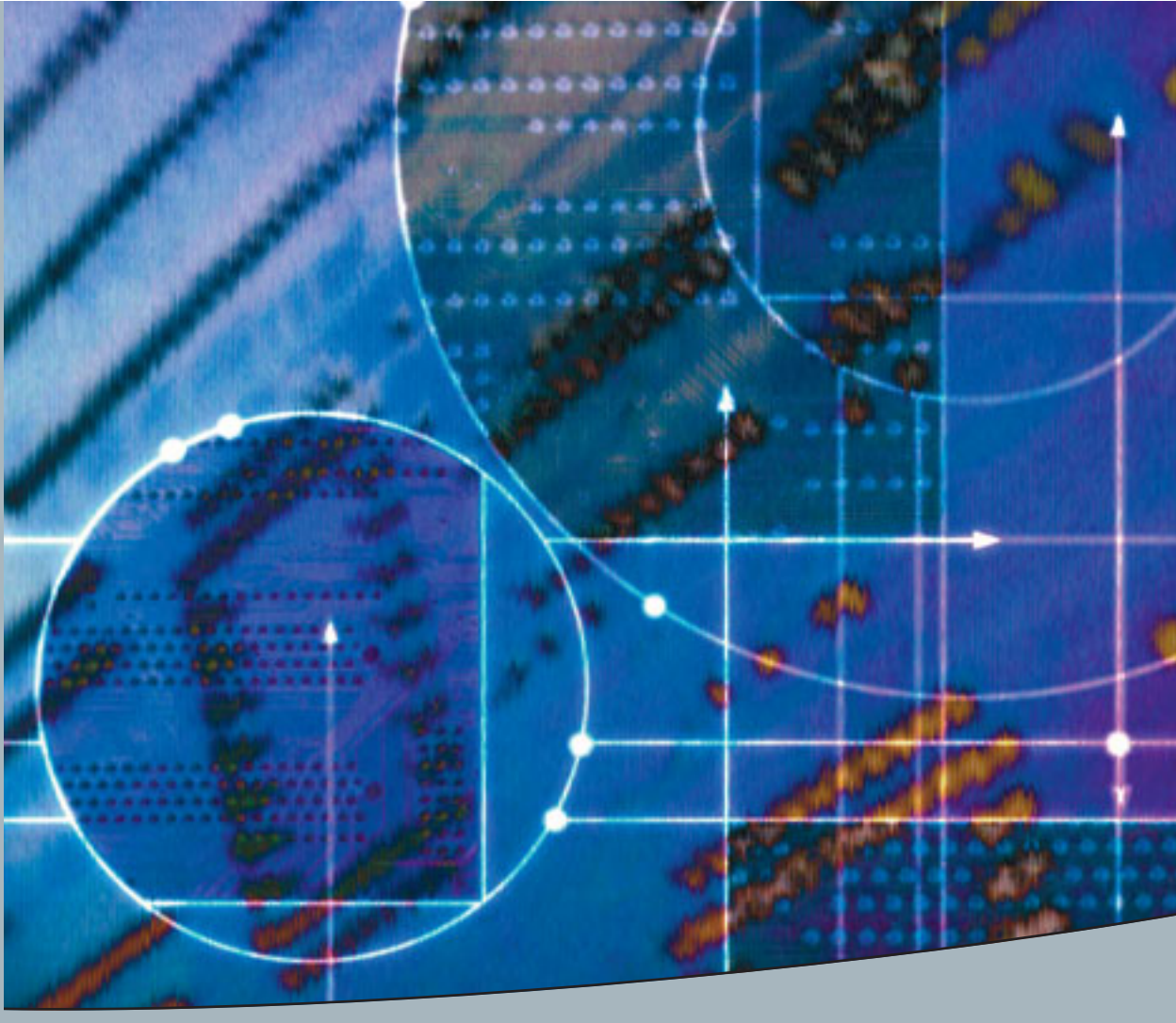

Basnivå för IT-säkerhet (BITS)

KBM REKOMMENDERAR ■ 2003:2

KRISBEREDSKAPS
MYNDIGHETEN

KBM REKOMMENDERAR ■ 2003:2

Basnivå för IT-säkerhet (BITS)

KBM REKOMMENDERAR

2003:1 Risk- och sårbarhetsanalyser
Vägledning för statliga myndigheter

2003:2 Basnivå för IT-säkerhet (BITS)

Titel: Basnivå för IT-säkerhet (BITS)
Utgiven av Krisberedskapsmyndigheten (KBM)
Omslagsfoto: PhotoDisc
Upplaga: 4 000 exemplar

ISBN: 91-85053-35-X
KBM:s dnr: 1123/2003
Grafisk form: AB Typoform
Tryck: Edita Ljunglöfs, Stockholm, december, 2003

Skriften kan erhållas kostnadsfritt från
Krisberedskapsmyndigheten, materielförvaltning
E-post: bestallning@krisberedskapsmyndigheten.se

Skriften kan laddas ned från Krisberedskapsmyndighetens webbplats
www.krisberedskapsmyndigheten.se

KBM REKOMMENDERAR 2003:2

Innehåll

Förord

Samhällsviktiga IT-system

Krisberedskapsmyndigheten (KBM) har ett sammanhållande myndighetsansvar inom informationssäkerhetsområdet och har kraven på samhällets förmåga att fungera även under olika krissituationer som utgångspunkt. IT-system som betraktas som samhällsviktiga intar en central roll när det gäller olika samhällsfunktioners möjligheter att bedriva sin verksamhet.

För att bedöma om ett IT-system ska betraktas som samhällsviktigt kartläggs vilken verksamhet som en organisation har krav på sig att bedriva även i fredstida kriser i samhället och eventuellt också vid höjd beredskap. Är sådan verksamhet beroende av ett visst IT-system för att kunna upprätthållas på avsedd nivå, kan detta IT-system anses vara samhällsviktigt.

Olika faktorer påverkar de krav som måste ställas på säkerheten i samhällsviktiga IT-system. Säkerhetsnivån måste i varje enskilt fall fastställas med utgångspunkt från en riskanalys. Med denna som underlag kan bedömas hur allvarliga konsekvenserna blir för egen eller andras verksamhet eller tredje man om ett IT-system inte fungerar på avsett vis.

Myndigheter med särskilt ansvar

I förordningen (2002:472) om åtgärder för fredstida krishantering och höjd beredskap ställs specifika krav på myndigheter med ett särskilt ansvar för fredstida krishantering och för förmågan att fungera under höjd beredskap.

Enligt 4 § i denna förordning ska myndigheter som har ett särskilt ansvar för fredstida krishantering planera och vidta förberedelser för att förebygga, motverka och begränsa identifierad sårbarhet och risker inom sina respektive samverkansområden. De ska därvid särskilt

beakta säkerhetskraven för bl.a. de tekniska system som är nödvändiga för att kunna utföra sitt arbete.

Enligt 11 § i denna förordning ska myndigheter med s.k. bevakningsansvar ansvara för att dator- och kommunikationssystem uppfyller sådana säkerhetskrav att de kan utföra sina uppgifter på ett tillfredsställande sätt även under höjd beredskap.

Årliga risk- och sårbarhetsanalyser

I syfte att stärka sin krishanteringsförmåga ställs, i förordningen (2002:472) om åtgärder för fredstida krishantering och höjd beredskap, krav på myndigheter att årligen analysera om det finns sårbarheter och risker inom myndighetens ansvarsområde som synnerligen allvarligt kan försämra förmågan till verksamhet inom området. Resultatet av arbetet ska värderas och sammanställas i en risk- och sårbarhetsanalys som ska redovisas samtidigt med årsredovisningen.

1. Allmänt om BITS

1.1 Syfte och omfattning

Av Krisberedskapsmyndighetens (KBM) "Planeringsinriktning för samhällets krisberedskap 2004" framgår att skalan för samhällets krishantering sträcker sig från normal fredsverksamhet till anpassning för verksamhet under höjd beredskap.

Samhällets normala robusthet och inbyggda beredskap avser i första hand förmågan att hantera normala fredstida störningar och olyckor men även händelser med mer omfattande konsekvenser.

Kraven på säkerheten i IT-verksamheten ska ställas i relation till de krav som ställs på organisationens verksamhet i övrigt. IT-säkerheten ska ligga på en sådan nivå att inte IT-stödet blir den svaga länken i organisationens verksamhet.

KBM definierar i dessa rekommendationer en säkerhetsnivå som minst måste uppnås för IT-system som bedöms nödvändiga för att upprätthålla en organisations normala verksamhet även under fredstida kriser. Denna säkerhetsnivå betecknas *basnivå*. Ambitionen är att denna basnivå ska vara väl balanserad och generellt ge en acceptabel säkerhetsnivå. Om denna basnivå är tillräcklig kan dock endast avgöras genom en risk- och sårbarhetsanalys i varje aktuellt fall.

BITS är upplagd så att varje avsnitt inleds med rekommendationer för basnivå som redovisas i en separat ruta. Den efterföljande texten redovisar, i olika utsträckning, motiven för valda rekommendationer och ger även ytterligare råd inom sina respektive områden.

KBM:s rekommendationer har som utgångspunkt haft olika standarder och standardiseringssträvanden som förekommer på olika håll, men anpassats och begränsats för att ge ett konkret stöd i arbetet att uppnå nämnda basnivå. Avstämningar har gjorts mot bl.a. ISO/IEC 17799, FA22, Guidelines for the Management of IT Security (GMITS ISO/IEC, TR 13335) och OECD Guidelines for the Security of Information Systems and Network.

Som komplement till dessa rekommendationer kommer KBM, mot bakgrund av 11 § i förordningen om åtgärder för fredstida krishantering och höjd beredskap, att utge föreskrifter och därtill hörande allmänna råd inriktade mot ytterligare åtgärder för IT-säkerhet som krävs för att en organisation även ska kunna upprätthålla sin verksamhet inför och under höjd beredskap.

För KBM:s rekommendationer för basnivå för IT-säkerhet (BITS) gäller att de:

- till sitt innehåll är konsistenta med ISO/IEC 17799 vad avser IT-säkerhet
- definierar en balanserad basnivå för säkerheten i IT-system.

1.2 Säkerhetsarbetets olika steg

KBM:s rekommendationer utgår från följande arbetsprocess för IT-säkerhetsarbetet:

- Organisationen definierar målen och inriktningen för säkerhetsarbetet i en IT-säkerhetspolicy. IT-säkerhetspolicyn är det övergripande dokument som styr IT-säkerhetsarbetet.
- Utgående från IT-säkerhetspolicyn tas en systemsäkerhetsplan fram för varje IT-system som bedöms viktigt för verksamheten. Systemsäkerhetsplanen beskriver vilka säkerhetskrav som ska ställas utifrån aspekterna sekretess, riktighet och tillgänglighet. Om kraven överstiger den basnivå som definieras i KBM:s rekommendationer behövs kompletterande säkerhetsåtgärder.
- IT-säkerhetspolicyn konkretiseras i IT-säkerhetsinstruktioner för användare, drift och förvaltning. I vissa fall kan det även finnas behov av systemspecifika instruktioner.
- En bedömning av om genomförda säkerhetsåtgärder har avsedd funktion samt ett ställningstagande till hur ytterligare krav på säkerhetsåtgärder ska hanteras ger underlag för den säkerhetsutvärdering som ett beslut om driftgodkännande ska baseras på.

1.3 Några centrala begrepp

I dessa rekommendationer är nedanstående begrepp centrala.

