Handelshögskolan
VID GÖTEBORGS UNIVERSITET
Institutionen för informatik
2003-06-05

Säkerhetsimplikationer vid införande av mobila enheter

Abstrakt

Användningen av handdatorer ökar och funktionaliteten på dem har utvecklats från att vara en ersättning till den vanliga adressboken till att nu vara en förlängning av de stationära datorerna. Syftet med denna uppsats var att klarlägga vilka faktorer som bör tas i beaktning vid införandet av handdatorer i organisationen och frågan som uppsatsen avsåg att besvara var: Vilka säkerhetsimplikationer medför implementering av mobila enheter i företag? För att svara på frågan gjordes både som en litteraturstudie och som en empirisk undersökning i form av en enkätundersökning. Litteraturstudien ledde fram till en hotbild som sedan lyftes in i ett ramverk skapat av centrala begrepp inom informationssäkerhet. Detta tillsammans med resultaten från den empiriska undersökningen visade att införandet av mobila enheter medför tre övergripande implikationer. Risken för att obehöriga kan ta del av affärshemligheter ökar, risken för säkerhetshål i företagets nätverk ökar och risken för att problem med kompabilitet mellan olika användare ökar.

Nyckelord: informationssäkerhet, handdator, mobil enhet, hot, policy

Författare: Stefan Edevåg
Handledare: Andreas Nilsson
Examensarbete II, 10 poäng

Security implications when introducing mobile devices

Abstract

Handheld computers are becoming more popular and the functionality has increased from just replacing the regular address book to being a lengthening of regular computers. The purpose of this paper was to examine what issues and factors should be taken into consideration when a company is planning to implement handheld computers into their organization. The main question of this paper was: What security consequences do an implementation of handheld computers in companies result in? In order to answer the question, both a literature study as well as an empirical study in the form of an inquiry was conducted. The literature study resulted in a list of threats that later was lifted into a framework, shaped by central concepts of information security. This together with the results from the empirical study showed that an implementation of handheld computers in a company results in three overriding consequences. The risk that unauthorized persons could take part of company secrets increases, the risk for security holes in the company's network increases and the risk for problems regarding compatibility towards different users increases.

Förord

Ett stort tack till min handledare Andreas Nilsson för alla goda råd och tips som jag har fått ta del av. Ett stort tack går även till de företag som ställt upp i min undersökning.

Göteborg, maj 2003

Stefan Edevåg

1 Inledning

1.1 Bakgrund

Sverige och många andra industrisamhällen har idag övergått från att vara varuproducerande samhällen till att vara service- och kunskapsproducerande samhällen. I och med övergången ökar behovet av nya modeller för att hantera och skydda information i olika former, detta eftersom skapande och utnyttjande av kunskap och tjänster blir lika väsentligt för samhället som traditionella råvaror. Behovet av kunskap skapar i sin tur ett beroende till informationssystem som kan hantera ett stort informationsutbud. (Höglund & Persson, 1985)

Det tjänsteproducerande samhället har vuxit fram under flera år och det för inte bara med sig ett ökat behov av informationssystem. Förändringen till en ny samhällsform skapar även andra fenomen. Ett varuproducerande samhälle är uppbyggt av industrier och stationära arbetsplatser i form av fabriker och kontor. Till en början har vi sett hur olika former av informationstekniker har inordnats i dessa arbetsplatser i form av telefoner och datorer som är kopplade till Internet eller intranät och så vidare. Det gemensamma för dessa tekniker är att de är bundna till en specifik plats, men i takt med att kunskapssamhället växer fram minskar antalet traditionella fabriker och kontor (Dahlbom, 1998). I takt med att antalet stationära arbetsplatser minskar ökar istället olika anställningsformer där de anställda i stor utsträckning är rörliga. Ett yrke som traditionellt sett varit knutet till rörlighet är försäljare i olika former. I dag ställs krav på att de flesta i en organisation skall vara rörliga. Det kan vara chefer som skall närvara på möten, säljare som besöker kunder eller servicetekniker som är på uppdrag. Detta skapar ett behov av mobila informationssystem.

Under 1990-talet har vi sett en makalös utveckling inom försäljningen av mobiltelefoner och nu börjar andra typer av mobila enheter leta sig in i organisationerna och detta kräver en ny typ av säkerhetstänkande. Handdatorer är portabla samtidigt som de är tillräckligt kraftfulla för att lagra känslig företagsinformation på, så som kontaktinformation eller lösenord. Användningen av handdatorer ökar och funktionaliteten på dem har utvecklats från att vara en ersättning till den vanliga adressboken till att nu vara en förlängning av de stationära datorerna. Därför ökar även risken för att känslig information hamnar i orätta händer, då handdatorernas storlek gör att de lätt tappas bort (McMillan, 2002). För att exemplifiera kan nämnas att passagerare i Londons taxibilar tappade bort runt 62,000 mobiltelefoner, 2,900 bärbara datorer och 1,300 PDA (Personal Digital Assistant) under en period på sex månader (Harrison, 2001).

Tidigare har säkerheten gått ut på att skydda de fysiska tillgångarna i företaget. Detta görs ofta genom till exempel staket, larm och övervakningskameror. Skyddet av de fysiska tillgångarna kan vara välmotiverat men i och med övergången till ett tjänstesamhälle kan detta dock vara av underordnad betydelse då företagets information och kunskap ofta är den mest värdefulla tillgången i dagens företag. (Svensson, 1999) För att skydda sina tillgångar måste företagen se till att vara uppdaterade inom säkerhetsområdet och ständigt anpassa sin verksamhet och sitt skydd efter nya hot som uppkommer.

Gollman (2000) framhåller att säkerhet handlar om att skydda tillgångar och för företag ligger fokus ofta på förebyggande åtgärder. Företagssäkerhet har tagit sig olika skepnader genom historien, men syftet har alltid varit att skydda verksamheten mot olyckor, skador och olika typer av kriminell verksamhet. Nu för tiden har datorsäkerhet fått allt större uppmärksamhet och det beror till stor del på framväxten av det globala nätverket Internet (Borg, Lozano, Löfgren, Malmgren och Palicki, 1997).

1.2 Problemformulering

Problemet som denna uppsats behandlar är:

Vilka säkerhetsimplikationer medför implementering av mobila enheter i företag?

1.3 Syfte

Syftet med denna uppsats är att klarlägga vilka faktorer som bör tas i beaktning vid införandet av handdatorer i organisationen. Med utgångspunkt ur problemformuleringen belyser uppsatsen de konsekvenser inom säkerhetsområdet som följer av införandet av handdatorer i företag. Resultatet presenteras på så sätt att en större mängd företag skall kunna använda det i sitt säkerhetsarbete.

1.4 Avgränsningar

Då uppsatsen behandlar ett brett ämne har det varit nödvändigt att avgränsa det område som behandlas. De aktuella avgränsningarna som vidtagits är följande:

- Undersökningen inriktar sig på säkerhetsimplikationer vid införande av handdatorer i organisationer och studien behandlar därför inte någon form av privat användande.
- Tekniska detaljer berörs ej ingående, utan enbart i den utsträckning som behövs för att tydliggöra och belysa vissa företeelser.
- Ekonomiska konsekvenser berörs inte i någon större omfattning.
- Teorier om mobilitet och organisationsstrukturer i moderna organisationer behandlas inte.

1.5 Disposition och terminologi

Uppsatsen är upplagd på så sätt att bakgrunden och uppsatsens frågeställning och syfte samt eventuella avgränsningar presenteras i uppsatsens inledning. I avsnittet som följer efter inledningen presenteras uppsatsens metodval, vetenskapliga synsätt och tillvägagångssätt vid den empiriska undersökningen. Fortsättningsvis kommer ett teoriavsnitt med en presentation av tidigare forskning som finns att läsa inom området informationssäkerhet samt de hot som företag ställs inför i dagens samhälle. Detta följs av en redogörelse för resultatet av teori samt resultatet av den empiriska undersökningen. Avslutningsvis kommer ett kapitel med en diskussion kring informationen som presenterats i uppsatsen samt en slutsats som belyser de säkerhetsimplikationer som uppstår i och med införandet av mobila enheter i verksamheten.

I somliga fall förekommer det engelska facktermer i uppsatsen som saknar bra synonymer på svenska. Jag har i dessa fall valt att använda mig av de engelska termerna och hoppas att på så sätt minska risken för missförstånd. I de fall som det finns bra svenska termer har jag använt dessa, såsom e-post istället för det engelska e-mail.

Här följer en lista över de vanligaste förekommande facktermerna:

Cracker
En cracker är en person som försöker forcera ett systems säkerhetsspärrar i syfte att sabotera programvara eller att komma åt, utnyttja eller eventuellt förändra skyddad information

Datavirus
Ett datavirus är en programvara som infekterar andra programvaror genom att förändra dem på olika sätt och samtidigt inkludera en kopia av sig själv. Avsikten med datavirus är oftast att spridas okontrollerat och helst utan att användaren märker något.

DOS (Denial of service)
En DOS-attack riktas mot ett nätverk i avsikt att överbelasta det genom att fylla det med värdelös trafik.

Handdator
En handdator är en bärbar dator som är så pass liten att den kan hållas i handen vid användning.

PDA (personal digital assistant)
Se handdator.

Shoulder surfing
Shoulder surfing innebär att titta över axeln på någon för att snappa upp information.

Social engineering
Social engineering är ett allmänt begrepp för säkerhetsattacker med hjälp av sociala kontakter och mänskliga relationer.

