand ska sårbarhetsanalyseras.

7.6.2 Analyshälpmedel

En av de viktigaste faktorerna i ett IT-säkerhetsarbete är genomförandet av en systematisk analys. Analysen bör vara metodbaserad för att ge det bästa möjliga resultatet. Vi har valt ett antal datoriserade och manuella analyshjälpmedel som vi har tänkt gå igenom.

7.6.2.1 SBA Nyckel

Det finns inom alla verksamheter en eller flera resurser som har större betydelse för verksamhetens funktion än övriga resurser. Förlust av sådana resurser kan orsaka stora svårigheter för verksamheten. Nyckelresurserna kan vara maskinella eller personella. Med hjälp av SBA Nyckel kan en IT-verksamhet självständigt analysera vilka nyckelfunktioner och nyckelpersoner som finns inom verksamheten. Modellen ger också möjligheten att dokumentera och redovisa olika samband, samt att kartlägga och dokumentera ansvarsförhållanden, funktionsuppdelningar samt andra viktiga problemområden. Resultatet av SBA Nyckel är ett underlag för beslut för eventuella ändringar i resurstilldelning, bemanning, val av teknologi etc. för att uppnå önskad säkerhetsnivå.

7.6.2.2 SBA Check

SBA Check är en metod för att identifiera de brister som kan uppstå i löpande verksamhet eller de brister som kan finnas i ett utvecklingsprojekt före driftsättning. Metoden har som syfte att besvara följande frågor:

- Fungerar beslutad säkerhetsnivå?

- Finns områden där säkerheten inte fungerar?
- Finns för hög säkerhet inom något område?
- Saknas kunskap om säkerheten inom något område?

Huvudsyftet med SBA Check är att värdera hur säkerheten inom organisationen fungerar. Metoden tar inte ställning till om det är rätt säkerhetsteknik som installerats utan agerar endast om vald teknik fungerar.

7.6.2.3 SBA Safer

SBA Safer är ett datoriserat verktyg för IT-säkerhetsarbete som bl.a. innehåller två moduler. Modul 1 är en tilläggsmodul för arbete med s.k. expertpaneler. Expertpanelens uppgift är att ge rekommendationer om t.ex. vilka nyckeltal och konsekvensområden som ska användas i en riskanalys, eller hur stora skadekostnaderna blir för vissa brister, eller hur mycket åtgärderna får kosta. Modul 2, även kallad ProSim som står för Profit Simulation, är en tilläggsmodul för den som har behov av att studera, analysera och värdera vilka kostnader och vinster man får vid olika bedömningar och förutsättningar i en riskanalys. Modul 2 använder förutom Monte Carlo-metoden flera vedertagna beskrivande statistiska mått och grafiska presentationer.

Med hjälp av SBA Safer kan analysledaren på ett enkelt sätt genomföra en analys. Man kan arbeta tillsammans med ansvariga och specialister ute i verksamhetens olika organisatoriska delar eller funktioner utan att dessa behöver komma till gemensamma möten.

SBA Safer sparar all information som analysen ger i databaser och detta medför bl.a. följande nya möjligheter i IT-säkerhetsarbetet:

- Information från tidigare genomförd analys kan användas som ingångsvärden vid nästa analys.
- En analys kan delas upp i tiden och delresultaten kan lagras. Detta innebär att komplexa system kan analyseras på ett effektivt sätt.
- SBA Safer stödjer förberedelsearbetet så att de mest sårbara verksamheterna enkelt kan identifieras.

- Med SBA Safer kan de ekonomiska konsekvenserna av brister i säkerheten direkt kopplas till företagets nyckeltal, vilket möjliggör för analysdeltagarna och verksamhetsledningen att se hur nyckeltalen påverkas av identifierade brister och dess konsekvenser.
- SBA Safer ger möjlighet att analysera många åtgärdsalternativ avseende såväl kostnad som effektivitet.

7.6.2.4 SBA Projekt

SBA Projekt är ett datoriserad hjälpmedel för att upptäcka tänkbara risker inom ett projekt och ge förslag på åtgärder som kan motverka de upptäckta riskerna. SBA Projekt presenterades första gången 1983. 1993 presenterades en datoriserad version av SBA Projekt. Versionen från 1994 innehåller ytterligare utvidgningar och förbättringar av metoden. SBA Projekt analyserar risker inom följande områden:

- projektets storlek
- verksamhetens förutsättningar
- teknologi
- projektorganisation
- projektens förutsättningar
- beställarpåverkan
- leverantörens uppdragsbedömning
- intern förankring
- beställarens uppdragsbedömning.

SBA Projekt kan användas av projektledare, säkerhetsansvariga, beställare, leverantörer, verksamhetsansvariga och revisorer.

7.6.2.5 Checklistor

Checklistor motsvarande dem som används i de datorstödda metoderna kan givetvis användas även utan datorstöd. Den som trots allt ändå föredrar att använda checklistor för den egentliga sårbarhetsanalysen måste i så fall själv sammanställa dessa. Man får emeller-

tid räkna med att också sammanställning och användning av egna frågor för en analys medför ett betydande arbete. Som sagts i början av det här kapitlet innebär det också risk för att analysen blir ojämn och inte tillräckligt systematisk.

I avsnitt 7.9 ges exempel på frågor, som skulle kunna användas för att få underlag att bedöma behovet av IT-säkerhetsinsatser inom en organisation.

7.6.2.6 Systemdiagnos

Systemdiagnos är en analysmetod som utvecklats inom ramen för ett av Riksdataförbundet (RDF) genomfört systemförvaltningsprojekt och är egentligen inte avsedd att användas vid sårbarhetsanalyser. Kompletterad med ett antal frågor kring personregister, IT-säkerhetsansvar och IT-säkerhetsorganisation m.m, är den emellertid ett alternativ till att enbart använda checklistor som man själv sammanställer.

7.6.2.7 Konventionell riskanalys

Inom organisationer där man har ett högt allmänt säkerhetsmedvetande är det troligt att man har metoder för riskanalys av olika delar av den egentliga verksamheten. En del sådana konventionella metoder för riskbedömning är säkert användbara även för analyser av IT-system. Även här är det fråga om att på ett systematiskt sätt bedöma sannolikheten för att oönskade händelser ska inträffa, beräkna skadekostnaden om händelsen inträffar och att slutligen fastställa om investeringar i tänkbara skyddsåtgärder är motiverade.

7.7 Genomförande av analysen

Vi har i föregående avsnitt behandlat olika metoder för att genomföra analyser. Det är synnerligen viktigt att man vid tillämpningen av de olika metoderna inte ser analysen som en isolerad företeelse utan som en beståndsdel i ett samlat och fortlöpande IT-säkerhetsarbete. Den utgör bl.a. grunden för upprättandet av den handlings-

plan för IT-säkerhet som bör finnas i varje organisation och som innehåller de aktiviteter som anses nödvändiga för att uppnå och bibehålla en viss IT-säkerhetsnivå.

7.7.1 Projektinitiering

Arbetet med att genomföra en sårbarhetsanalys, fram t.o.m. upprättandet av en handlingsplan för det fortsatta IT-säkerhetsarbetet, kan med fördel bedrivas i projektform.

Ansvaret för IT-säkerheten ligger ytterst hos ledningen och därefter följer verksamhetsansvaret på alla nivåer i en organisation. Det är således ledningen och verksamhetsansvariga chefer som ansvarar för att IT-säkerhetsarbetet initieras, och varje IT-säkerhetsprojekt måste ha ledningens stöd för att bli framgångsrikt.

Hur själva initieringen av ett projekt för sårbarhetsanalyser går till och vem som initierar projektet kan givetvis variera, men man bör följa de regler som finns för andra projekt inom organisationen.

7.7.2 Projektorganisation

Utformningen av projektorganisationen bör liksom projektinitieringen följa befintliga regler inom organisationen. Förutom den projektgrupp som ska utföra det egentliga projektarbetet behövs i de flesta projekt en styr- eller beslutsgrupp. Är projektet omfattande kan projektgruppen behöva utse särskilda arbetsgrupper för vissa delar av projektarbetet.

Medlemmarna i styrgruppen måste finnas på en sådan beslutsnivå inom organisationen att de kan fatta erforderliga beslut avseende projektgruppens arbete. I de flesta organisationer innebär detta att t.ex. administrativ chef/ekonomichef bör ingå i gruppen, liksom cheferna för berörda verksamhetsområden, d.v.s. de personer som har det övergripande ansvaret för IT-säkerheten. Dessutom bör IT-chefen eller annan person som har det IT-tekniska ansvaret inom organisationen ingå i styrgruppen.

Projektgruppens sammansättning påverkas givetvis av omfattningen på den verksamhet som berörs och uppläggningen av både

analyserna och IT-säkerhetsarbetet i övrigt. Samtidigt som det är bra att engagera så många människor som möjligt i IT-säkerhetsarbetet redan från början, får projektgruppen inte bli för stor. Viktigt är att personer som har god kännedom om olika verksamhetsområden finns med, liksom någon som har goda kunskaper om IT.

IT-säkerhetschefens/IT-säkerhetsansvarigs roll i den här typen av projekt blir helt beroende av på vilken nivå i organisationen denna funktion är placerad. Tänkbara placeringar är som ledare av projektgruppen eller, om placeringen i organisationen är på tillräckligt hög nivå, som ledare av hela projektet.

Om de fackliga organisationerna deltar i t.ex. IT-utvecklingsprojekt bör de beredas möjlighet att redan från början delta även i projekt av den här typen. Många av de säkerhetsåtgärder som brukar bli följden av genomförda sårbarhetsanalyser påverkar direkt personalens arbetssituation.

Ofta föredrar de fackliga organisationerna emellertid att stå utanför den egentliga projektorganisationen i olika IT-säkerhetsprojekt. Informationen till dem kan då i stället ske via projektledaren till exempelvis ordförande i lokal fackklubb vid bestämda tidpunkter.

7.7.3 Projektplan

Projektplanen ska klart ange vad som ska göras inom projektet. Inom stora organisationer och inom organisationer med såväl centrala som regionala och lokala enheter kan det vara nödvändigt att ha mer än ett analysprojekt. Dessa kan då fungera fristående från varandra och rapportera direkt till en styrgrupp. Det kan också finnas ett gemensamt överordnat projekt som ansvarar för samordningen.

En annan fråga som kan påverka projektplanen är om analyser ska genomföras inom projektets ram med projektdeltagarna som enda deltagare i analyserna, eller om projektets uppgift är att enbart välja ut de områden som ska analyseras. Det senare är tänkbart i större organisationer med en omfattande IT-verksamhet. I det fallet går det inte att samla kompetens för alla systemområden inom ett och samma projekt.

7.7.4 Projektarbetet

7.7.4.1 Val av analysområden och analysmetod

Oberoende av projektorganisation och avgränsningar som gjorts i projektplanen är första steget i det egentliga projektarbetet att identifiera IT-beroendet och att välja ut de verksamhetsområden/IT-system som ska analyseras.

När de system som är viktigast för verksamheten identifierats bör man kontrollera att system som innehåller något av följande informationsslag inte blivit bortglömda:

- system med personuppgifter som faller under datalagen
- system som innehåller sekretessbelagd information eller som genom bearbetning kan producera sådan
- system som hanterar stora ekonomiska transaktioner eller många ekonomiska transaktioner som är svåra att kontrollera
- system med viktiga data i övrigt.

Valet av metod för analysen av enskilda informationssystem eller andra analysobjekt kan sedan ske enligt tidigare angivna kriterier.

I de flesta organisationer kommer flera analyser att behöva genomföras. Projektgruppen måste därför göra upp en plan för i vilken ordning analyserna ska göras och få denna plan godkänd av styrgruppen.

7.7.4.2 Genomförande

De analysmetoder som har beskrivits i föregående kapitel bygger på att analyserna genomförs av en grupp personer som ska representera olika intressentgrupper inom organisationen. Fördelen med att använda dessa metoder är att man dels kan få olika intressenters syn på olika funktioner i ett system, dels har tillgång till en bred kompetens när det gäller att föreslå åtgärder för att avhjälpa de brister som upptäcks i analysen.

När det gäller SBA-metoden och Statskontorets metodhäften finns detaljerade beskrivningar i metodhäftena för hur analyserna ska genomföras samt rekommendationer som gäller deltagarna i analyserna.

Om man väljer att inte använda någon av de ”färdiga” metoder som finns, utan i stället använder t.ex. checklistor som man själv sammanställt, måste motsvarande anvisningar för hur genomförandet ska ske utarbetas och dokumenteras.

Om man har startat ett analysprojekt enligt den här beskrivna modellen är det viktigt att se till att de analyser som ska genomföras får rätt bemanning. Om projektplanen anger att projektet också ska genomföra analyserna, måste troligen projektgruppen kompletteras när analyserna ska göras. Ska analyserna genomföras utanför projektgruppen är det viktigt att denna är representerad i analysgrupperna med en eller flera personer.

7.7.4.3 Dokumentation

Varje analys som genomförs ska resultera i skriftliga förslag till åtgärder för att avhjälpa de brister som identifierats. Normalt brukar en rapport från en sårbarhetsanalys innehålla uppgift om:

- analysens omfattning, vilka brister som identifierats samt de negativa konsekvenser som kan drabba verksamheten om bristerna inte åtgärdas
- vad som bör göras för att åtgärda en viss brist
- hur åtgärden ska genomföras och av vem
- den beräknade kostnaden eller resursinsatsen och en önskvärd färdigtidpunkt.

I det här sammanhanget bör det observeras att en sårbarhetsanalys inte sällan berör sådana förhållanden att resultaten, eller en del av dem, behöver sekretessbeläggas.

De förslag som presenteras efter en analys bygger på deltagarnas kunskaper och idéer. Efter analysen är det i allmänhet nödvändigt att bearbeta dessa förslag. Detta gäller framför allt om många analyser har genomförts i en organisation. Den slutliga handlingsplanen för IT-säkerhetsarbetet måste ju bygga på fakta från samtliga analyser.

Sammanställningen av de olika förslagen görs lämpligen i en mindre grupp, där det måste finnas såväl teknisk kompetens som en övergripande kunskap om de områden som omfattas av analyserna.

De frågor som måste ställas vid genomgången av analysresultaten är bl.a. om:

- det finns något som deltagarna i analysen inte känner till om det område/det system som analyserats
- det finns andra lösningar än de gruppen/erna föreslagit för att avhjälpa identifierade brister
- det finns en annan lösning som samtidigt kan lösa andra problem
- de presenterade kalkylerna och tidsaspekterna är realistiska.