IT-säkerhet: De delar av begreppet informationssäkerhet som avser säkerheten i den tekniska hanteringen av information som bearbetas, lagras och kommuniceras elektroniskt samt administrationen kring detta.

IT-system: I begreppet IT-system ryms ett brett spektrum av IT-stöd. I första hand avses olika applikationsprogram, administrativa system, telefonisystem och interna nätverk. Bryggor och program som utnyttjas för integrering av olika system ska därvid anses tillhöra det sistnämnda.

Systemägare: Organisationens chef eller av denne särskilt utsedd aktör med ansvar för anskaffning, ny-/vidare-/avveckling, förvaltning, drift, säkerhet och användning i övrigt av ett IT-system inom ramen för antagna mål och ekonomiska ramar.

Central systemägare: Systemägare vid en organisation som har det övergripande ansvaret för ett IT-system som används gemensamt av flera organisationer.

IT-säkerhetspolicy: Dokument som anger mål och riktlinjer för organisationens IT-säkerhetsarbete.

Systemsäkerhetsplan: Dokument som utgör en risk- och sårbarhetsanalys för ett enskilt IT-system eller internt IT-nätverk och som redovisar de samlade kraven på detta avseende sekretess, riktighet och tillgänglighet. Av planen ska framgå vilka säkerhetsåtgärder som är vidtagna samt de eventuella ytterligare säkerhetsåtgärder som behöver vidtas för att kraven ska uppfyllas. Systemsäkerhetsplanen utgår från IT-säkerhetspolicyn och från aktuellt IT-systems/IT-nätverks roll i verksamheten.

IT-säkerhetsinstruktion: Konkreta regler och rutiner avseende IT-säkerhet som riktar sig till användare, driftpersonal eller personal för administration och förvaltning.

Basnivå: Säkerhetsnivå som minst måste uppnås för ett IT-system som bedöms nödvändigt för att upprätthålla en viss verksamhets basförmåga.

Driftgodkännande: Formellt organisationsbeslut att godkänna ett IT-system för drift.

2. Ledningens roll och ansvar

Basnivå

- Det ska finnas en rådgivande och samordnande funktion för IT-säkerhet.

Organisationens ledning är ytterst ansvarig för IT-verksamheten och därmed också för säkerheten i organisationens IT-resurser. Detta ansvar omfattar bl.a. att säkerställa att det finns ekonomiska resurser och personella resurser med rätt kompetens för IT-säkerhetsarbetet. I ansvaret ingår att utveckla och vidmakthålla ett dokumenterat ledningssystem för IT-säkerheten som omfattar organisationens sätt att arbeta med riskhantering, mål och styrmedel samt den säkerhetsnivå som ska gälla.

Organisationens ledning ansvarar för att övergripande och styrande dokument och planer för IT-säkerhetsarbetet tas fram.

En särskild roll för IT-säkerhet bör ligga på en rådgivande och samordnande funktion, som har den specialkompetens som krävs för att kunna omsätta olika krav i lämpliga säkerhetsåtgärder. Detta bör bl.a. omfatta att:

- samordna IT-säkerhetsarbetet inom organisationen
- medverka i framtagning av såväl IT-säkerhetspolicy, systemsäkerhetsplaner som IT-säkerhetsinstruktioner
- informera om och ge råd i IT-säkerhetsfrågor
- medverka i genomförandet av säkerhetsåtgärder
- följa upp att IT-säkerhetsinstruktioner följs och vid behov föreslå åtgärder
- samordna incidentrapporteringen inom organisationen.

3. Styrande dokument

3.1 IT-säkerhetspolicy

Basnivå

IT-säkerhetspolicyn ska:

- fastställas av organisationens ledning och dokumenteras
- fastställa fördelningen av ansvaret för IT-säkerheten inom organisationen och beskriva de olika rollerna
- fastställa riktlinjer för områden som är av särskild betydelse för organisationen.

För att på ett tillfredsställande sätt leda och styra IT-säkerhetsarbetet inom en organisation krävs en IT-säkerhetspolicy. IT-säkerhetspolicyn är ett övergripande och för IT-verksamheten gemensamt dokument som på ett tydligt sätt ska uttrycka ledningens engagemang, mål och riktlinjer för IT-säkerhetsarbetet och den måste vara accepterad och känd i organisationen.

Detaljer som berör enskilda IT-system redovisas i de systemsäkerhetsplaner som ska finnas för respektive IT-system. IT-säkerhetspolicyn är relativt långsiktig, medan systemsäkerhetsplaner kan behöva revideras vid exempelvis förändringar i verksamhetens inriktning och omfattning, större ändringar i systemens utformning, förändringar i hotbilden o.dyl.

För vissa områden inom organisationens verksamhet kan det finnas anledning att ta fram speciella riktlinjer, exempelvis vad som ska gälla för distansarbete och användning av Internet.

Ledningen har alltid det övergripande ansvaret för verksamheten och de IT-system som används som stöd. Delegering av ansvaret för IT-säkerhet sker normalt enligt samma principer som gäller för verksamhetsansvaret inom organisationen. Under ledningen är var och en som är ansvarig för någon del av verksamheten också ansvarig för IT-säkerheten inom sitt område.

3.2 Systemsäkerhetsplan

Basnivå

En systemsäkerhetsplan ska:

- upprättas för varje IT-system som bedöms viktigt för verksamheten
- fastställas av systemägaren och dokumenteras
- utpeka vem som är systemägare
- innehålla de samlade kraven på säkerhet som ställs på IT-systemet.

För att kunna bedöma säkerhetskraven på ett IT-system är det nödvändigt att klarlägga vilka verksamheter som systemet stöder och hur beroende de är av det.

Systemsäkerhetsplanen bör därför inledas med en skiss över systemet och en översiktlig beskrivning av den verksamhet som det stöder och vilken information det hanterar. Systemets kopplingar till andra interna och externa IT-system bör beskrivas. Detta gäller även hur information hämtas till systemet, hur den överförs till andra interna och externa system samt till andra verksamheter.

I systemsäkerhetsplanen klarläggs vilka säkerhetskrav som ska ställas för att:

- förhindra eller försvåra för en obehörig att få tillgång till informationen (sekretess)
- säkerställa att den information som produceras och bearbetas i IT-systemet är korrekt, aktuell och fullständig (riktighet)
- IT-systemets funktion och information är åtkomlig vid behov (tillgänglighet).

Utgångspunkten för detta är en riskanalys som baseras på bedömningar av vilka hot som finns mot IT-systemet, sannolikheten för att de realiseras och vad konsekvenser i så fall skulle bli. I riskanalysen ska även krav som emanerar från lagar och föreskrifter samt från den egna verksamheten beaktas.

Förutom generella lagar som t.ex. sekretesslagen, personuppgiftslagen, arkivlagen och säkerhetsskyddslagen, är vissa verksamheter även beroende av speciallagstiftning och föreskrifter som exempelvis socialtjänstlagen, registerlagar, tullagen och rikspolisstyrelsens föreskrifter.

Hot kan omfatta såväl avsiktliga händelser utförda av en angripare som oavsiktliga händelser uppkomna på grund av hanteringsfel, olyckor eller liknande.

Förändringar i verksamhetens inriktning och omfattning, förändrad hotbild och ändringar i systemutformning kan innebära att systemsäkerhetsplanen behöver revideras.

Systemsäkerhetsplanen ska avstämmas mot IT-säkerhetspolicyn och mot gjorda policyuttalanden.

3.3 IT-säkerhetsinstruktioner

Basnivå

- Det ska finnas dokumenterade, av ledningen beslutade, IT-säkerhetsinstruktioner.
- IT-säkerhetsinstruktion ska finnas för:
  - användare
  - förvaltning
  - drift

IT-säkerhetsinstruktion för användare: Redovisar de generella IT-säkerhetsregler som gemensamt gäller för personalens hantering av flertalet av organisationens IT-system och IT-resurser. Den kan exempelvis klargöra vad som gäller den egna arbetsstationen, vilka restriktioner som gäller för elektronisk post och vid användning av Internet m.m.

I vissa fall kan särskilda, av systemägaren beslutade, dokumenterade användarinstruktioner behöva tas fram för enskilda IT-system.

IT-säkerhetsinstruktion för förvaltning: Klarlägger rutiner för behörighetsadministration, rutiner för införande, förvaltning och avveckling av system, olika systemadministrativa åtgärder knutna till informationsbehandlings- och kommunikationsresurser o.dyl.

IT-säkerhetsinstruktion för drift: Avser den löpande hanteringen av driften, instruktioner för hur avbrott av olika längd ska hanteras, eventuella prioriteringar vid exceptionella händelser, hantering och förvaring av datamedia o.dyl.

4. Information och utbildning

Basnivå

- Utbildningsinsatser inom IT-säkerhet ska genomföras regelbundet.
- All personal ska få information om innehållet i organisationens IT-säkerhetspolicy samt om IT-säkerhetens betydelse för verksamheten.

Motiverad personal med goda kunskaper om IT-säkerheten och dess betydelse är en förutsättning för att upprätthålla önskad säkerhetsnivå. Bristande kunskaper kan exempelvis orsaka handhavandefel som ger störningar i verksamheten. Det är viktigt att personalen förstår vikten av IT-säkerhet, inte minst för att genomförda säkerhetsåtgärder ska uppfattas som legitima. Detta även med tanke på att vissa säkerhetsåtgärder kan upplevas som ett praktiskt hinder i den dagliga verksamheten.

Utbildning i IT-säkerhet får inte inskränka sig till att bara lära ut tekniska färdigheter utan måste även omfatta administrativa rutiner. Utöver att kunskapen om IT-säkerhet ska vara tillräcklig, är det också viktigt att säkerhetsmedvetandet och motivationen upprätthålls. Utbildningsåtgärder måste därför genomföras kontinuerligt.

Den information som användarna får kan med fördel delas upp i en allmän information om IT-säkerhetens roll för organisationens verksamhet och i olika moment som är anpassade efter respektive användares arbetsuppgifter.

För att systemägare ska kunna uppfylla sitt ansvar kan de ges en speciell information om vad som följer ansvarsrollen, t.ex. att ta fram en systemsäkerhetsplan, ansvaret för uppföljning av tilldelade behörigheter, granskning av loggar m.m.

5. Åtkomst till IT-resurser

5.1 Behörighetsadministration

Basnivå

- Det ska finnas en rutin för tilldelning, uppföljning och uppdatering av behörighet.
- Behörighetsrutinen ska dokumenteras (IT-säkerhetsinstruktion, förvaltning).
- Systemägaren ska fastställa vem som har rätt att besluta om behörighet.
- Dokumenterade rutiner ska finnas för hantering av behörighet för användare som slutar eller byter arbetsuppgifter (IT-säkerhetsinstruktion, förvaltning).
- Beslut om behörighet ska:
  - dokumenteras
  - sparas.
- Nya användare ska ges ett initialt lösenord som de ska byta till ett eget valt lösenord vid första användning.
- Före tilldelning av behörighet ska användare ges tillräckliga kunskaper om:
  - de IT-säkerhetsinstruktioner som generellt gäller för IT-verksamheten
  - de instruktioner som speciellt ansluter till den egna arbetsuppgiften.
- Borttagning av behörighet som upphört att gälla ska ske inom högst en vecka.
- Endast utsedd administratör ska kunna registrera, förändra eller ta bort användares åtkomsträttigheter.
- Det ska finnas utsedd personal i reserv och eventuella reservrutiner för hantering av behörighet.

