STATSKONTORET 1997:29 c

Handbok i IT-säkerhet

Del III

Skyddsåtgärder

STATSKONTORET 1997:29 c

Handbok i IT-säkerhet

Del III

Skyddsåtgärder

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 91-7220-299-8

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 3

1 Inledning

Denna del av handboken syftar till att informera om olika former av skyddsåtgärder med tillhörande administrativa åtgärder. Vi gör en genomgång av olika driftmiljöer och behandlar de olika krav på säkerhet som finns i respektive driftmiljö med exempel på lämpliga skyddsåtgärder.

Vidare behandlas kortfattat olika former av fysisk säkerhet samt olika standardiseringsorgan.

2 Grundkrav

I detta avsnitt behandlas de grundläggande aspekterna kring IT-säkerhet. Syftet är att strukturera de olika aspekterna på säkerheten i några tydliga och behandlingsbara områden.

2.1 Riktighet

Begreppet riktighet är ett samlingsbegrepp för begreppen personintegritet, systemintegritet och kvalitet. Med integritet menas att helheten ska skyddas mot obehörig förändring.

Förlust av riktighet innefattar alltså förlust av integriteten antingen i användardata eller andra IT-resurser som tillhandahåller servrar, program och nät. Förlusten kan orsakas av avsiktlig eller oavsiktlig obehörig förändring av data, tillägg eller radering av meddelanden eller data i databaser, filer, kommunikationstrafik, o.s.v.

Riktighet innebär att användardata eller andra IT-resurser som tillhandahålls, t.ex. program och nät, ska ha den rätta kvaliteten, d.v.s. vara objektivt sett felfri, vara noggrann, ha rätt detaljeringsgrad, vara aktuell, vara tillförlitlig och vara konsistent.

2.2 Tillgänglighet

Tillgänglighet innebär att möjligheten finns för behöriga användare eller andra resurser att utnyttja definierade resurser efter behov, i förväntad utsträckning och inom önskad tid. Förlust av tillgänglighet uppträder när behöriga användare hindras från att utföra sina funktioner eller när de hindrar andra behöriga användare från att utföra funktioner. Driftavbrott och störningar av olika slag är det mest typiska exemplet på tillgänglighetsförlust.

2.3 Sekretess

Med sekretess menas att känslig information inte får avslöjas för obehöriga. Förlust av sekretess innefattar försök av antingen en behörig användare eller en obehörig användare att få åtkomst till information, vilken användaren varken har eller ska ha rättighet till. Förlust av sekretess omfattar också oavsiktlig tillgång till känslig information av användare eller ”icke-användare”, t.ex. genom en arbetsplats-monitor som är synlig för andra, utskrifter vid skrivare eller fel-routad elektronisk post.

Begreppet konfidentialitet används ofta i samband med sekretess. Konfidentialitet är ett sorts insynsskydd och syftar till att skydda hemlig eller känslig information från obehörig insyn.

Obehörig åtkomst gäller inte bara informationen utan även andra IT-resurser. Genom obehörig åtkomst kan IT-resurserna missbrukas, t.ex. kan avsiktlig eller oavsiktlig körning av ”obehöriga program” (t.ex. virus) påverka eller förstöra riktigheten i systemet.

2.4 Spårbarhet

Spårbarhet och oavvislighet erbjuder skydd och återställande från förluster och brott mot säkerheten. Med brist på spårbarhet menas att användarna inte hålls ansvariga för sina förehavanden i IT-området. Systemadministratörer och systemoperatörer kan inte hållas ansvariga för sina administrativa aktiviteter, användarna kan inte hållas ansvariga för sin användning av tjänster eller utförande av transaktioner.

Oavvislighet är en sorts spårbarhet. Oavvislighet innebär att en användare i efterhand inte kan förneka att han/hon har skickat eller mottagit ett meddelande. Användaren kan heller inte förneka att han/hon har deltagit i eller orsakat en handling.

Autenticeringen av användare möjliggör spårbarhet. Finns det möjligheter att logga in under falsk identitet får man brist på korrekt spårbarhet. Det kan också leda till obehörig åtkomst och information kan t.ex. obehörigt modifieras.

3 Hot och risker i olika driftmiljöer

Detta kapitel behandlar, från en verksamhetsmässig och teknisk utgångspunkt, de hot och risker som föreligger inom området. Aktuella begrepp införs och förklaras.

3.1 Vad är ett hot eller en risk

Ett hot kan i korthet sägas vara en möjlig, oönskad händelse som, om den inträffade, skulle få negativa följder. Hot ska skiljas från risk som vi kan definiera som sannolikheten för att hotet ska realiseras, d.v.s. att händelsen ska inträffa.

Det är viktigt att varje organisation har klart för sig vilka hot som kan finnas mot just den egna verksamheten, och vilka av dessa hot som riktar sig mot IT-verksamheten och övrig informationshantering. Det är i det sammanhanget väsentligt att ta hänsyn till att hoten varierar i tiden med den aktuella händelseutvecklingen. För offentliga organisationer har detta betydelse, inte minst med tanke på att de ska kunna fungera även i kris och krig.

3.2 Generella hot och risker

De vanligaste hoten mot IT-verksamheten är mycket vardagliga händelser, som förorsakas av bl.a. brister i administrativa rutiner och i själva IT-verksamheten. Dessa **interna** hot hör till den kategori som man brukar kalla **oavsiktliga** hot. Alla organisationer som utnyttjar informationsteknik drabbas i mer eller mindre stor utsträckning av oönskade händelser som kan hänföras till den här gruppen t.ex. havererade skivminnen och överföringsfel. Utöver de oavsiktliga hoten finns även de **interna avsiktliga** hoten.

Många organisationer är dessutom utsatta för **externa** hot, som mestadels är vad man betecknar som **avsiktliga** hot, d.v.s. att någon enskild eller en organisation t.ex. försöker komma över viss information eller rent av försöker sabotera hela IT-verksamheten.

Förutom att man måste ha klart för sig vilka interna och externa, avsiktliga respektive oavsiktliga hot som är relevanta i den egna verksamheten, måste man också bedöma hur stor sannolikheten är för att hoten ska utlösas. Erfarenhetsmässigt vet man att vissa av de oavsiktliga hoten är relativt vanliga i många IT-verksamheter.

Det är viktigt att inte underskatta risken för att oavsiktliga och avsiktliga hot kan drabba verksamheten.

Interna hot

De övergripande hot som måste uppmärksammas inom all IT-verksamhet är:

- bristande engagemang från ledningen vad avser frågor kring informationsteknik, vilket ofta innebär att det saknas en uttalad policy för hur teknikstöd ska användas inom organisationen
- avsaknad av en policy för informationssäkerhet och IT-säkerhetspolicy (Informationssäkerhet omfattar även sådan information som inte är IT-relaterad)
- oklara ansvarsförhållanden i organisationen
- bristfällig dokumentation av såväl maskinella som manuella rutiner
- bristande kompetens hos olika personalkategorier.

Exempel på oönskade händelser som kan drabba de flesta informationssystem med IT-stöd är:

- fysiska hot såsom brand, stöld, vattenskada m.m.
- felaktig hantering av utrustning och felaktigt genomförda och/eller dåligt testade förändringar i program som kan medföra att program och register förstörs
- felaktig användning i kombination med dåliga kontrollfunktioner som medför att kvaliteten på utdata blir otillfredsställande
- någon manipulerar indata till systemet eller lägger in otillåten programkod för att komma över pengar eller annan information
- kopior på program/register saknas eller går inte att använda på grund av bristfälliga rutiner för reservkopiering.

Den här typen av händelser kan inträffa i alla organisationer som utnyttjar informationsteknik. Ofta är det den egna personalen som, mestadels **oavsiktligt**, förorsakar att händelserna inträffar. Anledningen är många gånger bristande utbildning för en viss arbetsuppgift eller stress i samband med en viktig och tidskritisk bearbetning. Många **oavsiktliga och avsiktliga** hot kan undvikas om goda administrativa säkerhetsrutiner tillämpas tillsammans med väl valda skyddsåtgärder.

Externa hot

För många organisationer är externa hot också en realitet, t.ex. man bedömer det inte som osannolikt att någon utomstående kan ha fördel av att komma över viss information eller t.o.m sabotera verksamheten. De typer av händelser som utgör hot i det här läget är t.ex.:

- Datamedium med svårersättliga indata försvinner under en transport.
- En obevakad bärbar dator med känslig information stjäls.
- En utomstående tar sig in i ett datorrum och skadar utrustning.
- En ”hacker” tar sig in i ett stordatorsystem och kommer på det sättet över information som han sedan säljer till en konkurrent.
- En person som utger sig för att komma från det budföretag som ansvarar för vissa magnetbandstransporter har placerat en stark sprängladdning i den väska där magnetbanden skulle ha varit. Laddningen detonerar fem minuter efter det att budet lämnat väskan och datahall inkl. utrustning skadas allvarligt. En person får också allvarliga skador.
- Virus kan komma in i datorn och nätet via disketter, överförda filer som bifogats e-post eller tagits hem via Internet. Det har även hänt att virus av misstag funnits på programdisketter distribuerade av seriösa leverantörer.

Även om några av de exemplifierade händelserna är mindre vanliga är de trots allt en realitet att räkna med. Virus och andra typer av otillåten programkod i köpta programvaror har t.ex. drabbat många PC-användare, och antalet ”hackers” torde snarare öka än minska.

Avsiktliga och oavsiktliga hot

Den statistik som finns när det gäller datorrelaterad brottslighet är mycket osäker, men det finns trots allt en klar trend i de fall som är kända och som utretts av polisen. De vanligaste avsiktliga hoten är inte som många tror externa hot, utan sådana som finns inom den egna organisationen. Den vanligaste databrottslingen är en person utan brottsligt förflutet och ofta välutbildad. Personen i fråga har tillgång till de resurser och medel (PC eller motsvarande, kunskap om verksamhet och IT-system, behörighet m.m.) som behövs för att utföra ett datorbrott.

Det som kan utlösa ett avsiktligt internt hot är ofta missnöje med arbetsgivaren, men kan också vara frestelsen att enkelt komma över en större summa pengar utan större risk för upptäckt.

Vissa myndigheter och företag måste också beakta de avsiktliga externa hot som utgörs av intressen hos främmande makt eller konkurrenter att komma över värdefull och känslig information. Ofta är emellertid det enklaste sättet för de organisationer som vill komma över den här typen av information att engagera en missnöjd medarbetare inom den organisation där informationen finns.

Ett av de mest tydliga generella hoten är virus. När man talar om datavirus är det viktigt att skilja mellan dessa och andra obehagliga händelser som kan inträffa i ett IT-system. Många händelser som beskrivs som virusangrepp är i själva verket någon annan företeelse vilken i och för sig kan förorsaka lika stor eller större skada än ett angrepp av virus. Vi ska därför försöka reda ut begreppen.

Datavirus

Datavirus är en självständig del av ett program som ligger dolt i ett annat program. Virusprogrammets instruktioner utförs inte förrän det program där det ligger dolt aktiveras. De är alltså beroende av redan existerande program eller filer och döljer sig bakom dessa.

Namnet har den här företeelsen fått på grund av att ett virus-program – precis som ett biologiskt virus – smittar den miljö där det inplanterats, genom att det vid exekvering kopierar sig själv till andra program i omgivningen. Smittmekanismen fungerar tämligen

enkelt. Viruset består av ett antal instruktioner som inledningsvis söker igenom alla tillgängliga filer. Tillgängligheten styrs av den aktuella användarens behörighet, var viruset för tillfället befinner sig, användarens programbibliotek m.m. Viruset läser in alla filer och granskar dem för att se om dess eget speciella kännemärke återfinns. Om så är fallet har det varit där tidigare och smittat ner den aktuella filen. Om filen inte smittats så förses den med en kopia av viruset och märks innan den återigen skrivs in på plats. Så har ytterligare en fil blivit smittad. Smittspridningen kan ske olika snabbt beroende på i vilken typ av program och datormiljö viruset har lagts in och vilka egenskaper det för övrigt utrustats med.

Ett datavirus förmåga att sprida sig till andra delar av ett system är i sig en egenskap som är oönskad, men än värre är problemet att det också kan vara utformat så att det medför omfattande konsekvenser. Vilka skador ett datavirus kan förorsaka beror dels på vilka avsikter skaparen haft dels på hur snabbt man upptäcker angreppet. Många datavirus innehåller tämligen harmlösa instruktioner som att åstadkomma en rolig utskrift på datorns skärm, t.ex. när ett visst datum infaller på en viss veckodag, medan andra innehåller instruktioner som att förstöra alla datafiler. Dessvärre ökar den senare sorten mest.

En allvarlig egenskap hos datavirus är att det kan hålla sig gömt i en dator under lång tid utan att man upptäcker att det finns där. Det betyder att de säkerhetskopior som man tagit efter smittillfället också är smittade. I det läget kan man inte bara slänga den senaste versionen där problemet uppenbarade sig och gå tillbaka till en gammal version utan det krävs hjälp av speciell programvara som i bästa fall kan återställa det som förstörts.

Logisk bomb

En logisk bomb är ett antal instruktioner i ett program som bara utförs om vissa villkor som specificerats uppfylls, t.ex. när ett visst datum infaller eller att det är en speciell typ av satsvis bearbetning som ska utföras. Exempel på logiska bomber är att alla filer i datorn raderas ett visst datum eller att vissa utskriftsprogram inte går att starta i samband med bokslut. En logisk bomb har egentligen ingenting med virus att göra, mer än att ett datavirus ofta kan innehålla en sådan.

Trojansk häst

Den trojanska hästen är en dold odokumenterad del av ett helt vanligt program som utför sina avsedda funktioner. Den dolda delen kan innehålla en logisk bomb, ett virus eller någon annan sorts obehaglig programkod, och kan ibland till och med radera ut sig själv för att sopa igen spåren när det onda uppsåtet är genomfört. Allt för att göra det omöjligt att spåra källan till det som inträffat.

Maskar eller bakterier

Detta är självständiga program som kopierar sig själva och breder ut sig i en enskild dator eller i ett nät. Följden blir att tillgängligheten i datorn/datorerna minskar, eventuellt blir belastningen så stor att inga andra program kan köras. Effekterna kan liknas vid vad ett virusprogram kan åstadkomma men skillnaden är att en mask/bakterie inte är dold i ett annat program utan har en egen programidentitet och måste startas av en person.

Det finns egentligen inga entydiga definitioner av ovanstående, d.v.s de är inte helt ömsesidigt uteslutande. Ett virus kan innehålla en logisk bomb; en trojansk häst kan i själva verket visa sig vara en mask, etc.

3.3 Specifika hot och risker

I följande avsnitt kommer hot och risker som är speciella för olika miljöer att beskrivas. Flera av ovanstående generella hot och risker gäller för alla miljöerna.

3.3.1 Arbetsplats

En arbetsplats är t.ex. en PC eller UNIX arbetsstation som är fysiskt åtkomlig för användarna. Den används främst av en person i taget. Bärbara datorer är definitionsmässigt också en arbetsplats. En arbetsplats kan fungera som en isolerad enhet eller vara ansluten till olika datakommunikationsnät.

Logiska hot

- Obehörig åtkomst på grund av att funktioner för identifiering och autenticering saknas.
- Obehörig åtkomst på grund av att identifierings- och autenticeringsinformation har så stora brister att det är möjligt att gissa sig till den.
- Bristande kunskap hos användarna vad gäller handhavande av identifierings- och autenticeringsinformation kan medföra att autenticeringsfunktionen förlorar sin styrka. Exempelvis, kan obehöriga få åtkomst genom att han/hon läser nedskrivna lösenord vid arbetsplatserna.
- Obehörig åtkomst kan bygga på återanvändning av autenticeringsinformation från användare, t.ex. genom att användaren lurats till autenticering av en opålitlig autenticeringsprocess som spelar in informationen.
- Obehörig åtkomst kan ske genom att någon tar över en inloggningsperiod från en användare som lämnat arbetsplatsen obevakad.
- Genom att starta om arbetsplatsen från ett annat medium, t.ex. en diskett eller en ansluten hårddisk, kan det vara möjligt att kringgå autenticeringsfunktionen.
- Användare kan byta program eller dokument med andra datorer och på så sätt introducera virus.
- Arbetsplatsen är inte korrekt konfigurerad och fungerar därför inte riktigt.
- Inkonsekvenser och konflikter mellan applikationer kan förorsaka problem.
- Lokal data kanske inte säkerhetskopierats och kan således gå förlorad.
- Det kan finnas felaktiga versioner av applikationer, vilket kan leda till oriktiga och inkompatibla förändringar av data.
- Det är också möjligt att kringgå det logiska skyddet genom fysisk åtkomst av hårdvaran.
- Användare kanske behöver dela arbetsplatser och kan då få åtkomst av all information som lagrats lokalt.

Administrativa hot

- Om alla arbetsplatser är konfigurerade på olika sätt är det svårt för personer att dela information och arbeta tillsammans. Inkonsekvent konfigurering är också en källa till många tekniska problem, t.ex. förlust av tillgänglighet på grund av systemkonflikter.
- Det saknas rutiner för återställande av en havererad arbetsplats.
- Brist på kontroll av versioner av lokalt lagrade data kan leda till förlust av riktighet.

3.3.2 Lokala nät

Med lokala nät menas nät som är geografiskt samlade. De lokala näten skyddas och administreras i allmänhet av den egna organisationen. Det lokala nätet ansluter servrar, arbetsplatser, skrivare och annan utrustning. Syftet med det lokala nätet är att möjliggöra utbyte av information och att dela resurser som är anslutna till noder i nätet. Lokala nät innefattar även alla former av applikationsoberoende, grundläggande tjänster som krävs inom nätet.

Enligt vår definition består ett lokalt nät av:

- Den fysiska utrustningen, t.ex. fastighetskablage, hubbar, switchar, routrar och nätkort.
- Servrar
- Nätprogramvara (Novell Netware, NT Server, Unix), som bildar det logiska nätet (innehåller kommunikationsprotokoll för data som överförs, samt den logiska strukturen som behövs för att erbjuda den anslutna utrustningen nättjänster).
- Nätapplikationer
- Annan kringutrustning, t.ex. arbetsplatsutrustning, skrivare, scanner och telefoniutrustning.

Med server menas en dator som inte är en enmansmaskin, utan som delas av flera, t.ex. stordatorer, UNIX filservrar, mailservrar. En server kan vara en maskin där användare loggar in eller en maskin som är en server i ett nät. Åtkomst av servrar sker via terminaler, arbetsplatser, oftast via särskilda applikationer.

Med nätapplikationer menas i detta fall distribuerade applikationer eller klient/server applikationer, d.v.s. sådana som utbyter meddelanden via ett nät. Nätapplikationer behövs för att dela resurser i ett lokalt nät.

Nätapplikationer består i allmänhet av två delar: en klient och en server. De körs var för sig som självständiga program, vanligtvis på olika datorer, men anslutna via ett nät. En klient kan t.ex. köras på en PC, medan servern kanske körs på en servermaskin, t.ex. en NT-maskin eller stordator.

Oönskade händelser i lokala nät kan t.ex. vara:

Logiska hot

- Eftersom en server ofta delas av många användare och aktiviteter, finns det risk för att en användare eller ett projekt belastar systemet i så stor utsträckning att övriga inte får den rätta tillgängligheten.
- Slutledning av information innebär att man ur öppen information kan härleda känslig (d.v.s. hemlig) information, t.ex. genom statistiska metoder. Ett exempel på denna typ av hot är när man genom att kombinera resultat från behörighetsmässigt riktiga databasfrågor kan härleda information som man inte har behörighet till.
- Kommunikationskanaler kan avlyssnas eller bevakas av obehöriga för att få tillgång till information, t.ex. autenticeringsinformation och trafikinformation.
- Inspelning av trafik kan inträffa t.ex. när en autenticeringssekvens snappas upp och spelas upp igen för att simulera en giltig autenticering. Detta hot innebär också att den obehöriga inte behöver tolka eller förstå autenticeringsinformationen.
- Användaridentiteter kan vara svåra att spåra om servrar och nätapplikationer använder olika identiteter på samma användare eller om privilegier delegerats.
- Data som kommuniceras kan manipuleras, t.ex. transaktioner fångas upp och förändras och sedan skickas vidare.
- Adresseringen i ett lokalt nät kan misslyckas eller förvanskas, vilken kan leda till att informationen sänds till en obehörig användare.

Administrativa hot

- Vid avsaknad av LAN-strategi kan kostnaderna för underhåll bli mycket stora och dessutom utgöra ett hinder för framtida utveckling.
- Dåligt testade system som tas i drift kan leda till låsningar eller överbelastning i nätet.
- Felsökning försvåras p.g.a. att dokumentation angående server, applikation eller annan utrustning saknas.
- Nyckelpersoner slutar och tar med sig oumbärliga kunskaper om den lokala nätmiljön.
- Felaktig konfigurering av nätkomponenter, både hårdvaru- eller programkomponenter.
- Oklara ansvarsförhållanden vid hopkoppling av lokala nät.
- Riktlinjer saknas för hur tilldelningen av nätadresser ska gå till.

3.3.3 Fjärrnät

Med fjärrnät menas nät som binder samman lokala nät och/eller geografiskt skilda datorer. Fjärrnät underhålls normalt sett inte av organisationen. Inte heller skyddar organisationen förbindelserna fysiskt.

Fjärranslutningar kan dels bestå av uppringda förbindelser, d.v.s. alla icke fasta förbindelser som kan upprättas på begäran antingen automatiskt eller interaktivt, dels fasta fjärranslutningar.

I dess enklaste form utgörs fjärranslutningen av hyrda ”kopparledningar” där egna modem används och kommunikationsnätet byggs upp av egna kommunikationsenheter. Mer avancerade fjärrförbindelser erbjuds i form nättjänster från en operatör, där all kommunikationsutrustning ingår. Kunden beställer det nätprotokoll som ska användas och den överföringshastighet som önskas. Vill man ändra t.ex. hastighet kan detta ordnas relativt enkelt av leverantören.

Fjärranslutning kan tjäna två helt olika syften, att erbjuda en extern förbindelse till en annan organisations nät eller att binda samman

en organisation till ett logiskt slutet nät, men där användarna är geografiskt åtskilda.

Hot och risker i fjärrförbindelser är delvis av samma karaktär som för lokala nät:

Logiska hot

- Användare eller systemoperatörer kan ansluta modem för fjärrförbindelser till sina arbetsplatser utan behörighet eller annan säkerhetsåtgärd. Detta kan exponera IT-miljön i en organisation för en mängd hot.
- En behörig användare kan slå fel nummer, bli felroutad eller luras att upprätta en falsk förbindelse. Detta kan lura användaren att avslöja autenticeringsinformation, sända känslig information eller ta emot manipulerad information.
- Data som sänds kan manipuleras under överföringen utan att applikation märker något, t.ex. kan en transaktion fångas upp och förändras innan den skickas vidare, eller att samma transaktion upprepas.
- Risken för avbrott i fysiska ledningar eller nättjänster som tillhandahålls av operatörer kan orsaka tillgänglighetsförluster samt eventuellt även förlust av information.
- Prestandaproblem i överföringen beroende på dålig kontroll på egen trafik eller överbelastning i operatörers nät.
- Eftersom information överförs via publika och geografiskt spridda kommunikationsmedia kan alla organisationer som utgör kommunikationstjänsten avlyssna all information som överförs.
- All trafik i ett publikt nät kan potentiellt utsättas för informationsläckage. Routingen av trafiken kan vara svår att kontrollera i publika nät. Alla användare av fjärrförbindelsen eller nätet kan därför potentiellt ha åtkomst till informationen.

Administrativa hot

- Obehörig installering av uppringda förbindelser, t.ex. en användare ansluter ett modem till sin arbetsplats för att kunna läsa elektronisk post hemifrån.

- Fjärrförbindelser kan installeras och konfigureras så att de är osäkra och inte uppfyller den användning de är avsedda för, t.ex. att de tillåter inkommande samtal, när de endast var avsedda för utgående samtal, t.ex. att de tillåter inkommande åtkomst eller flera protokoll, när de endast var avsedda för utgående åtkomst och vissa specifika protokoll, t.ex. elektronisk post eller EDI.
- Intrång eller säkerhetsincidenter hanteras inte ordentligt, t.ex. att man saknar möjligheter att spåra incidenter, återställa systemet vid intrång eller kunna förebygga liknande incidenter.
- Fjärrförbindelser kan användas inte enbart från hemmet, utan också från helt oskyddade miljöer, t.ex. hotell i olika delar av världen, andra företags telefonväxlar eller allmänna telefoner.
- Om en fjärrförbindelse upprättats mellan två lokala nät med olika riktlinjer för behörighetskontroll är det möjligt att oavsiktligt möjliggöra obehörig åtkomst av resurser via fjärrförbindelsen.
- Riktlinjer saknas för hur förbindelser till publika nät ska införas och dokumenteras. En förbindelse kan vara väl skyddad, t.ex. genom att endast tillåta inkommande åtkomst, medan en annan förbindelse kan tillåta åtkomst i båda riktningarna.

3.3.4 Distansarbete

Med distansarbete menas att anställda använder datorer och telekommunikation för att arbeta på annan plats än kontoret under en del av eller hela arbetsdagen.

Normalt sker allt datorarbete i den egna arbetsplatsen eller via teleförbindelser i någon form av klient/server-tillämpning mot ett centralt system.

Distansarbete förutsätter att det finns en accesserver som distansarbetaren kopplar upp sig mot under arbetet. Det förutsätts här att uppringda förbindelser används. Vid fasta förbindelser gäller det som står under fjärrförbindelser.

Risker som föreligger är:

- Obehörig åtkomst till nätet via accesservern. Är man väl inne i nätet gäller samma risker som vid Internetanslutning.

Orsaker som ökar riskerna kan vara att:

  – telefonnummer till modempoolen sprids
  – användaridentiteter och lösenord är för enkla och möjliga att gissa
  – okrypterade lösenord sänds över telelinjer och kan avlyssnas.

- avlyssning av känslig information via teleförbindelser
- dataförluster p.g.a. slarv med reservkopieringen på hemarbetsplatsen
- virus eller annan skadegörelse p.g.a. av att arbetsplatsen används till annat än arbete i hemmet.

3.3.5 Vid anslutning till Internet

Med anslutning till Internet menar vi en anslutning till det globalt täckande fjärrnät som kallas Internet. Via Internet kopplas lokala nät och geografiskt skilda datorer samman. Internet underhålls normalt sett inte av organisationen. Förbindelserna skyddas heller inte fysiskt av organisationen.

Internet-anslutningar kan dels bestå av uppringd förbindelse som är ett vanligt förfarande för enskilda arbetsplatser, och dels fast anslutning där en router förbinder ett lokalt nät med Internet. Fast anslutning används ofta när flera arbetsplatser ska ha tillgång till Internet. De hot och risker som är aktuella vid anslutning till Internet gäller i första hand när den egna utrustningen är uppkopplad med **fast förbindelse** till en router eller motsvarande på Internet. I övrigt kan många av de hot som nämns i avsnittet om fjärrnät ovan också tillämpas på Internet-anslutningar.

Utrustning som är utsatt för risker är den egna routern, brandväggen eller servern samt om kommunikationsprotokollet TCP/IP används i det egna nätet och all utrustning i nätet som kan nås via TCP/IP.

Exempel på hot och risker:

- Obehörigt intrång kan leda till att utomstående kan:

  - ändra textinnehåll på websidor
  - skaffa användaridentitet och lösenord
  - förstöra filer och program
  - plantera in virus
  - komma över känslig information.
- En dåligt installerad eller konfigurerad brandvägg kan utnyttjas på många olika sätt. Dessutom utgör den eventuella falska tryggheten en risk.
- Bristande rutiner eller avsaknad av policy för användningen av Internet kan förorsaka problem.

Det är viktigt att tänka på att effekterna av ett obehörigt intrång till stor del beror på hur bra den totala IT-säkerheten fungerar i organisationen. Det är alltså inte säkert att en aldrig så bra brandvägg hjälper om det finns andra vägar att ta sig in i nätet, där t.ex. administrationen av behörighetskontrollsystemet sköts bristfälligt eller att användarna har egna modemanslutningar.

3.3.6 Vid informationsspridning via Internet

Här avses informationsspridning med s.k. WWW-teknik, d.v.s. information eller tjänster erbjuds via en webserver till alla intressenter som har tillgång till Internet. Informationen som sprids kan vara av olika karaktär och detta medför att ägaren kan ställa olika krav på säkerhet och tillgänglighet.

Hot och risker som kan vara aktuella är:

- förändring av information i webserver
  - sådant som syns tydligt
  - detaljer i viktig information som kan vara svåra att upptäcka.
- blockering av tillgängligheten till olika tjänster
- sabotage av hela webservern.

I övrigt se avsnitten Fjärrnät och Vid anslutning till Internet.

3.3.7 Meddelandehantering

Meddelandehantering innebär att information utbyts mellan personer eller system på ett fördefinierat sätt. Med meddelande avses här alltså inte bara själva informationsinnehållet utan även formatet/strukturen för hur meddelandet paketeras på applikationsnivå. Exempelvis ett e-postmeddelande består av en kropp och ett huvud som vart och ett har ett speciellt format.

Allt som sänds via Internet eller något annat fjärrnät kan fångas upp och avläsas. Sekretessen kan jämföras med den som gäller när man skickar vykort. De hot och risker som är relevanta under denna punkt innefattas under obehörig användning och är delvis samma som för lokala nät samt fjärrförbindelser. Exempel på hot och risker är:

- Vid avlyssning av trafik kan känslig eller hemlig information snappas upp, t.ex. kreditkortsnummer.
- Data som sänds kan manipuleras, t.ex. kan ett meddelande fångas upp och förändras och sedan skickas vidare.
- Meddelanden med falsk avsändare sprids av obehöriga.
- Volymen av meddelande till vissa användare kan bli förödande stor p.g.a. av otaliga sändlistor med reklaminformation eller att någon obehörig vill minska tillgängligheten för en användare eller organisationen.
- Informationen i meddelandehuvudet på elektronisk post kan avslöja känslig information, t.ex. ämnesraden, avsändarens eller mottagarens adress eller transportväg även om det faktiska meddelandet är krypterat.
- En analys av meddelandetrafik kan t.ex. avslöja vilka en organisation eller person kommunicerar med, hur ofta och storleken på meddelandena.

3.3.8 Systemutveckling och -förvaltning

Begreppet systemutveckling definieras som de aktiviteter som avser analys, konstruktion och införande av ett system för IT-stödd informationsbehandling. Systemförvaltning kan beskrivas som de aktiviteter som avser att följa upp användningen av ett existerande

system och att genomföra de förändringar, rättelser och kompletteringar som behövs.

En förutsättning för att man ska kunna utveckla IT-system som uppfyller rimliga krav på säkerhet är att utvecklingsarbetet bedrivs på ett likartat och metodiskt sätt inom organisationen.

Hot och risker som kan vara aktuella är:

- Avsaknad av modeller och metoder för systemutvecklings- och förvaltningsarbetet kan medföra att brister och sårbarheter introduceras i systemen.
- Den rätta kompetensen saknas vilket leder till att man förbiser väsentlig säkerhetsproblematik.
- Bristfälliga rutiner vad gäller framställning av relevant dokumentation kan leda till att säkerhetshål inte kan åtgärdas effektivt och sårbarheten kan utnyttjas.
- Dåliga och för korta testfaser kan leda till att systemet inte visar sig uppfylla kraven på säkerhet.
- Avsaknad eller bristfälliga indata- och rimlighetskontroller i system kan leda till att nivån på säkerheten i realiteten är lägre än vid de manuella rutinerna.
- Användarna har inte utbildats i tillräcklig omfattning och systemet används därför på fel sätt.
- Systemet är inte användarvänligt.

4 Skyddsåtgärder

I detta kapitel behandlas sådana skyddsåtgärder som finns att tillgå för att skydda sig mot de hot och risker som behandlats tidigare. Såväl administrativa som tekniska skyddsåtgärder behandlas i kapitlet. Tanken men kapitlet är att ge en repertoar av tänkbara åtgärder för den fortsatta behandlingen av skyddsåtgärder inom olika specifika områden. Det är därför viktigt att läsaren försöker se till skyddsåtgärdens grundläggande egenskaper och karaktär mer än till dess tillämpning i detta kapitel. Här gäller det t.ex. att förstå vad kryptering innebär rent tekniskt och operativt och vad det allmänt sett kan ge för skydd.

4.1 Allmänt

Många av de skydd som man installerar kan inte förhindra att en viss händelse inträffar men de kan minska skadeverkningarna. Man brukar skilja mellan skydd som är:

förebyggande, d.v.s. skyddet förhindrar att en viss händelse inträffar

begränsande, d.v.s. skadeverkningarna begränsas om händelsen inträffar

rapporterande, d.v.s. skyddet innebär att händelsen inte förblir oupptäckt.

För att de tekniska skyddsåtgärderna ska få effekt krävs i de flesta fall att det också finns motsvarande administrativa skyddsåtgärder i form av dokumenterade regler för utveckling, förvaltning och drift av IT-systemen.

Vi behandlar i tur och ordning följande skyddsåtgärder:

Administrativa skyddsåtgärder

Kryptering

Behörighetskontrollsystem

Aktiva kort

Brandväggar

Säkerhetskopiering

Virusskydd

4.2 Administrativa skyddsåtgärder

Administrativa skyddsåtgärder kan skydda mot en mängd hot och svagheter, t.ex. konstruktionsfel i programvaran, svårigheter med att välja färdiga program, brister i installations- och driftrutiner.

De administrativa skyddsåtgärderna består i huvudsak av olika regelverk för den egentliga verksamheten och för IT-verksamheten. De administrativa skydden är mestadels en förutsättning för att andra typer av skydd ska få önskad effekt.