De bearbetade resultaten sammanfattas i en handlingsplan som utgör grund för det fortsatta IT-säkerhetsarbetet inom organisationen.

Av rapporten från analysprojektet bör det framgå dels vilka personer som deltagit i själva projektet, dels vilka personer som medverkat i övrigt.

7.8 Det fortsatta IT-säkerhetsarbetet

7.8.1 Handlingsplan

Till grund för allt IT-säkerhetsarbete bör, förutom en långsiktig IT-säkerhetspolicy med tillhörande långsiktig plan för IT-säkerhetsarbetet, ligga en handlingsplan som beskriver de åtgärder som ska vidtas inom den närmaste tiden. Det ska framgå av handlingsplanen vilka bedömningar som lett fram till åtgärdsförslagen. Resultaten av en genomförd sårbarhetsanalys ska arbetas in i handlingsplanen, antingen denna existerar tidigare eller nyupprättas som en följd av analysen.

Den mer kortsiktiga handlingsplanen bör innehålla uppgifter om bl.a:

- vilka system/områden som har analyserats
- de åtgärder som föreslås bli genomförda under den period som handlingsplanen omfattar samt den inbördes prioriteringen
- vilka åtgärder som återstår efter det att de tidsplanerade aktiviteterna i handlingsplanen är slutförda
- de effekter som de detaljplanerade åtgärderna förväntas ge
- hur handlingsplanen ska genomföras samt kostnaderna och/eller resursinsatsen för genomförandet.

Handlingsplanen bör inte göras alltför omfattande och de åtgärder som föreslås bör helst vara möjliga att genomföra inom en budgetperiod. Anledningen till detta är att en handlingsplan för IT-säkerhetsarbetet annars kan bli så omfattande, att det kan tyckas vara en omöjlig uppgift att över huvud taget genomföra de föreslagna åtgärderna. De som inte ryms inom detta tidsintervall kan presenteras som ingående i det långsiktiga IT-säkerhetsarbetet.

I anslutning till att den detaljerade handlingsplanen görs upp, ska sådana åtgärder som inte ryms inom planeringsintervallet, men som bedöms som viktiga för IT-säkerhetsnivån, redovisas i den långsiktiga planen. Konsekvenserna av att senarelägga vissa aktiviteter bör också redovisas. Detta gör det möjligt för beslutsfattaren att göra eventuella omprioriteringar.

7.8.1.1 Beslut och genomförande av åtgärder

Genomförande av ett analysprojekt på det sätt som här beskrivits är inledningen på ett aktivt IT-säkerhetsarbete. För att kunna genomföra de säkerhetshöjande åtgärder som krävs enligt handlingsplanen måste ledningen för myndigheten eller företaget fatta ett formellt beslut om detta.

Redan innan det formella beslutet fattas kan en förankringsprocess påbörjas i hela organisationen. Det gäller att alla berörda förstår att en god IT-säkerhet är en förutsättning för att verksamheten ska fungera tillfredsställande och att de föreslagna åtgärderna:

- bidrar till att lösa de säkerhetsproblem som finns
- kan bidra till en bättre arbetsmiljö, t.ex. färre avbrott i viktiga IT-system
- inte är avsedda att underlätta kontroll av individer.

Det formella beslutet av högsta ledningen måste i stora och decentraliserade organisationer följas av beslut även på lägre beslutsnivåer för att genomförandet ska lyckas.

Resultatet av risk- och sårbarhetsanalyser ska inte spridas till obehöriga. Däremot måste alla anställda känna till att IT-säkerhetsfrågorna är viktiga för den egna verksamheten. Under analysprojektets gång och i samband med att handlingsplanen presenteras ska därför lämplig information ges till alla berörda.

7.8.1.2 Uppföljning

Inga planer fungerar utan uppföljning och en viktig del i IT-säkerhetsarbetet är att kontrollera att de säkerhetsåtgärder som föreslagits verkligen genomförs.

I inledningen poängterades vikten av att risk- och sårbarhetsanalyser genomförs med vissa intervall för att göra det möjligt att kontrollera om t.ex. nya hot, ny teknik eller nya krav från olika intressenter medfört att befintlig säkerhetsnivå inte längre räcker till. Förnyade analyser kan i princip genomföras på samma sätt som beskrivits här, men som tidigare nämnts kan en uppföljningsanalys också genomföras t.ex. genom användande av checklistor.

Normalt leder det initialarbete som utförs i t.ex. ett analysprojekt till att en organisation får en formaliserad IT-säkerhetsorganisation som ansvarar för uppläggningen av det löpande IT-säkerhetsarbetet.

7.8.2 Exempel på handlingsplan för IT-säkerhetsarbete

Nedanstående handlingsplan är ett exempel på hur en sådan kan se ut och vilka aktiviteter den kan innehålla.

Aktiviteterna är givetvis beroende av om man tidigare arbetat aktivt med IT-säkerhetsfrågor inom organisationen och vilka brister som identifierats i de sårbarhetsanalyser som föregått upprättandet av handlingsplanen. Vi har i texten föreslagit att handlingsplanen inte bör omfatta fler aktiviteter än vad som kan genomföras under en budgetperiod. Den här handlingsplanen är, om den vore autentisk, troligen alltför omfattande för att kunna genomföras inom en sådan tidsperiod.

Vi har avsiktligt inte fyllt i vissa kolumner eftersom detta kanske skulle kunna uppfattas som någon form av rekommendation vad avser t.ex. kostnader för en viss åtgärd. Kostnader och resursåtgång styrs för många av aktiviteterna av organisationens storlek, IT-verksamhetens omfattning m.m.

Handlingsplan fr.o.m. datum X t.o.m. datum Y

Aktivitet	Kostnad	Tid	Ansvarig	Kommentarer
Styrning och samordning av IT-säkerhetsarbete				
Utse ansvarig för IT-säkerhet.		Omedelbart	Ledningen	
Utforma och fastställa IT-säkerhetspolicy.			Ledningen IT-säkansvarig	
Administrativa åtgärder				
Kartlägga beroende av nyckelperson.			Samtliga verksamhetsansvariga	
Fastställ rutiner för programändringar och godkännande av tester för system i drift.			Systemansvariga	
Inför regler för säkerhetskontroller i systemutvecklingen.			Systemansvariga IT-ansvarig	
Inför regler för överlämnande av program och system från test till produktion.			Systemansvariga IT-ansvarig	
Inför kvittensrutiner vid transport av lagringsmedier.			Driftansvarig	
Utbilda systemansvariga, användare och IT-personal i IT-säkerhet.			IT-säkansvarig	
IT-tekniska skyddsåtgärder				
Renodla test- och produktionsmiljöer.			IT- och driftansvariga	
Införa bättre avstämningskontroller i satsvisa bearbetningar.			IT-ansvarig	
Utred behovet av batteribackup för att klara korta elavbrott.			IT- och driftansvariga	
Se över utnyttjande av datorresurserna för att om möjligt förbättra svarstiderna vissa tider på dygnet.			Driftansvarig	
Byggnadstekniska skyddsåtgärder				
Installera utrustning för kontroll av inpassering till driftlokalerna.			IT-säkansvarig	
Komplettera utrustning för brandsläckning i lokaler som angränsar till datorrummet.			IT-ansvarig	
Avbrottsplanering				
Upprätta en plan för åtgärder vid ett allvarligt avbrott i driften.			IT- och driftansvariga	
Dokumentera användarnas rutiner vid långvariga avbrott.			Verksamhetsansvarig	
Behörighetskontroll				
Utred de tekniska möjligheterna att förbättra befintligt BKS.			IT-ansvarig	
Inför regler för byte av lösenord inom ramen för befintligt BKS.			Verksamhetsansvarig IT-ansvarig	
Genomför en klassificering av all information som bearbetas i IT-systemen.			Verksamhetsansvarig	

7.9 Exempel på frågor för att klarlägga behovet av risk- och sårbarhetsanalys

Risk- och sårbarhetsanalyser bör göras inom varje organisation som i nämnvärd grad är beroende av IT-stöd. Som en relativt enkel och tidig åtgärd för att öka medvetandet om behovet av analyser kan man ställa frågor av följande typ till ett antal personer med verksamhetsansvar inom olika delar av organisationen.

Har sårbarhetsanalyser genomförts tidigare på de IT-system som stöder Din verksamhet?

När gjordes analyserna?

Ledde analyserna till åtgärder för att avhjälpa bristerna?

Planeras sårbarhetsanalyser i dag?

Hur bedömer Du att situationen är för närvarande, allmänt sett, när det gäller IT-säkerhet inom Ditt verksamhetsområde?

Anser Du att det finns ett tydligt IT-säkerhetsmedvetande inom organisationen?

Finns det en IT-säkerhetschef/IT-säkerhetsansvarig utsedd med preciserade befogenheter och ansvar?

Finns det instruktioner för hur IT-säkerhetsarbetet ska bedrivas?

Vilken utbildning har personalen fått i IT-säkerhet?

Hur sker information i IT-säkerhetsfrågor?

Hur länge kan Din verksamhet fungera normalt om allt IT-stöd upphör att fungera – en timme, en dag, en vecka, två veckor eller längre?

Kan Du ange vilka de allvarligaste konsekvenserna blir om IT-stödet upphör att fungera?

Känner Du till vilka av IT-rutinerna som producerar den information som är viktigast för att verksamheten ska kunna bedrivas i normal omfattning?

Känner Du till vilken information i IT-systemen som är viktigast att skydda mot obehörig åtkomst?

Har en klassificering av informationen gjorts med avseende på dess vikt i verksamheten och behovet av skydd i integritetsfrågor?

Finns personregister av den typen att tillstånd krävs från Datainspektionen?

Uppfylls i övrigt datalagens krav när det gäller personregister?

Har Du en uppfattning om hur valet av teknisk IT-lösning påverkar sårbarheten inom organisationen (t.ex. typ av datakommunikation, stor användning av persondatorer i lokala nätverk, många tekniska samband mellan olika system)?

Frågorna kan också utformas på ett sådant sätt att de kan besvaras genom markering av ett antal givna svarsalternativ, t.ex. följande.

Har sårbarhetsanalyser genomförts tidigare på de IT-system som stöder Din verksamhet?

( ) Ja ( ) Nej ( ) Vet ej

Kan Du ange vilka de allvarligaste konsekvenserna blir om IT- stödet upphör att fungera? (Rangordna)

( ) Sämre beslutsunderlag

( ) Fördröjd handläggningstid

( ) Ökade kostnader

( ) Minskade intäkter

( ) Skada för externa intressenter

( ) Minskad goodwill

Om många personer ska besvara frågorna kan den andra varianten underlätta sammanställningen av svaren. Man bör emellertid tänka på att färdiga svarsalternativ i viss mån kan motverka en självständig analys av problemen i verksamheten.

8 Avbrotts- och katastrofplanering

8.1 Behov av avbrottsplanering

I de allra flesta IT-miljöer är det inte möjligt eller ekonomiskt försvarbart att skapa en skyddsnivå som garanterar att ett avbrott i IT-stödet inte inträffar. Enligt vår uppfattning måste alla organisationer som är beroende av ett fungerande IT-stöd ha en avbrottsplanering, som beskriver hur verksamhetens informationsbehov ska tillgodoses när IT-stödet upphör att fungera under kortare eller längre tid.

I organisationer där IT-beroendet är stort bör avbrottsplanerna innefatta även en förberedd reservdrift. Planering för reservdrift är alltså en viktig del av avbrottsplaneringen.

Det är inte i första hand storlek på eller typ av dator som avgör behovet av avbrottsplaner och eventuell reservdrift, utan vilken typ av informationssystem man är beroende av och hur allvarliga konsekvenserna blir vid ett avbrott.

Behovet av förberedda planer och reservdriftmöjligheter är helt olika för exempelvis ett system som körs periodiskt, kanske varje månad eller kvartal, jämfört med ett realtidsbaserat verksamhetsstöd eller övervaknings-/styrsystem inom sjukvården resp. kärnkraftsindustrin.

Begreppet avbrottsplanering täcker, som vi använder det här, ett något större område än den traditionella katastrofplaneringen. Den senare sammankopplas i huvudsak med stordatormiljöer, där man från början fastställt att någon form av reservdrift är nödvändig, om man drabbas av ett avbrott som får katastrofala eller mycket allvarliga konsekvenser för verksamheten. Idag kan vi få lika allvarliga konsekvenser om delar av ett nätverk eller en server slås ut.

Avbrottsplanering är emellertid inte enbart knuten till rena katastrofsituationer eller till stora komplexa IT-miljöer. De flesta datorer är mycket driftsäkra och det stora flertalet avbrott beror på felaktigheter i nät, programvaror eller på dåligt fungerande driftrutiner. (Den avbrottsplanering vi talar om här innefattar inte planering för hur IT-stöd ska ersättas under kris- och krigsförhållanden.)

Några exempel på anledningar till att det uppstår avbrott i IT-stödet är att:

- den centrala utrustningen, t.ex. centralenhet, skivminnen, server, kommunikationsdatorer, upphör att fungera
- störningar inträffar i telekommunikationer
- skador uppstår i lokala nätverk, PC, hubbar, switchar, routrar m.m.
- operativsystemet inte fungerar
- tillämpningsprogrammen inte fungerar
- lagrade data (register och databaser) har förstörts
- reservkopior inte går att använda/saknas
- säkerhetskopior saknas av data lagrad i PC
- viss känslig personalkategori (t.ex. driftpersonal, registreringspersonal) tas ut i strejk eller av annan anledning inte finns tillgänglig.

En avbrottsplan ska täcka alla de fall där avbrottet förorsakar så allvarliga störningar i verksamheten, att särskilda åtgärder blir nödvändiga att vidta, för att verksamheten efter avbrottet ska kunna återupptas under ordnade former och inom rimlig tid. Anledningen till avbrottet är i det här fallet av underordnad betydelse.

Ett övervägt beslut att inte ha någon dokumenterad avbrottsplan, baserat på en realistisk riskbedömning, är också en typ av avbrottsplanering och är i vissa situationer, om än ovanliga, den rätta säkerhetsnivån. Även för ett PC-baserat enanvändarsystem måste man veta under hur lång tid man kan undvara datorstödet, och med ledning av denna vetskap planera för hur arbetet ska fungera om persondatorn t.ex. blir stulen.

Avbrottsplanen får inte betraktas som en ersättning för andra säkerhetsåtgärder. Den är en viktig beståndsdel i den totala säkerheten, men för att den ska fylla sin funktion krävs att även andra säkerhetsåtgärder har vidtagits. I del 3, kapitel 4, beskrivs olika typer av skyddsåtgärder.