- Systemadministratörer/-tekniker ska alltid ha individuella användaridentiteter.
- Behörighetsregister ska endast vara åtkomligt för utsedd administratör.
- Antalet konton med privilegierade rättigheter och omfattningen av dessa rättigheter ska minimeras.

Behörighetsadministration omfattar dels beslut om vem som ska tilldelas en viss behörighet och dels det praktiska arbetet att registrera beslutade behörigheter i IT-systemet.

Reglerna för behörighetsadministrationen måste utformas så att de blir praktiskt användbara, kan följas och inte ges en alltför komplicerad behörighetsstruktur. Generellt kan sägas att administrationen underlättas om hanteringen av behörigheter baseras på rollbegreppet. I sådana fall tilldelas ingen användare unika rättigheter till enskilda filer eller dataposter, utan rättigheterna knyts i stället till en roll. Användare kan sedan knytas till en eller flera sådana roller. Därmed kan detaljeringsgraden i behörighetsadministrationen begränsas så att administration och uppföljning kan hanteras avsevärt mycket lättare.

Vanligtvis är det den person som har kunskap om vilken information användaren är i behov av, t.ex. närmaste chef eller uppdragsgivare, som beslutar om behörighet. Normalt ska inte administratören ha rätt att besluta om att tilldela eller förändra behörigheter. Denne ska dock kräva att beslut om behörighet finns, för att lägga in en användares behörighet.

Alla förändringar av behörigheter, t.ex. när en användare byter arbetsuppgifter, slutar sin anställning eller när ett konsultuppdrag avslutas, kan med fördel ske enligt samma rutin som vid tilldelning av behörighet. Detta innebär att förändringarna initieras av samma befattningshavare, eller dennes eventuella efterträdare, som godkänt behörigheten, att beslutet dokumenteras och att behörighetsadministratören verkställer beslutet.

Frekvensen av åtgärder i behörighetskontrollsystemet påverkar i hög grad utformningen av reservrutiner. Är frekvensen hög krävs i allmänhet att det finns en eller flera personer med rätt kunskap och behörighet som kan träda in. Vid låg frekvens kan lösenordet för behörighetsadministratören förvaras i förseglat kuvert inlåst i säkerhetsskåp och vid behov användas för att ge en person med grundläggande

kunskap en tillfällig behörighet att lösa uppgiften. Efter en sådan åtgärd ska alltid ordinarie administratör byta lösenord.

Användare med privilegierade rättigheter, som exempelvis superusers och system managers, har möjlighet att ta del av eller förändra all information och att ändra IT-systems utformning. Tilldelning av privilegier måste därför vara restriktiva och endast omfatta dem som oundgängligen krävs för att administrera IT-systemet. De privilegierade behörigheter som accepteras ska vara personliga. Anonyma konton av typen Root eller Administrator kan bara tillåtas om man för att använda kontot först tvingas logga in i eget namn och därefter kan växla behörighet till ett anonymt konto och att id-växlingen loggas. Alternativt kan dessa konton/lösenord förvaras i förseglat kuvert i säkerhetsskåp och användningen av dem regleras i säkerhetsinstruktion. På så sätt blir det möjligt att avgöra vem som haft tillgång till systemet.

Samma rutin som gäller för en förstagångsanvändare bör tillämpas om användaren behöver få ett nytt lösenord beroende på att denne exempelvis glömt sitt lösenord.

5.2 Behörighetskontroll

Basnivå

- Behöriga användare av IT-system ska vara registrerade i ett behörighetskontrollsystem med de rättigheter som beslutats.
- Minst en gång per år ska kontrolleras att bara behöriga användare är registrerade i behörighetssystemet.
- Om möjligt ska användare ges en behörighetsprofil som endast medger den åtkomst till aktuellt IT-system som krävs för att lösa arbetsuppgifterna.
- För lösenord ska gälla att:
  - varje användare ska ha en unik användaridentitet och ett lösenord som endast denne känner till och kan ändra
  - de ska bestå av minst 8 tecken för såväl användare som systemadministratörer/-tekniker och vara konstruerade så att de inte lätt går att pröva sig fram till eller gissa
  - användarna ska tvingas byta lösenord enligt tidsintervall som systemägaren beslutar
  - högst tre felaktiga inloggningsförsök inom en 6-timmars period ska tillåtas innan användarkontot låses
  - de inte ska tillåtas återanvändas.

- Varje arbetsstation ska ha automatisk låsning efter en viss beslutad tidsperiod understigande 10 minuter och upplåsning ska ske genom lösenord.
- Låst användarkonto ska öppnas först efter säker identifiering av användaren.
- Lagrade lösenord ska skyddas genom kryptering eller på annat sätt.
- Det ska finnas rutiner som förhindrar att standard- eller leverantörsbehörigheter kan användas.
- För IT-system med central systemägare ska denne säkerställa att det är konstruerat så att alla rekommendationer på basnivå avseende behörighetskontroll kan tillgodoses.

Med behörighet avses en användares rättighet att på ett reglerat sätt utnyttja ett IT-system och dess resurser. För att uppnå detta krävs samverkande tekniska och administrativa åtgärder.

Med behörighetskontroll avses administrativa och tekniska åtgärder för kontroll av användares identitet, för styrning av användares behörighet samt för uppföljning av användning. Sådan kontroll sker vanligen i ett behörighetskontrollsystem som möjliggör verifiering av identiteten, reglering av åtkomsträttigheter samt registrering av användarens aktiviteter i IT-systemet (loggning).

Ett lösenord bör bestå av en blandning av bokstäver, siffror och specialtecken för att försvåra möjligheterna att avslöja det.

För att en systemägare ska kunna ta ansvar för säkerheten i IT-system som används av flera andra organisationer, krävs att denne, som då är s.k. central systemägare, säkerställer att IT-systemet är konstruerat så att de grundläggande kraven kan tillgodoses i IT-systemet hos de övriga organisationerna.

Kryptering av lösenordsfil bör ske med en envägsfunktion.

För att kunna öppna ett låst användarkonto ska användaren vända sig till behörighetsadministratören, som öppnar kontot efter att ha identifierat användaren. Denne bör därefter tilldelas ett nytt lösenord enligt samma regler som gäller för en ny användare.

När en arbetsstation öppnas efter låsning bör den öppnas där sessionen avbröts. Vid låsning bör skärmbilden släckas eller ersättas med en speciell pausbild. Pausfunktionen bör aktiveras senast efter 10 minuter.

5.3 Loggning och spårbarhet

Basnivå

- Det ska finnas säkerhetslogg som registrerar användaridentitet, uppgift om inloggning och utloggning samt datum och tidpunkt för detta.
- Systemägaren ska fastställa vilka händelser utöver ovanstående som ska registreras i IT-systemets säkerhetslogg.
- Central systemägare ska säkerställa att IT-systemet är konstruerat så att uppgift om användarindentitet samt datum och tidpunkter för in- och utloggningar kan registreras i en säkerhetslogg.
- För säkerhetsloggar ska systemägaren besluta (IT-säkerhetsinstruktion, förvaltning):
  - hur ofta de ska analyseras
  - vem som ansvarar för analyser av dem
  - hur länge de ska sparas
  - hur de ska förvaras.
- För transaktionsloggar ska systemägaren besluta (IT-säkerhetsinstruktion, förvaltning):
  - hur ofta de ska analyseras
  - vem som ansvarar för analyser av dem
  - hur länge de ska sparas
  - hur de ska förvaras.

Syftet med loggning är att i efterhand kunna reda ut vilka transaktioner som gjorts, hur, när och av vem. Loggar är ett mycket viktigt underlag för att klargöra vad som skett vid misstanke om eller inträffade säkerhetsrelaterade incidenter. Det är därvid av avgörande betydelse att datorklockor är synkroniserade för att loggar ska vara tillförlitliga vid en utredning eller en uppföljning.

Det finns dock praktiska problem i samband med loggning. Först och främst måste man klarlägga vad som ska loggas. Loggsystemens komplexitet varierar genom att det är valfritt att aktivera eller avaktivera olika funktioner i loggsystemen. Ju fler detaljer som loggas desto större är sannolikheten att den önskade informationen faktiskt går att återfinna. Loggas för mycket riskerar man att överhopas av data och få hanteringsproblem vid lagring samtidigt som uppföljning

av loggarna försvåras. Loggas för lite kan man få problem med att göra en adekvat uppföljning.

En normal systemmiljö är ofta komplicerad och består av flera system länkade till varandra i t.ex. nätverk. I dessa miljöer förekommer flera olika loggar. Ofta krävs registrering i flera system, exempelvis in- och utloggning i nätverk, behörighets- och transaktionsloggar för enskilda applikationssystem samt loggning i kommunikationsutrustning, t.ex. brandväggar, för att få en tillräckligt klar bild av användares förehavanden. En samordning av flera loggar kan behövas för att få den spårbarhet som är loggningens egentliga syfte.

Systemägaren ska fastställa vilka händelser utöver den grundläggande säkerhetsloggningen som ska registreras i IT-systemets säkerhetslogg. Sådan uppgifter kan t.ex. vara felaktiga inloggningsförsök, behörighetstilldelning och förändring av behörighet.

För att en systemägare ska kunna ta ansvar för säkerheten i IT-system som används av flera andra organisationer, krävs att denne, som central systemägare, säkerställer att IT-systemet är så konstruerat att ovanstående kan tillgodoses i IT-systemet hos de övriga organisationerna.

I ett IT-system där flera användare är behöriga till all information och systemägaren av olika skäl beslutat att användaridentitet inte ska registreras och inte heller lösenord ska användas, kan systemägaren besluta att annan likvärdig åtgärd än loggning vidtas. Exempelvis kan tillträdeskontrollen förstärkas till de lokaler där möjligheter finns för åtkomst till IT-systemet. Detta kan ske t.ex. med kontrollsystem där uppgifter om inpassering loggas eller, i undantagsfall, med en manuell tillträdesjournal.

Säkerhetsloggarna måste följas upp kontinuerligt. En analys av dem ska inriktas mot alla former av överträdelser mot gällande regler. Systemägaren fastställer om analyser ska göras genom periodiska eller stickprovskontroller, om loggarna ska förvaras i säkerhetsskåp eller på annan plats, vilken personal som är behörig att ta del av säkerhetsloggarna etc.

Normalt räcker det att spara säkerhetsloggar i två år, men i vissa fall kan de av särskilda orsaker behöva sparas längre. Förutsättningar måste då finnas för att läsa informationen vid behov under den tid som loggarna sparas.

Med spårbarhet menas möjligheten att via registreringar identifiera och följa förloppet för olika händelser. Varje uppgift i register o.dyl.

ska kunna följas och kontrolleras med avseende på hur den är uppbyggd av grunddata eller andra uppgifter. För varje rutin ska man i efterhand kunna följa och kontrollera en händelses kronologiska och systematiska förlopp med avseende på:

- vilka behandlingsregler som tillämpats
- hur grunddata och uppgifter bearbetats eller sammanställts
- vilka transaktioner en uppgift, period eller bearbetning omfattar.

För att kunna genomföra spårningen i ett IT-system behövs kunskap om systemets bearbetningar och den kronologiska ordningen för dem. Hjälpmedlen för detta är en eller flera bevakningsfunktioner i form av loggning. Med utgångspunkt från en strategi för loggning och rätt inställningar i systemen kan dessa hjälpmedel säkerställa vems identitet som använts och när den använts. För att uppgifterna ska bli tillräckligt verifierade kan de ibland behöva kompletteras med tjänstgöringslistor, in- och utpasseringsuppgifter, attestuppgifter m.m.