Trojan
Med trojan menas ett program som till synes utför oskyldiga uppgifter, men innehåller även kod som gör att det blir möjligt att ta kontroll över den drabbade datorn.

2 Metod

2.1 Metodval

Inför ett metodval finns det vissa saker som bör tas i beaktning. Det finns ingen generell metod som går att applicera på alla problem, det gäller att känna till de olika metodernas möjligheter och begränsningar och utifrån detta kan man välja ut en lämplig metod. Utgångspunkten i valet av undersökningsmetod bör vara den frågeställning som man har för avsikt att undersöka. (Holme och Solvang, 1997)

Man skiljer mellan två olika metodiska angreppssätt, kvalitativa och kvantitativa metoder. Kvalitativa metoder innebär en ringa grad av formalisering samt en närhet till den källa som vi hämtade vår information från. Vid användningen av denna metodinriktning bör målet inte vara att pröva om informationen har en generell giltighet. Det centrala är istället att skapa sig en djupare förståelse för det aktuella problemet. Detta gör man framförallt genom att använda sig av olika sätt för informationsinsamling. Kvantitativa metoder är mer formaliserade och strukturerade samt kännetecknas av selektivitet och avstånd till informationskällan. Det är en nödvändighet för att man ska kunna göra jämförelser och pröva om resultaten man kommit fram till gäller alla enheter som man vill uttala sig om. (Holme och Solvang, 1997)

Kombinationen av två olika metodredskap förhindrar att den genomförda undersökningen blir metodbunden (Easterby-Smith, 2002). De olika metodredskapen har starka och svaga sidor som kompletterar varandra. Detta innebär att det kan finnas mycket att vinna på att kombinera kvantitativa och kvalitativa metoder. När man skall använda sig av en kombination av de två olika tillvägagångssätten så gäller det att veta vilka möjligheter och begränsningar som ligger i respektive angreppssätt. (Holme och Solvang, 1997)

För att komma fram till svaret på uppsatsens frågeställning användes en kombination av en kvantitativ enkätundersökning och en kvalitativ analysmetod. Genom att använda sig av en kvantitativ enkätundersökning så kan man nå en större mängd undersöknings-objekt. Detta är viktigt för undersökningen eftersom dess syfte är att styrka de uppgifter som kommit fram i uppsatsens teoriavsnitt. Undersökningen avser alltså påvisa att situationen som målas upp i teoriavsnittet existerar hos många företag som använder sig av handdatorer i verksamheten. Att styrka teorin anses nödvändigt då det är svårt att hitta information inom det undersökta området. Vid denna typ av undersökningsmetod bör man dock ta i beaktning att man endast får tillgång till den information som den undersökta personen själv väljer att förmedla. Det är även viktigt att man försäkrar sig om att man pratar med personer som besitter bra kunskap inom undersökningsområdet. Magnus Bergqvist (31 oktober, 2002) poängterade i sin föreläsning om etnografi som systemutvecklingsmetod att det inte är säkert att man kan lita på det som sägs vid enkätundersökningar och intervjuer. Den uppfattning som den undersökte personen har av undersökningsområdet kanske inte alltid stämmer överens med det som verkligen sker. En kvantitativ enkätundersökning är ändå att föredra eftersom undersökningen riktar sig till en ganska bred målgrupp och det från början är klarlagt vad det är för kunskap vi vill ha ut av undersökningen. I detta fall är det alltså inte så aktuellt med en

kvalitativ undersökning eftersom det skulle vara väldigt svårt att nå ut till och få ett större antal respondenter att ställa upp på en sådan undersökning.

Det är även av stor vikt att man har bra validitet i sin undersökning. Göran Wallén (1996) poängterar vikten av validitet i en undersökning och definierar det som att ”mätinstrumentet inte ska ge några systematiska fel.”. Det är därför viktigt att svaren i undersökningen verkligen motsvarar det som man avser att undersöka. Det är alltså viktigt att tänka på validiteten när man genomför en enkätundersökning eftersom man i denna undersökning riskerar att få en lägre validitet än vid exempelvis en deltagande observation där den som genomför undersökningen själv kan gå in och ”hämta” resultatet på det man avser att undersöka.

För att uppnå bra validitet i undersökningen så har validiteten ständigt funnits i åtanke vid konstruktionen av frågorna i enkäten. Genom att ständigt återgå till frågeställningen och syftet med undersökningen försäkrar man sig om att frågornas svar ger värdefull information. I utvecklingen av enkäten användes testpersoner för att få andras syn på om frågorna i enkäten var relevanta för undersökningens syfte. För att ytterligare stärka validiteten i undersökningen fick ett antal personer testa frågorna. På så sätt minskade risken för att frågorna skulle misstolkas och möjligtvis göra resultatet värdelöst. En stor fördel vid utformningen av enkäten är att använda så kallat iterativt arbetssätt. Genom detta arbetssätt kan utformningen av enkäten samt korrigering av upplägget och frågorna ske tills man nått ett tillfredställande resultat.

Det är även viktigt att undersökningen har en hög reliabilitet vilket innebär att andra ska kunna utföra undersökningen ytterligare gånger på samma sätt med hjälp av min dokumentation. Genom den dokumentation som förts och som leder läsaren genom arbetet med undersökningen är det relativt lätt att genomföra denna undersökning en gång till under samma premisser vilket ger undersökningen en bra reliabilitet.

2.1.1 Vetenskapligt synsätt

Vetenskapsteori behandlar hur vetenskaplig kunskap bildas och hur man går tillväga för att sätta den på prov (Wallén, 1996). Vetenskapsteorin behandlar även kunskapens roll i samhället. I denna studie används två olika vetenskapliga synsätt, positivism och hermeneutik.

Inom det positivistiska synsättet anser man att en vetenskaplig ansats endast är av värde om den kan verifieras empiriskt. Inom detta synsätt anser de alltså att det som inte är empiriskt prövbart, som till exempel känslor och värderingar inte kan räknas till vetenskaplig kunskap. Några typiska kännetecken för det positivistiska synsättet är:

- Tilltro till vetenskaplig rationalitet.
- Kunskap ska kunna testas empiriskt. Uppskattningar och bedömningar ska ersättas med mätningar.
- Det finns krav på att metoder ska resultera i tillförlitlig kunskap. För att uppnå detta har man mätkrav som validitet och reliabilitet.
- Förklaringar ska göras med termerna orsak - verkan.
- Forskaren måste förhålla sig objektiv till sitt forskningsarbete. (Wallén, 1996)

Hermeneutik kan översättas som tolkningslära och har bland annat ursprung i texttolkning. Den hermeneutiska inriktningen kan enligt Wallén (1996) ses som ett komplement till det positivistiska synsättet. Hermeneutik handlar framförallt om:

- Hermeneutik handlar om tolkning av innebörden i bland annat texter, handlingar och upplevelser.
- Tolkaren har en förförståelse i form av språklig och kulturell gemenskap.
- Tolkandet går till på så sätt att man växlar mellan ett del- och helhetsperspektiv. På så sätt växer tolkningen fram genom en växling mellan den aktuella delen man jobbar med och helheten som gradvis växer fram.
- Det är viktigt att man vid tolkandet tar hänsyn till den situation det tolkade materialet har uppkommit i samt vilken situation läsaren befinner sig i.
- Tolkning innebär ofta att man visar innebörder eller sammanhang som ”ligger bakom” det som vid första anblicken kanske verkar vara något helt annat. (Wallén, 1996)

I studien användes ett positivistiskt synsätt då sammanställningen av undersökningen skedde genom omvandling av undersökningssvaren till statistisk data. Vid den kvalitativa analysen användes både ett positivistiskt och ett hermeneutiskt synsätt eftersom det genomfördes en tolkning av undersökningens statistiska data, samt en presentation av dessa data med hjälp av grafer. Den slutliga analysen genomfördes utifrån det framtolkade undersökningsresultatet kombinerat med det som framkommit i teoriavsnittet. I denna analys användes endast en kvalitativ analysansats och ett hermeneutiskt synsätt.

2.2 Litteraturstudie

Undersökningarna förbereddes med en genomgång av befintlig litteratur inom det tilltänka undersökningsområdet. Litteraturgenomgången är en viktig del av forskningen och Urban Nuldén (21 november, 2002) förklarade dess syfte i en föreläsning som handlade om mobil-informatik metoden. Följande punkter förklarar enligt Urban Nuldén syftet med en litteraturgenomgång:

- Kunna skilja på vad som är gjort och vad som behöver göras.
- Identifiera centrala variabler.
- Syntetisera och se nya perspektiv.
- Få en begreppsapparat.
- Förstå strukturen på området.
- Identifiera hur andra forskat på området.
- Vilken forskning är state-of-the-art.

Syftet med litteraturstudien var att hitta luckor som idag inte behandlas i befintliga arbeten samt förslag från författare om områden för fortsatt forskning.

2.3 Enkät

Arbetet med enkäten inleddes genom att, med utgångspunkt i uppsatsens syfte, arbeta ihop ett antal frågor. Arbetet inleddes med att skriva ned olika funderingar som uppkom, för att sedan välja ut de som bidrog med värdefull information till arbetet. Detta var ett viktigt arbete, eftersom uppsatsen bygger på informationen som kommer av dessa frågor. Vid utformning av en enkät kan det vara lämpligt att försöka minimera antalet öppna frågor, då dessa kan upplevas som jobbiga att besvara.

