

Informationssäkerhet och arbetsrätt vid distansarbete – en studie av framtida distansarbete inom Försvarsmakten

Ina Nordqvist

Magisteruppsats¹
Institutionen för Data- och Systemvetenskap, DSV
Stockholms Universitet
April 1997

Sammanfattning

I likhet med många andra organisationer har anställda inom Försvarsmakten ett önskemål om att arbeta på annan plats än på kontoret. Om detta önskemål realiseras blir ett antal frågor aktuella, bland annat hur distansarbete påverkar informationssäkerhet och juridiska frågor. Försvarsmakten av idag saknar riktlinjer för hur distansarbete ska hanteras av arbetsgivaren och av arbetstagaren.

Detta arbete har kartlagt dels hur en god informationssäkerhet uppnås när en arbetstagare arbetar på distans och dels hur förutsättningarna för arbetsrätten och andra juridiska frågor påverkas vid distansarbete.

Utifrån genomförd kartläggning formulerades riktlinjer för handhavande av säkerhetstekniska lösningar och för aktuella lagar. Dessa riktlinjer kan summeras kortfattat; individuella avtal ska skrivas om de juridiska frågorna och hur parterna ska agera för att erhålla god informationssäkerhet, skriv riktlinjer för säkerheten och följ sedan dessa, ha tydlig ansvarsfördelning för tekniken och informationen i organisationen. Slutligen, ifrågasätt om alla arbetsuppgifter verkligen bör skötas från en distansarbetsplats.

¹ Denna uppsats motsvarar tjugo poäng

Förord

När sommaren 1996 började närma sig sitt slut träffade jag major Ulf Berglund. Han gjorde det då möjligt för mig, att som pionjär, skriva denna första magisteruppsats inom Försvarsmakten. Efter diskussioner enades vi om hur informationssäkerhet vid distansarbete skulle komma att behandlas. Jag vill här rikta ett tack till Ulf för Dina synpunkter under arbetet och för att Du var min länk in till Försvarsmaktens korridorer.

I ett mycket tidigt stadium av uppsatsskrivandet fick jag kontakt med avdelningsdirektören på Försvarsmaktens personalavdelning; Henrietta Göbel. Jag riktar min tacksamhet till Henrietta för Dina kommentarer och för Din ovärderliga förmedling av kontakter.

Jan Häggström på arbetsgivarverket vägledde mig i min kartläggning av hur de juridiska frågorna påverkas när en arbetstagare arbetar på distans. Jan är en man med gedigna kunskaper i området. Dessa kunskaper delar han gärna med sig av, Jan får på detta sätt ta del av min tacksamhet för detta.

Under arbetet med detta examensarbete har jag träffat och i olika omfattning pratat med anställda på enheter av Försvarsmakten. Utan att nämna någon vid namn, ska ni veta att jag uppskattar att ni tog er tid för mina frågor. Jag vill även rikta ett speciellt tack till alla företag och organisationer som jag har haft kontakt med under arbetets gång.

Sist, men absolut inte minst, vill jag rikta min uppskattning till min handledare Louise Yngström som upprepade gånger har läst igenom delar av uppsatsen och returnerat ett kommenterat exemplar.

Stockholm, april 1997

Ina Nordqvist

Innehållsförteckning

| | |
|--|-----------|
| SAMMANFATTNING | 1 |
| FÖRORD | 3 |
| 1. INLEDNING | 7 |
| 1.1 Bakgrund | 7 |
| 1.2 Problem | 7 |
| 1.3 Syfte | 7 |
| 1.4 Avgränsningar | 7 |
| 1.5 Metod | 8 |
| 1.6 Arbetssätt | 8 |
| 1.7 Disposition | 8 |
| 2. SÄKERHETSOMRÅDET—EN ÖVERSIKT | 9 |
| 2.1 Inledning | 9 |
| 2.2 Informationssäkerhet | 9 |
| 2.2.1 Definition | 9 |
| 2.2.2 Integritet | 10 |
| 2.2.3 Sekretess | 10 |
| 2.2.4 Tillgänglighet | 10 |
| 2.3 Säkerhetsfunktioner | 10 |
| 2.3.1 Behörighetskontroll | 10 |
| 2.3.2 Autenticering | 11 |
| 2.3.3 Åtkomstkontroll | 11 |
| 2.4 Säkerhetsfunktioner och -tekniker | 11 |
| 3. DISTANSARBETETS OLIKA FASSETTER | 12 |
| 3.1 Definitioner av distansarbete | 12 |
| 3.2 Typer av distansarbete | 13 |
| 3.3 Aktuella lagar | 13 |
| 3.3.1 Arbetsmiljö | 13 |
| 3.3.2 Arbetsskador | 14 |
| 3.3.3 Arbetstid | 14 |
| 3.3.4 Anställningstrygghet | 14 |
| 3.3.5 Semesterfrågor | 14 |
| 3.3.6 Skattefrågor | 14 |
| 3.3.7 Hyreslagen | 15 |
| 3.3.8 Försäkringsfrågor | 15 |
| 3.4 Aspekter för och emot distansarbete | 15 |
| 3.4.1 Fördelar för arbetstagaren | 15 |
| 3.4.2 Nackdelar för arbetstagaren | 16 |
| 3.4.3 Fördelar för arbetsgivaren | 16 |
| 3.4.4 Nackdelar för arbetsgivaren | 16 |
| 4. INFORMATIONSSÄKERHET OCH DISTANSARBETE | 17 |
| 4.1 Inledning | 17 |
| 4.2 Hot | 17 |
| 4.2.1 Informationsläckage | 17 |
| 4.2.2 Integritetsförlust | 18 |
| 4.2.3 Funktionsförlust | 18 |
| 4.2.4 Obehörigt användande | 18 |

| | |
|--|-----------|
| 4.3 Informationssäkerhet och hot | 18 |
| 4.3.1 Inledning | 18 |
| 4.3.2 Integritet | 19 |
| 4.3.3 Sekretess | 19 |
| 4.3.4 Tillgänglighet..... | 20 |
| 4.4 Tekniska lösningar | 20 |
| 4.4.1 Kryptering..... | 20 |
| 4.4.2 Digital signatur | 21 |
| 4.4.3 Kryptografisk kontrollsumma | 22 |
| 4.4.4 Behörighetskontroll | 22 |
| 4.4.5 Autenticering..... | 22 |
| 4.4.6 Åtkomstkontroll | 23 |
| 4.4.7 Loggning | 23 |
| 4.4.8 Tekniker som hindrar obehöriga användare..... | 23 |
| 4.5 Tillämpning av tekniska lösningar | 25 |
| 4.5.1 Inledning | 25 |
| 4.5.2 Fysisk säkerhet | 25 |
| 4.5.3 Säkerhet och persondatorn | 26 |
| 4.5.4 Säkerhet i nätverk..... | 27 |
| 5 RIKTLINJER FÖR DISTANSARBETE | 28 |
| 5.1 Inledning | 28 |
| 5.2 Riktlinjer för lagarna | 29 |
| 5.2.1 Arbetsmiljö | 29 |
| 5.2.2 Arbetsskador | 29 |
| 5.2.3 Arbetstid och tillgänglighet | 29 |
| 5.2.4 Anställningstrygghet | 30 |
| 5.2.5 Semesterfrågor | 30 |
| 5.2.6 Skattefrågor..... | 30 |
| 5.2.7 Hyreslagen | 30 |
| 5.2.8 Försäkringsfrågor | 30 |
| 5.3 Riktlinjer för tekniken | 31 |
| 5.3.1 Fysisk säkerhet | 31 |
| 5.3.2 Säkerhet och persondatorn | 32 |
| 5.3.3 Säkerhet i nätverk..... | 33 |
| 5.4 Riktlinjer för övriga frågor..... | 35 |
| 5.4.1 Beslutsfattare..... | 35 |
| 5.4.2 Arbetstagare | 36 |
| 6 SLUTSATSER | 36 |
| 6.1 Resultat | 36 |
| 6.2 Diskussion | 38 |
| 6.3 Framtida arbete | 38 |
| REFERENSER | 39 |
| Litteratur | 39 |
| Personer..... | 40 |
| BILAGEFÖRTECKNING | 40 |
| Bilaga 1 Avtal AMS (5 sidor) | |
| Bilaga 2 Avtal från SIG Security's årsbok 1996 (2 sidor) | |
| Bilaga 3 Avtal Siemens Nixdorf (7 sidor) | |
| Bilaga 4 Avtal Telia (4 sidor) | |
| Bilaga 5 Avtal Utrikesdepartementet (3 sidor) | |

1. Inledning

1.1 Bakgrund

Det är ingen ny företeelse att människor distansarbetar från till exempel hemmet. Journalister, forskare, författare och konstnärer har ur ett historiskt perspektiv alltid kunnat arbeta på distans. Advokater, läkare och arkitekter har ofta haft sitt kontor eller sin praktik i bostaden och vid behov tagit sin verksamhet till den plats där kunden har funnits.

I och med att informationsteknologin utvecklas och nya möjligheter uppkommer får en ny grupp av yrkesutövare tillfälle att arbeta på distans. Den grupp av människor som nu kan arbeta på distans är de som är delaktiga i de dagliga kontorsgöromålen.

Inom många organisationer börjar de anställda att uttrycka ett önskemål om möjligheten att arbeta på annan plats än kontoret. Om detta önskemål ska realiseras blir ett antal frågor aktuella. Dessa frågor berör teknik (hårdvara, mjukvara och kommunikation), avtal, ergonomi, ekonomi, sociala frågor, arbetstid och arbetsmiljö.

Hur kan dessa frågor lösas med bibehållen informations- och datasäkerhet?

Denna frågeställning är aktuell även inom Försvarsmakten (FM). Anställda inom FM har önskemål om att kunna arbeta med dator på annan plats än ordinarie tjänstgöringsplats.

Den debatt som har förts i olika medier är i allmänhet mest inriktad på de tidsbesparande faktorerna, de sociala aspekterna och möjligheten till fria arbetstider. Under det sista kvartalet av 1996 började dock debatten att beröra de säkerhetsfrågor som blir aktuella i samband med distansarbete. Om den debatt som förs i media ska kunna resultera i konkreta lösningar av säkerhetsproblemen, måste debatten kring säkerhetsfrågorna intensifieras under 1997.

Distansarbete tillämpas redan inom delar av samhället och i viss begränsad utsträckning även inom FM. Krav på sekretesskydd gör dock att stora delar av FMs verksamhet för närvarande inte kan hanteras med hjälp av konventionellt distansarbete.

Kraven på minskat resande, svårigheter med återkommande krav på flyttning mellan olika arbets-

platser mm, gör dock att vissa arbetsuppgifter bör vara lämpliga att lösa med hjälp av distansarbete.

1.2 Problem

Organisationen saknar idag klara riktlinjer för att hantera distansarbete.

1.3 Syfte

Examensarbetet syftar till att beskriva de problem och möjliga lösningar som kan bli aktuella vid införandet av distansarbete på FM.

De problem och möjliga lösningar som kan komma att identifieras, är inte unika för FM. Problemen som uppkommer vid införande av distansarbete är oberoende av organisation.

För att kunna definiera och behandla aktuella frågor kring distansarbete kommer författaren att göra en kartläggning av relevanta delar ur det arbetsrättsliga området samt informations- och datasäkerhetsområdet.

Studien av arbetsrätten och informations- och datasäkerhet vid distansarbete kommer att resultera i en rapport som innehåller:

- Kartläggning av arbetsrätt och andra aktuella juridiska frågor samt informationssäkerhetsfrågor med relevans för distansarbete.
- Riktlinjer för införande och handhavande av distansarbete. Dessa riktlinjer riktar sig dels till beslutsfattare och dels till användare inom en organisation.

1.4 Avgränsningar

Detta arbete kommer endast ytligt att behandla fördelar och nackdelar med distansarbete (tidsbesparingar, arbetstider etcetera) samt sociala och ekonomiska frågor.

Arbetet kommer inte att behandla frågor om ergonomi eller ekonomiska konsekvenser av distansarbete.

I uppsatsen definierar författaren distansarbete i enlighet med arbetsgivarverkets formulering [Jan Häggström]: "Distansarbete råder när en enskild arbetstagare som enligt överenskommelse med arbetsgivaren utför sitt arbete utanför huvudarbetsplatsen, utan att arbetet kräver detta, samt omfattar minst en dag per vecka och kräver någon form av informationsteknik".

1.5 Metod

Arbetet med detta examensarbete har följt systemisk metod, vilken är en vidareutveckling av Systemsynsättet [Churchman 1968]. De system som denna uppsats kommer att beröra är det reella systemet, verkligheten, och en avbildning av denna verklighet—systemmodellen. Modellen består av ett antal komponenter vars relation till varandra och till modellens helhet kommer att undersökas. Helhetens relation till reella systemet kommer också att studeras.

Systemisk metod, särskilt inom informationssäkerhetsområdet [Yngström 1996] innebär att en kreativ fas mellan vad som är tekniskt möjligt och organisatoriskt önskvärt skapas som underlag för syntesen.

Metoden omfattar:

- Avgänsning av systemet som ska studeras—i mitt fall gällde det i första hand distansarbetet som sådant, dess förutsättningar, regler, erfarenheter från olika användarorganisationer med mera.
- Definiera systemets omgivning—i mitt fall gällde det arbetet och huvudarbetsplatsen, dess regler, förutsättningar, sociala omgivning, säkerhetskrav med mera.
- Strukturera säkerhets- och kontrollsystemet så att det kan hantera både inre och yttre hot och risker—i mitt fall gällde det framförallt upprättande av riktlinjer för införande och handhavande av distansarbete.

Uppsatsen är explanativ, det vill säga beaktar endast observerbara och refererbara aspekter av verkligheten [Arbnor et al 1994, s. 146]. Författaren har inte använt sig av experimentella studier [Arbnor et al 1994, s. 244].

1.6 Arbetsätt

För att kunna göra en kartläggning dels av säkerhetsområdet och dels de juridiska frågor som aktualiseras vid distansarbete inhämtades och sammanställdes fakta från litteratur och aktuella konferenser [Nordqvist 1996a, Nordqvist 1996b, Nordqvist 1996c].

Efter att ha skapat en förståelse inom de båda områdena kontaktades företag, myndigheter och föreningar som själva hade infört eller hade annan erfarenhet av distansarbete.

De företag som kontaktades var Telia och Siemens Nixdorf. De myndigheter som kontaktades var Arbetsgivarverket, Arbetsmarknadsstyrelsen, Försvarsmakten och Utrikesdepartementet.

Föreningar som kontaktades var SIG Security, Svenska Industriförbundet (SIF) och Tjänstemännens Centralorganisation (TCO).

Utifrån teoretiska kunskaper, genomförd kartläggning och material från de kontaktade företagen, myndigheterna och föreningarna, kunde föreslagna riktlinjer presenteras.

1.7 Disposition

I kapitel två görs en presentation av informationssäkerhetsområdet. Läsaren bekantas med delarna av informationssäkerhet och olika säkerhetstekniker. Förklaring ges av de säkerhetsspecifika termer som kommer att användas senare i rapporten. Presentationen bygger på den litteratur som författaren har läst.

I kapitel tre definieras distansarbete, ges exempel på olika typer av distansarbete och en snabb presentation av fördelar respektive nackdelar med distansarbete görs. Den huvudsakliga delen i kapitel tre är dock diskussionen kring de lagar som aktualiseras när en arbetstagare ska arbeta på distans.

Kapitel fyra ger först exempel på hot som kan finnas när distansarbete tillämpas inom en organisation. Dessa hot översätts sedan till informationssäkerhetens termer, det vill säga en återkoppling görs till kapitel två. Förklaring görs av de tekniska lösningar som kan skydda organisationen och distansarbetsplatsen från de identifierade hoten. Slutligen beskrivs hur de tekniska lösningarna praktiskt kan skydda mot de exemplifierade hoten.

I kapitel fem presenteras riktlinjer för det avtal som bör skrivas mellan arbetsgivaren och arbetstagaren. Dessutom presenteras riktlinjer för hur användarna och beslutsfattarna bör agera för att uppnå en god informationssäkerhet vid distansarbete. Riktlinjerna bygger dels på uppgifter från kapitel tre och fyra och dels på de avtal som har lagts som bilagor till detta examensarbete.

I rapportens sista kapitel dras slutsatser, en diskussion förs kring offentlighetsprincipen, tystnadsplikten och det faktum att det inom försvarsmakten råder olika förutsättningar för distansarbete.

2. Säkerhetsområdet—en översikt

2.1 Inledning

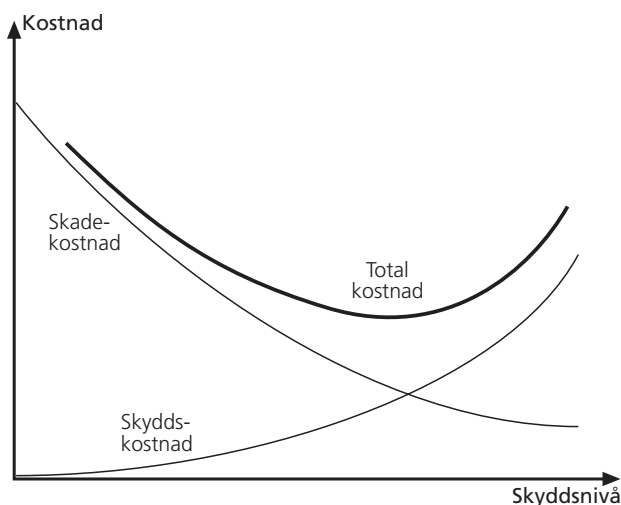
Information får allt större betydelse i vårt samhälle; det blir allt viktigare att informationen är korrekt och att den kommer till rätt person och i rätt tid. När informationen blir allt mer värdefull kan den också bli mer utsatt för stöld, förvanskning eller annat hot. Av denna anledning bör resursen information, hanteras och administreras på ett säkert sätt [Freese et al 1993, s. 16, 21].