Varje IT-system ska åtminstone ha möjlighet till full spårbarhet när det gäller information som bedömts ha ett högt skyddsvärde.

5.4 Informationsklassning

Basnivå

- Informationen i IT-system ska omfattas av klassning.
- Det ska finnas dokumenterade regler för klassning av information (IT-säkerhetsinstruktion, användare).

Att klassa informationen som ingår i ett IT-system är av grundläggande betydelse för IT-säkerhetsarbetet. Aspekter som styr klassningen är sådana som vikten av att information inte röjs, ekonomiska konsekvenser av om information är felaktig eller saknas, påverkan på olika beslut om informationen inte är korrekt o.dyl. Om det ställs extrema krav på viss information i ett IT-system, kan det övervägas om inte denna information ska tas bort ur systemet och behandlas i särskild ordning eller hanteras i en kompletterande procedur. På så vis kan ofta kraven på systemet sänkas.

För att inte riskera att klassificering görs slentrianmässigt, bör utbildning i hur detta ska ske genomföras med viss regelbundenhet,

exempelvis vartannat år. Nyanställda bör få utbildning i gällande regler för informationsklassning innan de ges behörighet till IT-system.

Ägare till den information som ska klassas är i allmänhet systemägaren för respektive IT-system. Av organisatoriska skäl kan det ibland vara praktiskt att delegera och även fördela informationsägarskapet.

Informationen klassas utifrån aspekterna sekretess, riktighet och tillgänglighet, d.v.s. vikten av att den skyddas mot obehörig åtkomst, inte är felaktig och är åtkomlig för behöriga vid behov.

Exempel på kriterier att ta hänsyn till vid klassning redovisas nedan.

Sekretessaspekten

Om informationen är en:

- handling (minnesanteckningar, mellanprodukter m.m.)
- allmän handling, offentlig eller sekretessbelagd.

Riktighetsaspekten

Att felaktig information inte får leda till:

- felaktiga beslut
- badwill
- kostnader p.g.a. sanktioner från annan intressent
- kostnader i allmänhet.

Tillgänglighetsaspekten

Att åtkomstbortfall inte får leda till:

- arbetsbortfall
- förseningar som blir kostnadsdrivande
- försämrad service.

5.5 Distansarbete och mobil datoranvändning

Basnivå

- Kraven på teknisk säkerhet och praktisk hantering av mobil utrustning ska dokumenteras (IT-säkerhetsinstruktion, användare).
- Systemägaren ska besluta om ett IT-systems information ska få bearbetas på distans med stationär eller mobil utrustning.

Det är allt vanligare förekommande att anställda arbetar utanför organisationens lokaler, i hemmet eller på annan plats. Hantering av bärbara datorer och annan mobil utrustning och dess uppkoppling mot det interna nätverket måste regleras. Det kan därvid vara lämpligt att upprätta avtal med aktuella användare för vad som ska gälla för distansarbete hemifrån.

Speciell försiktighet måste iakttas när det gäller distansarbete från hemmet samt vid användning av mobil utrustning som laptops, handdatorer, mobiltelefoner o.dyl. på plats geografiskt skild från organisationens arbetslokaler.

Frågor som kan vara aktuella att reglera för distansarbete kan exempelvis gälla följande:

- fysiskt skydd i eller utanför hemmet (stöldrisk)
- logiskt skydd (otillbörlig användning)
- om utrustningen endast får användas för arbetsgivarens arbete (virussmitta o.dyl.)
- hantering av utskrifter (obehörig tillgång)
- om lagring och säkerhetskopiering av information ska ske i egen dator eller hos arbetsgivaren (stöldrisk, obehörig tillgång och förstörelse m.m.)
- hur eventuella hjälpinsatser utifrån (remote) ska ske (obehörigt intrång)
- kontroll av skadlig programkod (virussmitta o.dyl.)
- om kryptering krävs vid överföring i vissa fall (obehörig tillgång och förändring)
- autenticering vid uppkoppling mot arbetsgivarens nätverk (obehörig tillgång och förändring).

5.6 Kryptering

Basnivå

- Finns beslut om kryptering av information ska riktlinjer för detta dokumenteras (IT-säkerhetsinstruktion, förvaltning).

Behovet av krypteringsteknik inom en organisation bör övervägas utifrån genomförda riskanalyser. I de fall ett sådant behov föreligger, bör organisationen utveckla riktlinjer för kryptering för att undvika olämplig eller felaktig användning. Riktlinjerna bör bl.a. beakta hur kryptonycklar ska hanteras samt vilka roller och vilket ansvar som ska gälla.

6. Drift och förvaltning

6.1 Införande och avveckling

Basnivå

- IT-system som tas i bruk ska ha stämts av mot de säkerhetskrav som verksamheten ställer.
- Regler ska finnas för hur datamedia med sekretessbelagd information ska avvecklas (IT-säkerhetsinstruktion, förvaltning).
- Systemägaren ska besluta hur lagringsmedia med IT-systemets information ska avvecklas.

Det är kostnadseffektivt att i största möjliga utsträckning arbeta förebyggande med IT-säkerhet. Ett viktigt inslag i säkerhetsarbetet är därför att redan i utvecklings- och inköpsfasen av ett IT-system utreda säkerhetskraven på systemet samt behovet av reservrutiner för detta. Detta gäller även vid större förändringar av befintliga IT-system. Rutiner för detta är därför angelägna. De kan avse sådant som kraven på certifierade och evaluerade produkter, tester, testmiljö, tidpunkter för tester och införande m.m.

Utgångspunkten bör vara att köpta system och program ska vara certifierade av ett oberoende organ eller att de är framtagna och utgivna av betrodda leverantörer.

Det är viktigt att det finns en definierad beslutsprocess för hur nya eller vidareutvecklade system eller IT-utrustning ska tas i bruk. Bland annat måste man förvissa sig om att ny IT-utrustning eller programvara är kompatibel med andra systemkomponenter.

Rutiner för inköp och installation av program är särskilt viktiga i nätmiljöer. Risken för att t.ex. datavirus överförs till andra miljöer i det lokala nätet är överhängande om en arbetsplats har blivit smittad.

Om IT-system som hanterar sekretessbelagd information avvecklas och utrustning med lagringsutrymme använts för drift av systemet,

måste sådana lagringsutrymmen fysiskt förstöras eller överskrivas på ett säkert sätt i stället för att vanlig radering används.

6.2 Systemutveckling och systemunderhåll

Basnivå

- Det ska finnas utsedda systemadministratörer.
- Det ska finnas personal med ansvar för systemunderhåll.
- I avtal ska regleras hur känslig information ska hanteras i samband med service.
- Fjärrdiagnostik ska ske under kontrollerade former.
- Det ska finnas dokumenterade regler för rättning av data (IT-säkerhetsinstruktion, drift).
- Regler ska finnas för hur system- och programutveckling ska genomföras (IT-säkerhetsinstruktion, förvaltning).
- Beslut om programändringar ska fattas av systemägaren.
- System- och programutveckling ska ske åtskilt från driftmiljön.
- Olika behörigheter ska användas för drift- och utvecklingsmiljö.
- Unika identiteter ska användas för personer som ges behörighet för tester och utveckling.
- Tester av modifierade IT-system ska ske åtskilt från driftmiljön.
- Systemägaren fattar beslut om tidpunkt för installation av nya programversioner.
- Implementation av programvara i såväl drift- som utvecklingsmiljö ska ske av behörig personal.
- Utveckling och förändringar i program ska dokumenteras.
- Det ska finnas rutiner för hur kunskap om förvaltning ska återföras till den egna organisationen för egenutvecklade program som utvecklats externt.
- Det ska finnas rutiner för hur utbildning ska genomföras för köpta system, som även ska omfatta kompletterande utbildning vid program- och funktionsändringar.
- Tillgången till egenutvecklade IT-systems källkod ska regleras i avtal.
- Upphovsrättsliga frågor ska vara reglerade i avtal.

I systemunderhåll ingår att kontinuerligt styra och ändra IT-system, i syfte att säkerställa dess kvalitet och nytta i verksamheten.

Normalt bör förbindelse för fjärrdiagnostik vara nerkopplad och endast kopplas upp efter direkt överenskommelse vid varje enskilt tillfälle.

Regler för rättning av data bör minst omfatta:

- vem som är ansvarig för datakvaliteten
- hur ofta kontroller ska genomföras.

Förvaltningsinstruktion för utveckling bör omfatta:

- ansvar för systemutveckling
- modell för systemutveckling
- förvaltningsmodell knuten till systemutvecklingsmodellen
- ledning av utvecklingsprojekten
- behörighetskontroll.

Systemägaren är ansvarig för säkerhetsåtgärderna vid utveckling av IT-systemet. Begäran om programändring bör attesteras av systemägaren (funktionalitetsaspekten) och i samråd med IT-säkerhetschefen (säkerhetsaspekten).

Nyutveckling och programunderhåll bör skiljas åt. Som regel bedrivs nyutveckling i projektform där samtliga säkerhetskrav ska beaktas. Vid programunderhåll är det som regel enbart nödvändigt att granska de säkerhetsåtgärder som direkt berörs av de vidtagna åtgärderna.

Systemägaren ska fatta beslut om när en ny version ska införas för att säkerställa att alla versioner som tas i drift har godkänts med avseende på säkerhetsaspekten. Verifieringen av att IT-systemet uppfyller uppställda säkerhetsmål sker vid systemtesten och i produktionen.

Om det programutvecklingshjälpmedel som används har egna behörighetsfunktioner ska de utnyttjas på sådant sätt att de samverkar med och eventuellt kompletterar befintlig behörighetskontrollfunktion.

Samma ansvarsförhållanden gäller vid förändring av ett IT-system som vid anskaffning. Med förändring avses utveckling, modifiering m.m.

Det är viktigt att tillgången till källkoden för egenutvecklade IT-system regleras. Om källkoden endast finns hos leverantören av IT-systemet och denne exempelvis går i konkurs, kan detta medföra att man förlorar tillgången till den. Finns tillgång till källkoden kan produkten utvecklas/vidareutvecklas hos en annan leverantör.

En lösning kan vara att deponera källkoden hos en tredje part om annan överenskommelse inte går att träffa.

Av sekretesskäl kan det vara viktigt att reglera åtkomsten till källprogram/-arkiv.

6.3 Dokumentation

Basnivå

- För ett IT-system ska finnas:
  - systemdokumentation
  - driftdokumentation
  - användarhandledning.
- Systemdokumentationen ska omfatta:
  - vad IT-systemets olika delar består av
  - övergripande beskrivning av de olika delarnas uppgift
  - en detaljerad systembeskrivning.
- En kopia av systemdokumentationen i sin helhet ska förvaras väl skild från originalet.
- Systemdokumentation med känslig information ska endast vara åtkomlig för behörig personal.
- Det lokala nätverket, dess ingående komponenter och varje förändring av det ska dokumenteras.
- Kopia av driftdokumentationen ska förvaras skyddad och åtskild från driftstället.
- Driftdokumentationen ska ange vilka säkerhetsfunktioner som administratören kan påverka.
- Driftdokumentationen ska innehålla instruktioner om hur IT-systemet ska installeras och konfigureras.
- All dokumentation ska i rimlig omfattning och grad vara fullständig och aktuell samt uppdateras vid förändringar i IT-systemet.