2.3.1 Urvalsmetod

Inför en undersökning är det oftast inte möjligt att undersöka hela populationen utan uppgifterna får hämtas från en urvalsgrupp. Detta gör man med förhoppning att gruppen ska vara representativ för hela populationen. Detta är dock inte något man kan förutsätta. Det finns framförallt två olika sorters urvalstekniker, sannolikhetsurval och icke-sannolikhetsurval. (Denscombe, 2000)

De grundläggande kraven för sannolikhetsurval är att sannolikheten för att en enhet i populationen ska komma med i urvalet ska vara känd. Sannolikheten behöver inte vara lika stor för alla enheter att innefattas i urvalet men den ska som sagt vara känd. I icke-sannolikhetsurval utgör de människor eller företeelser som ingår i undersökningen definitivt inte resultatet av ett slumpmässigt urval. De olika enheterna i populationen har därmed inte lika stor chans att tas med i urvalet. (Denscombe, 2000)

Det finns situationer när det är svårt eller inte önskvärt med ett sannolikhetsurval. I dessa situationer finns ett antal olika sorters icke-sannolikhetsurval och det som använts inför denna undersökning är ett subjektivt urval. Ett subjektivt urval går ut på att urvalet handplockas för det aktuella ändamålet. Urvalsmetoden används då forskaren redan besitter en viss kunskap om de människor eller företeelser som ska undersökas, forskaren väljer därför medvetet ut vissa undersökningsobjekt eftersom det anses troligt att dessa ger värdefull information till studien. Den fråga som forskaren bör ställa sig när han befinner sig i denna situation är vem eller vilka som sannolikt kommer att ge meningsfull informationen med tanke på det jag redan vet om undersökningstemat och den företeelse jag studerar. Fördelen med ett subjektivt urval är att forskaren kan närma sig de företeelser som han har god grund för att anta vara avgörande för undersökningen. På detta sätt belyses undersökningsfrågan och resultatet av undersökningen blir inte bara mer ekonomisk utan även mer informativ än konventionella sannolikhetsurval. I denna studie har ett subjektivt urval används för att undersökningen skall kunna utföras på respondenter som anses ha ett högt informationsvärde. Det subjektiva urvalet resulterade till att undersökningen utförs på 32 företag som befinner sig inom IT- och telekombranschen, då de i sina respektive verksamhetsområden ofta använder sig av ny teknik. (Denscombe, 2000)

2.4 Genomförande

Genom att studera tidigare litteratur och forskning har luckor som idag inte har behandlas i befintliga arbeten hittats samt förslag från författare på områden för fortsatt forskning. Dessa två delar har bidragit till utformningen av syftet och frågeställningen i uppsatsen. Litteraturstudien har även gett kunskap om vilka begrepp som finns inom området och vad de har för innebörd, vilket är kritiskt för att kunna dra korrekta slutsatser. Litteraturstudien har inneburit att de begrepp som förekommer har strukturerats upp vilket lett till en övergripande och strukturerad helhetssyn av området. Material som kommer fram under litteraturstudien utgör stommen i uppsatsens teoriavsnitt. I teoriavsnittet presenteras en teoretisk genomgång och presentation av hot vid informationssäkerhet. Dessa hot presenteras i ett teoretiskt ramverk där de kategoriseras som antingen administrativ säkerhet eller IT-säkerhet.

I arbetet runt uppsatsen utfördes även en webbaserad enkätundersökning avseende användningen av PDA samt de säkerhetsimplikationer som vidtas av de aktuella företagen. Med tanke på syftet med undersökningen så fanns ingen mening med att inleda enkäten med några demografiska frågor, som i andra fall kan vara att rekommendera för att få lite mer exakta uppgifter om respondenten. Enkäten bestod i

sin helhet av 10 frågor varav 4 stycken delvis var så kallade öppna frågor där respondenten fritt kunde skriva in ett svar på frågan. Två av de tio frågorna var beroende av vad respondenten svarade på den föregående frågan. Vid utformning av enkäter är det att föredra att man placerar ett antal enkla tvåvalsfrågor i slutet av enkäten för att förhindra att respondenterna avbryter medverkan i undersökningen på grund av att de inte orkar sätta sig in i de sista frågorna. Detta gäller framförallt undersökningar som innehåller lite fler frågor än i det aktuella fallet. Med tanke på att det bara fanns tio frågor i enkäten samt att dessa frågor inte var speciellt värdeladdade så borde det faktum att det inte finns enkla frågor i slutet vara av underordnad betydelse för om respondenterna slutförde sin medverkan i undersökningen. Det som kan ses som en bidragande orsak till att respondenterna inte ville besvara enkäten var att det kunde kännas osäkert att lämna ut information angående företagets säkerhetsåtgärder. Denna påverkansfaktor har dock minimerats genom att informationstexten som fanns i samband med enkäten upplyste alla inblandade om att de var helt anonyma vid medverkan i undersökningen och att ingen på något sätt kan koppla svaret till dem eller deras företag.

I undersökningen användes en webbaserad enkät, eftersom det gjorde att det var mycket lättare och gick snabbare att nå ut till respondenterna. Genom användning av ett webbaserat formulär så kan man snabbt nå ut till människor och ingen behöver ta sig an hanteringen av allt papper som uppstår om alla respondenter ska ha en varsin papperskopia. Vid pappersenkät är man även beroende av att någon delar ut enkäten till de berörda parterna samt att det är svårare att motivera företag att delta eftersom någon måste ta på sig ansvaret för att samla in alla enkätsvar.

Efter att utformningen av enkäten var avslutad och respondenterna var utvalda så skickades enkäten till respondenterna via en länk i ett e-post. Respondenterna kunde sedan fylla i undersökningsformuläret och sedan trycka på ”skicka” så skickades en förteckning över respondentens svar via e-post. I e-postmeddelandet uttryckte jag en önskan om att enkäten skulle besvaras av behörig personal.

Sammanfattningsvis behandlas den teoretiska genomgången, det teoretiska ramverket för kategorisering av hot mot informationssäkerheten samt resultatet av den empiriska undersökningen i uppsatsens diskussion och slutsats. Detta resulterar i ett antal riktlinjer för vilka säkerhetsåtgärder som bör vidtas vid införandet av handdatorer i verksamheten.

2.4.1 Analys

Analysen av undersökningsresultatet består av en kvantitativ och en kvalitativ del. Med hjälp av den kvantitativa delen togs det faktiska resultatet av undersökningen fram, det vill säga fördelningen av svaren på enkätundersökningen som sedan presenteras med hjälp av diagram. För att få en övergripande helhetsbild av resultatet användes sedan en kvalitativ analysmetod i form av en helhetsanalys som syftar till att se till helheten i den insamlade informationen. (Holme och Solvang, 1997)

Genom att först genomföra en enkätundersökning så får man fram svar på mer ytliga och grundläggande frågor när det gäller till exempel säkerhet och policys på företaget. För att analysera undersökningsresultatet ytterligare används helhetsanalys där man kan sätta ihop ett antal djupare frågor som uppkommit efter att ha tittat på resultatet av enkätundersökningen. Dessa frågor kan man sedan få svar på genom att genomföra fas tre i helhetsanalysen med en systematisk granskning av enkätsvaren. (Holme och Solvang, 1997)

2.4.2 Metodgranskning

Det finns ett antal svagheter som medföljer de val som gjorts gällande den vetenskapliga ansatsen och ramverket för undersökningen i uppsatsen.

Svagheten med undersökningen är urvalet som tagits ut genom ett subjektivt urval. I detta fall är det inte aktuellt att generalisera resultatet från undersökningen över branschen som undersöks, utan syftet med undersökningen är att ge information för hur företag handskas med säkerheten vid användning av handdatorer i verksamheten. Denna information sätts även i relation till informationen i teoriavsnittet.

Undersökning ger en bild av hur företagen handlar vid införandet av handdatorer i verksamheten och vilka bestämmelser som finns. Däremot går inte undersökningen djupare in på vad deras handlingar beror på vilket istället får ligga som en naturlig fortsättning på uppsatsen.

Valideringsmoment i webbenkäten innebar att det kom upp en varning om någon glömt eller hoppat över att svara på någon fråga och det gick då inte att skicka formuläret. Ett ofullständigt svar är mindre värdefullt och därför var det bättre att de inte svarar på undersökningen alls än att de endast fyller i ett fåtal frågor.

3 Teori

> *If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.*
>
> (Bruce Schneier, 2000)

IT-säkerhet är ett mycket vitt begrepp, men i grund och botten handlar det om att skydda information. Det finns idag ingen självklar skillnad mellan IT-säkerhet och informationssäkerhet, eftersom IT numera utgör en integrerad del av verksamheten hos företag och informationen överförs allt oftare i elektronisk form (Statskontoret, 1998). Att skydda information är ett stort arbete och görs genom att skydda alla de processer som hanterar information i ett företag, vilket kan vara allt från telefonsystem och faxmaskiner till datorer och informationssystem. Precis som Bruce Schneier (citat ovan) säger finns det inte någon enkel och generell lösning för att skydda sina tillgångar. Ett skydd måste byggas upp av en kombination av både tekniska och organisatoriska lösningar, vilket medför att arbetet kräver en bred kunskap. De fysiska och tekniska lösningarna tar sig ofta uttryck som säkra rum, videoövervakning, larm och antivirus, brandväggar och kryptering som några exempel. Organisatorisk säkerhet är dock minst lika viktig eftersom detta innefattar all mänsklig interaktion med informationskanalerna och rymmer de krav som ställs på personal och användare. Kraven kan t.ex. vara implementerade som en policy för användande av IT inom företaget.