De enskilda åtgärderna inom vart och ett av de här områdena kan vara:

- förebyggande eller preventiva skydd, som förhindrar att en viss händelse inträffar
- begränsande eller korrektivt skydd, som begränsar skadeverkningarna av en inträffad händelse
- rapporterande skydd, som innebär att en händelse inte förblir oupptäckt.

En upprättad avbrottsplan är en administrativ skyddsåtgärd som utgör ett huvudsakligen korrektivt skydd, d.v.s. den är avsedd att begränsa skadeverkningarna efter avbrott.

Liksom allt annat IT-säkerhetsarbete syftar avbrottsplaneringen till att uppnå en lämplig säkerhetsnivå som är anpassad till intressenternas och verksamhetens krav. Det är nödvändigt att ta vissa risker, men det är mycket viktigt att veta vilka risker man tar och vilka konsekvenserna blir, om IT-stödet upphör att fungera under en kortare eller längre tid.

8.2 Vem ansvarar för avbrottsplaneringen?

Som det har framhållits i del 2, kapitel 5, är det ledningen som har det övergripande ansvaret för organisationens IT-säkerhet. Inom organisationen är sedan ansvaret normalt delegerat till verksamhetsansvariga på olika nivåer. När det gäller enskilda IT-system är det den systemansvarige som ansvarar för att rätt IT-säkerhetsnivå uppnås och upprätthålls.

För att samordna IT-säkerhetsarbetet har många myndigheter och företag utsett en IT-säkerhetschef/IT-säkerhetsansvarig. Denna funktion har inget direkt ansvar för säkerheten i enskilda informationssystem, men ska bistå ledningen och systemägarna med den specialkompetens som krävs för ett framgångsrikt IT-säkerhetsarbete.

Verksamhetsansvariga och systemansvariga har ansvaret för att den egna verksamheten fungerar även vid olika typer av avbrott i IT-stödet.

I dagens alltmer integrerade bearbetningsmiljöer räcker det emellertid inte att enbart se på säkerheten inom varje verksamhetsområde eller system för sig. Det blir allt vanligare med informationsutbyte mellan olika datorsystem, såväl interna som externa, och detta påverkar givetvis avbrottsplaneringen. Även i stordatormiljöer där många applikationssystem delar på datorresurserna, utan att något egentligt informationsutbyte sker mellan systemen, påverkas avbrottsplaneringen av många olika systemansvarigas krav.

Avbrottsplaneringen måste således samordnas inom en organisation. I de flesta organisationer är det lämpligt att IT-säkerhetschefen får ansvaret för att en samordnad avbrottsplanering genomförs. Hur omfattande samordningsinsatserna behöver vara beror givetvis på omfattningen och arten av IT-stödet.

Vi ska i det följande redovisa vad som bör ingå i en avbrottsplanering och vad som påverkar behovet av reservdrift. Vi redogör också för ett antal olika reservdriftalternativ.

8.3 Underlag för avbrottsplanen

Ett viktigt inslag i avbrottsplaneringen är att få fastställt vad som är den ”längsta acceptabla avbrottslängden”, d.v.s. efter vilken tid ett avbrott medför helt oacceptabla konsekvenser (en katastrofsituation). Denna tidsgräns är av avgörande betydelse för om ett reservdriftalternativ ska ingå i avbrottsplanen.

Underlag för att fastställa denna tidsgräns kan erhållas på olika sätt. Ett sätt är att genom informationsklassificering skapa underlag för att bedöma intressenternas och verksamhetens känslighet för avbrott i IT-stödet. I samband med en sårbarhetsanalys kan man få motsvarande underlag.

En metod för informationsklassificering finns beskriven i del 2, kapitel 6. När det gäller genomförande av sårbarhetsanalys är SBA Scenario eller SBA Safer effektiva metoder.

Oberoende av vilken metod som används måste man för avbrottsplaneringen ha kännedom om storleken av konsekvenserna för olika intressenter vid avbrott av olika längd.

Underlaget bör helst omfatta bedömningar för fyra olika avbrottslängder, t.ex:

- korta avbrott, uteblivet datorstöd upp till ett par timmar
- medellångt avbrott, upp till en arbetsdag
- långt avbrott, upp till en vecka
- mycket långt avbrott, över en vecka.

Vilka tidsgränser som sätts för de olika typerna av avbrott bör bestämmas med hänsyn till de verksamhetsområden/informationsområden som ingår i bedömningen. Tidsgränserna kan således variera mellan olika organisationer, men även inom en och samma organisation. Vid bedömningen av de negativa konsekvenserna av olika långa avbrott kan man använda den i samband med säkerhetsanalyser vedertagna fyragradiga skalan:

- försumbar
- lindrig
- allvarlig
- mycket allvarlig (katastrofal).

När man ska bedöma de konsekvenser som kan bli följden vid olika avbrottssituationer är det viktigt att ta hänsyn, inte bara till hur den egna verksamheten och interna intressenter drabbas, utan även till följderna för externa intressenter. För vissa myndigheter, t.ex. de som ansvarar för utbetalningar av olika typer av bidrag, kan ett avbrott vid en tidpunkt då utbetalningar ska ske innebära försumbara konsekvenser för myndigheten. För mottagarna av bidragen kan några dagars försening emellertid vara allvarligt.

Behovet av avbrottsplaner styrs inte enbart av hur allvarliga konsekvenserna blir om ett avbrott inträffar, utan också av hur stor sannolikheten är för att ett avbrott ska inträffa. Detta styrs av vilka tänkbara hot som finns och vilken typ av skydd man redan har.

Olika hot riktar sig mot olika delar av det totala informationssystemet och de händelser som kan inträffa förorsakar olika typer av avbrott. Det finns ”en trolig längd” för olika typer av avbrott, d.v.s. att man erfarenhetsmässigt vet ungefär hur långt ett avbrott kommer att bli, beroende på vad som förorsakat avbrottet.

Genom att väga samman konsekvensernas storlek och sannolikheten för att en viss typ av avbrott ska uppstå får man en riskfaktor för avbrott. Det är bl.a. denna riskfaktor som styr hur omfattande avbrottsplaneringen behöver vara och huruvida ett reservdrift-alternativ måste finnas. I vissa system, t.ex. inom kärnkraftsindustrin och försvaret, kan konsekvenserna av ett avbrott vara så allvarliga att en detaljerad avbrottsplan måste finnas även om sannolikheten för att ett avbrott ska inträffa är mycket liten.

8.4 Vad innehåller en avbrottsplan

Det är omöjligt att i den här typen av handbok i detalj beskriva hur en avbrottsplan ska se ut för varje typ av tänkbar datormiljö och systemstruktur. Av den anledningen gör vi inte heller någon speciell uppdelning med avseende på datormiljöer utan beskriver vad som generellt bör ingå i en avbrottsplan.

> En avbrottsplan ska beskriva de förberedda åtgärder som ska vidtas när ett avbrott i IT-stödet inträffar. Planeringen ska täcka olika situationer, från kortare avbrott, med för verksamheten lindriga konsekvenser, till rena katastrofsituationer.

Avbrottsplanen omfattar och beskriver åtgärder som:

- minskar skadeverkningarna vid ett oförutsett avbrott i datorstödet
- vid behov, ersätter det IT-stöd som intressenterna och verksamheten är beroende av, där hänsyn tas till den förmodade avbrottstiden.
- syftar till att lämna information om avbrottet till berörda, såväl inom som, i förekommande fall, utanför den egna organisationen.

Man brukar dela in en avbrottsplan i tre olika delar, nämligen beskrivningar av:

- den organisation som ansvarar för de åtgärder som krävs för att hantera den uppkomna situationen (katastroforganisation)
- användarnas reservrutiner
- IT-enhetens reservrutiner.

Hur omfattande planen blir beror bl.a. på IT-stödets omfattning, typ av datorer samt verksamhetens känslighet för avbrott i IT-stödet och behovet av reservdrift. Givetvis blir avbrottsplanen för en ensam persondator eller en relativt enkel datorinstallation betydligt mindre omfattande än den för en stordator/servermiljö med många systemansvariga och en komplex systemstruktur.

I det följande beskrivs vilka olika punkter som bör ingå i respektive avsnitt i avbrottsplanen. I vårt exempel förutsätts att ett reservdriftalternativ ingår. Vilka överväganden som bör ligga bakom ett beslut om reservdrift behandlas i nästa kapitel.

8.4.1 Organisationen

Vid alla typer av avbrott, även korta avbrott med för verksamheten försumbara konsekvenser, krävs beslut av olika slag.

Vid avbrott med lindriga konsekvenser klaras de flesta problem inom den ordinarie drift- och förvaltningsorganisationen, under förutsättning att samråds- och informationsvägarna mellan IT-ansvariga, systemansvariga och användare fungerar enligt en fastställd och dokumenterad instruktion. Denna organisation ska finnas beskriven i avbrottsplanen med angivande av vilka personer som ingår och vilka funktioner de representerar.

I besvärliga avbrottssituationer, särskilt sådana där avbrottet kan väntas bli långvarigt och det kan bli aktuellt med reservdrift, krävs emellertid vanligen beslut, ofta av ekonomisk art, på en nivå som ligger över den normala drift- och förvaltningsorganisationen.

Det bör finnas en särskild, i förväg fastställd, organisation som kan leda och samordna insatserna när ett avbrott har den karaktären att den ordinarie drift- och förvaltningsorganisationen inte har tillräckliga befogenheter eller möjligheter att fatta alla erforderliga beslut. Beroende på de inträffade eller väntade konsekvenserna av ett avbrott träder hela eller delar av denna beslutsorganisation, som vi här kallar ledningsgrupp, i funktion.

Vid allvarliga avbrott är det ofta snabba, extraordinära beslut som måste fattas. Det är därför nödvändigt att det i planerna finns reglerat vilka befogenheter och vilket ansvar en sådan ledningsgrupp har.

I ledningsgruppen bör det ingå företrädare för de viktigaste verksamhetsområdena (de ”stora” systemägarna) inklusive IT-ledning och IT-säkerhetschef/motsvarande. Gruppen bör ledas av en person som har en inom hela organisationen ledande befattning.

Gruppen bör inte vara alltför stor. Helst bör den inte bestå av fler än sex personer. Det är emellertid viktigt att det finns ställföreträdare utsedda för de viktigaste funktionerna inom gruppen.

I större organisationer med omfattande IT-stöd kan det vara nödvändigt att ha ett antal undergrupper som ansvarar för att handlägga olika delproblem i samband med en akut avbrottssituation. Alla undergrupper ska, liksom ledningsgruppen, vara tillsatta i förväg för att snabbt kunna träda i funktion.

Ledningsgruppen har ansvaret för att avbrottsplanerna fungerar i alla situationer. Till ledningsgruppens ansvarsområde hör att:

- så snabbt som möjligt underrätta verksamhetens ledning om det inträffade
- besluta vilken information som ska ges till interna och externa intressenter
- när tillräcklig information om det inträffade föreligger, besluta om vilka reservrutiner som behöver aktiveras, t.ex. överflyttning av drift till reservanläggning
- samordna eventuella undergruppers insatser
- besluta om när återgång till normalrutin ska ske
- ombesörja att eventuella brister i reservrutiner och avbrottsorganisation åtgärdas.

Avbrottsplanen bör innehålla en noggrann dokumentation över ledningsorganisationen, med uppgifter om vilka personer som ingår och hur de kan nås, även utanför arbetstid. Dessa och andra uppgifter i avbrottsplanen bör bara spridas till de personer/funktioner i organisationen som kan tänkas behöva dem.

Av avbrottsplanen bör också framgå vilka befogenheter ledningsgruppen har att fatta beslut, i t.ex. ekonomiska frågor, utöver de befogenheter enskilda medlemmar har i den ordinarie organisationen.

8.4.2 Användarnas avbrottsplan

Med användarnas avbrottsplan eller reservrutiner menas här en beskrivning av de förberedda åtgärder som användarna av ett IT-system ska vidta vid olika typer av avbrott.

Reservrutinerna ska vara utformade så att de är användbara vid olika typer av avbrott, såväl vad gäller den troliga avbrottstiden, som var i behandlingskedjan de inträffar.

I användarnas reservrutiner bör ingå:

- instruktioner för hur, av vem och i vilken omfattning information om det inträffade ska och får lämnas till interna och externa intressenter av enskilda befattningshavare
- en förteckning (larmlista) över berörda funktioner/intressenter samt telefonnummer till dessa
- en aktuell prioriteringslista för de fall då flera system bearbetas i samma dator och endast en begränsad datorproduktion är möjlig
- en beskrivning av hur olika arbetsuppgifter på användarsidan ska organiseras och prioriteras
- en beskrivning av vilka reservrutiner, manuella och maskinella, som är aktuella vid olika typer av avbrott
- instruktioner för hur start av aktuella reservrutiner ska ske
- en detaljerad beskrivning av reservrutinerna, såväl de maskinella som de manuella
- en beskrivning av reservrutinernas svaga och kritiska punkter
- en beskrivning av beroendeförhållanden till andra interna och externa system
- en tydlig beskrivning av vilka rutiner och funktioner som inte täcks av reservrutiner och de negativa konsekvenser som detta förhållande kan medföra

- en beskrivning över hur man startar de ordinarie rutinerna efter det att avbrottet avhjälpts
- regler för hur och i vilken ordning man ska ”köra ikapp” de rutiner som har legat nere under avbrottet.

Förutom ovanstående rent operativa beskrivningar bör det, för att reservrutinerna ska vara användbara, även vara fastlagt:

- vem som är ansvarig för att avbrottsplanen hålls aktuell
- vilka aktualitetskrav som ska gälla för avbrottsplanerna
- vem som ansvarar för användarnas utbildning i avbrottsplanernas rutiner
- på vilket sätt och hur ofta de i avbrottsplanen beskrivna reservrutinerna ska övas
- vem som beslutar om övning och till vem resultatet av genomförd övning ska rapporteras
- vem som analyserar resultatet av övningar och föreslår eventuella förändringar i de befintliga planerna.

8.4.3 IT-enhetens avbrottsplan

För att det över huvud taget ska vara meningsfullt att ha en avbrottsplanering, där ett reservdriftalternativ kan vara en tänkbar del, måste vissa grundläggande säkerhetsåtgärder vara införda i den aktuella driftmiljön.

Enkelt uttryckt bör man se till att det är ”ordning och reda” i hela drift- och förvaltningsorganisationen och att alla de preventiva skyddsåtgärder som är ekonomiskt motiverade i den aktuella driftmiljön är vidtagna. Till dessa skyddsåtgärder hör bl.a. att man har säkra och väl fungerande rutiner för reservkopiering, vilket även inbegriper en säker förvaring av reservkopior.