En bra dokumentation, med rimliga krav på fullständighet och aktualitet, är en viktig förutsättning för en säker och ändamålsenlig förvaltning och drift av ett IT-system. Brister i dokumentationsregler och i dokumentationens kvalitet kan medföra svårigheter.

Anpassningar och modifieringar som görs på olika ställen i ett IT-system under årens lopp måste dokumenteras för att underlätta för-

ståelsen av systemuppbyggnaden och säkerheten. Behörighet att göra anpassningar och modifieringar, ansvaret för att göra sådana samt att de redovisas i systemdokumentationen bör regleras av systemägaren i IT-säkerhetsinstruktion, förvaltning.

Systemdokumentation

Systemdokumentationen riktas till den som ska underhålla och vidareutveckla IT-systemet och kan lämpligen delas in i en översiktlig och en detaljerad systembeskrivning.

Den översiktliga systembeskrivningen är till för att få en överblick över IT-systemet och förstå systemuppbyggnaden. Den kan t.ex. innehålla:

- en översikt som visar IT-systemets plats i organisationens totala datadrift
- det fysiska och logiska nätets struktur
- vilka delar/moduler systemet/programmet består av
- beskrivning av delarnas uppgift utan detaljer, gärna bilder som visar hur delarna är beroende av varandra
- viktiga datastrukturer, gärna med bilder.

Den detaljerade systembeskrivningen är till för den personal som ska genomföra förändringar eller tillföra nya funktioner. Den kan t.ex. innehålla:

- beskrivning av varje del/modul för sig
- beskrivning av datatyper
- en väl kommenterad programkod.

Delar av systemdokumentationen kan innehålla känsliga uppgifter om IT-systems säkerhetsfunktioner, t.ex. om behörighetskontrollsystemets uppbyggnad. Dokumentationen bör skyddas genom krav på erforderliga åtkomsträttigheter och ska hållas aktuell. I vissa fall kan det därför finnas behov av att reglera åtkomsten till dokumentationen.

Driftdokumentation

Driftdokumentation är till för den personal som ansvarar för den dagliga driften av ett IT-system. Klara instruktioner för hur systemet/produkten ska installeras och konfigureras måste ingå i driftdokumentationen.

Driftdokumentationen kan t.ex. omfatta:

- en översikt som visar IT-systemets plats i organisationens totala datadrift samt ingående utrustning
- det fysiska nätets struktur och ingående komponenter
- det logiska nätets struktur
- driftsinstruktioner för alla aktiviteter i driften
- konfigurationen, inställningar av olika parametrar i IT-systemet som t.ex. förändringar av defaultinställningar i operativsystem, routingtabeller
- telefonnummer till leverantörer eller motsvarande.

Användarhandledning

Användarhandledningen riktas till användare av IT-systemet. Den utformas med hänsyn till användarens kunskaper och behov och kan utgöras av:

- manual som riktas till normalanvändaren
- grundläggande användarguide som riktas till nybörjare. Kan eventuellt vara av lathundskaraktär.

Dokumentation över IT-system ska vara fullständig och aktuell och uppdateras vid alla former av förändringar i datasystemet. Detta är en förutsättning för att kunna förvalta, använda och förstå systemuppbyggnaden.

6.4 Skydd mot skadlig programkod

Basnivå

- Det ska finnas skydd mot skadlig programkod som ska:
  - minst omfatta detektering av sådan
  - uppdateras minst en gång i veckan
  - startas automatiskt.
- Systemägaren ska utifrån bedömd risk för angrepp av skadlig programkod vidta nödvändiga åtgärder.
- Rätten att installera nya program, programversioner eller att importera externa filer ska regleras och dokumenteras (IT-säkerhetsinstruktion, användare och/eller drift).

Skyddet mot skadlig programkod måste stå i relation till de skador ett angrepp kan förorsaka. Systemägaren ska därför göra en bedömning av risken för sådana angrepp och effekterna av dem och utifrån detta vidta åtgärder. Aktuella åtgärder mot skadlig programkod är sådana som bidrar till att:

- förebygga smitta från dem
- upptäcka dem
- förhindra smittspridning
- återställa ett smittat system.

Inga program mot skadlig programkod kan garantera ett komplett skydd eftersom nya typer av virus o.dyl. upptäcks kontinuerligt. Vissa antiprogram identifierar enbart förändringar i filer medan andra såväl identifierar den skadliga programkoden som tar bort den och reparerar skador den åstadkommit.

En viktig del av skyddet är att ha kontroll över vilka program som tillåts i IT-systemet och på vilket sätt information får tillföras detta, t.ex. via datamedia eller Internet. Rätten att installera program, nya versioner av program eller import av externa filer ska därför regleras i driftinstruktionen.

För IT-system som inte har kommunikation med andra system eller där program mot skadlig programkod inte kan användas av tekniska orsaker, kan systemägaren besluta att sådant skydd ej erfordras. I sådana fall är det ändå motiverat att installationer av nya program eller motsvarande sker under kontrollerade former för att förhindra virus o.dyl.

Detta kan t.ex. åstadkommas genom att nya program eller programversioner först testas i en isolerad miljö.

En annan möjlighet som bör beaktas för att skydda sig mot skadlig programkod är att dela upp organisationens nätverk i mindre enheter, så att en attack enbart drabbar en del av nätverket.

Program mot virus o.dyl. bör installeras på flera ställen i IT-miljön. Programmen kan vara av två typer, aktiva skydd eller passiva skydd (antingen i samma programvara eller som två olika programvaror). Den aktiva programvaran startas automatiskt, t.ex. vid uppstart av arbetsplatsen, och finns sedan i bakgrunden och letar kontinuerligt efter virus och virusliknande aktiviteter. Den kan även kontrollera program och datafiler innan de används.

Den passiva programvaran kan aktiveras vid specifika tidpunkter t.ex. vid låg belastning för att få en schemalagd körning.

På servern kan dess egna lagringsenheter sökas igenom med serverbaserade skydd. Sökningen kan ske i både programfiler och datafiler. Programvaran kan även ha funktioner för central administration och övervakning. Aktiva program medför prestandaförluster och är därför inte alltid så lämpliga i servern. På de lokala arbetsplatserna är det bra att ha både aktiva och passiva skydd. För bärbara datorer kan det vara lämpligt att göra kontroll innan påloggning sker till det lokala nätet.

6.5 Incidenter

Basnivå

Rutiner ska finnas fastlagda för hur:

- användare ska agera vid misstanke om intrång (IT-säkerhetsinstruktion, användare)
- incidenter ska hanteras (IT-säkerhetsinstruktion, drift)
- uppföljning av incidenter ska ske (IT-säkerhetsinstruktion, förvaltning).

Incidenter förekommer i de flesta organisationer. Upphovet till dem kan exempelvis vara interna eller externa intrång och intrångsförsök, felaktig användning av IT-systemen och IT-resurserna o.dyl. Att återkoppla erfarenheter från incidenter av olika slag är ett viktigt moment när det gäller att spåra brister och svagheter i IT-verksamheten. Riktlinjer för hur incidenter följs upp är därför angelägna.

6.6 Elförsörjning

Basnivå

- IT-utrustning som kräver avbrottsfri kraft ska identifieras och förses med sådan.
- UPS-utrustningars funktion ska testas regelbundet enligt leverantörens anvisningar.
- Elförsörjningen till centralt driftställe ska ske via en separat gruppcentral.

Med avbrottsfri kraft, s.k. UPS (Uninterruptible Power Supply) menas utrustning, vanligen batterier, som vid elavbrott försörjer IT-system med el under en kortare tid. Elförsörjningen med en UPS måste räcka den tid som behövs för att kunna stänga av aktuellt IT-system på ett sätt som gör att information inte går förlorad eller att reservkraftaggregat kan startas.

Utrustningar i ett IT-system som är av sådan betydelse att de ska utrustas med avbrottsfri kraft kan vara vissa viktiga servrar (exempelvis nätverksservrar) samt vissa kommunikationsutrustningar (exempelvis routrar).

Regelbundet måste kontrolleras att inte extra utrustningar som gör att UPS:ens kapacitet överskrids, ansluts till den avbrottsfria kraften.

Varje server bör ha en separat gruppledning. Kylanläggning, belysning m.m. bör anslutas till separat elcentral. En jordplint bör finnas i datorrummet.

Beroende på de fysiska förutsättningarna såsom elnät, stammar etc. kan olika nivåer av UPS inrättas. Generellt är det tillräckligt om centrala servrar och datakommunikationsutrustningar skyddas mot ett elbortfall på cirka ett par timmar.

6.7 Tillträdesskydd

Basnivå

- Beslut om vem som ska få tillträde till datorrum för att kunna utföra sina arbetsuppgifter ska fattas av systemägaren.
- Tillträde till datorrummet ska regleras (IT-säkerhetsinstruktion, förvaltning).
- För utrymmen med känslig information eller för IT-systems drift viktig dator- och kommunikationsutrustning ska gälla att:
  - tillträdet registreras och dessa uppgifter förvaras säkert
  - obemannade utrymmen låses
  - servicepersonal, städpersonal m.fl. ska, under övervakning, ges tillträde endast när detta krävs.

Tillträde till utrymmen med för IT-systems drift viktig dator- och kommunikationsutrustning kan regleras till vissa tider på dygnet. För att kunna följa upp vem som vid ett visst tillfälle besökt sådana utrymmen är det nödvändigt att besök registreras. Det kan exempelvis ske manuellt eller med kontrollsystem där in- och utpasseringar loggas.

Den enklaste formen av uppföljning är att alla tillfälliga, normalt ej behöriga, besök i aktuella utrymmen antecknas i en besöksliggare.

Om, som komplement till åtgärder för tillträdesskydd, stöldskydd i form av fastlåsning av utrustning används, rekommenderas att låsanordning som uppfyller Stöldskyddsföreningens normer väljs.

6.8 Klimat

Basnivå

- I direkt anslutning till för driften viktig dator- och kommunikationsutrustning ska det finnas kolsyresläckare i erforderligt antal.
- Brandbesiktning av datordriftställe ska genomföras i samråd med brandförsvaret.
- Brandlarm ska vara kopplat till larmmottagare.
- Larmsystem ska testas regelbundet.
- För datordriftställe ska gälla att
  - det ska placeras i brandsektionerat område
  - alla väggenomföringar ska vara brandtätade
  - utrymmet ska vara fritt från brännbart onödigt materiel.
- Det ska finnas möjlighet att reglera och mäta temperatur och fuktighet.
- Om utrymmen för datordrift har ledningar som innehåller vatten eller ånga ska åtgärder för fuktskydd vidtas.

Med hänsyn till de kapitalinvesteringar som gjorts i utrustningar kan andra säkerhetsåtgärder vara motiverade. Sådana kan t.ex. vara att låta datordriftstället och utrymmen för klimat- och elinstallationer var för sig utgöra separata brandceller.

Om larmindikationen går till plats inom organisationen bör denna vara under ständig observation. Vid brandlarm bör brandkårens personal vara informerad om lokalernas utformning. Utrymmen för datordrift kan ha hög grad av inbrottsskydd med bl.a. betongväggar och ståldörrar, som kan göra att de är svåra och tidsödande att nå. Det måste därför säkerställas att Brandförsvaret ges möjligheter till snabbt tillträde.