För att uppnå en god säkerhet krävs det en medvetenhet om vilka hot som föreligger och vilka risker som dessa hot ger upphov till. Utan förståelse för hot och dess samband med risker kan skydden inte anpassas till rådande förhållanden. Hoten kan vara interna eller externa, de kan vara avsiktliga eller oavsiktliga, kriminella eller inte kriminella. Det är upp till organisationen att själv bestämma vilka hot som ska betraktas som risker mot den egna verksamheten, vilka hot som är värda att skydda sig mot och till vilken nivå. När denna värdering är gjord, genom till exempel en riskanalys, ska enbart de risker återstå som är kända, men värderade att vara så små att de inte är värda att förebygga.

Hur mycket skyddsåtgärderna får kosta måste vägas mot den uppskattade minskningen av skadekostnaden. För alla organisationer finns det en gräns där skyddskostnaden inte längre reducerar skadekostnaden i motsvarande grad, se figur 2.1. Det är denna optimala balans mellan skydd och skador som eftersträvas—den ger den bästa ekonomin [Hamilton 1985, s. 128]. Huvudmålet bör vara att försäkra objekt som kan återanskaffas för pengar, och så gott det går säkra system och värden som inte kan återanskaffas [Freese et al 1993, s. 30]. Det går dock inte att försäkra sig eller säkra systemen mot alla typer av risker. Viss risk måste alltid accepteras, men det är vad säkerhet handlar om—att vara medveten om riskerna och att värdera dem.

För att företagets säkerhetsskydd ska fungera effektivt måste säkerheten ha en tydlig och uttalad roll i företagets policy och vara prioriterat i företagets organisation. Inom företaget är det säkerhetschefen som ska samordna säkerhetsarbetet [Elgemyr et al 1992, s. 251].

I denna uppsats kommer de definitioner som är i enlighet med den svenska standarden [ITS 1994] att användas.

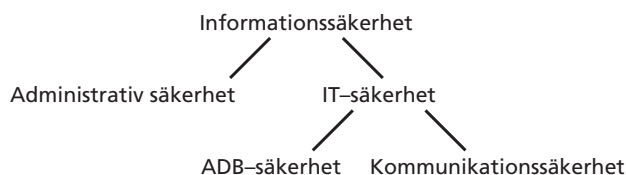


Figur 2.1 Förhållandet mellan skyddskostnad, skadekostnad och totalkostnad [ITS 1994, s. 16].

2.2 Informationssäkerhet

2.2.1 Definition

Då informationssäkerhet består av administrativ säkerhet och IT-säkerhet är ett bra samarbete mellan organisationen och tekniken en förutsättning för att informationssäkerhetsarbetet ska lyckas [Louise Yngström]. Den administrativa säkerheten är sådan säkerhet som uppnås med hjälp av administrativa regler och rutiner. IT-säkerhet handlar om att skydda data och system mot obehörig åtkomst, förändringar eller störningar vid databehandling. IT-säkerhet handlar också om skydd i samband med överföring av information, se figur 2.2.



Figur 2.2 Uppdelning av informationssäkerheten [ITS 1994, s. 7].

Information som är sparad eller lagrad i någon form ska skyddas mot oönskad förändring, påver-

kan eller insyn (integritet, informationskvalitet), det ska inte vara möjligt för obehöriga att ta del av informationen (sekretess) och de användare som har rätt till informationen ska komma åt den efter behov och inom önskad tid (tillgänglighet). Dessa delar presenteras i figur 2.3.



Figur 2.3
Informationssäkerhetens delar [ITS 1994, s. 9].

2.2.2 Integritet

När integritet nämns i denna uppsats avses kravet att en informationsmängd inte oönskat skapas, förändras eller förstörs [ITS 1994, s. 10]. Det ska med andra ord finnas skydd så att någon inte obemärkt kan skriva över, skapa ny, ändra eller radera den information som är lagrad i någon form, se figur 2.4.

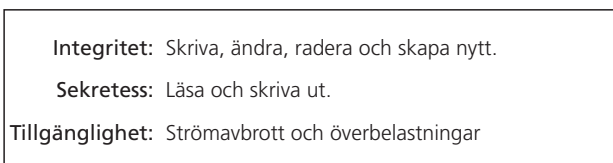
När det i svensk text avses information om personer i datorsystem används oftast termen personlig integritet. Om tveksamhet föreligger rekommenderar den informationstekniska standardiseringen (ITS) att uttrycken förtydligas med personlig integritet och systemintegritet [ITS 94, s. 10].

2.2.3 Sekretess

Avser skydd av information så att den inte görs tillgänglig eller avslöjas för obehöriga [ITS 1994, s. 12]. Obehöriga ska omöjligt kunna läsa, eller skriva ut den information som finns, se figur 2.4. För att sekretessen ska kunna sägas vara tillfredsställande, måste det finnas skydd mot obehörig läsning av informationen. Detta skydd kan till exempel vara kryptering.

2.2.4 Tillgänglighet

Resurserna ska finnas tillgängliga för användare som har rätt att använda dessa. Användarna ska kunna utnyttja resurserna efter behov, i förväntad utsträckning och inom önskad tid [ITS 1994, s. 14]. Det måste vara möjligt för behöriga användare att komma åt viktig information trots, till exempel, ett strömavbrott.



Figur 2.4
Exempel på vad säkerhetskraven ska skydda mot.

2.3 Säkerhetsfunktioner

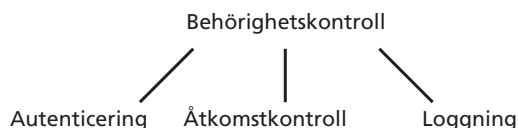
2.3.1 Behörighetskontroll

Oavsett om ett datasystem används internt eller på distans är säkerhetsfrågorna viktiga. Det är viktigt att veta vilka som har rätt att få åtkomst till resurserna. Det är också viktigt att hålla reda på vilken del av informationen som respektive användare har rätt att få åtkomst till. Slutligen är det viktigt att i efterhand kunna se vilka som har försökt att få åtkomst, vilka som har fått åtkomst och vad de har gjort i systemet. Dessa tre delar är de tre stegen som utförs i en behörighetskontroll.

Varje steg i en behörighetskontroll representeras av en säkerhetsfunktion. Denna säkerhetsfunktion anges inom parentes:

- Användarens uppgivna identitet kontrolleras. Om identiteten är godkänd är användaren behörig till att använda systemet eller resursen (autenticering).
- Kontroll av att enbart behöriga användare kommer åt information och resurser samt vad respektive behörig användare har rätt att utföra i systemet (åtkomstkontroll).
- Användarnas aktiviteter i systemet registreras (loggning).

I figur 2.5 förklaras hur autenticering, åtkomstkontroll tillsammans med loggning utgör behörighetskontrollen [ITS 1994, s. 36].



Figur 2.5
Behörighetskontrollens delar [ITS 1994, s. 36].

2.3.2 Autenticering

Autenticeringen är den viktigaste säkerhetsfunktionen eftersom alla andra säkerhetsfunktioner är beroende av denna [Ford 1994, s. 109]. Autenticering är kontroll av uppgiven identitet vid kommunikation mellan två system, eller vid utväxling av meddelanden mellan användare [ITS 1994, s. 42]. En användare styrker sin identitet genom att ange något som enbart han/hon har, är eller känner till. Autenticering kan ske på något av följande sätt [Ford 1994, s. 110]:

- Med något memorerat, till exempel sifferkod eller lösenord.
- Med något buret, till exempel ett aktivt kort eller en fysisk nyckel.
- Med biometriska egenskaper, till exempel ögonbottens mönster eller tumavtryck (statiska mönster), namnteckning eller sätt att skriva på tangentbordet (dynamiska mönster).
- Med ett intygande från en pålitlig person och som tidigare har verifierat identiteten i fråga, till exempel kan en persons identitet styrkas av föräldern till denna person.

Autenticering kan också innebära en kontroll av att ett meddelande inte har förändrats sedan det lämnade avsändaren (användare, dator, kommunikationsnod etcetera). Ofta användes då benämningen meddelandeautenticering [ITS 1994, s. 42].

2.3.3 Åtkomstkontroll

Åtkomstkontroll handlar om att endast behöriga användare ska ha tillgång till information efter deras behov. Detta behov kan klassificeras enligt någon av metoderna begränsad behörighet eller behovsenlig behörighet [ITS 1994, s. 18]. Begränsad behörighet innebär att användaren endast ges minsta möjliga behörighet som krävs för att uppgifterna ska kunna genomföras [Pfleeger 1989, s. 246]. Behovsenlig behörighet är att användaren enbart får tillgång till den del av den konfidentiella information som individen behöver för att fullgöra sina uppgifter [ITS 1994, s. 18].

Åtkomstkontroll avser även att reglera och kontrollera en användares åtkomst till olika resurser (program, processorer, informationsobjekt, skrivare etcetera) [ITS 1994, s. 46].

För att kunna koppla ihop behöriga användare med information och resurser krävs informations-

klassificering. Det innebär att informationen respektive resurserna delas in i olika grupper med avseende på deras säkerhetskriterier [ITS 1994, s. 20]. Åtgärden att klassificera information är en administrativ åtgärd och glöms därför ofta bort. Om den inte genomförs är det omöjligt att genomföra en bra åtkomstkontroll. Försvarsmakten har enligt gällande lagtext informationen i tre klasser; öppen, hemlig och kvalificerat hemlig information [Ulf Berglund].

2.4 Säkerhetsfunktioner och -tekniker

Integritet, sekretess, autenticering och åtkomstkontroll är alla funktioner som skyddar mot interna och externa hot. De kallas även för säkerhetstjänster [Ford 1994, s. 23]. För att exemplifiera säkerhetsfunktionerna jämförs de i figur 2.6 med icke elektroniska funktioner som är vanliga i vårt dagliga liv.

| | |
|------------------|--|
| Integritet: | Hologram på ID-kort, outplånlig färg. |
| Sekretess: | Vattenstämpel (osynligt bläck), sigill, förslutna kuvert, outplånlig färg. |
| Autenticering: | Foto-ID. |
| Åtkomstkontroll: | Vakt, lås, nycklar. |

Figur 2.6
Jämförelse mellan säkerhetsfunktioner/tjänster i den datoriserade respektive icke datoriserade världen [Ford 1994, s. 23].

De hot som säkerhetstjänsterna ska skydda mot är avbrott, avlyssning, modifiering och förfalskning [Pfleeger 1989, s. 4]. Warwick Ford har valt att beskriva hoten som funktionsförlust, informationsläckage, integritetsintrång och olämplig användning [Ford 1994, s. 17]. Oavsett vilka begrepp som används för att beskriva hoten, är det samma åtgärder som behövs för att minimera riskerna.

Åtgärder som kan vidtagas för att minimera riskerna kallas säkerhetstekniker och dessa beskrivs utförligare i kapitel 4. Säkerhetsteknikerna ska skydda tre typer av resurser; hårdvara, mjukvara och information.

3. Distansarbetets olika fasetter

3.1 Definitioner av distansarbete

Genom att studera ett antal projekt om distansarbete har det visat sig att det finns många olika definitioner av distansarbete. Alla studerade projekt inom ramen för detta arbete hade olika, men snarlika, definitioner. Nedan följer de mest intressanta definitionerna.

FMs definition av distansarbete: "Arbetsform där individer/grupper kan utföra sina ordinarie arbetsuppgifter från annat ställe än ordinarie arbetsplats och/eller på andra tider än ordinarie arbetstider. Detta genomförs med distansöverbyggande media." [FM 1995, s. 103]. FM klassar brev, dator, telefon, telefax och bildtelefon som distansöverbyggande media [FM 1995, s. 102].

FMs definition av distansarbete utesluter inte att arbetstagaren sitter hemma en kväll och författar ett brev, eller ringer ett tjänstesamtal som inte gjordes under den ordinarie arbetstiden.

Att en arbetstagare vid ett enstaka tillfälle gör denna form av arbete hemma vill författaren inte klassificera som distansarbete.

Utrikesdepartementet har i sitt projekt Distans-Arbete med Ny Teknik och Ekologi (DANTE), definierat distansarbete som: "Arbete på distans är arbete som förläggs utanför huvudarbetsplatsen och som till väsentlig del är beroende av den nya kommunikationstekniken. Därtill kommer UD:s definition att arbete skall ske regelbundet och i normalfallet 1-3 dagar i veckan" [UD 1996, s. 6].

UD:s definition innebär att det kan vara distansarbete när en arbetstagare regelbundet använder datorn hemma, för att den ordinarie arbetstiden inte räcker till. UD utesluter med andra ord inte att arbete som görs hemma under kvällar och helger klassas som distansarbete.

Arbetsgivarverkets definition av distansarbete är: "Distansarbete råder när en enskild arbetstagare som enligt överenskommelse med arbetsgivaren utför sitt arbete utanför huvudarbetsplatsen, utan att arbetet kräver detta, samt omfattar minst en dag per vecka och kräver någon form av informationsteknik".

Författaren förordar den sistnämnda definitionen för att den:

- Kräver att det finns någon form av avtal mellan arbetsgivaren och arbetstagaren. Distansarbete ska inte vara något som sker på initiativ enbart av den ena parten.
- Förespråkar inte att distansarbete sker från en speciell plats, det kan dock inte ske från huvudarbetsplatsen.
- Definierar att arbetet kan kallas för distansarbete när uppgifterna inte tvunget måste skötas på distans. Att en konsult arbetar hos kunder eller att yrkesinspektionen gör arbetsplatsbesök kan inte klassas som distansarbete.
- Elimineras möjligheten att klassa enstaka kvällsarbete som distansarbete. Att en arbetstagare regelbundet övertidsarbetar hemma kan inte klassas som distansarbete då arbetsgivaren inte gör en överenskommelse om detta.
- Anger att distansarbetet ska ske med hjälp av någon form av informationsteknik, till exempel dator, fax, modem eller mobiltelefon. För denna uppsats är detta att föredra då bland annat säkerhet i samband med datakommunikation kommer att diskuteras i kapitel 4.

När det för första gången ska införas distansarbete i organisationen blir de involverade tvungna att tänka igenom en mängd frågor. Arbetsgivare och arbetstagare bör dels ta ställning var för sig och dels diskutera frågorna tillsammans.

Några av de frågor som kan vara aktuella är:

- Vilka lagar är aktuella i sammanhanget? Vilket ansvar har arbetsgivaren när arbetstagaren sitter hemma och arbetar?
- Vilka fördelar respektive nackdelar kan parterna förvänta sig av distansarbetetsprojektet?
- Hur löses frågorna kring sekretess och företags-hemligheter när arbete sker på distans?
- Hur ska det gå att lätt få tag på arbetstagaren när denne arbetar på distans?
- Vad är maximalt antal dagar per vecka som arbetet får skötas på distans?

Svaren på dessa frågor beror självklart på vad arbetstagare och arbetsgivare har för syfte med distansarbetet.

3.2 Typer av distansarbete

I litteraturen redogörs för tre olika typer av distansarbete:

- Arbetstagaren har en ordinarie arbetsplats men arbetar vissa dagar/tider per vecka från hemmet.
- Arbetstagaren är anställd på företaget ifråga men den ordinarie arbetsplatsen är hemma.
- Arbetstagaren har en bärbar dator och arbetar huvudsakligen från kunder, flygplatser, hotellrum etcetera. Detta gäller främst för säljare, konsulter och tekniker.

När distansarbete nämns i denna uppsats avses huvudsakligen att arbetstagaren arbetar hemma vissa dagar eller tider per vecka. Om annan typ av distansarbete avses kommer en tydlig förklaring att ges.

I litteraturen beskrivs olika yrken och befattningar som är lämpliga för distansarbete. Dessa yrken och befattningar har alla vissa gemensamma grundförutsättningar [Forsebäck 1995, s. 87]: "Deras arbete innebär på ett eller annat sätt handhavande av data, information eller kunskap".

Det finns ett stort antal arbetsuppgifter som anses lämpliga att sköta på distans. I litteraturen finns det flera exempel på lämpliga uppgifter och aktuella yrken [Forsebäck 1995, s. 88, Paavonen 1992, s. 38-43]:

- Generering eller skapande av information eller kunskap. Till exempel författare, journalister, designer och konstruktörer.
- Insamling, selektering och bearbetning av information samt förädling av denna till kunskap. Till exempel utredare, forskare och produktutvecklare.
- Distribution eller förpackning av information. Till exempel informatörer, PR- och reklamkare, försäljare och speditörer.
- Bearbetning, analysering och tolkning av information. Till exempel beslutsfattare, systemanalytiker och statistiker.
- Rutinmässigt och enligt redan angivna kriterier, sammanställning av data eller information. Till exempel lönekontorister, bokförare, produktions- och personalplanerare och kalkylerare.

- Behandling av data eller information. Till exempel dataregistrerare, ord- och textbehandlare, programmerare.

I boken "Making Telecommuting Happen. A guide for Telemanagers and Telecommuters" beskriver Jack Nilles nästan 16.000 olika slags jobb, yrken eller befattningar som är möjliga att utöva på distans [Forsebäck 1995, s. 89].

3.3 Aktuella lagar

3.3.1 Arbetsmiljö

Enligt arbetsmiljölagen har arbetsgivaren ansvar för arbetsmiljön oavsett var arbetstagaren arbetar. Det har ingen betydelse om arbetet utförs i arbetsgivarens lokaler, i ett fordon, utomhus eller hemma hos den anställde [TCO 1996, s. 6]. Detta ansvar innebär, enligt 1 § i kapitel 2 i arbetsmiljölagen, att arbetsgivaren ska anpassa arbetsförhållandena till människornas olika förutsättningar i fysiskt och psykiskt avseende. Teknik, arbetsorganisation och arbetsinnehåll ska utformas så att arbetstagaren inte utsätts för fysiska eller psykiska belastningar som kan medföra ohälsa eller olycksfall [Ågren et al 1992, s. 103].

