STATSKONTORET 1997:29 a

Handbok i IT-säkerhet

Del I

Introduktion

Handbok i IT-säkerhet

Del I

Introduktion

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 91-7220-288-2

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 1

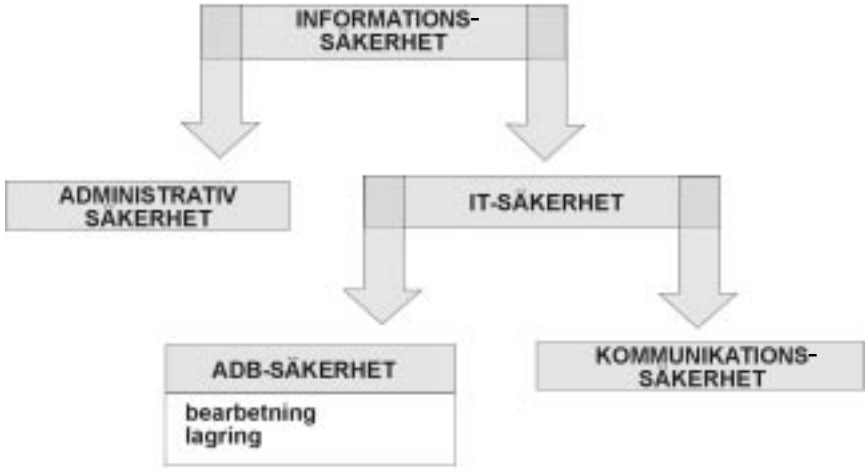
1 Introduktion

1.1 Allmänt

Informationssäkerhet inkluderar både traditionell datasäkerhet och säkerhet som är relaterad till hantering av information i olika verksamheter. Information är idag en viktig resurs för många organisationer. Om informationen inte hanteras på rätt sätt kan både verksamhetens mål och framtida fortlevnad äventyras.

Det är inte bara hemlig, känslig eller värdefull information som måste skyddas. Öppen information är oftast lika känslig vad gäller t.ex. obehörig förändring, d.v.s. att informationen blir felaktig. I många fall är det en kombination av olika skyddsåtgärder som behövs för att nå upp till önskad skyddsnivå.

Begreppet **IT-säkerhet** används för skyddsåtgärder som är av teknisk karaktär, t.ex. olika former av behörighetskontrollsystem. IT-säkerhet inkluderar både **ADB-säkerhet** och **kommunikationssäkerhet**. Med ADB-säkerhet eller ibland bara datasäkerhet menas säkerhet som rör själva behandlingen och/eller lagringen av data (program och information). Kommunikationssäkerhet avser säker-



Figur 1. Informationssäkerhetens omfattning.

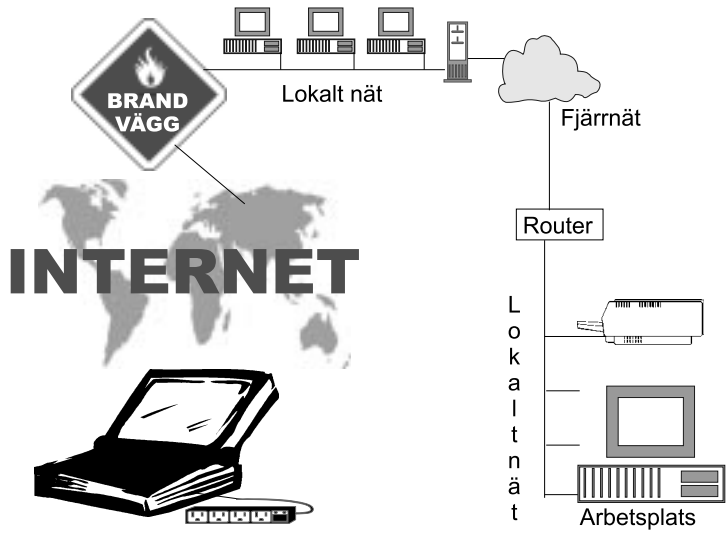
het vid överföring av data via något kommunikationsmedium. De tekniska skyddsåtgärderna måste i många fall kompletteras med **administrativ säkerhet** i olika former. Administrativ säkerhet innebär främst definiering av regler och rutiner för styrning och kontroll av IT-resurserna. Administrativ säkerhet kan alltså fungera som ett komplement till en teknisk skyddsåtgärd men också fungera som en skyddsåtgärd i sig.

1.1.1 IT-miljöer

I handboken identifieras ett antal **IT-miljöer**. Indelningen i IT-miljöer tillämpas främst i del 3, där vi identifierar hot och risker samt lämpliga skyddsåtgärder för respektive miljö.
IT-miljöerna är:

- **Arbetsplatsen**, t.ex. en PC eller en arbetsstation.
- **Lokalt nät**, gemensamma resurser som t.ex. servrar, nät, nät-applikationer och skrivare.
- **Fjärrnät**, t.ex. nät som kopplar samman två geografiskt spridda lokala nät inom samma organisation eller nät som kopplar samman olika organisationer.
- **Distansarbetsplats**, t.ex. användare som sitter hemma eller på annan ort och arbetar men som har tillgång till resurser i det lokala nätet, via modemförbindelse eller liknande.
- **Anslutning till Internet**, olika typer av anslutningar till Internet.
- **Informationsspridning via Internet**, t.ex. när man erbjuder tjänster i form av information till olika intressenter via Internet.
- **Meddelandehantering**, t.ex. formaliserad meddelande-överföring, som e-post och EDI.
- **Systemutveckling och Förvaltning**, t.ex. utveckling av nya system och vidareutveckling av befintliga system.

Syftet med uppdelningen i olika IT-miljöer är inte att respektive miljö ska behandlas som en isolerad företeelse. Tvärtom är det mycket viktigt att hantera hela organisationens IT-säkerhetsarbete som en helhet. Dagens system är hårt integrerade. Om ett hot inte hanteras med en lämplig skyddsåtgärd i en av IT-miljöerna kan detta påverka övriga IT-miljöers skyddsnivå.



Figur 2. IT-miljöer, från enskild arbetsplats till Internet.

2 Organisation, policy och ansvar

2.1 Krav

Kraven på IT-systemen ökar i takt med att användningen ökar. Användarna ställer högre krav på funktionalitet och säkerhet.

Krav på IT-säkerhet kommer från olika intressenter. Inom organisationen ställer bland andra ledningen och användarna krav. Andra intressenter som ställer krav på IT-säkerhet är allmänhet och andra externa intressenter som t.ex. leverantörer. Hanteringen av vissa typer av information kan dessutom påverkas av rättsliga krav. Detta beskrivs utförligare i del 2.

Kraven på IT-säkerhet formuleras olika i olika organisationer och verksamheter. Vi har valt att sammanfatta kraven på IT-säkerhet i fyra tillstånd:

- **Riktighet**
  Producerad information ska vara korrekt, aktuell och begriplig.
- **Tillgänglighet**
  IT-systemen ska vara tillgängliga för behöriga användare i beslutad omfattning på bestämda tider.
- **Sekretess**
  IT-systemets data/information och program skyddas så att de inte avsiktligt eller oavsiktligt görs tillgängliga eller avslöjas för obehöriga eller utnyttjas på ett otillåtet sätt.
- **Spårbarhet**
  Det ska finnas funktioner och rutiner som gör det möjligt att härleda alla operationer i IT-systemet till enskilda individer och program.

Dessa begrepp eller tillstånd används genomgående i denna handbok för att gruppera och identifiera hot, risker och lämpliga skyddsåtgärder.

2.2 Organisation och regelverk

2.2.1 Organisation och utbildning

Ledningen har alltid det övergripande ansvaret för IT-säkerheten. I övrigt bör IT-säkerhetsansvaret vara knutet till verksamhetsansvaret på alla nivåer inom organisationen. På grund av stora variationer vad gäller 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. Av samma skäl går det inte heller att fastställa en viss ”IT-säkerhetsorganisation” som kan gälla för alla organisationer.