IT-enhetens avbrottsplaner kan vara av varierande omfattning, beroende på framför allt hur stor själva datoranläggningen är. Dessutom påverkas givetvis planernas utformning och omfattning av om ett reservdriftalternativ finns och av vilken typ detta alternativ är.

IT-samordnare med ansvar för servrar och persondatorer har motsvarande funktion.

De flesta punkterna i uppräkningen nedan bör ingå även i de mindre datormiljöernas avbrottsplan, eftersom det eller de system som körs på en fristående PC, i ett lokalt nät mot en server, kan vara av minst lika stor betydelse för en verksamhet som ett stordatorbaserat system.

Oavsett storleken på dator bör det i IT-enhetens (eller motsvarande funktions) avbrottsplan ingå:

- en noggrann beskrivning av den tekniska bearbetningsmiljön, d.v.s. av hela datorinstallationen med alla tillhörande installationer för klimat, kommunikation m.m.
- en förteckning över vilka serviceavtal, reservutrustningar och återanskaffningstider som finns
- en heltäckande beskrivning av all system- och hjälpprogramvara som används, liksom av de tillämpningssystem som bearbetas i den aktuella datorinstallationen
- uppgifter om vilka alternativa reservdriftplaner som finns och hur de ska initieras
- en beskrivning över vilken kapacitet som krävs för att upprätthålla drift vid olika ambitionsnivåer
- en detaljerad och med samtliga systemägare överenskommen prioritering mellan olika system, både vad avser maskinresurser och kommunikation
- en detaljerad prioritering inom olika delar av enskilda tillämpningssystem, bl.a. med avseende på olika användarkategoriers behov av tillgång till kommunikation med datorsystemet
- uppgifter om de olika tillämpningssystemens krav i form av:
  - oacceptabla avbrottstider
  - kapacitetsbehov för såväl program som lagring av data
  - leveranstidpunkter
  - beroenden av andra interna och externa system
  - kritiska körningar

  - kritiska tidpunkter
  - återstartspunkter.
- instruktioner för driftpersonal avseende:
  - nödåtgärder, d.v.s. de omedelbara åtgärder som ska vidtas vid olika typer av störningar såsom allvarligt maskinhaveri, brand, översvämning, bombhot
  - åtgärder vid övergång till reservdrift
  - särskilda rutiner under reservdrift
  - åtgärder vid återgång till normaldrift.

Beskrivningen över vilka åtgärder som ska vidtas initialt, då en allvarlig störning inträffar, är en del av avbrottsplanen som även kan betraktas som en preventiv skyddsåtgärd. Ett riktigt agerande i initialskedet kan nämligen förhindra att en från början enbart allvarlig händelse utvecklas till en katastrof.

Åtgärdsinstruktioner

De detaljerade instruktionerna för åtgärder vid olika typer av allvarliga händelser ska vara väl kända av all berörd personal och ska omfatta uppgifter om:

- vilka åtgärder som får vidtas innan ledningsgruppen har tagit över ansvaret
- vilka som ska larmas samt på vilket sätt larmning ska ske
- vem som har rätt eller skyldighet att fatta beslut om larm
- vem som har ansvaret tills den förberedda ledningsgruppen har hunnit samlas och övertagit ansvaret.

De beskrivningar som avser reservdrift ska detaljerat ange:

- vem som ska fatta beslut om övergång till reservdrift
- vem som ansvarar för att information om övergången ges till samtliga berörda
- hur och av vem information ska lämnas till ansvariga för sådana externa system som berörs

- hur själva överflyttningen ska gå till
- hur och till vem information ska ges vad avser ambitionsnivå i form av systemprioriteringar m.m. under reservdriften
- vem som ansvarar för eventuella nyinstallationer av utrustning i ordinarie lokaler
- hur ny utrustning ska testas före återgång till normaldrift
- vem som ansvarar för beslut om övergång till normaldrift
- hur återgång till normaldrift ska ske
- hur ”ikappkörning” ska ske av de system eller delsystem för vilka någon maskinell reservrutin inte har funnits.

Den här beskrivningen av vad en avbrottsplan bör innehålla kan tyckas avskräckande, men omfattningen är i högsta grad beroende av hur stor IT-verksamheten är och hur höga krav på tillgänglighet intressenterna har.

8.5 Dokumentation och uppföljning

Att dokumentera avbrottsplanerna är initialt i många fall ett ganska omfattande arbete. Det är emellertid en förutsättning för att man ska kunna tala om en avbrottsplan. Arbetet underlättas avsevärt i de organisationer där man redan har väl dokumenterade drift- och förvaltningsrutiner.

För att tjäna sitt syfte måste dokumentationen hela tiden hållas aktuell. Användarna måste fortlöpande aktualisera den dokumentation som avser de egna reservrutinerna, t.ex. när systemförändringar inträffar eller ansvarsförhållanden ändras. På motsvarande sätt måste de IT-ansvariga hålla den dokumentation aktuell som rör maskinkonfiguration, programvaror och andra tekniska förhållanden. Om ledningsgruppens sammansättning, eller förutsättningarna för dess arbete, ändras bör gruppens ordförande svara för att alla berörda informeras.

Att upprätta en avbrottsplan och besluta om ett eventuellt reservdriftalternativ är inte ett engångsarbete. Framför allt bör ett beslut om att inte ha reservdrift omprövas, kanske en gång per år.

8.6 Behov av reservdrift

Behovet av reservdrift styrs inte av vilken typ av datorutrustning man har, utan av vilka krav intressenterna har på tillgång till informationen och hur allvarliga konsekvenserna blir, om IT-stödet upphör att fungera.

I takt med att en allt större del av myndigheters och företags information bearbetas i IT-system blir beroendet av ett fungerande IT-stöd mer och mer påtagligt. För att fastställa den egna organisationens behov av reservdrift utgår man från den bedömning av avbrottskänsligheten som går att utläsa ur en genomförd informationsklassificering eller säkerhetsanalys.

I de organisationer där avbrottskänsligheten är mycket hög, d.v.s. där konsekvenserna av ett avbrott blir mycket allvarliga redan vid avbrott på några timmar, måste rutinerna för reservdrift, åtminstone för de mest avbrottskänsliga systemen, ingå i initialinstallationen av systemet, eftersom sådana avbrottslängder inte är osannolika i någon driftmiljö.

I övriga fall måste man, för att kunna bedöma behovet av reservdrift, försöka fastställa hur stor sannolikheten är för att man ska drabbas av sådana händelser som medför en avbrottslängd, där konsekvenserna blir så allvarliga att de inte kan accepteras.

Som vi tidigare sagt finns det vissa händelser som man erfarenhetsmässigt vet hur långa avbrott de ungefär förorsakar, t.ex. fel på vissa hårdvaruenheter och avbrott i teleförbindelser. För den här typen av händelser har man också en ganska god kunskap om hur stor sannolikheten är för att de ska inträffa.

Problemen uppstår när det gäller att bedöma sannolikheten för att mer ”osannolika” händelser ska inträffa, t.ex. brand i datacentral, sabotage och naturkatastrofer. I de flesta stordatormiljöer finns preventiva och korrektiva skydd installerade för att t.ex. förhindra och begränsa skadorna vid en eventuell brand. Motsvarande skyddsåtgärder saknas ofta i servermiljöer, trots att den information som bearbetas i dessa miljöer kan vara utomordentligt betydelsefull för verksamheten.

Många organisationer har emellertid insett att även mindre datorer behöver visst skydd och har placerat sina servrar eller motsvarande i särskilda rum, s.k. ”server farms”. Ibland har man dock inte installerat de skydd som krävs för att driftmiljön ska kunna betraktas som tillräckligt säker. Bl.a. skulle många av dessa datorer kunna få allvarliga rökskador vid en brand i angränsande kontorsutrymmen.

De sämst skyddade driftmiljöerna är ofta PC-miljöerna, och det är också dessa som riskerar att drabbas av händelser som kan medföra att program och data som finns i systemet går förlorade vid t.ex. en brand. Bränder i kontor är inte så ovanliga att man kan bortse från risken att drabbas av en sådan händelse.

Givetvis kräver olika driftmiljöer helt olika insatser för att dokumentera och fastställa reservrutiner och skapa förutsättningar för reservdrift. Vad som är viktigt att komma ihåg är emellertid, att det är informationens betydelse och intressenternas krav på systemtillgänglighet som avgör huruvida man måste ha ett förberett reservdriftalternativ.

När man har fastställt att det finns behov av reservdrift gäller det att välja det alternativ som med hänsyn till de krav som finns är ekonomiskt försvarbart. Kostnaden för att genomföra reservdriftalternativet måste stå i rimlig proportion till de skadekostnader som kan uppstå i olika avbrottssituationer.

Vi ska i det följande beskriva ett antal olika reservdriftalternativ, med utgångspunkt från de krav som kan finnas på att snabbt kunna flytta över driften från ordinarie dator till en reservdator.

8.7 Olika reservdriftalternativ

8.7.1 Förutsättningar för reservdrift

Reservdrift innebär att man i en annan driftmiljö än den ordinarie utför planlagd körning av hela eller delar av den egna IT-driften.

För att en övergripande plan för reservdrift ska anses föreligga, ska ett antal kriterier vara uppfyllda:

- Dokumenterade regler för när och hur övergång till reservdrift ska ske måste finnas.
- Testkörning av det eller de system som är aktuella att flytta över ska ha skett i den nya miljön. Fortlöpande tester ska finnas periodiskt inplanerade.
- Om realtidsbearbetning mellan driftplatserna ska förekomma, ska en dokumenterad plan finnas även för hur kommunikationen ska fungera.
- Ett avtal ska vara slutet med ägaren av reservutrustningen, i de fall reservdrift ska ske utanför den egna organisationen.

En grundläggande förutsättning för att reservdrift ska kunna komma till stånd är också att såväl aktuell programvara som lagrad information finns tillgänglig. Detta innebär att vissa generella skyddsåtgärder måste vara av fullgod klass i de aktuella drift-miljöerna.

Vissa händelser, som t.ex. brand, sabotage, skivminneshaverier m.fl., innebär att såväl program som lagrad information, som finns i datorn eller närliggande utrymme, riskerar att bli förstörda. Därför är det nödvändigt att det finns säkerhetskopior av såväl program som lagrad information. Viktigt är att de reservkopior som finns på programvarorna överensstämmer med de aktuella programversioner som används. Det är också viktigt att säkerhetskopiorna finns förvarade på ett sådant sätt och på en sådan plats att de inte riskerar att bli förstörda på samma gång som originalen, samt att de rent tekniskt går att läsa in.

Generellt kan sägas att det i allmänhet inte är särskilt svårt eller tidskrävande att ersätta ren datorkraft. Om man har en egen ”tom” helt kompatibel dator som reservalternativ, eller en kompatibel

utrustning som används för utveckling och test, är det oftast relativt enkelt att tillämpa reservdrift. Med kompatibilitet menas då att inte bara själva utrustningen är densamma utan att även systemprogramvaran är helt överensstämmande, d.v.s. att såväl typ av programvara som versionsnummer överensstämmer.

I de följande beskrivningarna av olika reservdriftalternativ berörs inte olika datormiljöer. I princip kan vart och ett av de olika alternativen vara motiverat, beroende på vilka tillgänglighetskrav som finns i en viss verksamhet. Vi kommenterar emellertid avslutningsvis vilka reservdriftalternativ som är vanligast förekommande i olika datormiljöer.

8.7.1.1 Parallellbearbetning, ”hot site”

Den mest avancerade nivån av reservdrift utgörs av ”parallellbearbetning”, d.v.s. all datorbearbetning utförs parallellt i minst två av varandra oberoende miljöer. Datorerna, liksom alla tillhörande försörjningssystem, ska vara fysiskt åtskilda på ett sådant sätt att de inte kan påverkas av samma händelse. Även kommunikationen ska vara dubblerad. Denna typ av reservdrift kallas ibland för ”hot site”.

Om det ena datorsystemet slås ut så ska produktionen ändå kunna fortgå ostört med hjälp av det andra systemet utan att tid går förlorad.

8.7.1.2 Test-/utvecklingsdator, ”cold site”

Som nästa ambitionsnivå kan man se en förberedd, uttestad reservanläggning som ”normalt” används för utveckling och test, och där samma organisation har det totala ansvaret för båda installationerna. Överflyttning av produktionen ska testas med jämna mellanrum och dubblerad kommunikation ska finnas eller vara förberedd.

Aktuell version av de tillämpningsprogram som är planerade att kunna köras i reservmaskinen ska finnas lagrade och produktionsklara. Registerinformation ska kunna uppdateras kontinuerligt eller periodiskt från produktionsdatorn, och fastställda övade rutiner för överflyttning ska finnas. Reservdatorn ska, för att utgöra en användbar reserv, givetvis vara fysiskt åtskild från produktionsdatorn,

även vad gäller olika försörjningssystem som el, kyla m.m. Lösningen kallas ibland för ”cold site”.

Tid för överflyttning av förberedd datorproduktion enligt detta alternativ är maximalt några timmar.

8.7.1.3 Annan, egen produktionsdator

En tredje nivå av reservdrift är överflyttning av produktionen till annan av samma organisation ägd produktionsdator. För att en sådan maskin ska kunna användas som reservdriftalternativ, krävs troligen att delar av den ordinarie produktionen på båda datorerna läggs ned. Enda möjligheten att undgå detta är att båda anläggningarna tillsammans har en överkapacitet som motsvarar hela den aktuella produktionen, eller att båda datorerna också används för utveckling och test och denna verksamhet läggs ned.

Denna typ av reservdriftalternativ ställer således i allmänhet krav på en fastställd systemprioritering, där det klart framgår hur de olika systemen från de två driftmiljöerna ska prioriteras och vilka av de två miljöernas system som inte längre ska köras eller få en lägre prioritet.

Det här reservdriftalternativet kan tyvärr bara användas vid vissa typer av händelser, eftersom de organisationer som har två produktionsmaskiner oftast har placerat båda i samma fysiska utrymme. De delar helt eller delvis försörjningssystem i form av el och kyla med varandra, och ofta finns ingen förberedd lösning för ersättning av kommunikation.

Tidsåtgången för att flytta över produktionen till reservmaskinen kan i detta alternativ, för större system, uppskattas till 1/2-2 arbetsdagar.