All elektronik är mycket känslig för den rök som bildas vid brand i plastmaterial som exempelvis elkablar.

Helst bör utrymme med för driften viktig dator- och kommunikationsutrustning vara utrustad med automatisk släckningsanordning.

6.9 Säkerhetskopiering och lagring

Basnivå

- Säkerhetskopiering ska göras regelbundet.
- Systemägaren ska besluta och dokumentera (IT-säkerhetsinstruktion, drift):
  - vilken information som ska omfattas av säkerhetskopiering
  - intervallen för kopiering
  - hur många generationer säkerhetskopior som ska finnas
  - hur säkerhetskopior ska förvaras
  - om vissa säkerhetskopior ska förvaras på plats geografiskt skild från driftstället.
- Systemägaren ska besluta om och när kontroll av säkerhetskopiornas läsbarhet ska genomföras och detta ska dokumenteras (IT-säkerhetsinstruktion, drift).
- Systemägaren ska besluta om förvaring av och åtkomst till källkod för egenutvecklat IT-system.
- Systemägaren ska fastställa vilken information, lagrad på datamedia, som ska omfattas av särskilda förvaringsrutiner så att den inte kan läsas av obehöriga.
- Åtgärder som ska vidtas för att säkra att informationen är läsbar under hela förvaringstiden ska dokumenteras (IT-säkerhetsinstruktion, drift).
- För datamedia ska finnas regler (IT-säkerhetsinstruktion, drift) för:
  - förvaringstid för datamedia
  - klassning av datamedia
  - hur datamedia ska märkas och förtecknas.
- Datamedia, med för verksamheten väsentlig information, ska förvaras i skåp som är konstruerade för ändamålet.
- Endast behöriga personer ska ha tillgång till media med för verksamheten väsentlig information.
- Rutiner ska finnas för att spåra om datamedia med känslig information har bortförts från de lokaler de normalt förvaras i.
- Systemägaren ska besluta vilka åtgärder som ska vidtas vid fysisk transport av för verksamheten känslig information (IT-säkerhetsinstruktion, förvaltning).

Intervallen för säkerhetskopiering bestäms utifrån verksamhetens krav på informationens aktualitet vid återstart från säkerhetskopia. Systemägaren ska därför tillsammans med verksamhetsansvarig, om denne inte är systemägaren, i driftinstruktion fastställa reglerna för säkerhetskopiering av information.

I de flesta fall sker säkerhetskopiering i en för flera IT-system gemensam driftmiljö av särskilt utsedd personal. I sådana fall måste intervallet för säkerhetskopiering utgå från den verksamhet som har de högst ställda kraven på informationens aktualitet vid återstart. Av systemägarens beslut om säkerhetskopiering måste därför intervallet framgå men även hur säkerhetskopieringen ska genomföras. Säkerhetskopiering kan omfatta kopiering av all information eller kopiering av de förändringar som skett efter senaste kopieringstillfälle.

Ett beslut om säkerhetskopiering kan t.ex. bestämma att en kopia på dagliga förändringar förvaras i ett arbetsarkiv, att en veckokopia av all information förvaras i säkerhetsarkiv samt att en månadskopia av all information förvaras på en plats geografiskt skild från datadriftstället.

Åtgärder för att skydda information som lagras på datamedia kan delas upp i två typer. Dels sådana som är generella för alla datamedia dels sådana som avser datamedia som ska omfattas av särskilda förvaringsrutiner. För att kunna bedöma vilka datamedia, med för verksamheten väsentlig information, som ska skyddas mot obehörig åtkomst måste informationen som lagras på dessa datamedia klassas. Datamedia kan vara disketter, diskar i servrar, klienter eller minnen i bärbara datorer, men även utskrifter från IT-system. Klassningen, som beskrivs i avsnitt 5.4, måste ta hänsyn till gällande lagar och föreskrifter samt verksamhetens krav, liksom även till det värde som informationen har för verksamheten. Även andra intressenters specifika krav måste beaktas. Klassningen avgör vilka datamedia som ska omfattas av särskilda förvaringsrutiner.

Av säkerhetsinstruktionen ska framgå hur sådan datamedia ska förvaras, exempelvis om säkerhets- eller värdeskåp ska användas till vilka endast behöriga personer har tillgång.

Datamedia är mycket känsliga för värme och rök och måste därför förvaras i utrymme särskilt konstruerat för ändamålet. Systemägaren beslutar vilka förvaringsutrymmen som får användas.

Exempel på bestämmelser som styr vad som ska gälla för förvaringstid av information lagrad på media är arkivlagen och Riksarkivets

författningssamling. Se vidare Sveriges Provnings- och Forskningsinstituts (SP) information.

På lagringsmedia kan information av olika klassningsgrad förekomma. Det är därför viktigt att även datamedia omfattas av klassning.

Märkning och förteckning av datamedia bör gälla alla datamedier som hanteras inom organisationen, såväl användarnas som driftorganisationens. Märkningen bör innehålla uppgifter om systemtillhörighet och en unik identitetsuppgift eller motsvarande. Avsikten med märkning och förteckning är att datamedia inte ska förväxlas. Även säkerhetskopior och motsvarande bör märkas och förtecknas.

Det bör finnas särskilt tillträdesskydd till utrymme där datamedia förvaras, t.ex. säkerhetsskåp.

Det finns risk för att informationsmedia som fysiskt transporteras, exempelvis via post eller bud, kan utsättas för obehörig åtkomst, missbruk eller förvanskning. En bedömning måste därför göras, utifrån känsligheten i informationen, av hur datamedia ska emballeras, fysiskt förflyttas och av vem. Användning av kryptering och digitala signaturer bör övervägas.

6.10 Driftadministration

BASNIVÅ

- För drift av IT-system ska finnas en fastställd plan för:
  - bemanning
  - kompetenskrav
  - ersättare för systemadministratör.
- Driftjournal ska föras vid varje driftställe.
- Installation av nya programversioner ska noteras i driftjournal.
- Systemägaren ska besluta i vilken omfattning driften ska följas upp.
- Endast utsedd behörig ska ha rätt att installera nya program i nätverket.
- Det ska finnas dokumenterade procedurer för installationer av funktioner i nätet (IT-säkerhetsinstruktion, drift).

Driften av IT-systemet får inte byggas upp runt enbart en person. Detta är dock ofta fallet, speciellt i små organisationer. Om verksamheten

kräver en kontinuerlig drift av IT-systemet måste åtgärder vidtas för att kunna hantera situationer med begränsad personalstyrka under exempelvis semestertider och vid sjukdom. Det ska därför finnas fastställda bemanningsregler som anger vilka befattningshavare och vilken kompetens som krävs för drift etc. av IT-systemet. I de flesta fall innebär det också att det måste finnas en ersättare för systemadministratören med tillräcklig kunskapsnivå. För att kunna fullgöra sina uppgifter måste personalen för systemadministration få erforderlig arbetstid avsatt för kunskapsinhämtning och regelbunden utbildning.

Grunden för att säkerställa driftsäkerheten är att organisation och ansvar för den ordinarie driften av datasystemet är tydligt, att dokumentation är tillgänglig samt att befattningshavare har rätt utbildning. Att ansvaret för olika kontroller och uppföljningsmoment är fördelat är också väsentligt, liksom åtgärder för att upptäcka och korrigera fel. Allt detta i syfte att begränsa konsekvenserna för verksamheten vid fel eller avbrott i driften.

Ansvariga administratörer ska utses och namnges och tillräcklig arbetstid måste sättas av för dem så att de kan fullgöra sina arbetsuppgifter.

I den driftjournal som bör finnas vid varje driftställe som komplement till befintlig logg bör noteras de händelser som påverkat driftsituationen, t.ex. igångsättning och avstängning av IT-systemet, kopiering av sekundärminnen eller driftstörning. Om IT-systemet måste stängas av noteras slut- och starttid samt anledning till att man frångår normala reglerade tidpunkter för avstängning och igångsättning av IT-systemet. En driftjournal kan föras maskinellt eller manuellt.

7. Datakommunikation

7.1 Intern kommunikation

Basnivå

- Det ska finnas en ansvarig person för varje del av i nätverket ingående LAN eller nätsegment.
- Nätadministrationen ska skiljas från ordinarie systemadministration och underhåll av IT-systemet.
- Det ska finnas särskild behörighet till nätverket utöver den för respektive applikation.
- Samtliga administratörer ska inte ha fullständiga systembehörigheter, utan endast i den utsträckning som krävs för arbetsuppgifterna.
- Routingtabeller etc. ska endast vara åtkomliga för behöriga administratörer.
- Servrar ska skyddas genom behörighetskontrollsystem i operativsystemet eller genom att endast ge användarna tillgång till servern via en nätapplikation.
- För anslutningar mellan säkerhetsdomäner ska finnas dokumenterade riktlinjer för vad som är tillåtet.

Administrationen av bryggor och routrar m.m. bör vara knuten till ansvaret för övriga delar av nätet. Nätadministratören bör ha ansvar för att t.ex. konfigurera servrar, routrar och namnservrar och ska arbeta tillsammans med säkerhetspersonal för att upprätthålla säkerheten i nätet. Dessutom bör åtminstone en ersättare vara utsedd, som har tillräckliga kunskaper för att vid behov kunna träda in i den ordinaries ställe.

Åtkomstkontrollen bör bygga på säkerhetsdomäner. En domän bör vara ett visst verksamhetsområde som omfattar vissa IT-system och användare som lyder under samma säkerhetsregler och som har en gemensam säkerhetsadministration. Vid anslutning till andra säker-

hetsdomäner, kan åtkomstkontrollen baseras på adresser och protokoll, d.v.s. begränsas till routerfiltrering eller ske på högre nivå i OSI-skiktet, t.ex. på applikationsnivå.

Riktlinjerna för anslutningar mellan säkerhetsdomäner bör innehålla information om möjliga trafikriktningar, protokolltyper och tjänster.

Normalt ska inte samtliga administratörer ha fullständiga systembehörigheter utan endast vad som krävs för att fullgöra sina arbetsuppgifter.

Routingtabeller etc. måste skyddas mot obehörig insyn och förändring genom lösenord eller motsvarande.

Det behöver inte ställas krav på upprepad autenticering av användare, när de använder nätapplikationen, om autenticeringen ägt rum vid arbetsstationen. Nätapplikationen kan få information om användaridentiteter genom data från klientapplikationen eller genom att identifiera nätadressen.

7.2 Externa anslutningar

BASNIVÅ

- Systemägaren ska fastställa vilka och vilken typ av anslutningar till tele- och datanät som ska tillåtas.
- Beslut om anslutningar till tele- och datanät ska dokumenteras.
- Det ska finnas en aktuell förteckning över samtliga externa anslutningar.
- Systemägarens ansvar vid dataöverföring till och från IT-systemet ska klargöras.
- Systemägaren ska ta ställning till om nätoperatörens tjänster uppfyller verksamhetens säkerhetskrav.
- Om fjärrdiagnostik används ska sådan ske enligt fastställda rutiner.
- Det ska regelbundet kontrolleras vilka uppkopplingar som finns mot ett IT-system.
- Utifrån systemägarens krav ska behovet av autenticeringsmetod vid externa anslutningar klarläggas.
- Det ska finnas regler för hur autenticering ska ske vid externa anslutningar (IT-säkerhetsinstruktion, förvaltning).

