Sikkerhet, trusler og mulige tiltak ved bruk av PDA i organisasjoner

Hovedoppgave
ved
sivilingeniørutdanning i
informasjons- og kommunikasjonsteknologi

av
Svein Aslak Sønderland

Grimstad, mai 2001

Sammendrag

Oppgaven omhandler en generell oversikt over hva en Personal Digital Assistent (PDA) er, hva som finnes på markedet, nye bruksområder, sikkerhetsmekanismer og trusler som man kan forvente kommer i den nærmeste fremtid. Oppgaven tar også for seg en bedriftscase som klassifiserer sikkerhetstrusler og sikkerhetstiltak en bedrift må ta stilling til hvis de velger å bruke en PDA i et bedriftsnett.

Tallet på solgte PDA'er i Norge har mer enn doblet seg på et år. Det er stadig flere som ser hvilke mulighetene en PDA har. Denne trenden viser seg også på de fleste andre steder i verden. Hvis de rette tiltakene ikke blir iverksatt, kan denne utviklingen føre med seg store sikkerhetsproblemer.

Innføring av PDA'er i et bedriftsnett medfører en risiko for at PDA'en kan føre med seg virus, worm og trojanske hester. Det finnes forskjellige måter å håndtere disse nye truslene på. Det er viktig at det blir laget retningslinjer/restriksjoner ved bruk av PDA'er som er tilpasset den enkelte bedrift. Det finnes forskjellige antivirusprogrammer som sjekker synkroniseringen mellom PDA og PC. Det er oppdaget et virus og en trojansk hest som kan angripe selve PDA'en, men kun de som har Palm OS. Det finnes også antivirusprogram som beskytter mot denne type trusler. Programmet installeres på PDA'en.
Intrusion Detection System (IDS) er en annen sikkerhetsmekanisme som kan brukes for å finne trojanske hester som en PDA kan ha ført med seg inn i bedriftsnettet under synkronisering.

Forord

Denne rapporten utgjør avslutningen på min utdannelse som sivilingeniør innen informasjons- og kommunikasjonsteknologi (IKT) ved Høgskolen i Agder.

Diplomoppgaven er normert til et semesters arbeid dvs. 10 vekttall.
Arbeidet har pågått i tidsrommet fra januar til og med mai 2001.

Oppgaven er utført i samarbeid med System Sikkerhet ASA i Arendal. Jeg ønsker å takke System Sikkerhet ASA for oppgaven og faglig veileder Jorunn Terjesen (ved System Sikkerhet ASA) for gode råd og veiledning underveis.

Jeg ønsker også å takke Magne Arild Haglund og Vladimir Oleshchuk som var ansvarlige veiledere ved Høyskolen i Agder for gode råd og veiledning.

Grimstad, 28.mai 2001

Svein Aslak Sønderland

Innholdsfortegnelse :

1 Innledning

1.1 Bakgrunn for oppgaven

I samarbeid med System Sikkerhet ASA, et av landets ledende rådgivingsfirmaer innen IT-sikkerhet, har vi sett på et område som kan være et mulig nytt satsningsfelt for bedriften: Sikkerhet ved bruk av PDA i bedrifter.

PDA sikkerhet er et interessant felt fordi teknologien er forholdsvis ny og fordi salget av PDA'er viser at de snart er "allemannseie". I fjor ble det solgt 77.000 lomme-PC'er i Norge. I år venter mange en fordobling. Trenden vises også de fleste andre steder i verden.

Flere og flere bedrifter ser hvilke muligheter denne teknologien har, men ikke alle ser hvilke farer som lurer ved å kople en PDA inn i et eksisterende nettverk.

Med denne oppgaven ønsker jeg å kartlegge sikkerhetsaspekt ved denne nye teknologien.

1.2 Oppgavebeskrivelse

Oppgavebeskrivelsen er i tråd med tittelen " Sikkerhet, trusler og mulige tiltak ved bruk av PDA i organisasjoner"

Rapporten består av følgende deler:

- En generell oversikt over hva en PDA er, hvilke typer som er på markedet, nye bruksområder, sikkerhetsmekanismer og trusler som man kan forvente kommer i den nærmeste fremtid.
- En klassifisering av sikkerhetstrusler som kan forbindes med eller være direkte forårsaket av bruk av PDA i en organisasjon, for eksempel i et system som består av et lokalt nettverk som er innenfor en brannmur, en docking stasjon for PDA som er tilkoplet en maskin i nettverket og hvor PDA'en kan også brukes utenfor brannmuren.
- Mulige tiltak mot disse sikkerhetstruslene.
- En tenkt bedriftscase hvor det er utført analyse og gitt anbefalinger til en bedrift på sikkerhetstiltak med hensyn på bruk av PDA i et eksisterende system.