8.7.1.4 Reservdrift hos annan organisation

Ytterligare ett reservdriftalternativ är att teckna ett en- eller dubbelsidigt reservdriftavtal med en annan organisation, som har en likadan datorkonfiguration som den man själv har. Detta är en enkel och billig lösning, men den ställer stora krav på ett kontinuerligt och nära samarbete mellan de två driftorganisationerna.

Det är inte tillräckligt att konstatera att motparten har en datorutrustning med samma beteckning som den man själv har. För att man ska vara säker på att en överflyttning kommer att fungera någorlunda planenligt, måste omfattande tester av program och rutiner för överflyttningen ske regelbundet. Avtal mellan parterna måste reglera bl.a. hur uppdatering av operativsystemet med nya versioner ska ske. Det måste också klart framgå vilken maskinkapacitet som avtalet om reservdrift gäller.

Denna typ av lösning kräver att den mottagande parten ständigt har tillräcklig kapacitet ledig. Detta innebär att det antingen måste finnas ledig överkapacitet, eller att en prioritering måste vara förberedd från båda parters sida.

I den här typen av reservdriftalternativ är det mindre vanligt att det finns en förberedd total lösning av kommunikationsfrågan. Detta innebär att den produktion som läggs över i princip består av satsvisa bearbetningar. Den dokumentation av reservrutiner som ska finnas i avbrottsplanerna måste således innefatta en beskrivning över hur eventuella on-line rutiner ersätts. I vissa fall kan man ha förberedda rutiner för dataregistrering off-line, för senare satsvis uppdatering av register.

Att i samband med ett avbrott som kräver reservdrift försöka etablera kommunikation i mer omfattande skala med en reservanläggning av den här typen torde inte vara genomförbart inom rimlig tid.

En annan reservdriftmöjlighet är att teckna avtal med ett företag som affärsmässigt tillhandahåller reservdrift för andra organisationer. Det bör vid tecknandet av avtal vara möjligt för kunden att fritt välja vilken ambitionsnivå man önskar ha, exempelvis vad beträffar tiden för återstart. När det gäller kommunikation till reservdatorn ansvarar kunden själv för merparten av denna planering. Företaget brukar ställa hårda krav på kunderna vad avser planering av reservdriften samt tester av överflyttning av drift till reservmaskinen.

Den erforderliga tiden för att flytta en förutbestämd del av produktionen till reservdatorn ligger mellan en och tre dagar, exklusive den tid som det tar att återupprätta eventuell kommunikation. Att flytta kommunikationen, i den mån det överhuvudtaget är realiser-

bart, kan ta allt mellan en vecka och flera månader, beroende på hur omfattande den är.

Vad som sagts ovan gäller i första hand för mer konventionell databehandling, med stordatorer eller stordatorliknande lösningar. Alltmer blir tendensen dock tydlig att även mindre system, med s.k. verksamhetskritiska tillämpningar kan behöva förses med mer rigorösa reservdriftarrangemang. I detta sammanhang kan det ibland också handla om att ha avtalat om en snabb reservleverans av ny utrustning från sin ordinarie leverantör/supportpartner, om olyckan skulle vara framme. I vissa supportrelationer kräver ofta kunden att leverantören ska ha färdigkonfigurerade utrustningar av en viss typ i lager o.s.v.

Över huvud taget är det svårt att lösa reservdriftfrågan om flera parter är inblandade. Det visar sig också att alltfler IT-intensiva företag skaffar egna reservanläggningar, av modell ”cold site”, eller tecknar avtal med ett företag som tillhandahåller reservdrift. Fördelen med en egen reservdator, som normalt utnyttjas för utveckling och test, är att man på det sättet även har löst frågan med kommunikation till reservdatorn. En svårighet kan vara att hitta lämpliga lokaler som också ligger på lämpligt avstånd från ordinarie driftställe.

8.7.1.5 ”Manuell reservdrift”

Den lägsta nivån vad gäller reservdrift, är att medvetet inte ha något förberett reservdriftalternativ. Detta behöver i sig inte innebära något fel. Om man i säkerhetsanalysen har fastställt att beroendet av datorstöd är så lågt, och riskerna för ett långvarigt driftavbrott är så små, att en högre ambitionsnivå inte är ekonomiskt försvarbar, är detta ett realistiskt alternativ.

Vid ett val av denna ambitionsnivå är det dock oerhört viktigt, att det är ett medvetet och noga övervägt val. Ledningen och de verksamhetsansvariga på olika nivåer måste vara helt medvetna om vilka risker de tar med att inte ha någon reservdrift förberedd. Ett beslut av den här typen får absolut inte fattas av IT-chefen ensam.

8.8 Vilket alternativ för vilken datormiljö

8.8.1 Stordator

För stordatormiljöer är i princip alla de uppräknade alternativen tänkbara, även det sist nämnda ”manuell reservdrift”. Det förefaller emellertid osannolikt att det förekommer stordatormiljöer, där man i dag tecknar ett ömsesidigt avtal med annan juridisk person med innebörden att man ska dela på datorresurserna. Därtill är dagens stordatormiljöer alltför komplexa, dynamiska och kommunikationsintensiva.

En vanligare lösning av reservdrift för stordatormiljöer är att organisationen har dubblerade anläggningar, väl avskilda från varandra, där den ena normalt används för utveckling och test och eventuellt begränsad produktion av mindre viktiga system. Reservkommunikationen är ibland fullt utbyggd, ibland begränsad men med förberedelser gjorda för att man snabbt ska kunna bygga ut den.

8.8.2 Nät

För den här typen av datorer finns än så länge små möjligheter att teckna avtal om reservdrift på motsvarande sätt som när det gäller stordatorer.

Ett tänkbart alternativ inom en organisation som har många servrar är att man för reservdrift har en utvecklings-/testdator, som är fullt utbyggd med möjligheter till kommunikation från alla enheter. Detta förutsätter givetvis att alla datorerna är fullt kompatibla vad avser samtliga systemprogramvaror.

Sannolikheten för att flera datorer samtidigt ska skadas är troligen ganska liten, såvida man inte har all utrustning stående oskyddad i vanliga kontorslokaler och t.ex. en brand medför att en stor del av lokalerna förstörs.

Om man har kommit fram till att de system som körs i ett lokalt när är av så vital betydelse för en viss verksamhet, att reservdrift i dator måste finnas efter kanske bara en till två dagars avbrott, bör man se till att det finns åtminstone två identiska nät (installerade så långt

ifrån varandra som möjligt) inom organisationen. De system som normalt körs i det ena kan då lämna plats för de kritiska systemen från det skadade nätverket.

Det är inte realistiskt att tro, att man på kort tid kan köpa ny utrustning och installera ett nytt nät, särskilt inte om avbrottet förorsakats av en brand.

8.8.3 Fristående persondatorer

Detta är utan tvekan den tekniska miljö, för vilken det är enklast att ordna reservdrift, under förutsättning att man beaktar några viktiga generella säkerhetsregler. Förutom att reservkopior på program och data måste finnas även i en persondator, så bör man se till man har kompatibla datorer, vilket även i detta fall inbegriper att man ska ha samma version av operativsystem.

En viktig aspekt, när man använder persondatorn till ett för verksamheten mycket betydelsefullt system, är att se till att man inte har ett ”udda” fabrikat, d.v.s. ett som man är ensam om inom sin organisation. Reservdrift kan då vara helt omöjlig, om maskinen inte längre finns på marknaden.

8.9 Exempel på kontrollfrågor vid avbrotts- och katastrofplanering

I detta avsnitt har vi sammanställt ett antal frågor som kan vara till hjälp när man dels vill kontrollera om man har en fungerande IT-säkerhetsorganisation, vilket är en första förutsättning för en framgångsrik avbrottsplanering, dels om man har en genomtänkt plan för hur verksamheten ska fungera om IT-stödet faller bort för längre eller kortare tid.

Det är inte möjligt att i det här sammanhanget formulera alla de frågor som kan vara relevanta i en viss verksamhet. Frågorna ska ses som utgångspunkter. Den som använder frågelistorna bör alltså noga tänka igenom vilka följdfrågor och problem som kan vara aktuella inom den egna organisationen.

Man kan uttrycka det så, att ett ”ja” som svar på en fråga inte enbart bör innebära att problemområdet har uppmärksammats, utan också att frågan har penetrerats till ett för verksamheten anpassat djup, och att man därvid har funnit att relevanta åtgärder har vidtagits.

Vi har delat in frågorna i tre huvudtyper, nämligen:

- övergripande frågor, som bör besvaras av ledning och verksamhetsansvariga chefer
- användarspecifika frågor, som bör besvaras av systemansvariga och användare
- driftrelaterade frågor, som bör besvaras av IT- och driftansvariga.

8.9.1 Övergripande frågor

Finns en övergripande strategi som klargör hur stort behovet av ett fungerande IT-stöd är för verksamheten?

Finns en funktion inom organisationen som har ett direkt ansvar för IT-säkerhetsfrågor och samordning av IT-säkerhetsarbete?

Finns det en klar koppling mellan verksamhetsansvar och övergripande ansvar för IT-säkerheten inom den egna verksamheten?

Finns IT-säkerhetsansvariga utsedda på olika nivåer i organisationen?

Finns systemägare utsedda för alla tillämpningssystem?

Finns det dokumenterat, och är det allmänt känt, vilket ansvar och vilka befogenheter en systemägare har?

Finns det någon utpekad funktion som har ansvaret för att en avbrotts-/reservdriftplanering blir genomförd?

Har någon övergripande säkerhets-/sårbarhetsanalys för hela verksamheten genomförts?

Om JA på frågan ovan, har resultatet av analysen inneburit att några säkerhetshöjande åtgärder vidtagits?

Finns det någon handlingsplan som prioriterars bland de åtgärder som ska genomföras?

Finns det en övergripande beslutsorganisation för att handlägga mycket svåra störningar/katastrofer avseende IT-stödet?

Om JA på frågan ovan, finns det en noggrann instruktion för beslutsorganisationen?

Finns det en för hela organisationen gällande prioritering av de olika IT-systemen?

Om JA på frågan ovan, är denna prioritetslista samordnad med eventuella andra systemägares prioriteringar inom en gemensam databearbetningsmiljö?

8.9.2 Frågor för systemansvariga/användare

Finns systemansvariga utsedda för samtliga system?

Har någon säkerhets-/sårbarhetsanalys genomförts under de senaste två åren?

Har en maximalt tillåten avbrottstid bestämts för alla system?

Om JA på frågan ovan, har detta resulterat i att föreslagna säkerhetshöjande åtgärder genomförts eller planeras bli genomförda?

Finns det en inbördes prioriterad förteckning över organisationens samtliga IT-system?

I de fall databearbetningen helt eller delvis utförs av annan organisation, har den/de verksamhetsansvariga delgivits och accepterat prioriteringen av systemen inom den externa driftenheten?

Har avbrottsplanering genomförts, så att åtgärder beskrivits med tillräcklig detaljeringsnivå, relaterat till alternativa avbrottslängder?

Finns någon, utom systemägaren, som har ett uttalat ansvar för att handlägga frågor om avbrotts- och reservdriftplanering?

Finns en beslutsorganisation utsedd för att handlägga akuta frågor rörande avbrott i datorstödet?

Är reservrutiner, såväl manuella som maskinella, kända av berörd personal?

Har övning av såväl manuella som maskinella reservrutiner genomförts?

Finns ett klart uttalat ansvar för à-jourhållning av reservrutinerna?

8.9.3 Frågor för IT- och driftansvariga

Finns övergripande riktlinjer eller policy, fastställd av ledningen, som beskriver vilken ambitionsnivå som ska gälla för avbrotts- och reservdriftplanering?

Finns särskilt utsedd person som handlägger ovanstående frågor?

Har säkerhets-/sårbarhetsanalys genomförts tillsammans med den systemansvarige de senaste två åren?

Har samtliga systemansvariga prioriterat sina system?

Finns en för driftenheten total prioriteringslista för samtliga system? Prioriteringen ska vara utförd i samråd med samtliga berörda systemägare.

Finns detaljerade beskrivningar av vilka åtgärder som ska vidtas vid avbrott av olika längd, t.ex.:

- korta avbrott (upp till ett par timmar)?
- medellånga avbrott (ett par timmar till en dag)?
- långa avbrott (mer än en dag)?
- mycket långa avbrott (mer än två veckor)?

Finns maximalt tillåtna avbrottstider dokumenterade för samtliga system?

Finns behovet av reservdrift dokumenterat?

Är eventuella reservdriftplaner kända av de personer som behöver känna till dem?

Finns en förberedd katastroforganisation för IT-enheten?

Är kontakt- och beslutsvägar till systemansvariga eller till särskild ledningsgrupp vid allvarliga driftstörningar dokumenterade?

Genomförs regelbundet övning av planerade åtgärder vid olika typer av störningar?

Har eventuella reservdriftalternativ testats?

9 Utbildning

9.1 Behov av utbildning

Goda kunskaper hos personalen, ett högt risk- och säkerhetsmedvetande och en hög motivation i arbetet är av allra största betydelse för att upprätthålla en hög IT-säkerhetsnivå. En stor del av alla händelser som förorsakar störningar i IT-verksamhet har samband med bristande kunskaper, slarv eller slentrianmässig hantering. Sådana brister kan leda till direkta störningar i form av driftavbrott etc. De kan också medföra att svagheter uppstår i säkerhetssystemet, som gör att detta inte fungerar vid en störning. Ett exempel på detta är, att man inte har fått lära sig hur utrustningen för brandbekämpning fungerar.

Under senare år har säkerheten i IT-systemen kommit att bli beroende av fler människors sätt att utföra sina arbetsuppgifter. Som en följd av den ökade decentraliseringen av datorkraft i form av persondatorer, har många människor kommit att bli mer direkta användare av informationstekniken. Många arbetar med uppgifter som kan sägas ingå i förrutiner till de egentliga IT-rutinerna. Även andra människor har ofta arbetsuppgifter som kan påverka säkerheten.

Först och främst måste **kunskapen om det egna arbetet** vara god. Det är en absolut förutsättning för ett framgångsrikt säkerhetsarbete, att utbildningen för att sköta de ordinarie arbetsuppgifterna är tillräcklig.

Utbildningen för det egna arbetet behöver dock alltid kompletteras med **särskild IT-säkerhetsutbildning.** Ordet ”särskild” får inte tolkas så att säkerhetsutbildningen ska vara separerad från annan utbildning eller från annat IT-säkerhetsarbete. Tvärtom är det nödvändigt att en mycket nära samordning sker, på samma sätt som säkerhetsarbetet måste vara väl integrerat i hela systemutvecklingen och systemförvaltningen.