På en övergripande nivå bör alla organisationer som utnyttjar IT-stöd i sin informationshantering definiera:

- riktlinjer för IT-säkerhetsarbetet och en IT-säkerhetspolicy
- dokumentation som klart anger fördelningen av ansvaret för IT-säkerheten mellan verksamhetsansvariga och den som utsetts att leda/samordna IT-säkerhetsarbetet
- en handlingsplan för IT-säkerhetsarbetet, både på kort och lång sikt
- ett utbildningsprogram för all personal som är användare av IT-system, för att de ska få den kunskap som krävs för att arbeta med systemet på rätt sätt
- ett utbildningsprogram för IT-personalen, för att de ska få den kunskap som krävs för att kunna sköta den tekniska förvaltningen och driften av systemet.

De administrativa skyddsåtgärderna består således i stor utsträckning av dokumentation, som beskriver de regler och rutiner som ska gälla för olika delar av den verksamhet som berörs av IT-stödet, både i utvecklingsskedet och under systemets drift- och förvaltningsfas.

Omfattningen av regelverket varierar givetvis, beroende på bl.a. IT-verksamhetens omfattning och de datormiljöer man har, men den här typen av regler ska finnas även för t.ex. persondatormiljöer.

För organisationer, där olika störningar i IT-verksamheten medför **allvarliga** eller **mycket allvarliga** konsekvenser för verksamheten, är det speciellt viktigt att de generella administrativa skyddsåtgärderna finns och att reglerna efterlevs.

4.2.1 Systemadministration

Många störningar i IT-system beror på brister i utformningen av enskilda tillämpningssystem och dåliga rutiner för samverkan mellan olika system. En del av dessa brister beror på att systemen är utformade på ett sådant sätt, att olika typer av fel inte upptäcks i tid eller att driften av systemet kräver komplicerade ingrepp av den driftansvarige. Bristande utbildning av driftpersonal och stressade situationer kan medföra att allvarliga fel kan inträffa.

Kontinuerlig uppföljning av driften och de avvikelser och fel som uppträder i anslutning till den är en av de viktigaste skyddsåtgärderna i driftmiljön. Uppföljningen ska dels ge underlag för att bedöma om systemet, sett ur användarens synvinkel, uppfyller kraven på god tillgänglighet och kvalitet, dels bidra till att ge en så god miljö som möjligt för den personal som ansvarar för drift av systemet. Uppföljningen ska bl.a. ge besked om hur de maskinella resurserna utnyttjas för att man i tid ska se om datorn börjar bli överbelastad i något avseende, ge besked om vilken typ av driftstörningar som inträffar, deras frekvens och hur långa driftavbrott olika störningar medför.

Grundläggande är att man har en säker teknisk miljö och väl dokumenterade rutiner för hur driften ska bedrivas samt fungerande reservrutiner. Praktiska administrativa skyddsåtgärder skulle t.ex. kunna vara:

- Dokumenterade rutiner för hur olika användartyper rapporterar och följer upp säkerhetsincidenter eller brott mot säkerheten.
- Dokumenterade och fungerande rutiner för reservkopiering t.ex. en förändringskopia kan tas dagligen och en fullständig

säkerhetskopia varje vecka. Fullgoda förvaringsutrymmen för lagringsmedier bör också finnas.

- Rutinerna för säkerhetskopiering bör kunna verifieras. Säkerhetskopiorna bör kunna verifieras, d.v.s. att det är möjligt att använda dem.
- Dokumenterade rutiner för hur, när och i vilken omfattning olika loggar ska produceras och granskas.
- Rutinerna för hantering av loggfiler ska vara dokumenterade, t.ex. vilka loggar som lagrats hur länge och hur de säkerhetskopieras.

4.2.2 Systemutveckling och förvaltning

Konstruktionsfel i både hårdvara och program och kan leda till oönskade effekter. Dåliga utvecklingsmetoder eller medveten introduktion av fel kan medföra att oavsiktliga konstruktionsfel introduceras eller att avsiktliga inte upptäcks. Praktiska administrativa skyddsåtgärder för att undvika konstruktionsfel är t.ex:

- System- och programvaruutveckling ska ske enligt för organisationen fastställda modeller, metoder och hjälpmedel.
- Testverksamhet ska ske enligt fastställda regler och bör, liksom programutveckling, inte förekomma i produktionsmiljö.
- System- och applikationskomponenter som är relevanta för säkerheten ska identifieras och deras funktionalitet ska vara väldokumenterad. Vidare ska det verifieras genom tester att dessa fungerar korrekt innan de används.
- Säkerhetsrevision eller andra former av stark kontroll av motåtgärdernas korrekta funktion och effektivitet ska genomföras.

4.2.3 Installation och konfiguration

Rutinerna för inläggning av nya system- och programversioner (gäller såväl tillämpningssystem som systemprogramvaror) måste vara utformade så att risken för att fel ska uppstå blir så liten som

möjligt. Det måste finnas tydliga dokumenterade regler för hur man t.ex. ska kunna kontrollera att de nya versionerna verkligen fungerar på avsett vis.

Viktigt är också att det finns regler för när nya versioner av tillämpningsprogram får läggas in. Eftersom det alltid finns en viss risk för att störningar kan inträffa i sådana situationer bör antalet tillfällen, då programändringar får läggas in, fastställas till högst en eller två gånger per månad. Endast vid akuta felsituationer bör man frångå de fastställda reglerna.

Rutiner för inköp och installation av program är särskilt viktiga i fleranvändarmiljö. I lokala nät bör ingen annan än den som är nätansvarig ha rätt att installera nya program. Risken för att t.ex. datavirus överförs till andra resurser är överhängande, om ett persondatornät har blivit ”smittat” via en diskett eller en nerladdad programmodul från t.ex. Internet.

Exempel på administrativa skyddsåtgärder kan vara:

- Det ska finnas ett aktuellt register som beskriver datorsystemets maskinvaru- och programkonfigurering. Följande information bör finnas med: version, leverantör, kontaktperson, samt alla modifieringar.
- Det ska finnas en aktuell beskrivning av det interna kommunikationsnätets konfigurering. Externa kommunikationstjänster och syftet med dessa förbindelser ska vara dokumenterat. Följande information bör finnas: version, leverantör, kontaktperson, samt alla modifieringar.
- Det ska finnas dokumenterade rutiner för installation av program i datorsystemet.
- Systemen bör versionshanteras så att man kan identifiera alla förändringar i systemet och eventuellt kunna backa till tidigare systemversioner.
- Dokumenterade rutiner för att kunna verifiera att systemet installerats och konfigurerats korrekt, samt att verifiera att systemet kan tillhandahålla den säkerhet som behövs.

4.2.4 Specifika säkerhetsrutiner

För att de skyddsåtgärder som är specifika för säkerheten ska få önskad effekt krävs det oftast att det finns motsvarande administrativa skyddsåtgärder i form av dokumenterade regler för t.ex. hantering av krypteringsnycklar eller behörigheter. Exempelvis ger installationen av ett avancerat krypteringsskydd inget egentligt skydd om rutinerna för tilldelning och hantering av krypteringsnycklar, administration av systemet och uppföljning av systemanvändningen inte fungerar.

Specifika säkerhetsrutiner som bör definieras är t.ex:

- Tillgängliga säkerhetsåtgärder och deras implementering i datorsystemet ska vara dokumenterade. Alla applikationsspecifika säkerhetsåtgärder ska inkluderas. Dokumentation som beskriver datorsystemets konfigurering, plats och säkerhetsegenskaper, samt dess relevanta kommunikationsnät ska hanteras som hemlig information.
- Administration som rör säkerhetsparametrar eller liknande får endast utföras om det föreskrivna skyddet är i drift. Skyddsåtgärder och säkerhetsrutiner ska dokumenteras och godkännas av företagets säkerhetsorganisation.
- Säkerhetsrevision ska utföras årligen för att granska att säkerheten följs. Stickprov kan utföras periodvis.
- Det ska finnas dokumenterade rutiner för hur information om åtkomst ska följas upp av en identifierad ansvarig.
- Alla ändringar i riktighetskänslig information bör registreras i t.ex. loggar.
- Rutiner för hantering av krypteringsnycklar ska vara fastställda, exempelvis enligt följande:
  - Hemliga (symmetriska) nycklar bör bytas ut med jämna mellanrum och bör endast användas i ett sammanhang.
  - Krypteringsnycklar för dekryptering av känslig information ska skyddas minst lika noggrant som den okrypterade informationen.
  - Privata nycklar ska aldrig delas.

- Dokumenterade regler och rutiner för hur kryptografiska kontrollsummor och tillhörande krypteringsnycklar ska hanteras och användas bör finnas.
- Kryptografiska algoritmer ska godkännas av IT-säkerhetschefen. Algoritmer ska väljas med omsorg och vara erkänt motståndskraftiga. Krypteringsnycklar ska vara tillräckligt långa och vara av god kvalitet, t.ex. får det inte finnas kända svagheter i applikationen som genererar nycklar.

4.2.5 Behörighetsadministration

För att göra behörighetskontroll effektiv är samspelet mellan de tekniska och de administrativa åtgärderna utomordentligt viktigt. Administrativa åtgärder är bl.a. beslut om hur olika behörigheter ska fastställas, fördelningen av ansvar inom behörighetsadministrationen samt utformningen av regler för uppföljning och kontroll.

Det är informationsägaren som ska besluta om vem som ska ha tillgång till vad, och vad var och en ska ha befogenhet att göra i systemet. Ansvaret för att systemanvändningen följs upp är också informationsägarens, även om själva arbetet utförs av någon annan.

Den som beslutar om tilldelning av behörigheter ska själv inte ha behörighet att utföra uppdateringar av sin egen behörighet i behörighetskontrollsystemet, eftersom risken finns att någon då tilldelar sig själv en behörighet som denne inte bör ha.

Hur man bygger upp sin organisation för behörighetskontroll är naturligtvis beroende av hur organisationen i övrigt är utformad, vilken särskild säkerhetsorganisation som finns och hur IT-verksamheten ser ut. Oavsett hur kontrollsystemet och organisationen kring det byggs upp måste emellertid den bestämda grundvalen för arbetet vara att kontrollfunktionerna aldrig får göras mer vidsträckta eller utformas annorlunda än vad som klart motiveras av behovet av att skydda de olika resurserna i systemet. Man ska dock uppmärksamma att detta skyddsbehov också gäller användarna själva. Ett av motiven för att ha behörighetskontroll är att, om något oönskat inträffar, så ska den information som finns i loggen kunna utesluta ett antal personer från misstanke om att ha utfört det som förorsakat störningen. Nedan följer exempel på riktlinjer:

- Ansvarig ska enkelt kunna lägga till nya användare och ta bort gamla användare och ändringen ska omedelbart träda i kraft.
- Dokumenterade rutiner för hur användare tilldelas:
  - en användaridentitet i systemet
  - nya eller förändrade behörigheter.
- Åtkomsträttigheter till känsliga eller hemliga resurser i ett informationssystem bör endast kunna tilldelas genom ett godkännande av informationsägaren alternativt systemägaren.
- All åtkomst av information som lagrats på datamedia ska registreras. Information om åtkomst ska följas upp av identifierad ansvarig.
- Det ska finnas en rutin i drift som säkerställer att användaridentiteter av personer som inte längre arbetar i företaget raderas från datorsystemet. Detta krav gäller även tillfälliga användare, t.ex. konsulter och liknande.
- Dokumenterade rutiner för hur systemägaren och eventuella andra relevanta personer ska informeras om vilka användare som har åtkomst till information. Detta gäller alla typer av användare.
- Dokumenterade rutiner för hur användarnas behörigheter kontinuerligt ska granskas och utvärderas. Rutinerna ska även inkludera former för att få spårbarhet i dessa granskningar, d.v.s. någon form av formell bekräftelse från t.ex. systemägaren att behörigheterna verkligen gällde vid tillfället för granskning.
- Dokumenterade rutiner och kontrollfunktioner ska finnas för hur uppdatering av behörigheterna sker, t.ex. bör inga uppdateringar kunna göras eller känsliga resurser kunna nås om det logiska skyddet inte är i drift.

4.2.6 Återanvändning av lagringsmedia

Återanvändning eller förstörelse av lagringsmedia medför vissa säkerhetsrisker. Det är viktigt att man är medveten om de riktlinjer och rutiner som finns för hur man ska hantera lagringsmedia som ska återanvändas eller förstöras.

- Dokumenterade rutiner ska finnas för hur information på återanvändbara lagringsmedia, t.ex. band och disketter, ska raderas. Riktlinjer ska även finnas för hur dessa senare får återanvändas.
- Dokumenterade rutiner ska finnas för hur lagringsmedia som innehåller känslig eller hemlig information ska förstöras.

4.3 Kryptering

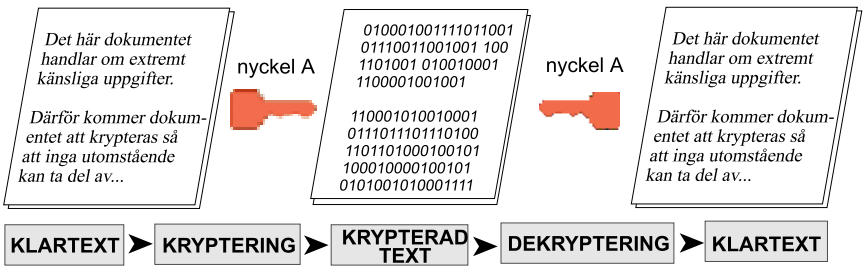
Kryptering är en effektiv åtgärd för att i samband med datakommunikation eller lagring skydda informationen mot insyn, avlyssning och förändring. Den enklaste formen av kryptering använder en hemlig algoritm för att kryptera respektive dekryptera en datamängd. Styrkan i denna metod bygger främst på att algoritmen hålls hemlig. Vill man uppnå en högre nivå av säkerhet anses s.k. öppna algoritmer vara lösningen. Med öppen algoritm menar man att algoritmen är känd, varvid säkerheten bygger på att en krypteringsnyckel hålls hemlig. Nyckeln byts sedan ut med jämna mellanrum. Det är enklare/effektivare att byta ut nycklar än att hitta på nya krypteringsalgoritmer. I fortsättningen behandlas endast öppna algoritmer.

Kryptering innebär att information kodas innan den sänds eller lagras, och att informationen endast kan göras läsbar av mottagaren under förutsättning att denne innehar rätt krypteringsnyckel. Kryptering av all information över ett nät försvårar både passiv och aktiv avlyssning. Detta kräver dock att krypteringsutrustning eller metod finns installerad på det IT-system som sänder informationen, och att motsvarande utrustning eller metod finns på det mottagande systemet.

För att kunna dekryptera en text måste både algoritmen och nyckeln vara känd. I många fall används en allmänt känd algoritm, t.ex. DES eller RSA. Vilken nivå av säkerhet man kan uppnå med olika algoritmer beror främst på vilken nyckellängd som kan användas. Ju längre nyckel desto bättre säkerhet. För vissa algoritmer finns det dessutom flera sätt att tillämpa algoritmen och vissa sätt är säkrare än andra. Algoritmens effektivitet/snabbhet minskar dock i de flesta fallen då nyckellängden ökar. Vissa tillämpningssätt minskar också algoritmens effektivitet.

4.3.1 Symmetrisk kryptering

I en symmetrisk krypteringsalgoritm används samma nyckel för kryptering och dekryptering. Detta innebär att nyckeln måste hållas hemlig. Vid överföring av krypterad information måste alltså sändare och mottagare antingen i förväg eller i själva transaktionen ha utväxlat en eller flera hemliga nycklar på ett säkert sätt.



Figur 9. Symmetrisk kryptering.

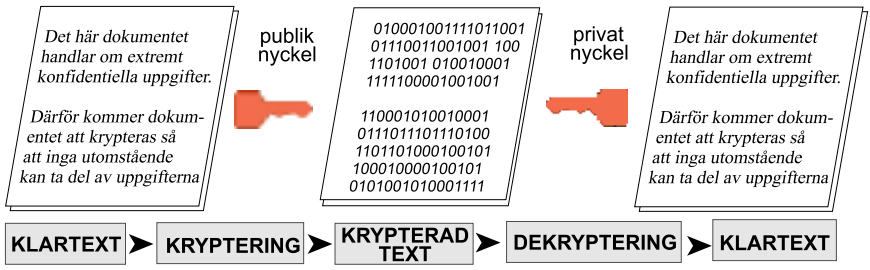
DES – Data Encryption Standard kom 1976 och är idag den mest spridda algoritmen för symmetrisk kryptering. DES är en block-orienterad algoritm, d.v.s. den krypterar data i 64-bits block. 64-bits okrypterad data blir 64-bits krypterad data. Samma algoritm används för kryptering och dekryptering. DES har flera tillämpningsätt. Triple-DES hör till en av dem, och anses vara en av de starkaste. I triple-DES krypteras texten tre gånger (krypteras-dekrypteras-krypteras) med två eller tre olika nycklar. Dekrypteringen görs i motsatt följd.

RC4 är en algoritm med variabel nyckellängd utformad av Ron Rivest för RSA Data Security Inc. (RC = Ron's Code). RC4 bygger på s.k. strömkryptering, d.v.s. informationsmängden behöver inte delas upp i block. RC4 motsvarar DES i styrka men är betydligt snabbare.

IDEA, International Data Encryption Algorithm är blockorienterad liksom DES. IDEA är en snabb algoritm, ungefär motsvarande DES.

4.3.2 Asymmetrisk kryptering

De asymmetriska algoritmerna bygger på olika nycklar för kryptering och dekryptering, där den ena nyckeln inte kan härledas ur den andra, d.v.s. dekrypteringnyckeln kan inte beräknas baserat på det krypterade dokumentet och krypteringsnyckeln. Detta nyckelpar benämns ofta öppen/hemlig eller publik/privat nyckel, d.v.s. en nyckel är allmänt känd – publik, medan den andra nyckeln är hemlig – privat.



Figur 10. Asymmetrisk kryptering.

Asymmetrisk kryptering kan bl.a. lösa tre viktiga uppgifter i ett säkerhetssystem:

- Säkert utbyte av nycklar över en ”öppen” förbindelse.
- Möjlighet för mottagaren/läsaren att verifiera avsändaren av ett meddelande.
- Möjlighet för mottagaren/läsaren att verifiera att ett meddelande inte ändrats.

Konceptet som använder publik nyckel introducerades av Whitfield Diffie och Martin Hellman 1976 samt, oberoende av dessa, av Ralph Merkle. Sedan dess har ett antal algoritmer med publik nyckel introducerats, men endast ett fåtal uppfyller kraven att vara både säkra och praktiskt användbara.

De främsta drivkrafterna bakom utvecklandet av asymmetriska algoritmer är svårigheten med att överföra nycklar i symmetriska system samt behoven av autenticeringsmetoder.

Den mest kända och använda asymmetriska algoritmen är *RSA,* uppkallad efter dess uppfinnare Ron Rivest, Adi Shamir och Leonard Adleman. Algoritmen introducerades 1978 och var den första fullvärdiga asymmetriska algoritmen som fungerar såväl för kryptering och nyckelutbyte som för digitala signaturer. RSA bygger på svårigheten att faktorisera stora tal, den privata respektive publika nyckeln är funktioner av ett par stora (100 – 200 siffror) primtal. Det är idag möjligt att faktorisera ett 110 siffrors tal så därför bör man i asymmetriska system välja en nyckel med mellan 154 siffror (512 bits) och 308 siffror (1024 bits).

4.3.3 Kryptografiska kontrollsummor

Beräkning av kontrollsummor är en teknik för att kontrollera att det inte förekommit någon manipulation av överförd eller lagrad informationsmängd. Den utgör ett bra skydd när någon exempelvis vill försäkra sig om att ekonomiska transaktioner inte utsätts för brott.

Beräkning av kontrollsumma är en metod för att beräkna ett unikt värde av en viss informationsmängd. Denna kontrollsumma kan ses som informationsmängdens ”fingeravtryck”, som sedan används i bl.a. den digitala signaturen.

Kraven på en algoritm för beräkning av kontrollsummor är:

- Det ska inte gå att förändra en text eller skapa en annan text som ger samma kryptografiska kontrollsumma.
- Det ska inte gå att härleda texten utifrån kontrollsumman.
- Algoritmen ska vara känslig så att ”små” obehöriga förändringar i ursprungsinformationen ska synas i den kryptografiska kontrollsumman.
- Beräkningsalgoritmen ska vara snabb.

Det första kravet är avgörande för användbarheten av en kontrollsumma. Det ska alltså inte vara möjligt att skapa två dokument med olika text som ger samma kontrollsumma, t.ex. genom att variera antalet blanksteg eller andra ”osynliga” tecken.

MD4 och MD5 är kontrollsumme-algoritmer konstruerade av Ron Rivest (RSA). MD4 introducerades 1990 och MD5 som en förbättring 1992. Båda genererar en 128 bits kontrollsumma.

SHA är utvecklat av NIST (National Institute of Standards and Technology) tillsammans med NSA (National Security Agency). Algoritmen introducerades 1992. SHA producerar en 160 bits kontrollsumma.

DES kan också användas för beräkning av kryptografiska kontrollsummor.

4.3.4 Digital signatur

Digital signatur är som namnet antyder en motsvarighet till ”analog” signatur – underskrift med bläckpenna. Liksom sin analoga motsvarighet ska den digitala signaturen bekräfta såväl innehållets riktighet (äkthet) som vem som ansvarar för dess innehåll. Den digitala signaturen är ett ”tillägg” till dokumentet och kan kontrolleras av den läsare som vill verifiera innehållet.

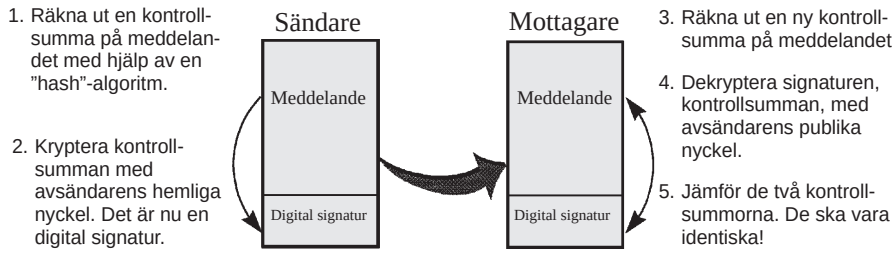
Den digitala signaturen skapas i följande steg:

1. En kontrollsumma beräknas på dokumentet.
2. Kontrollsumman krypteras med den hemliga nyckeln. Det krypterade resultatet är den digitala signaturen.

Den digitala signaturen lagras/överförs tillsammans med eller separat från ursprungsdokumentet. Till den digitala signaturen kan den publika nyckeln bifogas, eventuellt som en del av ett s.k. certifikat. Certifikatet innehåller förutom den publika nyckeln, identitetsuppgifter samt annan säkerhetsrelevant information.

Kontroll/verifiering av digital signatur görs i dessa steg.

3. En kontrollsumma beräknas på dokumentet vars innehåll ska verifieras.
4. Den digitala signaturen dekrypteras med den publika nyckeln (som mottagaren måste ha fått på ett säkert sätt).
5. Den beräknade kontrollsumman jämförs med den dekrypterade signaturen.



Figur 11. Digital signatur.

4.4 Behörighetskontrollsystem (BKS)

Behovet av att reglera åtkomsten till information i IT-systemen ökar i takt med möjligheterna till kommunikation mellan systemen. Behovet av åtkomstskydd varierar, beroende på vilken information som hanteras, men generellt kan sägas att information sällan är så betydelselös för informationsägaren att den inte behöver någon typ av skydd. Den starka utvecklingen av datakommunikation har stärkt behovet av behörighetskontroll, eftersom de ökade kommunikationsmöjligheterna dels har ökat antalet användare inom organisationen, dels har gjort det lättare för utomstående att nå IT-systemen.

Den enklaste formen av behörighetskontroll kan man träffa på i persondatormiljö, där en fristående persondator, eller ett minnesmedium, kan låsas in i ett säkerhetsskåp när utrustningen inte används. Detta är emellertid ingen metod som är tillämpbar i datormiljöer där flera personer delvis ska ha tillgång till samma resurser. I ett fleranvändarsystem är behörighetskontroll normalt en kombination av tekniska och administrativa åtgärder.

Ett behörighetskontrollsystem som reglerar åtkomsten till olika delar av systemet, och som även kan reglera vem som får göra vad i ett system, bör finnas i alla datormiljöer där flera användare är anslutna. I system där det enligt klassificeringen av information är **allvarligt** eller **mycket allvarligt,** om viss information sprids till obehörig eller någon gör en otillåten ändring, ställs speciellt höga krav på behörighetskontrollsystemets olika funktioner. Det är därför

viktigt att man har klart för sig vilken skyddsnivå man behöver ha för den information som ska bearbetas i systemet.

En definition av ett BKS är att det är ett system som kan kontrollera behörighet och som kan skydda information så att den endast är tillgänglig för den som har rätt till den. Ett BKS består av ett antal samverkande funktioner som tillsammans kan tillhandahålla ett grundläggande behörighetsskydd. En förutsättning för att man ska kunna ha kontroll över tillgången till olika resurser i ett IT-system är alltså att det finns ett behörighetskontrollsystem installerat i den dator som används.

Ett BKS ska kunna:

- identifiera och autenticera behöriga användare
- tilldela och kontrollera *åtkomst*, d.v.s. varje användare ska ha definierad åtkomst till ett antal resurser som han/hon behöver för att kunna utför sina arbetsuppgifter (resurs är i det här sammanhanget dator, lagringsmedier, skrivare, kommunikationsförbindelser, tillämpningsprogram, hjälpprogram och systemprogram samt alla typer av lagrade data)
- rapportera alla händelser i såväl BKS som de tillämpningssystem och andra resurser som BKS kontrollerar t.ex. genom *loggar.*

Ett BKS kan antingen vara inbyggt i den systemprogramvara som leverantören tillhandahåller, eller vara en fristående programvara som är utvecklad för en viss datormiljö. Kraven på ett BKS måste alltid ställas med utgångspunkt från verksamhetens behov.

4.4.1 Identifiering och autenticering

Identifiering innebär att en användare eller en resurs anger sin identitet för att få tillgång till system, information eller liknande. Identiteten kan vara t.ex. ett namn eller nummer. Identiteten måste vara unik inom ”systemet” så att man kan skilja mellan olika användare. Varje användare av ett IT-system ska alltså finnas registrerad i BKS med en egen identitet. Användaridentiteten är öppen information och måste kompletteras med något som varje användare ensamt känner till eller har tillgång till, detta för att kunna

autenticera/verifiera att den som utger sig för att vara någon verkligen är den personen.

Autenticering innebär alltså kontroll/verifiering av uppgiven identitet, t.ex. vid inloggning, vid kommunikation mellan två system eller vid utväxling av meddelanden mellan användare. Tre tekniker för autenticering av användare eller andra resurser kan identifieras. Dessa kan användas var och en för sig eller i olika kombinationer:

- Något man *VET* (t.ex. ett lösenord, personlig kod/PIN, eller en kombination av fakta från en persons bakgrund).
- Något man *HAR* (t.ex. en token, bärare eller en krypteringsnyckel).
- Något man *ÄR* (t.ex. biometriska egenskaper som fingeravtryck eller röstmönster).

Användandet av s.k. gruppidentiteter, där alla har samma identitet och lösenord, är inte att rekommendera, även om ett stort antal användare ska ha tillgång till samma resurser i systemet och utföra samma arbetsmoment. I varje system ska det gå att knyta en viss händelse i systemet till en specifik användare.

Något man VET

Lösenord, PIN eller dylikt

Det vanligaste sättet att autenticera är att varje användare har ett eget lösenord, som måste användas tillsammans med användaridentiteten för att man ska få tillgång till ett system eller en delresurs. För att ett BKS ska fungera på ett effektivt och ändamålsenligt sätt måste det finnas regler för lösenordshantering. Dessa regler måste kunna kompletteras/stödjas med tekniska funktioner i BKS. Dessa funktioner bör kunna konfigureras så att de uppfyller de krav som verksamheten ställer på säkerheten. Exempelvis bör det finnas funktioner som ställer krav på hur användaren väljer sitt lösenord, d.v.s:

- antalet tecken i lösenordet
- att det inte är för enkelt t.ex. egennamn eller upprepning av samma tecken

- att det måste innehålla specialtecken
- att det måste vara alfanumeriskt
- att användaren måste byta lösenord regelbundet
- att användaren inte väljer samma eller ett tidigare använt lösenord vid lösenordsbyten.

BKS ska skydda lösenordstabellen mot obehörig åtkomst och det bör också finnas funktioner som gör det möjligt att kryptera lösenordstabellen. Lösenordstabellen kan t.ex. krypteras med en envägsfunktion. Envägsfunktionen har den egenskapen att den är lätt att använda för kryptering men väsentligt mycket svårare att dekryptera. Vid autenticering av en användare krypteras lösenordet vid mottagandet och jämförs med motsvarande i lösenordstabellen.

Lösenordstabellen kan också vara krypterad med en ”vanlig” krypteringsalgoritm. Lösenordet krypteras då lokalt och går därmed inte i klartext över ett öppet nät. Vid autenticering dekrypteras lösenordet och jämförs med den identifierade användarens lösenord i lösenordstabellen (dekrypterad). Varje lösenord kan tillföras ett slumptal vid krypteringen av lösenordstabellen. Detta försvårar för en obehörig att kunna tyda om två användare har samma lösenord.

Lösenord som överförs antingen i klartext eller i krypterad form kan utsättas för s.k. trafikanalys. Genom att analysera trafiken kan en obehörig genom att t.ex. titta på paketens storlek eller frekvensen på trafiken, dra slutsatser om paketens innehåll, utan att egentligen ha sett innehållet. Autenticeringsinformation bör skyddas mot trafikanalys. Detta kan man göra genom att man ”slumpmässigt” tillför autenticeringsinformationen extra information så att paketen får olika storlek varje gång.

Ytterligare en funktion som kan höja säkerhetsnivån är att BKS efter identifieringen visar något som ”endast” är känt av användaren och systemet, t.ex. senaste inloggningsdatum och tid. Den behöriga användaren kan verifiera att informationen är korrekt innan t.ex. lösenordet matas in.

Vid inloggning kan det ibland finnas behov av att lägga till ytterligare attribut för att autenticeringen ska vara tillräcklig, t.ex. att användaren endast sitter vid en definierad arbetsplats. Detta kan öka styrkan på autenticeringen.

Av olika anledningar är metoden med lösenord inte särskilt säker. Även om ovanstående funktioner finns i drift finns det alltid möjligheter att användarna väljer lösenord som är möjliga att gissa. Om systemet kräver mycket långa lösenord finns det risk för att man måste skriva upp sitt lösenord på papper, vilket naturligtvis inte heller är godtagbart. Samma risk löper man om en användare måste ha olika lösenord till olika resurser. Vid användning av gemensamt lösenord för en grupp användare ökar givetvis risken för att lösenordet genom slarv ska bli känt utanför gruppen.

Engångslösenord

Engångslösenord är som namnet antyder lösenord som bara används en gång, d.v.s. användarens lösenord ändras varje gång han/hon identifierar sig mot systemet. En metod för detta är att användaren förses med en lista med lösenord som han/hon sedan använder i en bestämd ordning. En annan metod för detta är att användaren blir tilldelad en matematisk funktion i stället för ett lösenord. Vid identifiering och autenticering skickar systemet ett argument till användaren som sedan gör en beräkning med den tilldelade funktionen och returnerar resultatet till systemet. Systemet gör samma beräkning och jämför resultaten. Förfarandet bygger alltså på ett s.k. challenge-response förfarande. Den matematiska funktionen kan vara mer eller mindre komplicerad. Med den enklaste varianten kan användaren själv göra beräkningen.

Något man HAR

Engångslösenord

Enklare metoder för engångslösenord finns beskrivna i avsnittet *Något man VET*. Är den funktion som användaren blir tilldelad alltför avancerad kan användare omöjligt komma ihåg den eller göra beräkningen själv. Den finns då implementerad någonstans, exempelvis i en separat dosa. Funktionen eller dosan bli något man *HAR*. Principen kan även kompletteras med att användarens lösenord används som en del i funktionen.

Det finns också dosor eller programvaror som med jämna mellanrum genererar lösenord med hjälp av en lösenordsgenerator. Dosans/programvarans generator är synkroniserad med en likadan process i BKS. Processen i BKS jämför vid autenticeringen ett mottaget lösenord med det som den själv har genererat.

Stark autenticering

Stark autenticering är en sorts challenge-response eller handskakningsförfarande. Metoden bygger på en kryptografisk autenticering av en identitet med hjälp av en definierad algoritm (asymmetrisk eller symmetrisk) och en privat eller hemlig nyckel. Nycklarna är något man *HAR.* BKS sänder ett slumptal till den användare som ska autenticeras och han/hon krypterar slumtalet med sin privata eller hemliga nyckel. Informationen som krypteras kan också innehålla en tidsvarierande parameter. Vanliga tidsvarierande parametrar är löpnummer eller någon typ av tidsstämpel. Den krypterade informationen skickas sedan tillbaka och BKS (mottagaren) verifierar identiteten genom att kryptera med den delade hemliga nyckeln eller alternativt genom att dekryptera med motpartens publika nyckel. Resultatet jämförs sedan med ursprungsvärdet. Autenticeringen kan sedan upprepas fast åt andra hållet, d.v.s. BKS får autenticera sig mot användaren. Detta förfarande kallas ömsesidig autenticering.

Identifieringskort

Vanliga lösenord kan kombineras med olika former av kort. Kortet kan innehålla något unikt som ökar autenticeringsinformationen. Kortet kan vara t.ex. magnetremsekort eller aktiva kort. En kortläsare måste då anslutas till alla arbetsplatser.