1.3 Metode

Sikkerhet ved innføring av PDA i bedrifter har vært fokus i denne oppgaven. Siden dette er et tema som ikke har fått mye oppmerksomhet, har det vært vanskelig å finne gode kilder som tar for seg dette. Jeg har derfor være i kontakt med fagfolk. Mine veiledere ved HiA og System Sikkerhet ASA, PDA produsenter og distributører i Norge, firmaet PDA2day og andre firma og enkeltpersoner har vært til god hjelp under prosjektarbeidet.
Jeg har prøvd å sammenligne PDA sikkerhet med veletablerte sikkerhetsløsninger.

1.4 Leserveiledning

Kapittel 1 leder leseren inn i problemstillingen. Kapittel 2 beskriver forskjellige PDA'er, ulike operativsystem, hva PDA'er brukes til i dag, og hvordan man kan forvente at bruken av PDA vil endre seg i den nærmeste framtiden. Kapittel 3 og 4 tar for seg forskjellige nettverks- og PDA trusler. Kapittel 5 gjennomgår en bedriftscase med tiltak mot PDA truslene. Kapittel 6 inneholder konklusjonen på rapporten, mens kapittel 7 inneholder de forskjellige referansene. Rapporten avsluttes med vedleggene.

2 Personal digital assistent (PDA)

2.1 Hva er en PDA?

En PDA er en personlig digital assistent, altså en digital utgave av en filofax. Men overgangen fra den gode gamle filofax'en til PDA'en betyr mer enn det å gjøre dine avtaler og memo'er digitale. En PDA betegnes som en håndholdt PC eller lomme-PC, dette gjøres ikke bare fordi den er mindre enn en PC, men også fordi den har nesten den samme funksjonaliteten som en PC.

Tabellen under sammenligner de 3 mest vanlige PDA typene [10] [12] [13]:

Tabell 1 Sammenligning av PDA'er.

	Palm Vx	**Psion Revo Plus**	**Compaq iPAQ H3630**
			
Operativsystem (OS):	Palm OS 3.5	EPOC	Pocket PC
Agenda/kalender (j/n):	Ja	Ja	Ja
Kontaktliste (j/n):	Ja	Ja	Ja
Huskeliste (j/n):	Ja	Ja	Ja
Notatblokk (j/n):	Ja	Ja	Ja
Tekstbehandling (j/n):	Nei	Ja	Ja
Regneark (j/n):	Nei	Ja	Ja
E-post (j/n):	Ja	Ja	Ja
WAP (j/n):	Nei	Ja	Nei
Internett (j/n):	Nei	Ja	Ja
Mp3 (j/n):	Nei	Nei	Ja
Videoavspilling (j/n):	Nei	Nei	Ja
Bildevisning (j/n):	Nei	Nei	Ja
Vekt (g):	113	200	179
Størrelse (cm):	11,4x7,9x1,0	15,7x7,9x1,8	13,0x8,3x1,6
Tastatur (j/n):	Nei	Ja	Nei
Håndskrift (j/n):	Ja	Nei	Ja
Fargeskjerm (j/n):	Nei	Nei	Ja
Bakgrunnsbelysning (j/n):	Ja	Nei	Ja
Høytaler (j/n):	Ja	Ja	Ja
Prosessor (MHz):	20 MHz Motorola Dragonball	36 MHz Arm 710	206 MHz strong - ARM SA 1110
Minne (MB):	8	16	32
Batteritype:	Lithium-ion	2x700mAh AAA NiMH	Li-Polym
Batterivarighet:	1 mnd	1 uke	2 døgn
Skjermbeskrivelse:	160x160 pixels, 16 gråfarger	160x480 pixels, 4 gråfarger	240x320 pixels, 4096 farger
IR-port (j/n):	Ja	Ja	Ja
USB-port (j/n):	Nei	Nei	Ja
Audio-utgang (j/n);	Nei	Nei	Ja
Diktafon (j/n):	Nei	Nei	Ja
Utvidelsesport (j/n)	Nei	Nei	Ja

Det er flere produsenter som lager PDA'er. De lager sitt eget særpreg over produktet, men velger ofte et standardisert operativsystem. De mest vanlige operativsystemer som brukes i dag er Palm, EPOC og Pocket PC (Windows CE). Linux er også på full vei inn i markedet. Operativsystemet er en av de faktorene som bestemmer hvilken funksjonalitet PDA'en skal ha. Mange PDA'er gir også mulighet til å bygge ut funksjonaliteten ganske mye.