I fortsättningen av detta kapitel är det dock bara den utbildning som tar sikte på de särskilda säkerhetsfrågorna som vi talar om.

En god utbildning i IT-säkerhet får inte inskränka sig till att lära ut enbart kunskaper och tekniska färdigheter. Vi har i flera sammanhang

i handboken påpekat vikten av att ett risk- och säkerhetsmedvetande upprätthålls inom hela organisationen och att personalen är väl motiverad, när det gäller att iaktta de säkerhetsbestämmelser som finns och är vaksam mot brister. Även goda kunskaper om hur en säkerhetsåtgärd ska genomföras minskar avsevärt i betydelse, om den som ska vidta åtgärden inte förstår varför den är nödvändig, eller tror att det inte har så stor betydelse om man då och då skulle glömma att genomföra den.

Varje verksamhetsansvarig har ett ansvar, inte bara för att kunskapsnivån i IT-säkerhetsfrågor är tillräcklig, utan också för att risk- och säkerhetsmedvetandet och motivationen upprätthålls. Det krävs planmässiga och kontinuerliga utbildningsåtgärder för att åstadkomma detta.

I detta kapitel kommer vi framförallt att uppehålla oss vid frågor om vilka personalkategorier som behöver utbildning i IT-säkerhet och vilket innehåll utbildningen lämpligen kan ha. Vi diskuterar också tänkbara former för utbildningen. Frånsett ett kortare inslag om utbildningsplanering går vi däremot inte in på frågor om generell utbildningsmetodik och -teknik.

Behovet av utbildning i IT-säkerhet varierar naturligtvis i hög grad mellan olika organisationer. De beskrivningar som görs i det följande kan i vissa stycken kännas omfattande för en liten organisation. Vår avsikt är att ange lämplig inriktning och ge uppslag inför planering av utbildning. Var och en måste anpassa materialet efter det egna behovet.

Gränsen mellan utbildning och information i IT-säkerhetsfrågor är flytande. Vi kommer i fortsättningen att för enkelhetens skull ofta låta begreppet ”utbildning” täcka även åtgärder som normalt kanske skulle kallas ”information” .

9.2 Vilka behöver utbildning

Man kan utgå från att så gott som all personal inom en organisation som använder IT behöver någon form av utbildning i IT-säkerhetsfrågor. Men behovet varierar givetvis en hel del mellan olika personalkategorier, beroende på arbetsuppgifter och förkunskaper.

När det gäller inriktningen av utbildningen kan man exempelvis skilja mellan behov av:

- allmänt orienterande utbildning
- fördjupad utbildning i IT-säkerhetsarbetets bedrivande, metoder och tekniker
- målinriktad utbildning med anknytning till specifika arbetsuppgifter eller områden.

I det följande ger vi exempel på utbildning för olika personalgrupper.

9.2.1 Användare

Med användare menar vi här personer som i sitt dagliga arbete direkt eller indirekt kommer i kontakt med IT-systemet men som, utöver det ansvar för IT-säkerheten som följer med den egna arbetsuppgiften, inte har något särskilt ansvar för IT-säkerhetsfrågor.

Användare bör ges utbildning på två nivåer – dels en allmän, orienterande utbildning, dels en målinriktad utbildning, som är anpassad till den egna arbetsuppgiften.

Den **orienterande** utbildningen ska ge en allmän kunskap om och förståelse för IT-säkerhetsfrågornas roll i organisationens verksamhet. Den kan lämpligen innehålla korta översikter över bl.a:

- betydelsen av IT i verksamheten
- följderna av störningar i IT-verksamheten
- vissa begrepp inom IT-säkerhetsområdet
- hot och risker
- innebörden av risk- och sårbarhetsanalys
- möjliga skyddsåtgärder.

Dessutom bör den ta upp frågor om:

- organisationen av IT-säkerhetsarbetet inom myndigheten eller företaget

- vad man ska göra och vem man ska vända sig till om man upptäcker brister i säkerheten eller vill veta hur man ska förfara i ett visst fall
- vilka gällande säkerhetsföreskrifter som finns inom organisationen och hur dessa föreskrifter finns dokumenterade
- betydelsen av att befintlig dokumentation används och att reglerna följs
- hur användaren får fortlöpande information i IT-säkerhetsfrågor
- vem som är ”offentlighetsansvarig” respektive ”rättelseansvarig” (inom en myndighet)
- gällande lagstiftning av betydelse, offentlighetsprincipen, sekretesslagen, datalagen, bokföringslagen
- system för behörighetskontroll, inklusive handhavande av lösenord.

Den allmänna, orienterande utbildningen behöver kompletteras med **en mer målinriktad,** som direkt ansluter till arbetsuppgiften. I den kan man behandla bl.a:

- vilka särskilda hot och risker som finns i den egna arbetsrutinen
- vad man kan göra för att minska riskerna
- vilka särskilda skyddsåtgärder som är vidtagna i anslutning till den egna arbetsrutinen
- vilka försiktighetsåtgärder den enskilde ska vidta i sitt arbete
- hur utrustning och datamedier, inklusive pappersutskrifter, ska hanteras från säkerhetssynpunkt
- konsekvenser av felhantering eller liknande
- vad användaren ska göra vid driftstopp
- vad användaren ska göra om det börjar brinna, var utrustning finns för brandbekämpning och hur den ska användas.

Den målinriktade utbildningen måste anpassas efter arbetsuppgiftens karaktär, vikten av den information som produceras och risker-

na för störningar i just det arbetet. Personal som arbetar med personregister behöver exempelvis ha särskild utbildning i datalagens föreskrifter. De personer som vid myndigheter utses till ”offentlighetsansvariga” enligt sekretesslagen, eller ”rättelseansvariga” enligt datalagen, behöver givetvis god utbildning i sekretess- och datalagstiftningen.

Utbildningen av användare kan givetvis behöva varieras efter den tekniska utrustning som är aktuell. Ett exempel på detta är att risker och skyddsåtgärder vid användning av persondator delvis är av andra slag än vid användning av terminal.

Det finns emellertid också en annan, ur säkerhetssynpunkt viktig, skillnad mellan användning av persondator och användning av terminal. Persondatoranvändaren, särskilt den som använder en fristående persondator, kan ofta sägas vara både systemansvarig och driftansvarig, och har därigenom också ett större eget ansvar för säkerheten. Ett enkelt exempel på detta är att den som använder en fristående persondator i regel själv måste tänka på att ta reservkopior. I utbildning för användare av persondator är det angeläget att också sådana här ansvarsfrågor, och konsekvenserna av dem, tas med.

9.2.2 IT-personal

Också IT-personal behöver särskild säkerhetsutbildning. Till IT-personal räknas här inte bara driftoperatörer och annan personal som har till särskild uppgift att sköta den löpande driften av datorerna, utan också systemerare, programmerare och annan personal som arbetar med utveckling och förvaltning av IT-systemen. Säkerhetsaspekterna måste från början vara integrerade i systemutvecklingen och finnas med även vid de förändringar i systemet som senare görs. Den personal som arbetar med utveckling och förvaltning måste alltså ha utbildning i IT-säkerhet, likaväl som driftpersonalen. När det gäller driftpersonal är det angeläget att i det här sammanhanget inte glömma bort personer som arbetar vid mindre datoranläggningar, eller i nätverk av persondatorer, med uppgifter som har karaktären av driftövervakning men som kanske bara upptar en del av arbetstiden. Det kan vara personal av typen ”driftansvarig”, ”systemadministratör”, ”nätadministratör” etc.

IT-personalen kan, när det gäller behovet av utbildning, sägas inta en särställning. Säkerheten i IT-systemet beror i mycket hög grad på deras sätt att sköta sitt dagliga arbete. För IT-personalen är utbildningen i de egna arbetsuppgifterna särskilt viktig för säkerheten. Det är också i många fall svårt att skilja IT-personalens ordinarie arbetsuppgifter från specifika säkerhetsåtgärder. Det gäller t.ex. en operatörs handhavande av datamedier. IT-personalen måste i likhet med annan personal ha särskild utbildning i säkerhetsfrågor, och denna bör också integreras med utbildningen för de löpande arbetsuppgifterna.

När det gäller särskild IT-säkerhetsutbildning måste IT-personalen liksom vanliga användare ha både en orienterande, allmän utbildning och en utbildning som avser säkerhetsåtgärder, som är direkt knutna till arbetsuppgiften. Denna senare utbildning behöver vara mer omfattande än för en vanlig användare. Grundläggande för all utbildning är att inskärpa ett medvetande om vilken betydelse IT-personalens sätt att arbeta har för upprätthållandet av IT-säkerheten, och vilka konsekvenserna kan bli vid felhantering o.d.

Säkerhetsfrågor vid hantering av utrustning och datamedier är givetvis särskilt viktiga för IT-personal. Frågor som dessutom tillkommer utöver vad som angivits ovan för ”användare” är t.ex:

- betydelsen för säkerheten av att driftrutinerna fungerar väl och att alla föreskrifter följs
- säkerhetsföreskrifter i systemhandbok, drifthandbok o.d.
- betydelsen av att dokumentera vad som görs
- sekretessfrågor avseende de olika IT-system som hanteras
- brandberedskap, åtgärder vid brand, utrymningsvägar
- hantering och förvaring av datamedier, inklusive reservkopior
- åtgärder vid driftavbrott.

9.2.3 Verksamhetsansvariga

De personer som har verksamhetsansvar eller systemägaransvar har också ansvaret för att IT-säkerheten upprätthålls inom sina respektive verksamhetsområden eller IT-system. För att kunna ta detta

ansvar måste de verksamhetsansvariga vara väl orienterade om de grundläggande förutsättningarna för ett framgångsrikt IT-säkerhetsarbete. De måste bl.a. kunna ta ställning till förslag från IT-säkerhetschef eller annan särskilt utsedd IT-säkerhetsansvarig.

En utbildning för verksamhetsansvariga kan innehålla orienterande inslag om:

- IT-stödets betydelse för verksamheten
- betydelsen av säkerhet i IT-systemet och de arbetsrutiner som berörs av IT-stödet
- ansvaret för IT-säkerheten
- betydelsen av att ett säkerhetsmedvetande finns inom hela organisationen
- betydelsen av utbildning
- betydelsen av andra administrativa åtgärder
- organisation av IT-säkerhetsarbetet
- samverkan mellan verksamhetsansvariga och säkerhetsansvariga
- hot och risker
- behovet av och tillvägagångssättet vid säkerhetsanalys
- befintliga och möjliga skyddsåtgärder.

9.2.4 IT-säkerhetschef och andra särskilt utsedda IT-säkerhetsfunktioner

Inom varje organisation som använder IT bör det finnas en person – ”IT-säkerhetschef’, ”IT-säkerhetsansvarig” e.d. – som närmast under ledningen svarar för samordning av IT-säkerhetsarbetet inom hela organisationen. De arbetsuppgifter som är förknippade med detta ansvar kan i en organisation med liten IT-verksamhet vara en del av en ”IT-samordnares” arbete. Där det finns en säkerhetschef med ansvar för säkerhetsfrågor i allmänhet, kanske denne också är ”IT-säkerhetschef”. I en organisation med omfattande IT-verksamhet kanske IT-säkerhetschefen har flera underställda IT-säkerhetsspecialister och samverkar med särskilda ”IT-säkerhetshandläg-

gare" inom organisationens linjeavdelningar. Dessa personer, som vi här sammanfattande kallar IT-säkerhetsansvariga, har det gemensamt att de har tilldelats ett särskilt IT-säkerhetsansvar. Dessa måste ha en fördjupad utbildning som svarar mot de krav detta ansvar ställer. Också denna fördjupade utbildning kan givetvis behöva differentieras, beroende på vilken omfattning ansvaret och arbetsuppgifterna för respektive IT-säkerhetsansvarig har.

En IT-säkerhetschef och de andra personer som ska tjänstgöra som specialister inom IT-säkerhetsområdet måste ha en god allmän kunskap om tekniker och metoder i IT-säkerhetsarbete. I deras utbildning kan ingå moment som avser:

- vanliga hot och risker
- gällande lagstiftning, sekretess- och offentlighetsfrågor
- säkerhetsanalys, klassificering av information
- olika IT-tekniska driftformer; skyddskrav relaterade till tekniken
- olika slag av skyddsåtgärder
- organisation av IT-säkerhetsarbetet
- arbetsuppgifter och arbetssätt för en IT-säkerhetsansvarig.

De allmänna kunskaperna om tekniker och metoder för att bedriva IT-säkerhetsarbete kan behöva kompletteras med **kunskaper om den egna organisationen** och de sär-skilda förutsättningar som råder där. En sådan kompletterande utbildning kan t.ex. innehålla avsnitt om:

- verksamhetens organisation
- IT-stödets omfattning och utformning
- hot och risker i verksamheten
- slag av information som behandlas, dess betydelse för verksamheten och därav följande krav på sekretess eller på hög grad av tillgänglighet
- befintlig datorutrustning, kommunikationslinjer etc.
- existerande skydd och säkerhetsrutiner
- lokaldisposition, allmänna regler för tillträde etc.

9.2.5 Annan personal

Någon form av säkerhetsutbildning med nära anknytning till de egna arbetsuppgifterna bör ges också åt personal som kanske inte direkt uppfattas som användare eller i övrigt engagerade i IT-verksamheten, men som ändå i sitt arbete kan påverka säkerheten i ett IT-system. Ett exempel är att en vaktmästare eller en lokalvårdare måste veta att man inte bör placera brännbart material i ett datorrum eller att vissa dörrar ska hållas låsta. Alla måste också vara medvetna om andra säkerhetsåtgärder som i och för sig har mer med allmän säkerhet att göra, men som har stor betydelse också för IT-säkerheten, t.ex. att inte blockera utrymningsvägar eller ställa upp saker framför brandredskap.

9.2.6 Ny personal

Man får inte glömma bort nyanställdas behov av utbildning. Det kan som regel inte genast tillgodoses inom ramen för den ordinarie utbildningen. Någon form av **första utbildning** i de mest angelägna säkerhetsfrågorna behövs alltså. Den måste givetvis anpassas efter den nyanställdes förkunskaper och blivande arbetsuppgifter. De säkerhetsfrågor som är särskilt förknippade med den egna arbetsuppgiften bör ha en framträdande plats i en sådan introduktionsutbildning, som så snart tillfälle ges bör kompletteras med den utvidgade utbildning som kan behövas.

Med nyanställda kan man i det här sammanhanget jämställa personer som av olika skäl får nya arbetsuppgifter inom organisationen. De behöver kunskap om vilka nya säkerhetsfrågor som är aktuella till följd av de förändrade uppgifterna.