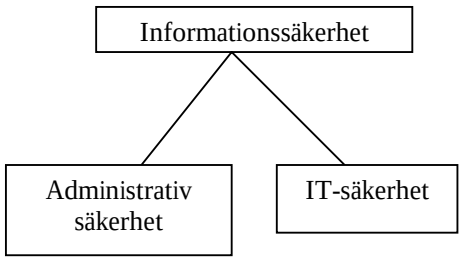
I teoriavsnittet ämnar jag behandla följande aspekter av informationssäkerhet:

1. Administrativ säkerhet
2. IT-säkerhet
3. Hot

Av dessa aspekter används de två översta för att skapa ett ramverk. Identifierad hotbild lyfts sedan in i detta ramverk, för att senare utvärderas.

3.1 Informationssäkerhet

Historiskt sett har säkerhet ofta varit tätt knutet till att hålla information hemligt och även idag anser många att informationssäkerhet går ut på att hindra obehöriga från att läsa känslig information (Gollman, 2000). Att enbart hindra obehöriga att läsa information räcker dock inte för att definiera informationssäkerhet, eftersom företag även är beroende av att deras information är riktig och tillgänglig.



Figur 3.1 Informationssäkerhetens två beståndsdelar.

3.1.1 Administrativ säkerhet

Informationssäkerhet kan delas in i administrativ säkerhet och IT-säkerhet (se figur 3.1). För att kunna uppnå bra informationssäkerhet krävs det alltså ett bra samarbete mellan företagets organisation och teknik. Administrativ säkerhet innebär i första hand att regler och rutiner för styrning och kontroll av IT-tillgångar definieras.
De administrativa reglerna och rutinerna kan t.ex. specificeras i företagets policy. Denna typ av säkerhet kan både fungera som ett komplement till en teknisk skyddsåtgärd, men även fungera som en skyddsåtgärd i sig. (Statskontoret, 1997a)

3.1.2 IT-säkerhet

IT-säkerheten uppnås genom att man hindrar obehöriga att komma åt företagets data och system och på så sätt förhindra att de läser, förändrar eller stör databehandlingen inom företaget (Nordqvist, 1997). All typ av säkerhet går i grunden ut på att det finns en tillgång som man vill försvara och i dagsläget är ofta information den viktigaste och mest värdefulla tillgången för ett företag.

Idag har de flesta företag viktig information som varken får försvinna eller bli felaktig. Listan över denna typ av information kan göras lång och innehåller bl.a. order, produktregister och kundregister. Givetvis varierar det från företag till företag vad som är viktig information, men varje företag eller verksamhet har sina viktiga uppgifter. Information och data som samlats in under flera år kan vara svårersättligt och mycket svårt att återskapa. Även om uppgifterna går att återskapa tar det tid och kostnaderna för att ersätta viktiga uppgifter kan därför bli mycket höga. (Beckman, 1993)

Det är därför av stor vikt att bara de användare som är behöriga får tillgång till informationen.

3.1.3 Informationssäkerhet på företag

Oavsett om handdatorn stjäls eller tappas bort så kan det få ödesdigra konsekvenser för företaget i fråga. Givetvis är det inte värdet på själva enheten som medför att företaget kan förlora stora summor, utan värdet ligger i informationen som är lagrad på den. Både en undersökningen utförd av tidsskriften Computer Sweden (Nordner, 2002) och en undersökning utförd av Pointsec Mobile Technologies, Infosecurity Europe och Computer Weekly (Protect Data, 2002) visar att användare sparar information som kontaktuppgifter, e-postmeddelanden och kalender på sina handdatorer. Denna information kan vara väldigt intressant för eventuella konkurrenter, då de till exempel kan få information om offerter vid budgivning för att få olika uppdrag. Rudy Bakalov, säkerhetschef på PricewaterhouseCooper säger till industryweek.com att många säkerhetsansvariga ser PDA som ett oönskad barn, det vill säga något som de helst skulle vilja vara utan (industryweek.com, 2002-12-30). Rudy Bakalov säger vidare att det är få organisationer som har implementerat några direkta direktiv för hur handdatorer skall och får användas. En undersökning utförd av tidningen Computer Sweden (Nordner, 2002) visar även den att företag sällan har en säkerhetspolicy för handdatorer, då endast 26 % av de svarande säger att det finns säkerhetsregler för handdatorer på deras arbeten.

3.1.4 Hot

The average computer user is going to pick dancing pigs over security any day.
(Bruce Schneier, 1999)

All säkerhet bygger i grund och botten på att det finns något utav värde, en tillgång, att skydda. Då man talar om informationssäkerhet betyder det att denna tillgång skall kunna knytas till någon form av informationshantering. Dessa tillgångar eller resurser kan vara såväl informationen i sig eller den teknik som används för att lagra eller behandla den, såsom databaser eller servrar. Information som tillgång handlar det inte bara om sådan information som finns lagrad i organisationens informationssystem, utan även icke-formaliserad information som kanske inte ens finns dokumenterad. Alla dessa olika former av tillgångar kan utsättas av ett flertal olika hot. (Oscarson, 2001)

Oscarson (2001) definierar hot som oönskade handlingar eller händelser, som utförs eller orsakas av människor, av människan skapade artefakter eller naturliga fenomen och som antas kunna riktas mot aktuell tillgång.

När ett hot förverkligas inträffar en händelse som påverkar organisationen negativt. En säkerhetsincident är en ogynnsam händelse där någon form av informationssäkerheten hotas. Det kan vara någon form av intrång som äventyrar informationens konfidentiellitet, ett datavirus som påverkar integriteten eller en denial of service-attack som hindrar anställda eller andra behöriga från att ta del av företagets information. Exakt vad som definieras som en incident kan variera för varje företag eller organisation beroende på många olika faktorer. (Kossakowski, 2003)

De hot som riktas mot verksamheten kan delas upp i två grupper, de som kommer utifrån och de som kommer inifrån organisationen. Externa hot är mestadels avsiktliga hot, d.v.s. någon har för avsikt att sabotera informationssystemet eller komma över viss information (Statskontoret, 1997c). Några exempel på externa hot som föreligger är:

- Virus – Många av de virus som kan infektera informationssystem skadar informationen på något sätt och hotar på sätt integriteten hos informationen.
- Intrång (crackers, trojaner, social engineering) – De flesta former av intrång syftar till att komma över information och hotar därför företagets konfidentiellitet.
- Denial of service – Denna typ av angrepp används för att sabotera tillgängligheten till information.

Ett vanligt skydd mot externa hot är brandväggar, men ett frekvent hål i säkerhetssystemet där crackers kan kringgå brandväggarna är uppringda förbindelser till maskiner på det interna nätverket. En brandvägg skyddar endast systemet till en viss nivå och då endast mot externa hot. (Gollman, 2000)

Trots alla de externa hot som finns mot en organisations informationssystem är detta inte de vanligaste avsiktliga hoten. Tvärtom finns de flesta hoten inom den egna organisationen. En BRÅ-undersökning visar att anställda och konsulter är ansvariga för mer än hälften av den IT-relaterade brottsligheten som drabbar företag och myndigheter (Korsell, 2000). De interna hot som leder fram till denna brottslighet är väldigt svåra att värja sig mot, eftersom hoten redan finns inne i organisationen. Det försvar som företag har byggt upp för att skydda sig mot externa hot är verkningslöst, då de interna hoten vanligen består av en person med tillgång till datorsystemen.

Efter litteraturstudien har följande övergripande hot identifierats. De berör vad en organisation bör beakta vid införande av mobila enheter.

1. Obehörig åtkomst på grund av att funktioner för identifiering och autenticering saknas.

2. Obehörig åtkomst på grund av att funktioner för identifiering och autenticering har stora brister. Stora brister kan innebära att det är möjligt att gissa sig till dem eller att angriparen läser nedskrivna lösenord vid handdatorn. Detta medför att en obehörig användare kan läsa, ändra eller radera information i dokument.

3. Obehöriga användare kan avlyssna trådlös datakommunikationen mellan två parter. Obehörig insyn kan också uppstå när en annan användare än avsedd mottagare avsiktligt eller oavsiktligt får tillgång till ett meddelande eller andra informationsmängder.

4. Bristfällig dokumentation av såväl maskinella som manuella rutiner. Avsaknad av dokumentation kan lätt leda till missförstånd, vilket i sin tur kan leda till att produkten används på ett felaktigt sätt.

5. Datamedium (exempelvis CompactFlash minnen) med svårersättlig eller konfidentiell data försvinner (stjäls eller förläggs) utanför företagets område. Faran är inte enbart att oersättlig data försvinner (ifall informationen inte har säkerhetskopierats), den kan även läsas av obehöriga.

6. Virus kan komma in i handdatorn och nätet via överförda filer som bifogats e-post eller tagits hem via Internet. Virus kan förstöra delar eller all information på handdatorn eller i nätet. Virus kan även sprida hemlig information till obehöriga.

7. Trojanska hästar kan även de hota informationen i företaget på liknande sätt. Skillnaden är att det ofta är en aktiv angripare som ligger bakom trojanska hästar, medan virus sprider sig mer slumpmässigt.

8. Obehörig åtkomst kan ske genom att någon tar över en inloggningsperiod från en användare som lämnar handdatorn obevakad.