Vanligt är dock att man inom organisationen utser en funktion som kan fungera som rådgivare och samordnare för IT-säkerheten. Specialkompetens krävs ofta för att kunna omsätta verksamhetens krav på IT-säkerhet i lämpliga säkerhetsåtgärder. Den samordnande funktionen bör representeras av en ”IT-säkerhetschef”.

IT-säkerhet bör ingå som en del i IT-organisationens ansvar. Ofta använder man ett antal ansvarsbegrepp när man definierar IT-organisationen och en IT-säkerhetsorganisation. De ansvarsbegrepp som definieras är:

- Verksamhetsansvar
- Systemägaransvar
- Informationsägare
- Systemansvar
- Egenansvar/Användaransvar
- Registeransvarig och offentlighetsansvarig
- IT-säkerhetsansvariga.

Ansvarsbegreppen behandlas utförligare i del 2, kapitel 5.

Användarnas förmåga att uppfylla det IT-säkerhetsansvar som åligger dem avgörs av vilken kompetens och kunskap de har. Främst är det rätt kompetens och kunskap vad gäller de egna arbetsuppgifterna som är nödvändig. Viktigt är att användarna har relevant kunskap vad gäller just IT-säkerhet. En hög arbetsmotivation krävs också för att upprätthålla en bra säkerhetsnivå. Missnöjda användare bör man betrakta som en säkerhetsrisk.

Nyanställda bör, så tidigt som möjligt, får ta del av de regler och riktlinjer som deras arbetsuppgifter berörs av. Vidare kan ytterligare (och eventuellt kontinuerlig) utbildning i IT-säkerhet, beroende på vilken typ av tjänst man har, vara nödvändig.

Vad som är rätt kunskap och kompetens förändras över tiden. Kontinuerlig kompetensuppbyggnad bidrar till en bra säkerhetsnivå och säkerhetsmedvetenhet.

I del 2, kapitel 9.2 diskuteras bland annat vilka personalkategorier som behöver utbildning i IT-säkerhet och vilket innehåll utbildningen lämpligen kan ha. Tänkbara personalkategorier som identifieras är:

- **Användare**, d.v.s. de använder IT-systemet i sitt dagliga arbete men har inget direkt ansvar för IT-säkerheten, förutom egenansvaret.
- **IT-personal**, d.v.s. personal som arbetar med t.ex. drift, systemutveckling och förvaltning.
- **Verksamhetsansvariga**, d.v.s. de som är ansvariga för en verksamhet eller ett system.
- **IT-säkerhetschef** och andra särskilt utsedda IT-säkerhetsfunktioner, d.v.s. funktioner som på olika sätt samordnar IT-säkerhetsarbetet inom en organisation.
- **Annan personal**, d.v.s. personal som inte direkt kommer i kontakt med IT-systemen i sitt arbete.
- **Ny personal**, d.v.s. nyanställda eller personer som byter arbetsuppgifter inom organisationen.
- **Tillfällig personal**, d.v.s. konsulter, examensarbetare o dyl.

Olika former för utbildning diskuteras också i del 2, kapitel 9.3 t.ex.:

- Kurser som erbjuds av externa företag.
- Interna, eventuellt skräddarsydda, kurser.
- Praktisk träning och erfarenhetsutbyte.
- Skriftlig information i olika former, t.ex. för kontinuerlig kompetensuppbyggnad.

Olika utbildningsaktiviteter ska ingå som en del i den kort- och långsiktiga planeringen av kompetensuppbyggnaden inom organisationen. Utbildningen kan vara av typen allmän orientering, fördjupad utbildning eller målinriktad utbildning för specifika arbetsuppgifter. Uppföljning och kontinuitet är väsentligt för att få fullgott utbyte av alla typer av utbildningsinsatser.

2.2.2 Policy och riktlinjer

Ett IT-system ska på bästa sätt stödja en organisations hantering av information. IT-systemet erbjuder olika möjligheter att lagra, bearbeta eller kommunicera information. Policy och riktlinjer ska styra:

- hur information hanteras och används i IT-systemet
- hur man hanterar och använder ingående resurser t.ex. applikationer och systemprogramvara.

En policy är ett långsiktigt dokument som fastställer den inriktning som ska gälla principiella frågor inom en organisation. En IT-säkerhetspolicy fastställer inriktningen som ska gälla IT-säkerhetsfrågor inom organisationen.

Riktlinjer har en mer konkret inriktning än policyn och ska garantera en enhetlig tillämpning av en viss policy inom organisationen. Riktlinjerna ska revideras i takt med verksamhetens inriktning och den tekniska utvecklingen. I del 2, kapitel 4 behandlas detta område utförligare.

2.2.3 Informationsklassning

Information som hanteras inom en organisation bör värderas. Värderingen baseras på känslighetsgraden och eventuella rättsliga krav, t.ex. datalagen och bokföringslagen.

Klassning av information utförs normalt av informationsägaren/systemägaren och är ett resultat av följande moment:

- **Avgränsning**
  Identifiera vital icke klassad information. Avgränsningen är viktig eftersom det inte finns något värde i att processen tar för lång tid. Information är ofta en färskvara.

- **Värdering**
  Värderingen av information ska baseras på de konsekvenser som kan uppstå i verksamheten om den utsätts för t.ex. obehörig åtkomst eller felaktig förändring.

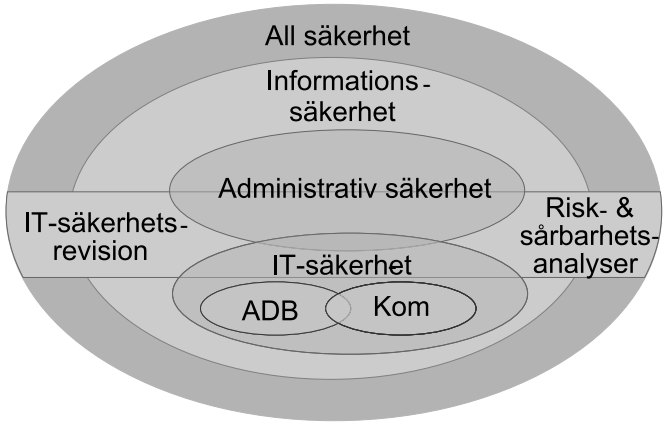
- **Klassning**
  Informationsägaren/systemägaren ansvarar för att **bedömning** och en **gradering** av informationen genomförs utifrån definierade regler, anvisningar samt gällande rättsliga krav.

- **Gradering**
  Graderingen baseras på olika informationsklasser till vilka skyddsåtgärder och riktlinjer kopplas.

Riktlinjerna för IT-säkerhet bör delas in i nivåer så att de anvisar vilka skyddsåtgärder som är kopplade till en viss klass.

2.3 Analys och revision

Känsligheten hos eller värdet av information som hanteras eller tjänster som erbjuds interna och externa intressenter är utgångspunkten. IT-säkerhetsarbetet bör ses som en integrerad del i den normala IT-verksamhets- och organisationsutvecklingsarbetet.
I del 2 behandlas rent administrativa skyddsåtgärder. Flera av dessa skyddsåtgärder omfattar även annan säkerhet än IT-säkerhet, till skillnad från de skyddsåtgärder som behandlas i del 3.



Figur 3. Analys och revision av säkerhetsfrågor.

Ett bra sätt att få reda på informationens och tjänsternas värde är att genomföra en sårbarhetsanalys där hotbilder och riskbedömning ingår. **Analyserna** omfattar ofta även **informationssäkerhetsfrågor**.

2.3.1 Risk- och sårbarhetsanalys

Risk- och sårbarhetsanalyser är metoder för att upptäcka brister samt fastställa konsekvenser av en oönskad händelse. I metoden ingår också att bedöma sannolikheten att händelsen ska inträffa samt att åsätta en kostnad om händelsen inträffar.

Risk- och sårbarhetsanalys är en av åtgärderna som ingår i säkerhetsarbetet. Nya system ska alltid genomgå en risk- och sårbarhetsanalys och befintliga system bör revideras regelbundet. Riskbedömningen ska vara **dokumenterad** och **signerad/godkänd** av systemägaren för alla IT-resurser.