Något man ÄR

Det säkraste sättet att identifiera och autenticera användare är s.k. biometriska tekniker, vilka emellertid ännu så länge i allmänhet är alltför kostsamma. I dag finns några framträdande sådana metoder, nämligen fingeravtryck, handgeometri, retinaavläsning (ögonbottenavläsning), röstmönster, signaturdynamik (namnteckning) samt tangentnedslagsdynamik.

Motringning

För uppkoppling från en distansarbetsplats finns det utrustning för motringning, som tar emot ett samtal till datorn, kopplar ner det och ringer tillbaka på ett förutbestämt nummer, kopplat till den identitet som anges vid den första uppringningen. Sådan motringning kan öka säkerheten, men med moderna telefonväxlar finns

möjligheter till vidarekoppling som styr om samtal till en annan telefon, vilket medför stora risker för obehörig åtkomst.

Exempel på vad som bör gälla för identifierings- och autenticeringsfunktionerna i BKS:

- Varje användare bör ha personlig identifiering och autenticering.
- Styrkan i autenticeringsmekanismen ska vara känd.
- Följande regler bör om möjligt tillämpas för lösenord:
  - Lösenordet bör bestå av minst sex tecken.
  - Inga enkla lösenord bör väljas (d.v.s. inga ord från lexikon eller uppslagsverk eller lösenord som enbart består av bokstäver).
  - Autenticeringsinformation (t.ex. lösenord) bör endast lagras i krypterad form.
  - Lösenord bör ändras med minst 60 dagars intervall.
  - Gamla lösenord bör inte kunna återanvändas inom ett år.
- En identitet bör spärras för inloggning efter definierat antal på varandra följande felaktiga lösenord.
- Endast IT-säkerhetsansvariga bör kunna upphäva ovan nämnda spärrar.
- Längden på en autenticering bör kunna begränsas tidsmässigt för inaktiva inloggningsperioder (automatisk utloggning).

4.4.2 Åtkomstkontroll

Åtkomstkontrollen syftar till att förhindra att en användare får tillgång till andra data, program eller övriga resurser än just dem, som han eller hon behöver i sitt arbete.

Hur finmaskig åtkomstkontrollen behöver vara i en organisation styrs av en mängd faktorer. En grundligt genomförd informationsklassificering med avseende på informationens känslighet i olika avseenden utvisar i vilken mån det finns information som bara bör vara tillgänglig för vissa användare. Observera att även IT-perso-

nalens tillgång till olika resurser ska regleras genom behörighetskontroll.

Behörighet att få tillgång till olika resurser bör beskrivas i form av behörighetsprofiler, som lagras i BKS. En sådan behörighetsprofil ska beskriva vilka resurser som ska vara tillgängliga, och ange vad man får göra, t.ex. ta del av information, lägga in nya uppgifter, förändra och ta bort. Varje användare av systemet knyts sedan till den behörighetsprofil som svarar mot de behov vederbörande har i sitt arbete av att få tillgång till ett visst IT-system eller en viss delresurs. Åtkomstkontrollen bör innehålla funktioner som gör det möjligt att:

- definiera rättigheter per användare vad gäller att läsa, kopiera, skriva, ändra, radera och exekvera filer eller program
- kunna skilja på användargrupper
- kontrollera alla IT-resurser som hanteras, t.ex. servrar, fysiskt och logiskt hårddiskutrymme, filer, databaser, kommunikationsingångar och skrivaranslutningar
- spärra användaridentiteter som har brutit mot uppställda åtkomsträttigheter
- upphäva aktiverade spärrar men endast med aktuellt skydd i drift
- specificera tidsperioder som anger när olika användare tillåts upprätta sessioner och initiera processer. Det ska gå att specificera veckodag, datum och/eller klockslag.
- specificera antalet samtidiga sessioner för användarna
- användarna själva kan förändra åtkomstskyddet på de objekt som de själva skapat eller givits rättighet att ändra åtkomstskyddet på
- definiera ett grundskydd för alla nya filer som skapas
- kontrollera att alla processer som initieras av IT-systemets objekt är valida. Detta gäller även de processer som initieras av serviceprogram av olika slag.
- förhindra att användare utan definierad och godkänd systemidentitet får tillgång till IT-systemets resurser

- hindra all manipulering med processer som initierats av BKS
- förhindra att obehöriga användare får åtkomst eller möjlighet att återskapa data från frigjort sekundärminne.

4.4.3 Loggning

Ett BKS ska kunna tillhandahålla funktioner så att alla händelser i datorn lagras i en s.k. loggfil. Av loggen ska bl.a. framgå vilka användare som har varit inloggade i systemet, vilka resurser de utnyttjar och tidpunkten för olika aktiviteter. När olika tillämpningsprogram aktiveras ska loggen innehålla t.ex. uppgift om vem som aktiverat aktuellt program, tidpunkten för detta och även viss information från de bearbetningar som utförts.

En särskild logg ska finnas som registrerar all information om händelser i själva BKS-systemet, t.ex. registrering av nya användare och deras behörigheter, ändringar i behörighetsinformation, försök till åtkomst av resurser som man inte är behörig att använda och försök att komma in i systemet med felaktig identitet och/eller lösenord.

Det bör helst finnas möjlighet att få direktrapportering till en särskild organisatorisk funktion vid försök till obehörig åtkomst och andra onormala händelser i systemet.

Rapportfunktionens utformning i ett BKS är av stor betydelse för möjligheterna att på ett effektivt sätt följa upp systemanvändningen och åtgärda de brister som kan förekomma.

Exempel på funktioner som loggfunktionen bör kunna erbjuda:

- möjligheter att automatiskt lagra rapporter på lagringsmedium
- möjligheter att tillämpa kontinuerlig utskrift av rapporter, d.v.s. rapportering sker omgående via skrivare. Det bör också vara möjligt att kombinera omedelbar utskrift och lagring av rapporter.
- enkel definiering av vilken typ av rapportering som ska ske
- funktioner för sökning i elektroniskt lagrade rapporter
- funktioner som möjliggör att man enkelt kan definiera hur rapporteringen ska presenteras på såväl bildskärm som skrivare.

- funktioner för rensning i rapportarkiv enligt definierade regler för detta
- funktioner för flexibel definiering av vilken information som ska finnas med i loggen, t.ex.:
  - typ av händelse (d.v.s. anledningen till att händelsen loggas)
  - användaridentitet av den användare som är ansvarig för händelsen
  - datum och tid för händelsen
  - ursprunglig dator- eller nodidentitet ur vilken händelsen härrör.
- funktioner som möjliggör att alla misslyckade försök att logga in under en särskild användaridentitet visas för användaren nästa gång han/hon loggar in
- möjligheter att registrera alla säkerhetsrelevanta händelser i IT-systemet, t.ex:
  - felaktigt angivna identiteter och lösenord, försök till obehörigt utnyttjande av resurser
  - upprättade sessioner och processer
  - pågående sessioner och processer
  - avbrutna/avslutade sessioner och processer
  - samtliga giltiga identiteter
  - samtliga i systemet ingående resurser
  - samtliga resursers behörigheter
  - lösenord som inte bytts inom föreskriven tidsperiod
  - identiteter som blivit ogiltiga på grund av överskriden giltighet
  - samtliga åtgärder/aktiviteter som initieras av behörighetsadministratören.
- möjligheter att följa upp alla misslyckade inloggningsförsök.

4.5 Aktiva kort

Ett aktivt kort, innebär enligt en vanlig definition:

”kort utrustat med en eller flera integrerade kretsar inkluderande komponenter för lagring och bearbetning av data”.

Det aktiva kortet är alltså i sig en ”dator” med:

- Processor
- Minne
- I/O (gränssnitt mot omvärlden).

4.5.1 Funktioner på det aktiva kortet

Till skillnad från magnetremsekort kan aktiva kort lagra relativt stora mängder information. Den lagrade informationen kan också bearbetas på kortet med hjälp av den inbyggda datorn. Det aktiva kortet kan även ha funktioner för åtkomstkontroll till kataloger och filer på kortet. Vanligtvis är denna funktion implementerad med s.k. PIN-kodsverifiering. Många aktiva kort är också utrustade med speciell logik för att öka kapaciteten vad gäller kryptering eller autenticering. De är i dessa fall oftast knutna till en eller ett par algoritmer, vanligen DES eller RSA.

Ibland använder man sig av begreppet IC-kort (Integrated Circuit Cards) när man talar om aktiva kort. IC-kort är ett överordnat begrepp som även omfattar kort som inte har någon inbyggd dator, t.ex. minneskort. Telefonkorten är exempel på IC-kort som inte har någon processor utan enbart ett minne med förlagrade markeringar.

Fördelarna med aktiva kort är bland annat:

- Kompakt – kreditkortsformat.
- Stort minnesutrymme – om man jämför med t.ex. magnetremsekort.
- Information skyddad mot kopiering – säkra minnesareor.
- Möjligheter till bearbetning på kortet.

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

Identifiering – identifiering av en person.
Digitala signaturer – på elektroniska dokument.
Kryptering – av dokument och kommunikation.
Lagring av information – hemlig eller känslig information.

Kryptering

Kryptering på det aktiva kortet har fördelen att krypteringsnyckeln aldrig blir tillgänglig utanför det aktiva kortet, t.ex. i samband med att den läses av i en läsutrustning, vilket avsevärt minskar risken att nyckeln kommer i orätta händer.

Identifiering och autenticering

En av de vanligaste applikationerna för aktiva kort i säkerhetssystem är autenticering. Det aktiva kortet erbjuder här en högre säkerhet jämfört med magnetremsekort och lösenordsrutiner. Till skillnad från magnetremsekort eller liknande kan det aktiva kortet ges en helt unik identitet som inte går att kopiera till ett annat aktivt kort. Det är också möjligt att ge tillgång till denna unika identitet endast genom ett lösenord/PIN-kod. Med detta är det möjligt att automatiskt verifiera ett kort samt att rätt PIN-kod används.

Autenticering mot det aktiva kortet sker normalt i följande steg (s.k. challenge-response förfarande):

1. Användaren stoppar kortet i en kortläsare.
2. Användaren identifierar sig genom att slå in PIN-kod på kortläsarens tangentbord.
3. Kortläsaren (läsutrustningen) skickar ett slumptal till kortet.
4. Det aktiva kortets processor krypterar slumptalet med en (privat) nyckel lagrad på kortet.
5. Läsutrustningen dekrypterar talet från kortet med motsvarande (publika) nyckel och jämför resultatet. Om det dekrypterade talet är samma som det ursprungliga slumptalet anses identiteten fastställd.

När användaren har autenticerat sig mot kortet används en liknade procedur för autenticering mot andra måldatorer.

Digital signatur

De aktiva kortet kan användas för signering av dokument med digital signatur.

Lagring av information

På det aktiva kortet finns det möjligheter att lagra information som endast är åtkomligt via en PIN-kod. Informationen kan t.ex. vara hemlig eller känslig. Det aktiva kortet fungerar även som en utmärkt lagringsplats för t.ex. krypteringsnycklar eller andra mekanismer för autenticering.

4.5.2 Utgivning och hantering av aktiva kort

Användningen av aktiva kort innebär att en organisation måste byggas upp som ansvarar för utgivning och hantering av aktiva kort. De aktiviteter som ingår är bl.a. följande:

- nyckelgenerering (symmetriska och asymmetriska)
- kontroll av personuppgifter
- elektrisk personalisering
- grafisk personalisering
- distribution av kort
- utlämnande av kort till användare
- distribution av PIN-kod
- spärrning av kort eller återtagande av kort
- hantering av låsta kort (användaren har angivit fel PIN-kod för många gånger)
- tekniska eller logiska fel i maskin- och programvaran (t.ex. när kortet inte fungerar p.g.a. fysiskt fel).

4.6 Brandväggar

En brandvägg består av en eller flera nätkomponenter som placeras mellan två datornät för att enligt en förutbestämd policy kontrollera och begränsa trafiken mellan dem. De nätkomponenter som ingår i en brandvägg är vanligen routerutrustningar och specialanpassade datorer. All trafik mellan de två datornäten passerar genom brandväggen och endast trafik som är godkänd enligt den förutbestämda policyn tillåts passera. För att kunna erbjuda en effektiv funktion måste brandväggen även kunna skydda sig själv från angrepp.

En brandvägg ska av övervakningsskäl även innehålla funktionalitet för loggning av såväl normal som otillåten trafik och bör erbjuda verktyg för analys av loggad trafik. Det bör också finnas möjlighet att koppla larm till trafik som indikerar säkerhetsöverträdelser.

Det finns olika typer av brandväggar. Allt från ett ”enkelt” paketfilter, som släpper igenom eller blockerar trafik beroende på information i IP- och TCP-header, till en avancerad applikationsgateway.

I en brandväggslösning ingår även organisationen runt brandväggen. Eftersom brandväggen fungerar i en föränderlig miljö måste den genomgå ständig utveckling för att ge skydd mot nya typer av angrepp. En förutsättning för att brandväggen ska ge optimalt skydd är därför en väl definierad och genomtänkt administrationsvägledning.

4.6.1 Komponenter

I en brandvägg kan en router användas för att filtrera paket. I de flesta routrar kan man sätta upp accesskontrollistor för varje fysisk port. Accesslistorna kan utformas som kombinationer av avsändar-/mottagaradress, protokolltyp och portadress. En applikationsgateway är en speciellt anpassad dator, i vilken en eller flera s.k. proxyapplikationer körs. Applikationsgatewayen agerar på en användares uppdrag, d.v.s. för varje tjänst som en användare utnyttjar finns det en proxyapplikation som svarar för förbindelsen från nätets utsida till dess insida eller omvänt. Proxyapplikatio-

nerna sorterar alltså inkommande och utgående trafik på applikationsnivå. Detta innebär att då nya applikationsprotokoll dyker upp måste modifieringar göras i brandväggen för att kunna hantera den nya trafiken.

4.6.2 Utvärdering av brandväggar

I dag finns ett flertal olika brandväggar ute på marknaden och det kan vara svårt att veta vilken brandvägg som lämpar sig bäst för den egna verksamheten. Nedan följer ett antal utvärderingskriterier.

Kostnader vad gäller införskaffande och eventuella extrakostnader:

- pris
- extra utrustning
- administrationskostnader
- eventuella modifieringar av klientprogramvaror.

Ingående funktioner bör även utvärderas både med avseende på de behov man har i dag men också med avseende på framtida behov. Funktioner som man bör utvärdera är bl.a.:

- antalet nätgränssnitt
- kapacitet
- hur olika tillämpningar hanteras
- övervakningsmöjligheter, vid intrång och om brandväggen slutar fungera
- behov av administration och kompetens
- hur brandväggen passar in i befintlig nätarkitektur och utrustning.

4.6.3 Riktlinjer för brandväggen

Två alternativa inriktningar kan urskiljas vad gäller riktlinjer för hur en brandvägg ska installeras och administreras i en verksamhet.

- Riktlinjer A – Det som uttryckligen inte är tillåtet är förbjudet vilket innebär att:

  - brandväggen ska blockera allt
  - tjänster tillåts från fall till fall, d.v.s. efter en ordentlig genomgång av behovsbilden kontra riskbilden
  - användarna är relativt begränsade i sin handlingsfrihet.
- Riktlinjer B – Allt som uttryckligen inte är förbjudet är tillåtet vilket innebär att:
  - det ställs stora krav på brandväggsadministratören som delvis måste ha förmågan och kompetensen att förutse vilka typer av hot och risker som kan tänkas uppstå och därmed hela tiden jaga säkra alternativ
  - användarna har total frihet

Av dessa två inriktningar är den första, Riktlinjer A, att rekommendera.

4.6.4 Brandväggen i befintlig miljö

Vid t.ex. informationsspridning via Internet bör man överväga hur man ska konfigurera sin informationsspridningsmiljö. Inblandade komponenter är informationsdatabaser, WWW-servrar och andra tjänsteservrar samt brandväggen. De olika alternativen innebär både fördelar och nackdelar. Tre alternativ har identifierats. En WWW-server används som genomgående exempel på tjänsteservrar.

1. Tjänsteservrar utanför brandväggen och informationsdatabasen innanför

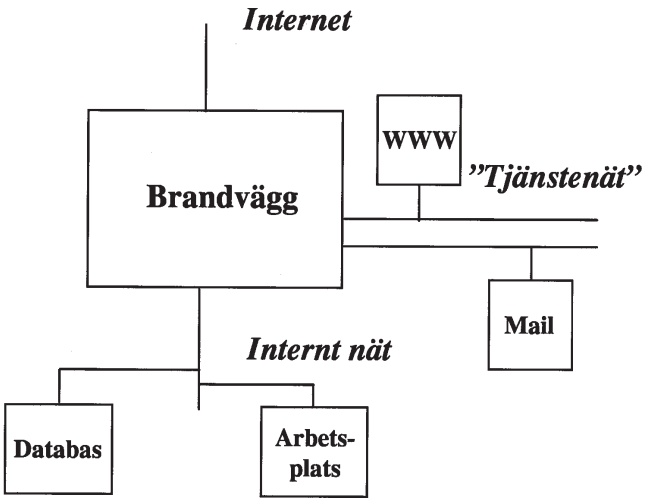
En tunnel måste konfigureras genom brandväggen. Tunneln innebär att brandväggen endast ska släppa in trafik från t.ex. WWW-servern (IP-nummeridentifierad), enligt ett visst format och på en viss port o.s.v. Brandväggen pratar sedan med databasen på ett visst portnummer. Databasen måste kunna prata TCP/IP. Restriktioner vad gäller åtkomsträttigheter i databasen bör också konfigureras så att databasen hålls konsistent och korrekt.

Fördelar:

- Endast en databas behövs (ingen spegling), databasen är dessutom ganska skyddad av brandväggen, jämfört med om den skulle varit placerad utanför brandväggen.

Nackdelar:

- En ”öppning” genom brandväggen finns.
- Overhead, eftersom varje paket måste öppnas och analyseras.



Figur 12. Tjänsteservrar utanför brandväggen och informationsdatabasen innanför.

2. WWW-servern körs i s.k. dual-mode

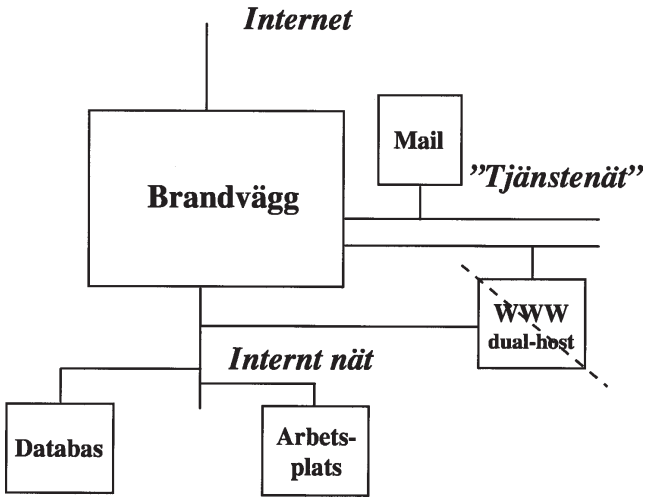
WWW-server konfigureras så att ingen IP-forwarding är möjlig.

Fördelar:

- Lättare att uppdatera innehållet (HTML-dokument o dyl.) i webservern. Om web-servern är säkrad (ingen IP-forwarding och inga andra TCP/IP servrar igång etc.) så är databasens innehåll väl skyddat. Ingen spegling av databas behövs. Ingen lucka finns i brandväggen.

Nackdelar:

- Att stänga av IP-forwarding i UNIX-miljö är komplicerat.
- Eventuella buggar i webservern kan vara en stor säkerhetsrisk. Om någon obehörig lyckas bryta sig in i webservern så har denne full tillgång till det interna nätet.



Figur 13. WWW-servern körs i s.k. dual-mode.

3. Spegling av informationsdatabasen

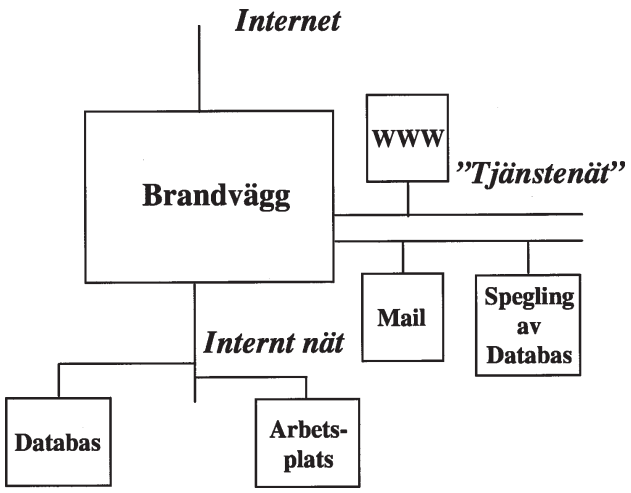
WWW-servern placeras tillsammans med en speglad version av originaldatabasen utanför brandväggen. En speciell applikation känner av uppdateringar i originaldatabasen och uppdaterar den speglade databasen med definierad kontinuitet.

Fördelar

- Eftersom inga luckor finns in mot det interna nätet så måste denna uppsättning anses vara den mest säkra ur intrångs-synvinkel.

Nackdelar

- Ej realtidsuppdaterad information.
- Två databaser måste administreras.



Figur 14. Spegling av informationsdatabasen utanför brandväggen.

4.7 Säkerhetskopiering

En säker driftmiljö kräver strikta rutiner för hur reservkopior på lagrade data och program ska tas samt riktigt utformade förvaringsutrymmen för lagringsmedier. En generation av lagrade data och program ska alltid förvaras på en plats som är väl avskild från den övriga driftmiljön. Sådana säkerhetskopior ska kunna användas i en nödsituation, t.ex. då såväl utrustning som övriga kopior av data och program har förstörts.

Med jämna tidsintervall måste man testa att de reservkopior som man har tagit verkligen går att använda. Det har t.ex. visat sig att när man har tagit kompletta reservkopior av persondatorns hela skivminne, så kan det ibland vara svårt att åter läsa in informationen från reservkopiorna. Det kan därför vara nödvändigt att ta selektiva kopior på de program och data som man har lagrade.

Om man planerar för att kunna flytta över sina egna bearbetningar till en annan persondator, i det fall den egna datorn av någon anledning inte går att använda, måste man också testa att de säkerhetskopior man har tagit går att läsa in på den tänkta reservdatorn. Reservkopieringsprogramvaran bör kunna erbjuda funktioner som innebär följande:

- Reservkopior tas enligt de regler som är fastställda, d.v.s. med bestämda tidsintervall och av olika systemresurser. I alla datormiljöer, där flera användare delar på samma datorresurser, ska det finnas antingen programvara för automatisk reservkopiering eller också en speciell organisatorisk funktion som ansvarar för att reservkopiering blir gjord.
- Med fastställda intervall ska reservkopior testas så att man vet, att såväl de rent tekniska som de administrativa rutinerna fungerar.
- Selektiv säkerhetskopiering av specifika program eller filer.

Det bör finnas åtminstone tre generationer säkerhetskopior av program och data. En generation ska förvaras i datamediaskåp, skilt från den lokal där övriga säkerhetskopior förvaras.

4.7.1 Strategi för säkerhetskopiering

Viktiga saker att tänka på när man ska definiera riktlinjer för verksamhetens säkerhetskopiering och hantering:

- Vilken är den mest kritiska informationen och var finns den?
- Hur ska säkerhetskopior tas? Centralt och/eller lokalt? Lokal säkerhetskopiering kan vara kostsamt men kan vara nödvändig i vissa situationer.
- Hur ska man hantera mobila användare?
- Regler för filstruktur, lagringsplats och namnkonventioner kan underlätta hanteringen av säkerhetskopior.

Att arbetsplatserna bara innehåller oviktig information och att all viktig information lagras på den centrala servern stämmer inte alltid. Det förekommer, i större utsträckning än man tror, att användare lagrar viktig information lokalt på hårddisken. Idag finns det produkter (LAN-baserade säkerhetskopierings-servrar) som kan ta säkerhetskopior på persondatorer som är anslutna till det lokala nätet. För mobila användare är det relevant att vid uppkoppling mot det lokala nätet eller med schemalagda mellanrum under en uppkopplingsperiod, ta reservkopior.

4.8 Virusskydd

När man talar om datavirus är det viktigt att skilja mellan dessa och andra obehagliga händelser som kan inträffa i ett IT-system. Många händelser som beskrivs som virusangrepp är i själva verket någon annan företeelse vilken i och för sig kan förorsaka lika stor eller större skada än ett angrepp av virus.

Datavirus är en självständig del av ett program som har dolts i ett annat program och virusprogrammets instruktioner utförs inte förrän det program där det ligger dolt aktiveras. De är alltså beroende av redan existerande program eller filer att dölja sig bakom. Det finns också virus som fungerar som självständiga program.

Viruset består av ett antal instruktioner som inledningsvis söker igenom alla tillgängliga filer. Tillgängligheten styrs av den aktuella användarens behörighet, var viruset för tillfället befinner sig, användarens programbibliotek m.m. Viruset läser in alla filer och granskar dem för att se om dess eget speciella kännemärke återfinns. Om så är fallet har det varit där tidigare och smittat ner den aktuella filen. Om filen inte smittats så förses den med en kopia av viruset och märks innan den återigen skrivs in på plats. Så har ytterligare en fil blivit smittad. Smittspridningen kan ske olika snabbt beroende på i vilken typ av program och datormiljö viruset har lagts in och vilka egenskaper det för övrigt utrustats med.

Ett datavirus förmåga att sprida sig till andra delar av ett system är i sig en egenskap som är oönskad, men än värre är problemet att det också kan vara utformat så att det medför omfattande konsekvenser. Vilka skador ett datavirus kan förorsaka beror dels på vilka avsikter skaparen haft dels på hur snabbt man upptäcker angreppet. Många datavirus innehåller tämligen harmlösa instruktioner som att åstadkomma en rolig utskrift på datorns skärm, t.ex. när ett visst datum infaller på en viss veckodag, medan andra innehåller instruktioner som att förstöra alla datafiler.

En allvarlig egenskap hos datavirus är att det kan ligga dolt i en dator under lång tid utan att någon upptäcker att det finns där. Det betyder att de säkerhetskopior som man tagit efter smittillfället också är smittade. I det läget går det inte bara slänga den senaste versionen där problemet uppenbarade sig och gå tillbaka till en gammal version utan det krävs hjälp av speciell programvara som i bästa fall kan återställa det som förstörts.

Skydden man tar till ska stå i relation till de skador ett virusangrepp kan förorsaka och en bedömning av hur stor man anser risken för ett angrepp vara.

När det gäller skydd mot datavirus är det fråga om:

- att förebygga att man överhuvud taget blir smittad
- att upptäcka ett smittat program och då förhindra smittspridning
- att återställa ett smittat system.

Som alltid när det är fråga om skyddsåtgärder i IT-sammanhang är det främst de förebyggande åtgärderna som ska prioriteras. Givetvis måste det också finnas en plan för hur man ska bete sig om olyckan skulle vara framme, men när det gäller datavirus kan det vara för sent om man försummat alla förebyggande åtgärder.

Det är också, som vi tidigare framhållit, de administrativa åtgärderna som är de viktigaste och de är även när det gäller virus en förutsättning för att andra skyddsåtgärder ska ha avsedd effekt. Att införskaffa ett antivirusprogram och ändå tillåta vem som helst att läsa in okontrollerade program är ingen effektiv skyddsåtgärd.

Vi ger i det följande exempel på:

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

4.8.1 Förebyggande skydd

De förebyggande skydden varierar beroende på en rad olika faktorer, t.ex. vilken datormiljö man har, hur stor organisationen är, hur ansvaret är fördelat mellan olika personalkategorier, (t.ex. mellan nätansvariga och annan IT-personal). De förebyggande skydden är en blandning av administrativa, tekniska och byggnadstekniska skyddsåtgärder.

Varje organisation bör se till att ha instruktioner för olika personalkategorier, så att alla vet vem som ansvarar för vad. Det är viktigt att även användarna informeras om vad som är tillåtet respektive otillåtet i den IT-miljö där de arbetar. Speciellt i en miljö med lokala nät, där persondatorer med diskettenhet är anslutna, är det viktigt att alla känner till de restriktioner som finns (bör finnas) när det t.ex. gäller att läsa in program i sin PC.

Även om man har antivirusprogram bör man följa vissa råd, varav många har att göra med att ha ordning och reda i sin IT-verksamhet.

Nedan följer en checklista med åtgärder för att åstadkomma ett bra förebyggande skydd mot virusangrepp:

- Skydda datorn fysiskt och logiskt mot obehörig användning.
- Se till att utnyttja alla de möjligheter som finns till behörighetskontroll av alla som har tillgång till systemet. Ge aldrig högre behörighet än den som en viss användare behöver för att utföra sina arbetsuppgifter.
- Ge den som har de högsta privilegierna till systemet två olika behörigheter, förutom den högsta även en relativt låg prioritet som normalt ska användas.
- Använd enbart program som kommer direkt från en känd programvaruleverantör. Det är ovanligt att virus sprids den vägen.
- Testa nya program i en helt isolerad miljö.
- Ta aldrig emot piratkopierade program. Risken finns att de kommer från en smittad miljö.
- I fleranvändarmiljöer, vilket alla typer av nät kan sägas vara, bör program endast få läsas in från en bestämd enhet och endast av den eller de personer som har denna behörighet.
- Se till att originaldisketter eller andra lagringsmedia till program (gäller i synnerhet systemprogramvaran) samt en kopia förvaras åtskilda på väl skyddade och brandsäkra ställen. Alla sådana lagringsmedia ska vara skrivskyddade. Detta görs lite olika beroende på vad det är för diskettyp.
- Om personalen har möjlighet att själva ta kopior på diskett av sina egna data måste det finnas rutiner för hur kopior ska tas och förvaras. Personalen måste upplysas om vad som kopieras centralt och vad de själva måste kopiera.
- Spara original till program skrivskyddat och var noga med regelbunden säkerhetskopiering av program och data.
- Undvik att t.ex. låna ut datorer eller portabla hårddiskar till en okänd miljö. Risken finns att enheten kan vara smittad när den kommer tillbaka.

- Tillåt inte att program laddas till datorn direkt via något allmänt kommunikationsnät t.ex. Internet utan att de först virustestas. Många gratisprogram är tillgängliga på detta sätt och risken finns att sådana program kan vara smittade.
- Skydda det interna systemet med hjälp av s.k. brandväggar mot intrång via fasta externa kommunikationsförbindelser.
- I miljöer där egen programutveckling sker måste restriktioner finnas för vilka som får lägga in nya program i systemet. Alla operationer som har med inläggning av program att göra måste kunna loggas och detsamma gäller alla programändringar som sker.
- Var restriktiv med användningen av fjärrdiagnostik och se till att sådana åtgärder kan övervakas, t.ex. loggas.
- Se till att det finns någon ansvarig för alla bibliotek och tillåt inte att vanliga användare får privilegier som gör att de kan skapa egna bibliotek på gemensamma areor i en fleranvändar-/ nätmiljö.

4.8.2 Hur upptäcks virus

Det finns ett antal olika sätt att upptäcka datavirus. Det absolut tråkigaste sättet är att upptäcka att man drabbats av ett. Detta kan yttra sig olika beroende på vilket virus man drabbats av, t.ex:

- Det sker en oväntad utskrift av ett meddelande på skärmen.
- Systemet börjar plötsligt att gå trögt, det tar längre tid att ladda program eller att starta datorn.
- Program som ska finnas i systemet går inte att hitta.
- Ledigt utrymme minskar plötsligt drastiskt trots att man själv inte lagrat nämnvärd mängd data.
- Okända filer dyker upp i programbiblioteket.
- Programmets längd och skrivdatum har ändrats trots att inga ändringar gjorts.

Vissa av de här händelserna kan inträffa även om man inte drabbats av virus. Alla som under en längre tid har arbetat med datorer vet

att liknande saker kan hända när man t.ex. fått en ny version av ett program. I miljöer där egen programutveckling sker är det inte heller ovanligt att det skickas jul- och nyårshälsningar till personalen via datasystemet.

Det är inte desto mindre viktigt att vara uppmärksam när oväntade händelser inträffar, och att gå till botten med orsaken till dessa händelser.

Vad som händer är egentligen oförutsägbart förutom när man drabbats av ett känt virus med kända effekter. Annars är det helt beroende av vad virustillverkaren vill åstadkomma, om det bara är ett ”oskyldigt” skämt eller om man vill åstadkomma allvarlig skada.

Upptäckt av virus när man redan smittats kan visa sig vara en alltför sen upptäckt, om man t.ex. har dåliga rutiner för programhantering och säkerhetskopiering.

Ett virus bör naturligtvis helst upptäckas innan en fil har smittats. En effektiv detektering kan egentligen bara uppnås med hjälp av en kryptografisk kontrollsumma. Detta förutsatt att filen inte redan var smittad. Den kryptografiska kontrollsumman är beroende av varje bit i t.ex. en programfil och räknas fram på en garanterat ”ren” fil och läggs sist i filen. Varje gång programmet körs räknas summan fram på nytt och jämförs med den lagrade summan.

Ett annat sätt att undersöka om man drabbats av ett virus är att kontrollera om en fil ändrar utseende eller längd. Detta är emellertid ingen bra metod om man arbetar med program där det är fullt legalt att införa ändringar.

Många program för virusdetektering letar bl.a. efter teckensträngar från kända virus. Problemet är att dessa program inte upptäcker nya virus och eftersom gamla virus ibland modifieras upptäcks inte heller varianterna av den kända versionen. Man bör mycket noga ta reda på hur de antivirusprogram som finns fungerar och hur ofta man får uppdateringar till programmen. En del program ger varningar alltför ofta vilket gör att man till sist tröttnar och inte bryr sig när det verkligen hänt något. En del program ligger hela tiden i minnet och tar upp så mycket plats att andra program inte kan fungera effektivt.