För arbetsgivaren innebär detta rent praktiskt att denne ska kontrollera arbetsmiljön innan distansarbetet inleds. Arbetsgivaren är enligt lag ansvarig för arbetsmiljön på distansarbetsplatsen så att den är tillfredställande vad det gäller säkerhetskrav, de ergonomiska kraven och den psykosociala miljön [Forsebäck 1995, s. 130].

Arbetstagarens intresse företräds av skyddsombudet. Detta ombud ska fungera som en kanal mellan arbetstagaren och arbetsgivaren. För att den fackliga organisationen ska ha rätt att utse ett särskilt skyddsombud, krävs det att minst fem arbetstagare regelbundet arbetar på arbetsstället. Om distansarbetaren och distansarbetsplatsen organisatoriskt tillhör huvudarbetsplatsen företräds han/hon av det ordinarie skyddsombudet [TCO 1996, s. 7].

Yrkesinspektionen är en statlig myndighet som ansvarar för att arbetsmiljölagarna efterlevs på respektive arbetsplats. För att kontrollera detta har yrkesinspektionen rätt att göra besök på enskilda arbetsplatser. Det finns dock restriktioner mot besök på hemarbetsplatser [TCO 1996, s. 7].

Dessa besök kan endast göras om arbetsgivaren eller arbetstagaren speciellt begär det, eller om det finns särskild anledning.

3.3.2 Arbetsskador

En arbetsskada är den skada som har uppkommit till följd av olycksfall eller annan skadlig inverkan i arbetet. I lagen omfattas även olycksfall vid färd till eller från arbetet—om färden orsakades av och stod i nära samband med arbetet [Rembe 1992, s. 389]. Arbetstagarna är försäkrade för detta genom lagen om arbetsskadeförsäkring. Denna arbetsskadeförsäkring omfattar alla som förvärvsarbetar, således gäller den även vid distansarbete [SIG Security 1996, s. 39].

Om arbetstagaren får en arbetsskada ska han/hon bevisa att det handlar om en skada som har uppkommit genom arbetet. Denna bevisföring är i princip densamma oavsett om skadan skedde på distansarbetsplatsen eller på huvudarbetsplatsen. I socialförsäkringen anges det att såvida arbetstagarens uppgifter inte är helt orimliga, ska de gälla vid bevisföringen av arbetsskadan [Paavonen 1992, s. 47]. För att underlätta vid eventuell bevisföring är det viktigt att det finns en överenskommelse om distansarbete med arbetsgivaren. Utan överenskommelse kan det bli mycket svårt att få en skada som har skett på distansarbetsplatsen godkänd som arbetsskada [TCO 1996, s. 8].

3.3.3 Arbetstid

I arbetstidslagen är det reglerat hur lång arbetstiden får vara och hur den ska förläggas [Rembe 1992, s. 216]. I arbetstidslagen finns det ingen vägledning för frågan om och när övertidsarbete är tillåtet. Denna fråga får parterna själva reglera genom kollektivavtal.

Arbetstidslagen gäller enbart då arbetsgivaren har möjlighet att kontrollera hur och var arbetstiden förläggs [TCO 1987, s. 26]. Eftersom arbetsgivaren inte anses kunna kontrollera detta vid distansarbete, har denna typ av arbetsform undantagits från lagen [Forsebäck 1995, s. 130, Paavonen 1992, s. 45]. Reglerna för detta återfinns i 2 § i arbetstidslagen [TCO 1987, s. 26].

Under 1996 har ett arbete skett med att anpassa arbetstidslagen till EUs arbetsdirektiv. Dessa omfattar även arbete som utförs från hemmet [TCO 1996, s. 6].

3.3.4 Anställningstrygghet

Individens anställningstrygghet regleras av lagen om anställningsskydd. Denna lag omfattar alla i såväl enskild som offentlig tjänst, oberoende av anställningsform [Rembe 1992, s. 180]. Det finns dock vissa undantag; för dessa hänvisas läsaren till litteratur där lagen om anställningsskydd finns beskriven.

I händelse av att arbetsgivaren måste avskeda eller permittera de anställda ska en viss turordning iakttagas. Denna turordning ska enligt lagen om anställningsskydd knytas till de så kallade driftsenheterna [Jan Häggström]. En driftsenhet är i regel den verksamhet som bedrivs inom en viss byggnad eller inom ett visst inhägnat område [Rembe 1992, s. 190]. Om arbetsgivaren betraktar respektive hemarbetsplats som en egen driftsenhet blir arbetstagarens anställningsskydd mycket försvagat. Lagen om anställningsskydd medger därför möjlighet att, om det på orten finns flera driftsenheter, upprätta en turordningslista inom ett geografiskt område [Paavonen 1992, s. 48].

För den distansarbetande arbetstagaren är den bästa lösningen att han/hon organisatoriskt tillhör huvudarbetsplatsen och att detta regleras i avtalet med arbetsgivaren [SIG Security 1996, s. 38, TCO 1996, s. 6].

3.3.5 Semesterfrågor

I likhet med arbetstidslagen, gör semesterlagen undantag för de arbetstagare som arbetar på så sätt att arbetsgivaren omöjligen kan övervaka arbetet [TCO 1987, s. 29]. Exempel på ett sådant arbetssätt är distansarbete från hemmet. För att arbetstagare som arbetar på distans ska ha rätt till semester står det i semesterlagen att en distansarbetare är berättigad till en semesterlön på 12% av utbetalad lön [Jan Häggström]. Arbetstagaren antas själv ordna sin ledighet i samband med att denna semesterlön betalas ut [TCO 1987, s. 29].

3.3.6 Skattefrågor

Från och med januari 1996 (1997 års taxering) har skattefrihet införts på förmåner som är av begränsat värde för den anställde, men som har stor betydelse för utförandet av arbetsuppgifterna. I Kommunalskattelagen (SFS 1995:651) står det: "Om en vara eller en tjänst, som en anställd erhåll-

ler av arbetsgivaren, är av väsentlig betydelse för utförandet av hans arbetsuppgifter, skall förmånen av varan eller tjänsten inte tas upp som inkomst, om förmånen är av begränsat värde för den anställda och inte utan svårighet kan särskiljas från nyttan i anställningen” [Knodt 1995, s. 29, UD 1996, s. 35].

Vad gäller skatteavdrag för hemarbetsplatsen har skattemyndigheten en ytterst restriktiv hållning [Forsbäck 1995, s. 132]. Det är avgörande att distansarbetaren kan bevisa att det verkligen finns ett behov av arbetsutrymme i bostaden. Arbetsutrymmet som används ska vara väl avskilt från bostaden och får bara användas för arbetet [TCO 1996, s. 8].

3.3.7 Hyreslagen

När en anställd arbetar på distans är naturligtvis arbetsgivaren involverad, dessutom kan hyresvärderna ha åsikter angående distansarbete från hemmet. Om distansarbetet blir av mer omfattande och varaktig natur, kan frågor kring hyreslagen aktualiseras. Enligt lagen kan hyresgästen förlora sin hyresrätt om lägenheten används för annat ändamål än det avsedda och om avvikelser har betydelse för hyresvärderna [Paavonen 1992, s. 49, TCO 1996, s. 8]. Även bostadsrättslagen innehåller motsvarande reglering.

Så länge som arbetet i hemmet inte vållar några besvär för hyresvärderna, bör det inte finnas något i hyresrätten som hindrar detta [SIG Security 1996, s. 39]. Det bör inte heller bli problem om arbetstagaren får ersättning av arbetsgivaren för användningen av ett rum i hemmet. Det kan likställas med att hyresgästen har en inneboende, vilket är tillåtet enligt hyreslagen [TCO 1996, s. 8].

Den arbetstagare som bor i villa och önskar att arbeta på distans från hemmet kommer att ställas inför ett problem. Enligt plan- och bygglagens 1 § i kapitel 8 krävs ett nytt bygglov för att villan ska få användas för ett annat ändamål än vad den en gång byggdes för [Forsbäck 1995, s. 131, TCO 1987, s. 30].

3.3.8 Försäkringsfrågor

I samband med att arbetstagare ska arbeta på distans kommer två typer av försäkringsfrågor att bli aktuella [Jan Häggström]; egendomsskada och personskada. Egendomsskada är skada eller för-

lust av arbetstagarens egendom eller arbetsgivarens utrustning. Personskada är när arbetstagaren eller annan person skadar sig i eller kring arbetsmiljön.

Om tredje man, till exempel arbetstagarens barn, skadar sig på distansarbetsplatsen kan det jämföras med om personen hade skadat sig under ett besök på huvudarbetsplatsen [Jan Häggström]. Arbetsgivarens ansvarsförsäkring, som omfattar ansvar mot tredje man, ska gälla oavsett var arbetsplatsen finns [TCO 1996, s. 12].

Vad gäller försäkringar för de arbetstagare som idag arbetar på distans, är det vanligt att arbetsgivaren förlitar sig på att arbetstagaren har ett eget försäkringsskydd. Vid en eventuell olycka, egendomsskada eller personskada, utnyttjas arbetstagarens egna hem- eller olycksfallsförsäkring. Arbetsgivarverket, som företräder arbetsgivarna, anser att arbetsgivaren ska ersätta arbetstagaren för de självriskkostnader och bonusförluster som uppkommer när hemförsäkringen utnyttjas för den skada som har orsakats av arbetsgivarens utrustning.

Arbetstagarnas organisationer har åsikten att arbetsgivaren ska teckna en försäkring för den utrustning som ställs på distansarbetsplatsen [TCO 1996, s. 14]. Vidare anser fackförbunden att arbetsgivaren ska stå för kostnaderna som uppkommer om arbetsutrustningen i hemmet behöver extra skydd mot inbrott och skadegörelse [TCO 1996, s. 11].

3.4 Aspekter för och emot distansarbete

3.4.1 Fördelar för arbetstagaren

Att arbeta på distans ska vara ett beslut som tas av individen själv. Beslutet påverkas av individens livsperspektiv det vill säga, ålder, familjeförhållanden, personliga egenskaper, förutsättningar och personliga bedömningar.

Den arbetstagare som har valt att sitta hemma och arbeta några gånger per vecka gör detta, med stor sannolikhet, för att det medför fördelar för personen i fråga. Några av dessa fördelar kan vara [Forsbäck 1995, s. 123, Paavonen 1992, s. 51 och 68, TCO 1996, s. 3, UD 1996, s. 25]:

- Möjlighet till ökad koncentration. Inga arbetskamrater som tittar förbi och avbryter med några trevliga ord om ämnen utanför det gemensamma arbetet.

- Slippa långa, tröttande och ibland stressande arbetsresor.
- Möjlighet att bestämma sina egna arbetstider. Det är långt ifrån alla som är mest produktiva mellan klockan 8 och 17.
- Variationen att vissa dagar kunna arbeta på distans och andra dagar på huvudarbetsplatsen kan i sig stimulera arbetstagaren.

Dessa och andra fördelar som distansarbete medför leder i slutändan till ökad produktivitet hos arbetstagaren [Forsebäck 1995, s. 123]. Denna produktivitetsökning kan generellt mätas till någonstans mellan 20 och 30%. Produktivitetsökningen sker en gång och blir tydlig i full skala först efter ett eller ett par år [Forsebäck 1995, s. 124].

3.4.2 Nackdelar för arbetstagaren

Det är inte bara positivt att arbeta på annan plats än huvudarbetsplatsen. Det finns en mängd identifierade nackdelar som uppkommer i samband med distansarbete. Dessa nackdelar blir tydligare ju fler dagar per vecka som arbetstagaren arbetar på distans.

Exempel på identifierade nackdelar är [Forsebäck 1995, s. 101-106, TCO 1996, s. 3, UD 1996, s. 25]:

- Risk för social isolering. Distansarbetaren har ofta kontakt med kunder och medarbetare via elektroniska medier. Efter en tid kan distansarbetaren sakna det fysiska mötet.
- Missar den information som de anställda informellt distribuerar under en arbetsdag.
- Svårighet att skilja på arbetstid och fritid. Detta nya fenomen kallas för "workoholism".
- Distansarbetaren står utanför företagets informella kontaktnät. Den som står utanför detta blir lätt "osynlig", även vad gäller löne- och kompetensutveckling.

3.4.3 Fördelar för arbetsgivaren

När arbetstagarna ges möjlighet att arbeta på distans går ofta arbetsgivaren in i ett nytt och osäkert projekt. Denna nya arbetsform innebär möjliga vinster för arbetsgivaren, men den innebär också stora risker. I likhet med arbetstagarna kan arbetsgivaren förvänta sig både fördelar och nackdelar med distansarbete.

De fördelar som arbetsgivaren kan förvänta sig har i litteraturen grupperats in i tre huvudgrupper [Forsebäck 1995, s. 86]; ökad produktivitet, kostnadsbesparingar och personalpolitiska motiv. Exempel på respektive grupp är [Forsebäck 1995, s. 122, Paavonen 1992, s. 59, 63 och 74, UD 1996, s. 25]:

- Ökad effektivitet och produktivitet hos de anställda.
- Lokalkostnaderna kan minskas när ett antal av de anställda arbetar på distans.
- Kostnaden för sjukfrånvaro minskar när anställda som känner sig lite sjuka kan arbeta hemifrån.
- Personalomsättningen kan komma att minska när de anställda har möjlighet att arbeta på distans. På detta sätt kan det vara lättare att behålla nyckelpersoner inom organisationen.

3.4.4 Nackdelar för arbetsgivaren

När de anställda tillåts att arbeta på distans innebär detta vissa nackdelar för arbetsgivaren. Exempel på nackdelar som kan bli verklighet i samband med distansarbete är [Forsebäck 1995, s. 112, TCO 1996, s. 4 UD 1996, s. 25]:

- Ökade kostnader för utrustning och service som den distansarbetande personalen behöver.
- Det ställs nya krav på arbetsledningen när de anställda arbetar decentraliserat. De anställda måste i större utsträckning tillåtas ta egna beslut.
- De anställda som arbetar på distans tar inte del av den information som informellt sprids mellan arbetstagarna.
- När anställda arbetar på distans ökar risken för tekniska avbrott och det leder till större problem att tillämpa säkerhets- och sekretessregler.
- Arbetsgivaren får svårare att ordna möten med kort varsel.

4. Informationssäkerhet och distansarbete

4.1 Inledning

När organisationen låter arbetstagare arbeta på distans ställs det höga krav på informationssäkerhet. Det existerar ett antal hot mot informationen. Dessa hot kan identifieras med hjälp av en riskanalys. Den hotbild som då fås fram ska kontinuerligt revideras med hjälp av ny riskanalys.

I denna uppsats diskuteras hot som i allmänhet finns mot en verksamhet. För att identifiera de hot som existerar mot informationen i en specifik organisation ska en riskanalys göras för den enskilda organisationen. När riskerna har identifierats ska tänkbara skydd mot dessa hot formuleras och realiseras.

Detta kapitel börjar med att identifiera ett antal hot och fortsätter med att placera respektive hot i ett samband med informationssäkerhet. I avsnitt 4.4 presenteras vanligt förekommande tekniska lösningar för att minimera riskerna som hoten för med sig. Det sista avsnittet förklarar utifrån informationssäkerhetens synvinkel hur de tekniska lösningarna skyddar mot identifierade hot.

4.2 Hot

4.2.1 Informationsläckage

Detta hot innebär att information exponeras eller avslöjas för obehöriga personer eller enheter [Ford 1994, s. 17]. Information som läcker ut kan komma från datorer, datornät, övrig utrustning eller icke digitala informationskällor.

Informationen kan komma ut på huvudsakligen två sätt. Antingen genom stöld eller genom avlyssning av informationen.

Stöld av information kan ske på två olika sätt. Det första sättet medför att informationen helt förloras, det andra sättet medför att en kopia av informationen kommer i orätta händer. Den första typen av stöld blir aktuell om den anställdes dator eller lagringsmedia stjäls ur till exempel bilen eller hemmet. Den andra typen av informationsstöld är aktuell när någon lyckas kopiera information på något sätt. Informationen kan kopieras över på en diskett, kopieras i en kopiator, skrivas av eller, om det inte är en för stor mängd, memoreras.

Det andra sättet som information kan läcka ut på är genom att någon avlyssnar den. Avlyssning av information kan ske i tre olika situationer.

Den första situationen då avlyssning kan ske är när information förs över en telefonledning, ett publikt nätverk eller med hjälp av annan lösning av ett Wide Area Network (WAN). Informationen som överförs kan vara tal, fax eller datakommunikation. Informationen kan överföras via modem, fax, telefon eller mobiltelefon. Ledningen som används för överföringen kan vara av koppar, fiberoptik eller trådlöst. Beroende vilken form av ledning som används är informationen olika svår att avlyssna [Elgemyr et al 1992, s. 207]. Vid en jämförelse mellan kopparkabel och fiberoptik är den sistnämnda svårare, men inte omöjlig, att avlyssna. Vad det gäller avlyssning av trådlös kommunikation, är det lätt att avlyssna den om överföringen är analog [Elgemyr et al 1992, s. 209]. Mobiltelefonnätet NMT är analog radioöverföring. Det nyare mobiltelefonnätet GSM använder digital överföring och därför något säkrare än det äldre NMT. GSM-samtalen förs över i förvrängd form mellan mobiltelefonen och basstationen. Däremot är samtalet helt tolkningsbart då de kopplas in på det publika telefonnätet [Elgemyr et al 1992, s. 210]. Under den tid som GSM-samtalet inte är i förvrängd form är detta samtal lika sårbart för avlyssning som annan telefonkommunikation.

Risken för dataintrång är större om modem och uppringd linje används istället för en fast uppkoppling. Å andra sidan innebär fast uppkopplad linje att det blir lättare att utföra avlyssning i och med att det blir lättare att lokalisera linjen [Elgemyr et al 1992, s. 208].

Den andra situationen då avlyssning är möjlig är då en persondator används men då den inte är uppkopplad på ett nätverk. Angriparen avlyssnar de signaler som avges från informationsbehandlande utrustning, så kallade röjande signaler (RÖS).