I en risk- och sårbarhetsanalys ingår följande delar:

1. Beskriva hotbilder.
2. Kalkylera konsekvenser och skadekostnader.
3. Bedöma sannolikhet för att hoten ska inträffa.

Resultatet av analysen ska vara vägledande vid klassning av IT-resurser, t.ex. informationsklassning, som i sin tur leder till lämpliga skyddsåtgärder.

SBA-metoden (SårBarhetsAnalys) är ett lämpligt verktyg för att genomföra sårbarhetsanalyser och riskbedömningar.

SBA-metoden är ett resultat av ett samarbetsprojekt genomfört av näringsliv, stat och kommun. Metoden finns väl dokumenterad (även kurser) och kan användas inom alla verksamheter där IT ingår, se vidare del 2, kapitel 7.

2.3.2 IT-säkerhetsrevision

IT-säkerhetsrevision innebär att man utifrån en förutbestämd modell tar en ögonblicksbild av IT-säkerheten i en viss organisation eller del av denna. Revisionen syftar till att ge en verklig bild av IT-

säkerheten i verksamheten. IT-säkerhetsrevisioner bör genomföras regelbundet, t.ex. en gång om året, och stickprov kan genomföras ännu oftare.

En IT-säkerhetsrevision kan visa på att:

- befintliga skyddsåtgärder inte används
- befintliga skyddsåtgärder inte är tillräckliga och att man måste genomföra en risk- och sårbarhetsanalys för att kunna definiera vilka skyddsåtgärder man måste komplettera med.

2.4 Avbrottsplanering

Hur ska en verksamhet fungera vid kortare eller längre avbrott i IT-systemen? Varje organisation bör ha en avbrottsplanering som inkluderar riktlinjer för hur man ska kunna tillgodose verksamhetens informations-, kommunikations- och bearbetningsbehov vid avbrott i IT-systemen. Konsekvenser och kostnader av kortare och längre avbrott bör vägas mot kostnader för utökade skyddsåtgärder och olika reservdriftalternativ.

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

- skador uppstår i lokala nätverk, PC, hubbar, switchar, routrar m.m.
- lagrade data (register och databaser) har förstörts
- säkerhetskopior inte går att använda eller saknas
- viss känslig personalkategori (t.ex. driftpersonal, registreringspersonal) tas ut i strejk eller av annan anledning inte finns tillgänglig.

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.

Ledningen har det övergripande ansvaret för avbrottsplaneringen. I större organisationer bör det finnas en samordnande funktion som ansvarar för att avbrottsplaneringen görs enligt definierade riktlinjer och på ett enhetligt sätt i hela organisationen. På verksamhetsnivå är det verksamhets- och systemansvariga som ansvarar för att verksamheten även fungerar vid avbrott.

En avbrottsplan bör baseras på någon typ av risk- och sårbarhetsanalys som visar på riskerna i systemen samt vilka konsekvenser eventuella avbrott har på verksamheten. Avbrottsplanen arbetas sedan fram utifrån en värdering av konsekvenserna på verksamheten. Avbrottsplanen bör testas och revideras årligen eftersom hoten och riskerna ständigt förändras.

Vem som ska göra vad vid korta eller långa avbrott måste vara klart definierat, d.v.s. en organisation måste finnas som hanterar situationen och vidtar nödvändiga åtgärder. Vid avbrott med lindriga konsekvenser kan de flesta problem hanteras inom den ordinarie drift- och förvaltningsorganisationen. Hela den organisation som ska hantera avbrott bör finnas beskriven i avbrottsplanen. Personerna som ingår ska vara namngivna tillsammans med de funktioner som de ansvarar för. Ibland kan det vara nödvändigt att utforma en specifik avbrottsplan för användarna.

För olika verksamheter kan olika reservdriftalternativ vara aktuella. I del 2, kapitel 8.8 identifieras olika alternativ för stordatormiljöer, nätverk och fristående persondatorer.

3 Skyddsåtgärder

3.1 Hot och risker

För att kunna införa effektiv IT-säkerhet, antingen för en enskild IT-resurs eller för hela organisationen, är det nödvändigt att känna till vilka hot som finns mot systemet, vilka svagheter systemet har och hur sårbart det är. Denna kunskap är nödvändig för att kunna välja de mest relevanta och kostnadseffektiva säkerhetsåtgärderna.

- **Ett hot** är en handling eller händelse som kan komma att skada en IT-resurs, t.ex. information eller en applikation.
- **Sårbarhet** är en punkt där ett hot kan skada systemet. Sårbarhet är således **en svaghet** som ett hot kan utnyttja för att åstadkomma skada.
- **Risk** är sannolikheten för att hotet ska realiseras.

3.1.1 Hot

Hoten kan komma från olika håll. Till exempel:

- olyckor, hårdvaruhaveri, programvaruhaveri och miljöfaror
- obehörig användning av behörig personal
- obehörig användning av obehöriga personer som skaffar sig åtkomst till systemet via obehöriga metoder.

Begreppsmässigt kan hoten struktureras i följande tre grupper:

- Logiska hot, d.v.s. hot mot IT-resurser, funktioner och tjänster.
- Administrativa hot, d.v.s. hot mot administrativa rutiner och organisatoriska lösningar.
- Fysiska hot, d.v.s. skadegörelse, miljöpåverkan eller stöld. Dessa hot behandlas inte i någon större utsträckning i denna handbok. I del 3, kapitel 13 behandlas fysiskt skydd övergripande.

Exempel på **logiska hot** är:

- *Inloggning under falsk identitet.* Obehöriga användare eller ett obehörigt program loggar in under falsk identitet eller kringgår autenticeringsfunktionen (se vidare 3.2.2.2).
- *Avsaknad av möjligheter att spåra och bevisa obehöriga handlingar*. Användare förnekar att de har skickat eller mottagit ett meddelande eller orsakat en handling.
- *Obehörig åtkomst.* En behörig användare (intern eller extern) lyckas gå förbi reglerna för åtkomstkontroll, t.ex. genom att åtkomstkontrollistan modifieras.
- *Avlyssning eller informationsläckage.* Att obehöriga användare avlyssnar kommunikationen mellan två parter. Obehörig insyn kan också uppstå när en annan användare än avsedd mottagare avsiktligt eller oavsiktligt får tillgång till ett meddelande eller andra informationsmängder.
- *Trafikanalys.* Obehöriga kan iaktta kommunikationsmönster och utifrån detta dra vissa slutsatser vad gäller innehåll och kommunikationsfrekvens.
- *Dålig tillgänglighet*. I detta fall hindras en behörig användare att utföra funktioner. Dålig tillgänglighet kan uppstå t.ex. om obehöriga hindrar viss trafik från att komma fram eller att man genererar överflödig trafik som förhindrar fullgod tillgång till kommunikationsresurserna.
- *Modifiering/tillägg/borttag av information*. Avsiktlig eller oavsiktlig modifiering, tillägg eller radering av meddelanden, data eller program i databaser eller vid överföring.
- *Modifiering/tillägg/radering i program*. I olika datavirus ingår ofta någon typ av illasinnad funktion.

Exempel på **administrativa hot** är:

- *Brister och oklarheter i roll- och ansvarsfördelning*. Exempelvis kan ledningen ha missat att definiera eller på ett felaktigt sätt definierat vissa nyckelroller som är väsentliga för samordningen och realiseringen av IT-säkerheten.

- *Avsaknad av relevanta riktlinjer och rutiner* vad gäller:
  - säkerhetsadministration
  - inköp av programvara
  - kontroll av program- och maskinvara
  - installation
  - drift och underhåll.

3.2 Skyddsåtgärder

Här identifieras ett antal olika skyddsåtgärder. Vi redogör för skyddsåtgärder som är av mer teknisk karaktär samt eventuella administrativa rutiner som stödjer dessa.

Skyddsåtgärder kan delas in i två kategorier:

- **Administrativa skyddsåtgärder**, d.v.s. regler eller rutiner för vilka arbetsmoment som måste genomföras och hur.
- **Logiska skyddsåtgärder**, d.v.s. skyddsåtgärder av teknisk karaktär i form av maskin- och/eller programvara.