9. Handdatorn kan vara felaktigt konfigurerad vilket medför att den inte fungerar alls eller att den fungerar felaktigt. Detta kan t.ex. gälla inloggningsrutiner, antivirusprogram, brandväggar etc.

10. Inkonsekvenser och konflikter mellan applikationer kan förorsaka problem, då olika applikationer exempelvis kan behandla data på olika sätt. Om alla arbetsplatser är konfigurerade på olika sätt är det svårt för personer att dela information och arbeta tillsammans. Inkonsekvent konfigurering är också en källa till många tekniska problem, t.ex. förlust av tillgänglighet på grund av systemkonflikter.

11. Det är också möjligt att kringgå det logiska skyddet genom direkt, fysisk åtkomst av hårdvaran. På detta sätt kan en angripare komma åt data från en riktigt konfigurerad enhet, t.ex. genom att manipulera hårdvaran.

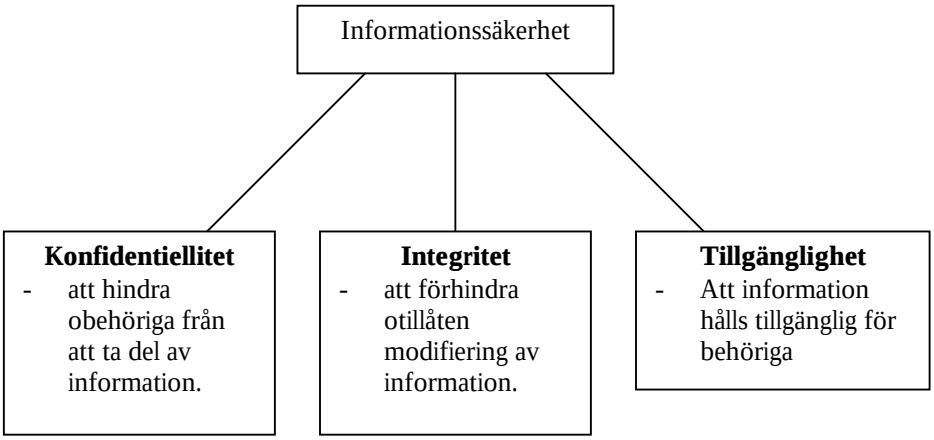
12. Det saknas rutiner för återställande av en havererad arbetsplats. Det räcker alltså inte med att ta backup, informationen skall även kunna återställas på ett tillfredsställande sätt.

13. Missnöjda anställda kan föra ut känslig data och information ur företaget, då en handdator har ett förhållandevis stort lagringsutrymme, samtidigt som den är tillräckligt liten att stoppa i t.ex. en ficka.

14. Dålig utbildning kan medföra att de anställda inte vet hur de skall och får använda program och/eller hårdvara. Detta medför att de av misstag kan öppna säkerhetsluckor och på andra sätt kompromissa säkerheten för företaget.

3.1.5 Mening med informationssäkerhet

Oscarson (2001) menar att det man vill uppnå med informationssäkerhet kan delas upp i tre olika delar (se figur 3.4).



Figur 3.4 Dessa tre delområden utgör tillsammans meningen med informationssäkerhet.

Oscarson (2001) påpekar att de tre ovan nämnda begreppen konfidentiellitet, integritet och tillgänglighet ofta betecknas som aspekter av informationssäkerhet och att de tillsammans utgör en definition av informationssäkerhet. Han menar dock att de snarare representerar meningen med informationssäkerhet, dvs. vad man vill uträtta med informationssäkerhet.

- Konfidentiellitet avser skydd av information som förhindrar att informationen finns tillgänglig eller kan avslöjas för obehöriga. Behovet av att skydda information och program finns hos i stort sett alla företag. Några exempel på sådan materiel som måste skyddas är information i samband med produktutveckling och marknadsföringsplaner. (Stadskontoret, 1997c)

- Integritet avser att det ska finnas skydd så att ingen obemärkt kan skapa ny, skriva över, ändra eller radera företagets lagrade information (Nordqvist, 1997). Det är alltså av stor vikt för företaget att den information som finns är korrekt, aktuell och fullständig. Om informationen är felaktig eller inaktuell så kan det innebära att felaktig information sprids både internt och externt samt att beslut inom företaget fattas på felaktiga grunder.

- Tillgänglighet innebär att företagets resurser ska finnas tillgängliga för de individer som är behöriga att använda dessa (Nordqvist, 1997). Användarna ska kunna utnyttja resurserna efter behov. I och med att fler och fler har mobila arbetsplatser så ökar kraven att företagens system ska ha en hög tillgänglighet. Det är en förutsättning för att arbete ska kunna bedrivas var användaren än befinner sig. Dålig tillgänglighet kan till exempel resultera i att visst arbete inte utförs i tid och att svar inte kan lämnas till externa intressenter som förväntar sig en hög servicenivå.

Det är av stor vikt att företag har god kontroll och åtgärdar hot som är aktuella för de tre områden som presenterats ovan. Företagen måste därför granska hotbilden som finns mot företaget och därefter utvärdera om de skyddsåtgärder som finns inom respektive område. Därefter kan man göra en bedömning av företagets informationssäkerhet.

3.2 Ramverk

Arbetet med informationssäkerhet kan delas upp i två typer av säkerhet (Statskontoret, 1997a). Det handlar i ena fallet om administrativ säkerhet, det vill säga regler och rutiner för hur och när olika moment skall utföras och i andra fallet om IT-säkerhet, det vill säga säkerhet för informationen som hanteras i olika typer av datasystem. Tillsammans med Oscarsons definition av meningen med informationssäkerhet (konfidentiellitet, integritet och tillgänglighet) utgör dessa två typer mitt teoretiska ramverk för att studera säkerhetsimplikationer vid införandet av mobil plattform.

	Konfidentiellitet	Integritet	Tillgänglighet
• Administrativ säkerhet			
• IT-säkerhet			

Figur 3.5 visar hur de olika aspekterna av informationssäkerhet bildar ett ramverk.

Jag ämnar i mitt resultat kartlägga implikationer inom ramverket ovan.

4 Resultat

Resultatet består av två delar; en kartläggning över användningen av mobila datorer i näringslivet (genom enkätundersökning) samt kartläggning av teoretiska implikationer genom teori och tillämpning av presenterat ramverk.

4.1 Implikationer från Teori

Nedan följer identifierade hot som lyfts in i tidigare definierat ramverk.

	Konfidentiellitet	Integritet	Tillgänglighet
• Administrativ säkerhet	2, 4, 5, 6, 7, 8, 13, 14	2, 4, 7, 8, 14	2, 4, 5, 6, 7, 8, 10, 12, 14
• IT-säkerhet	1, 3, 6, 7, 9, 11	1, 7, 9	1, 6, 7, 9

Figur 3.5 Hotbilden har lyfts in i tidigare presenterat ramverk.

Nedan följer en förklaring till varför hoten har lyfts in på respektive plats i ramverket:

1. Funktioner för identifiering och autenticering är vanligtvis lösenord, men kan även vara t.ex. biometri. Gemensamt är att de är av teknisk karaktär och definieras därför som IT-säkerhet. Om identifiering och inloggning inte fungerar finns risk att obehöriga kan få åtkomst till information, som då kan läsas, ändras eller raderas.

2. Om funktionerna för identifiering och autenticering istället har brister i sin utformning, så att lösenord är så pass lätta att det går att gissa sig till dem eller att de är nedskrivna på lappar är detta av administrativ karaktär. I övrigt är risken densamma som ovan beskrivna hot.

3. Avlyssning av trådlös datakommunikation är av teknisk karaktär och kan leda till att obehöriga kan ta del av hemlig information.

4. Regler, rutiner och dokumentation är i sin natur av administrativ typ. Om en produkt av okunskap används på fel sätt kan säkerhetshål öppnas, men informationen kan även påverkas negativt direkt. Användaren kan t.ex. spara ett felaktigt dokument, radera fel akt etc.

5. Att information försvinner beroende på att det fysiska medium som den är sparad på stjäls eller förläggs beror ofta på brister i rutiner och regler och är därmed av administrativ karaktär. Om informationen inte heller är säkerhetskopierad är även detta av administrativ karaktär. Ett stulet CompactFlash minne med viktig information som inte har säkerhetskopierats hotar därför både konfidentiellitet och tillgänglighet.

6. Hot från virus kan vara av både administrativ och teknisk karaktär. Detta beror på att ett tekniskt virusskydd aldrig kan garantera en virusfri miljö, då det konstant kommer nya typer av virus. I teorin kan inte heller ett väl fungerande virusskydd garantera säkerhet, eftersom användarna omedvetet eller medvetat kan stänga av det. Ett virus hotar både tillgänglighet och konfidentiellitet hos informationen, då det kan både förstöra den eller exempelvis skicka ut dokument vi e-post.

7. Trojanska hästar hotar verksamheten på samma sätt som virus, men då det även är möjligt att fjärrstyra en dator med en trojansk häst, kan dokument ändras och på sätt hotas även integriteten i informationen.

8. Om en användare lämnar en inloggad handdator obevakad är detta ett administrativt hot. Tekniska lösningar (som t.ex. inloggning) är verkningslösa, då användaren redan gått förbi dessa. Information på en obevakad handdator kan läsas, raderas eller ändras.

9. Felaktigt konfigurerad mjuk eller hårdvara kan leda till att säkerheten inte fungerar på något plan, då viktiga funktioner kan vara avslagna eller inte fungera på annat sätt.