2.2 Forskjellige operativsystem

2.2.1 Innledning

Det finnes i hovedsak 4 operativsystem for PDA. Disse er:

- EPOC
- Palm OS
- Windows CE/Pocket PC
- Linux

Ikke alle produsentene har egenutviklede operativsystemer. EPOC har blitt utviklet av et firma som heter Symbian Ldt som eies av Motorola, Nokia, Ericsson Matsushita og Psion. Palm har utviklet sitt eget Palm OS. Microsoft har utviklet Windows CE og deres nye OS Pocket PC. Linux er som de fleste vet et åpent system.
Tabellen under viser hvilke OS de kjente produsentene bruker:

Tabell 2 Produsentens forskjellige OS.

Operativ system	**Produsenter**
EPOC	Psion, Ericsson, Nokia, Sharp (til neste år)
Palm OS	Palm, Handspring, Sony, TRG og IBM
Windows CE/Pocket PC	Compaq, HP, Palmax, Casio og Symbol.
Linux	Sharp, Compaq og Palmax.

Det er grunnleggende forskjeller mellom de ulike operativsystemene og da spesielt mellom Palm OS og Pocket PC/ Windows CE. Palm OS er basert på at Palm'en skal være en liten og lett håndholdt PC som kan bruke enkle programmer. Det er ikke meningen at den skal kunne kjøre avanserte multimedia programmer eller brukes tilnærmet likt en PC, detter er derimot Pocket PC/Windows CE laget for. EPOC ligger et sted mitt i mellom disse, de fleste mobiltelefoner med PDA funksjoner bruker dette operativsystemet.

2.2.2 Palm OS

Palm OS er det klart mest brukte operativsystemet i dag. Palm har per februar 2001 en markedsandel på ca 60 %, men det er ventet at blant annet Microsoft med Pocket PC i større grad kommer til å ta markedsandeler fra Palm OS. Palm OS er designet slik at det skal kunne kjøre små enkle programmer kjapt og effektivt. Samtidig har Palm's PDA'er lite minne og små prosessorer. Dette gjør at man bare kan kjøre et program av gangen. Hovedtanken bak Palm's produkter er at de skal ha en enkel konstruksjon med programmer som bruker lite ressurser. Palm'en skal på ingen måte være en PC.
Palm Pilot inneholder blant annet tidsplanlegger, kontakter, notatblokk og huskeliste. Det er slike programmer den er designet for å kjøre. I tillegg kan den kjøre programmer som regneark, Multimail og AvantGo, der Multimail gir deg mulighet til å motta og sende mail, mens AvantGo er en nyhetsleser.

2.2.3 Pocket PC/Windows CE

Microsoft operativsystemet Pocket PC er en videreutvikling av Windows CE [14].
Noen av de nye funksjonene i operativsystemet er at det finnes støtte for elektroniske bøker samt muligheten for å bruke Windows Media Player. Brukervennligheten til operativsystemet er også forbedret.
PDA'er med Pocket PC/Windows CE som operativsystem har et veldig bra utgangspunkt i og med at den kan brukes på flere typer prosessorer. Som Palm OS er den designet for bruk på håndholdte PC'er uten tastatur. Den krever en mye kraftigere prosessor og mer minne enn maskiner kjørt på Palm OS. Som et eksempel har Palm sine PDA'er fra to til åtte megabyte minne mens PDA'er kjørt på Windows CE/Pocket PC stort sett i dag opererer med fra 16 til 64 megabyte minne. Det er også vesentlige forskjeller i prosessorstyrke der Palm Vx [12] bruker en 20 MHz prosesser og Compaq iPaq [13] benytter seg av en prosessor på 206 MHz. Det er med andre ord snakk om to forskjellig produkter. Pocket PC/Windows CE er en miniutgave av Windows og inneholder miniutgaver av Microsoft Word, Excel mm. Samtidig har den støtte for multimedia- funksjoner. Enkelte PDA'er med Pocket PC/Windows CE åpner for kjøring av små filmsnutter og for å spille MP3. Det følger også med Internett Explorer som gjør at du kan surfe på nettet via din håndholdte pc. Det er helt andre muligheter med en PDA basert på Pocket PC/Windows CE enn med Palm OS. Pocket PC/Windows CE åpner for at man kan kjøre flere programmer samtidig, noe Palm OS ikke gir mulighet for. Pocket PC/Windows CE inneholder også flere programmer slik som regneark og mail program. Dette følger ikke med hvis du kjøper Palm OS.