Skyddsåtgärderna måste användas för att möta ett speciellt hot. Dessutom kan vissa skyddsåtgärder möta fler än ett hot. Vissa hot bekämpas effektivare genom att flera skyddsåtgärder samverkar.

En del av svårigheterna med IT-säkerhet är att välja en kombination av skyddsåtgärder som är kostnadseffektiv, användbar, effektiv, kompatibel och som därtill möter de förväntade hoten i önskad grad.

Skyddets styrka är av vital betydelse när man ska bestämma vilket skydd som tillfredsställer säkerhetsbehovet. Skyddsåtgärdernas styrka bestäms av två faktorer:

- I vilken utsträckning skyddsåtgärderna möter de identifierade hoten.
- Skyddsåtgärdens pålitlighet, d.v.s. skyddsåtgärdens effektivitet och livslängd.

Skyddsåtgärder kan sättas in på olika sätt t.ex. för att förebygga, upptäcka och varna för hot eller för att återställa följderna av skadan. Att **förebygga** ett hot är den bästa strategin. Det innebär att hotet inte kan utnyttja en sårbarhet. I vissa lägen är det inte möjligt att förebygga. Skyddsåtgärden kan då **rapportera** skadan samtidigt eller omedelbart efter det att skadan inträffat. Det kan också finnas skyddsåtgärder som har funktioner för att återställa eller **begränsa** delar eller samtliga följder av hotet efter det att det inträffat.

Kostnaden för en skyddsåtgärd är dels den direkta kostnaden, d.v.s. en engångskostnad för att anskaffa skyddsåtgärden och dels de kontinuerliga kostnaderna för underhåll och administration.

En utförligare redogörelse av de skyddsåtgärder som beskrivs i följande avsnitt finns i del 3, kapitel 4.

3.2.1 Administrativa skyddsåtgärder

I del 2 behandlas rena administrativa skyddsåtgärder, d.v.s. IT-säkerhetspolicy och riktlinjer, organisation, utbildning, analyser av olika slag o.s.v.

I del 3 behandlas de administrativa skyddsåtgärder som är knutna till driften eller specifika IT-säkerhetskomponenter. Exempel på administrativa skyddsåtgärder som tas upp i del 3 är riktlinjer och rutiner för:

- systemutveckling och förvaltning
- installation och konfiguration
- specifika säkerhetskomponenter
- behörighetsadministration
- återanvändning av lagringsmedia.

De administrativa skyddsåtgärderna är minst lika viktiga som de tekniska. Vilken nytta gör t.ex. ett behörighetskontrollsystem om det inte finns en tydlig ansvarsfördelning vad gäller hur och vilka nya användare som får läggas till och uppdateras?

3.2.2 Logiska skyddsåtgärder

3.2.2.1 Kryptering

Kryptering är en kraftfull mekanism i IT-säkerhetssammanhang. Traditionellt förknippar man kryptering med insynsskydd, d.v.s. en informationsmängd bearbetas på ett sådant sätt att den endast är läslig för behöriga. Kryptering i olika former kan dock användas för att uppfylla andra krav på säkerhet. I del 3, kapitel 4.3 beskrivs två olika krypteringstekniker; symmetrisk kryptering och asymmetrisk kryptering. Vidare behandlas två tekniker för att utnyttja kryptering i syfte att nå andra säkerhetsfunktioner än insynsskydd (sekretess), t.ex. riktighet och spårbarhet.

Kryptografiska kontrollsummor är en säkerhetsfunktion som använder kryptering. Funktionen erbjuder möjligheter att i efterhand kontrollera att en informationsmängd inte har förändrats av någon obehörig, under lagring eller överföring.

Digitala signaturer är ett sätt att skapa elektroniska underskrifter. Upphovsmannen signerar en informationsmängd på ett sätt som bara han/hon kan. Senare kan signaturen verifieras, vilket innebär att man kan kontrollera informationsmängdens äkthet med avseende på innehåll och ursprung (upphovsmannens identitet).

3.2.2.2 BKS

Ett behörighetskontrollsystem (BKS) består av tre komponenter:

- *identifiering och autenticering*
- *åtkomstkontroll*
- *loggning.*

Vid *identifiering* anger användaren vem hon/han är med hjälp av en unik identitet. Identiteten kan vara unik i just den applikationen eller i hela IT-systemet. Systemen nöjer sig vanligtvis inte bara med en identifiering utan vill på något sätt *autenticera*/verifiera identiteten också, d.v.s. kontrollera att det verkligen är Kalle som är Kalle och inte Pelle som obehörigt utger sig för att vara Kalle. Den vanligaste metoden för autenticering är enkla lösenord. Varje användare tilldelas ett lösenord som han/hon byter med jämna mellanrum. Den unika identiteten kan vara öppen information medan lösenordet

måste hållas hemligt. Andra metoder är engångslösenord, d.v.s. lösenordet används endast en gång eller vid ett specifikt tillfälle.

Korrekt identifiering och autenticering är grundläggande i alla säkerhetskomponenter. Om en användare har lyckats kringgå autenticeringsfunktionen kan andra säkerhetsfunktioner förlora i styrka, t.ex. funktioner för åtkomstkontroll och loggning. Åtkomstkontrollen baseras ju på en identifierad användare, liksom loggning. För om man inte kan lita på identifierings- och autenticeringsfunktionen kan man heller inte begränsa åtkomsten till resurser på ett korrekt sätt eller bevisa något med loggfunktionen.

Åtkomstkontrollen i ett BKS reglerar tillgången till olika resurser i ett IT-system. Åtkomstkontrollen kan definieras på både användar- och rollnivå. Olika rättigheter som man definierar är t.ex. läs-, skriv-, exekverings-, borttags- och tilläggsrättigheter.

Loggfunktionen i ett BKS är till för att registrera och rapportera händelser i systemet, t.ex. försök till obehörig inloggning. Vilka händelser som ska loggas definierar man i enlighet med de riktlinjer som finns för loggning. En loggfunktion bör innehålla verktyg för att administrera och analysera loggar.

3.2.2.3 Aktiva kort

Aktiva kort är kort i kreditkortsformat med ett litet chip inmonterat. Chipet är i sig en liten dator med processor, minne och I/O (gränssnitt mot omvärlden). Kortet kan lagra mer information än ett magnetkort och har dessutom möjligheten att utföra bearbetningar på kortet med hjälp av den inbyggda processorn. Denna möjlighet medför att det aktiva kortet är attraktivt i olika säkerhetstillämpningar.

Det aktiva kortet kan ingå som en viktig och framförallt säkerhetshöjande komponent när det gäller:

- **Identifiering och Autenticering –** verifiering av en identitet mot en målmiljö genom kryptografiska metoder, där krypteringen görs på kortet.
- **Digital signatur** – kan göras på kortet och krypteringsnyckeln behöver aldrig lämna kortet.

- **Kryptering** – bearbetningen kan göras på kortet eller med hjälp av nycklar som lagras på kortet.
- **Lagring av information** – hemlig eller känslig information kan lagras på kortet, t.ex. krypteringsnycklar och lösenord.

3.2.2.4 Brandvägg

Brandväggar förekommer oftast i samband med anslutning och informationsspridning via Internet. Brandväggar kan också användas för att kontrollera trafiken mellan andra nätverk, t.ex. två lokala nät inom en organisation.

Idag finns ett antal olika typer av brandväggar, allt från ett ”enkelt” paketfilter, som släpper igenom eller blockerar trafik beroende på information i transportprotokollen, till avancerade applikationsgateways som analyserar applikationsprotokollen. De komponenter som ingår i en brandväggsfunktion är oftast routerutrustningar samt specialanpassade datorer.

I brandväggen bör det finnas funktioner för övervakning. Övervakningen kan ske med hjälp av en loggfunktion. Loggfunktionen bör kunna logga både normal och otillåten trafik. Den bör även innehålla verktyg för att kunna analysera loggarna samt möjligheter att koppla larm till trafik som indikerar säkerhetsöverträdelser.

3.2.2.5 Säkerhetskopiering

Säkerhetskopiering kan i dagens IT-miljöer vara komplicerat, speciellt om användarna sitter spridda geografiskt. Det finns dock kraftfulla verktyg som underlättar säkerhetskopiering av information som lagras på gemensamma servrar. Verktygen innehåller också ofta funktioner för säkerhetskopiering av de lokala arbetsplatserna.