4.8.3 Åtgärder vid smitta

Det är lätt att gripas av panik och vidta illa genomtänkta åtgärder. Erfarenheten säger att virusangrepp sällan är katastrofala. Om man hittar ett datavirus i sin dator är det viktigt att arbeta metodiskt för att återställa program- och datafiler.

Den misstänkta smittan kan ha drabbat en fristående PC, ett nät som inte är anslutet till något annat nät eller ett komplext system av nät som även har kontakter med externa nät och kanske även med stordatormiljöer.

Åtgärderna blir naturligtvis av olika stor omfattning bl.a. beroende på den miljö som drabbats och på vilket virus man drabbats av.

Den som är ytterst ansvarig för det system som smittats måste givetvis underrättas och likaså en eventuell virusexpert inom organisationen liksom den som ansvarar för informations- och IT-säkerhetsfrågor. Om man misstänker att konsekvenserna av smittan kan bli allvarliga, som t.ex. ett längre driftavbrott, bör även ledningen underrättas.

Om man inte har egen kompetens när det gäller virusbekämpning bör man omedelbart ta kontakt med extern expertis. Maskin- och/eller programvaruleverantören kanske kan 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:

- Den första åtgärden blir att så snabbt som möjligt stänga av och isolera de utrustningar som drabbats eller som man tror drabbats. Alla som berörs måste underrättas och få information om hur långt man tror att avbrottet blir.

- Det är viktigt att så snabbt som möjligt försöka fastställa när smittan har skett och vilka smittvägarna är. I det här skedet är det t.ex. viktigt att kunna fastställa när senaste programladdning skett i systemet. Har man dåliga driftuppföljningsrutiner och tillåter alltför många att lägga in program kan detta vara ett nog så tidsödande arbete.

- Visar det sig att viruset kan ha funnits länge i systemet kanske det inte finns några versioner av säkerhetskopior som är

osmittade och då måste man undersöka om det finns programvaror för att återställa smittade filer och program. För att kunna göra detta krävs att man vet vilket virus man smittats av eftersom olika åtgärder krävs för olika virus.

- All utrustning som smittats måste saneras (hårddiskar, disketter och andra lagringsmedia som varit i bruk sedan smittillfället). Det gäller att hitta alla disketter och andra lagringsmedia som använts för säkerhetskopiering och för lagring av data. Många gånger kan ett datavirus som tagits bort komma tillbaka under de närmaste veckorna. Detta beror på att någon kopia av viruset finns kvar på en diskett som undgått sanering, eller på att någon anställd har fått in det på en persondator hemma.
- Om man har programutbyte med externa intressenter och vet att program lämnats till dessa efter smittillfället måste också dessa underrättas.
- När man startar om på nytt är det viktigt att systemet varit helt avstängt. Operativsystemet finns förhoppningsvis på en garanterat smittfri uppsättning disketter och kan laddas in när systemet startas igen. Övriga program på originaldisketter kan också läsas in om man garanterat vet att de är smittfria och om man med säkerhet har identifierat det program där virussmittan fanns.
- Dokumentera alla steg i den process som genomlöps för att rensa systemet. Det kan vara värdefullt om man skulle drabbas igen att se vad som gjordes och de eventuella problem som uppstod.

4.8.4 Virusprogramvara

Virusprogramvaran bör installeras på flera ställen i IT-miljön. Virusangreppen tacklas då på en bredare och mer heltäckande basis.

Virusprogrammen kan vara av två typer aktiva virusskydd och passiva virusskydd (antingen i samma programvara eller som två olika programvaror).

Den aktiva programvaran kan startas automatiskt t.ex. vid uppstart av arbetsplatsen. Sedan ligger den minnesresident i bakgrunden och letar kontinuerligt efter virus och virusliknande aktiviteter. Den kan

även kontrollera program och datafiler innan de används. Det aktiva, residenta, virusskyddet kan även i många fall leta efter misstänkta handlingar vid öppnandet och stängandet av fil eller skrivning av fil till lagringsenhet.

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

4.8.5 Virusskydd på server och arbetsplats

På servern kan dess egna lagringsenheter sökas igenom med serverbaserade virusskydd. Sökningarna kan schemaläggas, t.ex. gör man genomsökningar bara under lågtrafikperioder. Sökningen kan ske i både programfiler och datafiler. Virusprogramvaran kan även ha funktioner för central administration och övervakning. Aktiva virusskyddsprogram medför prestandaförluster och är därför inte alltid så lämpligt i servern.

På de lokala arbetsplatserna är det bra om man har både aktiva och passiva virusskydd. För bärbara datorer kan det vara lämpligt att göra viruskontroll innan påloggning sker till det lokala nätet.

4.8.6 Brandväggsbaserade virusskydd

Yttre anslutningar mot Internet eller andra fjärrnät kan skyddas redan vid brandväggen (proxybaserad). Viruskontroll kan här ske på såväl ingående som utgående trafik:

- Kommunikation via elektronisk post och diskussionsgrupper.
- Kommunikation via Webnavigering.
- Filöverföring.

Virusskyddsprogramvaran kan förutom ovan nämnda format stödja även olika paketeringsformat och komprimeringsformat. Virusskyddsprogramvaran behöver också en databas med kända virusinstruktioner och signaturer.

5 Säker arbetsplats

I detta kapitel behandlas hur en arbetsplats, främst en arbetsplats i ett lokalt nät, kan hanteras och förses med olika skyddsåtgärder för att uppnå lämplig säkerhet. Framställningen ansluter i en del avseenden till Allterminalkonceptet vad gäller behov och krav för en säker arbetsplats.

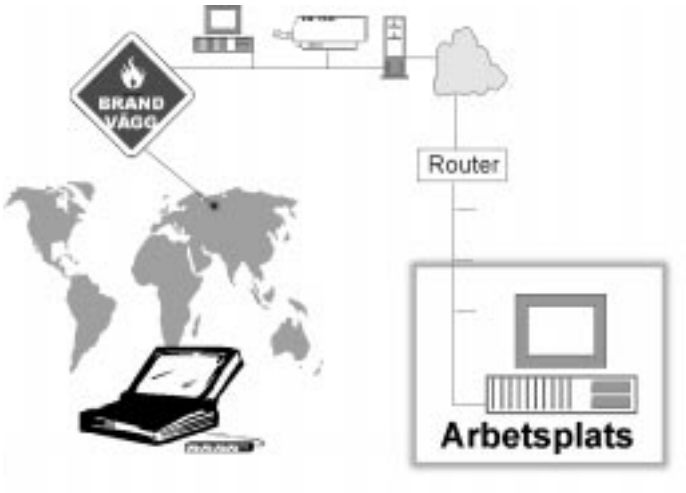
Definitionen av en *arbetsplats* finns i del 3, kapitel 3.3.1.

5.1 Utmärkande för denna miljö

En betydelsefull skillnad mellan användning av persondatorer och andra datormiljöer är att en persondatoranvändare ofta är såväl systemägare och systemansvarig som IT-ansvarig och driftansvarig. Av detta följer att personen i fråga ofta i stor utsträckning ansvarar för säkerheten i sitt persondatorsystem.

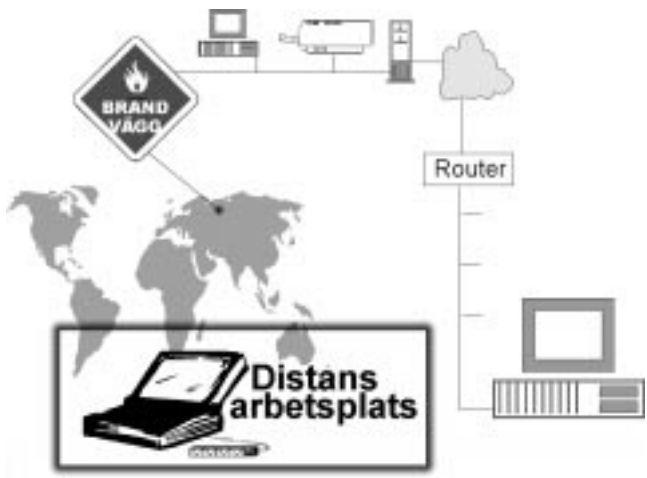
Man kan konstatera att persondatormiljöer i allmänhet har låg IT-säkerhetsnivå. På PC finns i allmänhet ingen godtagbar åtkomstkontroll av lokalt lagrad data. Flera användare måste i vissa fall dela arbetsplatsen och kan då få åtkomst till all information som lagrats lokalt. Central säkerhetskopiering av lokalt lagrad data är inte alltid möjligt och information kan således gå förlorad om detta inte hanteras lokalt. Det är också svårt att kontrollera hur användarna byter program eller dokument med andra datorer. Ett vanligt sätt att introducera virus i miljön är just när användare överför data, t.ex. via diskett, elektronisk post eller nerladdning av filer från Internet.

En persondator var, som namnet antyder, ursprungligen en dator avsedd att användas fristående av en person och för begränsade arbetsuppgifter. Idag är flera arbetsplatser hopkopplade i lokala nät. Det är inte heller ovanligt att man kopplar ihop flera sådana nät med varandra. Det är också vanligt att en arbetsplats fungerar som en terminal till en stordator. Motivet för att koppla samman arbetsplatser i nät är att ge fler användare tillgång till samma information. Ett annat är att underlätta administrationen av bl.a. säkerhetskopiering och programadministration.



Figur 15. IT-miljöer, säker enskild arbetsplats.

Rörligheten hos användarna ökar. Möjligheten att komma åt resurserna på det lokala nätet när man är på resande fot eller arbetar på distans av någon annan anledning är ett krav från många användare. Det är inte längre självklart att de arbetsplatser som ska administreras finns lokalt i huset. Samma krav som tidigare måste dock gälla vad gäller riktighet, tillgänglighet, sekretess och spårbarhet.



Figur 16. IT-miljöer, distansarbetsplats.

5.1.1 Skyddsnivåer

Nedan följer ett exempel på indelning i olika skyddsnivåer för arbetsplatssäkerheten. Denna indelning baseras dels på olika nivåer av säkerhet och dels på i vilken grad man har lyckats införa en enhetlig säkerhetsarkitektur för miljön och för den totala IT-verksamheten.

Nivå 1

På denna nivå finns ingen enhetlig skyddsnivå. Man använder de säkerhetsåtgärder som finns i produkten. En PC kan t.ex. vara utan användarautenticering och åtgärder för åtkomstkontroll, medan en UNIX arbetsstation kan vara försedd med både användarautenticering och åtkomstkontroll av filer.

Nivå 2

På denna nivå ska alla arbetsplatser tillhandahålla ett enhetligt logiskt skydd. Det genomförs genom identifiering, autenticering samt eventuellt åtkomstkontroll av resurserna.

Nivå 3

På denna nivå krävs inte bara starkt skydd av användardata och annan känslig data. Lokalt lagrade data måste skyddas genom kryptering för sekretess och riktighet. Ytterligare motåtgärder för tillgänglighet måste också finnas.

5.2 Administrativa skyddsåtgärder

Meningen med de administrativa skyddsåtgärderna är framför allt att skapa ordning i informationshanteringen. Det ska således även finnas ett regelverk för arbetsplatsanvändningen inom en organisation.

Regelverket vid användning av olika typer av arbetsplatser måste innehålla regler relaterade till vissa hot som är mer uttalade i denna miljö.

När man diskuterar hot som förekommer kring arbetsplatser kan man först konstatera, att det här, liksom i andra driftmiljöer, är vanligt med brister i regler och rutinbeskrivningar – vem får och vem ska göra vad, och hur ska det göras.

5.2.1 Organisation och ansvar

Brister i roll- och ansvarsfördelning vad gäller administration och upprätthållande av en rimlig säkerhetsnivå på arbetsplatserna kan bero på att vissa nyckelroller inte har fastställts eller att de fastställts på ett felaktigt sätt. Det är därför viktigt att:

- Säkerhetschefen med hjälp av systemadministratörer eller liknande, leder och stödjer arbetet inom IT-säkerhetsområdet för att skydda IT-resurserna, t.ex. arbetsplatserna.
- Arbetsplatserna bör ha en systemägare. I detta ansvar ingår både det generella ansvaret för underhåll och administration och ansvaret för säkerheten på arbetsplatsen. Systemadministratörer utses för att administrera och underhålla arbetsplatserna. Deras arbetsbeskrivningar ska vara väldefinierade.
- Användaren har ett egenansvar, d.v.s. han/hon är skyldig att följa de regler som gäller för användning av arbetsplatsen och dess resurser.

5.2.2 Systemadministration

Systemadministration av arbetsplatser kan vara en komplex uppgift. Faktorer som påverkar är dels hur homogen miljön är och dels i vilken utsträckning arbetsplatserna är spridda geografiskt. Användarnas olika datormognad påverkar också uppgiften. Vid framtagning av riktlinjer och rutiner för systemadministrationen bör dessa faktorer beaktas. Grundläggande för systemadministrationen är följande:

- En viktig administrativ skyddsåtgärd, som ofta glöms bort i persondatormiljöer, är att se till att man har kontroll över den utrustning och de program som finns. Dels bör man ha en förteckning över all arbetsplatsutrustning, dels bör det framgå var utrustningarna är placerade. Hänsyn måste även tas till bärbara

datorer som ofta finns på annan ort men som också ska administreras. Följande information bör finnas för varje arbetsplats vad gäller maskin- och programvarukonfiguration:

  – någon typ av identifiering
  – version
  – leverantör
  – kontaktperson, samt
  – alla modifieringar.

- Säkerhetsåtgärderna och deras implementering i arbetsplatserna ska vara dokumenterade. Alla applikationsspecifika säkerhetsåtgärder ska inkluderas.

- Säkerhetsincidenter eller brott mot säkerheten som observerats av användare, systemadministratörer eller operatörer ska rapporteras till namngiven ansvarig. Det måste också finnas rutiner för hur man ska informera berörda användare i sådana situationer.

- Regler och rutiner för hur lokal säkerhetskopiering ska gå till bör definieras, t.ex. att man vid en viss tidpunkt varje dag, eller ett visst antal gånger per vecka, samlar in disketter som framställts vid arbetsplatserna. För att sådana rutiner ska fungera tillfredsställande krävs också regler för hur disketter ska märkas samt regler för kvittens av att man lämnat ifrån sig en säkerhetskopia. Det är också vanligt att användaren själv får ansvara för eventuell lokalt lagrad information och programkod. Policyn lyder att all viktig information ska lagras centralt på gemensamma servrar, där regelbundna säkerhetskopior görs.

- Mobila användare har i större utsträckning information lagrad lokalt. Riktlinjer för hur den informationen ska säkerhetskopieras bör finnas.

- På grund av risken för att en arbetsplats ska ”smittas” av virus måste dokumenterade rutiner finnas som reglerar inläsning av nya programvaror. Rutinerna bör innehålla riktlinjer för hur och på vilken utrustning ny programvara ska testas.

- Dokumenterade rutiner bör även finnas för användningen av virusprogram lokalt på arbetsplatsen t.ex. bör det finnas riktlinjer för:

  - vilka virusprogram som ska användas, aktiva eller passiva, eller både och
  - hur ofta virusprogrammet ska köras
  - vad man ska göra om man upptäcker virus
  - hur ofta virusprogrammet ska uppdateras
  - o.s.v.

- För administration av lokala loggar bör det finnas dokumenterade rutiner hur konfiguration av loggning samt granskning av loggfiler ska gå till. Hanteringen av framtagna loggfiler ska vara dokumenterade, t.ex. vilka loggar som lagrats hur länge och hur de säkerhetskopieras.

5.2.3 Installation och konfiguration

Felaktig installation eller konfiguration kan leda till förlust av tillgänglighet, riktighet och ibland även sekretess eftersom t.ex. ett felaktigt installerat BKS kan leda till att obehöriga får möjlighet till insyn i sekretesskänslig information.

- Regler bör finnas vad gäller vem som får köpa och installera program på persondatorer.
- Alla arbetsplatser inom en organisation, inklusive mobila arbetsplatser, ska i så stor utsträckning som möjligt följa en eller ett par typkonfigurationer. Detta underlättar för användarna att dela information. Det underlättar också för systemadministratören som enklare kan avhjälpa problem och förhindra alltför långa avbrott och förlust av tillgänglighet.
- Arbetsplatserna bör versionshanteras både vad gäller maskin- och programvara så att man kan identifiera alla förändringar i systemet och backa till tidigare systemversioner d.v.s. konfigurationsadministrationen måste tillåta återställande till vilket annat skede som helst, om uppdateringar medfört brister.
- Komponenter i arbetsplatsen som är relevanta för säkerheten, t.ex. säkerhetsprogramvara och kortläsare, ska verifieras genom tester. Dels ska de testas så att de fungerar korrekt innan de används första gången och dels ska de testas kontinuerligt.

5.2.4 Säkerhetsrutiner och behörighetsadministration

Säkerhetsrutiner och behörighetsadministration på de lokala arbetsplatserna är självklart integrerad i den vanliga systemadministrationen. Nedan följer dock ett antal punkter som rör dessa områden specifikt och som är viktiga att poängtera:

- Administration av behörigheter på de lokala arbetsplatserna bör kunna ske centralt. Detta gäller även initiering och konfigurering av en eventuell loggfunktion. Central administration underlättar möjligheterna att göra snabba uppdateringar.

- Liksom vid användning av BKS i lokala nät eller liknande behöver man definiera ansvariga användare som har behörighet att göra t.ex. tillägg eller borttag av användare och uppdatering av deras rättigheter. Ansvarig ska enkelt kunna definiera nya användare och ta bort användare och uppdateringarna ska träda i kraft omedelbart.

- Administration som berör säkerhet, t.ex. konfigurering av lokala loggar eller behörigheter, får endast utföras om det föreskrivna skyddet är i drift.

- Säkerhetsrevision vad gäller arbetsplatssäkerheten ska utföras årligen för att granska att säkerheten följs.

- Rutiner för hur krypteringsnycklar ska hanteras och används lokalt bör definieras.

- Rutiner för hantering av aktiva kort eller andra typer av kort bör definieras. Detta gäller inte bara för administratören. Även användaren ska få tydliga instruktioner hur korten ska användas och hanteras.

- Om kryptografiska algoritmer används bör de godkännas av organisationens IT-säkerhetschef. Algoritmen bör uppfylla de dokumenterade riktlinjer som man definierat för en fullgod algoritm. Nycklarnas kvalitet och längd bör även de följa de definierade riktlinjerna.

- Det ska finnas rutiner som säkerställer att personer som inte längre arbetar i företaget raderas från datorsystemet. Detta krav gäller även tillfälliga användare, t.ex. konsulter och liknande.

5.3 Riktighet

Även i persondatormiljö måste kvalitetsaspekterna beaktas. Det är således viktigt att man utvärderar bl.a. färdiga programvaror innan de köps in. Både köpta och egenutvecklade programvaror bör ha indataverifiering, såsom rimlighetskontroller, konsekvenskontroller och avstämningskontroller. Användardialoger och felhanteringsrutiner bör också vara utformade så att systemet är lätt att använda och så att risken för fel minimeras.

Behörighetskontrollsystem, BKS finns för persondatorer. Med hjälp av ett sådant system kan man hindra otillåtna ändringar i system- och säkerhetsprogramvara. Information som lagras lokalt kan också skyddas från obehörig förändring genom ett BKS. Ett BKS, kan erbjuda följande vad gäller kraven på riktighet:

- För vanliga arbetsplatser kan det finnas behov av att skydda lokalt lagrad programvara från obehörig förändring. I många fall lagras inte information lokalt p.g.a. problematiken kring säkerhetskopiering. Det finns därför inte alltid behov av ett BKS för att skydda lokalt lagrad information.

- Bärbara datorer eller distansarbetsplatser generellt lagrar i större utsträckning information lokalt och där finns det därför ett större behov av ett lokalt BKS.

Både åtkomstkontroll och loggning är beroende av att man först gjort en korrekt *Identifiering och autenticering* av användarna, d.v.s. det är väsentligt att man kan garantera riktigheten i identifieringsinformationen. Metoderna för identifiering varierar. Allt från identifiering och autenticering med användaridentitet och enkla lösenord till stark autenticering med aktiva kort som dessutom kräver att säkerhetsprogramvaran identifierar sig på samma sätt, s.k. ömsesidig autenticering. Använder man enkla lösenord är det svårt att garantera riktigheten. Lösenord går att gissa, medan man med s.k. stark autenticering med aktiva kort använder nya lösenord vid varje identifiering. S.k. biometriska metoder ger också en hög nivå på säkerheten. I dagsläget saknas det dock etablerade produkter för dessa metoder. Oberoende av vilken metod man väljer för att autenticera sina användare är det viktigt att metoden är känd och går att verifiera. Användaridentiteterna bör vara unika och identifieringen och autenticeringen mot arbetsplatsen ska vara

personlig. Åtkomsträttigheterna till resurserna i arbetsplatsen bör minst baseras på någon grupptillhörighet.

Identifierings- och autenticeringsfunktionen i BKS bör innehålla funktionalitet som kan:

- kontrollera att ett eventuellt lösenord följer definierad lösenordspolicy
- spärra användaridentiteter vid definierat antal på varandra följande felaktiga inloggningsförsök
- begränsa längden på en autenticerings giltighet till definierat antal minuter av inaktiva inloggningsperioder (automatisk utloggning).

Ett *virusskydd* bör installeras på alla arbetsplatser. Aktiva och passiva virusskyddsprogramvaror kompletterar varandra och båda är därför oftast nödvändiga. Den lokala hårddisken ska regelbundet undersökas, t.ex. när man startar datorn. I vilken omfattning man väljer att köra virusskyddsprogramvaran beror på hur stor man anser risken vara att man blir smittad. Ett bra virusskydd kan erbjuda följande, vad gäller kraven på riktighet:

- skydd mot obehörig förändring av programvara
- identifiering av smittad programvara
- återställande av smittad programvara.

Kryptografiska kontrollsummor kan tillämpas på både programvara och på information. Kontrollsumman garanterar på ett säkert sätt att informationen eller programmet inte har förändrats av någon obehörig, förutsatt att inte t.ex. programmet var virussmittat redan innan kontrollsumman beräknades första gången. Algoritmen som används bör följa definierade riktlinjer för kryptografiska kontrollsummor. Vad gäller kraven på riktighet kan krypotgrafiska kontrollsummor erbjuda identifiering av obehörig förändring av information och program.

Säkerhetskopiering bör göras, t.ex. kan man backa till en icke smittad version av en programvara eller fil efter det att man med en kryptografisk kontrollsumma upptäckt att programvaran förändrats av någon obehörig. Man kan på det sättet tillgodose de krav man har på riktighet.

5.4 Tillgänglighet

Skyddsåtgärderna i persondatormiljö syftar dels till att skydda datorer och lagringsmedier, så att de inte stjäls eller upphör att fungera av andra anledningar, dels till att förhindra att obehöriga kan komma åt lagrad information och program. Båda fallen kan påverka tillgängligheten till resurserna i arbetsplatsen.

Om det är möjligt bör arbetsplatserna inom en organisation följa en eller ett par *typkonfigurationer*. Detta underlättar för användarna att dela information. Det underlättar också för systemadministratören som *enklare kan avhjälpa problem* och förhindra alltför långa avbrott och förlust av tillgänglighet. Generellt kan man också minska mängden problem genom att så långt möjligt följa antagna standarder vad gäller maskin- och programvara.

Det är viktigt att utvärdera färdiga programvaror innan de köps in. Tillgängligheten till dessa program grundar sig bl. a. på i vilken utsträckning programmen själva är robusta och användarvänliga. Programvarorna bör därför ha kontroller för indataverifiering, som t.ex. rimlighetskontroller, konsekvenskontroller, avstämningskontroller, samt dialoger som är användarvänliga och felhanteringsrutiner så att risken för fel minimeras och tillgängligheten ökar.

Många av de kända virusen arbetar så att de på olika sätt minskar tillgängligheten till delar av arbetsplatsen eller gör arbetsplatsen oanvändbar under kortare eller längre perioder. Virusskydd är därför nödvändigt.

Arbetsplatser som delas av flera användare och innehåller information som lagras lokalt på disken bör ha funktioner som styr åtkomsten till lokal information, program, systemfiler och säkerhetsprogram. Oavsiktlig eller avsiktlig radering eller förändring av t.ex. systemprogramvara kan i slutändan leda till förlust av tillgängligheten till vissa eller alla resurser på arbetsplatsen. Vanligt är att användare själva går in och gör ändringar i, t.ex. egenutvecklade program, och efter en tid fungerar inte programmen på samma sätt hos de olika användarna. Det är svårt för en systemadministratör att kunna garantera tillgänglighet i en sådan situation.

Åtkomst bör endast godkännas till de lokala resurser användaren verkligen behöver (t.ex. behöver inte de flesta användarna ha tillgång till systemfiler och liknande).

Central arkivering av organisationens programvaror säkerställer att program finns tillgängliga i händelse av någon typ systemhaveri på arbetsplatsen. ”Annan” programvara och information som lagras lokalt bör *säkerhetskopieras,* antingen lokalt eller centralt om det är möjligt.

Vid *avbrott* av olika slag i persondatormiljön måste det finnas riktlinjer för hur man ska handla så att normal tillgänglighet kan upprätthållas. Riktlinjerna bör testas regelbundet, framför allt vid större förändringar i arbetsplatsens konfiguration. Att ordna *reservdrift* för en eller flera arbetsplatser brukar inte innebära några större problem förutsatt att man har rutiner för detta samt att man kontinuerligt följer bra rutiner för hur säkerhetskopiering ska göras och hur man återskapar en säkerhetskopia. Tillgängligheten kan garanteras i hög utsträckning om man har:

- reservmaskiner (standardiserat fabrikat)
- säkerhetskopior
- rutiner för att återskapa driftmiljön.

5.5 Sekretess

Skyddsåtgärderna i persondatormiljöer syftar bl.a. till att förhindra obehöriga från att ha insyn i lagrad sekretesskänslig information. Det är inte ovanligt att sekretesskänslig information bearbetas och lagras i persondatorer. Den som är informationsansvarig bör därför fastställa behovet av skydd för sådan information.

Ett lokalt *BKS* skyddar lokalt lagrad information från obehörig insyn. Har man inget BKS lokalt bör inte heller sekretesskänslig information lagras lokalt.

Identifierings och autenticeringsinformation bör skyddas mot insyn. Sekretesskänslig information, t.ex. lösenord bör lagras krypterat på den lokala disken.

Särskilda säkerhetsåtgärder, som kan behöva vidtas vid hantering av sekretesskänslig information, är kryptering. *Kryptering* av lokalt lagrad information på arbetsplatsen skyddar mot obehörig insyn. En stulen bärbar dator som innehåller sekretesskänslig information

och som skyddas av ett BKS är inte helt säker. En obehörig användare kan läsa informationen direkt från disken. Om informationen är krypterad är den däremot inte öppen för insyn även om någon obehörig får tag i datorn. Sammanfattningsvis kan man säga att:

- saknar man ett starkt fysiskt skydd, som ofta är fallet med bärbara datorer, bör lokalt lagrad sekretesskänslig information krypteras
- för stationära datorer i fleranvändarmiljöer räcker det oftast med ett modernt BKS.

5.6 Spårbarhet

På arbetsplatsen kan man uppnå spårbarhet om man har bra identifierings och autenticeringsfunktioner samt om man har en lokal loggfunktion. Digitala signaturer kan ytterligare öka möjligheterna till spårbarhet.

Utifrån den typ av information som lagras och bearbetas i den lokala arbetsplatsen bör man definiera vilken metod som ska användas för *identifiering och autenticering* mot arbetsplatsen. Andra säkerhetsfunktioner, t.ex. spårbarhet är beroende av riktigheten i identifieringen och autenticeringen. För att uppnå spårbarhet bör varje användare ha en personlig identifiering och autenticering. Skyddsåtgärder ska finnas så att det är omöjligt att kringgå lösenordsskyddet eller andra säkerhetsfunktioner, t.ex. genom att försöka starta arbetsstationen från ett annat medium eller genom att avbryta uppstartsprocessen.

En viktig del i arbetet med att uppnå kravet på spårbarhet är att användarna själva är medvetna om att de kan hållas ansvariga för sina förehavanden när de använder organisationens databehandlingsutrustning, inte bara den egna lokala arbetsplatsen.

Spårbarheten underlättas om personal som inte är anställd (t.ex. konsulter), tilldelas användaridentiteter som är lätta att skilja från den övriga personalens.

Kraven på spårbarhet lokalt på arbetsplatsen varierar beroende på vilken information som bearbetas och lagras samt om flera använ-

dare delar på samma arbetsplats. *Loggning* är en mekanism som används för att uppnå spårbarhet. Det är viktigt att man använder det på rätt sätt och att man har bra verktyg för att t.ex. granska loggfiler eller konfigurera larmfunktioner. Loggfunktionen ingår oftast som en del i BKS. Loggfunktionen kan också vara mer eller mindre avancerad. Viktigt är dock att det finns funktioner för central loggning. Exempel på vad som kan vara väsentligt att logga i den lokala arbetsplatsen är:

- försök att bryta behörighetsreglerna
- misslyckade autenticeringsförsök
- förändringar av säkerhetskonfigurering, t.ex. tillägg av användare, tillägg av behörigheter, installation av programvara och säkerhetskopiering.

Lokalt lagrad information kan med fördel signeras med en s.k. *digital signatur* för att skaparen av informationen vid ett senare tillfälle ska kunna verifieras.

Programvaruleverantörer kan signera programvara som distribueras via öppna nät eller något annat osäkert medium. Innan installation på den lokala arbetsplatsen kan signaturen och programvaran verifieras. Detta förfarande blir allt vanligare.

5.7 Övriga frågor kring säker arbetsplats

Persondatorer kan i de flesta fall inte behandlas som separata företeelser eftersom de oftast är anslutna till ett lokalt nät och ibland även till andra typer av nät, t.ex. Internet.

Persondatorer är ett mycket effektivt verktyg för avlyssning av nät. Den kan avlyssna och analysera trafik på nätet och plocka ut t.ex. användaridentiteter och lösenord, vilket i sin tur kan möjliggöra obehörig åtkomst till information eller andra resurser.

Arbetsplatsens förmåga att överföra och hämta data via nätet ökar också säkerhetsproblematiken. Säkerheten i servrar, så som stordatorer, degenereras genom att hemlig information hämtas ut från den skyddade servern och lagras oskyddat på arbetsplatsen.

Varje arbetsplats utgör en möjlig öppning till det egna nätet men också till/från externa nät. Ett uppringbart modem anslutet till en arbetsplats innebär att det egna nätet kan kopplas ihop med omvärlden på ett okontrollerat sätt.

Även i ”säkra” nät kommer persondatorn att utgöra en risk. Trots alla säkerhetsåtgärder är det persondatorerna och deras användare som utgör de allvarligaste säkerhetsproblemen.

Säkerheten bygger ytterst på systemadministratörens kompetens och på användarens förmåga att rätt utnyttja säkerhetsmekanismerna. Attityden till säkerhet och medvetenhet om bristerna i skyddet är också viktigt. Det krävs resurser i form av tid och utbildning för att uppnå denna kompetens och detta medvetande.

6 Säkerhet i lokala nät

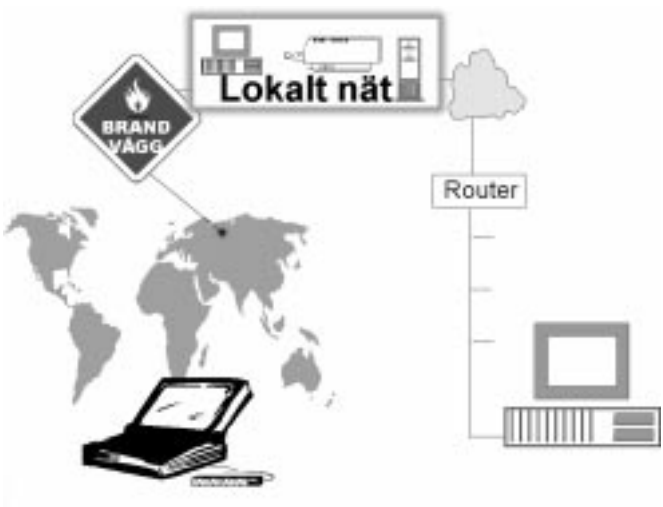
I kapitlet behandlas, från en generell utgångspunkt, vilka åtgärder som är nödvändiga för att säkerställa olika skyddsnivåer i ett lokalt nät. Det bör ses i sitt sammanhang, med bl.a. Säker arbetsplats och andra kapitel i handboken, för att ge en heltäckande bild av området.

Definition av ett *lokalt nät* finns i del 3, kapitel 3.3.2.

6.1 Utmärkande för denna miljö

Huvudsyftet med att koppla samman persondatorer och arbetsstationer i ett lokalt nät är i allmänhet att ge fler personer tillgång till samma information och resurser och att skapa enklare eller säkrare driftrutiner.

Kopplar man samman flera arbetsplatser i ett nät är det naturligt att säkerhetsproblemen och behovet av skyddsåtgärder ökar. Fler människor och större mängd information kan beröras av ett eventuellt fel. Sammankopplingen i sig kan skapa både sekretessproblem och andra problem.



Figur 17. IT-miljöer, lokalt nät.

Lokala nät är decentraliserade till sin natur, vilket gör administrativa åtgärder svårare. Samtidigt som nätet är flexibelt och öppet medför fördelarna att det blir mer sårbart, vilket motiverar ett förebyggande säkerhetstänkande.

Ett lokalt nät kännetecknas tekniskt sett av dess topologi samt det eller de kommunikationsprotokoll som används.