Det finns flera olika former av RÖS, några exempel är:

- Akustisk RÖS avges av nedslagen på ett tangentbord eller ljudet från en skrivare [Elgemyr et al 1992, s. 211].
- Optisk RÖS inträffar när någon obehörig kan läsa vad som finns på till exempel en dator-

skärm, eller vad som skrivs på tangentbordet [SIG Security 1995, s. 31].

- Elektromagnetisk RÖS är den strålning som till exempel en datorskärm eller överföringskablar har [Elgemyr et al 1992, s. 211].

Den sista situationen då avlyssning är möjlig är när kommunikation förs i en lokal eller liknande. Denna kommunikation kan vara samtal mellan två personer eller samtal i stationär- eller mobiltelefon. Avlyssningen kan antingen ske genom att befinna sig på samma plats och lyssna eller att bära en bandspelare. Det andra sättet att avlyssna denna typ av kommunikation är att placera någon form av avlyssningsutrustning på den plats där samtalet förs.

4.2.2 Integritetsförlust

Som det beskrevs i avsnitt 2.2.2 innebär kravet på bibehållen integritet att informationen inte oönskat och obemärkt skapas, ändras eller förstörs, avsiktligt eller oavsiktligt, av behörig eller obehörig användare. Hotet integritetsförlust är således att behörig eller obehörig användare olovligen skapar ny, ändrar i eller förstör befintlig information. Användaren kan komma över informationen när den skickas okrypterad via ett nätverk, när en persondator är oskyddad eller obevakad eller när dokument på distansarbetsplatsen förvaras så att obehöriga kan komma åt den.

Om information skapas, ändras eller förstörs av någon som inte är behörig att göra detta, leder det i slutändan till att informationens riktighet och pålitlighet äventyras [Ford 1994, s. 17].

4.2.3 Funktionsförlust

Detta hot innebär att användarna inte kan komma åt den information som de har behörighet till. Anledningen till funktionsförlusten kan vara att datorn har slutat fungera, att många användare är uppkopplade så att en individ inte får tillgång till önskade resurser, att en användare kör stora informationsmängder vilket leder till att resurserna blir upptagna med detta, att datorn är försvunnen eller skadad eller att energitillförsel (el) saknas.

4.2.4 Obehörigt användande

Hotet obehörigt användande kan aktualiseras vid ett flertal tillfällen; om en dator blir stulen, om det blir inbrott på en arbetsplats, om någon obehörig användare ringer upp företagets kommuni-

kationsserver eller om en behörig person använder systemet på ett obehörigt sätt.

Oavsett anledningen till att hotet blir verklighet kan det i sämsta fall leda till att hoten informationsläckage, integritetsförlust och funktionsförlust blir verklighet. Om den obehöriga användaren läser något av den lagrade informationen har ett informationsläckage ägt rum, om inkräktaren raderar filer som finns lagrade har han eller hon orsakat integritetsförlust och slutligen kan behöriga användare nekas tillträde för att angriparen tar systemresurser i anspråk.

En typ av obehörigt användande som är vanligt förekommande är så kallade telehackare [Jacobs-son 1996, s. 6]. Dessa hackare utnyttjar företagets telefonväxel för att ringa gratis över hela världen.

En annan typ av obehörigt användande är att en angripare falskt utger sig för att vara behörig användare. Detta kallas för maskerad eller spoofing [ITS 1994, s. 54]. Alternativt kan en obehörig användare utge sig för att vara ett annat system, så kallad IP-adress-spoofing [SIG Security 1996, s. 121].

Slutligen kan en obehörig användare få tillgång till en dator eller ett system genom att använda en behörig användares lösenord. Detta lösenord kan angriparen på något sätt tagit reda på eller fått vetskap om genom att ha provat sig fram.

4.3 Informationssäkerhet och hot

4.3.1 Inledning

Som det beskrivits i kapitel två består informationssäkerhet av tre olika delar; integritet, sekretess och tillgänglighet. För att säkerheten ska kunna kallas för god krävs det att dessa delar, var och en, har setts över och lösts med hjälp av lämplig teknisk och administrativ lösning. Varje hot som existerar mot en organisations information, berör en eller flera av dessa delar i informationssäkerheten.

De säkerhetsansvariga inom organisationen bör ta ställning till hur integriteten, sekretessen och tillgängligheten ska vara vid hanteringen av information. Om de ansvariga för informationssäkerheten tillsammans med användarna av informationen, sätter upp tydliga riktlinjer för hur integritet, sekretess och tillgänglighet skall upprätthållas är det möjligt att se när organisationens informationssäkerhet är hotad.

För att kunna sätta upp riktlinjer för en organisations informationssäkerhet är det viktigt att veta vilka hot som finns mot informationen, vad det är som är hotat och hur hotet kan elimineras. I föregående avsnitt redogjordes det för möjliga hot mot en organisations information. I nästa avsnitt förklaras vilken del av informations säkerheten som påverkas av respektive identifierat hot. Kapitlet avslutas med en diskussion kring de tekniska lösningar och hur dessa kan användas för att skydda organisationens information.

4.3.2 Integritet

Om information skapas och lagras på rätt sätt och bibehålls vid överföring, har god informationsintegritet erhållits [Pfleeger 1989, s. 396].

Av de hot som beskrevs i avsnitt 4.2 kan följande leda till att informationens integritet hotas:

- En obehörig användare skapar ny information, förändrar eller raderar information eller program som han/hon utan berättigande har kommit åt.
- Behörig användare ändrar, raderar eller lägger till information på ett sätt som han/hon inte är behörig att göra. Användaren kan göra detta med eller utan uppsåt.
- Felaktig informationsklassificering kan innebära att olämpligt många personer inom organisationen kan komma åt att ändra i den information som finns lagrad.

Dessutom kan informationens integritet hotas om systemet blir smittat av virus eller blir utsatt för andra programrelaterade angrepp.

För illustrering av vilka hot som berör informationsintegriteten hänvisas till figur 4.1.

4.3.3 Sekretess

I avsnitt 4.2 beskrevs potentiella hot mot informationen inom en organisation. Av de beskrivna hoten kan följande leda till att informationens sekretess går förlorad, jämför med figur 4.1:

- Om en dator stjäls finns stor risk att tjuven kan ha möjlighet att läsa informationen som finns lagrad på den.
- En kopia av information försvinner. Risken är stor att denna kopia kan komma i fel händer.
- Avlyssning av datakommunikation, RÖS eller mänsklig kommunikation.
- En behörig användare läser information som denne egentligen inte har med att göra. Detta kan ske genom en olyckshändelse eller genom ren nyfikenhet.
- Klassificeras informationen felaktigt kan det leda till att olämpligt många personer inom organisationen kan ta del av informationen.
- En obehörig användare tar sig in i organisationens nätverk till exempel med hjälp av en anställdes användaridentitet och lösenord.

| | Integritet | Sekretess | Tillgänglighet |
|--------------------------------------|------------|-----------|----------------|
| Information helt förlorad: | | • | • |
| Kopia förlorad: | | • | |
| Ledning avlyssnas: | | • | |
| RÖS avlyssnas: | | • | |
| Lokal avlyssnas: | | • | |
| Skapa/ändra information: | • | | |
| Otillgänglig information: | | | • |
| Experiment av behörig användare: | • | • | • |
| Felaktig klassificering: | • | • | • |
| Trasig hårdvara: | | | • |
| Obehörigt intrång: | • | • | • |
| Datavirus/programrelaterade angrepp: | • | • | • |

Figur 4.1
Matris över diskuterade hot och vilken del av säkerheten som respektive hot berör.

Ett ytterligare hot mot organisationens informationssekretess är risken för att få in trojanska hästar i datasystemen. Detta är program som skenbart eller reellt utför en funktion, men som samtidigt utför oönskade funktioner. Den oönskade funktionen kan till exempel vara uppletning av lösenord och sedan användning av modemmet för att skicka lösenordet till en i förhand bestämd mottagare.

4.3.4 Tillgänglighet

Informationens tillgänglighet blir hotad om de som har rätt att ta del av denna information inte kan göra detta i förväntad utsträckning och inom önskad tid.

Av de hot som har exemplifierats i avsnitt 4.2 är det följande som kan hindra anställda inom en organisation att komma åt information, jämför med figur 4.1:

- Informationen förloras helt genom exempelvis en stöld eller att den raderas av någon som är obehörig att göra detta.
- En användare uppehåller systemet med till exempel tunga beräkningar. Detta hindrar andra användare att komma åt resurserna.
- En behörig användare gör något som hindrar andra användare att senare komma åt samma information. Det kan till exempel vara att informationen flyttas till en annan plats, att informationen raderas eller att en server felaktigt stängs av.
- Datoresurserna är skadade eller obrukbara till exempel på grund av brand, vattenskador, elavbrott eller problem med telefonförbindelsen.
- En obehörig användare har fått reda på en anställdes användaridentitet och lösenord och med detta tar sig in i organisationens nätverk. Den behöriga användaren kan under denna tid inte logga in.

Exempel på ytterligare hot mot tillgängligheten kan vara när datorn inte fungerar på det sätt som det är avsett. Detta i sin tur kan vara orsakat av datavirus eller att datorn har blivit för varm eller för kall när den förvaras. En dator kan även bli obrukbar om den blir utsatt för andra programrelaterade angrepp än virus såsom maskar eller trojanska hästar.

4.4 Tekniska lösningar

4.4.1 Kryptering

Kryptering är en metod att dölja innebörden i ett meddelande för obehöriga läsare, det vill säga att bevara meddelandets integritet och sekretess. Kryptering innebär att omvandla ett meddelande från klartext till kryptotext. Dekryptering är det motsatta förfarandet.

Ett meddelande krypteras med hjälp av en matematisk algoritm och en krypteringsnyckel. Algoritmen är en uppsättning matematiska regler som anger hur klartext ska omvandlas till kryptotext. Krypteringsalgoritmen kan vara tillgänglig för vem som helst, det är nyckeln för dekodning som måste hållas hemlig.

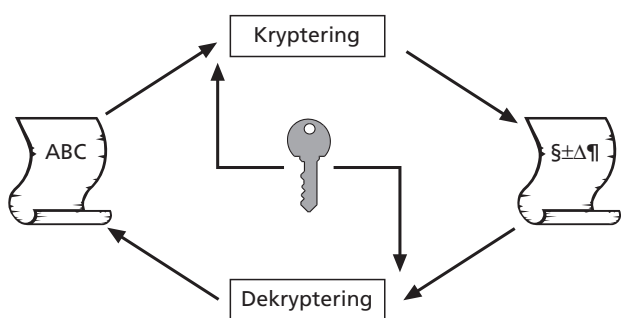
Vad det gäller nyckeln kan samma användas för för kryptering som för dekodning—symmetriskt kryptosystem, se figur 4.2. Alternativet är att använda en nyckel för kryptering och en annan nyckel för dekodning—asymmetriskt kryptosystem, se figur 4.3.

Nycklarna i ett asymmetriskt kryptosystem kallas ibland för publika och privata nycklar, ibland för öppna och hemliga nycklar och ibland för krypteringsnyckel respektive dekodningsnyckel. Författaren har valt den förstnämnda benämningen då den tydliggör hanteringen av krypteringsnycklarna.

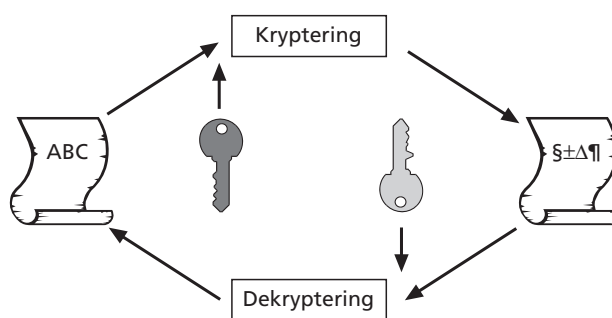
Den mest spridda symmetriska krypteringsalgoritmen är Data Encryption Standard (DES). Sammanfattningsvis gäller följande för DES och andra symmetriska krypteringsalgoritmer:

- Använder samma nyckel för kryptering och dekodning.
- Det är en snabb metod för att kryptera ett meddelande.
- Det är komplicerat att distribuera nyckeln.

Den nyckel som används får endast vara känd för personer som har rätt att ta del av det krypterade meddelandet. När en nyckel ska distribueras måste det således ske över ett media där risken är obefintlig att någon obehörig kan ta del av nyckeln.



Figur 4.2
Kryptering med symmetrisk algoritm.



Figur 4.3
Kryptering med asymmetrisk algoritm.

1976 kom det asymmetriska kryptosystemet [Levy 1994, s. 163] där två olika nycklar, en publik nyckel och en privat nyckel, används. Den publika nyckeln kan spridas till vem som helst, den privata nyckeln måste däremot hållas hemlig av ägaren till denna.

Varje användare har sin egen privata nyckel och kan ha kännedom om ett flertal olika publika nycklar. Vilken publik nyckel som ska användas beror på vem som ska kunna dekryptera meddelandet, det vill säga vem som ska använda sin privata nyckel.

Vid kryptering och överföring av till exempel ett brev, krypterar avsändaren brevet med mottagarens publika nyckel. När mottagaren har fått det krypterade brevet, dekrypteras detta med den privata nyckeln, se figur 4.3. Varje privat och publik nyckel bildar ett par, det är endast den privata nyckeln som kan dekryptera vad motsvarande publika nyckel har krypterat.

Den asymmetriska krypteringsalgoritmen möjliggör användning av digitala signaturer och kryptografisk kontrollsumma.

Den mest använda asymmetriska krypteringsalgoritmen är RSA. Namnet är initialerna hos personerna som först presenterade krypteringsalgoritmen; Rivest, Shamir och Adleman. Sammanfattningsvis gäller följande för RSA och andra asymmetriska krypteringsalgoritmer:

- Använder privat och publik nyckel för att kryptera respektive dekryptera ett meddelande.

- Den publika nyckeln kan ges till vem som helst.
- Den privata nyckeln måste hållas hemlig.
- Möjliggör användning av digitala signaturer och kryptografisk kontrollsumma (se nedan).

Eftersom den publika nyckeln kan ges till vem som helst är det viktigt att kunna koppla den till en specifik användaridentitet. Annars kan någon byta ut en nyckel och skicka dokument i någon annans identitet. Denna ihopkoppling av nyckel och användar identitet görs med hjälp av nyckelcertifikat som innehåller användarens nyckel, användarens namn och eventuellt annan information. Certifikatet signeras av en instans som är betrodd av flera användare, en så kallad certifieringsinstans [ITS 1994, s. 58, Nordqvist 1996c, s. 5].

4.4.2 Digital signatur

En digital signatur är i likhet med en underskrift ett sätt för en person att godkänna innehållet av ett dokument. Den digitala signaturen gör det möjligt för mottagaren av ett meddelande att kontrollera vem som är avsändare. Eftersom avsändaren sätter sin unika signatur på det som skickas iväg, kan han eller hon senare inte neka till att ha skickat iväg dokumentet ifråga.

En digital signatur ska enbart kunna skapas av avsändaren själv, vilket gäller om användaren krypterar meddelandet med sin privata nyckel. Vem som helst kan sedan kontrollera identitetens hos avsändaren genom att dekryptera meddelandet med den publika nyckeln [Ford 1994, s. 79]. Detta förfarande är tvärt emot förfarandet vid den kryptering som syftar till att bibehålla informationens sekretess, se figur 4.3.

En digital signatur utgår ifrån att användaren kan placera något unikt på ett dokument. Det unika som användaren har är den privata nyckeln, därför kan digitala signaturer endast skapas när asymmetrisk krypteringsalgoritm används.

4.4.3 Kryptografisk kontrollsumma

Om ett oskyddat meddelande överförs mellan användare, finns det ingen möjlighet att upptäcka om något i meddelandet har ändrats under transporten. En förändring i ett meddelande kan orsakas av tekniskt fel eller att meddelandet hamnade i fel händer innan det nådde fram till avsedd mottagare. När ett meddelande tas emot är det bra om det är möjligt att upptäcka om någonting i meddelandet har ändrats. På så sätt kan mottagaren se om informationen i meddelandet är samma som avsändaren avsåg att skicka.

Om avsändaren beräknar ett kontrollvärde på meddelandet, så kallad kryptografisk kontrollsumma, kan mottagaren upptäcka om det har skett någon förändring av meddelandet [ITS 1994, s. 65].

Tekniskt går skapandet av den kryptografiska kontrollsumman till så att summan beräknas ur meddelandet med hjälp av en hashfunktion. Resultatet från hashfunktionen skyddas genom kryptering eller digital signatur och bifogas till meddelandet. Meddelandet kan i sin tur skyddas med kryptering eller med digital signatur. Mottagaren dekrypterar meddelandet och räknar fram kontrollsumman med hjälp av en hashfunktion som är identisk med den som avsändaren använde sig av. Om mottagarens resultat överrensstämmer med det i meddelandet bifogade resultatet, är meddelandet oförändrat sedan det skickades iväg [Ford 1994, s. 76]. Att skapa en kontrollsumma är oberoende av vilken krypteringsalgoritm som används, således kan kryptografisk kontrollsumma användas vid både symmetrisk och asymmetrisk krypteringsalgoritm.

Att beräkna en kryptografisk kontrollsumma kan även vara användbart då information ska lagras och eventuella förändringar senare ska vara möjliga att upptäcka [ITS 1994, s. 65].

Kryptografisk kontrollsumma kallas i litteraturen även för sigill, integritetskod (MIC) och autentiseringskod (MAC).

4.4.4 Behörighetskontroll

Det skydd som hindrar att obehöriga användare startar och använder datorutrustningen kallas för behörighetskontroll. Detta skydd består av flera olika delar, till exempel autentisering, reglering av åtkomsträttigheter och loggning av aktiviteter, jämför avsnitt 2.3.1.

För att skydda datorutrustningen kan ett BehörighetsKontrollSystem (BKS) användas. BKS är en mängd säkerhetsfunktioner som tillsammans utför behörighetskontrollen i systemet som skyddas [ITS 1994, s. 37]. De BKS som finns på marknaden innehåller vanligtvis funktioner för identifiering och verifiering av användarens identitet, reglering av åtkomsträttigheter och möjlighet till att registrera aktiviteter i systemet [ITS 1994, s. 37].