10. Inkonsekvenser och konflikter mellan applikationer är av administrativ karaktär, då regler och rutiner reglerar hur och vilka program som får användas. Har man dåliga rutiner kan detta t.ex. få som följd att en person skickar ett dokument till en annan person, som i sin tur inte kan ta del av informationen eftersom de har olika typer av dokumenthanterare på sina handdatorer.

11. När väl en obehörig användare har direkt tillgång till hårdvaran är företaget beroende av att informationen är skyddad av tekniska skydd. Informationen kan i annat fall läsas av en eventuell obehörig användare.

12. Vid förlust av information måste denna information återskapas (om det finns backup). Rutiner som beskriver hur detta skall ske är av administrativ karaktär.

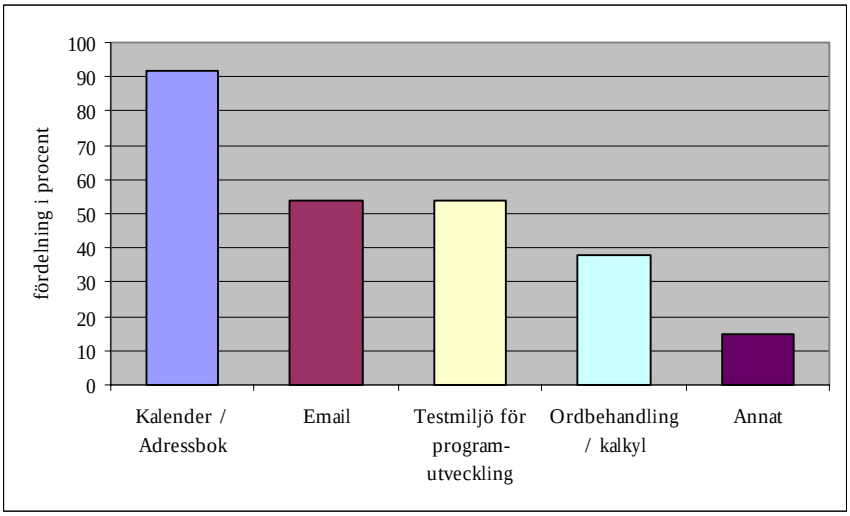
13. Utan direkta påbud är det lättare för en anställd att både för sig själv och för andra rättfärdiga sitt handlande.

14. Dålig utbildning kan precis som dålig dokumentation leda till att en produkt av okunskap används på fel sätt.

4.2 Empirisk undersökning

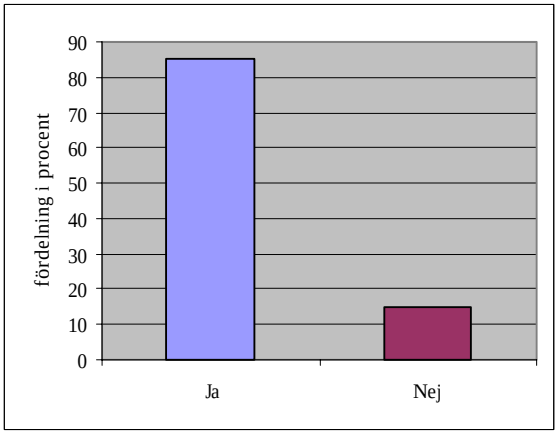
Nedan följer resultatet av undersökningen som syftade till att kartlägga användandet av handdatorer.

Undersökningen gjordes på en grupp av 32 företag inom IT och telekombranschen, då de i sina respektive verksamhetsområden ofta använder sig av ny teknik. Av de 32 företagen svarade 19 stycken på enkäten, vilket gör svarsfrekvensen till ungefär 59 %. Detta får ses som ett relativt bra resultat. Av de 19 svarande använde 13 företag handdatorer och 6 svarade att de inte hade några handdatorer i organisationen.



Figur 4.1 Vad företagen använder sina datorer till.

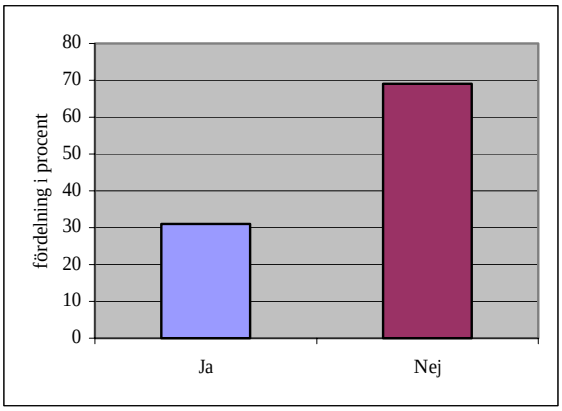
Undersökningen visar att kalender och adressbok var de mest använda funktionerna, då 92 % av respondenterna sade att de använde dessa tillämpningar (se figur 4.1). Handdatorerna användes även i ganska stor utsträckning till att skicka e-post (54 %) och som testmiljö för programutveckling (även här 54 %). Ordbehandling och kalkylprogram var lite ovanligare, då endast 38 % sade att handdatorerna användes till detta. Andra saker som handdatorerna användes till var som terminal till traditionella system och produktionsstöd.



Figur 4.2 Hur företagen svarade på frågan ifall användarna själva fick installera programvara.

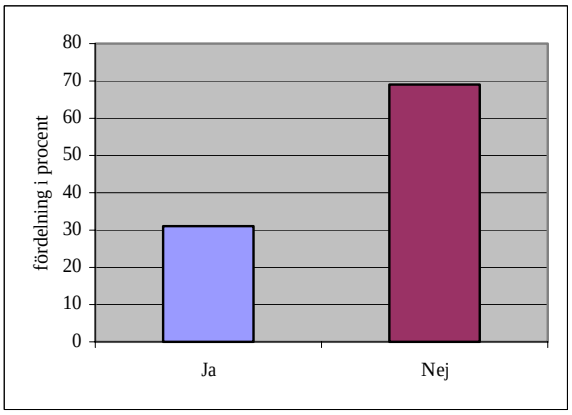
På frågan om företagen tillåter att användarna själva installerar programvara svarade 85% av respondenterna att det var tillåtet, medan 15% svarade att det inte var tillåtet (se figur 4.2).

De företag som svarade att det inte var tillåtet för användarna att själva installera programvara fick en följdfråga. Detta för att ta reda på ifall företagen ifråga hade implementerat några tekniska hinder för att förhindra att användarna installerar egen programvara. Av de två företagen som svarade att det inte var tillåtet var det bara det ena som hade någon form av tekniskt skydd.



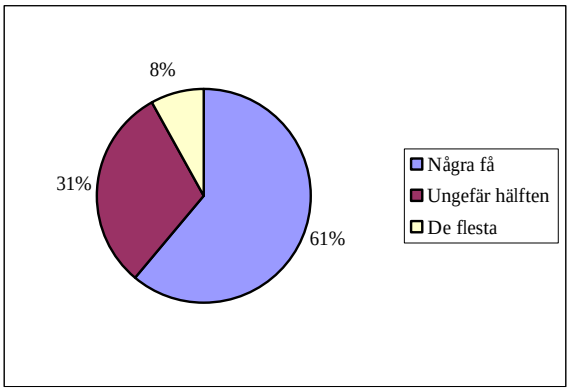
Figur 4.4 Andelen företag som har en särskild dokumenterad policy för användandet av handdatorer.

Fråga nummer fyra i enkäten ämnade ta reda på ifall företagen som medverkade i undersökningen hade en särskild, dokumenterad, policy för användande av handdatorer. En klar majoritet, 69 %, svarade att de inte hade en särskild policy för handdatorer. 31 % svarade att de hade en policy för handdatorer (se figur 4.4).



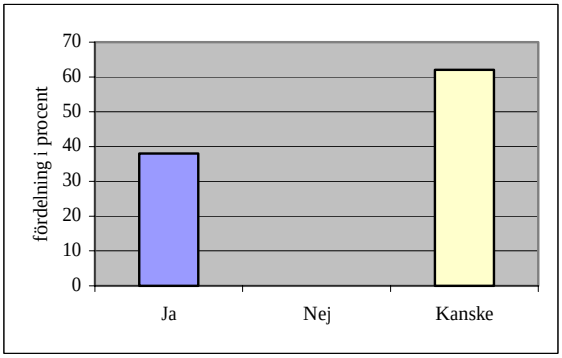
Figur 4.5 Hur många företag som kräver någon speciell säkerhetsåtgärd vid användande av handdatorer.

En klar majoritet av företagen (69 %) svarade att de inte kräver någon form av säkerhetsåtgärd vid användande av handdatorer. De företag som krävde säkerhetsåtgärder (31 %) begärde att användarna antingen nyttjade lösenordsskydd vid inloggning eller en kombination av lösenord och kryptering (se figur 4.5).