Det är viktigt att systemägaren har klart för sig vad dennes ansvar vid dataöverföring till och från IT-systemet innebär, exempelvis i händelse av förlust eller förändring av data eller avseende säkerhetsåtgärder vid sändning/mottagning av data.

Om dataöverföring sker mellan två organisationer med skilda ansvar är det systemägaren för det mottagande IT-systemet som ansvarar för informationen från det att den kommer in i IT-systemet. En samverkan i säkerhetsfrågor mellan de båda systemägarna och mellan dessa och nätoperatören måste därför ske.

Systemägaren måste också beakta att ansvarsfrågorna kompliceras av att dataöverföringen ofta sker med hjälp av kommunikationslinjer och annan kommunikationsutrustning över vilka systemägaren inte förfogar. En separat nätoperatör har ofta ansvaret för att överföringen tekniskt fungerar i enlighet med överenskomna specifikationer. Detta innebär också att nätoperatören är ansvarig för de säkerhetsåtgärder som behövs för att skydda utrustningen i nätet. Nätoperatören är i sin tur beroende av att nätägaren upprätthåller en god säkerhet.

Den säkerhetsnivå som definieras av systemsäkerhetsplanens krav på ett IT-system ställer också indirekta krav på eventuella externa kommunikationer och kommunikationstjänster. Systemägaren behöver kännedom om vilka säkerhetskrav som tekniken och köpta kommunikationstjänster kan uppfylla. Det kan visa sig att kompletterande egna åtgärder måste vidtas.

Alternativa vägar vid sidan av organisationens brandvägg (se avsnitt 7.3) i form av uppringande eller uppringningsbara modem in till det interna nätverket måste undvikas för att det inte ska vara möjligt att kringgå det skydd som brandväggen ger. En aktuell förteckning över samtliga anslutningar gör det möjligt att regelbundet identifiera dem som godkänts. Att anslutningar inte otillåtet etablerats kan då kontrolleras. Detta inkluderar även alla former av anslutningar för underhåll och service av leverantörer och eventuell fjärrdiagnostik.

Förteckningen över externa anslutningar i form av modem och andra åtkomstvägar bör för varje förbindelse innehålla:

- telefonnummer
- plats för uppringningsutrustningens anslutning, maskinnamn, o.s.v.
- typ av ansluten utrustning med referens till teknisk beskrivning av de förbindelser som finns upprättade.

Det finns olika typer av autenticeringsmetoder med olika grad av skydd. Val av metod görs mot bakgrund av riskanalyser. Bland olika metoder märks sådana som baseras på krypteringsteknik, aktiva kort, utnyttjande av anrops/svarsprotokoll och motringningsrutiner.

7.3 Brandväggar

Basnivå

- Det ska finnas en brandväggsfunktion installerad.
- Brandväggen ska vara den enda kanalen för IP-baserad datakommunikation till och från organisationen.
- Ansvaret för administration av brandväggen ska dokumenteras (IT-säkerhetsinstruktion, förvaltning).
- Brandväggens utformning och konfiguration ska dokumenteras.
- Brandväggen ska vara försedd med skydd mot skadlig programkod.
- Systemägaren ska besluta (IT-säkerhetsinstruktion, förvaltning):
  - vad som ska loggas i brandväggen
  - vem som ansvarar för uppföljningen av loggarna
  - hur ofta uppföljning ska ske
  - hur länge loggarna ska sparas.

En brandvägg består av en eller flera nätkomponenter som placeras mellan två datanät för att enligt en fastställd policy kontrollera och begränsa trafiken mellan dem. All trafik mellan datanäten ska passera genom brandväggen och endast trafik som är godkänd enligt policyn ska tillåtas passera. Brandväggen måste även kunna skydda sig själv mot angrepp. En brandvägg består dels av de komponenter som ingår i själva funktionen, oftast routrar och datorer med särskild programvara som ger möjlighet att kontrollera trafiken mellan nätverk, dels av organisationen kring brandväggen.

Brandväggen styr vilken datakommunikation som tillåts till och från verksamheten och har därför en mycket central roll. Den är normalt gemensam för ett flertal system, vilket gör att enskilda systemägare inte ensamma kan besluta om hur policyn ska utformas och hur brandväggen ska konfigureras. Varje verksamhet måste i samråd med varandra och med brandväggsadministratören besluta om hur konfi-

gurationen och ändringar av den ska göras. Den säkerhetsnivå man kräver avgör valet av brandvägg.

Utgångspunkten ska vara att all IP-baserad datakommunikation ska gå genom en brandväggsfunktion. Telefoni via Internet är en teknik som är på stark frammarsch. Sådan IP-telefoni är en röstkommunikation som går över ett kombinerat nätverk för data och tal via ett IP-datanätverk. Ett problem har varit att många valt att inte låta IP-telefonitrafiken går genom brandväggen. Skälet till detta har varit att samtalskvaliteten inte ska försämras, men idag finns brandväggsprodukter som löser detta problem.

En brandvägg kräver noggrann installation och en genomtänkt policy för att nå avsedd skyddseffekt. Som regel är brandväggen en gemensam resurs för en organisation vilket innebär att dess säkerhetsnivå måste ta hänsyn till säkerhetskrav från flera verksamhetsområden.

Exempel på frågeställningar som kan vara aktuella när policyn för en brandvägg ska utformas är följande:

- vilka tjänster ska brandväggen tillhandahålla
- vilka uppgifter ska döljas av brandväggen, exempelvis strukturen på det egna nätet, egna ip-adresser och användaridentitet
- vad ska loggas i brandväggen
- ska e-post kontrolleras i brandväggen
- ska viruskontroll ske i brandväggen
- vilken kontroll ska ske av Internetaccess/loggning
- krävs integritetskontroll av brandväggsprogramvara
- vilken övervakning ska ske, logiskt av vad och när, rapportering
- vilket fysiskt skydd behövs för brandväggen (begränsad tillträdeszon)
- hur ska brandväggsadministrationen ordnas
- vilken autenticeringskrav ska gälla för brandväggen, t.ex. vid fjärråtkomst (remote access)
- vad ska säkerhetskopieras.

Att administrera en brandvägg är komplicerat och kräver ingående kunskaper om såväl hur den konfigureras som om den verksamhet den ska skydda. En person bör därför utses som ansvarig för adminis-

trationen av brandväggen. En komplett dokumentation omfattar utformningen av brandväggsprodukten, tillhörande tjänsteservrar, underliggande system som agerar i värddator för produkten samt den nätverksteknik som används. Det bör observeras att information om brandväggens egenskaper kan vara känslig och bör hanteras i enlighet med detta.

Brandväggar finns av följande huvudtyper:

Paketfiltrerande router
En brandvägg av den här typen använder en router och en uppsättning regler som gäller för vilka paket som ska släppas igenom eller inte. Reglerna baseras på avsändarens adress, mottagardatorns adress och tjänst. All denna information ligger i filhuvudet till varje inkommande paket. Den här typen av brandvägg ger relativt låg säkerhet, men till låg kostnad och med minimala problem. Det finns olika typer av verktyg (menyer) som underlättar att konfigurera reglerna för filtreringen.

En paketfiltrerande router kallas även Packet-filtering Gateway eller Network-Level Firewall.

Application Gateways
En brandvägg av denna typ använder serverprogram (proxies) som körs i brandväggen. Dessa proxies tar emot en extern begäran, undersöker den och vidarebefordrar en godkänd begäran till en intern host (dator) som kan ge den efterfrågade tjänsten. En brandvägg av typen Application Gateway kallas även Proxyserver eller Application-Level Firewall.

Skillnaden mellan filtrerande router och application gateway kan sägas vara att den förra bara kollar uppkopplingen, medan den senare även kollar vad uppkopplingen användstill.

Hybrid Gateways
Genom att kombinera de olika brandväggstyperna, så att man låter trafiken först gå igenom en filtrerande router och sedan en application gateway har man skapat en hybrid gateway.

Stateful Inspection
Stateful Inspection är en filtrerande router som inte bara kontrollerar att datapaketen som anländer har en godkänd avsändar- och mottagaradress utan även analyserar paketens innehåll.

Val av brandvägg:

Om verksamheten kräver högsta möjliga säkerhet ska all internettrafik gå genom en Application Gateway, där det finns en proxy för varje tjänst som tillåts. I praktiken kan Stateful Inspection vara lika säkert. Totalt modemförbud, stark autenticering och så fullständig loggning som möjligt ska tillämpas.

7.4 Elektronisk post

Basnivå

Det ska finnas dokumenterade regler (IT-säkerhetsinstruktion, användare) för:

- vilken information som får skickas med elektronisk post
- filöverföring via elektronisk post som minst omfattar viruskontroll av meddelanden och bifogade filer.

En analys bör genomföras för att klarlägga vilka säkerhetsåtgärder som krävs för användning av elektronisk post. De hot som bör beaktas vid en sådan analys är:

- avlyssning av meddelande
- hinder så att meddelande inte kommer fram (t.ex. s.k. mailbombning)
- modifiering av innehållet
- modifiering av avsändare.

System för elektronisk post består av två delsystem. User agent är den programvara man installerar i klienten och Transfer agent är programvaran som förflyttar data mellan sändare och mottagare. User agent implementerar ofta protokollet MIME (Multipurpose Internet Mail Extension) som är en funktion som tillåter brevmeddelanden att bifoga bilder, röster, videofilmer eller textfiler. MIME är en potentiell källa för lagring av virus, logiska bomber och liknande.

Elektronisk post kan modifieras antingen i mottagarens brevlåda eller i det s.k. Postkontoret som ligger i servern. Där mellanlagras alla brev som skickas till och från användarna. Det finns idag ingen helt säker e-posthantering. Kryptering och digital signatur är idag de enda kända åtgärderna för att motverka hot mot e-posthantering.

De regler som gäller för vilken information som får skickas med elektronisk post bör minst omfatta klassificering av informationen med utgångspunkt från lagstiftningens och verksamhetens krav.

De bör även innehålla regler för:

- vilka användare som ska ha tillgång till e-postsystem
- vilka information som ska krypteras och vilken som ska ha digital signatur
- kryptering, nyckelhantering och nyckelöverföring
- nätövervakning, kontroll av angrepp och behörighetskontrollsystem
- val av standardprotokoll och datakommunikationsalternativ
- funktioner för användarstöd inom organisationen.

För organisationer bör det vara reglerat hur inkommande ärenden via elektronisk post ska registreras. Hänsyn måste tas till de regler som gäller för allmänna handlingar. Detta kan innebära särskilda rutiner främst för användare och registrator.

7.5 Trådlösa nät

BASNIVÅ

- Används trådlösa lokala nät, ska nätverkets systemägare besluta om åtgärder mot obehörig avlyssning och utnyttjande ska vidtas.

Allt fler organisationer bygger upp trådlösa nät för sin verksamhet, s.k. WLAN (Wireless Local Area Net). Dessa består av basstationer (accesspunkter) som sammanbinds med radiokommunikation och trådlösa klienter som exempelvis kan vara bärbara eller stationära PC och handdatorer. Det vanligaste är att det trådlösa nätet är en förlängning av ett existerande trådbaserat nät, men helt trådlösa nätverk kan även byggas upp.

Trådlösa nätverk får inte det fysiska skydd som trådbaserade nät har, där nätverkskablar är dragna inne i en byggnader. Radiovågorna når även platser som man inte har kontroll över. En risk när det gäller trådlösa nät är att falska accesspunkter kan sättas upp utanför en byggnad i syfte att locka till sig klienter inom byggnaden och därigenom exempelvis lura av användarna deras lösenord. För trådlösa nät-

verks infrastruktur finns inte bara behov av autenticering av klienter utan klienter bör även kräva autenticering av infrastrukturen.