Delarna i ett BKS—loggning, autentisering och åtkomstkontroll, kommer att beskrivas var för sig.

4.4.5 Autentisering

Som har beskrivits i avsnitt 2.3.2 innebär autentisering att uppgiven identitet kontrolleras när två system kommunicerar eller när användare utbyter meddelanden med varandra.

Autentiseringen bör helst ske med hjälp av hårdvara. Vanligen har användaren då en unik identifieringsnyckel som förvaras till exempel i ett aktivt kort eller en nyckeldosa [SIG Security 1996, s. 110]. Det aktiva kortet stoppas in i en kortläsare och användaren verifierar sin identitet med ett lösenord. Denna metod stödjer två autentiseringsprinciper; något du har (kortet) och något du vet (lösenordet).

Metoden att använda en nyckeldosa fungerar enligt följande princip; nyckeldosan räknar, enligt en algoritm, om ett slumptal som användaren får av systemet där inloggningen sker. Svaret som omräkningen ger skickas tillbaka som ett lösenord. Värddatorn har utfört samma algoritm och jämför sitt eget svar med det som togs emot från användaren. Är de båda svaren identiska släpps användaren in i systemet. Detta tillvägagångssätt att autentisera användaren kallas för stark autentisering eller kryptografisk autentisering och det lösenord som användaren skickade till värddatorn är ett så kallat engångslösenord [ITS 1994, s. 64].

Om lösenordet däremot skickas i klartext till systemet där autentiseringen sker, kallas det för enkel autentisering. I mottagande server finns en

lista över alla lösenord och om det lösenord som servern tar emot finns i listan släpps användaren in i systemet.

4.4.6 Åtkomstkontroll

Informationen i en organisation ska inte vara tillgänglig för alla. Detta gäller dels obehöriga användare men också för användare som har tillgång till systemet. Det är viktigt att klarlägga vem som behöver veta vad. Dessa två aspekter är åtkomstkontrollens uppgifter—hindra obehöriga användare att upprätta en kommunikation och att reglera vad behöriga användare får göra med resurserna i systemet [ITS 1994, s. 46].

För att kunna hindra obehöriga användare att komma i kontakt med systemet i fråga kan ett flertal tekniska och administrativa skyddsåtgärder vidtagas. De tekniska åtgärderna kan till exempel vara autentisering av användarna, fysiskt skydd av resurserna, bevakning mot obehörigt tillträde, skydd av hårdvaran, skydd mot obehörig avlyssning och skydd i operativsystemet [Ford 1994, s. 149, ITS 1994, s. 46]. Administrativ säkerhet innebär åtgärder som fastställande och spridande av organisationens säkerhetspolicy, kartlägga och bekräfta vem som har ansvaret för informationen och klassificering av informationen [ITS 1994, s. 46]. Ett urval av de olika tekniska säkerhetsåtgärder som finns kommer att diskuteras i delkapitel 4.4.8.

För att kunna reglera användarnas åtkomst till informationen ska organisationens regler om vem som ska ha tillgång till vilken information, överföras till att fungera i datorsystemet. Användarna ska tilldelas behörighet efter vilken information de har rätt att ta del av. Användarnas behörighet kan baseras på individen själv, på dennes roll eller gruppmedlemskap inom organisationen [Ford 1994, s. 15]. Slutligen kan användarnas behörighet baseras på informationens känslighet. Varje objekt klassificeras efter informationens känslighet och användarna får tillgång till en viss nivå i klassificeringshierarkin [Ford 1994, s. 154, Pfleeger 1989, s. 246].

Den sist nämnda metoden för att reglera användarnas möjlighet att komma åt information inom organisationen, är den som oftast används inom myndigheter och militära organisationer [Pfleeger 1989, s. 246]. Det är i dessa typer av verksamheter

där klassificering av informationen oftast är förekommande. Metoden bygger på en modell som har utvecklats av Bell och LaPadula. Detta är en modell som beskriver tillåtna informationsflöden i ett säkert datorsystem. Användarna tilldelas läs- och skrivrättighet. För en fördjupning av Bell- LaPadula modellen och andra informationsflödesmodeller hänvisas till kapitel 7 i "Security in Computing" av Charles P. Pfleeger.

4.4.7 Loggning

Att föra logg innebär att kontinuerligt samla information om de operationer som utförs i datorsystemet. Att registrera händelser kan i efterhand användas till att analysera vilka operationer som har utförts och vilka användare som har initierat dessa operationer. Det vanligaste är att loggningen omfattar tidpunkt, användarens identitet, berörda objekt (filer, program eller registerposter), berörda resurser och utförda operationer.

Syftet att logga händelser i ett datorsystem är att kunna genomföra uppföljningar av systemets utnyttjande. Förutsättningen är att loggen verkligen visar det som behöver kontrolleras samt att det finns lämpliga hjälpmedel för att göra analyser.

Beroende på vilken information som önskas kring systemets utnyttjande avgör omfattningen av loggningen. Den kan antingen vara total, det vill säga omfatta alla händelser i systemet. Detta leder till närmast ohanterligt stor mängd logginformation. Alternativt kan ett urval händelser loggas, till exempel enbart obehöriga intrång, under vissa tider eller enbart loggning för vissa register och resurser.

Om de anställda informeras om att loggning sker kan detta fungera som ett preventivt skydd av systemen. Förutom att hindra interna säkerhetsöverträdelser kan loggningen avslöja om utomstående försöker göra intrång i systemet [Freese et al 1993, s. 134]. Det är viktigt att den logg som registrerar användarnas aktiviteter, inte möjliggör uppföljning som riskerar intrång i användarnas personliga integritet.

4.4.8 Tekniker som hindrar obehöriga användare

Åtkomstkontrollen ska se till att obehöriga användare inte kommer i kontakt med systemet ifråga. Åtkomstkontrollen kan bevaka gränsen

mellan organisationens interna datorsystem och omvärlden. Åtkomstkontrollen kan också bevaka olika delar av organisationens interna datorsystem, som då är uppdelat i så kallade säkerhetsdomäner [SIG Security 1995, s. 155]. Säkerhetsdomänerna kan byggas med hjälp av så kallade brandväggar, intelligenta hubar, routers med krypteringsfunktion eller med hjälp av nätverkslösningar.

Modem

Ett modem omvandlar signalen från en dator till en signal som kan transporteras på det allmänna telefonnätet, och vice versa.

För att öka säkerheten vid användande av modem kan en metod för motringning användas. Detta innebär att förbindelsen kopplas ned efter att användaren har identifierat sig. Om användaren finns registrerad i datorsystemet, kopplar systemet åter upp förbindelsen till ett för användaren registrerat telefonnummer. Denna metod används också när debiteringen för sessionen ska belasta systemägaren istället för användaren [ITS 1994, s. 44].

Då det vid motringning är en tidslucka mellan ned- och uppkoppling finns risken att en angripare tar över förbindelsen. För att få högre säkerhet än vad som kan fås med ett motringningsmodem kan organisationen använda sig av ett krypteringsmodem. Detta är ett modem som har förmåga att kryptera den trafik som kommuniceras mellan parterna. Det krävs att båda parterna har modem som innehåller samma krypteringsnyckel. Nackdelar med krypteringsmodem är att de enbart kan skydda kommunikation över det allmänna telefonnätet och finns det många modem inom organisationen blir administrationen av krypteringsnycklarna komplicerad.

Brandvägg

En brandvägg är en dator som avskiljer ett publikt nätverk, till exempel Internet, från organisationens interna nät. Denna dator har programvara som möjliggör att viss trafik inte släpps in i det interna datorsystemet.

Brandväggens främsta uppgift är att stänga ute otillåten trafik och inte att kontrollera att överföring sker säkert. Om en organisation har behov av att kunna nå företagets interna nätverk från det publika nätverket löses detta med hjälp av autentisering [SIG Security 1995, s. 131].

Förutom att stänga ute den trafik som är otillåten enligt organisationens säkerhetspolicy kan brandväggen autentisera användare, fokusera organisationens säkerhetsinsatser till en punkt, skydda åtkomst till känslig information på nätet, logga och analysera nätverkstrafiken [SIG Security 1995, s. 131]. Den vanligaste konfigurationen av en brandvägg är att släppa igenom e-post och World Wide Web (WWW). Om brandväggen öppnas för att kunna släppa igenom viss typ av information ökar risken för den del av systemet som är bakom brandväggen och som kommer att använda denna information [SIG Security 1995, s. 86]. Till exempel; alla brandväggar har inte möjlighet att se om de elektroniska brev som slussas in i systemet innehåller makrovirus eller virusmittade filer.

Det kan förekomma fel i brandväggens programvara, brandväggen kan installeras eller konfigureras fel och en brandvägg kan svårigen stoppa alla felaktiga filer. Av dessa anledningar ska brandväggen kompletteras med skydd i datorprogrammen, i persondatorerna och det ska finnas väl fungerande säkerhetsrutiner i organisationen.

Intelligenta hubar

En hub, eller ett nav som den också kallas, är en enhet som kopplar ihop datorutrustningen som står i organisationens lokaler. En intelligent hub kan styra vilka anslutningar som får kommunicera med varandra. Den kan också förvränga delar av kommunikationen för att förhindra obehörig avlyssning [SIG Security 1995, s. 87].

De främsta nackdelarna med att använda intelligent hub är att den enbart kan skydda det lokala nätverket och att administrationen blir betungande om ett flertal intelligenta hubar används utspritt över organisationen [SIG Security 1995, s. 88].

Krypterande router

I samband med datorkommunikation används en enhet som väljer den bästa vägen för det som ska föras från avsändare till mottagare. Denna enhet kallas för router. En router används i komplexa nätverk där det kan göras flera olika vägval till mottagaren. Routern ser på adressen på brevet och väljer den för tillfället bästa transportvägen [Freedman 1991, s. 513].

En router med krypteringsfunktion har möjlighet att kryptera den trafik som kommuniceras över

ett publikt nätverk (WAN) [SIG Security 1995, s. 90].

Följande fakta bör beaktas när krypterande routers används [SIG Security 1995, s. 90]:

- Alla routers som används måste köpas från samma leverantör för att kommunikationen ska kunna ske obehindrat.
- Det lokala nätverket kan inte skyddas av den krypterade routern. (Det kan däremot den intelligenta hubben.)
- Det går inte att erhålla åtkomstkontroll med hjälp av en krypterande router. Detta kan däremot åstadkommas med hjälp av en brandvägg.

4.5 Tillämpning av tekniska lösningar

4.5.1 Inledning

Ett företag kan skydda sin information och sina resurser i huvudsak med tre olika angreppsvinklar; fysiskt skydd, logiskt skydd och organisatoriskt skydd.

Fysiskt skydd är det som avser att skydda allt utanför organisationens datorsystem [ITS 1994, s. 8]. Det är med andra ord skydd mot till exempel inbrott, brand eller vattenskador. Skyddet kan vara uppbyggt kring olika sorters larm, inbrottsäkra lås och fönster eller driftsövervakning.

Nästa skyddsnivå vad gäller organisationens säkerhet är det logiska skyddet. Det ska bland annat skydda information och program som finns lagrade på datorns hårddisk samt hindra obehöriga att komma över organisationens information [SIG Security 1996, s. 91].

Organisatoriskt skydd omfattar anställdas beteende och de konsekvenser detta medför [SIG Security 1996, s. 91]. Merparten av organisatoriska skyddet omfattar utbildning av och information till de anställda. Detta skydd kommer att diskuteras vidare i kapitel fem— Riktlinjer för distansarbete.

För organisationen är det viktigast att skydda data och program, därefter kommer skydd av den tekniska utrustningen [SIG Security 1996, s. 92]. Det är avsevärt svårare att ersätta förlorad information än vad det är att ersätta förlorad utrustning [Nordqvist 1996a, s. 3].

Av denna anledning kommer kapitlet fokusera på tillämpningar av tekniska lösningar för logiskt skydd. För tydlighetens skull har denna diskussion delats upp i två delar; säkerhet i samband med användande av en persondator och säkerhet i, kring och mellan datornätverk.

4.5.2 Fysisk säkerhet

Det är viktigt att skilja på fysiskt skydd på huvudarbetsplatsen och på hemarbetsplatsen. I denna uppsats kommer inte fysisk säkerhet på huvudarbetsplatsen att beröras, då författaren förutsätter att denna är ordnad oavsett om organisationen har, eller inte har, infört distansarbete.

Då en organisation tillåter att de anställda arbetar på distans innebär det ökade risker för organisationens integritet, sekretess och tillgänglighet. Ju mer distribuerad organisationens information är desto svårare är det att ha kontroll över att ingen obehörig person kommer över information eller utrustning.

Eftersom en organisations information av olika anledningar distribueras, speciellt i samband med distansarbete, bör lämpliga åtgärder vidtagas för att förbättra integritet, sekretess och tillgänglighet.

Om obehöriga personer kommer in på arbetsplatsen kan de orsaka tre problem; de kan stjäla utrustning eller information, förstöra utrustning eller få syn på alternativt förstöra känslig information. Åtgärder som hindrar detta är låsta dörrar och fönster, stöldskyddad dator, inbrottslarm, diskettlås och utloggning efter en viss tids inaktivitet. Skyddsåtgärder som hindrar att utrustningen förstörs av annan anledning än av mänsklig vilja, är till exempel brandutrustning på arbetsplatsen.

Ett bra skydd mot både stöld och brand är att låsa in känslig information i ett förvaringsskåp [Nordqvist 1996a, s. 3]. Det är viktigt att rätt typ av förvaringsskåp väljs. Vissa typer av skåp är brandsäkra under förutsättning att enbart papper förvaras i skåpet [Elgemyr et al 1992, s. 96]. Om syftet är att förvara datamedia ska ett förvaringsskåp som är avsett för detta väljas.

Den som arbetar på distans kan vidtaga några förebyggande åtgärder som underlättar situationen om olyckan skulle vara ett faktum. Om den tekniska utrustningen märks med företagets organisationsnummer och datorns tillverkningsnummer

noteras separat, underlättas spårandet av den stulna utrustningen [Nordqvist 1996c, s. 2]. Arbetstagare som arbetar på distans bör ta säkerhetskopior med jämna mellanrum. Dessa säkerhetskopior ska inte förvaras på samma plats som originalet, då syftet är att lätt komma igång efter en stöld eller en brand.

De främsta fysiska hoten mot en persondator är inte brand eller översvämnings olyckor. Istället är det främsta hotet användarens beteende vid användande av datorn [SIG Security 1996, s. 106]. Ofta utsätts en dator för omkullvälta kaffekoppar, brödsmlor, gem, damm, cigarettrök eller andra för datorn främmande föremål. När en dator används bör användaren vidtaga allmän försiktighet så att hårdvaran inte skadas.

När arbetstagaren är på tjänsteresa kan den lös- tagbara hårddisken om möjligt förvaras i krypterad form och förvaras på annan plats än själva datorn. Det är mycket viktigt att de anställda är medvetna om riskerna med att lämna datorn, eller viktiga data, utan uppsikt. De anställda måste få information om att hotellrummet inte är en säker plats att lämna datorn på. Ett tips till de resande arbetstagarna är att lämna datorn (CPU) på hotellrummet och ta med hårddisken i fickan.

4.5.3 Säkerhet och persondatorn

De problem som uppkommer när persondatorer används beror inte på maskinerna i sig, utan orsaken är användarna av maskinerna. Många användare är inte medvetna om de hot och risker som existerar mot informationen i och med att den lagras på en persondator.

De hot som finns när en persondator används, aktualiserar alla delar av informationssäkerheten— integritet, sekretess och tillgänglighet [Pfleeger 1989, s. 347].

Integritet

Ett bra integritetsskydd innebär att ingen obehörig användare har möjlighet att ändra eller förstöra den information som existerar inom organisationen. De tekniska lösningar som tillsammans skapar ett integritetsskydd är:

- Stark autentisering av användaren vid uppkoppling. Detta hindrar att obehöriga kommer åt program och filer.
- Kryptering av den information som finns lagrad på hårddisken. Detta försvårar för obehöri-

ga att komma åt informationen på hårddisken om datorn till exempel stjäls.

- Virussydd ska finnas på varje persondator. Det är även lämpligt att undvika piratkopierad mjukvara.

Dessutom bör användarna hantera och förvara informationen på ett sätt så att obehöriga inte har möjlighet att förändra, förstöra eller skapa ny information.

Sekretess

God sekretess uppnås när enbart behöriga användare har möjlighet att läsa information som finns lagrat i en dator, lagringsmedia eller är skrivet på ett papper.

För att uppnå en god sekretess vad det gäller persondatorn finns det flera tekniker som tillsammans skapar ett acceptabelt skydd:

- Kryptering av den information som finns på hårddisken. Detta försvårar för obehöriga att läsa vad som är lagrat på hårddisken om datorn till exempel stjäls.
- Användarna bör hantera känsliga data på ett sätt så att informationen inte avslöjas för obehöriga. Exempel på detta är att en upplagd persondator, ett lagringsmedia eller en utskrift inte ska lämnas obebvakad.
- Hanteringen och förvaringen av hård- och mjukvara ska vara i enlighet med organisationens riktlinjer för informationssekretessen.
- Skydd mot RÖS-avlyssning.
- Stark autentisering av användaren vid uppkoppling. Autentiseringen kan ske med hjälp av någon kombination av flera autentiseringsprinciper (något du bär, något du har eller något du vet).
- Virussydd ska finnas på varje persondator. Det är även lämpligt att undvika piratkopierad mjukvara.

Tillgänglighet

Användaren ska ha tillgång till de resurser som han eller hon har rätt att utnyttja, de ska kunna utnyttjas efter behov, i förväntad utsträckning och inom önskad tid [ITS 1994, s. 14].

Under förutsättning att den fungerar, är den stationära datorutrustning som är placerad på hemarbetsplatsen rimligtvis tillgänglig dygnet runt.