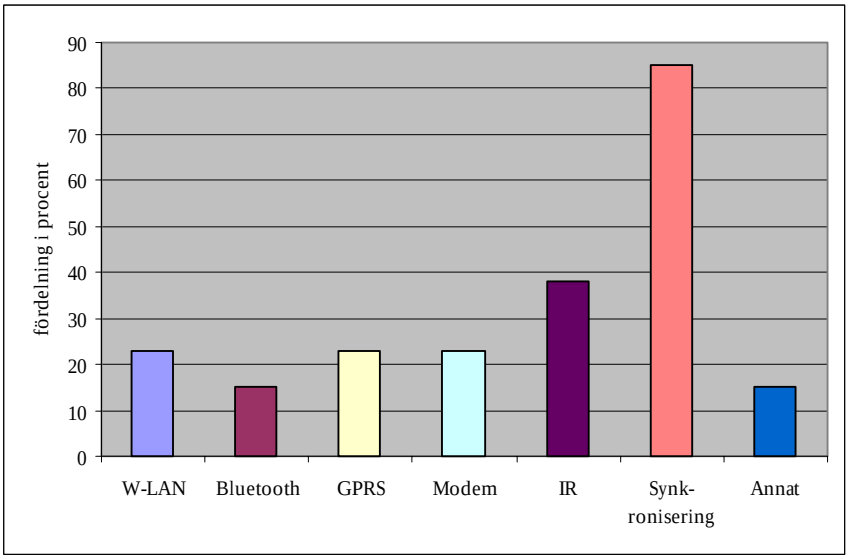
Figur 4.6 Hur utbredd användningen är av handdatorer är i företagen, dvs. hur många av de anställda som använder handdatorer.

Det är fortfarande bara ett fåtal i företagen som använder sig av handdatorer, då endast 8 % svarade att en majoritet i deras företag använder handdatorer. Hela 61 % svarade att det endast var ett fåtal som använde sig av handdatorer. 31 % svarade att ungefär hälften av företagets anställda nyttjade handdatorer (se figur 4.6).



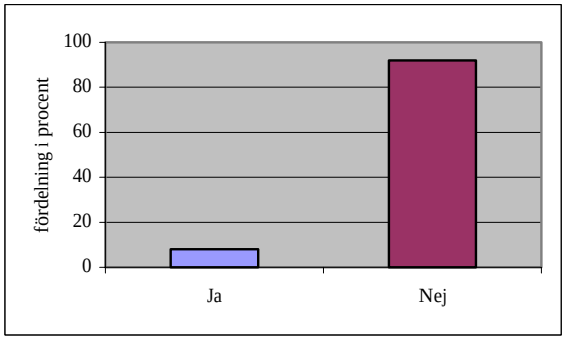
Figur 4.7 Hur de företag där ett fåtal anställda använder handdatorer ställer sig till frågan ifall de i framtiden skall utöka antalet handdatorer..

De företag som svarade att bara ett fåtal av de anställde använde sig av handdatorer fick frågan ifall de i framtiden skall utöka antalet handdatorer i verksamheten. Inget företag sade nej och 38 % svarade ja. 62 % var osäkra och svarade kanske (se figur 4.7).



Figur 4.8 Vilka möjligheter det finns att koppla upp sig mot företagens nätverk.

Alla svarande uppgav att det fanns någon form av möjlighet att koppla upp handdatorn till företagets nätverk. Den absolut vanligaste formen var synkronisering av handdatorn mot en lokal PC, då 85 % svarade att denna möjlighet gavs. Näst vanligast var uppkoppling och överföring av filer via IR (38 %) och sedan följde de andra typerna av uppkoppling ganska tätt därpå. Modem, GPRS och W-LAN var lika vanligt (23 %), medan Bluetooth endast användes i 15 % av fallen. Två företag uppgav att det inte var offentliga uppgifter, därav 15 % på ”Annat” (se figur 4.8).



Figur 4.9 Andelen företagen som ändrade det befintliga nätverket vid införandet av handdatorer i verksamheten.

Sista frågan var ifall företagens befintliga nätverk ändrats på något sätt vid införandet av handdatorer. 92 % svarade att ingen ändring gjorts och ett företag uppgav att de gjort ändringar i nätverket (se figur 4.9). Detta företag uppgav också att medvetenheten om riskerna med handdatorer ökade och att policys var på väg att tas fram.

5 Diskussion

Diskussionen som följer är indelad i två delar; en inledande del avseende teoretiska säkerhetsimplikationer baserat på resultatet från uppsatsens teoriavsnitt och en avslutande del avseende användningen av handdatorer på företag. Denna del baseras på det sammanställda resultatet från den empiriska undersökningen. På detta följer sedan en slutsats.

5.1 Teoretiska implikationer

Här följer en diskussion angående olika säkerhetsimplikationer som identifierats utifrån det tidigare definierade ramverket.

Efter att i resultatet ha identifierat och placerat hoten i ramverket så är det möjligt att utläsa att de flesta hoten identifierats som hot mot den administrativa säkerheten (se figur 5.1).

	Konfidentiellitet	Integritet	Tillgänglighet
• Administrativ säkerhet	2, 4, 5, 6, 7, 8, 13, 14	2, 4, 7, 8, 14	2, 4, 5, 6, 7, 8, 10, 12, 14
• IT-säkerhet	1, 3, 6, 7, 9, 11	1, 7, 9	1, 6, 7, 9

Figur 5.1 Ramverket visar att de flesta hot är av administrativ karaktär.

För att vidare granska de administrativa hoten kan man titta på de tre delområden konfidentiellitet, integritet och tillgänglighet. Ur ramverket kan det då utläsas att en majoritet av hoten placerats under rubrikerna konfidentiellitet och tillgänglighet (se figur 5.2). Då dessa kategorier är överrepresenterade vad gäller antalet hot till skillnad mot kategorin integritet, visar det att de flesta hot som riktas mot företag hotar dess konfidentiellitet och tillgänglighet. Som man kan utläsa av ramverket så är de flesta hoten under kategorin integritet även med under de två övriga kategorierna (konfidentiellitet och tillgänglighet). Detta innebär att företagen genom att skydda sig mot hot mot konfidentielliteten och tillgängligheten även kan få ett skydd mot det som hotar integriteten. Företagen kan alltså genom att koncentrera sig på de vanligaste hoten få en bra nivå på sin informationssäkerhet.

	Konfidentiellitet	Integritet	Tillgänglighet
• Administrativ säkerhet	2, 4, 5, 6, 7, 8, 13, 14	2, 4, 7, 8, 14	2, 4, 5, 6, 7, 8, 10, 12, 14
• IT-säkerhet	1, 3, 6, 7, 9, 11	1, 7, 9	1, 6, 7, 9

Figur 5.2 Ramverket visar att de flesta administrativa hot riktas företagets konfidentiellitet och tillgänglighet.

Ytterligare en reflektion som kan göras utifrån det teoretiska ramverket är att en majoritet av de identifierade administrativa hoten kan härröras till anställda, dvs. hoten kommer huvudsakligen från personer inom företaget. Anställda som agerar på ett för företaget skadligt sätt är inte alltid medvetna om skadeverkningarna, då handlingarna inte alltid är medvetet skadliga. En anställd kan t.ex. skriva ner sitt, i den anställdes tycke, svåra lösenord för att komma ihåg det. Detta kan av en angripare utnyttjas för att kunna logga in i företagets nätverk och på så sätt tillskansa sig information. Andra fall kan en anställd medvetet angripa företaget inifrån. Det är dock viktigt att företag inte behandlar sina anställda som potentiella hot eller brottslingar, eftersom detta lätt kan leda till missnöjda anställda. Missnöjda anställda kan i förlängningen skada företagets informationssäkerhet då de känner sig felaktigt behandlade och inte har lojalitet till företaget.

5.2 Empirisk undersökning

Den empiriska undersökningen som utfördes i form av en enkätundersökning visade tydligt att en majoritet av företagen i någon utsträckning använde sig av handdatorer. Samtidigt visade det sig att en klar majoritet inte implementerat någon särskild policy som omfattar användandet av de mobila enheterna. Detta leder lätt till att användarna själva sätter gränserna och beslutar vad som är ett säkert och acceptabelt användande. Många företag kan tänkas anta att en eventuell övergripande policy för datorer kan användas, men de speciella egenskaper som en handdator har gör både att en sådan policy inte alltid kan appliceras på dem. Vidare finns en risk att användarna själva inte identifierar och använder handdatorn som en dator vilket kan innebära att det krävs ett annorlunda säkerhetsmedvetande. Givetvis bör företagen lita på sina anställda att de agerar med sunt förnuft, men det är alltid lättare att tänja på gränserna om det inte finns några explicita regler. Något som är självklart för några är inte självklart för andra, vilket gör att man inte kan överlåta beslutandet till användarna.

Undersökningen visade även att ett vanligt användningsområde var både att skicka e-post och att använda handdatorn till ordbehandlig och kalkylering. Både e-post och ordbehandling är två väldigt vanliga orsaker till virusspridning i traditionella datormiljöer och det finns all anledning att misstänka att det även kan bli så på handdatorer inom en nära framtid. Ytterligare en stor virus och trojan-risk föreligger vid nerladdningen och installation av okänd programvara från Internet. Hela 85 % av de tillfrågande företagen svarade att användarna fritt fick installera programvara. Detta leder även till att företagen riskerar att få en handdator miljö som i det närmaste är anarkistisk, vilket även leder till att det blir mycket svårt för en säkerhetsavdelning att ha en överskådlig syn på handdatormiljön i företaget. Att tillåta användarna att fritt installera programvara på handdatorn kan även skapa svårigheter vid delning av dokument eftersom ett vanligt textdokument som skrivits i ett program inte kan öppnas och läsas i ett annat.

I dagsläget visade det sig att handdatorerna används av ett fåtal på företagen, så eventuella säkerhetsrisker minskar på detta sätt. Dock svarade ingen i undersökningen nej på frågan ifall de skall utöka antalet handdatorer i framtiden, vilket gör frågan än viktigare i framtiden när företag i större utsträckning implementerar handdatorer i sin datorpark.