2.2.4 EPOC

PDA produsenten Psion Group laget første versjon av EPOC. Senere overtok firmaet Symbian [16] Ldt utviklingen. Symbian Ldt eies av flere store konsern innen mobil kommunikasjon som Ericsson, Nokia, Motorola, Matsushita og Psion. Det er i hovedsak disse produsentene som bruker operativsystemet.

EPOC [17] er et velfungerende operativsystem. Dette operativsystemet dominerer på PDA'er med tastatur. Eksempelvis; Psion modellene [10] , Ericsson MC 218 [11] og Nokia Communicator [8]. EPOC har støtte for synkroniseringen både med seriekabel og USB. Operativsystemet støtter en webbrowser, men på de tidlige utgavene er denne relativt dårlig. De nye webbrowserne er ofte av typen Opera. Av programmer som kjører på EPOC plattformen kan man trekke frem et velfungerende mail-program, et tekstbehandlingsprogram som synkroniserer med ren tekst i Word og et regneark som synkroniserer med enkle Excel-ark. Det er mange gode programmer tilgjengelig til EPOC.

2.2.5 Linux

Linux operativsystemet er allemannseie. Sharp lanserer sin første PDA med Linux som operativsystem desember 2001. Compaq IPAQ kan bruke Linux, men det er bare noen få som blir levert med det. De fleste modellene bruker Pocket PC/Windows CE.

Linux på PDA ligner veldig på det som brukes på PC'er. Dette er litt spesielt i forhold til de andre operativsystemene. Selv om grensesnittet på f.eks. Pocket PC ligner på Windows er det ganske store forskjeller i kildekoden. Dette har både fordeler og ulemper i forhold til sikkerhet. At det finnes mange hackere som kan Linux gjør systemet mer sårbart, men at kildekoden er åpen gjør sikkerheten bedre.

2.3 Hvilke typer PDA'er finnes på markedet?

2.3.1 Innledning

Det er flere produsenter som lager egne håndholdte PC'er [6]. De mest vanlige er Palm, Psion, Compaq, Handspring, Ericsson, Casio, Nokia, Hewlett Packard, IBM og Palmax. Produsentene lager PDA'ene med sine egne egenskaper som gjør at de skiller seg fra hverandre. Det er for eksempel stor forskjell i modellenes operativsystemer, maskinvareutrustning som prosessorkraft og minnestørrelse. Enkelte har dessuten multimedia-egenskaper og utbyggingsmuligheter, som ikke finnes hos andre. Noen PDA'er er utstyrt med små keyboard, mens andre har trykk-følsom (håndskriftsgjenkjenner) som kan motta informasjon ved at man skriver på den med en slags plastpenn.

Palm er desidert størst i markedet og hadde en markedsandel på 53% i år 2000. På de neste plassene kommer Psion og Compaq med en markedsandel på litt over 10 prosent hver. Aktørene tror på en dobling av salget i forhold til i fjor. Da vil verdien på markedet i Norge nærme seg 700 millioner kr. Men PDA-produsentene må kjempe for å beholde markedsandelene for mobiltelefonprodusentene vil ha sin del av kaka.

Antoine Barre, Compaq Europa, har kommet med følgende spådom: "Lomme-pc'en og mobiltelefonen vil nok nærme seg hverandre stadig mer, og på sikt vil de nok smelte sammen".

I tabellen under [1] kan man se hvordan de forskjellige selskapene har fått/tapt markedsandeler de 2 siste årene. Man ser også at antallet solgte PDA'er er mer enn fordoblet fra 1999 til 2000:

Tabell 3 Markedsandeler.