9.2.7 Tillfällig personal

Med tillfällig personal menar vi personer som arbetar inom organisationen under en begränsad period, exempelvis konsulter eller examensarbetare.

Tillfällig personal får inte glömmas bort vad gäller utbildning i organisationens säkerhetsfrågor och rutiner. Utbildningen bör genomföras snarast efter det att personen i fråga har börjat sitt arbete. Frågor som rör själva arbetsuppgiften ska ha en framträdande plats i säkerhetsutbildningen.

9.3 Former för utbildning och information

Utbildning och information kan ges i många olika former, t.ex. som:

- ”färdiga” kurser som tillhandahålls på marknaden
- schemalagd utbildning i egen regi
- kortare orienteringar i aktuella frågor, ”informationsdagar” o.d.
- inlärning i det praktiska arbetet med stöd av mer erfarna arbetskamrater
- särskilda praktiska övningar
- tillvaratagande av externa erfarenheter, studiebesök, konferenser o.d.
- spridning av skriftligt informationsmaterial.

9.3.1 Externa och interna kurser

Kurser, seminarier o.s.v., tillhandahålls av utbildningsinstitut, bransch- eller intresseorganisationer och utbildningsföretag. Sådan **extern** utbildning finns av olika omfattning. Det finns längre kurser som närmast är avsedda för personer som har, eller väntas få, särskilt ansvar för IT-säkerhetsfrågor. Bland kortare kurser finns både sådana som avser att ge en allmän orientering i IT-säkerhet och sådana som tar sikte på avgränsade delar av IT-säkerhetsarbetet, t.ex. metoder för att göra risk- och sårbarhetsanalyser.

Utbildning kan också anordnas **internt,** i meningen att den planeras inom den egna organisationen och mer eller mindre ”skräddarsys” för dess behov. Planering och genomförande kan ske med eller utan hjälp av konsult eller utbildningsföretag. Förutsättningarna för internt ordnad utbildning är bättre om det inom organisationen redan finns någon eller några personer med goda kunskaper om IT-säkerhet.

Fördelen med externa, ”färdiga” kurser är främst att de inte kräver så mycket egna arbetsinsatser och specialkompetens. Nackdelen är att den färdiga kursen sällan passar riktigt väl till den egna organisationens behov. Som påpekats i ett föregående avsnitt måste en viktig del av utbildningen knyta an till arbetsområdets särskilda förhållanden. Den delen av utbildningen måste givetvis utformas

och planeras av personer med god kännedom om den aktuella verksamheten. De kurser och seminarier som erbjuds på marknaden är alltså aldrig ensamt tillräckliga för att ge den utbildning som behövs.

Allmänt kan man säga att utbildningen bör utformas och genomföras i så nära anslutning till deltagarnas egen verksamhet som möjligt. I större organisationer innebär det ofta att en decentralisering av utbildningen är önskvärd.

Vid köp av IT-utrustning förekommer det ibland att en viss utbildning från leverantörens sida ingår i priset. Oavsett om särskilda säkerhetsfrågor ingår bör möjligheterna att få en sådan utbildning utnyttjas, eftersom den kan väntas vara anpassad direkt till den utrustning som personalen ska arbeta med.

Regelbundet återkommande ”informationsdagar” eller ”informationspass” är lämpliga inslag framför allt i fortbildning på IT-säkerhetsområdet och för att vidmakthålla ett säkerhetsmedvetande. Se avsnittet ”Uppföljning och kontinuitet”.

9.3.2 Praktisk träning och erfarenhetsutbyte

För att de kunskaper som förvärvas under en kurs ska bestå och ha ett värde måste möjlighet ges att tillämpa dem i praktiskt arbete efter kursen. För det ändamålet är det angeläget att arbetsorganisationen utformas så, att den nyutbildade får stöd av mer erfarna kollegor. Därigenom befästes och utvecklas de teoretiska kunskaperna. En sådan **träning i det praktiska arbetet** kan inte ersätta den teoretiska utbildningen, men ska ses som ett viktigt komplement till denna. Den är dessutom en utmärkt form för att höja säkerhetsmedvetande och motivation, som är så viktiga för att IT-säkerheten ska kunna upprätthållas.

Särskilda **praktiska övningar** är erfarenhetsmässigt en effektiv form för utbildning och, inte minst, för att upptäcka brister i organisation och rutiner. Begränsningar kan sättas bl.a. av möjligheterna att anordna övningar under tillräckligt realistiska förhållanden. Till det som med fördel kan övas hör snabbstopp av driften, återladdning av säkerhetskopior, utrymning av lokaler, brandbekämpning.

Utbyte av erfarenheter med andra organisationer och företag är ofta givande. Det kan ske genom t.ex. direkta kontakter i aktuella frågor, deltagande i mer eller mindre formella samarbetsgrupper, deltagande i konferenser, seminariedagar o.d. Inom Dataföreningen i Sverige finns en särskild grupp, SIG Security, för erfarenhetsutbyte inom IT-säkerhetsområdet. Även inom Swedish Network Users Society (SNUS) finns en arbetsgrupp för IT-säkerhetsfrågor.

9.3.3 Skriftlig information

Till utbildning i form av kurser o.d. bör det finnas särskilt utarbetat utbildningsmaterial. Det bör dessutom inom organisationen finnas skriftligt material av mer eller mindre ”stående” karaktär, som anger de policies, instruktioner, praktiska råd etc., som bör tillämpas i IT-säkerhetsarbetet.

Till det material som alltid bör finnas, och som har betydelse för IT-säkerheten, hör **ordinarie arbetsinstruktioner.** Många av de skyddsåtgärder, som man vidtar för att uppnå och bibehålla en god säkerhetsnivå, är direkt knutna till olika personalgruppers ordinarie arbetsuppgifter. Det gäller både användare och IT-personal. Säkerhetsinstruktioner för specifika arbetsuppgifter, t.ex. datordrift, kan därför med fördel ingå i arbetsinstruktionerna.

De ordinarie instruktionerna behöver kompletteras med instruktioner och annan information som särskilt avser IT-säkerhetsområdet. Ibland är sådan information samlad i en ”IT-säkerhetshandbok” eller liknande. Eftersom olika personalgrupper behöver olika slag av information är det dock i allmänhet inte lämpligt att sprida en enda typ av handbok, som förutsätts innehålla all information.

Till den information som bör ges vid spridning hör en **allmän IT-säkerhetsinformation,** som orienterar om problemområdet och hur den egna organisationens IT-säkerhetsarbete bedrivs. Den kan t.ex. bestå av information om:

- policy för IT-verksamheten
- policy för IT-säkerheten
- ansvarsförhållanden och organisation i IT-säkerhetsfrågor
- lagstiftning som påverkar verksamheten och kraven på IT-säkerhet

- realistiska hot inom den egna verksamheten
- andra faktorer av betydelse för säkerhetskraven
- generella säkerhetsåtgärder, som alla måste känna till, t.ex. vilken typ av behörighetskontroll som används, vilka regler som gäller för tilldelning av behörighet och hantering av lösenord
- generella regler för tillträdeskontroll och andra åtgärder, som har att göra med skydd av lokaler, datorutrustning och personal
- vilka verksamhetsanknutna säkerhetsföreskrifter som finns.

Den allmänna informationen kompletteras lämpligen med en selektivt spridd **verksamhetsanpassad IT-säkerhetsinformation,** som knyter an till respektive personalkategoris särskilda arbetssituation. Den bör ge upplysning om bl.a:

- vem som är närmast ansvarig för IT-säkerhetsfrågor inom den egna arbetsenheten
- till vem man ska vända sig om ett IT-system inte fungerar som det ska
- säkerhetsrutiner inom den aktuella verksamheten
- särskilda säkerhetsföreskrifter för enskilda IT-system (t.ex. att vissa utdata från ett system måste förvaras på ett särskilt sätt)
- särskilda instruktioner för personal som använder fristående persondatorer
- särskilda instruktioner för personal som arbetar med persondatorer, som är anslutna till lokala nät.

Den verksamhetsanpassade dokumentationen kan av naturliga skäl behöva delas upp efter de olika delverksamheter som avses.

Beträffande IT-personal måste det finnas instruktioner för både systemerare/programmerare och driftpersonal. Det mesta av sådana instruktioner hör till det som bör ingå i de ordinarie arbetsinstruktionerna i drifthandbok och i anvisningar för utveckling och förvaltning av IT-system. I drifthandboken kan dock ofta särskilda säkerhetsföreskrifter för enskilda IT-system behövas.

För att informationen, både den allmänna och den verksamhetsanpassade, ska bli läst och tillämpad bör stor möda läggas ner på att

göra framställningen klar, konkret och anpassad till respektive personalgrupps kunskaper och arbetsförhållanden. En lättläst typografi är inte minst viktig. Ofta kan korta, koncisa sammanfattningar göras som **”lathundar”**.

Varje verksamhet förändras ständigt och det är av grundläggande vikt att all information (inklusive den i IT-säkerhetshandboken, se nedan) hålls aktuell för att inte förlora sitt värde. Vid den tekniska utformningen av dokumenten bör man därför ta hänsyn till de varierande krav på uppdatering som kan finnas. Det är exempelvis troligt att den verksamhetsanpassade dokumentationen behöver uppdateras mer ofta än den allmänna.

IT-säkerhetschefen och hans medarbetare bör ha en komplett IT-säkerhetshandbok, som innehåller alla de riktlinjer och regler som gäller för IT-säkerhetsarbetet inom organisationen. Ett exemplar av denna handbok bör dessutom finnas tillgänglig hos var och en av de verksamhetsansvariga, eller de personer, till vilka de verksamhetsansvariga delegerat ansvaret för IT-säkerhetsfrågor inom sina respektive verksamhetsområden. Handboken bör innehålla komplett dokumentation över:

- lagstiftning som berör verksamheten, och dess påverkan på IT-verksamheten
- policies och riktlinjer för IT-verksamheten och IT-säkerhetsarbetet
- ansvarsförhållanden och organisation på IT-säkerhetsområdet
- regler för planering, uppföljning och rapportering av IT-säkerheten
- handlingsplaner för IT-säkerhetsarbetet
- arbetsordningar, instruktioner, befattningsbeskrivningar på IT-säkerhetsområdet
- gällande säkerhetsrutiner och företagna skyddsåtgärder
- beredskapsplaner och planer inför svårare olyckor
- regler för hur och när risk- och sårbarhetsanalyser ska genomföras och hur de ska dokumenteras
- regler för informationsklassificering

- regler för hur säkerhetsfrågorna ska beaktas vid inköp av maskin- och programvaror
- regler för administration (tilldelning, registrering och uppföljning) av system för behörighetskontroll
- annan information som IT-säkerhetschef och verksamhetsansvariga behöver för att kunna bedriva ett effektivt IT-säkerhetsarbete.

Det material som har beskrivits i det föregående bör i valda delar användas som studiematerial vid särskilt anordnad utbildning i IT-säkerhet.

Den information som vi hittills har talat om kan behöva kompletteras med **fortlöpande information** om nyheter och förändringar, som inte är av det slaget att de påverkar gällande instruktioner o.d., men som det ändå bedöms som angeläget att sprida kännedom om. För att information av detta slag ska ha effekt bör den vara kortfattad, konkret och lättläst. Den bör distribueras i bestämda former och inte alltför tätt.

9.4 Utbildningens genomförande

9.4.1 Ansvar och organisation

Ansvaret för att personalen har tillräcklig utbildning i IT-säkerhet, liksom ansvaret för att IT-säkerheten generellt sett är tillfredsställande, ingår alltid i verksamhetsansvaret på olika nivåer i organisationen. Detta ansvar, att kontrollera utbildningsnivån, kan, liksom ansvaret för andra IT-säkerhetsfrågor, delegeras av den verksamhetsansvarige till en ”IT-säkerhetshandläggare”, ”IT -säkerhetsansvarig” e.d.

För att ge utbildningen det innehåll som behövs, med tanke på hotbild och säkerhetsläge inom verksamheten, krävs sakkunskap i IT-säkerhetsfrågor. Att utforma och föreslå innehåll i utbildningen bör därför åligga den ”IT-säkerhetschef”, eller person med motsvarande funktion, i vars verksamhet IT-stödet är av betydelse.

Det praktiska arbetet med att genomföra utbildningen kan ordnas på olika sätt. I större organisationer kan det finnas en särskild utbildningsenhet. Ofta finns en administrativ avdelning, som bland sina uppgifter har att svara för utbildning. Oavsett om det redan finns en funktion med ett uttalat ansvar för utbildningsfrågor eller inte, så bör en utbildningsansvarig utses, som har att svara för det praktiska genomförandet av utbildningen.

Den här skisserade arbetsfördelningen kan också beskrivas så, att:

Verksamhetsansvarig

- fortlöpande kontrollerar behovet av utbildning i IT-säkerhet inom sitt verksamhetsområde
- informerar IT-säkerhetschef och utbildningsansvarig om behov av utbildning
- följer upp effekterna av genomförd utbildning inom sitt verksamhetsområde.

IT-säkerhetschefen

- föreslår innehåll i utbildningen med utgångspunkt från bl.a. den rådande kunskapsnivån, hot och risker mot verksamheten och tillgängliga metoder och tekniker för skydd
- föreslår anskaffning eller utformning av lämpligt utbildningsmaterial
- följer upp all utbildning på IT-säkerhetsområdet tillsammans med den utbildningsansvarige
- föreslår generella utbildningsinsatser, t.ex. årligen återkommande utbildningsdagar, och gör det på grundval av sina allmänna kunskaper på området, samt inom organisationen gjorda erfarenheter.

Utbildningsansvarig

- vidtar de praktiska förberedelserna inför utbildningen
- genomför eller övervakar genomförandet av utbildningen

- gör tillsammans med IT-säkerhetschefen generell uppföljning av all utbildning.

De här olika arbetsuppgifterna måste naturligtvis ingå som arbetsmoment i en integrerad planering, i vilken alla intressenter samverkar. Planeringen kan t.ex. ske i en särskild arbetsgrupp, där företrädare ingår för berörda verksamhetsansvariga, IT-säkerhetschef och utbildningsfunktion. Den utbildningsansvarige bör också ingå i den projektgrupp eller liknande, som har till uppgift att planera IT-säkerhetsarbetet i stort.

Som vid all utbildning är det av grundläggande betydelse att de som utbildas är väl motiverade, och att deras kunskaper om det egna arbetet tas till vara. Målgruppen för utbildningen bör därför på lämpligt sätt företrädas i den grupp som genomför utbildningsplaneringen.