6.1.1 Skyddsnivåer

Nedan finns ett exempel på indelning i olika skyddsnivåer för ett lokalt nät. Denna indelning baseras dels på olika nivåer av säkerhet och dels på i vilken grad man har lyckats införa en enhetlig säkerhetsarkitektur för miljön och för den totala IT-verksamheten.

Nivå 1

På denna nivå saknas en enhetlig skyddsnivå. Man använder endast de säkerhetsåtgärder som redan finns i programvaran. Dock är det troligt att servrar har ett antal säkerhetsåtgärder och de kan därför vara på en högre säkerhetsnivå än arbetsplatserna.

Nivå 2

Här ska alla nätapplikationer och servrar ha en enhetligt skydd. Det sker genom identifiering och autenticering, spårbarhet och åtkomstkontroll hos resurserna.

Användarna har personliga användaridentiteter.

Nivå 3

På denna nivå krävs ett starkt skalskydd, d.v.s. identifiering och autenticering ska baseras på starkare mekanismer än enkla lösenord.

Nivå 4

Varje meddelande som överförs förses med ett starkt skydd. Andra komponenter som nätapplikationerna behöver, t.ex. nätoperativsystemet, arbetsplatser och servrar ska också tillhandahålla samma säkerhetsnivå.

6.2 Administrativa skyddsåtgärder

I fleranvändarmiljöer, som lokala nät, uppstår en speciell problematik eftersom det dels medför ett antal fördelar eftersom flera användare kan dela på samma resurser och dels en komplexare användarhantering. Det gäller därför att göra en bra avvägning utifrån de krav på tillgänglighet och säkerhet som inblandade intressenter ställer.

6.2.1 Organisation och ansvar

Namngivna nätadministratörer ska utses för administration och underhåll av nätet. Dessa personer har ansvar för att konfigurera servrar, routrar och namnservrar och ska arbeta tillsammans med säkerhetspersonal för att upprätthålla säkerheten i nätet. Dessutom bör åtminstone en ersättare namnges, som har tillräckliga kunskaper för att vid behov kunna träda in i stället för den ordinarie.

Säkerhet och tillgänglighet hos tjänsterna är beroende av ett korrekt underhåll av det lokala nätet, servrar och ansluten utrustning. Det är därför viktigt att ansvarsfördelningen är tydlig mellan systemadministratörer, nätadministratörer och säkerhetspersonal.

6.2.2 Systemadministration

Allmänt

- Till de nödvändiga administrativa åtgärderna hör att upprätta *dokumentation* över det lokala nätet och dess ingående komponenter samt att hålla den aktuell. Den bör innehålla hur nätet är uppbyggt och vad det innehåller, samt ansvarig för respektive del. Även driftrutiner och de regler och rutiner som gäller i säkerhetsarbetet ska vara beskrivna.

Inköp, installation och konfigurering

- Rutiner för inköp och installation av program är särskilt viktiga i nätmiljöer. I dessa bör ingen annan än den som är nätansvarig ha rätt att installera nya program. Detta är av stor betydelse om persondatornätet är kopplat till servrar eller stordatorer. Risken

för att t.ex. datavirus överförs till andra miljöer i det lokala nätet är överhängande, om en arbetsplats har blivit ”smittad” via en programskiva.

- Innan ett nät konstrueras och installeras, ska krav och förslag till konstruktion noggrant dokumenteras. Denna dokumentation kan användas för att kontrollera att säkerhetskraven mäts och senare kontrollera den faktiska implementeringen.

- Dokumenterade procedurer för nätinstallationer ska finnas. Detta krävs för installation av nya nät och ny utrustning som ansluts till nätet. Kravet gäller tilldelning av nya adresser, omkonfigurering av nodlistor, tilldelning och installation av nya nät och routrar för anslutning, o.s.v.

- Endast korrekt tilldelade nätadresser och namnrymder får användas när nät installeras. Tilldelning av nätadresser ska administreras centralt. Felaktig tilldelning av nätadresser kan förhindra anslutning till andra nät.

- Alla nätadresser ska dokumenteras och får endast utdelas av nätadministratören, eftersom adresserna ska vara väldefinierade och inte motstridiga.

- Nätets korrekta konfigurering ska verifieras regelbundet. Verifiering ska bygga på konstruktionsdokumenten och klassificering av domän.

Administration av behörighetskontroller

- Ett tänkbart skydd mot användning av program, som inte godkänts av den nätansvarige, är att persondatorerna i nätet inte förses med diskettenheter. Helst bör i så fall endast den ”huvudmaskin”, som bara får användas av nätadministratören, vara försedd med läsmöjlighet för diskett.

- Om sekretessbelagd information ska kunna lagras på ett minne, som är gemensamt för flera användare, måste givetvis ett väl fungerande BKS finnas.

- Särskilda rutiner måste också finnas för tilldelning och registrering av behörigheter. Det är viktigt att de verksamhetsansvariga har kännedom om vilka funktioner som finns för behörighets-

kontroll i nätets operativsystem eller i applikationen, så att de kan avgöra hur behörighetstilldelningen ska gå till.

- Dokumentation, som detaljerat beskriver ett lokalt nät (t.ex. tilldelade adresser, namnrymd, konfigurering av routrar och liknande information) ska behandlas som hemlig information och skyddas i enlighet med detta.

- Regler kan också behöva utformas för hur utdata, som produceras på gemensamma skrivare, ska tas om hand och distribueras. Särskilda rutiner kan behöva tillgripas för sekretesskänsliga uppgifter.

Avbrottsplanering

- Eftersom det i persondatornät är vanligt att flera användare delar på vissa resurser, t.ex. skivminne och skrivare, är det viktigt att man bevakar belastningen på dessa resurser, så att onödiga störningar i verksamheten undviks.

- Definierade rutiner för planerade avbrott är viktigt för att minimera effekterna av att de gemensamma resurserna inte är tillgängliga p.g.a. installationer, uppgraderingar och service.

- Rutiner för central *säkerhetskopiering* bör definieras. För gemensamma resurser i form av programvara samt gemensam information, måste en ansvarig utses att vid vissa tidsintervall på lämpligt lagringsmedium framställa säkerhetskopior, så att man vid behov kan återskapa den gemensamma lokala miljön.

- Om enskilda användare har egna ”bibliotek” som lagras på ett gemensamt skivminne, och själva ska ansvara för reservkopiering, är det viktigt att man har fastställt också regler för hur och när detta ska ske.

- Nätets användning och prestanda ska bevakas och analyseras, så att användningen är känd och lämplig prestanda i nätet kan tillhandahållas.

- Nätens prestanda och säkerhet ska testas regelbundet. Det är speciellt viktigt för nätförbindelser mellan olika organisationer. Testerna ska godkännas av ägaren till IT-resurserna och övervakas av säkerhetsorganisationen.

Loggning

- Rutiner för hur, när och av vem loggning ska göras bör definieras. Rutiner måste även finnas för granskning av loggar samt uppföljning av säkerhetsrelevanta händelser. Det finns i huvudsak två typer av händelser som är av intresse att logga:
  - Normal aktivitet, d.v.s. hur det lokala nätet fungerar, eventuella fel som uppstår, driftstopp i nätet etc.
  - Otillåten aktivitet, t.ex. felaktiga inloggningsförsök, otillbörlig åtkomst av gemensamma resurser såsom filer och servrar.

6.3 Riktighet

Ett lokalt nät och dess ingående komponenter bildar en komplex sammansättning av maskin- och programvara. Kraven på riktighet måste tillämpas på olika nivåer i det lokala nätet. Exempelvis måste riktigheten i nätoperativsystemet bevaras samtidigt som informationen mellan en klient och en server i en nätapplikation också måste skyddas mot obehörig förändring. Kommunikationsprotokollen är i allmänhet robusta vad gäller s.k. överföringsfel. Om data går förlorad innebär det oftast förlust av hela nätet, snarare än förlust av enskilda data.

Servrar och nät

- Alla användare ska vara identifierade.
- Riktigheten i nätet bör skyddas genom begränsad åtkomst och lösenordsskydd av routingtabeller och annan riktighetskänslig information.
- Åtkomst och administration av nätkomponenter (t.ex. routrar) i nätet är endast tillåtet inom säkerhetsdomänen. Ingen fjärradministration är tillåten, såvida inte stark autenticering kan användas.
- Om man önskar uppnå en hög nivå på säkerheten bör åtkomst och administration av nätkomponenter (t.ex. routrar) i nätet endast tillåtas om kommunikationen är sekretesskyddad och skyddad mot manipulering.

Riktigheten måste även kontrolleras genom att införa funktioner för upptäckt av obehörig förändring:

- *Digitala signaturer* kan användas för att verifiera att programvara är korrekt eller att en fil eller ett meddelande inte har ändrats av obehörig sedan signaturen applicerades.
- *Kryptografiska kontrollsummor* kan tillämpas på både programvara och information. Kontrollsumman garanterar att informationen eller programmet inte har förändrats av någon obehörig, förutsatt att inte programmet var virussmittat redan innan kontrollsumman beräknades. Kontrollsummor kan tillämpas på mycket riktighetsskänslig information och program. Algoritmen som används bör följa definierade riktlinjer för kryptografiska kontrollsummor.
- *Återskapa integritet* är mekanismer och rutiner vid upptäckt av förändring, för att återskapa systemets integritet, d.v.s. återställa det till senast kända riktiga tidpunkt.
- *Virusskydd* som med jämna mellanrum genomsöker gemensamma resurser för att säkerställa att filer eller programvara inte är smittade.

Olika funktioner kan införas för att övervaka riktigheten av driften, d.v.s. nätets funktionalitet:

- *Larm* kan med fördel installeras i systemet. Det finns olika programvaror som genomsöker nätet för att upptäcka misstänkta aktiviteter och varnar övervakningssystemet.
- *Inventory management* utnyttjar program som kan användas för att spåra och kontrollera all maskin- och programvara i systemet. Detta kan fungera som ett komplement till administrativa rutiner för att veta vad som egentligen finns, och var det finns.

Nätapplikationer

- Om identifierings- och autenticeringsåtgärder finns ska de användas. Varje användare ska ha en personlig identifiering och autenticering.
- Det är inte nödvändigt att upprepa autenticering av användare, vid användning av nätapplikationer, om autenticeringen ägt

rum vid arbetsplatsen. Nätapplikationen kan få information om användaridentiteter genom data från klientapplikationen eller genom att identifiera nätadressen.

- Vid krav på hög säkerhet bör upprepad autenticering äga rum vid servern, inte enbart vid arbetsplatsen så fort en nätapplikation används.
- Vid krav på hög säkerhet bör ömsesidig autenticering verifiera identitet och behörighet hos både klient och server.
- Vid krav på extra hög säkerhet bör autenticering äga rum vid varje begäran eller varje utbyte av meddelanden i nätapplikationen. Autenticeringen kan vara en del av protokollet eller också en del av det faktiska meddelandet (t.ex. genom digitala signaturer).
- Vid krav på hög säkerhet bör inte känslig information laddas ner eller föras ut från miljön där den lagras.
- Endast behöriga, identifierade användare ska kunna nå åtkomst av nätapplikationen d.v.s. det ska vara omöjligt att kringgå åtkomstkontrollen i nätapplikationen om man har lokal åtkomst av data och resurser.
- Vid krav på hög säkerhet bör all information som mottagits och laddats ner från en nätapplikation skyddas så att den endast kan nås av behöriga, identifierade användare. Skyddet kan vara en del av eller en egenskap i meddelandet, via t.ex. kryptering.
- Vid krav på hög säkerhet bör åtkomstkontrollen tillhandahålla en större detaljeringsgrad till resurserna hos nätapplikationen än till applikationen i sin helhet. Vissa användare kan få åtkomst av vissa data, medan andra användare kan ha andra åtkomsträttigheter.

6.4 Tillgänglighet

Kraven på tillgänglighet bör uppfyllas genom en kombination av åtgärder som både kompletterar och överlappar varandra. Tillgängligheten till resurser i det lokala nätet måste baseras på skyddande, rapporterande och återställande åtgärder.

Servrar, nät, nätapplikationer och annan kringutrustning

BKS är en skyddande åtgärd som minskar riskerna vad gäller obehörig användning av resurser i det lokala nätet. Rimlighetskontroller i programvaran kan också fungera som en skyddande åtgärd. Dessa två åtgärder kan skydda mot eller minska konsekvenserna då obehöriga eller behöriga användare, medvetet eller omedvetet tar i anspråk resurser av olika eller samma slag så att kraven på tillgängligheten från behöriga inte kan uppfyllas.

God tillgänglighet kräver en väl genomförd nätstrategi, nätkomponenter baserade på bra produkter, installerade och konfigurerade av kompetent personal. En förutsättning för att hålla hög tillgänglighet är att nätet går att övervaka via någon form av utrustning. Utrustningen ska ha funktioner som möjliggör bevakning och administration av nätkomponenter via nätet. Önskvärda funktioner är:

- grafisk presentation av nätkomponenter
- larm när komponenter eller förbindelser slutar att fungera
- möjlighet att i detalj kontrollera och anpassa nätkomponenter via nätet
- övervaka trafikvolymen
- larma när nya okända komponenter kopplas in i nätet.

Vid *avbrott* av olika slag i lokala nät måste det finnas riktlinjer för hur man ska handla så att normal tillgänglighet kan upprätthållas. Riktlinjerna bör testas regelbundet, framför allt vid större förändringar i nätets konfiguration. Att ordna *reservdrift* för gemensamma resurser bör inte vara något större problem förutsatt att man har extra resurser fria, följer bra rutiner för hur säkerhetskopiering ska göras och hur man återskapar en säkerhetskopia. Tillgängligheten kan garanteras i hög utsträckning om man har:

- reservmaskiner (standardiserade fabrikat)
- säkerhetskopior
- rutiner för återskapande av driftmiljön och nätet.

6.5 Sekretess

När ett antal resurser ska delas mellan flera användare måste dessa resurser skyddas så att de endast är tillgängliga för behöriga användare. Skydden som ska uppfylla kraven på sekretess är dels av typen skyddande d.v.s. man vill förhindra åtkomst till resurserna och dels vill man göra resurserna oanvändbara för obehöriga.

Servrar

- Servrar bör skyddas genom ett BKS antingen i operativsystemet eller att användaren endast får tillgång till servern via en nätapplikation. Normalt tillhör användaren en grupp som åtnjuter olika rättigheter. Efter autenticering kan användare utföra transaktioner enligt gruppens rättigheter.
- På en server finns det ofta en mängd olika resurser, t.ex. databaser och applikationer, som också ofta använder samma information. Det är viktigt att man vid installation är medveten om att informationen måste skyddas mot att obehöriga kan härleda information ur annan information genom att använda olika resurser för att komma åt information. En analys av något slag bör genomföras så att man kan identifiera möjliga härledningar som kan leda till slutledning av känslig information.

Nätet

- Alla användare ska vara identifierade och ha unika användaridentiteter.
- Åtkomstkontroll ska bygga på säkerhetsdomäner. Detta kräver att domäner identifieras.
- Vid anslutning till andra domäner, kan åtkomstkontrollen baseras på adresser och protokoll, d.v.s. begränsas till router-filtrering.
- Vid krav på hög säkerhet bör all utrustning klassificeras enligt en definierad metod för att få anslutas till nätet.
- För alla förbindelser med andra domäner bör det finnas riktlinjer för vad som är tillåtet och inte. Riktlinjerna ska innehålla information om möjliga trafikriktningar, protokolltyper och tjänster.

De kan också innehålla information om storlek och innehåll i meddelandena som får överföras.

- Routingtabeller och annan känslig information ska skyddas mot obehörig insyn och förändring genom begränsad åtkomst och lösenordsskydd.

- Vid krav på hög säkerhet bör man skydda sig mot trafikanalys på nätnivå genom generering av brus eller liknande.

- Routingkontroll är mekanismer som säkerställer att data endast transporteras över rätt nät, subnät, länkar eller system med rätt attribut. En hub kan fungera som ett filter genom att sortera bort paket från vissa avsändare eller till vissa mottagare. Bryggor kan kontrollera att sändare och mottagare tillhör samma grupp och först därefter släppa igenom paket. Med terminalserver lägger man på en extra länk mellan persondator och nätet.

Nätapplikationer

- Om identifierings- och autenticeringsåtgärder finns ska de användas. Varje användare ska ha en personlig identifiering och autenticering. Det finns emellertid inga 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. Se vidare avsnittet om Riktighet ovan.

- Om hög säkerhet krävs bör alla meddelanden mellan klient och server skyddas med kryptering.

- Autenticeringsinformation som är en del av klient/server-autenticeringen bör skyddas från att avslöjas för att undvika återuppspelningsattacker av autenticeringen.

Annan kringutrustning

Speciell utrustning eller speciellt placerad utrustning bör användas vid t.ex. utskrift av sekretesskänslig information.

6.6 Spårbarhet

Loggning är den klassiska skyddsåtgärden för att uppfylla kraven på spårbarhet. Loggfunktionerna kan finnas i operativsystemet eller i en nätapplikation. Viktigt är att man har verktyg som kan sammanställa logginformation från flera olika system så att det lokala nätet kan analyseras dels i olika system men också som en helhet.

Nät, servrar, nätapplikationer och annan kringutrustning

- Vid krav på hög säkerhet bör identiteten hos både klienten och servern verifieras genom hela kommunikationskedjan. Identiteten kan antingen tillhöra den person som initierade överföringen eller applikationen som utför överföringen.
- Vid krav på hög säkerhet bör det finnas funktioner (t.ex. digitala signaturer) som med mycket hög pålitlighet verifierar att avsändaren faktiskt sänt den mottagna informationen.
- Vid krav på hög säkerhet bör det finnas funktioner (t.ex. kvitton baserade på asymmetrisk kryptering) som med mycket hög pålitlighet verifierar att mottagaren faktiskt mottagit den sända informationen.
- Överförda eller mottagna signerade meddelanden ska registreras i applikationsloggen.
- Loggning och uppföljning av säkerhetsrelevanta händelser måste finnas. Det ska vara möjligt att välja vilka händelser som ska följas upp.

Följande händelser bör loggas:

- Alla förbindelser (t.ex. förbindelser som kommer genom gateways och brandvägg) som kommer utifrån in i nätet.
- Alla identifierings- och autenticeringsperioder i nätet.
- Alla försök att få åtkomst till en nätapplikation ska loggas. Detta krav gäller både lyckade och misslyckade försök att nå applikationen.

- Användning av en resurs på hög nivå (t.ex. ett anrop), men inte hela innehållet i trafiken.
- Följande information om åtkomst av en nätapplikation ska loggas:
  - användaridentitet (om möjligt)
  - nätadressens källa och destination
  - datum och tid för händelsen
  - protokoll och tjänst som använts
  - all information om typen av anrop och mängden överförd data (storlek i bytes, antal paket, o.s.v.).
- Vid krav på hög säkerhet bör alla åtkomster av nätapplikationer följas upp vid servern.

6.7 Övriga frågor kring lokala nät

Det är en vanlig företeelse att det råder brist på kompatibilitet mellan datorer och mellan programvaror till datorer. Vid försök att låta olika slag av datorer samverka i ett system uppstår det därför ofta problem, som kan påverka säkerheten. Generellt kan man minska denna typ av problem genom att så långt möjligt följa vedertagna standarder.

Sammankoppling av datorer kräver kommunikationslinjer, och ofta även andra slag av särskild utrustning. Det blir allt vanligare att man kopplar samman lokala nät över publika nät. Två brandväggar, oftast av samma märke eftersom brandväggsleverantörerna inte använder samma protokoll för denna typ av trafik, i varsin ända av ett publikt nät kan kommunicera krypterat och riktighetskontrollerat. Vid uppkoppling sker dessutom en ömsesidig autenticering mellan de kommunicerande brandväggarna. Ett eller flera s.k. VPN (Virtual Private Network) kan på detta sätt byggas upp för geografiskt spridda organisationer.

Brandväggar används i allt större utsträckning för att separera olika säkerhetsdomäner inom ett lokalt nät eller inom en organisation, alltså inte bara vid fjärranslutningar.

Ett stort säkerhetsproblem i lokala nät är att man ofta arbetar med olika miljöer (stordatorer, NT-servrar, UNIX-servrar o.s.v.) och olika applikationer som alla kräver någon form av identifiering och autenticering. Användarna måste hålla reda på ett antal olika lösenord och detta leder till att lösenorden ofta skrivs ner på pappers-lappar i anslutning till arbetsplatsen, eller så använder man samma eller enkla lösenord för alla system. Autenticeringservrar kan vara lösningen på detta problem. Idag finns det ett antal olika koncept på marknaden. Koncepten bygger på att en central autenticerings-server (en per säkerhetsdomän) hanterar den initiala autenticeringen av alla användare. Vid uppkoppling mot en annan server eller liknande hanteras denna autenticering av autenticeringsservern, helt transparent för användaren. Konceptet kallas single-sign-on, d.v.s. användaren loggar endast in en gång. Kerberos från MIT är ett exempel på ett sådant koncept.

7 Säkerhet i fjärrnät

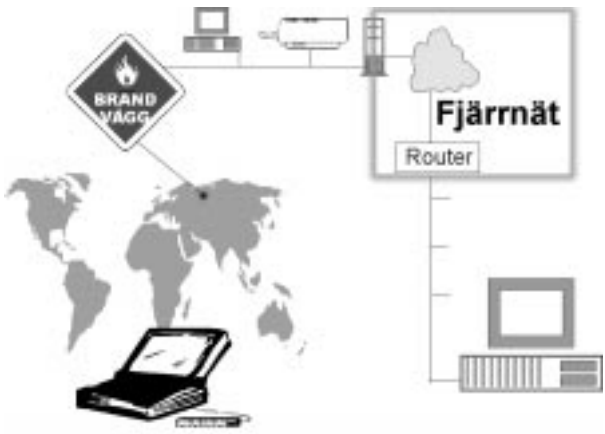
I kapitlet behandlas säkerhetsfrågor specifikt kring fjärrnätproblematiken. Speciell tonvikt ligger på olika former av uppringda fjärrnät eller fjärrnätförbindelser. Dessa är ur säkerhetssynpunkt speciellt viktiga att fokusera.

Definition av ett *fjärrnät* finns i del 3, kapitel 3.3.3.

7.1 Utmärkande för denna miljö

Fjärrnät innebär datakommunikation över fjärrförbindelser som är fasta eller uppringda. Utvecklingen inom fjärrkommunikation går från att tidigare varit baserad på analoga modemförbindelser, till digitala fjärrnättjänster. Modemförbindelsen kan bestå i att en operatör tillhandahåller ledningar för analog överföring, där kunden själv ansvarar för allt utom själva ledningen. I det senare fallet erbjuder leverantören en nättjänst med önskade förutsättningar. Det kan t.ex. vara Ethernet- eller ATM-gränssnitt avsett för TCP/IP med en överföringshastighet på minst 512 Kbps, tillgänglighet på 97 % samt att övervakning ingår.

Efter avregleringen av telemonopolet har flera nya leverantörer av nättjänster framträtt på marknaden utöver Telia. Några av dem är



Figur 18. IT-miljöer, fjärrnät.

teleoperatörer såsom Tele2, Global One, Telenordia, andra är leverantörer av olika IT-tjänster/produkter, t.ex. WM-data, IBM och Cap Gemini.

Statskontoret (och det tidigare Stattel) har genomfört centrala upphandlingar av nättjänster som statliga och kommunala myndigheter kan utnyttja utan att var och en ska behöva upphandla på egen hand.

7.1.1 Skyddsnivåer

Nedan följer ett exempel på en tänkbar indelning i olika skyddsnivåer för fjärrnät. Denna indelning baseras dels på olika nivåer av säkerhet och dels på i vilken grad man har lyckats införa en enhetlig säkerhetsarkitektur för miljön.

Nivå 1

Användning och förekomst av fjärrförbindelser ska dokumenteras. Grundläggande skalskydd behövs vid anslutning till publika nät t.ex. autenticering baserad på nätadresser eller enkla lösenord. Endast begränsat skydd behövs vid anslutning av lokala nät inom samma organisation. Om fjärrförbindelsen inte är fast krävs autenticering när förbindelse upprättas.

Nivå 2

En fjärrförbindelse ska erbjuda starkt skalskydd. Skydd mot obehörigt initierad förbindelse genom loggning och uppföljning av förbindelsens användning, användare, uppkopplingstid, o.s.v. När förbindelse upprättas krävs stark autenticering för det lokala nätet eller användaren som ansluts.

Nivå 3

Fjärrförbindelsen ska betraktas som en integrerad del av det interna systemet eller nätet. Detta kräver ett starkt skalskydd och skydd av data. Utrustningen på båda sidor måste samverka för att tillhandahålla det integrerade skydd som behövs.

Nivå 4

Fjärrförbindelser är inte tillåtna.

7.2 Administrativa skyddsåtgärder

En rad åtgärder av administrativ natur är grundläggande för att IT-säkerhet, inklusive säkerhet vid datakommunikation, ska kunna skapas och upprätthållas.

7.2.1 Strategisk planering

Datakommunikation bör alltid byggas upp på grundval av en **långsiktig planering,** d.v.s. en strategi, som ingår som en integrerad del av den allmänna IT-strategin, och som godkänts och fastställts av ledningen.

Till de frågor som ska besvaras för att man ska kunna göra en långsiktig planering av datakommunikationen inklusive säkerhetsfrågor, hör exempelvis:

- Vilken information finns det behov av att överföra?
- Vilka är kraven på överföringen (volymer, snabbhet, säkerhet, ekonomi)?
- Vilka alternativa sätt att överföra informationen finns?
- Hur uppfyller de olika alternativen de ställda kraven?
- Vilka existerande standarder för datakommunikation ska följas?
- I vilken mån ska det vara tillåtet att i kommunikationsnätet koppla samman datorer av olika typer?
- Vilka är riskerna för störningar i det valda alternativet?
- Vilka typer av preventiva eller korrigerande åtgärder ska man vidta för att möta störningar?
- Vad kostar ett kortare respektive längre avbrott i kommunikationen?
- Vilka andra konsekvenser får ett avbrott?
- Vilka är riskerna för att obehöriga kommer över information och vilka konsekvenser kan det få?
- Hur länge kan man bedriva olika delar av verksamheten vid avbrott?

En strategisk planering av datakommunikationen måste bygga på en klar uppfattning om betydelsen av den information som ska överföras. Den kan därför behöva föregås av en **säkerhetsanalys** och en **klassificering av informationen,** på motsvarande sätt som gäller för annan information i IT-systemet.

7.2.2 Organisation och ansvar

Med IT-säkerhetspolicyn sammanhänger också att det fastställs en intern **organisation och ansvarsfördelning** i säkerhetsfrågor. Därvid måste ansvaret för säkerheten vid datakommunikation inbegripas. Det kan vara nödvändigt att utse en särskild kommunikationsansvarig, som också har ansvar för de särskilda säkerhetsfrågor som uppstår som en följd av kommunikationen. För stora nät kan det behövas en hel driftorganisation. Det är nödvändigt att klargöra gränserna mellan kommunikationsansvarig, verksamhetsansvarig, särskilt utsedd säkerhetsansvarig, driftansvarig, nätadministratör o.s.v.

En annan viktig åtgärd är att **utbilda och informera** personalen om de säkerhetsregler som gäller och motiven för dem. Alla måste göras medvetna om det egenansvar för IT-säkerheten som var och en har. Utbildning, information och ledningens allmänna attityd, uttryckt i policy och på andra sätt, är motivationshöjande åtgärder som utgör ett viktigt förebyggande skydd mot bl.a. slarv och felhantering som hör till de mer frekventa hoten även vid kommunikation.

Viktiga hållpunkter vid upprättande och användning av fjärrförbindelser av olika slag är att:

- Fjärrförbindelse ska endast upprättas om det finns ett definierat behov av detta. Behoven ska identifieras och dokumenteras t.ex. användning, kommunikationsriktning, protokoll, samt applikation som använder protokollen.
- Ska två lokala nät kopplas samman bör en säkerhetsrevision genomföras för att kontrollera att det inte förekommer säkerhetsbriser på något håll.
- Fjärrförbindelser bör om möjligt begränsas till en anslutningspunkt. Flera anslutningspunkter minskar möjligheterna att upprätthålla ett enhetligt skydd.

- Dokumentation, som beskriver fjärrförbindelserna i detalj, t.ex. abonnentnummer och annan känslig information, ska behandlas som sekretesskänslig information.
- Man bör kontrollera att användare inte själva installerar modem eller annan fjärrförbindelseutrustning till sina arbetsplatser.
- Avtal ska skrivas med företaget som tillhandahåller fjärrförbindelsen. Avtalen ska fastställa kraven på säkerhetsnivå, tjänstens tillgänglighet, krav på logiskt skydd, t.ex. kryptering och slutna användargrupper.
- Dokumentation vad gäller användare som använder fjärrförbindelsen, ska finnas. Om olika tjänster eller funktioner erbjuds ska listan också innehålla en specifikation över vilka tjänster som erbjuds varje användare.
- Rutiner för hantering av loggar som rör fjärrförbindelserna ska finnas.
- En aktuell lista över anslutna modem och möjliga vägar att ringa in ska finnas. Listan ska för varje förbindelse innehålla:
  - telefonnummer
  - vart uppringningsutrustningen anslutits, maskinnamn, o.s.v.
  - typ av ansluten utrustning (modemtyp, o.s.v.) och referens till teknisk beskrivning av säkerhetsmekanismernas faktiska konfigurering. Detta omfattar vilken sorts förbindelse som kan upprättas, samtalsriktning, protokoll, etc.
- Man bör med jämna mellanrum byta ut telefonnumret till en uppringd förbindelse.
- Fjärrförbindelserna ska verifieras kontinuerligt. Verifieringen ska genomföras enligt en fördefinierad mall.
- Till de nödvändiga administrativa åtgärderna hör också att upprätta **dokumentation** över kommunikationssystemets ingående komponenter och att hålla den aktuell. Systemet bör beskrivas både på en övergripande nivå samt så detaljerat som är motiverat med hänsyn till olika behov. Utom driftrutiner ska de regler och rutiner som gäller i säkerhetsarbetet vara beskrivna. Dokumentation kan lämpligen utformas som en handbok som i tillämpliga delar ges ut till alla användare.

7.3 Riktighet

7.3.1 BKS

Användare som ansluter sig från externa förbindelser ska autenticeras innan någon åtkomst till IT-resurserna är möjlig. Användaridentiteterna bör vara unika och lösenord eller dylikt personligt valt. Vill man öka säkerheten bör autenticeringen bygga på starkare mekanismer t.ex. stark autenticering med aktiva kort.

Vid sammankoppling av lokala nät via uppringda förbindelser bör man använda någon typ av autenticeringsmekanism mellan näten. Exempel på en sådan mekanism är CHAP (Challenge Handshake Protocol) i PPP (Point to Point Protocol). Båda parter bör autenticera sig mot varandra, s.k. ömsesidig autenticering.

7.3.2 Kryptografisk kontrollsumma

Kryptografiska kontrollsummor är en teknik som bidrar till att kontrollera att det inte förekommer någon manipulation av överförd information. Den utgör ett bra skydd när någon exempelvis vill försäkra sig om att ekonomiska transaktioner inte utsätts för påverkan.

7.4 Tillgänglighet

7.4.1 Nätövervakning

God tillgänglighet kräver en väl genomförd nätstrategi, nätkomponenter baserade på bra produkter, installerade och konfigurerade av kompetent personal.
En förutsättning för att hålla hög tillgänglighet är att nätet går att övervaka via någon form av utrustning. Utrustningen för nätövervakning ska ha funktioner som möjliggör bevakning och administration av nätkomponenter via nätet. Önskvärda funktioner är:

- grafisk presentation av nätkomponenter
- larm när komponenter eller förbindelser slutar att fungera
- möjlighet att kontrollera och anpassa nätkomponenter via nätet

- övervaka trafikvolymen
- larma när nya okända komponenter kopplas in i nätet
- loggnings- och spårningsfunktioner.

7.4.2 Avbrottsplanering

Den som använder sig av datakommunikation måste också ha en **avbrottsplanering.** Risken för kortare eller längre avbrott till följd av ledningsbrott eller andra typer av störningar i kommunikationen är stor. Också risker för överbelastning av linjer, programfel etc. måste beaktas. Man måste utreda, besluta och dokumentera vad som ska göras vid avbrott av kortare eller längre varaktighet. Reservrutiner måste utformas och testas.

Utvecklingen av ett nät för datakommunikation måste vara en integrerad del av systemutvecklingen i allmänhet. En generell, grundläggande säkerhetsåtgärd kan vara att nätet får en utformning, en arkitektur, som är genomtänkt. En **god nätarkitektur** löser visserligen i sig inte säkerhetsproblemen men kan förenkla dem. I det sammanhanget finns det anledning att vara särskilt vaksam inför de komplikationer som kan uppstå när man med kommunikationslinjer vill knyta samman olika slag av utrustningar.

Uppföljning och omprövning av valda lösningar måste göras fortlöpande.

7.4.3 Skydd av kopplingspunkter

Dataöverföring över telelinje berör ofta både IT-systemägares och en särskild telenätägares ansvarsområden. Det fysiska gränssnittet mellan ansvarsområdena markeras kanske av ett kopplingsskåp eller liknande utrustning. Sådana kopplingspunkter är sårbara för bl.a. fysisk åverkan och avlyssning.

Det förhållandet att utrustningen befinner sig i gränszonen mellan ansvarsområden kan leda till att det uppstår oklarheter eller missförstånd om vem som ska upprätta erforderligt skydd för utrustningen. Det är därför angeläget att ta med dessa kopplingspunkter på den checklista, som man tillämpar i säkerhetsarbetet.