En annan viktig aspekt när det gäller säkerheten är skyddet mot avbrott. Väggar och inredning kan störa radiovågornas utbredning så att man får dålig eller ingen täckning. Störningar kan dessutom variera över tiden och därför vara svåra att lokalisera.

Ett trådlöst nät kan störas av annan radioutrustning. Störningar kan även komma från den egna utrustningen genom att radiovågor reflekteras och kommer i motfas mot den direkta signalen och släcker ut den. Även om de trådlösa näten och de tekniker för överföring som används är toleranta mot störningar, bör störningsrisken beaktas vid en installation.

Utifrån vissa aspekter kan ett trådlöst nät betraktas som mer säkert mot avbrott än ett trådbaserat. Att skada en kabel är lätt, avsiktligt eller oavsiktligt, och felet kan vara svårt att lokalisera. En accesspunkt som sätts upp på en skyddad plats är mycket svårare att sätta ur funktion genom fysisk påverkan. Den kan dock sättas ur funktion genom aktiv störning.

Varje accesspunkt i ett trådlöst nät sänder med täta intervaller ut sin identitet och detta kan avlyssnas och utnyttjas för att obehörigt tas sig in i nätet. Det finns därför ingen garanti för att en accesspunkt med rätt identitet tillhör nätet. Vem som helst kan ju konfigurera en accesspunkt.

ACL (Access Control List) är en funktion som ofta byggs in i accesspunkterna. En station som inte finns med på en accesspunkts ACL kan inte kommunicera med denna. I ACL, som lagras i accesspunkten, lägger nätverksadministratören in de MAC-adresser (nätverkskort) som ska ges tillgång till nätet. Detta ger en viss säkerhet, men kräver en hel del administration för att hållas aktuell. Ett problem är att MAC-adresser aldrig kodas ens om krypteringsalgoritmen WEP används och att det går att ändra MAC-adress på ett nätverkskort med hjälp av särskild mjukvara. Även om det är möjligt att ta reda på en MAC-adress och sedan lura accesspunkten att släppa in en obehörig, är dock ACL en barriär som en inkräktare måste ta sig igenom och därför bidrar till ökad säkerhet.

Standarderna för trådlösa nät innehåller en säkerhetslösning som omfattar såväl autenticering och kryptering som integritetskontroll. Denna säkerhetslösning kallas WEP (Wired Equivalent Privacy). Avsikten med WEP är att hindra att man alltför lätt ska kunna ta sig in i

eller avlyssna nätet med hjälp av lätt tillgänglig utrustning som en bärbar PC. WEP är ingen heltäckande säkerhetslösning utan bör kombineras med andra lösningar. Kryptolösningen för WEP har en svaghet, eftersom kryptonycklarna är statiska, d.v.s. att de inte ändras med tiden, och att de dessutom är gemensamma för alla användare. Vidare saknar standarden en metod för distribution av nycklar. Arbete pågår på olika håll för att stärka krypteringsfunktionerna i WLAN. Det är vanligt att krypteringsnyckeln för ett WLAN lagras i hårdvaran, vilket innebär att om någon stjäl hårdvaran så har denne full tillgång till nätverket.

Ytterligare exempel på hur man kan skydda sig mot intrång är att placera det trådlösa nätet utanför en brandvägg och använda VPN-klienter. Ett annat exempel är att bygga in säkerheten i applikationerna snarare än i nätverket självt och t.ex. låta applikationerna ta hand om krypteringen.

En annan risk i ett WLAN är att någon tar sig in i nätverket och oavbrutet sänder data vilket leder till att alla andra stationer i nätverket står och väntar på sin tur. På detta vis kan ett helt nätverk blockeras.

8. Kontinuitetsplanering

Basnivå

- Systemägaren ska besluta om den längsta tid som IT-systemet bedöms kunna vara ur funktion innan verksamheten äventyras.
- Det ska finnas en avbrottsplan som ska omfatta de återstarts- och reservrutiner för datadriften som vidtas inom ramen för ordinarie drift för att IT-systemet ska kunna återstartas inom fastställd tid.
- Avbrottsplanen ska dokumenteras.
- Omständigheter som ska betecknas som katastrof för verksamheten ska klarläggas.
- Test av att IT-systemet kan återstartas från säkerhetskopior ska genomföras regelbundet om detta är praktiskt möjligt.
- Återstartsrutiner ska:
  - finnas för IT-system
  - dokumenteras (IT-säkerhetsinstruktion, drift).
- Befintliga reservrutiner ska dokumenteras (IT-säkerhetsinstruktion, drift).
- Datamedia och säkerhetskopior av dessa ska förvaras i olika brandceller eller särskilt utformade förvaringsutrymmen.

Kontinuitetsplaneringen är en process som bl.a. innebär att ta fram en avbrottsplan och en katastrofplan.

Avbrottsplan

Avbrottsplaneringen måste anpassas till hur kritiskt IT-systemet är för verksamheten och vara en integrerad del i det totala säkerhetsarbetet för verksamheten. Därför måste IT-systemen ges en prioritetsordning. Utgångspunkt för avbrottsplaneringen är systemsäkerhetsplanen. I systemsäkerhetsplanen definieras bl.a. vilka krav verksamheten ställer på tillgängligheten till IT-systemet. Systemägaren ska därför besluta

om det längsta avbrott som kan accepteras för att inte verksamheten ska äventyras. Avbrottsplaneringen utgår från att återstart ska kunna ske innan denna avbrottstid passerats.

Avbrottsplanen ska beskriva de åtgärder som ska säkerställa fortsatt verksamhet vid störning eller avbrott i IT-driften inom en viss tid och redovisa de reserv- och återstartsrutiner för IT-driften som krävs för detta. Ett stort antal åtgärder kan därvid vara aktuella.

De områden, med inriktning mot detta, som redovisas i KBM:s rekommendationer och de avsnitt de redovisas i är:

- dokumentation (6.3 Dokumentation)
- bemanning (6.10 Driftadministration)
- brand (6.8 Klimat)
- skydd mot skadlig programkod (6.4 Skydd mot skadlig programkod)
- elförsörjning (6.6 Elförsörjning)
- säkerhetskopiering och förvaring av datamedia (6.9 Säkerhetskopiering och lagring).

Utöver detta finns andra områden som kan vara aktuella att beakta, t.ex.:

- redundans, speglade diskar, raidteknik, cluster etc.
- alternativa kommunikationsvägar
- felhantering
- återstartsrutiner.

Det är också viktigt att reglera ansvarsförhållanden vid avbrottssituationer, exempelvis ansvaret för de åtgärder som krävs för att hantera den uppkomna situationen.

Avbrottsplanen ska dokumenteras, antingen som ett särskilt avsnitt i driftinstruktionen och/eller driftdokumentationen med hänvisningar till andra delar av densamma eller som en fristående avbrottsplan.

Katastrofplan

Organisationens ledning ska överväga om det finns särskilda skäl att upprätta en katastrofplan. Utgångspunkten för en katastrofplan är att verksamhetsledningen ska bedöma vilka omständigheter som skulle medföra konsekvenser som betecknas som katastrofala för verksamheten. En katastrofsituation behöver inte endast uppstå vid ett avbrott

i verksamheten, utan även genom att sekretessbelagda uppgifter blir åtkomliga för obehöriga. Likaså kan brister i riktigheten i informationen medföra att felaktiga beslut tas som leder till allvarlig ekonomisk skada för en organisation.

Katastrofplanering är därmed en process som till stor del måste ledas och inriktas av verksamhetsledningen och har som mål att skapa förutsättningar för att upprätta en katastrofledning som operativt ska kunna leda verksamheten.

9. Driftgodkännande

Basnivå

- IT-system ska driftgodkännas av systemägaren.
- Driftgodkännande ska ske mot systemsäkerhetsplanens krav.
- Beslutsunderlaget för driftgodkännande ska innehålla en sammanfattning med förslag till beslut om att IT-systemet antingen ska driftgodkännas, driftgodkännas med krav på kompletterande säkerhetsåtgärder eller inte driftgodkännas.
- Beslut om driftgodkännande, eventuellt med krav på kompletterande säkerhetsåtgärder, eller inte driftgodkännande ska dokumenteras.
- Beslut om driftgodkännande av ett IT-system ska redovisa hur kraven enligt IT-systemets systemsäkerhetsplan är tillgodosedda.
- Vid förändringar i IT-systemet ska från fall till fall bedömas om driftgodkännandet måste förnyas.
- Central systemägare ska fastställa:
  - vilka gemensamma delar av IT-systemet som ska driftgodkännas centralt
  - vad som ska driftgodkännas lokalt.
- Underlag för lokalt driftgodkännande ska ange vilka delar av IT-systemet som ska driftgodkännas lokalt och vilka förutsättningar som gäller för detta.
- Av ett IT-systems driftgodkännande ska avgränsningarna till andra IT-system framgå.

Driftgodkännande avser den process som utmynnar i ett formellt beslut som fastställer att ett IT-system i en given miljö uppfyller ställda säkerhetskrav. Normalt är det systemägaren som beslutar om driftgodkännande. Jämförelser mellan krav och vidtagna åtgärder kan i

allmänhet inte uttryckas i absoluta mått, utan görs oftast i allmänt formulerade nivåtermer.

Före driftgodkännande sker en granskning av IT-systemets säkerhet av personal som systemägaren utser. Granskningen omfattar ett enskilt IT-system, där avgränsningar mot andra IT-system ska framgå av systemsäkerhetsplanen och utvärderas med avseende på hur basnivån och övriga krav enligt systemsäkerhetsplanen uppfylls.

Om beslutet är driftgodkännande efter kompletterande säkerhetsåtgärder ska i beslutet anges en tidpunkt då identifierade brister ska vara åtgärdade för att driftgodkännandet ska vara giltigt. Den tidpunkten bör inte ligga längre än cirka ett halvår framåt.

För att systemägare inom en organisation ska kunna ta ansvar för säkerhetsskyddet för IT-system som används av flera organisationer, krävs att denne, som då är central systemägare, dels granskar de gemensamma delarna av IT-systemet och dels sammanställer ett underlag för övriga organisationers driftgodkännande.

Central systemägare ska fastställa vilka gemensamma delar av IT-systemet som ska granskas centralt. Gemensamma delar kan t.ex. vara:

- teknisk plattform
- infrastruktur, nät och nättjänster
- program, applikationer.

Resultatet av den gemensamma granskningen ska ingå i underlaget för lokalt driftgodkännande och av underlaget ska framgå vilka delar av IT-systemet som ska driftgodkännas lokalt och vilka förutsättningar som gäller för detta.

Ansvarsgränserna är av stor betydelse, varför underlaget för organisationers driftgodkännande måste innehålla en tydlig gränsdragning mellan centrala och lokala ansvarsområden. Vidare måste underlaget innehålla en beskrivning och värdering av tekniska och administrativa säkerhetsåtgärder från ett centralt perspektiv, det vill säga de förutsättningar som är gemensamma för alla som använder IT-systemet.

ISBN: 91-85053-35-X

Krisberedskapsmyndigheten

Box 599
101 31 Stockholm

Tel 08-593 710 00
Fax 08-593 710 01

kbm@krisberedskaps
myndigheten.se

www.krisberedskaps
myndigheten.se