Det finns dock ett antal olika aspekter som man måste ta hänsyn till eftersom säkerhetskopiering av lokala arbetsplatser kan vara mycket tidskrävande och medföra stor resursåtgång:

- Ska användarna själva få ansvara för lokalt lagrad information och programvara eller ska säkerhetskopior tas på de lokala arbetsplatserna?

- Vilken information lagras lokalt? Skulle den informationen kunna lagras centralt?
- Är det möjligt att ta säkerhetskopior av de lokala arbetsplatserna med tanke på administrationskostnaderna?
- Vad behöver användarna veta om säkerhetskopiering? Exempelvis bör användarna ha fått information om vad som säkerhetskopieras och när det görs.

Användare som arbetar på distans, antingen i hemmet eller på annan ort (s.k. mobila användare) måste informeras om gällande rutiner och regler för säkerhetskopiering. Mobila användare har i många fall ingen möjlighet att lagra informationen centralt på en server. För dessa användare bör det finnas rutiner för hur och när information och program på deras bärbara datorer ska säkerhetskopieras.

3.2.2.6 Virusskydd

För att skydda den egna organisationens resurser och externa informationsmottagare bör man använda virusskydd i sin interna datormiljö. Virusskydd bör ha funktioner för:

- att förebygga smitta
- att upptäcka ett smittat program och då förhindra smittspridning
- att återställa ett smittat system.

En grundregel vid planeringen av virusskydd är att försöka stoppa dataviruset så tidigt som möjligt innan vidare spridning och skada hinner ske. I del 3, kapitel 4.8 behandlas exempel på:

- olika typer av förebyggande skydd
- hur man kan upptäcka virussmitta
- vad man vidtar för åtgärder vid smitta.

Vi identifierar också tre typer av programvaror för virusskydd som i viss mån arbetar i olika IT-miljöer:

- Brandväggsbaserade virusskydd

- Serverbaserade virusskydd
- Arbetsplatsbaserade virusskydd.

Om man inte har egen kompetens när det gäller virusbekämpning bör man omedelbart ta kontakt med extern expertis då smitta konstaterats. Maskin- och/eller programvaruleverantören bör kunna bistå eller i vart fall hänvisa till någon expert på området. Oberoende av om saneringen av systemet ska göras med egna resurser eller med hjälp av extern expertis är arbetsgången densamma.

3.3 Skyddsåtgärder i olika IT-miljöer

I denna handbok har ett antal IT-miljöer identifierats. I del 3 behandlas respektive miljö utförligt. Framställningarna av respektive IT-miljö baseras på kraven på riktighet, tillgänglighet, sekretess och spårbarhet. För varje krav identifieras ett antal skyddsåtgärder som kan tillgodose olika skyddsnivåer. I följande avsnitt sammanfattas de kapitel i del 3 som behandlar skyddsåtgärder för olika IT-miljöer.

3.3.1 Arbetsplats

Kapitlet 3.3.1 i del 3 behandlar vi arbetsplatser som är anslutna till ett nät eller fristående arbetsplatser. Arbetsplatserna innehåller idag så pass mycket resurser att de ofta är ett utmärkt verktyg för att utnyttja svagheter i IT-system. Ofta saknas det lokala BKS på arbetsplatserna och detta innebär att t.ex. säkerheten i servrar kan undermineras eftersom hemlig information kan hämtas ut från den skyddade servern och läggas oskyddat på disk i arbetsplatsen.

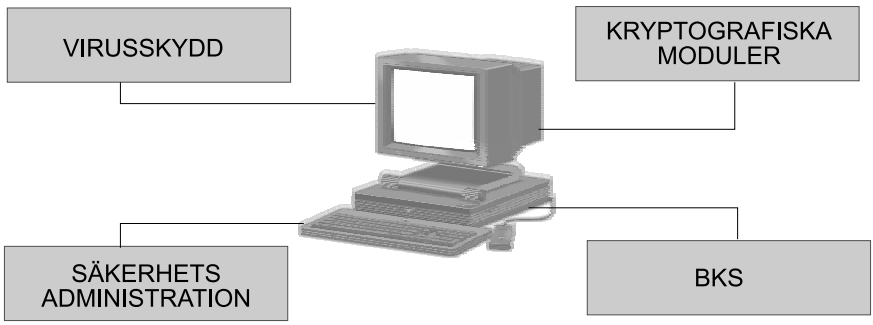
Arbetsplatserna befinner sig oftast i relativt öppna miljöer, till skillnad från servrar som ofta är inlåsta i speciella rum, dit endast driftpersonal har tillträde. För distansarbetsplatser och bärbara datorer kan miljöerna variera.

Arbetsplatserna är i många fall mycket lättillgängliga för obehöriga. De skyddsåtgärder som bl.a. diskuteras i del 3, kapitel 5 är:

- Ett lokalt BKS kan öka skyddsnivån på den lokala arbetsplatsen väsentligt. Ett BKS kan förhindra obehörig åtkomst till arbetsplatsen och dess lokala resurser.
- Bärbara datorer är attraktiva stöldobjekt och även om man har ett BKS installerat kan obehöriga användare komma åt lokalt lagrad information genom att läsa den direkt från disken. För att möta kraven på bl.a. sekretess även på de bärbara datorerna bör man tillämpa någon typ av *diskkryptering*.

Arbetsplatser är i de flesta fallen kopplade till t.ex. ett lokalt nät. Användaren kan vid sin lokala arbetsplats få tillgång till gemensamma resurser via nätet. Vid val av produkter och komponenter för att säkra arbetsplatsen bör man vara medveten om vilka säkerhetskrav som finns på andra resurser i nätet. Säkerhetsarkitekturen på arbetsplatsen bör stämma överens med övrig säkerhetsarkitektur. Viktiga komponenter i en säker arbetsplats är:

- virusskydd,
- BKS,
- säkerhetsadministration och
- kryptografiska moduler.



Figur 4. Skyddsåtgärder vid arbetsplatsen.

3.3.2 Lokalt nät

Lokala nät finns i de flesta organisationer. Nätet underlättar delning av gemensamma resurser.

I stora organisationer kopplar man ofta ihop flera lokala nät. Ur säkerhetssynvinkel försvårar detta möjligheterna att kontrollera säkerheten i det lokala nätet. Finns det svagheter i något av de lokala näten, t.ex. en icke säkrad modemförbindelse till Internet, påverkar denna säkerhetsrisk övriga lokala nät. Innan två nät kopplas ihop bör man därför komma överens om en gemensam säkerhetspolicy och befintlig säkerhet bör analyseras. Om skillnader råder mellan näten måste åtgärder vidtas innan man kan koppla ihop sig.

Ett vanligt säkerhetsproblem i miljöer med många olika applikationer och måldatorer är att användarna ofta har ett flertal olika användaridentiteter och lösenord att hålla reda på. Många användare börjar då skriva ner sina lösenord i anslutning till arbetsplatsen eller använder samma lösenord mot många/alla applikationer och måldatorer. Idag finns det färdiga produkter som hanterar denna problematik. Koncepten bygger oftast på att man loggar in på en s.k. autenticeringsserver. Denna server hanterar sedan all övrig inloggning till applikationer och måldatorer.

Elektronisk post är en nätapplikation som idag finns i de flesta organisationer och underlättar informationsspridningen inom och mellan organisationer. Viktigt är dock att inse att informationen som sprids kan vara öppen, hemlig eller känslig och bör skyddas på lämpligt sätt. Idag finns det endast ett fåtal applikationer för elektronisk post som har funktioner för säkerhet. Användningen av elektronisk post bör därför ske med omdöme. Det är t.ex. relativt enkelt att manipulera med avsändaradressen och i och med detta kunna utge sig för att vara någon annan.