7.5 Sekretess

7.5.1 BKS

Den mest grundläggande tekniska åtgärden för att skydda sig mot att obehöriga personer, externa eller interna, kommer över information är att använda ett **system för behörighetskontroll (BKS).** Den starkt ökade användningen av datakommunikation har emellertid i hög grad ökat risken för intrång och därmed också behovet av behörighetskontroll. Betydelsen av ett BKS varierar dock, beroende på vilket överföringssätt man valt. En uppringd telelinje ger betydligt större sårbarhet för intrång än en fast uppkopplad förbindelse.

Vid fjärrförbindelse måste man beakta både utgående och inkommande trafik. Autenticering och åtkomstkontroll kan vara nödvändig i båda riktningarna. Exempelvis kan man formulera riktlinjer som säger att åtkomstkontroll för inkommande förbindelser bör bygga på användarautenticering (enkla lösenord eller engångslösenord) och bör vara begränsad till vissa tjänster och protokoll, medan åtkomstkontroll för utgående förbindelser kan baseras på nätadressen från vilken uppkopplingen sker och specifika tjänster och protokoll, d.v.s. användarautenticering krävs inte.

Åtkomstkontrollen för trafik som kommer utifrån kan behöva sättas extra hårt för vissa känsliga resurser, d.v.s. man tillåter helt enkelt inte åtkomst till vissa känsliga resurser via fjärrförbindelser.

7.5.2 Kryptering

Kryptering är en effektiv åtgärd för att i samband med datakommunikation skydda informationen mot avlyssning och förändring.

Kryptering innebär att informationen kodas innan den sänds, och att den görs läsbar av mottagaren endast under förutsättning att denne innehar rätt krypteringsnyckel. Kryptering av all information över ett fjärrnät försvårar både passiv och aktiv avlyssning. Detta kräver att krypteringsutrustning finns installerad vid det IT-system som sänder informationen, och att en motsvarande utrustning finns vid det mottagande systemet.

Är information eller data som överförs sekretesskänslig bör den skyddas genom kryptering på länknivå och/eller applikationsnivå.

Bedömer man att riskerna för trafikanalys vid fjärrförbindelser är stora, bör man överväga att använda någon metod för att generera brus i överföringarna.

Autenticeringsinformation bör alltid skyddas mot avslöjande. Lösenord bör därför endast överföras i krypterat skick.

Man ska ha klart för sig, att även där kryptering används kan det vara möjligt att förändra den information som överförs, i syfte att t.ex. sabotera överföringen. I vilken mån detta får skadliga konsekvenser beror på vilken metod för kryptering man använder, och om andra slag av kontroller finns, t.ex. avstämningskontroller.

Det finns olika hjälpmedel på marknaden för att kryptera information.

7.5.3 Motringning

Det finns utrustning för s.k. motringning. Denna arbetar normalt så att den tar emot ett samtal till datorn, kopplar ner det och ringer sedan direkt tillbaka på ett förutbestämt nummer, kopplat till den identitet som anges vid den första uppringningen. Motringning kan öka säkerheten, men är generellt sett inte tillräckligt bra om man kräver god IT-säkerhet. Tekniken används främst om man vill att samtalet ska betalas av den man ringer upp i första momentet.

7.6 Spårbarhet

Funktioner för generell spårbarhet ligger normalt, om de finns, i operativsystem, BKS eller tillämpningsprogram. Loggnings- och spårningsfunktioner kan och bör finnas i övervakningsprogrammet för nätet. Där används det framförallt i samband med felsökning.

Användare ska informeras om sitt ansvar och spårbarhet när de använder fjärrförbindelser. Alla försök att upprätta förbindelse ska loggas, oberoende av om de lyckats eller inte.

Följande information loggas för alla fall där förbindelse upprättats:

- information om vilka tjänster som används

- information för varje tjänst om mängden överförd data i varje riktning, t.ex. antal bytes
- alla förändringar i autenticeringsinformationen.

Digital signatur bör användas när det är viktigt att säkerställa att en transaktion verkligen är utförd av den som utger sig för att gjort det, eller omvänt, att man inte ska kunna förneka det som är utfört.

8 Säkerhet vid distansarbete

Kapitlet behandlar olika aspekter kring distansarbete. Både distansarbete via egna nät och distansarbetslösningar via Internet omfattas av detta kapitel. Naturligen berörs också ett antal näraliggande områden, t.ex. säkerhet i fjärrnät, säker arbetsplats m.fl.

Definition av en *distansarbetsplats* finns i del 3, kapitel 3.3.4.

8.1 Utmärkande för denna miljö

Med distansarbete menas att anställda använder datorer och telekommunikation för att arbeta på annan plats än kontoret under en del av eller hela arbetsdagen.

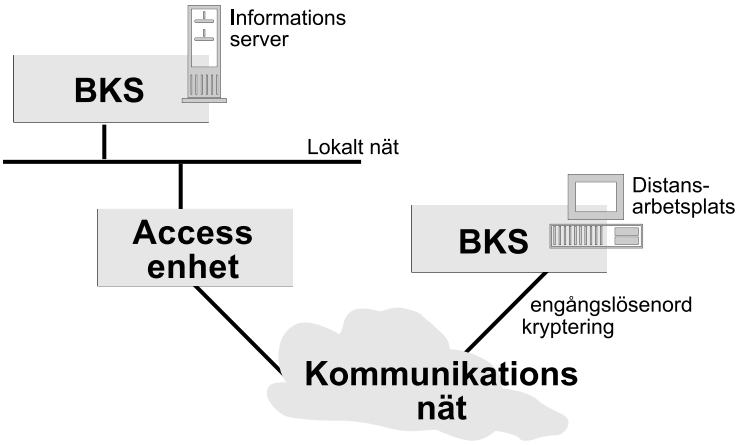
Normalt sker allt datorarbete i den egna arbetsplatsen eller via teleförbindelser i någon form av klient/server-tillämpning mot ett centralt system. I det senare fallet fungerar tillämpningen som om arbetet sker i det lokala nätet och alla skyddsåtgärder som finns centralt gäller för distansarbetaren.

8.2 Skyddsåtgärder

Distansarbetsplatsen kan ur säkerhetssynpunkt jämföras med en vanlig arbetsplats vad gäller PC:n samt förutsättningarna för viss typ av fjärrkommunikation. Dessutom kan det råda en fysiskt sett mer oskyddad miljö. De skyddsåtgärder som beskrivs i tidigare kapitel kan tillämpas för en distansarbetsplats.

Allmänna råd:

Satsa på en gemensam teknisk strategi inom organisationen för hur distansarbetsplatsen ska kommunicera med det centrala nätet. Bygg säkerhetslösningen baserad på vedertagna standarder.



Figur 19. Skyddsåtgärder för distansarbetsplats.

Tänk igenom och klargör vilken ansvarsfördelning som gäller för utrustning och information vid distansarbete.

Sammanfatta i en anvisning för distansarbete, de administrativa skyddsåtgärder som ska följas samt eventuella övriga villkor.

8.3 Riktighet

- All känslig information bör krypteras både vid lagring och överföring för att försvåra att informationen manipuleras.

8.4 Tillgänglighet

- Använd endast PC:n som arbetsredskap.
- Ta alltid säkerhetskopior efter slutfört arbete.

8.5 Sekretess

- Identifiering och autenticering mot centralt system bör minst motsvara en skyddsnivå som erhålls med engångslösenord.
- Arbetsplatsen bör utrustas med ett eget skal- och åtkomstskydd för att försvåra obehörig användning.
- Om man hanterar känslig information i arbetsplatsen bör den ha ett BKS som kan kompletteras med ett aktivt kort.
- Lösenord ska hanteras i krypterad form.
- Tänk på att kommunikation som sker via t.ex. GSM-nätet endast är kodad i luften, när det sänds vidare i telenätet sker detta i klartext (mobil distansarbetsplats).
- Använd inte Internet som kommunikationslänk utan att använda skyddsåtgärder avsedda för detta ändamål.

8.6 Spårbarhet

Funktioner som möjliggör spårbarhet ligger inte i distansarbetsplatsen.

Digital signatur bör användas när det är viktigt att säkerställa att en transaktion verkligen är utförd av den som utger sig för att gjort det, eller omvänt, att man inte ska kunna förneka det som är utfört.

9 Säkerhet vid anslutning till Internet

Kapitlet behandlar viktiga säkerhetsaspekter och lösningsmöjlighet kring anslutningen mellan en organisation och Internet. Naturligen ligger tonvikten på fast anslutning och sådan anslutning som innebär att en organisation både vill och ”inte vill” ha trafik med Internet.

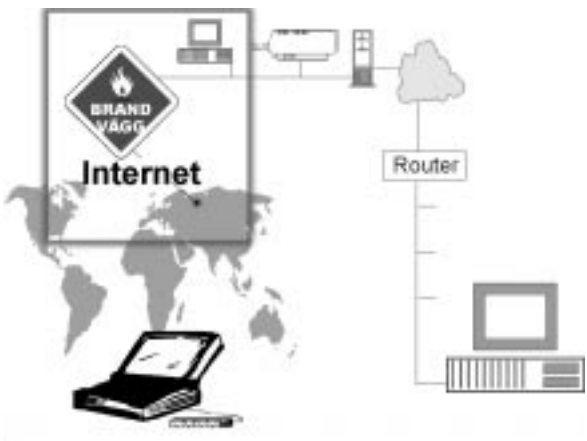
Definition av en *anslutning till Internet* finns i del 3, kapitel 3.3.5.

9.1 Utmärkande för denna miljö

Det finns, med avseende på den risk man exponerar sig för, två principiellt olika anslutningsmöjligheter till Internet:

- anslutning via eget lokalt nät
- anslutning via en persondator som är fristående, d.v.s. inte ansluten till något nät, endast lokala resurser är tillgängliga.

I det senare fallet är risken betydligt mindre att anslutningen innebär stora säkerhetsrisker för den interna verksamheten. Väljer man



Figur 20. IT-miljöer, anslutning till Internet.

detta alternativ kan man säga att man har god säkerhet vid anslutning till Internet. Det är framför allt säkerheten vid anslutning via eget nät som berörs i detta avsnitt.

Säkerhet i detta sammanhang omfattar alla handlingar som vidtas för att skydda resurserna innanför Internet-anslutningen. Det finns inte någon enskild produkt som erbjuder ett komplett skydd, utan en kombination av produkter och åtgärder måste användas för att skydda sig. Många risker som identifieras vid anslutning till Internet är inte unika för Internet utan de förekommer också i andra typer av fjärrförbindelser eller nätmiljöer. Det privata nätet är inte bara öppet för åtkomst från interna användare utan även global åtkomst är möjlig.

Säkerhet vid anslutning till Internet bör bestå av en kombination av skyddsåtgärder som kompletterar varandra t.ex. olika typer av fysisk säkerhet, säkerhet i operativsystemet, säkerhet i nät samt säkerhet i applikationer.

9.1.1 Skyddsnivåer

Skyddsnivåerna som tillämpas i fjärrnät gäller även här, se kapitel 7.1.1.

9.2 Administrativa skyddsåtgärder

Vid anslutning till Internet bör en handbok tas fram som beskriver regler och riktlinjer för hur anslutning till Internet ska hanteras och administreras. Handboken bör spridas, i lämpliga delar, till alla som på något sätt berörs av anslutningen. Den bör innehålla:

- värdering av hot och risker
- vad som behöver skyddas
- bedömning av kostnader vid en attack och kostnader för skydd
- regler och riktlinjer vid användning och administration
- definition av roller och ansvar.

9.2.1 Organisation och ansvar

- Säkerhetschefen med hjälp av systemadministratörer eller motsvarande person, leder och stödjer arbetet inom IT-säkerhetsområdet för att skydda IT-resurserna som ligger innanför anslutningen, t.ex. databaser och filer.
- Ansvarig utses för säkerheten vid anslutningen till Internet. I detta ansvar ingår både det generella ansvaret för underhåll och administration samt ansvaret för övervakning och åtgärder vid anslutningen. Systemadministratörer utses för att administrera och underhålla.
- Användaren har ett egenansvar, d.v.s. är skyldig att följa de regler och riktlinjer som gäller för användande av anslutningen till Internet.

9.2.2 Administration

En Internet-anslutning måste administreras och underhållas. Ofta krävs det både djup och bred kompetens hos berörd personal, både vad gäller datakommunikation och IT-system generellt:

- Anslutningar till Internet får endast upprättas efter godkännande av IT-säkerhetschefen.
- Hur underhåll och administration av anslutningen till Internet ska skötas ska vara dokumenterat och en ansvarig ska vara utsedd. Rutiner krävs både för installering av nya förbindelser, samt omkonfigurering och verifiering av existerande förbindelser.
- Anslutningar till Internet bör ej upprättas såvida det inte finns ett väl definierat behov samt en planerad användning. Man bör fastställa användningen vad gäller kommunikationsriktning, vilka protokoll som ska stödjas samt applikationer som använder protokollen.
- Internetanslutningen bör om det är möjligt begränsas till en punkt i det interna nätet. Det kan annars vara svårt att upprätthålla ett enhetligt skydd, dels i det lokala nätet och dels i anslutningspunkten.

- Dokumentation som beskriver Internet-anslutningen i detalj bör hanteras som riktighets- och sekretesskänslig information.
- Klara riktlinjer ska finnas vad gäller användarnas rättigheter att installera modem eller annan utrustning till sina arbetsplatser för att få tillgång till Internet.
- Dokumentation ska finnas över alla datorer, användare eller applikationer (vilket som är lämpligt) som använder Internet-anslutningen.
- Konfigureringen av Internet-anslutningen bör kontrolleras och verifieras årligen enligt definierade rutiner.
- Automatiserade metoder kan hjälpa till att upptäcka intrång och försök till sabotage. Riktlinjer måste sedan finnas som definierar vilka insatser som ska sättas in. Larm bör kopplas till kritiska händelser så att ansvariga uppmärksammas och nödvändiga åtgärder kan vidtas.
- Dokumenterade rutiner för hantering av loggar som registrerar trafiken till och från Internet ska finnas. Dessa rutiner kan t.ex. innefatta mätvärden för kontroll av servicenivå och registrering av misslyckade uppkopplingsförsök.

9.3 Riktighet

Vid anslutning till Internet avser riktighet främst att säkerställa att tillgångar innanför anslutningen inte påverkas av obehöriga utifrån samt att säkerställa att transaktioner som överförs till och från det interna nätet behåller sin riktighet. Riktigheten i det interna nätet kan bevaras genom användning av BKS vid åtkomst till interna resurser. Åtkomstkontrollen bygger på identifiering och autenticering. Metoden för autenticering kan baseras på nätadresser, enkla lösenord eller någon form av engångslösenord:

- Identifiering och autenticering ska utföras innan åtkomst av lokala IT-resurser tillåts för användare från en extern förbindelse. Styrkan i autenticeringsmetoden kan bygga på enkla lösenord som krypteras innan de överförs. Om autenticeringen

avser åtkomst till resurser som är av känslig karaktär kan det vara nödvändigt att använda starkare metoder, t.ex. stark autenticering och aktiva kort.

- Vid krav på hög säkerhet kan det finnas behov av att använda digitala signaturer på överförd information, t.ex. elektronisk post. Ursprunget kan då verifieras.
- För att säkerställa att leverans har skett finns olika kvittens- och mottagningsbevisprinciper, t.ex. att returnera en bekräftelse med sin digitala signatur efter mottagande.
- Transaktionens riktighet bevaras genom att tillämpa digitala signaturer och kryptering. Med kryptografiska kontrollsummor kan man kontrollera att riktighet kvarstår både på dataelementen som utgör transaktionen och på informationen som ingår i transaktionen.
- Återfå riktighet – en mekanism i systemet som har funktioner för att gå tillbaka till den senast kända korrekta tidpunkten för transaktionen. Detta gäller även andra resurser i systemet som har förlorat sin riktighet. Då kan man med en säkerhetskopia återskapa systemet.
- Virusskydd bör installeras i anslutningen till Internet för att identifiera smittad programvara, filer o.s.v. som passerar.
- Åtkomstkontroll sker med hjälp av en brandvägg. En brandvägg består egentligen av ett antal olika komponenter och beroende på hur man kombinerar dessa uppnår man olika nivåer av skydd.

9.4 Tillgänglighet

Den viktigaste åtgärden är att se till att anslutningen inte påverkas utifrån så att den försämras eller upphör att fungera samt att nätet innanför inte utsätts för störningar eller sabotage:

- Skydd mot attacker. Det finns en mängd hot och metoder för att sabotera en anslutning till Internet. En riskbedömning kan klarlägga vilka hot man kan tänkas bli drabbad av och som man därför måste skydda sig mot.

- Möjligheter att obehörigt förstöra eller modifiera program eller data kan försvåras om endast behöriga användare släpps igenom. Styrkan i identifierings- och autenticeringsmetoden är avgörande för vilken effekt åtkomstkontrollen får.
- Styrning och kontroll av trafik som går via Internet-anslutningen är nödvändig. Att störa kommunikationen/trafiken genom att på olika sätt överbelasta anslutningen kan undvikas genom lösningar som känner igen vissa beteenden eller inför begränsningar på hur mycket som går att göra samtidigt. Denna funktionalitet finns ofta i en brandvägg.
- All elektronisk post bör kontrolleras om de innehåller skadliga bilagor, t.ex. virussmittade filer. Vissa virus kan begränsa tillgängligheten till resurser.
- Vid nerladdning av färdig kod (som t.ex. Java, Postscript and Word Basic) från Internet bör dessa filer vara försedda med någon form av signatur eller annan säkerhetsgaranti, för att minska risken att sprida osäkra och påverkade exekverbara filer.
- Säkerhetsrevision – att i förväg kontrollera nivån av säkerhet – kan göras på olika sätt:
  - En traditionell intern IT-säkerhetsrevision av anslutningen.
  - Det finns företag som åtar sig att utföra kontroll av säkerheten genom att försöka komma åt skyddad data genom inbrott och därigenom avslöja svaga länkar i systemet.
  - Programvara som söker igenom nätet och avslöjar svaga länkar.
- Antivirusprogram bör installeras i anslutning till brandväggen. Oberoende av antalet och omfånget av virusskydd, måste anställda informeras om riskerna med att ladda ner filer från Internet, speciellt när det gäller programvara från okända källor.
- Kontrakt ska upprättas med tjänsteproducenten om servicenivå, bandbredd, tillgänglighet, o.s.v. Villkoren ska vara väldefinierade och överenskomna, liksom testmetod av dem.
- Kommunikationsutrustning eller kommunikationsprotokoll ska erbjuda felkontroll och återställande av fel för att säkra hög nivå av korrekthet i överförd data och hög tillgänglighet av förbindelsen.

- Tilläggs- och reservförbindelser ska finnas tillgängliga i händelse av fel på kommunikationsförbindelsen eller använd förbindelse. Att välja olika transmissionsnät för förbindelserna ökar möjligheterna att erhålla redundans i trafiken.
- Reservförbindelsen ska testas regelbundet. Säkerheten i reservlinjen ska också verifieras.

9.5 Sekretess

Kraven på sekretess berör dels data och information innanför anslutningen och dels transaktioner till och från nätet:

- Det interna nätet skyddas av en *brandvägg*. Tillgång till och från Internet är bara tillåtet via denna. Brandväggen är konfigurerad i enlighet med de riktlinjer som gäller vid anslutning till Internet.
- Tillgång är inte tillåten från icke tillförlitliga nät, om inte eventuell autenticering och kryptering bedöms ge ett tillräckligt skydd.
- Åtkomstkontroll sker genom att kontrollera vem som får komma ut och vem som får släppas in. En kontrollista på vilka nätadresser som är tillåtna kan användas för att filtrera bort obehöriga.
- Vid starkare autenticering bör autenticeringsinformationen skyddas mot avslöjande, för att förhindra återuppspelningar av autenticeringsprocessen. Engångslösenord i kombination med aktiva kort skyddar mot detta.
- Genom att implementera någon form av *kryptering* av transaktioner kan skydd mot insyn åstadkommas. Det kan ske på länknivå eller applikationsnivå.
- Det kan vara viktigt att inte utåt avslöja vilka som sitter på det interna nätet och deras adresser. Adresskydd implementerat i anslutningen kan översätta de interna riktiga adresserna till andra som används utåt.
- Utvärdering ska göras för att fastställa om trafikanalys är ett relevant och allvarligt hot mot Internet-anslutningen. I så fall ska den bemötas med lämpliga åtgärder i form av t.ex. kryptering och/eller generering av brus.

9.6 Spårbarhet

Användare måste informeras om sitt ansvar och kraven på spårbarhet när de använder Internet. Loggfunktionaliteten i en eventuell brandvägg samt användning av digitala signaturer kan hjälpa till att uppfylla kraven på spårbarhet:

- Alla försök att upprätta trafik ska loggas, oberoende av om de lyckats eller inte.
- Följande information ska loggas för alla fall där förbindelse upprättats:
  - modemets telefonnummer, portnummer eller modempool
  - användare eller det som upprättat förbindelsen, t.ex. nät
  - datum och tid för förbindelsens upprättande och när förbindelsen avbröts
  - all information om mängden överförd data i varje riktning, t.ex. antal bytes, antal filer eller antal TCP/IP-paket.
- Loggning för utgående uppringda förbindelser ska även innehålla information om plats, nätadress eller vilket telefonnummer som ringts.
- Även följande information ska loggas för alla fall där förbindelse upprättats:
  - information om vilka tjänster som används. Vid IP-förbindelse betyder detta information om vilka olika Internetprotokoll som används
  - information för varje tjänst om mängden överförd data i varje riktning, t.ex. antal bytes
  - alla förändringar i autenticeringsinformationen.
- Det bör finnas verktyg för att granska loggfiler eller konfigurera larmfunktioner.
- Varje användare som ska passera genom anslutningen ska vara unikt identifierad. Dataursprung hör ihop med riktighet. Det uppnås med kryptering eller digital signatur och kan ses som en förlängning av användarautenticering. Autenticitet är en förutsättning för att uppnå spårbarhet. I samband med transaktioner blir oavvislighet allt viktigare.

9.7 Övriga frågor kring anslutning till Internet

Ett viktigt mål för att skapa säkerhet vid anslutning till Internet är att skapa medvetenhet. Anställda ska rapportera alla brister i säkerhet internt eller externt. Skadan kan bli lika stor av ouppmärksamhet och slapphet inom organisationen, som av externa illasinnade angripare. En policy för Internet-användning bör finnas och ingå vid utbildning av nya anställda. Den bör fokusera på procedurer för datasäkerhet, virusmedvetenhet, hur man ska använda e-post och den externa anslutningen generellt.

Tekniken utvecklas och nya element kommer att föras in i näten. Dessa nya tekniker kan komma att förändra säkerhetsantaganden eller ha sidoeffekter som inte kan förutses. Speciellt brandväggar och virusskydd lever i en föränderlig värld. Dessa skydd är inte ”generella” utan baseras på det man vet idag, t.ex. kända virus och kända protokoll. Kompetensen i organisationen vad gäller problematiken kring Internet är viktig eftersom t.ex. en felkonfigurerad brandvägg leder till en stor säkerhetsrisk. Att kontinuerligt uppdatera sig vad gäller hot och risker samt se till att man har valt kunniga och pålitliga leverantörer för säkerhetsprogramvarorna är en process som ständigt måste pågå. Virusskyddsprogramvaror och brandväggar bör uppdateras kontinuerligt .

10 Säkerhet vid informationsspridning via Internet

Speciellt då myndigheter vill sätta upp egna tjänsteservrar på Internet, t.ex. WWW eller FTP-tjänster, uppstår särskilda frågeställningar kring säkerhet. Avsnittet behandlar hur säkerhetsfrågorna bör tacklas i detta sammanhang.

Definition av *informationsspridning via Internet* finns i del 3, kapitel 3.3.6.

10.1 Utmärkande för denna miljö

Informationen som ska spridas ligger lagrad i en webserver eller motsvarande. Kraven på tillgänglighet och riktighet för denna typ av tillämpning är mycket stora eftersom webservern fungerar som en aktiv källa för information. Användarna kommer åt informationen via Internet och ska normalt endast kunna läsa informationen i dessa fall. Man kan beskriva detta som ett s.k. spridningssystem.

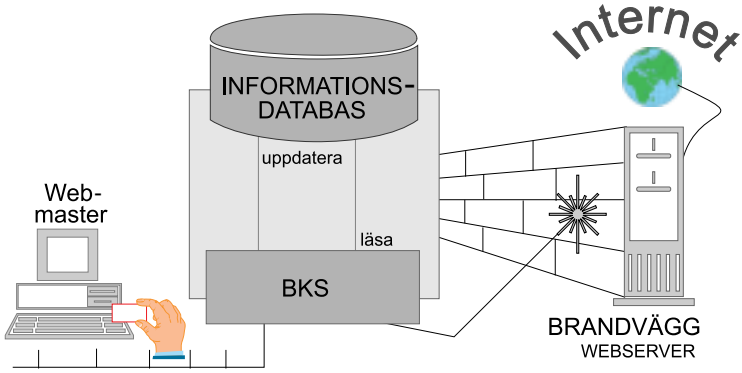
10.2 Skyddsåtgärder

Det handlar om att skydda webservern för obehörig och skadlig åtkomst men för att klara kraven på tillgänglighet och riktighet ställs även höga krav på sekretess. Förutsättningarna för skyddsåtgärder kan liknas vid dem som beskrivs i Säkerhet vid anslutning till Internet. De skyddsåtgärder som redovisas i det kapitlet kan även tillämpas i denna miljö.

Det stora hotet för en webserver är normalt externt och kommer via Internet. Därför är det viktigt att få till stånd en brandvägg med bra funktioner, både skyddstekniska och administrativa. Brandväggen får inte vara det enda skyddet utan måste kompletteras med ett

behörighetskontrollsystem i själva informationsservern. Funktionerna i detta och hur högt man ska lägga kraven för säkerheten måste avgöras av hur informationen/funktionen klassificeras.

Information som ligger på en webserver ska endast få uppdateras av behörig personal. Detta kan realiseras genom att använda ett behörighetskontrollsystem (BKS).



Figur 21. Skyddsåtgärder vid informationsspridning via Internet.

10.3 Riktighet

Använd funktioner, t.ex. kryptografiska kontrollsummor som upptäcker om filer, främst HTML-filer obehörigt har förändrats.

10.4 Tillgänglighet

Skyddsåtgärder för att höja tillgänglighet kan vara:

- Övervakning av utrustningen via något övervakningsprogram som automatiskt larmar eller vidtar olika åtgärder beroende på vad som hänt.
- Förberedelse för oönskade situationer av olika slag. Nya hot för att sabotera webservrar dyker ständigt upp.

10.5 Sekretess

- Säkerhetshöjande åtgärder för att täppa till säkerhetshål måste vidtagas i den dator som utgör webserver. Bevakning av nyheter inom området måste ske kontinuerligt.
- Behörighetskontrollsystemet måste anpassas till de säkerhetskrav som ställs. Kombination med aktiva kort ger ett bra skydd.

10.6 Spårbarhet

- Loggar i BKS ska kunna visa vem som gjort vad.
- Loggar i vissa brandväggar eller routrar kan ibland visa varifrån ett angrepp kommer.

11 Säker meddelandehantering

Kapitlet behandlar specifikt de förhållanden och möjligheter som föreligger för att specifikt kunna skydda meddelanden som transporteras via ett fjärrnät eller via Internet. Begrepp inom meddelandeområdet klargörs och diskuteras.

Definition av *meddelandehantering* finns i del 3, kapitel 3.3.7.

11.1 Utmärkande för denna miljö

Meddelandehanteringssystem är ett datoriserat kommunikationssystem som överför information i form av meddelanden på ett i förväg bestämt format. Exempel på meddelandehanteringssystem är elektronisk post eller e-post och fax.

E-post tillåter sändning och mottagning av meddelanden, dokument, statistisk information o.s.v. enligt ett i förväg bestämt format. Mottagaren kan efter eget behov läsa informationen, ändra, spara eller radera den. Sändaren kan dela med sig av informationen, välja läsare eller mottagare av meddelandet.

Ett annat sätt att överföra dokument elektroniskt är EDI (Electronic Data Interchange). EDI är ett sätt att utbyta affärsdata mellan två eller flera informationssystem enligt en internationell standard. Tanken bakom EDI är att EDI-meddelanden som kan bestå av beställningar, fakturor och leveransplaner ska kunna utväxlas fritt mellan olika företags datorer och samtidigt kunna kopplas till de interna systemen för att automatiskt initiera t.ex. tillverkningsprocesser, leveranser och utbetalningar.

Vi har tidigare konstaterat att det finns en del risk- och säkerhetsproblem vad det gäller meddelandehanteringssystem. Vissa av riskerna är inte enbart förknippade med meddelandekommunikation, men bör ändå nämnas.

11.2 Administrativa skyddsåtgärder

Bland administrativa skyddsåtgärder som ger skydd i meddelandehanteringssystem kan följande nämnas:

- Utforma en meddelandehanteringspolicy, som reglerar användningen av meddelandehanteringssystem i verksamheten och även anger riktlinjerna för hur meddelandehanteringssystem ska få integreras i annan IT-verksamhet.
- Klassificera informationen med utgångspunkt från lagstiftningens och verksamhetens krav.
- För meddelandehanteringssystem är datakommunikationsfrågor viktiga varför en genomtänkt datakommunikationsstrategi bör följas.
- Upprätta avtal med de organisationer med vilka man avser att utbyta affärsdokument eller andra viktiga dokument via meddelandehanteringssystem.
- Med utgångspunkt från policy, lagstiftningskrav och informationsklassificering utforma ett regelverk som ska gälla för meddelandehanteringssystem. Regelverket ska innehålla regler för:
  - Dokumentutbyte inklusive noggrann ansvarsuppdelning (personligt ansvar).
  - Vilka dokument som ska krypteras och vilka ska ha digital signatur.
  - Kryptering, nyckelhantering och nyckelöverföring.
  - Nätövervakning, kontroll av angrepp och behörighetskontrollsystem.
  - Vilka användare som ska ha tillgång till meddelandehanteringssystem.
  - Val av standardprotokoll och kommunikationsalternativ.
  - Funktioner för användarstöd inom organisationen.
  - Vilka dokument som ska skickas via meddelandehanteringssystem.

- Utse en person som ska ansvara för funktion, säkerhet och rutiner för felrapportering för meddelandehanteringssystem.
- Ge utbildning till all personal som använder meddelandehanteringssystem om hur funktionen och administrationen kring systemen är uppbyggd.
- Administrera behörighetskontrollsystem inklusive loggar.
- Granska och lagra transaktionsloggar och dokumentloggar.
- Logga nätöverföring avseende såväl förbindelser som utrustning.
- Arkivera en mottagen datafil i ursprungligt skick innan den bearbetas vidare i den egna organisationen.
- Arkivera gamla nycklar under tillfredsställande skydd.
- Utforma en handlingsplan för IT-säkerhetsarbetet gällande meddelandehanteringssystem.
- Ofta innebär införande av meddelandehanteringssystem också att nya arbetsrutiner måste införas. Gamla arbetsuppgifter försvinner och nya tillkommer. Man måste i tid vara observant på de problem som kan uppstå och utbilda och informera den personal som berörs.

11.3 Riktighet

I ett meddelandehanteringssystem är det viktigt att meddelandet aldrig obehörigt kan ändras eller förfalskas vare sig under lagring eller transport utan att det upptäcks. Innehållet i ett dokument ska bl.a. vara:

- korrekt
- komplett
- aktuellt
- tillförlitligt

Bland åtgärder som kan användas för att skapa skydd för riktighet finns:

- Kryptering av både lagrad information och vid kommunikation. I ett meddelandehanteringssystem bör det finnas möjligheter att kryptera meddelanden. Om det finns risk att någon obehörig modifierar eller fabricerar meddelanden så kan krypteringsteknik också implementeras som säkerhetsåtgärd.

  Om kryptering används mellan två applikationer måste hanteringen av krypteringsnycklar lösas. Att distribuera dessa på ett säkert sätt kan vara svårt. Nycklar kan distribueras via kurirer. Ett sändebud skickas till varje plats med en ny krypteringsnyckel. Det är viktigt att ändra nycklar då och då, eftersom en obehörig kan samla in en stor mängd krypterad text och starta ett försök till dekryptering. Nyckeldistribution över långa avstånd via kurirer är inte effektivt.

  I ett nät kan man t.ex. använda en nyckelserver som sköter distributionen av nycklar. Det är då viktigt att äktheten hos dessa nycklar kan verifieras.

- Ett dokuments ”äkthet” eller autenticitet kan bevisas genom digitala signaturer. En digital signatur medverkar till att avsändaren är den som han eller hon utger sig för att vara och dokumentet är också knutet till underskriften.

  För att uppnå ett skydd mellan två ändsystem är det därför väsentligt att den digitala signaturen utgör en integrerad del av meddelandet och är skapad av meddelandets behöriga utställare. Endast på detta sätt är det möjligt för utställaren att ta personligt ansvar för meddelandet och dess innehåll. Genom användningen av digital signatur erhålls automatiskt skydd mot att meddelandet kan förnekas av utställaren. När mottagaren svarar med ett kvittensmeddelande med digital signatur kan inte heller denne förneka att meddelandet har mottagits.

  Det är också mycket viktigt att den digitala signaturen har social och juridisk acceptans för att kunna jämställas med en handskriven signatur.

- Dataöverföringen måste säkerställas såväl inom som utanför organisationen. Det är mycket viktigt att kommunikationen kan garantera hög tillgänglighet och auktoriserad användning av systemet samt äkthet och spårbarhet för alla meddelanden som hanteras. Mottagaren av meddelandet måste med säkerhet kunna

bevisa att innehållet inte manipulerats. Om indikation erhålls att meddelandet kan ha blivit förändrat under sändningen bör det förkastas och relevanta loggar undersökas.