Merke	Ant. enheter. solgt 2000	Ant. enheter. solgt 1999	Endring i prosent
Palm	40242	11860	239,30%
Psion	8276	4379	89,00%
Compaq	8016	1881	328,20%
Ericsson	5560	927	500,40%
Casio	4146	2098	97,60%
Nokia	3416	5535	-38,30%
Hewlett Packard	2294	3161	-27,40%
IBM	2262	480	371,30%
Andre	1982	237	739.70%
Totalt:	76335	32124	137,60%

2.3.2 PDA'er med Palm OS som operativsystem

PDA'er som bruker Palm OS er små og veldig brukervennlige. De har fokusert på de enkle tingene og på at PDA er et verktøy når du er "ute på tur". Programmene er designet slik at de skal bruke lite ressurser og ta liten plass. Palm OS skal støtte enkle programmer som tidsplanlegger, kontakter mm. Andre positive momenter med Palm OS er at alt du gjør lagres av seg selv. Palm'en starter også opp igjen der du slo den av dersom du ikke bruker hurtigtaster. Samtidig er Palm OS det operativsystemet som det finnes flest programmer til i dag.

Bildet under viser en Palm Vx [12]. Dette er en av de mest vanlige PDA'ene som er på markedet.

Palm har på folkemunne etter hvert blitt et felles uttrykk for PDA'er, fordi Palm Pilot var først ute og er dominerende på markedet. Men dette er ikke helt riktig. Palm er bare en av flere type PDA'er.

Deres posisjon er ikke helt ulik den Microsoft har klart å tilegne seg i operativsystem- og programvaremarkedet. I den senere tiden har det kommet mange store og gode konkurrenter som HP, Compaq og Casio for å nevne noen.

Figur 1 Palm Vx.

Palm er en av de få produsentene av PDA'er som har utviklet sitt eget operativsystem. Operativsystemet er et ganske enkelt system som ikke krever så mye prosessorkraft og minne. Informasjonen blir behandlet på en litt annen måte enn i en vanlig PC. En PC henter data inn i prosessoren før noe kan gjøres. Det som er spesielt med Palmen er at den jobber rett fra minnet. All data er lagret på samme måte som i en database.

De produsentene som bruker Palm OS har også et litt annet utgangspunkt enn f.eks. de produsentene som velger å bruke Microsofts mer avanserte Pocket PC operativsystem.

De mest kjente produsentene som i dag bruker Palm OS som operativsystem er: Palm, Handspring, Sony, TRG, IBM og Oregon Scientific.

2.3.3 PDA'er med Pocket PC/Windows CE som operativsystem

Operativsystemet Pocket PC/Windows CE er som tidligere nevnt en miniutgave av Windows. De inneholder miniutgaver av de mest vanlige Windows programmene [7].
Pocket PC/Windows er et mer avansert operativsystem en f.eks. Palm OS. Dette gir PDA'er som bruker Pocket PC/Windows CE mange flere muligheter enn de som bruker andre operativsystem. Det er ikke uvanlig at man kan kjøre multimedia applikasjoner ol. Den største ulempen med dette operativsystemet er at det er mye mer komplekst og krevende. Maskinvareutrustningen som prosessorkraft, minne og batteri er tilsvarende større. Dette er noe som igjen fører til at PDA'en blir gjerne større og tyngre en f.eks. Palmer.

Figur 2 på neste side viser bilde av Compaq IPAQ H36300 [13]. Dette er en PDA som bruker Pocket PC som operativsystem.

Figur 2 Compaq IPAQ H36300

I tabell 1 side 7 kan man se at Compaq IPAQ H36300 har god funksjonalitet, og den har også gode utbygningsmuligheter. Det er mulig å få PCMCIA-holder som festes på baksiden av PDA'en. Det finnes flere typer PCMCIA kort på markedet. Noen kort kan brukes for å kommunisere med Bluetooth, WLAN, og HiperLAN/2 og GSM. Det er bare et tidsspørsmål før man kan få kjøpt kort som kan kommunisere gjennom GPRS og UMTS. Det finnes også kort som inneholder GPS, man har da mulighet for kartvisning med posisjon. Dette er noe som er mer og mer brukt i større byer.

De mest kjente produsentene som i dag bruker Pocket PC/Windows CE som operativsystem er: Compaq, HP, Palmax, Casio og Symbol.

2.3.4 PDA'er med EPOC som operativsystem

PDA'er med EPOC ligger nok et sted midt mellom Palm OS og Pocket PC i funksjonalitet. EPOC har støtte for at flere programmer kan gå samtidig og er et velfungerende operativsystem uten støtte for de tyngste multimedia-applikasjoner. De fleste rene PDA'er som kjører på EPOC operativsystem har tastatur.