En stordator behandlas i denna handbok som en vanlig server i det lokala nätverket. Ur säkerhetssynpunkt bör man också behandla den som det. Mot stordatorn ansluter man terminaler eller andra arbetsplatser som fungerar som terminalemulatorer. Terminaler förekommer dock i allt mindre utsträckning eftersom det finns behov av att använda arbetsplatsen för andra ändamål i t.ex. klient/server-applikationer. Användarna har därför möjligheter att från

stordatorn ladda ner information och lagra den lokalt eller sprida den till andra system. Detta är ju något som inte var möjligt med terminaler.

I del 3, kapitel 6 behandlas det lokala nätet i sin helhet, d.v.s. servrar, nät, nätapplikationer, kringutrustning. I ett lokalt nät är t.ex. administrativa skyddsåtgärderna mycket viktiga och rutiner behövs för t.ex.:

- systemadministration
- installation och konfiguration
- loggning
- behörighetstilldelning
- säkerhetskopiering
- avbrottsplanering
- o.s.v.

Andra skyddsåtgärder som behandlas är behovet av kryptering, starkare autenticering än vanliga lösenord, virusskydd, åtkomstkontroll o.s.v.

3.3.3 Fjärrförbindelser

Fjärrnät innebär datakommunikation över fjärrförbindelser som är fasta eller uppringda. Vid anslutning till och användning av olika fjärrnät måste man hitta rätt gränssnitt mellan sin egen verksamhet och den eventuella leverantören av fjärrnätstjänsten. Det är viktigt att man klart definierar vem som ansvarar för vad. Ett avtal ska skrivas med företaget som tillhandahåller fjärrförbindelsen. Avtalet bör bl.a. innehålla riktlinjer vad gäller kraven på säkerhetsnivå, tjänstens tillgänglighet och krav på kvaliteten på överförd information.

Kopplar man ihop lokala nätverk över fjärrförbindelser bör man i förväg ha kommit överens om en gemensam säkerhetspolicy.

I del 3, kapitel 7 behandlas området fjärrnät. Bland annat diskuteras behov av och möjliga lösningar vad gäller:

- nätövervakning
- BKS
- loggning
- kryptering
- skydd av kopplingspunkter
- o.s.v.

Området har många gemensamma nämnare med området Anslutning till Internet (se 3.3.5).

3.3.4 Distansarbete

Distansarbete och s.k. mobila användare blir allt vanligare. Användarna ställer krav på en flexiblare arbetssituation. Ett av kraven är att det ska finnas möjligheter att arbeta i hemmet under liknande förutsättningar som på den ordinarie arbetsplatsen. Detta innebär att distansanvändaren minst måste ha tillgång till resurserna som ligger på det lokala nätet.

Mobila användare är användare som t.ex. reser mycket i sitt arbete och därför ofta bär med sig sin dator. Från olika platser har användaren möjlighet att koppla upp sig mot det egna lokala nätet.

I del 3, kapitel 8 behandlas skyddsåtgärder för mobila arbetsplatser och distansarbetsplatser. Viktiga skyddsåtgärder är bl.a.:

- Ett BKS på arbetsplatsen som skyddar mot obehörig användning av arbetsplatsen samt medveten eller omedveten förändring av lokalt lagrad information eller andra resurser.

- Rutiner för säkerhetskopiering som är extra viktigt för mobila användare eftersom de oftast inte har möjlighet att lagra information centralt i det lokala nätet.

- Kryptering av lokalt lagrad information som är speciellt viktigt på mobila arbetsplatser. Det är relativt enkelt att stjäla en bärbar dator och även om det finns ett BKS installerat kan man få tillgång till lokalt lagrad information genom att läsa den direkt från minnesenheten.

3.3.5 Anslutning till Internet

Brandväggar är en säkerhetsfunktion som man ofta förknippar med anslutningar till Internet. En brandvägg kan dock vara minst lika viktig vid anslutning till andra fjärrnät eller andra lokala nät. Olika brandväggar innehåller dessutom olika mycket funktionalitet. Det kan därför vara nödvändigt att utöka skyddet i anslutningen, t.ex. med komponenter för starkare autenticering av användare och viruskontroller av inkommande och utgående trafik.

Många ser möjligheter med Internet, både kommersiella och icke kommersiella. Möjligheterna omformas och nya tillämpningar och protokoll dyker ständigt upp. Detta innebär också att hotbilden blir allt mer komplex. Nya protokoll medför nya möjligheter att utnyttja brister. Vid anslutning till Internet måste man alltså dels skydda sig mot alla kända hot och risker i kommunikations- och applikationsprotokoll och dels skydda sig mot nya hot och risker som eventuellt kan uppstå.

I del 3, kapitel 9 behandlas viktiga säkerhetsaspekter och lösningsalternativ vad gäller en anslutning till Internet. Det är t.ex. viktigt att:

- användarna förstår riskerna med användning av Internet
- det finns funktioner som ytterligare kan identifiera och autenticera användare som vill komma åt lokala resurser från Internet
- det finns logg- och larmfunktioner som kan hantera onormala händelser eller hot
- det finns funktioner för viruskontroll, av t.ex. bilagor till e-post, i själva anslutningen eftersom man annars riskerar att smitta den lokala miljön
- brandväggen är rätt konfigurerad
- åtkomst till det lokala nätet endast får ske via en brandvägg.

3.3.6 Informationsspridning via Internet

Internet gör det möjligt att effektivt sprida information till allmänhet och andra intressenter. Säkerhetsaspekten är dock väsentlig, för

har man inte kontroll över anslutningen kan avgiften till operatören vara den lilla kostnaden i sammanhanget. Erbjuder man en tjänst via t.ex. en web-server eller ftp-server måste man kunna garantera riktigheten hos tjänsten och informationen.

En web-server måste uppdateras kontinuerligt med hjälp av ett antal olika applikationer som hämtar och lämnar information i en informationsdatabas. Detta innebär att det är minst tre grupper av resurser som måste skyddas:

- web-servern
- informationsdatabaser samt
- applikationer.

I del 3, kapitel 10 diskuteras olika skydd. En rätt konfigurerad brandvägg är en av skyddsåtgärderna. Ett BKS är också en viktig skyddsåtgärd bland annat för att skydda informationen och applikationerna från obehörig förändring. Erbjuder man andra tjänster, t.ex. försäljningstjänster behöver man ytterligare säkerhetshöjande åtgärder vad gäller identifiering och autenticering av användare.

3.3.7 Meddelandehantering

Elektronisk post och EDI (Electronic Data Interchange) är två exempel på meddelandehanteringssystem. Elektronisk post används i allt större utsträckning för att sprida information, inom och utanför organisationer. EDI används oftast för applikationer där själva innehållet i meddelandet går att standardisera, t.ex. i samband med handel eller beställningar. Innehållet i dessa meddelanden eller ibland även dess existens kan behöva skyddas på olika sätt. Värdet av ett meddelande bör vägas mot de hot och risker som finns vid överföringen. Meddelandehanteringssystemen bör sedan utökas med säkerhetsfunktioner i lämplig omfattning. I del 3, kapitel 11 behandlas olika skyddsåtgärder bl.a.:

- kryptering för insynsskydd, sekretess
- digitala signaturer för att kunna verifiera avsändaren och innehållet
- asymmetrisk kryptering för att kunna garantera att det är endast är rätt mottagare som kan få tillgång till innehållet i meddelandet.

3.3.8 Systemutveckling och förvaltning

Ett strukturerat arbetssätt med hjälp av modeller och metoder är i huvudsak de skyddsåtgärder som bör användas vid systemutveckling. Andra viktiga frågor som bör beaktas vid systemutveckling är:

- att undvika situationer där man måste lita på nyckelpersoner. I stället bör kompetensen breddas.
- att missnöjd personal kan vilja åsamka företaget skada. Vid systemutveckling och förvaltning finns det ypperliga tillfällen att plantera in illasinnad kod i för övrigt korrekta applikationer.

I del 3, kapitel 12 beskrivs systemutveckling noggrant i ett antal steg:

- Verksamhets- och informationsanalys, som med tanke på behovet av avstämning och beslut under arbetets gång kan delas i:
  - föranalys, under vilken den ursprungliga idén ges en sådan substans att man kan fatta beslut om hur och på vilket sätt man ska gå vidare med projektet
  - detaljanalys, som ska ge erforderliga detaljer och underlag för den egentliga systemutformningen och konstruktionen.
- Systemutformning/systemkonstruktion, som även innefattar tester, inklusive ett slutligt produktionstest, fram till färdigt produktionssystem.
- Införande, som ska föregås av ett formellt godkännande från beställaren.