Alla företag svarade att användarna hade någon form av möjlighet att koppla upp sig och majoriteten erbjöd vanlig synkronisering mot en stationär dator. Dock använde sig en förhållandevis stor andel av företag av modemuppkopplingar. Detta betyder att det finns möjlighet att ringa upp nätverksanslutna datorer utifrån. En borttappad handdator kan alltså i värsta fall ge en direktlinje till företagets nätverk. Även trådlösa uppkopplingsmöjligheter som W-LAN sparar ofta inloggningsdata och en borttappad handdator kan även här ge en angripare tillgång till företagets nätverk.

5.3 Slutsats

Resultatet av undersökningen visade att det var få företag som krävde speciella säkerhetsåtgärder vid användandet av handdatorer. Detta aktualiserar än mer behovet av anpassning av företagens policys för att även inbegripa handdatorer. Risken finns att företag låter handdatorerna ligga utanför sin säkerhetspolicy och på så sätt överlåter på användarna själva att sköta säkerheten. Även om användarna använder inloggningsskydd och kryptering så räcker tekniska lösningar oftast inte för att skydda ett system eftersom en utrustning som inte används på rätt sätt gör att investeringen är bortkastad. Väl fungerande administrativa rutiner är minst lika viktiga som tekniska lösningar. Detta är särskilt viktigt då det är just de administrativa hoten som är den vanligaste typen av hot.

Även om fokus bör ligga på den administrativa säkerheten behövs även olika former av IT-säkerhet. De flesta av dagens handdatorer levereras med möjlighet till lösenordsskydd och eventuellt även möjlighet till kryptering av filer. Det finns även en stor mängd tredjepartstillverkare som erbjuder förbättrade inloggningsrutiner och som även snart kommer börja leverera brandväggar och antivirusprogram speciellt anpassade till handdatorer. Ändå är det förhållandevis få företag som idag kräver någon form av säkerhetsåtgärd vid användande.

Införandet av mobila enheter i verksamheten medför tre övergripande implikationer som innebär att:

- Risken för att obehöriga kan ta del av affärshemligheter ökar då handdatorn är tillräckligt kraftfull för att lagra känslig företagsinformation på samt att den ofta ger möjlighet att koppla upp sig mot företagets interna nätverk. Detta betyder att en borttappad eller stulen handdator utgör ett stort hot mot företagets informationssäkerhet.

- Risken för säkerhetshål i företagets nätverk ökar om användarna själva installerar programvara på sina handdatorer. Detta då det ökar risken att programvara som innehåller säkerhetshål eller trojaner installeras.

- Risken för att problem med kompabilitet mellan olika användare ökar om användare tillåts installera egen programvara. Detta då exempelvis dokumentet som skapats i en handdator inte nödvändigtvis kan läsas på en annan handdator.

Policyn som reglerar de anställdas användning av plattformen inom företaget måste uppdateras för att även innefatta den nya mobila plattformen. Även policyn som IT-avdelningens administrativa regler måste uppdateras och anpassas efter användningen av handdatorer i företaget. Det är viktigt att IT-avdelningen ser till att det finns en enhetlig plattform på alla handdatorer.

6 Referenslista

Beckman, A. (1993). *PC säkerhet – En handbook*. Stockholm: Affärsinformation

Borg, Lozano, Löfgren, Malmgren & Palicki. (1997). *IT-säkerhet för ditt företag.* Uddevalla: Bonnier DataMedia

Dahlbom, B. (1998). *Från ingenjör till itenjör*. URL: http://www.viktoria.se/~dahlbom/

Denscombe, M. (2000). *Forskningshandboken –för småskaliga forskningsprojekt inom samhällsvetenskaperna.* Lund: Studentlitteratur

Easterby-Smith, Thorpe & Lowe. (2002). *Management Research – An Introduction.* London: SAGE

Gollman, D. (2000). *Computer Security.* West Sussex: Wiley

Harrison, L. (2001). *62,000 mobiles lost in London's black cabs*. URL: http://www.theregister.co.uk/content/archive/21388.html

Holme & Solvang. (1997). *Forskningsmetodik.* Lund: Studentlitteratur

Höglund & Persson. (1985). *Information och kunskap. Informationsförsörjning – forskning och policyfrågor*. Umeå: INUM

Korsell, L. (2000). *IT-brott kan förebyggas*. URL: http://www.bra.se/extra/apropa/?button_read_old_article.181.=1

Kossakowski, K. (2003-03-05). *Glossary of Computer Security Incident Handling Terms and Abbreviations.* URL: http://www.cert.dfn.de/eng/pre99papers/certterm.html

McMillan, O. (2002). *PDA Security Policy - Worth Its Weight in Gold* URL: http://www.infosecnews.com/opinion/2002/03/20_02.htm

Nordner, A. (2002). Arbetsgivaren äger handdatorn. *Computer Sweden, nr 135*

Nordqvist, I. (1997). *Informationssäkerhet och arbetsrätt vid distansarbete – en studie av framtida distansarbete inom Försvarsmakten.* (Magisteruppsats). Stockholms universitet, Institutionen för Data- och Systemvetenskap.

Oscarsson, P. (2001). *Informationssäkerhet i verksamheter* (avhandling för filosofie licentiatexamen, Linköpings universitet).

Protect Data. (2002). *4 av 5 använder PDA utan policy.* URL: http://www.protectdata.se/newscenter/news_news_full_arch.jsp?ID=1557&Y=2002

Schneier, B. (1999). *Security in the real world - How to evaluate security technology.* URL: http://www.counterpane.com/real-world-security.pdf

Schneier, B. (2000). *Secrets and Lies - Digital Security in a Networked World.* New York: Wiley

Statskontoret. (1998). *Sammanhållen strategi för samhällets IT-säkerhet.* Stockholm: Statskontoret

Statskontoret. (1997a). *Handbok i IT-säkerhet II.* URL: http://www.statskontoret.se/pdf/199729A.pdf

Statskontoret. (1997c). *Handbok i IT-säkerhet III.* URL: http://www.statskontoret.se/pdf/199729C.pdf

Svensson, T. (1999). *Företagens skydd och säkerhet – Om lagar och praktisk tillämpning.* Kristianstad: Industrilitteratur

Teresko, J. (2001). *Guidelines For Implementing PDA Solutions.* URL: http://www.industryweek.com/CurrentArticles/asp/articles.asp?ArticleId=1158

Wallén G. (1996). *Vetenskapsteori och forskningsmetodik*. Lund: Studentlitteratur

Bilaga 1

Webbaserade enkäten

Handelshögskolan
VID GÖTEBORGS UNIVERSITET

Denna enkätundersökning genomförs som en del av min d-uppsats i informatik vid Göteborgs universitet. De inlämnade enkäterna kommer inte på något sätt kunna kopplas ihop med någon enskild person eller företag och kommer endast bearbetas av mig som utför enkätundersökningen.

Din medverkan i undersökningen är av stor betydelse för mig, då min d-uppsats delvis bygger på informationen som jag får ut från de inlämnade enkätsvaren. Jag är därför väldigt tacksam om du kan ta dig tid att fylla i de följande 10 frågorna.

Enkäten kräver att ni har en webbläsare som har stöd för JavaScript. En del av frågorna är följdfrågor och beroende på hur du svarar så är det möjligt att vissa frågor inte är aktuella för dig. Dessa frågor är gråskuggade och går inte att fylla i.

Tack på förhand,
Stefan Edevåg

Har ni några anställda som använder sig av handdatorer för verksamhetsrelaterade uppgifter?

- Ja
- Nej

Till frågorna –>

Handelshögskolan
VID GÖTEBORGS UNIVERSITET

1. Vad används handdatorerna till?

- ☐ Kalender/Adressbok
- ☐ Ordbehandling och kalkylprogram
- ☐ Email
- ☐ Testmiljö för utveckling av programvara
- ☐ Annat, nämligen

2. Är det tillåtet för användarna att själva installera programvara?

- ○ Ja
- ○ Nej

3. Om 'Nej' på fråga två, finns något tekniskt skydd som hindrar användarna att installera programvara?

- ○ Ja
- ○ Nej

4. Har företaget en särskild, dokumenterad, policy för användande av just handdatorer?

- ○ Ja
- ○ Nej

5. Kräver ni någon speciell säkerhetsåtgärd vid användande av handdatorer?

- ○ Nej
- ○ Ja
  - ☐ Lösenordsskydd
  - ☐ Kryptering
  - ☐ Biometri
  - ☐ Annat, nämligen

6. Hur utbredd är användningen av handdatorer i ert företag?

- ○ Några få använder handdator
- ○ Ungefär hälften använder handdator
- ○ De flesta använder handdator

7. Om ni bara har ett fåtal, planerar ni att utöka antalet handdatorer i framtiden?

- ○ Ja
- ○ Nej
- ○ Kanske

8. Om det finns möjlighet till uppkoppling till företagets nätverk via handdatorn, hur sker detta?

- ☐ W-LAN
- ☐ Bluetooth
- ☐ GPRS
- ☐ Modem
- ☐ IR
- ☐ Synkronisering mot stationär dator
- ☐ Annat, nämligen

9. Ändrades företagets befintliga nätverk på något sätt vid införandet av handdatorer?

- ○ Nej
- ○ Ja, på följande sätt:

Skicka!