9.4.2 Utbildningsplanering

I detta avsnitt vill vi i korthet lämna några synpunkter på planering av utbildningen.

Utbildningsplaneringen måste baseras på att verksamhetsansvariga på alla nivåer är medvetna om utbildningens betydelse och att de kan förmedla denna insikt till den övriga personalen. Det behövs med andra ord ett gynnsamt ”utbildningsklimat”. Resurser måste kunna avsättas för utbildningen. Det innebär bl.a. att den personal som behöver utbildas måste ges möjlighet att avsätta tillräckligt med tid, både för att genomgå utbildningen och senare för praktisk träning.

Det är naturligtvis av grundläggande betydelse att utbildningen har sådant innehåll och sker i sådana former att den känns meningsfull och stimulerande. Den bör så långt möjligt ordnas så att deltagarna ges tillfälle att aktivt arbeta med problem som de känner igen från sin dagliga verksamhet. Som tidigare har nämnts är det lämpligt att de som ska utbildas får möjlighet att vara med redan vid utbildningsplaneringen, t.ex. genom att få föra fram egna erfarenheter och synpunkter på behovet av och lämpliga former för utbildningen.

Syftet med planeringen är att anpassa utbildningen till personalens behov och organisationens resurser. I en mindre organisation med litet utbildningsbehov erbjuder detta kanske inte så stora problem. Det kan gå relativt lätt att få en överblick över både behov av kunskaper, nuvarande utbildningsläge och tillgängliga resurser. Även i sådana fall är det dock tillrådligt att en ordentlig **utbildningsplan** görs och dokumenteras i skrift.

Ju mer personal som behöver utbildas desto viktigare blir en väl systematiserad planering. Den kan utgå exempelvis från en åtgärdslista av nedanstående slag. Listan bör kunna ge vägledning även i sådana fall, då utbildningsbehovet inte är så omfattande, eftersom den kan sägas representera ett antal ”logiska steg” i planeringsarbetet:

- Utgå från verksamhetens organisation och nuvarande eller planerat sätt att utnyttja IT-stöd i olika delverksamheter.
- Bedöm vilka IT-säkerhetskunskaper som kommer att behövas. Identifiera berörda avdelningar och personalgrupper (befattningar) och deras respektive behov av kunskaper. Detta kan definieras som behov av t.ex:
  - orienterande utbildning
  - allmänt fördjupad utbildning
  - fördjupad utbildning på vissa områden (t.ex. i anslutning till den egna arbetsuppgiften).
- Klarlägg nuvarande utbildningsläge. Bedöm olika personalgruppers (befattningars) nuvarande kunskaper i IT i allmänhet och i IT-säkerhetsfrågor. Sammanställ resultaten per personalgrupp, med samma kategoriindelning som gjordes beträffande behovet av kunskaper. Om kunskaperna inom en grupp bedöms som mycket ojämna kan man behöva dela upp den i flera ”utbildningsgrupper”, se nedan.
- Bedöm utbildningsbehovet. Jämför kunskapsnivån inom respektive personalgrupp med behovet. Gör med ledning av detta en indelning av utbildningsbehovet i ”utbildningsgrupper”. För varje grupp anges t.ex. vilken typ av utbildning som behövs, graden av förkunskaper, specialisering till delområden och ungefärligt antal personer som behöver utbildningen.

- Kartlägg interna och externa utbildningsresurser. Utred vilken egen utbildningskompetens som är tillgänglig, vilka externa utbildningsmöjligheter som finns inom de aktuella ämnesområdena, och vilka möjligheterna är att finansiera extern utbildning.
- Gör en grov utbildningsplan som anger utbildningsgrupper, ungefärligt antal personer i varje grupp, typ av utbildning, utbildningens längd, ungefärliga tidpunkter, utbildningsarrangör.
- Gör kostnadskalkyler och sök godkännande av planen på ansvarig nivå.
- Gör detaljerade planer.
- Genomför utbildningen.
- Följ upp. Dokumentera hur utbildningen fungerar och vilka brister som kvarstår.

9.4.3 Uppföljning och kontinuitet

Utbildning i IT-säkerhet får aldrig ses som ett engångsarbete. Det ligger i verksamhetsansvaret att fortlöpande kontrollera att kunskapsnivån är tillfredsställande. Man kan, som tidigare har påpekats, utgå från att grundutbildningen bör följas av regelbundet återkommande information. Ibland kan fortbildningskurser behövas.

Ett grundläggande syfte med fortlöpande information och utbildning är att hålla säkerhetsmedvetandet vid liv. Erfarenheten visar att säkerhetsmedvetandet är störst strax efter utbildning, eller efter det att en incident eller olycka inträffat, och att det därefter gradvis avtar.

Det kan vara svårt att upprätthålla säkerhetsmedvetandet enbart genom löpande skriftlig information. Ett bra komplement till denna kan därför vara att ibland samla personalen till kortare genomgångar, ”informationspass”. Ofta kan man förmodligen inte avsätta så mycket tid för sådana samlingar. De bör av effektivitetsskäl sannolikt vara av karaktären korta men intensiva och konkreta. De kan innehålla t.ex:

- kort genomgång av förändringar i hotbild, verksamhet och organisation som påverkar säkerhetsbedömningarna

- redovisning av inträffade incidenter
- diskussion av säkerhetsläget
- redovisning av nya och ändrade säkerhetsåtgärder
- repetition av säkerhetsåtgärder på sådana punkter där det visat sig att brister finns.

Vid samlingar av det här slaget är det också angeläget att personalen ges tillfälle att redovisa och diskutera problem och egna iakttagelser av brister i säkerheten.

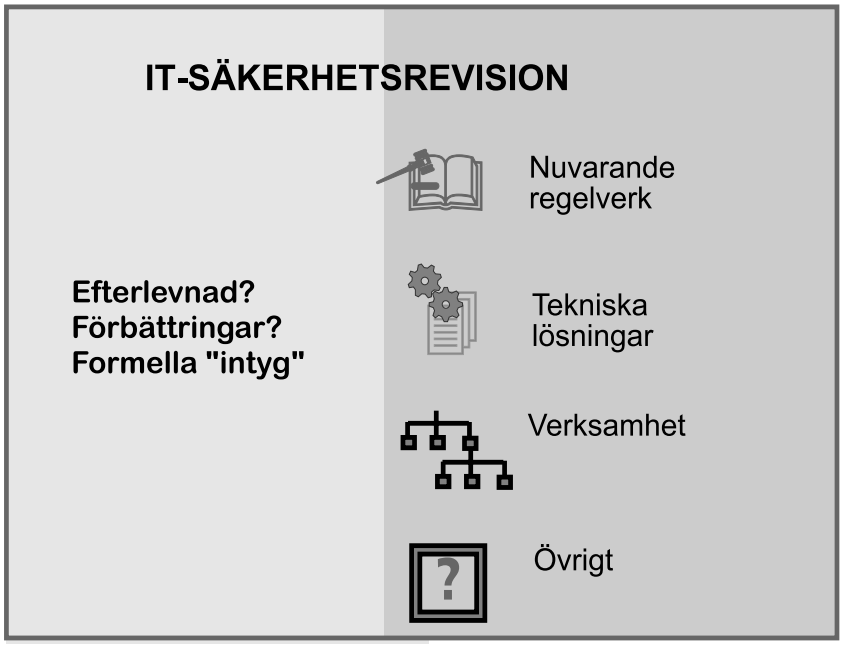
För att upprätthålla kunskaper och säkerhetsmedvetande är också, som tidigare sagts, återkommande praktiska övningar, t.ex. när det gäller brandberedskapen, av stor betydelse.

Kravet på kontinuitet i utbildningsplaneringen gäller under IT-systemets alla faser såsom utveckling, drift och förvaltning. Det har tidigare påpekats att personal som är engagerad i utvecklingen av IT-systemet behöver utbildning i IT-säkerhet. Utbildningsplaneringen för de människor som ska använda det nya systemet måste påbörjas redan på ett tidigt stadium av systemutvecklingen. Normalt behöver en väsentlig del av grundutbildningen vara gjord när ett nytt system tas i drift. Därefter krävs fortlöpande kontroll och omprövning av behovet.

10 IT-säkerhetsrevision, ackreditering

10.1 Vad är IT-säkerhetsrevision

Med IT-säkerhetsrevision menas en internt eller externt utförd genomgång av hur en organisations samlade IT-säkerhet hanteras. Revisionen innebär att man tittar på ungefär samma saker som beskrivits tidigare under avsnittet Risk- och sårbarhetsanalyser. Skillnaden ligger främst i att revisionen är mer granskande och värderande. Den syftar ofta till att primärt klarlägga verklig efterlevnad av gällande regler och anvisningar och verkligt utnyttjande av tekniska skyddsåtgärder etc. Det är från detta verkliga utgångsläge som man lämpligen gör en risk- eller sårbarhetsanalys.



Figur 8. IT-säkerhetsrevision.

Ackreditering kan ses som ett specialfall av IT-säkerhetsrevision.

Att ackreditera någon med avseende på IT-säkerhet kan ses som ett sätt att säkerställa att någon annan – en tilltänkt samverkansorganisation, leverantör, konsult eller annan typ av samverkanspart, i sin verksamhet uppfyller ställda krav på IT-säkerhet. Ett syfte med detta är förstås att inte utsätta den egna organisationen för en försvagning av den totala IT-säkerhet genom att man startar samarbete med en ny part.

Den analys som görs i samband med en ackreditering påminner även den till innehåll och uppläggning mycket om de egna risk- och sårbarhetsanalyser som behandlats ganska utförligt på annan plats i denna handbok. Skillnaden är att ackrediteringsaktiviteten utförs främst som en ren granskningss- och godkännandeprocedur. Om den visar oacceptabla brister leder det i princip enbart till att det tilltänkta samarbetet inte blir av – ackrediteringen uteblir!

Den säger kanske inte så mycket om orsakerna till och eventuella åtgärder för att överkomma klarlagda brister. Dessa förväntas istället den granskade organisationen själv åtgärda i sitt eget intresse. Detta sker genom ett metodiskt säkerhetsarbete såsom beskrivits på andra platser i denna handbok.

10.2 Hur ofta bör man genomföra en IT-säkerhetsrevision

IT-säkerhetsrevision bör genomföras regelbundet och repetitivt. För vissa organisationer kan det var motiverat att göra det i någon form minst ett par gånger per år. För andra kan det räcka med att göra det t.ex. vart annat år. Växlande scheman där man gör växelvis stora och mindre genomgångar kan också var lämpliga. Vid de små genomgångarna fokuseras speciellt sådant som man erfarenhetsmässigt vet är svaga punkter i den egna organisationen.

Externt initierad ackreditering kan var motiverad att genomföra i bl.a följande fall:

- När en överordnad organisation överväger att slå samman två organisationer.

- När en organisation vill påbörja ett fördjupat samarbete med en annan organisation.
- När en ny strategiskt viktig leverantör ska engageras.
- I samband med ett kvalitetscertifieringsarbete.

10.3 Vem genomför revisionen

En bärande tanke för både den internt och den externt initierade IT-säkerhetsrevisionen är att den ska utföras av någon som ansvars- och bedömningsmässigt kan vara så objektiv och saklig som möjligt – någon med oklanderlig integritet för uppgiften. Bedömningen ska verkligen kunna fungera som ett kvalitetsmått på hur väl den granskade organisationen ”står” vad avser sin IT-säkerhet. Det är viktigt att i förväg bestämma sig för vilken etik som ska gälla vad avser spridning av resultatet av granskningen. Vems är resultatet och hur ska detta hanteras, antaget att granskningen kan utfalla såväl positivt som negativt för den granskade organisationen.

En möjlig modell, speciellt vid externt initierad ackrediteringsgranskning är att man överenskommit om en tillåten ”åtgärdstid” under vilken brister ska ha rättats till. Detta innebär att granskningen som sådan i princip upprepas åtminstone två gånger.

Följande utgör exempel på organisationer som kan förväntas utföra en IT-säkerhetsrevision, med tillräcklig tyngd och bibehållen integritet:

- Organisationens egna säkerhetsfunktioner/IT-säkerhetsfunktioner.
- Större eller medelstora konsultföretag – ett krav ska vara att sådana konsultföretag har acceptabla kvalitetssystem för styrning av sitt konsultarbete. Detta bl.a för att säkerställa dokumentkvalitet och dokumentintegritet.
- Statliga, kommunala eller andra myndighetsbetonade tillsynsorganisationer, t.ex. RRV, Kommunala revisionsenheter etc.
- Försäkringsbolag, Certifieringsorganisationer m.fl.

10.4 Hur genomförs revisionen

Det är viktigt att IT-säkerhetsrevisionen utförs koncentrerat och distinkt. Det är just att fånga ett verkligt läge som är syftet med det hela. Därför finns det inget motiv att sträcka ut den över för lång tid. Detta eftersom det kan innebära att förändringar löpande sker under granskningens gång och man får till slut svårt att veta vad det är man värderar – är det nuläget eller läget som rådde då vi startade?

I en del fall kan det var möjligt att genomföra en vettig IT-säkerhetsrevision under en till två arbetsdagar. Under denna tid så intervjuar och granskar de ansvariga utredarna verksamheten. Någon form av fast mall som överenskommits i förväg ska alltid användas. Under någon ytterligare dag sammanställs resultaten och presenteras för ansvariga. I större organisationer med geografiskt och ansvarsmässigt utspridda verksamheter tar det normalt längre tid. Längre än två veckor ska man normalt dock aldrig hålla på. I så fall är det bättre att dela upp arbetet i olika granskningar med varierande omfattning.

Vid externt initierade revisioner kan det vara motiverat att också studera följande:

- andra externrelationer som den tilltänkta partnern har
- partnerns personalomsättning
- partnerns kvalitetssystem i stort
- etc.

Regelrätta intrångsförsök i en säkerhetsnod i den granskade organisationen, t.ex. en brandvägg, kan vara lämpliga inslag i en både internt som externt initierad säkerhetsrevision. Erfarenheter har visat att det kan vara relativt enkelt att slå ut en säkerhetsnod, t.ex. en brandväggsserver. Att däremot ta sig förbi den är betydligt svårare. Redan en ”lyckad” utslagningsattack (eng Denial-of-service-attack), kan dock i ett totalperspektiv vara en mycket allvarlig brist hos den tilltänkta partnern. T.ex. i den form att upprepad extern utslagning leder till att brandväggen temporärt kopplas ur, varvid organisationens interna nät ligger öppet för obehöriga.