Tekniska lösningar som finns för att minska risken att resurserna blir otillgängliga för användarna är:

- För att förhindra att information försvinner kan fysiskt skydd tillämpas; låsa fast datorn, låsbara skåp och säkerhetskopiering.
- Regelbunden säkerhetskopiering av informationen som finns lagrad på hårddisken. Denna säkerhetskopiering underlättar uppstarten efter en systemkrasch.
- Förvaring och hantering av hård- och mjukvara ska ske på ett sätt så att de inte kan ta skada eller stjälas. Till exempel bör inte utskrifter lämnas utan uppsikt—de kan stjälas.
- En dator är känslig mot kyla, värme, fukt och hårda stötar, därför bör en dator hanteras varsamt och förvaras på lämpligt sätt.
- Virussydd ska finnas på alla persondatorer. Piratkopierad mjukvara bör undvikas.

Så länge som en resurs inte är avsedd att delas av flera användare bör den enskilda användaren inte tillåta att annan användare, till exempel familjemedlemmar, utnyttjar resursen.

Organisationen bör tillhandahålla original program av systemfiler och teknisk hjälp i händelse av att en användare använder persondatorn eller annan utrustning på ett sätt så att de blir otillgängliga. I händelse av att användaren experimenterar med datorsystemet kan inställningar eller andra driftsberoende datafiler ändras eller raderas.

Innan organisationens datorsystem drabbas av ett längre stopp bör en katastrofplan utarbetas. Syftet med denna är att hålla organisationen och aktiviteterna igång—även i en katastrofsituation.

4.5.4 Säkerhet i nätverk

Detta kapitel förutsätter att den kommunikation som sker förs över ett säkert kommunikationsmedium och att detta medium används genomgående i datornätverket.

Ett säkert kommunikationsmedium är där dataöverföringarna sker från behöriga användare till behörig och avsedd mottagare. Överföringen ska vara omöjlig att förstöra eller ändra utan upptäckt. Det ska också vara omöjligt att avlyssna.

kommunikationen. Överförd information ska också vara tillgänglig för den avsedda mottagaren.

Integritet

Att ha god integritet i ett datornätverk innebär att enbart behöriga användare har möjlighet att ändra, radera och skapa ny information. Detta kan realiseras med hjälp av följande tekniker:

- Klassificering av organisationens information är en metod för att se till att enbart behöriga användare kan ändra den information som finns lagrad i datornätverket. Klassificeringen hindrar behöriga användare att göra förändringar i de delar av nätverket där de egentligen inte har något att göra.
- Om användaren använder stark autentisering vid uppkoppling mot nätverket hindras obehöriga från att utnyttja de resurser som tillhör nätverket.
- Åtkomstkontroll används för att stoppa obehöriga användare från att komma in i nätverket. Åtkomstkontroll kan också användas för att låta behöriga användare komma åt hela eller en viss del av nätverket. På så sätt kan ett urval användare ändra i den information som finns lagrad.
- Om aktiviteterna i nätverket loggas kan det hjälpa till vid ett spårningsarbete ifall information har förändrats, om användare har experimenterat med nätverket eller om det har skett obehörigt intrång i nätverket.
- Att använda digital signatur vid överföring av information på nätverket innebär att avsändaren senare inte kan förneka att informationen sändes av honom eller henne.
- Beräkning av kryptografisk kontrollsumma på informationen som skickas i nätverket eller som finns lagrad, möjliggör ett upptäckande om ändringar har gjorts av någon som var obehörig att göra detta.
- Information som transporteras över nätverket och som lagras på datorer vilka är anslutna till nätverket bör krypteras. Då obehöriga användare inte ser vad det är för information, blir det svårare för dem att ändra i informationen. Kryptering kan göras med hjälp av krypteringsprogram, krypteringsmodem, intelligenta hubar eller krypterande routers.

- En brandvägg kan användas för att ha kontroll på trafiken mellan det interna och det externa nätverket. Med en brandvägg kan i viss mån virus filtreras bort, obehöriga användare kan hållas på avstånd och tillsammans med åtkomstkontrollen kan det interna nätverket delas upp i olika delar.
- Organisationen bör ha ett aktuellt antivirusprogram som regelbundet uppdateras, eftersom det ofta upptäcks nya typer av virus.
- Det bästa skyddet mot virus är att personalen inom organisationen har kunskap om virus, hur det sprids och hur man bäst skyddar sig.

Sekretess

- Klassificering av organisationens information är en metod för att se till att enbart behöriga användare kan läsa den information som finns lagrad i datornätverket.
- Om stark autentisering används vid uppkoppling mot nätverket hindras obehöriga från att få tillgång till och insyn i organisationens datornätverk.
- Åtkomstkontrollen hindrar obehöriga från att ta del av informationen i nätverket.
- Loggning av aktiviteter i nätverket underlättar upptäckt ifall någon obehörig användare har kommit in i nätverket.
- All information i och kring nätverket bör krypteras så att obehöriga användare inte kan ta del av den.
- Datorutrustningen och eventuellt lokalerna bör RÖS-skyddas.
- Skyddet mot att mänsklig kommunikation avlyssnas är att informera de anställda om att inte ha konfidentiell diskussion bland allmänheten.
- Brandvägg kan användas för att obehöriga användare inte ska kunna ta del av informationen i nätverket. Brandväggen kan också dela upp det interna nätverket så att informationsklassificeringen kan realiseras.
- Organisationen bör ha ett aktuellt antivirusprogram och regelbundet utbilda personalen om risken med och skyddet mot virus.

Tillgänglighet

God tillgänglighet i ett nätverk innebär att behöriga användare kommer åt de resurserna som tillhör nätverket i fråga. Följande tekniska lösningar finns för att säkerställa att användarna kan komma åt resurser i förväntad utsträckning och inom önskad tid:

- Klassificering av organisationens information kan hindra behöriga användare att, med eller utan avsikt, göra något som påverkar möjligheten att utnyttja resurserna i datornätverket.
- Autentisering och åtkomstkontroll hindrar obehöriga från att upptaga resurser som behöriga användare ska använda. Dessutom kan autentisering och åtkomstkontroll hindra att en användare experimenterar i datornätverket.
- Om aktiviteterna i nätverket loggas, kan det hjälpa till vid ett spårningsarbete ifall en behörig eller en obehörig användare har påverkat datornätverkets tillgänglighet för de behöriga användarna.
- Genom att brandväggen håller obehöriga användare på avstånd får de behöriga användarna tillgång till datornätverket.
- Ett antivirusprogram bör användas och det bör uppdateras regelbundet. Personalen bör utbildas om riskerna med datorvirus och hur de ska agera i händelse av att de drabbas av datorvirus.
- Om organisationen har krav på att alltid ha tillgång till datorerna kan det vara lämpligt med reservsystem och avbrottsfri kraft (UPS).
- Inom organisationen kan det finnas möjlighet för de anställda att få experthjälp om datorn eller programvaran inte fungerar. Denna hjälp bör distansarbetaren kunna få över telefonen.

5 Riktlinjer för distansarbete

5.1 Inledning

När en organisation ska införa distansarbete finns en mängd frågor att tänka på och att ta ställning till. Detta kapitel klargör, utifrån de två tidigare kapitlen, hur arbetsgivare och arbetstagare bör agera. Informationen i kapitlet bygger på de tidigare kapitlen i denna uppsats. Dessutom görs

hänvisningar till de fem bilagorna till examensarbetet. Dessa bilagor är fem olika avtal om distansarbete som antingen används inom ett företag eller är publicerade av SIG Security.

Referenser görs till bilagorna för att tydliggöra hur respektive fråga har lösts i pågående projekt kring distansarbete. Samtliga avtal tar upp arbetsrättsliga frågor. De företag som har dokumenterat hur de ska uppnå en god informationssäkerhet, har klassat dessa dokument som konfidentiella. Författaren har därmed inte kunnat ta del av företagets ställningstagande i denna fråga. Avsnittet om riktlinjer för tekniska frågor är därför inriktat på vad som praktiskt kan göras för att bibehålla informationssäkerheten vid distansarbete.

Det sista avsnittet behandlar frågor som inte naturligt ingår i de två andra grupperna.

5.2 Riktlinjer för lagarna

5.2.1 Arbetsmiljö

I avtalet som arbetsgivaren och arbetstagaren skriver bör det betonas att arbetsgivaren har fullständigt ansvar vad det gäller arbetsmiljöfrågorna. Det är lämpligt att arbetsgivaren ser till att arbetstagaren har en god arbetsmiljö på distansarbetsplatsen. För att arbetsgivaren ska kunna försäkra sig om att det råder en god arbetsmiljö, kan nödvändiga kontorsmöbler inköpas åt arbetstagaren. Det förekommer att arbetsgivaren köper in skrivbord, kontorsstol och bordsbelysning [Bilaga 1, s. 2 och 5, Bilaga 3, s. 3] Arbetstagaren får betala ifall en om- eller tillbyggnad görs, ventilation måste installeras, eller en sanering behöver göras för att distansarbetet ska kunna påbörjas i bostaden [Bilaga 1, s. 2 och 5].

Då det är frivilligt att börja distansarbete borde arbetstagaren acceptera att arbetsgivaren inspekterar arbetsmiljön när distansarbetet inleds. Det är då lämpligt att arbetsgivaren dokumenterar vilket utgångsläge som gäller; hur kontorsrummet är möblerat. Det är för den möbleringen och det möblemang som arbetsgivarens ansvar gäller. Om arbetstagaren sedan möblerar om eller byter möblemang är inte arbetsgivaren ansvarig för en eventuellt dålig arbetsmiljö.

Arbetsgivarens ansvar för arbetsmiljön kan mycket väl relateras till graden av distansarbete. Om arbetstagaren arbetar på distans en dag per vecka är det rimligt att kravet på arbetsgivarens

ansvar blir mindre än om distansarbete sker fyra dagar per vecka.

5.2.2 Arbetsskador

Även om arbetsskadeförsäkringen gäller då arbete sköts på distans, är det viktigt att det finns en överenskommelse mellan arbetsgivare och arbetstagare om att distansarbete sker. Om det inte finns en överenskommelse kan arbetstagaren få problem vid bevisföringen om att skadan har skett under arbetstid [SIG security 1996, s. 39].

Arbetsmarknadsstyrelsen har i sitt avtal med arbetstagarna som arbetar på distans uttryckligen förklarat de är skyddade av arbetsskadeförsäkringen under sin arbetstid [Bilaga 1, s. 2]. Siemens Nixdorf refererar till Försäkringskassan som oavsett platsen för arbetet tillämpar samma regler för sjukdom, arbetsskador och så vidare [Bilaga 3, s. 1].

5.2.3 Arbetstid och tillgänglighet

Eftersom arbetstidslagen inte är tillämplig vid distansarbete (se avsnitt 3.3.3), bör arbetstiden preciseras i avtalet som skrivs. Arbetsmarknadsstyrelsen och Telia har gjort på detta sätt [Bilaga 1, s. 1 och 4, Bilaga 4, s. 1].

Ett annat sätt för arbetsgivaren att hantera arbetstagarens arbetstid och eventuella övertid är att tillämpa så kallad oreglerad arbetstid. Detta innebär att distansarbetaren fritt får disponera sin tid, och kan då inte få någon övertidsersättning. Detta tillvägagångssätt rekommenderas av arbetsgivarverket i det allmänna löne- och förmånsavtalet (ALFA) [Arbetsgivarverket 1996, s. 26, Bilaga 5, s. 1].

I ALFA kapitel 4, 14 § står det att överenskommelsen om att tillämpa oreglerad arbetstid ska vara skriftlig och avse en period om högst ett år. I samma kapitel 28 § förklaras att den arbetstagare vars arbetstid inte kan kontrolleras, eller den arbetstagaren som får förtroendet att själv disponera sin tid ska ha oreglerad arbetstid [Arbetsgivarverket 1996, s. 26 och 34].

Det bör i avtalet regleras när arbetstagaren ska vara tillgänglig för medarbetare, chefer, kunder med flera. Det vanligaste är att det i avtalet är tydligt definierat under vilka tider och var någonstans som arbetstagarens arbete ska ske [Bilaga 1

s. 1 och 4, Bilaga 2, s. 1, Bilaga 3, s. 2 och 5, Bilaga 4, s. 2, Bilaga 5, s. 1 och 2].

För att arbetstagaren ska kunna delta i den sociala kontakten på arbetsplatsen och ha framgång i sin kompetens- och karriärutveckling, bör antalet dagar begränsas då arbetet sköts på distans. Det är mycket svårt för den anställde att delta i det informella kontaktnätet på huvudarbetsplatsen om distansarbetets omfattning är 5 dagar i veckan.

5.2.4 Anställningstrygghet

För att garantera den anställdes anställningstrygghet när distansarbete tillämpas bör distansarbetsplatsen organisatoriskt tillhöra huvudarbetsplatsen. Fyra av fem studerade avtal har löst frågan om anställningstrygghet på detta sätt [Bilaga 1, s. 4, Bilaga 2, s. 2, Bilaga 3, s. 1, Bilaga 5, s. 1].

5.2.5 Semesterfrågor

Enligt Jan Häggström på Arbetsgivarverket ska distansarbetaren få semester lön på 12% av den utbetalade lönen. Arbetstagaren får sedan själv ordna med sin ledighet. I praktiken tillämpas detta förfarande då arbetstagaren uteslutande arbetar på distans [TCO 1987, s. 29].

I de fall då distansarbete är ett komplement till att arbeta på huvudarbetsplatsen regleras semesterfrågan i det avtal som skrivs mellan arbetstagaren och arbetsgivaren. En lämplig lösning är att i avtalet specificera att arbetstagaren har rätt till semester som om denna hade arbetat på huvudarbetsplatsen under den aktuella tidsperioden [Bilaga 2, s. 2, Bilaga 5, s. 1].

5.2.6 Skattefrågor

Den utrustning som arbetstagaren har på sin distansarbetsplats bör vara anpassad för arbetsuppgifterna. På så sätt kan arbetstagaren slippa förmånsbeskattning för erhållen utrustning. Generellt kan det sägas att om arbetstagaren enbart ska utföra enklare ordbehandling på distansarbetsplatsen bör utrustningen inte vara en multi-mediedator. Det är också viktigt att utrustningen inte används för privat bruk eller med egna datorprogram om förmånsbeskattning ska undvikas [Bilaga 1, s. 5, Bilaga 3, s. 5, Bilaga 4, s. 2, Bilaga 5, s. 2].

Om arbetstagaren får hyresersättning av arbetsgivaren för att upplåta en del av sin bostad till arbetsutrymme, betraktas denna ersättning som inkomst av tjänst. Följaktligen ska hyresersättningen beskattas. Att göra skatteavdrag för detta ställer sig skattemyndigheten mycket restriktiva mot.

Möjligheten finns att undvika det komplexa regelverket som en hyresersättning medför, genom att i avtalet specificera att ingen ersättning betalas ut för den del av bostaden som tillhandahålls för arbetet [Bilaga 3, s. 3, Bilaga 4, s. 2, Bilaga 5, s. 3].

Arbetstagaren får vanligtvis inte ersättning för städningen av kontorsytan i hemmet, inte heller för att förbrukningen av elektricitet ökar när arbetet sköts hemifrån [Bilaga 3, s. 1 och 3, Bilaga 4, s. 2]. Inom vissa organisationer står arbetsgivaren för telefonkostnaderna som har samband med distansarbetet [Bilaga 1, s. 2, Bilaga 5, s. 3].

Slutligen kan det nämnas att Skattelagstiftningen är dåligt anpassad till distansarbete [UD 1996, s. 8]. Det går nästan att påstå att skattesystemet missgynnar distansarbete från hemmet, eftersom arbetsresor är avdragsgilla medan avdrag för arbetsrum i bostaden behandlas som sagt, mycket restriktivt av skattemyndigheten [Paavonen 1992, s. 102].

5.2.7 Hyreslagen

Till syvende och sist är det hyresvärden som avgör ifall distansarbetet innebär en kontorisering av bostaden. För att undvika att hyresgästen förlorar sin hyresrätt kan det vara lämpligt att innan distansarbetet påbörjas, kontrollera med sin hyresvärd om dennes inställning i frågan [Bilaga 1, s. 2].

Så länge som distansarbetet inte stör grannarna eller innebär något större slitage på lägenheten, borde arbete från hemmet inte innebära några problem med hyresvärden eller bostadsrättsföreningen. Att i sin egna villa avsätta ett rum för distansarbete vållar i praktiken inga problem kring bostadsfrågan [SIG Security 1996, s. 71].

5.2.8 Försäkringsfrågor

När en arbetstagare ska arbeta på distans, placeerar ofta arbetsgivaren datorutrustning i arbetstagarens hem. Då detta sker bör försäkringsfrågan begrundas. Det är inte säkert att arbetsgivarens försäkring omfattar den utrustning som är place-

rad utanför arbetsgivarens lokaler. Det är inte heller säkert att arbetstagarens hemförsäkring täcker sådan egendom som inte tillhör försäkringstagaren. Av de studerade avtalen är majoriteten formulerade så att arbetstagarens hemförsäkring ska utnyttjas vid skada som har orsakas av eller har ett tydligt samband med arbetsgivarens utrustning [Bilaga 1, s. 2 och 5, Bilaga 3, s. 2 och 3, Bilaga 4, s. 2, Bilaga 5, s. 2]. Det kan därför vara lämpligt att arbetstagaren kontrollerar med sitt försäkringsbolag att hemförsäkringen skyddar utrustningen och de skador som denna kan orsaka i hemmet. I händelse av att hemförsäkringen behöver nyttjas betalar arbetsgivaren självriskkostnader och bonusförlust [Bilaga 1, s. 2 och 5, Bilaga 3, s. 2, Bilaga 4, s. 2, Bilaga 5, s. 2].

Tjänstemännens Centralorganisation (TCO) förespråkar att arbetsgivaren själv ska teckna en försäkring för utrustningen. Ifall utrustningen orsakar skador i arbetstagarens hem ska hemförsäkringen utnyttjas och arbetsgivaren ersätta för självrisk och bonusförlust [TCO 1996, s. 14,].