När nya applikationer utvecklas, gamla vidareutvecklas eller förändras bör man på ett tidigt stadium ta hänsyn till den säkerhetsproblematik som berör applikationen eller kopplingen till andra applikationer. De förslag som man tar fram bör följa de inom organisationen föreslagna riktlinjerna för IT-säkerhet.

3.4 Standarder

Inom IT-säkerhetsområdet och angränsande tekniker som t.ex. aktiva kort pågår ett aktivt standardiseringsarbete.

Standarder, inte bara IT-säkerhetsstandarder, är ett viktigt medel för att kunna uppnå och bibehålla en relevant säkerhetsnivå. Vid val av produkter och lösningar bör man vara uppmärksam på i viken utsträckning de stödjer relevanta standarder eller ”de facto”-standarder. Att följa standarder innebär för det mesta:

- längre livslängd på produkter och lösningar
- kompatibilitet med gamla eller nya produkter och lösningar
- genomtänkta produkter och lösningar
- öppna lösningar
- mindre leverantörsberoende.

I del 3, kapitel 14 behandlas ett antal olika standardiseringsorgan som är relevanta för standardiseringen inom IT-säkerhetsområdet.

Standardiseringsarbetet är en kontinuerlig och pågående process. I del 3, kapitel 13 finns det referenser till lämpliga informationslämnare vad gäller standardiseringsläget inom IT-säkerhetsområdet.

Ordlista

ADB-säkerhet; datasäkerhet	Säkerhet avseende skydd av data och system mot obehörig åtkomst och obehörig eller oavsiktlig förändring eller störning vid datalagring och -behandling.
Administrativ säkerhet	Säkerhet som i huvudsak uppnås med hjälp av administrativa regler och rutiner. Den tekniska säkerheten och den administrativa säkerheten kompletterar i de flesta fallen varandra.
Angrepp; attack	Handling som syftar till att åstadkomma skada eller inskränkningar för verksamheten.
Användare	Person som utnyttjar ett system och dess resurser.
Användargrupp	Grupp av användare som för ett visst syfte givits ett gemensamt namn. Syftet kan exempelvis vara gemensam behörighet.
Användaridentitet	Identitet för en användare.
Asymmetrisk kryptering	Kryptosystem där olika nycklar används för kryptering och dekryptering.
Åtkomstkontroll	Funktioner i ett system som syftar till att reglera och kontrollera en användares åtkomst till olika resurser.
Autenticering	Kontroll av påstådd identitet av en person eller någon annan resurs/upphovsenhet.
Avlyssning	Obehörig åtkomst av information genom registrering och tolkning av data under överföring.
Avsändningsbevis	Till en informationsmängd fogat ursprungsbevis som styrker avsändarens identitet och det faktum att denne verkligen avsänt informationen. Används för att uppnå oavvislighet.
Avsiktligt hot	Hot i illvilligt syfte.
Behörighet	Rättighet för en användare eller annan resurs att utnyttja olika resurser i ett system utifrån definierade ramar. Rättigheterna bör stämma överens med personens/resursens uppgifter och ansvar i den verksamhet som personen är aktiv.

Behörighets-kontroll	Administrativa och tekniska åtgärder för kontroll av användares identitet, styrning av användarens behörighet att använda systemet och dess resurser samt registrering av denna användning.
Behörighets-kontrollsystem	Säkerhetsfunktioner som tillsammans utför behörighetskontroll i ett system.
Behörighets-tilldelning	Fastställande och godkännande av åtkomsträttigheter för en användare till olika systemresurser.
Blockkrypto	Kryptosystem där klartexten indelas i lika stora block (eventuellt efter utfyllnad), som krypteras var för sig.
Brandvägg	Benämning på en gateway mellan olika nätverk avsedd att skydda interna IT-resurser från obehörig åtkomst. Begreppet ”brandvägg” används framförallt för gateways mellan interna nätverk och publika, t.ex. Internet.
Cold Site	En datacentral eller andra dataresurser som förbereds för att finnas tillgängliga vid eventuell förlust av ordinarie dataresurser. En cold site behöver inte omedelbart finnas tillgänglig, till skillnad från en hot site. Tiden för igångsättning kan vara ett fåtal dagar.
Certifikat	En användares öppna nyckel i ett asymmetriskt kryptosystem, vilken tillsammans med dennes namn och eventuell annan information signerats för att kopplingen mellan identiteten/användaren och den publika nyckeln ska gå att verifiera.
Databrott	Allmän beteckning för alla slags brott som har anknytning till datorsystem.
Dataintrång	Obehörig tillgång till information i IT-miljön.
Digital signatur	Omvandling av ett meddelande (eller ett kondensat av detta) på ett sätt som endast avsändaren kan utföra och som tillåter mottagaren att kontrollera meddelandets äkthet, innehåll och avsändarens identitet.
Egenansvar/ Användaransvar	Det är varje användares skyldighet att följa de säkerhetsföreskrifter som gäller, dels generella, dels de som är specifika för de egna arbetsuppgifterna.
Engångslösenord	Ett lösenord som endast används en gång eller vid ett visst tillfälle.

Envägsfunktion	Matematisk funktion som beräkningsmässigt är lätt att utföra, men där inversen beräkningsmässigt är mycket svår och/eller tidsödande.
Funktion för beräkning av kontrollsumma	Matematisk funktion som avbildar värden från en mängd av godtyckligt långa datasträngar till en mängd bestående av kortare datasträngar med fast längd, s.k. kryptografiska kontrollsummor.
Fysisk säkerhet	Säkerhet i ett systems omgivning avseende byggnads- eller andra fysiska skyddsåtgärder.
Hemlig nyckel	Nyckel som används vid symmetrisk kryptering.
Hot	Möjlig, oönskad händelse som ger negativa konsekvenser för verksamheten.
Hot Site	En datacentral eller andra dataresurser som förberetts för att finnas tillgängliga vid eventuell förlust av ordinarie dataresurser. En hot site måste omedelbart finnas tillgänglig, till skillnad från en cold site. Tiden för ingångsättning kan vara ett fåtal timmar.
Identifiering	Process vari användare eller resurs anger sin identitet.
Identitet	Unik representation av en person eller av en annan resurs i IT-systemet.
Inferens	Indirekt åtkomst till information, d.v.s. utan direkt tillgång till data som representerar denna. Genom statistiska beräkningar kan hemlig känslig information härledas ur öppen information.
Informationsägare	Äger ansvarsmässigt informationen, d.v.s. beslutar om vilka som har behörighet att bearbeta, läsa, ta bort, kopiera informationen o.s.v.
Initialvärde	Slumpvärde eller annat variabelt värde som används för att ge varierande startpunkter i en krypteringsalgoritm.
Integritet	Förändringsskydd, en helhet med förmåga att upprätthålla ett värde genom skydd mot oönskad förändring och påverkan. Förändringsskyddet kan gälla t.ex. ett systems integritet, en personlig integritet eller informationskvalitet.
IT	Informationsteknik