- En del meddelandehanteringssystem försöker höja säkerheten genom att ha inbyggda regler i datorn för vem som får kommunicera med vem, t.ex. i form av slutna användargrupper, vars deltagare bara får sända meddelanden till varandra.
- Sekvensnumrering kan användas vid kommunikation för att skapa en möjlighet att kunna konstatera att inget meddelande tas emot utanför sekvenskedjan.
- Behörighetskontrollsystem för åtkomstskydd och verifiering av individ. Ett behörighetskontrollsystem kan bl.a. skapa bevis för vem som matat in transaktionsdata till applikationen. Exempelvis i EDI-sammanhang, när transaktionen överförs till EDI-konverteraren för att konverteras till EDI-meddelande bör detta bevis överföras till EDI-meddelandet.
- Lösenord bör användas för autenticering av en användare.

Kryptering av känslig information är en vanlig skyddsåtgärd vid vanlig datakommunikation och kan även användas vid telefax-överföringar. Som vi tidigare har nämnt är ett problem än så länge att en säker kryptering bygger på en säker hantering av hemliga nycklar hos såväl sändare som mottagare. Detta kräver en viss administration och om någon obehörig kommer över den krypteringsnyckeln är systemet inte säkert.

Genom kryptering kan man hemliggöra innehållet i dokumentet för obehöriga men man kan inte vara säker på dokumentets äkthet d.v.s. om sändaren är den person som säger sig vara.

11.4 Tillgänglighet

Tillgänglighet i meddelandehanteringssystem innebär att möjligheten ska finnas för behörig användare att utnyttja meddelandehanteringssystemet i förväntad utsträckning och inom önskad tid.

Bland åtgärder som kan användas för att skapa skydd för tillgänglighet finns:

- Avtal rörande sändningstider/öppethållande. Med detta menas att genom överenskommelse om när sändning kan ske erhålls en kortare tid under vilken all utrustning måste fungera. Detta underlättar även bevakning och hantering av mottagna dokument.
- Alternativa kommunikationsmöjligheter ska finnas.
- Val av kommunikationsprotokoll kan påverka säkerheten.
- Utrustning för såväl system som telekommunikation ska erhålla tillräcklig kapacitet.
- Utrustningen ska ha en hög funktionssäkerhet och god beredskap att åtgärda fel och störningar.
- Alla meddelanden bör viruskontrolleras, även bifogade filer i elektronisk post.
- Avtal med betrodd leverantör av IT-resurser och meddelandehanteringssystem ska finnas.
- Färdiga program ska anskaffas från betrodd leverantör och viruskontroll ska ske innan program tas i bruk.

11.5 Sekretess

Med sekretess i meddelandehanteringssystem menas att endast de som är behöriga ska ha tillgång till information som överförs i form av meddelanden. Den som inte är auktoriserad ska förhindras att få tillgång till information.

Bland åtgärder som kan användas för att skapa skydd för sekretess finns:

- Behörighetskontrollsystem är ett måste i meddelandehanteringssystem. Ett sådant system kan användas för att:
  - Identifiera användaren. Användaridentiteten ska alltid vara unik.
  - Verifiera användarens identitet med t.ex. ett personligt lösenord, engångslösenord eller genom digital signatur.

  - Bekräfta användarens behörighet att använda efterfrågad funktion/resurs.
  - Dokumentera de händelser som berör BKS-funktionaliteten (loggning).
- Kryptering kan användas för skydd av både lagrad information och information som kommuniceras via något nät.
- En del meddelandehanteringssystem försöker höja säkerheten genom att ha inbyggda regler i datorn för vem som får kommunicera med vem, t.ex. i form av slutna användargrupper, vars deltagare bara får sända meddelanden till varandra.

När det gäller skyddsåtgärder för fax kan följande användas:

- I de fall där man har persondatorer med faxfunktioner, t.ex. ett PC-nät där servern är utrustad för att kunna sända och ta emot fax kan ett behörighetskontrollsystem användas.
- Kryptering kan användas vid telefaxöverföringar.
- Mellanlagring/Faxbrevlåda, är en funktion som innebär vidarebefordran av fax som mellanlagras i ett datorminne som inte behöver finnas i själva faxapparaten. Den här funktionen kan användas som ett skydd mot obehörig läsning på mottagarsidan eftersom man kan arrangera så att faxet inte sänds vidare till mottagaren förrän denne sänder en begäran till den mellanlagrande utrustningen, som i det här fallet tjänar som faxbrevlåda. Mottagaren måste här ange ett lösenord för att sändningen ska komma igång.
- Spärrat mottagarminne, som är ett sätt att skydda information på mottagarsidan, är att inte låta faxen skriva ut inkommande meddelande utan först lagra dem i ett mottagarminne. Utskriften sker först sedan mottagaren genom ett lösenord aktiverar utskriften.
- Kuvertering av inkommande fax. Det finns numera särskild utrustning som direkt kan kuvertera inkommande faxmeddelanden i anslutning till utskriften.

11.6 Spårbarhet

För att varken avsändaren eller mottagaren av ett meddelande i ett meddelandehanteringssystem i efterhand ska kunna förneka vad de gjort kan man använda sig av en säkerhetsfunktion som heter spårbarhet. Syftet med denna säkerhetsfunktion är att dokumentera vem som gjort vad.

Kraven på spårbarhet kan bland annat uppfyllas genom:

- Behörighetskontrollsystem för åtkomstskydd och verifiering av individ. Ett behörighetskontrollsystem kan bl.a. skapa bevis för vem som matat in transaktionsdata till applikationen. Exempelvis i EDI-sammanhang, när transaktionen överförs till EDI-hanteraren för att konverteras till EDI-meddelande bör detta bevis överföras till EDI-meddelandet.
- Använd digital signatur. På detta sätt erhålls skydd mot att meddelandet kan förnekas av utställaren. När mottagaren svarar med ett kvittensmeddelande med digital signatur kan inte heller denne förneka att meddelandet har mottagits.
- Använd lösenord för verifiering av en användare.
- Loggning av alla in- och utgående meddelanden är en mycket god form av bevis under förutsättning att loggarna är skyddade så att de inte kan ändras i efterhand och att det finns möjlighet att erhålla korrekt tid i systemen.
- När det gäller fax kan även ett behörighetskontrollsystem användas åtminstone i de fall där man har persondatorer med faxfunktioner.

11.7 Övriga frågor kring säker meddelandehantering

Vid användning av datorstödda meddelandesystem kan det finnas behov av etikregler. Med etikregler menar vi principer för lämpliga och olämpliga sätt att använda mediet. Etik är en objektivt definierad standard för rätt och fel.

Det är upp till varje organisation att formulera de etikregler som ska gälla där.

12 Säkerhet vid systemutveckling och systemförvaltning

Kapitlet belyser hur säkerhetsarbetet ska utföras under systemutvecklingsprocessen och den efterföljande förvaltningsfasen. Grundläggande för avsnittet är att det ansluter till förhärskande synsätt på modern systemutveckling, där säkerhetsfrågorna är en självklar och prioriterad del i alla avseenden. Avsnittet ansluter inte till någon specifik systemutvecklingsmodell utan försöker hantera frågeställningarna från en generell utgångspunkt.

Definition av *systemutveckling/systemförvaltning* finns i del 3, kapitel 3.3.8.

12.1 Utmärkande för systemutveckling

Begreppet systemutveckling definieras som de aktiviteter som avser analys, konstruktion och införande av ett system för datorstöd i någon mening. Systemförvaltning kan på motsvarande sätt beskrivas som de aktiviteter som avser att följa upp användningen av ett existerande system och att genomföra de förändringar, rättelser och kompletteringar som behövs.

Vid systemutveckling handlar det alltid om att ta fram ett systemstöd för att rationalisera eller vidareutveckla en speciell verksamhet. En självklar del är då att systemstödet ska innebära hjälp och effektivisering i utförande av alla de **kontroller** som verksamheten normalt kräver. Applikationens kontroller eller kontrollfunktioner i systemlösningarna får i detta sammanhang därför en särskilt vital betydelse.

Från säkerhetssynpunkt är det av fundamental betydelse att utveckling respektive förvaltning av ett datasystem ses som sammanhängande faser i en process, där säkerhetsfrågorna beaktas från början till slut. Lika grundläggande är att det finns en insikt hos de verksamhetsansvariga om att det under hela denna process är de

själva som har ansvaret för att säkerhetsnivån i systemen är tillräcklig.

Det är grundläggande att säkerheten ska styras av en övergripande IT-policy och IT-säkerhetspolicy, och att olika ansvarsroller är definierade och fungerar inom organisationen. En bärande princip ska vara, att med ett visst verksamhetsansvar följer också ansvar för de IT-system som stöder verksamheten och för säkerheten i dessa system.

12.2 Riktighet, tillgänglighet, sekretess och spårbarhet i utvecklingsarbetet

En förutsättning för att man ska kunna utveckla datasystem som uppfyller rimliga krav på säkerhet är att utvecklingsarbetet bedrivs på ett likartat och metodiskt sätt inom organisationen. Detta kräver att man arbetar efter en förutbestämd modell för hur systemutvecklingen ska bedrivas och vilka utvecklingshjälpmedel, rutiner etc. man ska tillämpa. På motsvarande sätt behövs en förvaltningsmodell för att man ska kunna bedriva systemförvaltningsarbetet på ett effektivt sätt.

Genom att man utnyttjar en bra och modern systemutvecklingsmodell kommer alla väsentliga aspekter på säkerhet och integritet att kunna beaktas och behandlas på ett systematiskt sätt under systemets utveckling och efterföljande liv. Just i det systematiska angreppssättet ligger mycket av nyckeln till den inbyggda säkerhet som man vill uppnå. Det finns i dag på marknaden ett antal systemutvecklingsmodeller. Under senare år har dessa ofta vidareutvecklats till att omfatta kopplingar till företagens ordinarie kvalitetssystem, samt utvidgningar för att kunna hantera objektorienterad analys och utveckling. Information om vilka modeller och metoder som är tillämpliga, moderna och bra får sökas på marknaden bland konsult- och rådgivningsföretag och genom kontakter med användarorganisationer som har erfarenheter av de olika metoderna. En del modeller behandlar IT-säkerhetsfrågorna mer uttryckligt än andra. Ibland kan det vara nödvändigt att göra tillägg eller tillfälliga utvidgningar i den egna utvecklingsmodellen för att behandla speciella säkerhetsaspekter.

Säkerheten i ett datasystem grundläggs under systemets utvecklingsfas. Säkerhetsåtgärder som man då försummar att vidta kan vara svåra eller i värsta fall omöjliga att genomföra när systemet tagits i drift. Ett system ska uppfylla följande grundkrav:

- god tillgänglighet, d.v.s. att informationen ska finnas tillgänglig när användarna behöver den
- god ändamålsenlighet och funktionalitet, d.v.s. att systemet ska vara anpassat till verksamheten och ha en sådan teknisk utformning och konstruktion att drift och systemteknisk förvaltning underlättas
- information som kan vara sekretessbelagd eller integritetskänslig ska kunna skyddas
- den information som produceras ska vara aktuell och tolkningsbar och så långt det är möjligt korrekt.

För att ett system, som fyller de för verksamheten relevanta säkerhetskraven, ska kunna skapas, krävs att det i utvecklingsprojektet finns företrädare såväl för olika informationsanvändare och verksamhetsansvariga som för IT-personal. Det är givetvis också angeläget att personer med särskilda kunskaper på IT-säkerhetsområdet finns med.

Kravet på tillgång till specialister av olika slag är minst lika stort i dag som tidigare, om man vill kunna utnyttja moderna utvecklingshjälpmedel och ny teknik på ett effektivt sätt. Framför allt måste man i de flesta utvecklingsprojekt, förutom kunniga systemerare, på ett tidigt stadium ha med t.ex. kommunikationsexperter, databasexperter och driftansvariga. Deras kunskaper om den tekniska miljön är ovärderlig, bl.a. när det gäller att bedöma lämpliga tekniska skyddsåtgärder.

Enkelt uttryckt kan man säga att riktighet, tillgänglighet, sekretess och spårbarhet i utvecklingsarbetet uppnås på följande sätt:

Riktighet Riktighet vad avser det utvecklade systemets förmåga att hålla information oförvanskad, erhålls genom ordentlig kvalitetssäkring av hela utvecklingsarbetet och genom upprepade granskningar och godkännandeaktiviteter avseende applikation

och systemlösning, fram mot ett färdigt system. Riktighet av den information som hanteras under ett systemutvecklingsarbete säkerställs genom kvalitet i medarbetarval och noggranna rutiner för dokumentation, programvarubibliotek och versionshantering.

Tillgänglighet Tillgänglighet erhålls genom att ställa krav på den miljö som utvecklingsprojektet ska genomföras i. Dokumentationssystem och utvecklingsdatorer, är dessa ”single-point-of-failures” eller finns redundans i lösningen på något sätt?

Sekretess All information i utvecklingsarbetet ska vara underordnad regler för åtkomst och behörighet, såväl fysisk som logisk.

Spårbarhet Spårbarhet uppnås främst genom val och tillämpning av ett modernt versionshanteringsstöd, med loggfunktioner och möjlighet att återskapa tidigare lägen i utvecklingsarbetet. Vidare uppnås spårbarhet genom noggrant förd projekt- och beslutsdokumentation.

12.3 Utvecklingsprocessen

För att kunna vidta de rätta skyddsåtgärderna måste man redan på ett tidigt stadium dokumentera de övergripande säkerhetskraven i det planerade systemet. Under hela utvecklingsskedet måste man sedan detaljspecificera, detaljutforma, kontrollera och testa samt godkänna de enskilda skydden. Utvecklingsarbetet kan på olika sätt delas in i tidsfaser.

- Verksamhets- och informationsanalys, som med tanke på behovet av avstämning och beslut under arbetets gång kan delas in 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 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.

Varje etapp i utvecklingsprocessen ska avslutas med att beställaren fattar **ett formellt beslut** om hur projektet ska fortsätta. Även inom en etapp kan det ibland bli nödvändigt att låta uppdragsgivaren ta ställning till om projektet ska drivas vidare enligt de ursprungliga planerna eller om dessa måste förändras.

De här formella besluten är nödvändiga för att uppdragsgivaren ska ha möjlighet att på ett tidigt stadium få kännedom om bl.a. vilka eventuella hinder som kan finnas för att uppfylla vissa IT-säkerhetskrav. Sådana hinder kan vara t.ex. att den maskin- och systemprogramvara som man redan har inte medger installation av ett tillräckligt bra behörighetskontrollsystem. En generell säkerhetsåtgärd, som gäller alla faser, är att alltid låta utvecklingsarbetet ske i en teknisk miljö, som är helt avskild från driften av befintliga system.

12.3.1 Föranalys

Redan i det första skedet i ett utvecklingsprojekt måste man:

- fastställa vilka lagar och förordningar, t.ex. datalagen, sekretesslagen och tryckfrihetsförordningen, som kan komma att påverka systemutformningen
- beskriva de kontrollfunktioner som finns i verksamheten och fastställa principerna för hur olika kontrollfunktioner ska samverka i det nya systemet
- fastställa principerna för behörighetskontroll
- fastställa principerna för informationsklassificering
- dokumentera den övergripande kommunikationsstrukturen i det planerade systemet samt ange vilka andra interna och/eller externa IT-system som berörs
- fastställa vilka kvalitetskrav som finns vad avser informationen

- bedöma huruvida en framtida förändrad inriktning eller omfattning av den berörda verksamheten kan komma att påverka kraven på informationshantering
- fastställa ansvar och befogenheter för systemet.

Några av de här punkterna kan ha stor betydelse för beslut i frågan om ett projekt ska drivas vidare, och i så fall på vilket sätt. De måste därför redan på det här stadiet belysas ingående. Observera att alla de här punkterna måste gås igenom även om man från början bestämt sig för att köpa en färdig programprodukt. För att kunna utvärdera olika leverantörers programvaror måste man först ha klart för sig vilka säkerhetskrav som ska ställas.

Tryckfrihetsförordningen och sekretesslagen påverkar i hög grad myndigheternas informationssystem. Rätten för enskilda att ta del av allmänna, offentliga handlingar kan komplicera den rent tekniska utformningen av system. Särskilt där man har information som är blandad, i meningen att delar av informationen kan bli belagd med sekretess. Sådana systemlösningar bör så långt möjligt undvikas. Datalagens krav om skydd av den personliga integriteten innebär att man från början noga måste tänka igenom vilken personinformation man behöver i sina system och vilka åtgärder som behövs för att skydda denna information. Som stöd för att bedöma behovet av skyddsåtgärder kan man använda Datainspektionens allmänna råd, formulerade i olika publikationer som kan erhållas från Datainspektionen.

Ett annat exempel på lagstiftning som måste beaktas före utveckling av ett datasystem är bestämmelserna i säkerhetsskyddsförordningen, som ställer krav på säkerheten vid de statliga myndigheter som befattar sig med uppgifter som rör rikets säkerhet. Bl.a. föreskrivs att myndighet före inrättandet av system, som kan komma att innehålla uppgifter som kan vara känsliga för totalförsvaret, ska samråda med överbefälhavaren, och avseende rikets säkerhet i övrigt (sabotage, terrorism m.m.) med säkerhetspolisen. Även förvaltningslagen med bestämmelser om bl.a. myndigheternas serviceskyldighet, liksom arkivförfattningar, bokföringsbestämmelser och eventuell särskild lagstiftning inom det egna verksamhetsområdet, måste beaktas från början av utvecklingsarbetet.

En bedömning av vilka särskilda åtgärder, som kan komma att krävas på grund av lagstiftning, är en viktig del av beslutsunderlaget för projektets fortsättning. Redan på det här stadiet ska man således kunna dokumentera exempelvis krav på kryptering av information, krav på avskild driftmiljö, krav på en teknisk lösning som medger åtminstone en ”förhandsgallring” när det gäller att bedöma om en handling är offentlig eller kan tänkas bli belagd med sekretess.

Riktighet och kontrollfunktioner

När man inför nytt IT-stöd för en viss verksamhet ska systemet givetvis kunna utföra åtminstone de kontroller som finns i de befintliga manuella rutinerna eller i ett befintligt IT-system. Ofta ger också tekniken möjligheter att införa fler och säkrare kontroller. Man bör alltså utgå från de kontroller som är önskvärda, och sedan undersöka de tekniska möjligheterna att realisera önskemålen.

För att man verkligen ska få en fullgod kontrollstruktur i sitt totalsystem krävs, att man på ett tidigt stadium har analyserat och dokumenterat hela kontrollstrukturen i den befintliga informationshanteringen. Det finns många exempel på att man vid införandet av IT har fått en betydligt sämre kontrollstruktur än i ett tidigare helt eller delvis manuellt system. För att beslutsfattaren ska kunna ta ställning till en totallösning, måste den tänkta kontrollstrukturen i det nya systemet vara dokumenterad på ett tidigt stadium. Lösningen kan bl.a. påverka behovet av manuella kontrollrutiner som ett komplement till det maskinella systemet.

Behovet av behörighetskontroll har inte bara att göra med känslig personinformation eller lagstiftning som ställer krav på skydd av information. För alla IT-system, som har flera användare, bör man ha någon form av behörighetskontroll som reglerar vem som får göra vad i systemet.

Hur omfattande behovet av behörighetskontroll är måste dokumenteras på ett tidigt stadium. Det kan exempelvis påverka val av maskin- och systemprogramvaror.

De allvarligaste säkerhetsproblemen finns i dag ofta i samband med kommunikation. De flesta IT-system går att nå från arbetsplatser av olika slag, och i många fall förutsätts att olika IT-system ska utbyta

information med varandra. För att kunna bygga in en hög säkerhet i kommunikationen till ett system och mellan olika system är det viktigt, att man redan i det första utvecklingsskedet har klart för sig vilken typ av kommunikation som ska vara möjlig.

Man måste också kartlägga den säkerhet som finns, t.ex. typ av behörighetskontrollsystem, i de befintliga system som det planerade systemet är tänkt att samverka med. En bristfällig säkerhet i dessa system kan medföra att man kanske måste avstå från en viss typ av samverkan eller lägga ned resurser på att förbättra säkerheten i befintliga system.

12.3.2 Detaljanalys

I det här steget ska systemet detaljutformas och den tekniska lösningen fastställas. På alla de punkter som berörts i föregående avsnitt måste slutliga lösningar presenteras. Bl.a. ska det då vara helt klart:

- hur maskinella och manuella kontrollfunktioner ska utformas och hur de ska samverka
- vilka krav man måste ställa på olika funktioner i behörighetskontrollsystemet
- om någon information behöver krypteras
- vilka krav på tillgänglighet som måste uppfyllas
- hur säkerhetskontrollerna ska fungera vid eventuella samband med andra system
- hur reservkopieringsrutinerna ska fungera
- vilka loggfunktioner som ska finnas
- vilket reservdriftalternativ som ska väljas och riktlinjerna för hur manuella reservrutiner ska fungera
- eventuellt behov av förstärkning av befintliga generella administrativa, tekniska och fysiska skydd
- vilket utbildningsbehov som finns.

Det är vanligt att man i den här utvecklingsetappen tar fram någon form av systemprototyp. Om man inom en organisation beslutar sig för att använda denna metodik ska man noga utreda vilket verktyg som ska användas. Att i en och samma tekniska miljö tillåta användandet av flera olika verktyg kan få allvarliga negativa konsekvenser, särskilt om man för vissa system vill använda ett verktyg i hela kedjan, d.v.s. även för utveckling av det riktiga produktionssystemen. Det är viktigt att man i prototypen tar med de kontrollfunktioner som ska finnas i det färdiga systemet, och inte bara koncentrerar sig på att skapa ”användarvänliga” dialoger. Lika viktigt är att få klarhet i om alla krav på kontroller kan tillgodoses. Om det visar sig att vissa typer av t.ex. konsekvenskontroller eller avstämningskontroller inte går att utföra måste det dokumenteras i detta skede.

12.3.3 Systemutformning och systemkonstruktion

Ibland utgår man i utvecklingsprojekt från att det ska vara möjligt, inte bara att använda högnivåverktyg för att ta fram en systemprototyp, utan också att använda denna prototyp i mer eller mindre oförändrat skick även för produktion. Det har tyvärr visat sig att till synes användarvänliga prototypsystem ibland blir synnerligen ”användarovänliga” när de tas i produktion, med t.ex. oacceptabla bearbetningstider. För att undvika sådana överraskningar måste man ha tillgång till detaljerade uppgifter om datamängder, typ av bearbetningar o.s.v., för att personer med teknisk kompetens ska kunna avgöra om den tänkta maskinutrustningen kapacitetsmässigt räcker till.

I de flesta utvecklingsprojekt av någorlunda omfattning innebär systemkonstruktionsfasen att ett stort antal program ska produceras, för att så småningom sammanfogas till en fungerande enhet, alternativt samverkande delsystem. IT-systemets utformning och konstruktion måste styras av bl.a:

- klart fastställd ansvarsfördelning mellan verksamhetsansvariga och IT-ansvariga
- en övergripande strategi för utformning av informationssystem inom organisationen (informationsarkitekturen)
- principer och regler för programkonstruktion

- regler för dokumentationsstandard
- regler för hur programgemensamma resurser ska hanteras
- regler för hur programtester ska genomföras och vilka testdata som ska användas
- regler för hur och av vem systemtester ska genomföras och godkännas samt hur och av vem testdata ska framställas
- regler för vilka maskinella resurser som ska användas i samband med tester och regler för vem som ansvarar för att t.ex. testdatabaser återställs efter genomförda tester
- versionshanteringsplattform, d.v.s. hur man i projektet säkerställer att dokumentation och källkoder hanteras på ett konsistent och betryggande sätt
- regler för hur och med vilken ansvarsfördelning produktionstester ska genomföras samt vilka kriterier som ska gälla för att ett produktionstest ska kunna godkännas
- utbildningsmaterial tas fram
- alla användarinstruktioner färdigställs
- driftdokumentationen färdigställs
- utbildningen genomföras så långt det är möjligt (helst bör det finnas ett utbildningssystem tillgängligt när produktionstesterna påbörjas)
- införandet detaljplaneras
- regler för administration av behörighetskontrollsystemet fastställas (tilldelning, registrering, uppföljning o.s.v.).

12.3.4 Införande

Införandet av ett IT-system kan vara en lång och ibland komplicerad process. Mycket beror på hur omsorgsfull man varit i de föregående faserna i utvecklingsprocessen, och hur väl man planerat införandet. Systemets storlek och komplexitet och organisationens IT-mognad har också stor betydelse för hur pass smärtfri införandeprocessen blir.

Varje införande av ett IT-system ska föregås av ett formellt godkännande av beställaren. Detta ska inte vara enbart ett undertecknande av ett papper, utan beställaren ska genom lämpliga kontroller ha övertygat sig om att den färdiga produkten svarar mot de krav som ställts.

Har projektet genomförts på ett riktigt sätt brukar överlämnandet av systemet från projektgruppen till drift- och förvaltningsansvariga inte utgöra något stort problem. Det är emellertid viktigt att alla inblandade parter är överens om, att systemet är klart att tas i produktion. Eventuella fel i program, som identifierats men ännu inte åtgärdats, måste redovisas så att verksamhetsansvariga kan avgöra om systemet ändå ska införas eller om man ska vänta.

I organisationer, där man redan har ett omfattande IT-stöd, är man i allmänhet medveten om de problem som kan uppstå i samband med att ett nytt system ska tas i bruk. Det är emellertid även där vanligt att man t.ex. underskattar utbildningsbehovet och behovet av fortlöpande information under ”inkörningsperioden”.

Det är systemägarens ansvar att se till att all personal som är beroende av ett visst system får den utbildning och information som behövs, för att de ska kunna använda systemet på rätt sätt. Det är också viktigt att alla känner till vilka säkerhetsbestämmelser som finns för ett visst system. Systemägaren måste t.ex. kunna motivera varför man har en viss typ av behörighetstilldelning till olika delar av systemet.

Det finns inga system där man inte någon gång råkar ut för att fel inträffar. Systemet får emellertid inte vara så dåligt testat, att man i början riskerar att råka ut för fel var och varannan dag. Risken för att ett sådant system aldrig når upp till en acceptabel IT-säkerhetsnivå är stor, eftersom förvaltningsprocessen redan initialt får en skev inriktning. För att testningen av ett system ska bli rättvisande, är det viktigt att systemets tänkta användningsområde och användningssätt avspeglas väl i testsituationen.

De viktigaste förutsättningarna för att man ska lyckas är således att systemet initialt är av god kvalitet samt att den personal som berörs har fått tillräcklig utbildning, är motiverad att börja arbeta med det nya systemet och har förståelse för de säkerhetsåtgärder som vidtagits.

12.3.5 Säkerhetsanalyser kring utveckling och förvaltning

Under ett utvecklingsarbete är det viktigt att vid vissa tidpunkter göra en kontroll av dels att projektet som sådant fungerar tillfredsställande, dels att IT-säkerhetsfrågorna beaktats. En första analys bör göras på ett tidigt stadium av utvecklingsarbetet. Det finns olika sätt att göra sådana kontroller, men erfarenhetsmässigt har det visat sig att den s k SBA-metoden, rätt använd, ger svar på många viktiga frågor både vad avser projektarbetet och IT-systemet som sådant.

SBA Scenario, bör användas för att kontrollera sårbarhets- och säkerhetsnivån i systemet. En första analys bör göras så snart man har en någorlunda klar bild av hur systemet är tänkt att fungera, och sedan bör man regelmässigt göra en analys under senare delen av konstruktionsfasen.

Nyckelpersonalproblem har drabbat många verksamheter i samband med införande av nya IT-system. För att i tid gardera sig kan man göra en speciell analys av personalsituationen inom den verksamhet som berörs, framför allt vad avser den kompetens som behövs inom olika funktioner. Detta påverkar i hög grad utbildningsbehovet. **SBA Nyckel** är här ett bra hjälpmedel.

SBA Projekt bör användas i varje projekt, dels initialt för att bl.a. bedöma de totala projektriskerna, dels under projektets gång för att kontrollera att projektet fungerar tillfredsställande. SBA Projekt behandlar bl.a. frågor som rör bemanningen av projektet, projektmiljön, IT-mognaden i den verksamhet som berörs, den teknik som man tänker använda samt kompetensen hos projektmedlemmarna. I ett projekt där riskerna är stora inom någon eller några av de här områdena är risken också stor att viktiga IT-säkerhetsaspekter inte beaktas. SBA Projekt används dock inte för själva säkerhetsanalysen.

12.4 Systemförvaltning och säkerhet

De beskrivningar av säkerhetsproblem, risker och skyddsåtgärder etc., som har gjorts i tidigare i den här vägledningen, är alla tillämpliga under ett IT-systems förvaltningsfas. Det är emellertid

en säkerhetsfråga av helt avgörande betydelse att rätt uppfatta innebörden och vikten av systemförvaltning – nödvändigheten av att under ett IT-systems hela livstid aktivt arbeta på att identifiera behovet av och genomföra de förändringar som krävs, på grund av att hotbild, lagstiftning och andra förutsättningar för verksamheten ändras.

Varje system som utvecklas för att ge stöd till en viss verksamhet utgör en investering i verksamheten. Mestadels uppgår investeringen i varje enskilt IT-system till betydande belopp. På samma sätt som när det gäller förvaltning av t.ex. fastigheter och andra tillgångar, gäller även för IT-system att förvaltningen av det investerade kapitalet ska ske effektivt och till en så låg kostnad som möjligt.

Även om man initialt har ett system som uppfyller de krav som ställts, både vad avser verksamhetsstöd och IT-säkerhet, vet man erfarenhetsmässigt att alla system blir före-mål för ingrepp av olika slag när de tagits i produktion. Det som föranleder ingreppen är bl.a. behovet att:

- korrigera fel som upptäcks i systemet
- anpassa systemet till ändringar i verksamheten, nya och förändrade lagar eller ändrad IT-miljö
- förbättra systemet med hänsyn till verksamheten eller teknikutvecklingen
- sanera systemet, d.v.s. avlägsna onödiga systemdelar.

Om inte dessa åtgärder genomförs enligt fastställda regler och med stor noggrannhet riskerar man, att även sådana system som initialt hade en hög kvalitet snabbt degenererar. Även uteblivna åtgärder, t.ex. anpassningar till nya verksamhetskrav, kan få motsvarande effekt, eftersom stödet till verksamheten försämras.

En av de vanligaste åtgärderna som föreslås, som en följd av att man har genomfört säkerhetsanalyser på befintliga system, är att förvaltningen av systemen ska förbättras. En aktiv och väl fungerande systemförvaltning är en av de viktigaste säkerhetshöjande åtgärderna i IT-verksamheten och bidrar, i kombination med en väl fungerande driftmiljö, i hög grad till en minskad sårbarhet. Jämsides med den löpande systemförvaltningsprocessen, där de ovan

uppräknade aktiviteterna ingår, måste man också ha en välplanerad vidareutveckling och en långsiktig planering av systemets livslängd, där avvecklingsplanering utgör en viktig del.

Den verksamhetsansvarige är således den som ytterst ansvarar för att förvaltningen av de IT-system som är knutna till verksamheten fungerar enligt fastställda och bra regler. På motsvarande sätt som när det gäller IT-säkerhetsansvaret följer förvaltningsansvaret ansvaret för verksamheten nedåt i organisationen till det egenansvar var och en har, som är användare av systemet eller enbart informationsanvändare.

Den IT-säkerhetsorganisation som förutsätts finnas inom verksamheten har ingen direkt motsvarighet i förvaltningsorganisationen. Man brukar inte utse någon för hela organisationen gemensam systemförvaltningsansvarig. Däremot har man i många organisationer ”systemförvaltare”, som ansvarar för förvaltningen av enskilda system. Normalt brukar förvaltningsansvaret för enskilda system ligga på den som är systemansvarig närmast under systemägaren.

En av de vanligaste anledningarna till att man får störningar i egenutvecklade system är sådana förvaltningsåtgärder som innebär att man gjort någon typ av ingrepp i systemet. Störningarna kan vara av olika slag och medföra mer eller mindre allvarliga konsekvenser för verksamheten, allt ifrån kortvariga avbrott i dialogåtkomsten till dygnslånga förseningar av satsvisa bearbetningar. Ingreppen kan också förorsaka att felaktiga utdata produceras, vilka i värsta fall även distribueras till interna och externa mottagare.

Oberoende av vad som föranlett ingreppet i systemet, upptäckta programfel, anpassning eller förbättring av vissa systemdelar, beror de oönskade effekterna mestadels på att man saknar eller inte följer givna regler för hur sådana ingrepp ska göras.

Vanliga anledningar till att olika typer av ingrepp i systemen medför störningar är att:

- dokumentationen är bristfällig
- ändringarna utförts på ett felaktigt sätt
- ändringarna i det enskilda programmet inte testats ordentligt
- hänsyn inte tagits till att andra delar av systemet än det där ingreppet skett påverkas

- ingen fullständig testning gjorts innan man överfört ändrade systemdelar/program till produktion.

Det här är ganska vanliga företeelser och anledningen är oftast att man inte har reglerade rutiner för hur och när olika typer av ingrepp får göras i systemen. De olika förvaltningsåtgärderna genomförs oplanerat och utan samordning eller prioritering. Detta medför också att ett antal personer ständigt är sysselsatta med att göra olika typer av ingrepp i systemen. Eftersom det också mestadels saknas regler för testverksamhet och godkännande av tester, samt formaliserade rutiner för överföring till produktion av ändrade program, tenderar antalet ingrepp på grund av programfel att öka.

Tidigare har detta varit ett utpräglat problem för stora system i centraldatormiljöer. Samma problem tenderar att bli allt vanligare i server- och PC-miljöer, där man numera också ofta har egenutvecklade system.