SIG Security förespråkar i sin tur att arbetsgivaren ska ha en försäkring som täcker såväl arbetsgivarens utrustning som skada som utrustningen orsakar [Bilaga 2, s. 2].

I framtiden kan försäkringsbolagen komma att reservera sig för att hemförsäkringarna ska täcka den egendom som försäkringstagaren har lånat. Hemförsäkringen kan komma att omfatta endast den egendom som försäkringstagaren äger.

5.3 Riktlinjer för tekniken

5.3.1 Fysisk säkerhet

Innan distansarbetet inleds är det viktigt att det finns en god fysisk säkerhet. Om den fysiska säkerheten försummas vid distansarbete ökar risken att information eller utrustning stjäls. Det fysiska skyddet kan delas in i fyra grupper; hindra obehöriga att komma in på distansarbetsplatsen, hantering och förvaring av organisationens information, användarens beteende på distansarbetsplatsen och slutligen skyddsåtgärder som är lämpliga att vidtaga på en tjänsteresa.

Inbrottskydd

Inbrottskyddet på distansarbetsplatsen syftar till att hindra obehöriga personer att komma in på distansarbetsplatsen. Helst ska det finnas ett skydd som hindrar att de överhuvudtaget ser vilken utrustning som används. Syftet med inbrottskyddet är således att förhindra inbrott. Det är även önskvärt att förhindra brand, översvämningsolyckor etcetera.

Det finns enkla åtgärder som den distansarbetande anställde kan vidtaga för att öka skyddet mot inbrott och andra olyckor:

- Lås fast utrustningen till exempel i skrivbordet med godkända låsanordningar.
- Ha lås på datorns diskettenhet.
- Montera en säkerhetsdörr som uppfyller svensk säkerhetsstandard.
- Montera fönsterlås som uppfyller nödvändiga säkerhetskrav.
- Lås alltid dörrar och fönster när bostaden lämnas.
- Iakttag försiktighet med stearinljus och andra öppna lågor.
- Möblera distansarbetsplatsen så att den inte exponeras i onödan. Placera inte datorerna så att det utifrån syns vilken utrustning som används.

Om ett inbrott trots allt sker, finns det åtgärder som underlättar i en sådan situation. Dessa åtgärder bygger på att de har gjorts i förebyggande syfte:

- Märk all utrustning med företagets organisationsnummer.
- Skriv upp utrustningens tillverkningsnummer och förvara denna information på annan plats.
- Ha brandutrustning (brandsläckare och brandvarnare) på distansarbetsplatsen och lär dig att använda dig den.
- Tag säkerhetskopior av alla dokument. Förvara dessa kopior fysiskt avskilda från originalen.

Försäkringsbolagen ställer många av ovanstående punkter som krav för att en vanlig hemförsäkring ska gälla. Åtgärderna borde således inte innebära större uppoffringar för distansarbetaren i samband med att distansarbete ska påbörjas.

Förvaring och hantering av information

Säker hantering och förvaring av organisationens information, innebär att obehöriga personer, som befinner sig på distansarbetsplatsen, inte på något sätt kan ta del av informationen.

Åtgärder som kan vidtagas på distansarbetsplatsen är:

- Lås in pärmar och känsliga dokument när arbetsdagen är slut. Låt dem inte ligga framme på skrivbordet.
- Lås in bärbar utrustning när arbetsdagen är slut eller när bostaden lämnas.
- Förvara dokument och inlåst utrustning i ett förvaringsskåp som kan skydda innehållet vid både angrepp och brand.
- Kasta inte digitala- eller pappersdokument i hushållssoporna.
- Tag med digitala lagringmedia och känsliga pappersdokument till kontoret för en korrekt förstöring.
- Tag ofta säkerhetskopior av digitala dokument. Förvara dessa kopior utanför distansarbetsplatsen, till exempel på huvudarbetsplatsen.
- Ha en skärmläckare med lösenord som aktiveras då datorn har varit inaktiv under en viss tid.

Beteendefrågor

Den anställdes beteende är avgörande huruvida informationens säkerhet kan bibehållas. En anställd kan även orsaka att information försvinner genom att hårdvaran förstörs.

Den distansarbetande yrkesmänniskan kan tänka på följande för att bibehålla den digitalt lagrade informationen:

- Förtär inte mat eller dryck vid datorn, inte heller citrusfrukter då fruktsaften har en lätt frätande inverkan på elektroniken.
- Bruka inte våld mot någon del av utrustningen.
- Stoppa inte in främmande föremål i någon del av utrustningen.
- Diskutera inte sekretessbelagda uppgifter i en mobiltelefon eller direkt med en kollega på allmänna platser.
- Följ organisationens säkerhetsföreskrifter.

- Iakttag försiktighet vad det gäller risken för brand, vattenskador, inbrott etcetera.

På tjänsteresa

Då en anställd är på tjänsteresa ökar risken att information eller utrustning kan stjälas. Anledningen till detta är att den anställda transporterar dokument, träffar många okända människor och befinner sig i, för honom eller henne, okända miljöer.

För att minimera risken att dokument eller utrustning försvinner kan den resande tänka på följande:

- Lämna inte en bärbar dator eller dokument utan uppsikt på tågstationer, flygplatser etcetera.
- Om det är möjligt—förvara hårddisken separat från den bärbara datorn (CPU).
- Ett hotellrum erbjuder inte en riskfri förvaring för datorn och dokumenten. Lämna CPU på rummet och tag med hårddisken till middagsrestaurangen.
- Både datorer och disketter är känsliga för avmagnetisering, temperaturskillnader och för kraftiga stötar.

5.3.2 Säkerhet och persondatorn

När en persondator används på en distansarbetsplats bör åtgärder vidtagas så att integriteten, sekretessen och tillgängligheten bibehålls. Dels bör olika tekniska lösningar implementeras och användas och dels bör de anställda ha en medvetenhet om vilka problem som kan uppkomma när information lagras på datorer.

Sekretess

Majoriteten av de frågor som berör sekretess berör också integritet. Det enda hotet mot sekretessen som inte samtidigt kan hota integriteten är RÖS. För att minska risken att någon obehörig tar upp RÖS från persondatorn kan distansarbetaren tänka på följande:

- Möblera distansarbetsplatsen på ett sådant sätt att datorskärmen inte går att läsa utifrån.
- Placera utrustningen så att det försvåras för obehöriga att komma i närheten av den. Till exempel bör inte utrustningen placeras i ett rum som ligger mot gatan.

- Ljudalstrande utrustning kan, om behov finns, isoleras och ställas på ett ljudisolerande underlag.
- Eftersom det inte går att uppnå ett fullständigt skydd mot RÖS, bör kanske den känsligaste informationen inte behandlas på distansarbetsplatsen.

Integritet och sekretess

Många av de hot som finns i och med att en persondator används hotar både integriteten och sekretessen. Beroende på vad inkräktaren gör påverkas den ena, den andra eller båda.

Oavsett vilket hotet är och vad inkräktaren tar sig för, ökar följande åtgärder chanserna att bibehålla god integritet och sekretess:

- Stäng alltid av datorn då du inte har uppsikt över den.
- Kryptera all känslig information som förvaras på ett lagringsmedium.
- Lås inte funktionerna för autenticering, till exempel att skriva in lösenord.
- Avslöja inte ditt lösenord för någon.
- Byt ofta lösenord. Speciellt viktigt när det finns minsta misstanke om att det har avslöjats för någon.
- Välj enbart bra lösenord, det vill säga längre än sex tecken och gärna en kombination av bokstäver och siffror.
- Skriv inte upp ditt lösenord.
- Använd inte disketter som kommer från okänd källa.
- Ha alltid den senaste versionen av viruskyddet aktivt.
- Låna inte ut persondatorn till övriga familjemedlemmar, vänner eller bekanta.

Tillgänglighet

En persondator på distansarbetsplatsen och informationen som den innehåller kan bli otillgänglig för användaren. För att minimera risken att datorn eller information blir otillgängligt för distansarbetaren kan följande åtgärder vidtagas:

- Utrustning och de lagringsmedia ska hanteras med varsamhet.

- Förvara bärbar utrustning i angrepps- och brandsäkra skåp.
- Ha viruskydd installerat och aktivt på persondatorn.
- Befatta dig inte med piratkopierade program, varken spel eller nyttoprogram.
- Ha, om behov finns, ett system för avbrottsfri kraft (UPS).
- Om persondatorn börjar uppträda på något annorlunda sätt—var misstänksam.

I händelse av att informationen eller datorresurserna blir otillgängliga kan följande förebyggande åtgärder underlätta ett snabbt igångsättande:

- Arkivera originaldisketterna till alla nyttoprogram. Dessa disketter ska vara skrivskyddade.
- Tag säkerhetskopior av informationen som finns på persondatorn.
- Formulera en avbrottsplan och en katastrofplan.
- Tillhandahåll en supportavdelning för de arbetstagare som arbetar på distans. Om persondatorn eller dess information blir otillgänglig ska distansarbetaren kunna få hjälp av organisationen.

5.3.3 Säkerhet i nätverk

När arbetstagaren arbetar på distans är ett vanligt förfarande att elektronisk uppkoppling mot huvudarbetsplatsen sker. Denna uppkoppling sker ofta med hjälp av ett modem. När arbetstagaren är uppkopplad bör säkerhetsåtgärder vidtagas så att obehöriga inte kan ta del av eller ändra i den information som sänds mellan de kommunicerande datorerna. Det är också viktigt att distansarbetaren har möjlighet att få den elektroniska uppkoppling som önskas. För att organisationen ska ha en god säkerhet i sitt kommunikationssystem bör åtkomstkontroll, autenticering, loggning och brandvägg användas.

Ett fåtal av de säkerhetsfrågor som aktualiseras när två datorer kopplas ihop över ett publikt nätverk berör enbart informationens integritet eller sekretess. De allra flesta säkerhetsfrågor som är aktuella i detta sammanhang berör både informationens integritet, sekretess och tillgänglighet. Detta avsnitt har därför delats in i fem delar, där respektive del består av rekommendationer kring de åtgärder som berör samma delar av informationssäkerheten.

Integritet

Det finns tillfällen då det är viktigt att den information som transporteras elektroniskt mellan två datorer förblir oförändrad under transporten.

Det kan i en organisation uppkomma situationer då det utan tvekan måste gå att säga vem det är som är ansvarig för ett visst dokument.

Följande punkter kan hjälpa distansarbetaren i båda situationerna:

- Om den information som överförs måste vara identisk när den kommer fram ska kryptografisk kontrollsumma beräknas.
- Beräkna kryptografisk kontrollsumma på kontakt, avtal, ekonomisk information med mera.
- Ifall det är ett dokument som är eller kan tänkas hamna i ett juridiskt sammanhang, bör användaren skapa en digital signatur.
- Skapa en digital signatur på de dokument där en underskrift skulle göras om det inte vore ett digitalt dokument. Till exempel på kontrakt, avtal, policies och protokoll.

Sekretess

En av de frågor som hotar sekretessen är, i likhet vid användande av en persondator, risken för RÖS. Skillnaden är dock den att vid kommunikation mellan datorer är även de röjande signalerna från överföringskablar aktuella. Den andra typen av fråga som enbart aktualiserar sekretess är avlyssning med hjälp av tjuvkoppling i telefonskåp eller friliggande telefonledningar.

Åtgärderna är samma för dessa båda typer av sekretesshot:

- Kryptera all datatrafik som är av känslig karaktär.
- Avgör om modem och uppringd linje eller en fast uppkoppling ska användas.
- Överväg om konfidentiell information i själva verket ska överföras elektroniskt.

Integritet och sekretess

Av de hot som existerar när information transporteras i ett nätverk kan några påverka både integritet och sekretess. Det enda sätt som finns för att skydda den information som förs över ett nätverk är att kryptera. Följande punkter kan vara

värda att tänka på vid kommunikation mellan två datorer:

- Både inloggningen och informationsöverföringen ska vara krypterad.
- Kryptera all kommunikation, både den som förs på LAN och den som förs på WAN.
- Arbeta gärna med flera olika krypteringsnycklar.
- Förvara kopior av krypteringsnycklarna på minst två oberoende platser. Till exempel på distansarbetsplatsen och i ett bankfack.
- Kryptera och dekryptera information när datorn inte är uppkopplad på ett offentligt nätverk.
- Ha i åtanke att ett elektroniskt brev inte har något skydd för varken sekretess eller integritet.

Enligt den svenska försvarsmaktens riktlinjer är DES för närvarande inte godkänt för att skydda dokument. För hantering av certifiering (se avsnitt 4.4.1) och digitala signaturer har försvarsmakten godkänt RSA som krypteringsalgoritm [Ulf Berglund].

Tillgänglighet

Under förutsättning att datorn på distansarbetsplatsen fungerar är den alltid tillgänglig för distansarbetaren—den ska av säkerhetsskäl inte användas av någon annan än distansarbetaren.

Vad som kan bli otillgängligt för distansarbetaren är möjligheten att komma ut på det publika nätverket (WAN), att komma in på organisationens interna nätverk (LAN) eller att komma åt en specifik del av LAN. Om dessa tillgänglighetsproblem uppstår kan följande underlätta för distansarbetaren:

- Möjlighet att kontakta en supportavdelning för att kunna ställa frågor och få rekommendationer.
- Organisationens modempool bör vara dimensionerad för antalet distansarbetare. Arbetstagnationer som arbetar på distans ska inte mötas av en upptagetton de gånger som LAN kontaktas.
- I händelse av att LAN är otillgängligt bör användaren ha instruktioner så att arbetet under en viss tid, ändå kan skötas.

Integritet, sekretess och tillgänglighet

Majoriteten av de hot som uppkommer när en persondator kopplas upp mot ett nätverk involverar integritet, sekretess och tillgänglighet. Det är inte nödvändigt att alla tre delar av informationssäkerheten hotas samtidigt. Beroende på det specifika hotets händelseförlopp kan det leda till att en eller flera av informationssäkerhetens delar hotas.

Följande åtgärder minskar risken att hoten blir verklighet:

- Använd stark autentisering, kombinera gärna två eller fler autentiseringsprinciper.
- De tekniker som möjliggör god åtkomstkontroll ska värderas och anpassas till den egna organisationen.
- Rutiner för lösenord ska finnas; när de ska bytas och hur de får se ut.
- Skriv säkerhetsregler där det tydligt framgår vilka användare som får göra vad i nätverket och under vilka tider de får göra detta.
- Implementera säkerhetsreglerna i brandväggen.
- Användarna får inte ha för stor tilltro till att brandväggen räcker för att uppnå god säkerhet. Även varje enskild persondator måste ha ett skydd mot eventuella angrepp.
- Det måste finnas någon inom organisationen som underhåller och gör uppföljningar i brandväggen. Utan uppföljning är detta skydd snart meningslöst.
- Radera de konton som tillhör före detta anställda så fort deras anställning har upphört.
- Det bör finnas en begränsning av den tid som de distansarbetarna kan vara uppkopplade mot organisationens nätverk. Detta hindrar att anställda är uppkopplade timmar i sträck.
- Det bör finnas funktioner så att användarna måste upprepa autentiseringen under pågående session. Detta hindrar att en obehörig användare tar över förbindelsen.

Om ett hot trots ovanstående åtgärder blir verklighet kan följande punkter begränsa skadeverkligheterna:

- Klassificera all information. Det är det enda sättet att skilja på information som kräver skydd och information som är offentlig.

- Ha förståelse för de olika klassificeringsnivåerna och vad felklassificering kan leda till.
- Begränsa användarnas tillgång till informationen. Det räcker för en användare att ha tillgång till den information som arbetsuppgifterna kräver, den så kallade "need-to-know" principen.
- Logga händelser i nätverket. Till exempel kan alla, lyckade och misslyckade, inloggnings till systemet registreras.
- Det bör inom organisationen finnas någon som är ansvarig för att regelbundet gå igenom loggen och vid behov göra uppföljning av denna.
- Ha ett uppdaterat virusskydd aktivt på alla datorer som är anslutna till nätverket.
- Det bör finnas en åtgärdsplan ifall något obehörigt intrång sker på nätet.

5.4 Riktlinjer för övriga frågor

5.4.1 Beslutsfattare

När en arbetstagare önskar att distansarbete finns några frågor som en beslutsfattare bör ha i åtanke innan projektet inleds och under projektets gång. Följande punkter är aktuella för beslutsfattarna inom en organisation:

- Skriv avtal med de anställda som önskar att arbeta på distans. I avtalet bör det bland annat framgå vad som är arbetstid, vad som klassas som tjänsteresa och hur utrustningen ska hanteras.
- Sker avtalsbrott från arbetstagarens sida, ska disciplinåtgärden vara samma som om händelsen skett på huvudarbetsplatsen.
- Bedöm vilka av arbetstagarens arbetsuppgifter som är lämpliga för distansarbete. En förutsättning är att arbetstagaren kan uppvisa resultat och/eller prestation.
- Kan den anställdes alla arbetsuppgifter skötas på distans, eller behövs ett påbud att vissa uppgifter ska skötas från huvudarbetsplatsen, till exempel på grund av sekretess.
- Bedöm om arbetstagaren av sekretess och integritets skäl behöver ha ett enskilt arbetsrum på distansarbetsplatsen.
- Se till att distansarbetarna kan utföra sitt arbete även om de inte kommer i kontakt med företags nätverk vid önskad tidpunkt.

- Förbjud piratkopierade program, både spel och nyttoprogram.
- Tag fram en katastrofplan som kan följas om något allvarligt händer; inbrott, brand etcetera.
- All personal bör kontinuerligt utbildas och in-formeras om säkerhetsfrågor, organisationens hotbild etcetera.
- Distansarbete bör drivas som ett tidsbegränsat projekt och en utvärdering bör göras när projekt-tiden har gått ut.

När arbetstagarna sköter sitt arbete på distans kan det uppstå problem med kommunikation, ledning och kontroll av arbetet. Ju fler dagar per vecka som någon distansarbetar desto tydligare och mer akuta blir problemen [Paavonen 1992, s. 69 och 71, Forsebäck 1995, s. 111].