IT-resurs	Del i ett IT-system som kan tillhandahålla t.ex. funktioner och tjänster.
IT-säkerhet	Säkerhet i ett IT-system. IT-säkerhet kan delas upp i ADB-säkerhet och kommunikationssäkerhet.
IT-säkerhets-ansvariga	Funktion som särskilt ansvarar för IT-säkerhetsfrågorna inom en enhet/avdelning. Funktionen ansvarar för att säkerhets-regler och riktlinjer inom säkerhetsdomänen följs på ett korrekt och enhetligt sätt.
IT-säkerhetschef	Har huvudansvaret för samordning av IT-säkerhetsarbetet. IT-säkerhetschefen skall gentemot linjeavdelningarna ha en enbart rådgivande, inte beslutande, funktion.
Klartext	En informationsmängd som inte är krypterad.
Kommunikations-säkerhet	Säkerhet i samband med överföring av data via ett kommunikationsnät.
Konfidentialitet	Insynsskydd, skydd som medför att en informationsmängd blir obegriplig för obehöriga.
Kortutfärdare	Organisation som utfärdar aktiva kort till kortinnehavare. Kortutfärdaren ansvarar för att korten är korrekta.
Kryptering	Omvandling av klartext till kryptotext med hjälp av ett kryptosystem och aktuell krypteringsnyckel.
Krypteringsnyckel	En varierbar information som styr en krypteringsalgoritms omvandling av klartext till kryptotext och/eller omvänt.
Kryptografisk kontrollsumma	Kondensat eller hashsumma. Ett kontrollvärde som beräknas på en informationsmängd med hjälp av en algoritm och en hemlig nyckel i syfte att möjliggöra att obehöriga förändringar upptäcks.
Kryptotext	Information som bildats av klartext genom kryptering för att göra innehållet obegripligt för obehöriga.
Logg	Kronologiskt insamlad information om de handlingar som utförs i ett system. Registrerade uppgifter och händelser i loggen skall kunna utnyttjas till att i efterhand rekonstruera och analysera vilka operationer som utförts och vilka användare som initierat dessa.
Logisk bomb	Dold funktion i ett program eller programsystem som under vissa villkor utlöser en icke auktoriserad händelse.

Lönndörr	En ej dokumenterad funktion i ett program som kan utnyttjas till att kringgå normala kontroller i programmets användning och som därvid exempelvis kan åsidosätta säkerhetsskyddet.
Lösenord	Teckensträng som anges för att verifiera en användaridentitet.
Mask	Program som mångfaldigar sig i ett distribuerat system.
Meddelande-autenticering	Verifiering av ursprung, äkthet och integritet hos ett meddelande.
Motringning	Metod för att säkerställa att begärd uppkoppling mot ett system via ett nät (t ex telefonnätet) kommer från en behörig abonnent genom att systemet i sin tur ringer upp denne.
Mottagningsbevis	Till en informationsmängd relaterat bevis som styrker identiteten hos den som mottagit meddelandet och styrker att meddelandet faktiskt har tagits emot. Används för att uppnå oavvislighet.
Nyckelhantering	Administration och tekniska metoder för generering, förvaring, distribution, användning och bottag samt eventuell certifiering av krypteringsnycklar på ett säkert sätt.
Oavsiktligt hot	Ett hot som inte är illasinnat, d.v.s. tekniska fel, misstag eller miljöfaktorer (översvämning, blixtnedslag, o.s.v.).
Oavvislighet	Princip som används vid överföring av data vari dess avsändande och/eller mottagande ej i efterhand ska kunna förnekas.
Personalisering	Aktivitet mellan korttillverkning och distribution till kortinnehavaren. Vid personaliseringen skapas kort, kortutgivarapplikations- och kortinnehavare-specifika kataloger och filer, vilka sedan skrives på kortet.
PIN-kod	Personal Identification Number. Lösenord, begreppet används ofta i samband med olika typer av kort och behörighetskontrollsystem.
Privat nyckel	Den ena av nycklarna i ett nyckelpar vid asymmetriska kryptosystem. Den privata nyckeln ska hållas hemlig. Nyckeln används bland annat för skapande av digitala signaturer.
Publik nyckel	Nyckel som görs allmänt känd och som används vid kryptering i asymmetriska kryptosystem. Nyckeln används bland annat för verifiering av digitala signaturer.

Registeransvarig	Den för vars verksamhet personregister föres (enligt datalagen). Jfr Informationsägare.
Riktighet	Egenskap hos IT-resurser (information, program och tjänster) som hanteras i ett IT-system som innebär att de är korrekta, aktuella och begripliga.
Riktlinjer	Se säkerhetsriktlinjer.
Risk	Produkten av sannolikheten för ett framgångsrikt angrepp och därmed uppkommande av skada.
Röjande signaler, RÖS	Icke önskvärda elektromagnetiska eller akustiska signaler som alstras i informationsbehandlande utrustningar och om de kan fångas upp och tydas av obehörig, kan bidra till att konfidentiell information avslöjas.
Säkerhetsfunktion	Specifik teknisk egenskap hos ett system genom vilken det, tillsammans med övriga säkerhetsfunktioner, upprätthåller säkerheten enligt definierad nivå.
Säkerhetskopia, reservkopia	Kopia av en informationsmängd som skapats för att kunna utnyttjas vid förlust av den ursprungliga informationsmängden.
Säkerhetslogg	Logg över säkerhetskritiska händelser.
Säkerhets-mekanism	Teknik som används vid realisering av en säkerhetsfunktion eller del av denna.
Säkerhetspolicy	Formellt fastställd uppsättning mål som beskriver övergripande säkerhetskrav på informationshanteringen inom en organisation.
Säkerhetsriktlinjer, Riktlinjer	Fastställda riktlinjer för hantering av information, inkluderande dess bearbetning, lagring, distribution och presentation samt stödjande IT-system. Rutiner definieras för att man ska kunna följa riktlinjerna.
Sårbarhet	Svaghet i ett system eller i en verksamhet, i form av bristande förmåga att motstå hot.
Sekretess	Den egenskap hos IT-resurser som innebär att IT-resurserna endast är åtkomliga genom auktoriserade rutiner och vars innehåll inte avslöjas för obehöriga på något annat sätt. Informations- eller datasekretess är exempel på sekretess hos IT-resurser.

Sessionsnyckel	En krypteringsnyckel som endast används för meddelanden, under en session.
Sigill	Se kryptografisk kontrollsumma.
Signera	Att förse en informationsmängd med en digital signatur.
Slumptalsgenerator	Program eller komponent som fortlöpande eller vid behov genererar en sekvens av värden helt styrt av ett startvärde och en algoritm.
Spårbarhet	Att kunna spåra handlingar och händelser till användare och hålla dem ansvariga för sina handlingar. När en handling inte inträffar inom ett system utan i ett meddelande som sänds, är benämningen vanligtvis oavvislighet.
Stark autenticering	Autenticering av en identitet med hjälp av en kryptografisk algoritm och tillhörande privat/hemlig nyckel.
Strömkryptering	Kryptering som inte behöver delas upp i lika stora block utan krypteringen sker byte för byte.
Symmetrisk kryptering	Kryptosystem där samma krypteringsnyckel används för kryptering och dekryptering.
Systemägaransvar	Ledningen är ytterst systemägare till organisationens samtliga IT-system. Delegering av systemägaransvaret följer delegering av verksamhetsansvaret, men det skall betonas att systemägare bör utpekas på nivån närmast under ledningen. I systemägarens ansvar bör ingå bl.a. att fastställa resursramar för IT-stödet, liksom att besluta vilken IT-säkerhetsnivå som skall gälla. Se även informationsägare.
Systemansvarig	Person som ansvarar för driften av ett visst system.
Tillförlitlig tredje part	Enhet som är betrodd av en grupp användare med avseende på specificerade säkerhetsrelaterade tjänster. Exempelvis certifiering av publika nycklar.
Tillförlitlighet	Mått på i vilken grad ett system levererar den information av given kvalitet det säger sig leverera samt tilltro till denna nivå.
Tillgänglighet	Möjlighet att utnyttja resurser efter behov i förväntad utsträckning inom önskad tid.
Tjänst	Tjänst eller del av tjänst som man erbjuder anställda, allmänheten eller andra intressenter.

Trafikanalys	Undersökning av trafikflöden i ett kommunikationsnät för att erhålla uppgifter om t.ex. trafikintensitet, meddelandelängder, avsändar- och mottagaradresser.
Trap door, Lönndörr	En ej dokumenterad funktion i ett program som kan utnyttjas till att kringgå normala kontroller i programmets användning och som därvid exempelvis kan åsidosätta säkerhetsskyddet.
Trojansk häst	Program som verkar utföra eller reellt utför en förväntad, önskad funktion men som **även** utför oönskade funktioner.
Virus	En självreproducerande instruktionssekvens som ligger gömd i ett annat program och innehåller en utlösningsdel och en skadedel.