System som förvaltas på detta sätt riskerar att snabbt degenerera. Ett första steg i att införa bättre systemförvaltningsrutiner är att åtminstone skapa regler för, dels hur och när ingrepp i program får göras, dels hur tester ska genomföras och godkännas. I princip ska inga andra ingrepp i program få göras oplanerat än de som krävs för att åtgärda sådana fel som förorsakar störningar som inte är att betrakta som lindriga. Detta innebär t.ex., att man kan avvakta även med att åtgärda ett upptäckt programfel.

På motsvarande sätt som när det gäller systemutveckling bör systemförvaltning bedrivas likartat inom hela organisationen och följa en fastställd besluts- och arbetsmodell. Systemförvaltning är en naturlig fortsättning på varje utvecklingsprojekt och därför bör utvecklings- och förvaltningsmodellerna vara anpassade till varandra.

Huvudprinciperna för hur systemförvaltningsarbetet bör organiseras och genomföras gäller för alla typer av IT-system, oberoende av i vilken typ av dator bearbetningen sker. Att följa ett enhetligt och systematiserat arbetssätt vid systemförvaltning bör ses som en grundläggande säkerhetsåtgärd i sig.

Att införa en systemförvaltning enligt en fast modell kräver en hel del förberedelser, och i organisationer, där man inte tidigare haft någon fast struktur för systemförvaltning, kan det vara lämpligt att

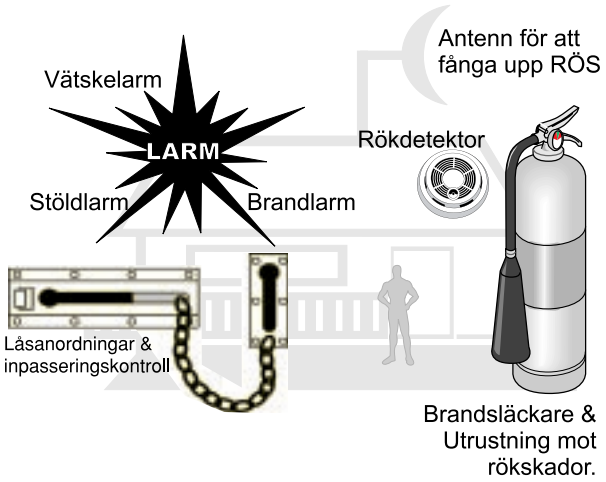
använda ett någorlunda väl fungerande system som pilotprojekt. Förutom att man mestadels måste utarbeta en hel del instruktioner för bl.a. uppföljnings- och genomförandefaserna måste man också fastställa vilka beslutsnivåer man ska ha för de olika typerna av förvaltningsinsatser.

Sist men inte minst är det viktigt att utbilda och informera den personal som berörs av systemförvaltningsarbetet. Systemförvaltningens betydelse för en ökad säkerhet i IT-verksamheten måste klargöras för såväl beslutsfattare som annan personal. Man bör också se till att alla är medvetna om att en aktiv systemförvaltning kräver hög kompetens, vilket bör göra det lättare att engagera erfarna medarbetare till dessa arbetsuppgifter.

13 Fysiskt skydd

13.1 Generella skydd

I de flesta IT-miljöer måste de administrativa och IT-tekniska skyddsåtgärderna kompletteras med **byggnadstekniska**. Till de senare räknar vi allt som sammanhänger med brandskydd, larm som inte är direkt knutet till datordriften, elförsörjning, tillträdesskydd samt skydd mot röjande signaler (RÖS).



Figur 22. Byggtekniska skyddsåtgärder.

13.1.1 Tillträdesskydd

Här redovisas exempel på åtgärder som räknas som tillträdesskydd:

- Till alla lokaler, där det finns servrar placerade, ska det finnas särskilda anordningar för att förhindra att andra personer än driftpersonalen har tillträde.
- Rum som används för servrar eller andra mindre datorer ska inte användas till annan verksamhet. Till rummet ska bara den personal ha tillträde som ansvarar för drift av datorn. I komplexa persondatormiljöer kan det också vara nödvändigt att placera gemensam utrustning i särskilda rum som kan låsas.

- Särskilda rum där modem och annan kommunikationsutrustning är placerad ska vara låsta, och endast personal som är behörig ska kunna komma in i sådana utrymmen.
- I kontorsutrymmen där känslig information bearbetas i persondatorer eller andra mindre datorer måste dörrar kunna låsas, om utrustningen och programvaran inte har sådana IT-tekniska skydd som förhindrar obehöriga att komma in i systemet. Vad gäller bearbetning av känslig information i servrar eller andra fleranvändarsystem, kan det också vara nödvändigt att skaffa helt egen utrustning för sådana system som kräver speciella skyddsåtgärder.
- Larm kan behöva installeras i fönster som ligger i markplan eller är lätt åtkomliga från angränsande tak eller på annat sätt.
- Särskilda arkiv (datamediaskåp, magnetbandsarkiv) måste finnas för förvaring av datamedier. Observera att datamedier inte kan förvaras i vanliga kassavalv, kassaskåp eller säkerhetsskåp, eftersom de dels är mycket värmekänsliga, dels lätt skadas av vissa gaser som utvecklas vid brand. Datamedier på vilka känslig information lagras måste förvaras på ett sådant sätt, att man har såväl fullgott brandskydd som inbrottsskydd av hög klass.
- Datorer som används för bearbetning av sekretessbelagd eller annan känslig information, måste också placeras med tanke på risken för avlyssning av röjande signaler. Även de terminaler som används vid arbete med sådant material måste skyddas mot avlyssning.

Även när det gäller många byggnadstekniska skyddsåtgärder måste de, för att få full effekt, kompletteras med administrativa skydd. Det är exempelvis föga meningsfullt att ha tillträdesvägar larmade, om personalen kopplar bort larmen, därför att man tycker att det är lättare att arbeta om dörrarna står öppna. De tekniska åtgärderna måste alltså kompletteras med instruktioner, regler för handhavande o.s.v.

13.1.2 Miljöskydd

Byggnadstekniska åtgärder i form av installation av brandsläckningsutrustning, brandlarm, vätskelarm o.s.v., ska vidtas i den om-

fattning som krävs för olika driftmiljöer. Detsamma gäller åtgärder som rör inredning, byggnadsmaterial, försörjningssystem, som inte hänförs till det IT-tekniska området m.m:

- Särskild brandsläckningsutrustning kan behöva anskaffas till kontorslokaler där persondatorer finns. Även en mindre brand kan ge rökskador på datamedier och datorer.

- För att skydda utrustningen mot t.ex. rökskador vid en brand i angränsande kontorsutrymmen bör man se till att dörrar och väggar håller en godkänd brandklass. Man bör också se till att rök inte kan tränga in via ventilationssystem och liknande. Datorer och lagringsmedier skadas nämligen mycket lätt av de gaser som utvecklas i samband med en brand.

- Om det finns risk för vattenläckage i datorrummet, eller i nära anslutning till detta, kan man behöva installera golvbrunnar för att förhindra vattenskador på utrustningen.

- Många störningar i IT-system förorsakas av brister i elförsörjningen. Överbelastningar i elnätet kan förorsaka problem och likaså kan en felaktig placering av olika utrustningsenheter förorsaka störningar som medför tillfälliga driftstopp. Alla datorutrustningar bör ha någon form av skydd mot tillfälliga avbrott i elförsörjningen. Även om man inte har behov av komplett reservkraft, underlättar t.ex. en batteribackup, d.v.s. reservbatterier som vid behov automatiskt träder i funktion, och återupptar driften efter ett strömavbrott. En oplanerad och plötslig systemnedgång medför i allmänhet ingen direkt skada på utrustningen, men förorsakar ofta problem när driften ska återupptas igen. Den här typen av skydd kan i dag fås till en rimlig kostnad och bidrar i hög grad till en bättre driftmiljö.

- De utrymmen där man förvarar kopior på program och register kan behöva någon form av klimatreglering, eftersom lagringsmedier har vissa krav på temperaturer och luftfuktighet.

13.1.3 RÖS, EMP

Alla typer av datorutrustning, som alstrar eller överför information, kan behöva särskilt skydd mot s.k. röjande signaler, RÖS. All

elektrisk utrustning alstrar elektromagnetiska signaler, som kan uppfattas och tolkas i omgivningen. Det är i allmänhet dessa signaler vi avser när vi talar om RÖS. Att här närmare beskriva de olika typer av RÖS som kan vara aktuella i IT-sammanhang skulle föra för långt, men alla användare av IT bör vara medvetna om att RÖS kan alstras i alla slag av datorer och datorenheter, inklusive bildskärmar, tangentbord, skrivare och kommunikationsledningar.

Avlyssning av RÖS är mer eller mindre komplicerad och kräver olika typer av utrustning. Enklast att avlyssna är video-rös, d.v.s. de signaler som alstras i en dataskärms bildgenerator. De kan vara ”strålande” eller ledningsbundna. Beroende av typ av terminal och miljö kan signalerna uppfångas på varierande avstånd.

De strålande signalerna kan fångas upp med hjälp av en antenn och en mottagare. I mycket gynnsamma fall kan en modifierad TV tjäna som mottagare. De ledningsbundna signalerna fångas upp genom fysisk inkoppling på någon ledare, t.ex. elledning, och med samma typ av mottagare.

För att skydda sig mot RÖS kan vissa IT-tekniska och byggnadstekniska åtgärder vidtas. Till de IT-tekniska räknar vi de skydd som kan byggas in i terminaler och annan IT-utrustning. Även kraftledningar kan skyddas genom t.ex. avstörningsfilter. Ett gott skydd ger även de fiberoptiska kablar som blir allt vanligare vid åtminstone intern kommunikation.

EMP

EMP, elektromagnetisk puls, är en typ av strålning som uppstår vid t.ex. blixtnedslag eller atomsprängningar. Ämnet är alltför komplicerat för att utvecklas här, men vi vill nämna problemet, eftersom risken för att en datorutrustning ska slås ut av en EMP är betydligt större än man trodde för några år sedan. Bl.a. är det fullt möjligt att framkalla denna effekt på ett ganska enkelt sätt. De organisationer som bedömer att man skulle kunna utsättas för avsiktliga angrepp bör vidta byggnadstekniska åtgärder i samband med t.ex. nyinstallation av datorutrustning. Det bör här påpekas att ett full-gott EMP-skydd även ger ett gott RÖS-skydd.

13.1.4 Kabeldragning

De byggnadstekniska skyddsåtgärderna avser även åtgärder som rör kabelteknik och kabeldragning. Vi talar här i första hand om installation av interna nät.

Generella kabelsystem är resultatet av en idé som bygger på att datakablar är en del av byggnaden och inte av systemet. Det har visat sig att kablaget blir väsentligt lättare att underhålla om installationen föregås av en grundlig analys.

Samma kabel ska fungera tillsammans med olika datorfabrikat och gå att anpassa till flera nätprinciper, terminaltyper och kommunikationsstandarder, vilket i sig medför ett leverantörsoberoende.

Generella kabelsystem sänker inte materialkostnaderna. En tumregel vid projekteringen är snarare att varje arbetsplats ska förses med minst ett vägguttag, oavsett om det för tillfället finns något direkt behov av en datanätanslutning. Arbetet med kabelläggning i spridningsnätet görs på detta sätt endast en gång och innebär givetvis en hög initialkostnad. Detta ska emellertid vägas mot att ändringar i nätet kan elimineras under hela kabelns livslängd, cirka 15 år.

Spridningsnätet kan installeras med skärmade eller oskärmade kablar. Skärmad kabel kostar nästan dubbelt så mycket som oskärmad, men tar å andra sidan mindre plats och är lättare att installera, eftersom man slipper bekymra sig för jordning. Oskärmad kabel ger större räckvidd i bussnät av Ethernettyp. Skärmad kabel tillåter snabbare trafik och vissa typer av lokala nät kräver skärmad kabel. Skärmad kabel ger också bättre skydd mot störningar och avlyssning.

Samtidigt som man bör skydda alla typer av ledningar mot avsiktlig och oavsiktlig åverkan och andra hot, bör de placeras så att de är lätta att komma åt vid service och i samband med att fel uppträder. För driftansvariga är det också viktigt att veta hur alla ledningsdragningar är gjorda, om det blir aktuellt med kompletteringar av t.ex. det interna kommunikationsnätet.

Skydd av kopplingspunkter

Dataöverföring över telelinje berör ofta både IT-systemägares och en särskild telenätägares ansvarsområden. Det fysiska gränssnittet mellan ansvarsområdena markeras kanske av kopplingsskåp eller liknande utrustning. Sådana kopplingspunkter är sårbara för t.ex. fysisk åverkan eller avlyssning.

Det förhållandet att utrustningen befinner sig i gränszonen mellan ansvarsområden kan leda till att det uppstår oklarheter eller missförstånd om vem som ska upprätta erforderligt skydd för utrustningen. Det är därför angeläget att ta med sådana här kopplingspunkter på den ”checklista” eller liknande, som man lämpligen använder i säkerhetsarbetet.

13.2 Specifika skydd

13.2.1 Stordator

De byggnadstekniska skyddsåtgärder som måste vidtas i anslutning till en stordator eller stordatorliknande installation är normalt betydligt mer omfattande än i servermiljö. Ska datorn placeras i en byggnad som redan finns kan ombyggnadskostnaderna bli mycket höga, och vissa skyddsåtgärder kan till och med vara svåra att genomföra. Vid nybyggnad är det lättare att ta hänsyn till de olika krav som kan ställas, exempelvis vad avser skydd av olika försörjningssystem, indelning av driftmiljön i olika tillträdeszoner och brandzoner, placering av själva datorhallen i huskroppen, skydd av olika tillträdesvägar för personal och transporter.

Byggnadstekniska skyddsåtgärder i stordatormiljöer är, liksom de IT-tekniska skyddsåtgärderna, en fråga för experter. För den byggnadstekniska delen finns för myndigheterna vissa normer angivna.

När det gäller IT-tekniska skyddsåtgärder avseende datorutrustning och olika försörjningssystem, blir dessa givetvis mer omfattande i en stordatormiljö än i servermiljöer. Vi ger här bara ett exempel. Det är hämtat från ett område, där det fortfarande även inom stordatormiljöer kan finnas brister.

Det måste finnas ett fullgott skydd mot avbrott i elförsörjningen. Eftersom en oplanerad nedgång i ett stordatorsystem kan förorsaka flera timmars driftavbrott, även om elavbrottet bara varar någon minut, är en batteribackup som klarar 10–15 minuters eltillförsel en minimiskyddsåtgärd i stordatormiljön. Om man tror att ett avbrott ska bli långvarigt, har man då tid att avsluta pågående bearbetningar under ordnade former vilket underlättar återstarten.

En stordatorinstallation är också starkt beroende av en god förebyggande service på utrustningen och på de larmsystem som är anslutna till utrustningen.

13.2.2 Nät

Sammankoppling av persondatorer i nät kräver i regel också särskilda byggnadstekniska åtgärder. Sådana kan motiveras, inte bara av att en större mängd information hanteras och att fler användare berörs, utan också av att man i nät ofta har ganska kraftfulla gemensamma resurser i form av skivminnen och skrivare.

Den persondator som utgör huvudmaskin, liksom övriga gemensamma resurser, bör placeras avskilt. Rummet bör hållas låst, och man kan behöva byta ut dörrar för att få högre motståndskraft mot brand. Endast den som är nätansvarig bör ha tillträde till rummet. Det kan också i vissa fall vara motiverat med detektorer som larmar vid brand. Dörr- och väggkonstruktioner samt ventilationssystem bör vara sådana, att utrustningen inte omedelbart skadas av värme, rök eller gas vid en brand i angränsande lokaler.

Servrar

Hur stor omfattningen är av de byggnadstekniska skyddsåtgärder som behöver vidtas i en servermiljö styrs av många olika faktorer, bl.a. hur stor installationen är och hur känslig den information är som bearbetas i systemet.

I servermiljöer, där känslig information bearbetas eller i mycket komplexa servermiljöer, kan det krävas ytterligare byggnadstekniska skyddsåtgärder. Det kan exempelvis vara nödvändigt att avskärma datorrummet för att eliminera risken för avlyssning av

röjande signaler från utrustningen, vilket förekommer inom försvaret. Det kan också krävas installation av särskild utrustning i anslutning till datorrummet för att kontrollera in- och utpassering.

Servrar kan liksom stordatorer behöva någon form av kylanläggning, och det bör finnas larmsystem som signalerar när temperaturen i datorrummet blir så hög, att det finns risk för att någon del av utrustningen ska skadas. Ett annat alternativ är att ha automatisk nedtagning och avstängning av systemet om larmet slår till. Vidare kan det även i en servermiljö vara nödvändigt att reglera luftfuktigheten. Om man installerar någon form av utrustning för det ändamålet bör även den vara försedd med någon typ av larm.

Vid mindre serverinstallationer kan det vara en överdriven skyddsåtgärd att installera automatisk brandsläckningsutrustning. Rökdetektorer bör emellertid finnas i datorlokalen och även i det rum där t.ex. skrivare är placerade. Handbrandsläckare ska finnas lätt tillgängliga och personalen ska veta hur de används.

Det är inte ovanligt att man förvarar kopior på program och register i vanliga plåtskåp eller, om man har känslig information, i s.k. säkerhetsskåp. Även om skyddet mot stöld, avsiktlig förstöring m.m. är fullgott skyddar inte dessa skåp mot brand och rökskador. Alla typer av lagringsmedier måste förvaras i särskilda datamediaskåp eller i särskilda rum, som har samma motståndskraft mot värme och rök som datamediaskåpen har.

Helst bör själva datorn också vara placerad åtskild från skrivare och operatörsterminaler. Särskilt om de system som körs på datorn producerar stora mängder utdata på papper till många olika mottagare, finns det flera anledningar till att utskriftsfunktionerna bör avskiljas från själva datorrummet. En anledning är att en av de vanligaste orsakerna till bränder i datacentraler är antändning av skrivarutrustning, på grund av att t.ex. pappersdamm fattat eld. När man väljer lokal för sin dator är det också viktigt att tänka på, att det inte finns vatten- eller avloppsledningar som kan läcka in i lokalen.

Givetvis ska de rum där man placerar datorer och kringutrustning hållas låsta och endast vara tillgängliga för den personal som ansvarar för driften av datorn.

13.2.3 Fristående persondatorer

Installation av ett stort antal persondatorer innebär ganska stora investeringar. Man bör således kontrollera om det kan vara motiverat att göra det svårare för utomstående att komma in i lokalerna. Också risken för att obehöriga ska komma åt information kan motivera särskilt tillträdesskydd. Behovet av byggnadstekniska åtgärder för det ändamålet hänger samman med vilka IT-tekniska skyddsåtgärder som har vidtagits.

Det kan också ofta vara motiverat med en utökning av antalet handbrandsläckare. Dessa bör vara tydligt utmärkta och personalen ska veta hur de ska hanteras.

Beroende på hur känslig den information är som bearbetas i systemet, och riskerna för att någon utomstående skulle vilja skada verksamheten, kan ytterligare skyddsåtgärder behövas. Så kan exempelvis RÖS-skydd och förstärkt tillträdesskydd vara motiverade även i den här typen av datormiljö.

För att förhindra stöld bör man inte placera persondatorer i utrymmen där det är svårt att ha kontroll över utrustningen. Inte heller bör man placera datorer intill fönster i markplan, om dessa fönster ligger så att det är lätt att slå sönder dem och bära bort utrustningen. Om det är svårt att placera utrustningen skyddat, kan man se till att den sätts fast i ett bord, eller på annat sätt göra det svårt att flytta den.

Eftersom mycket av den information och de program som används i persondatorer finns på hårddiskar eller på disketter, ofta i anslutning till arbetsplatserna, är det viktigt att förhindra att dessa stjäls eller förstörs. Det bör således finnas låsbara förvaringsskåp för lagringsmedier, så att dessa kan låsas in när ingen är i rummet. Likaså måste man se till att hårddiskar och disketter inte utsätts för alltför hög värme, vattenläckage, vätskespill, magnetism eller annan åverkan som kan göra dem obrukbara.

För att undvika driftavbrott på grund av störningar i elförsörjningen bör man ha t.ex. någon form av batterireserv, som medger att systemet stängs av under kontrollerade former vid elavbrott.

Några mer omfattande byggnadstekniska skyddsåtgärder brukar inte vara nödvändiga om man enbart har fristående persondatorer.

14 Standardiseringsarbetet inom IT-säkerhetsområdet

I kapitlet summeras väsentliga delar av sådant standardiseringsarbete som har direkt eller indirekt betydelse för IT-säkerhet. Standardiseringsarbetet är i sig mycket rörligt vilket innebär att läsaren själv bör verifiera eller efterforska den senast utvecklingen inom de olika områden som behandlas i avsnittet. Detta för att utröna vilken status arbete har och vilken roll det spelar för den egna organisationen.

Mycket av innehållet i detta kapitel är hämtat från SIS och ITS webbservrar.

14.1 Standardiseringens syfte

Syftet med standardisering är att förenkla verksamheter i samhället. Det förutsätter därför samarbete och samförstånd mellan företrädare för producenter, konsumenter, handel och olika samhällsintressen. Det förutsätter också att dessa deltar aktivt i arbetet genom att satsa resurser och kunnande samt har erfarenhet och internationell överblick inom sina respektive fackområden.

Standardisering avser att tillgodose behov och önskemål från många olika parter och att så långt möjligt möta samtliga intressen.

Vid standardisering vägs tekniska, sociala, ekonomiska och andra aspekter samman så att resultatet blir lösningar som stärker konkurrenskraft, öppnar marknader, främjar kvalitet och säkerhet och erbjuder olika parter en gemensam bas för vidare utveckling.

De flesta standarder kommer fram i samarbete mellan experter från hela världen. Dessa experter representerar både producenter och konsumenter. Standardiseringsprocesserna kan vara mycket segdragna och tar ibland flera år. För en internationell standard är den genomsnittliga tiden, från koncept till färdig publicerad standard, tre år. Det är därför ganska vanligt att man måste börja använda

standarder innan de har blivit officiellt antagna förutsatt att standarden är relativt stabil.

I IT-säkerhetsarbetet är det viktigt att man i så stor utsträckning som möjligt använder och efterfrågar befintliga standarder. Detta gäller även om standarden inte explicit behandlar säkerhetsproblematiken. Att följa standarder garanterar i de flesta fallen långsiktig, kompatibilitet och kvalitet. Det är också viktigt att så långt möjligt sätta sig in i det långsiktiga standardiseringsarbete, så att man inte väljer lösningar, som i onödan försvårar anslutning till kommande standarder, och därmed minskar möjligheterna till kommunikation med andra IT-system.

Standardisering bidrar till skapandet av ”öppna”, lättillgängliga system. Standarder underlättar för aktörerna på marknaden. Systembeställaren behöver inte bli leverantörsberoende och leverantörer behöver inte skräddarsy sina lösningar varje gång ny teknik utvecklats.

14.2 Standardiseringsorgan

Internationell standardisering sker både globalt för hela världen och europeiskt för Västeuropa. IEC (International Electrotechnical Commission) svarar för den globala standardiseringen inom elområdet. ISO (International Organization for Standardization), svarar för den globala standardiseringen inom övriga områden. Tre organisationer svarar för det västeuropeiska standardiseringsarbetet: CENELEC (European Committee for Electrotechnical Standardization) på elområdet, ETSI (European Telecommunications Standards Institute) på telekommunikationsområdet och CEN (European Committee for Standardization) för övriga områden. De närmaste åren prioriteras gemensamma europastandarder för EUs inre marknad och för att undanröja tekniska handelshinder mellan länderna i Europa. Ett av de särskilt viktiga områden som man har identifierat är just säkerhet. En stor del av det västeuropeiska standardiseringsarbetet bygger på internationella standarder.

Sverige deltar aktivt såväl i det globala som i det västeuropeiska standardiseringsarbetet.

Nedan följer ett antal relevanta standardiseringsorgan som bl.a. arbetar med frågor kring IT-säkerhet.

14.2.1 ISO och IEC

Den internationella standardiseringsorganisationen ISO, International Organization for Standardization, svarar för global standardisering inom alla områden utom det elektrotekniska området, telekommunikationsområdet och vissa specialområden inom livsmedel.

ISO är en sammanslutning av nationella standardiseringsorgan som svarar för standardisering och fastställande av standard i respektive land. ISO har endast en medlem från varje land. Svensk ISO-medlem är SIS. ISO har ca 110 medlemmar.

ISO har nära samarbete med den elektrotekniska standardiseringen inom IEC, International Electrotechnical Commission, med telekommunikationsstandardiseringen inom Internationella Teleunionen, ITU, med CEN samt med andra internationella organisationer.

Standardiseringsarbetet, d.v.s. utarbetande av internationell standard, sker i tekniska kommittéer (Technical Committees, TC), underkommittéer (Sub-Committees, SC) och arbetsgrupper (Working Groups, WG).

Det tekniska arbetet inom ISO resulterar i 600-700 nya och reviderade ISO-standarder om året.

Överföring av internationell standard till nationell standard är frivillig för medlemsorganisationerna. Dock förväntas medlemsländerna acceptera och överföra sådan ISO-standard som man röstat ja till. Sverige har varit mycket trogen mot ISO och överför normalt ISO-standard till svensk standard. En mycket stor andel svensk standard är därför baserad på och överensstämmande med internationell standard.

ISO och IEC har från den 1 februari 1990 gemensamma regler för det tekniska standardiseringsarbetet och för utformningen av internationell standard.

För standardisering inom informationsteknikområdet svarar ISO/IEC Joint Technical Committee 1, JTC1, för vilken ITS svarar för det svenska engagemanget. JTC1 har över 100 underkommittéer och arbetsgrupper, varav ett flertal arbetar med informationssäkerhet. ISO och IEC arbetar alltså tillsammans kring dessa frågor.

IEC arbetar annars främst med frågor som rör elektriska och elektroniska områden.

14.2.2 ITU

The International Telecommunication Union, ITU är en internationell organisation som arbetar med standardiseringen av telekommunikation och radiokommunikation. Syftet med arbetet är bland annat att bibehålla och dessutom utveckla det internationella samarbetet mellan medlemmarna i ITU för att förbättra det rationella användandet av telekommunikation.

14.2.3 CEN

Den västeuropeiska standardiseringsorganisationen CEN, European Committee for Standardization, svarar för västeuropeiskt standardiseringsarbete inom alla områden utom elektroteknik och telekommunikation.

Dokument som CEN tar fram kan vara:

- europeiska standarder, *EN*
- för-standarder, *ENV*
- harmoniseringsdokument, *HD.*

EN standarder ska ikraftsättas som svensk standard om inte mycket starka t.ex. legala skäl ligger till grund för annat. En EU norm, d.v.s. en EN-standard är tvingande vid offentlig upphandling av konkurrensskäl.

Många standarder från ISO/IEC inom IT-säkerhetsområdet har CEN givit ut som EN.

CEN består av de centrala nationella standardiseringsorganen i samtliga EU- och EFTA-länder. Svensk medlem i CEN är SIS. CEN har även ett antal ”affilierade” medlemmar i central- och Östeuropa.

CEN bildades 1961 som ett samarbetsorgan mellan standardiseringsorganen i Västeuropa. Uppgiften var bl.a. att utarbeta europeisk standard inom de områden där det inte pågick något internationellt arbete.

CEN finansieras i huvudsak genom medlemsavgifter och uppdrag från EG och EFTA.

Standardiseringsarbetet inom CEN bedrivs i över 1 000 tekniska kommittéer och arbetsgrupper för i stort sett alla fackområden utom elektroteknik och telekommunikation.

För europeiskt standardiseringsarbete inom telekommunikationsområdet svarar ETSI, European Telecommunications Standards Institute.

Den standardiseringsverksamhet som tidigare bedrivits inom teleförvaltningarnas europeiska samarbetsorganisation CEPT överfördes till ETSI våren 1988. Syftet var bl.a. att öppna deltagandet i standardiseringsarbetet för tillverkare, användare, nätoperatörer och andra.

ETSI är teleförvaltningar, tillverkare, användare, nätoperatörer, forskningsinstitutioner och standardiseringsorgan. Vid röstning om fastställande av Europastandard och i andra frågor där det krävs nationell röstning svarar ITS för den svenska rösten.

ETSI har till uppgift att utarbeta och fastställa europeisk telekommunikationsstandard, betecknad ETS, tillfällig telekommunikationsstandard, betecknad I-ETS, samt underlag (TBR) till obligatorisk standard (CTR) för anslutning till telenäten.

Arbetet sker inom kommittéer. Dessutom tillsätts administrativa grupperingar när sådana behov finns.

På global nivå samarbetar ETSI med ITU (Internationella Teleunionen) och andra regionala telestandardiseringsorganisationer på andra kontinenter.

14.2.4 IETF

Internet Engineering Task Force ansvarar för Internet-standarder. Medverkan i IETF grundas på individuella tekniska bidrag och inte på formella representanter från t.ex. nationella standardiseringsorgan.

Det finns två typer av Internet dokument, dels s.k. Internet-Drafts och dels Request for Comments (RFCs). Internet-Drafts har ingen formell status och kan förändras när som helst. Ett sekretariat har dock ett register där alla Internet-Drafts registreras. RFCs är officiella dokument och arkiveras för all framtid och efter det att en RFC blivit publicerad som standard får den inte förändras.

RFCs är arkiverade dokument som kan ha olika status i sig, d.v.s. de kan vara:

- Proposed Standard – Specifikationen ska först och främst vara komplett och trovärdig dessutom ska det gå att bevisa och demonstrera dess användbarhet.

  I detta läge ska en specifikation befinna sig i mellan sex månader till två år för att bevisa sin överlevnadspotential. Efter denna period går man antingen vidare på något sätt eller så lägger man ner förslaget.

- Draft Standard – Flera oberoende men inbördes kompatibla implementationer ska finnas som bygger på specifikationen och bevis ska finnas för att implementationer fungerar bra.

  I detta läge ska specifikationen befinna sig i minst fyra månader dock inte längre än två år. Efter denna period går man antingen vidare på något sätt eller så lägger man ner förslaget.

- Standard – Specifikationen och gjorda implementationer ska ha visat en funktionell stabilitet under en lång tid, d.v.s. lösningen ska ha framtidsutsikter.

14.2.5 OECD

OECD (Organisation for Economic CO-operation and Development) arbetar i ett fler-tal kommittéer. En sådan kommitté är ICCP (Information Computer Communications Policy). ICCP har bl.a.

tagit fram ett dokument ”Guidelines for the Security of Informations Systems” som blivit antaget av de 24 medlemsländerna.

14.2.6 SIS och ITS

SIS (Standardiseringen i Sverige) ska vara centralorgan och samordna arbetet inom svensk standardisering.

En av de viktigaste uppgifterna för SIS är att vara medlem i de internationella standardiseringsorganisationerna ISO och CEN. SIS ska företräda Sverige, direkt eller indirekt, i de internationella standardiseringsorganen, auktorisera standardiseringsorgan med ansvar för standardisering inom sitt fackområde (sin bransch), fastställa svensk standard, utge och sälja svensk standard samt verka för användning av standarder.

ITS – Informationstekniska standardiseringen är auktoriserat av SIS för standardisering inom det informationstekniska området.

ITS har till uppgift att:

- fungera som nationellt standardiseringsorgan för IT-området i Sverige och bereda svenskt ställningstagande i nordisk, europeisk och global standardisering samt att därvid påverka prioritering och utformning av internationell standard
- sprida kännedom och kunskap om befintlig standard på IT-området
- ta fram svensk IT-standard när den behövs (främst genom överföring av internationell standard och undantagsvis, när speciella skäl föreligger, genom utveckling av särskild svensk standard med huvudinriktning på deltagande i internationell IT-standardisering)
- samordna svenska insatser, samla svenska insatser till områden där de ger störst effekt samt sträva efter att vidmakthålla svenska resurser på en rimlig nivå
- fungera som samordnande organ i Sverige för provning och certifiering på IT-området

- underhålla en strategisk plan som är förenlig med den internationella utvecklingen
- utforma och genomföra årliga verksamhetsplaner, vars mål är relaterade till den strategiska planen.

ITS är en ideell förening med informationsteknikens alla parter som intressenter. Tillsammans deltar parternas experter och ITS i det nationella, europeiska och internationella standardiseringsarbetet.

IT-området indelas i ett antal arbetsområden som vart och ett representeras av en arbetsgrupp inom ITS. Exempel på arbetsområden är:

- datakommunikation (OSI, protokoll, funktionsstandard)
- telekommunikation (gränssnitt, digitala flertjänstnät, radiosystem som GSM, DECT och TETRA)
- informationsskydd och -säkerhet, (kryptering)
- dataorganisation, regler för dataelement, elektroniskt informaionsutbyte (EDI)
- transaktionskort (identifieringskort, aktiva kort)
- lagringsmedier (disketter, magnetband)
- datarepresentation (teckenkoder)
- textbehandling (dokumentstrukturer, meddelandehantering)
- streckkoder
- terminologi
- lands- och valutakoder.

ITS är medlem i ETSI, där arbetsuppgiften är att föra fram och samordna svenska ställningstaganden i samband med röstningar. ITS ansvarar också för viss nationell koordinering av Internationella Teleunionens (ITU) standardiseringsarbete.

ITS ansvarar för kontakterna med ISO/IEC JTC 1 ”Information Technology” och ISO/TC 68 ”Banking and related financial services”. ITS ansvarar också för CENs IT-säkerhetsarbete inom bl.a. aktiva kort.

14.3 Var får man tag i information om standardiseringen

Från ITS som beskrivs ovan kan man får mer information om befintlig och pågående standardisering vad gäller informationsteknik, inklusive telekommunikation.

ITS
Electrum 235
164 40 KISTA
Besöksadress: Isafjordsgatan 26, C 6

Telefon: 08 – 793 90 00
Telefax: 08 – 751 53 63
Internet:info@its.se
http://www.its.se/

Information om standardiseringen kring Internet kan man få på IETF's hemsida, http://www.ietf.org (december 1997).