Den tid som distansarbete sker är det viktigt att arbetsgivaren fokuserar på vilka resultat som arbetstagaren uppnår och inte, som traditionellt är, den fysiska närvaron. Det är avsevärt mycket viktigare att arbetstagaren vet vad som ska göras och inte hur det ska göras. För att arbetstagaren ska kunna veta detta, krävs klara mål och tydliga spelregler. Arbetsledningen ska värna om den nödvändiga tydligheten, sätta övergripande mål och hålla samman arbetsstyrkan. De arbetstagare som arbetar på distans måste få förtroende att fatta de snabba besluten på egen hand. En informationsbaserad organisation bygger på decentralisering av både beslutsfattande och ansvar. Detta ger en smidig och snabb organisation.

Det finns några punkter som projektet distansarbete bör vila på [Forsebäck 1995, s. 101]:

- Projektet ska ha ett bestående värde för både arbetstagare och arbetsgivare.
- Det ska vara frivilligt att delta i projektet.
- Både arbetstagare och arbetsgivare ska kunna återgå till den gamla arbetsformen.
- Arbete på distans ska inte ske fem dagar i veckan. Arbetet på distans ska kompletteras med möten med arbetskamrater och arbetsledning.

5.4.2 Arbetstagare

När en arbetstagare arbetar på distans finns det några viktiga punkter för honom eller henne att tänka på:

- Det bör finnas någonstans dit arbetstagaren kan vända sig om det uppstår problem på distansarbetsplatsen.
- Arbetstagaren ska veta hur han eller hon ska gå tillväga om information eller hårdvara till exempel går sönder eller försvinner.
- Arbetstagare och arbetsgivare ska komma överens om vad som är känsligt material. På grund av sekretess och integritet får det känsligaste materialet inte hanteras på distansarbetsplatsen.
- Det ska vara tydligt vilken typ av information som arbetstagaren får hantera på distansarbetsplatsen.
- Distansarbetaren bör skriva ett avtal med övriga familjemedlemmar. Det kan bli konflikter med familjen för att hushållssysslorna inte sköts när dagarna faktiskt tillbringas i hemmet.
- Distansarbetaren bör ha en ordnad barnomsorg under arbetstid. Det är möjligt att arbetsgivaren ställer detta som ett krav i det avtal som skrivs mellan arbetsgivaren och arbetstagaren.
- Distansarbetaren ska alltid följa de säkerhetsföreskrifter och säkerhetsrutiner som organisationen förordar.

6 Slutsatser

6.1 Resultat

Detta examensarbete har berört två viktiga områden i samband med att en arbetstagare börjar arbeta på distans; arbetsrätten och de tekniska lösningarna för att bibehålla informationssäkerheten. Inom respektive område finns det frågeställningar som arbetstagaren och arbetsgivaren måste vara överens om innan distansarbetet inleds.

Innan distansarbetet påbörjas bör det inom organisationen skrivas avtal och regler kring säkerhetsfrågorna. Det bör skrivas en säkerhetspolicy, formuleras en avbrottsplan och en katastrofplan. Dessutom måste ansvarsfrågorna vara tydliga, det måste finnas någon som är ansvarig för brandväggen, för loggen och för övrig implementerad säkerhetsteknik. Det ska i alla situationer vara klart och tydligt vem det är som har ansvaret för informationen inom organisationen.

Arbetsgivaren bör i varje enskild önskan om att arbeta på distans gå igenom individens förutsättningar för detta. Följande frågor bör arbetsgivaren beakta innan distansarbete blir aktuellt:

- Hur är arbetstagarens hemförhållanden? En arbetstagare med problem i äktenskapet bör generellt inte arbeta på distans. Undantag från detta är om problemen har orsakats av att arbetstagaren på grund av arbetet tvingas till veckopendlning.
- Har arbetstagaren missbruksproblem? En alkohol- narkotika- eller spelmissbrukare bör inte arbeta på distans.
- Är arbetstagarens arbetsuppgifter av sådan karaktär att de går att sköta på distans?
- Har arbetstagaren förmåga att arbeta självständigt?
- Hur stort behov har arbetstagaren av ett socialt umgänge på arbetstid?
- Har arbetstagaren lång erfarenhet av de arbetsuppgifter som kommer att skötas på distans?
- Har arbetstagaren en god organisationsförmåga och lätt för att kommunicera på avstånd?
- Har arbetstagaren en god portion självförtroende?
- Är arbetstagaren pålitlig?
- Är arbetstagaren resultatnriktad och en god problemlösare?
- Har arbetstagaren motivation och självdisciplin?

Om det blir aktuellt med distansarbete i organisationen är det lämpligt att först driva ett pilotprojekt [Nordqvist 1996b, s. 4]. Detta pilotprojekt ger möjlighet att förstå hur distansarbete påverkar den egna verksamheten och gör det möjligt att genomföra utvärderingar. Som det beskrevs i kapitel 5.4.1, ska det vara frivilligt att delta i projektet och det ska ha ett bestående värde för alla deltagare.

Innan distansarbetet påbörjas bör ett avtal skrivas mellan arbetsgivaren och den enskilda arbetstagaren. I detta avtal ska frågor kring arbetsrätten regleras, avtalas vilka kostnader som arbetsgivarens ska stå för och tydliggöras hur utrustningen är försäkrad. Det kan vara lämpligt att i avta-

let nämna hur distansarbetaren och arbetsgivaren ska agera så att en god informationssäkerhet erhålles.

För att den definition av distansarbete som har valts i avsnitt 3.1 ska vara tillämpbar, måste ett avtal skrivas mellan arbetstagaren och arbetsgivaren. Anledningen är att definitionen inleds med "distansarbete råder när en enskild arbetstagare som enligt överenskommelse med arbetsgivaren...". Definitionen innebär således att ett avtal måste tecknas mellan arbetstagaren och arbetsgivaren.

Det avtal som skrivs mellan arbetsgivaren och arbetstagaren bör vara tidsbegränsat. Detta möjliggör att på ett naturligt sätt göra en utvärdering när projektet tar slut. Dessutom bör det under projektets gång vara regelbunden kontakt mellan arbetstagaren och arbetsgivaren. För att garantera detta är det lämpligt att i avtalet skriva att distansarbete inte får ske mer än ett visst antal dagar per vecka. Övriga dagar ska arbetstagaren vara på huvudarbetsplatsen och delta i möten och andra aktiviteter.

En förutsättning för att arbetstagaren ska kunna fullgöra sina arbetsuppgifter under distansarbetet är att den nödvändiga tekniken finns tillgänglig. Om distansarbete sker under många av veckans dagar kan det vara en fördel att det på distansarbetsplatsen finns en stationär jobbtelefon. Detta underlättar för distansarbetaren att skilja privat-samtal från arbetssamtal. Denna installation av ett speciellt telefonabonnemang för arbetet, underlättar för arbetsgivaren om denne ska betala de kommunikationskostnader som arbetstagaren har i tjänsten.

Vad det gäller informationssäkerheten när en arbetstagare arbetar på distans bör, som tidigare nämdes, säkerhetspolicy, avbrottsplan och katastrofplan skrivas. Det måste vara tydligt vem som har ansvar för informationen respektive den implementerade säkerhetstekniken. För att organisationen ska kunna ha en god sekretess och integritet kan det bli aktuellt att begränsa vilken information som får hanteras på distans. Beroende på vilken sorts information som arbetstagaren hanterar kan han eller hon få en begränsning om att vissa arbetsuppgifter inte får skötas på distans, utan får enbart hanteras på huvudarbetsplatsen.

6.2 Diskussion

Delar av den information som hanteras inom en myndighet är allmänna handlingar som var och en i samhället har rätt att ta del av. I sekretesslagen regleras vilken information som undantas från offentlighetsprincipen och som således omfattas av tystnadsplikten.

Den information som utan undantag omfattas av offentlighetsprincipen är de dokument som kommer in till myndigheten och de dokument som myndigheten skickar till annan dito eller till en enskild person. Vad det gäller den information som skapas inom myndigheten ifråga är de dokument som har slutbehandlats och arkiverats allmänna handlingar.

Om myndigheten tillåter att distansarbetaren hanterar information som omfattas av tystnadsplikten kan de ansvariga anses vara oaktsamma. Röjande av uppgifter som omfattas av tystnadsplikten är straffbart även då det har skett av oaktsamhet.

Frågan som författaren ställer är hur de lagliga kraven på offentlighetsprincipen och tystnadsplikten kan tillgodoses vid distansarbete. Ska var och en ha rätt att ta del av information som en distansarbetare tar emot eller arkiverar i persondatorn på distansarbetsplatsen? Hur ska tystnadsplikten tillgodoses om sådan information ska användas på en distansarbetsplats? Ansvariga inom myndigheten bör diskutera dessa och liknande frågor med jurister innan en arbetstagare börjar distansarbeta.

Under arbetet med detta examensarbete insåg författaren att möjligheten till distansarbete för de anställda inom försvarsmakten skiljer sig mycket åt. För några är det fullt möjligt att arbeta på distans och för andra är det helt otänkbart. Skillnaden beror helt och hållet på vilken typ av information som den anställde hanterar i sitt arbete.

Författaren diskuterade distansarbete med anställda inom olika delar av försvarsmakten. Dels anställda som till stor del hanterar öppen information och dels anställda som i huvudsak hanterar kvalificerat hemlig information. Båda grupperna var överrens om att öppen information kan vara intressant att kunna läsa på distans. Till exempel elektronisk post och kommersiella nyhets-

databaser. De var helt överrens om att hemlig information inte ska hanteras på annan plats än på huvudarbetsplatsen. Skulle konfidentiell information förvaras i hemmet ökar risken för inbrott i hemmet.

Den grupp som i huvudsak arbetar med öppen information har vid flera tillfällen känt ett behov av att kunna arbeta på distans. Arbetsuppgifterna som kan hanteras på distans är att skriva rapporter, läsa elektronisk post och komma åt det öppna datorsystemet inom försvarsmakten.

Den grupp som hanterar kvalificerat hemlig information talade om för författaren att dessa tankenbanor inte har väckts. Detta beror på att det idag inom avdelningen är strängt förbjudet att arbeta på distans. Mycket lite av den information som avdelningen hanterar får på något sätt lämna de lokaler där arbetet utförs.

6.3 Framtida arbete

Under arbetet med denna uppsats har författaren kommit i kontakt med områden som inom den närmaste framtiden kommer att förändras. Anledningen till förändringarna kan vara att olika aktörer ändrar reglerna för distansarbetare eller det är den utveckling som sker inom säkerhetsområdet.

Ett område som inom kort kommer att förändra situationen för distansarbetare är försäkringsfrågan. Försäkringsbolagen börjar reagera negativt mot att hemförsäkringen utnyttjas för den utrustning som ägs av arbetsgivaren. Istället ska arbetsgivaren teckna en egen försäkring för detta. Detta ämne har nyligen aktualiserats inom försäkringsbolagen och det är därför intressant att bevaka utvecklingen i framtiden.

Ett annat område som håller på och förändras är förmånsbeskattningen av att arbetsgivaren erbjuder hemdator till de anställda. Det har blivit fler och fler företag som vill erbjuda sina anställda möjligheten med dator i hemmet. Denna utveckling kommer att tvinga fram en förändring av förmånsbeskattningen. Vad denna förändring kommer att bli och vad den kommer att innebära för distansarbetarna är intressant att bevaka.

Enligt Jan Häggström på arbetsgivarverket kommer de under våren 1997 att publicera en folder med den policy som arbetsgivarverket förespråkar vid distansarbete. Denna folder blir intressant att ta del av.

Det sista men det mest komplexa, området som är intressant att bevaka är den utveckling som sker inom informationssäkerhetsområdet. Inom detta område sker en kontinuerlig utveckling av tekniska lösningar, krypteringsmetoder, längden på krypteringsnycklar, möjligheter att autentisera, med mera. Företag med verksamhet inom informationssäkerhet presenterar med jämna mellanrum nya metoder och produkter för att öka informationssäkerhet bland annat vid distansarbete. Det är därför av intresse att följa med i utvecklingen och sträva efter en god informationssäkerhet med hjälp av de produkter som marknaden har att erbjuda.

Referenser

Litteratur

- [Arbetsgivarverket 1996] Arbetsgivarverket, "Allmänt löne- och förmånsavtal—ALFA", cirkulär 1996:A6, 143 sidor.
- [Arbnor et al 1994] I. Arbnor och B. Bjerke, "Företagsekonomisk metodlära", Studentlitteratur, andra upplagan, 1994, 563 sidor.
- [Churchman 1968] C. W. Churchman, "The Systems Approach", Dell Publishing Co, Inc. New York, 1968, 243 sidor.
- [Elgemyr et al 1992] A. Elgemyr, L. Mattsson, "Stora säkerhets boken", Publica, första upplagan, 1992, 308 sidor.
- [FM 1995] Försvarsmakten, "Handbok för personaltjänst".
- [Ford 1994] W. Ford, "Computer Communications Security", Prentice Hall, Inc. Englewood Cliffs, New Jersey, 1994, 494 sidor.
- [Forsbäck 1995] L. Forsbäck, "20 sekunder till jobbet", TELDOK rapport nr 101, 1995, 200 sidor.
- [Freedman 1991] A. Freedman, "The Computer Glossary", Amacom, femte upplagan, 1991, 670 sidor.
- [Freese et al 1993] J. Freese, S. Holmberg "Data-säkerhet—praktisk handbok för beslutsfattare", Affärsinformation AB, tredje upplagan, 1993, 288 sidor.
- [Hamilton 1985] G. Hamilton, "Detta är Risk Management", Studentlitteratur, 1985, 170 sidor.
- [ITS 1994] Informationstekniska standardiseringen (ITS), "Terminologi för Informationssäkerhet", rapport 6, utgåva 1, mars 1994, 160 sidor.
- [Jacobsson 1996] H. Jacobsson, "Organiserade telehackare utnyttjar företagsväxlar", Computer Sweden, årgång 14, nr 47, 16 augusti, 1996.
- [Knodt 1995] H. Knodt, "Skattefria distansverktyg het politisk potatis", Distans, årgång 2, nummer 4, 1995.
- [Levy 1994] S. Levy, "Prophet of Privacy", Wired, nr 2, november, 1994.
- [Nordqvist 1996a] I. Nordqvist, "Skydd 96—ADB-säkerhetsdagarna 17 och 18 september 1996", konferensrapport/960919.IN, Försvarsmakten, 4 sidor.
- [Nordqvist 1996b] I. Nordqvist, "Networks Telecom 96 24-26 september", konferensrapport/960927.IN, Försvarsmakten, 5 sidor.
- [Nordqvist 1996c] I. Nordqvist, "NORDSEC '96—Nordic Workshop on Secure Computer Systems 7-8 november", konferensrapport/961111.IN, Försvarsmakten, 6 sidor.
- [Pfleeger 1989] C. Pfleeger, "Security in Computing", Prentice Hall, Inc. Englewood Cliffs, New Jersey, 1989, 538 sidor.
- [Rembe 1992] A. Rembe, "Juridik till vardags", Wahlström & Widstrand, 1992, 508 sidor.
- [Paavonen 1992] W. Paavonen, "Arbete på distans — förutsättningar och konsekvenser", licentiatavhandling från företagsekonomiska institutionen, Stockholms universitet, 1992, 117 sidor.
- [SIG Security 1995] SIG Security, "Säker Datakommunikation", SIG Security's årsprojekt 1995, 216 sidor.
- [SIG Security 1996] SIG Security, "Distansarbete och säkerhet", SIG Security's årsprojekt 1996, 194 sidor.
- [Schoderbek et al 1990] P. P. Schoderbek, C. G. Schoderbek och A. G. Kefalas, "Management Systems—Conceptual Considerations", BPI/IRWIM Richard D, Irwin Inc. fjärde upplagan, 1990, 458 sidor.
- [TCO 1987] TCO, "På lagom distans—för och emot distansarbete", Artikelnr 09 62447-144, 36 sidor.

[TCO 1996] TCO "Jobbet på distans—att avtala om distansarbete i hemmet", Artikelnr 10 215-001, 16 sidor.

[UD 1996] Utrikesdepartementet, "DistansArbete med Ny Teknik och Ekologi—DANTE", rapport PUG 1996:2, 72 sidor.

[Yngström 1996] L. Yngström, "A Systemic-Holistic Approach to Academic Programmes in IT Security", doktorsavhandling från data och systemvetenskapliga institutionen, Stockholms universitet, 1996, 176 sidor.

[Ågren et al 1992] Y. Ågren och B. Larsson, "Internkontroll inom arbetsmiljön", Publica, upplaga 1:1, 1992, 129 sidor.

Personer

Ulf Berglund, Major, Högkvarteret, Försvarsmakten, MUST. Tel 788 75 00.

Jan Häggström, förhandlingssekreterare Arbetsgivarverket. Tel 700 13 00.

Louise Yngström, fil.dr, DSV/KTH. Tel 16 20 00.

Bilageförteckning

Bilaga 1 Avtal AMS (5 sidor)

Avtal som arbetsmarknadsstyrelsen tecknar med de anställda som arbetar på distans.

Bilaga 2 Avtal från SIG Security's årsbok 1996 (2 sidor)

SIG Security genomför varje år ett årsprojekt. 1996 var projektet "Distansarbete och säkerhet". Resultatet av projektet presenterades i en bok med samma namn. Bilaga 2 i denna bok är ett exempel på avtal för distansarbete.

Bilaga 3 Avtal Siemens Nixdorf (7 sidor)

Avtal som Siemens Nixdorf tecknar med de anställda som arbetar på distans.

Bilaga 4 Avtal Telia (4 sidor)

Avtal som Telia tecknar med de anställda som arbetar på distans.

Bilaga 5 Avtal Utrikesdepartementet (3 sidor)

Bilaga 3 i Utrikesdepartementets utredning om distansarbete med ny teknik och ekologi (DANTE).