Figur 3 PsionRevo Plus

Bildet over viser PsionRevo Plus [10]. Spesifikasjonene for denne står i tabell 1 side 7. Jeg har valgt å bare se på denne modellen siden den er representativ for alle rene PDA'er med EPOC som operativsystem

Mobiltelefoner med PDA funksjonalitet som bruker EPOC.

Flere og flere mobiltelefon-produsenter har begynt å legge PDA-egenskaper inn i telefonene. Bildet under er av Ericsson R380s [11]. Den er en av de mest avanserte som finnes på markedet. Dette er en telefon som ikke har tastatur.

Figur 4 Ericsson R380s

Tabellen under viser spesifikasjonene til EricssonR380s:

Tabell 4 Spesifikasjoner Ericsson R380s

Funksjoner	
Agenda/kalender	
Kontaktliste	
Huskeliste	
Notatblokk	
E-post	
Tekstmeldinger	
WAP	
Internett	
Vekt	164 g
Størrelse	13,0x5,0x2,6 cm
Håndskrift	
Høyttaler	
Operativsystem	EPOC
Batteritype:	Lithium-ion
Batterivarighet:	4/106 timer
Mikrofon	

Telefonen har avansert PDA verktøy, slik som adressebok, kalender, notisblokk og support for synkronisering med de mest brukte applikasjonene (outlook, lotus, mm).

Nokia 9210 [8]er en annen telefon som bruker EPOC som operativsystem. Den har stort sett de samme egenskapene som Ericsson R380s [11] og Motorola Accompli A6188 [9], men den har tastatur og er derfor utrustet med forskjellige tekstbehandlingsprogrammer, regneark og notisblokk.

De mest kjente produsentene som i dag bruker EPOC som operativsystem er: Ericsson, Nokia, Motorola, Matsushita og Psion.

2.3.5 Mobiltelefoner med PDA funksjoner.

Bildene under viser de 3 mest vanlige mobiltelefonene [8] [9] [11] som har PDA funksjonalitet.
Disse telefonene har mye av den samme funksjonaliteten som en ren PDA.

Figur 5 Nokia 9210

Figur 6 Ericsson R380s

Figur 7 Motorola Accompli A6188

Magcom [15] er en ny norsk produsent som vil prøve å konkurrere med de mer veletablerte produsentene. Mobiltelefonen blir kalt Magcom og er avbildet under:

Figur 8 Magcom Magcom

Telefonen innfridde ikke helt de forventningene som var satt til den. Telefonen har ikke støtte til bredbånd, det vil si GPRS eller UMTS. Dette er noe som kommer i senere utgaver. Den har heller ikke Bluetooth.

Dette er en telefon som har nettleser for Web (html) og WAP, E-postleser Pop3 (vanlig mail) og avtalebok, kalender, notater og oppgaver kan synkroniseres mot Outlook.

Fremdeles har mobiltelefon-produsentene mye igjen før de kan konkurrere med en ren PDA. Dette skyldes i hovedsak størrelse, pris, funksjonalitet og prosessor/minne utrustning.

2.3.6 Tilleggsutstyr

Det finnes forskjellig typer tilleggsutstyr til PDA'er. Faktorer som hvilket operativsystem som blir brukt, produsent og hvor ny PDA'en er, bestemmer hvilken ny funksjonalitet man kan tilegne PDA'en. I tillegg til kabler, tasker og software kan det kjøpes utstyr som gir PDA'en tilleggsfunksjonalitet slik som:

- Kamera
- MP3 Spiller
- Global Positioning System (GPS)
- Visittkort skanner
- Modem
- Modul for Bluetooth
- Modul for fjernkontroll funksjonalitet
- Stemmeopptaker
- Strekkodeleser
- Ekstra minnekort
- Ekstra batteri
- IR
- Tastatur (også sammenleggbart)
- PCMCIA kort holder
    - Modem – kort (hustelefon)
    - Modem – kort (GSM. Kan da også brukes som mobiltelefon)
    - GPRS – kort (Er laget men, har ikke funnet denne ute for salg ennå)
    - Minne – kort
    - Kort med overgang til skjerm eller Prosjektør

Bildene under viser tilleggsutstyr. På figur 9 er det avbildet PCMCIA Expansion Pack som brukes sammen med PDA'en Compaq IPAQ. Denne PCMCIA-kort holderen kan også lese minnekort. Holderen har innbygget batteri, siden PCMCIA kort kan dra mye strøm.
Figur 10 viser en Palm med tastatur som tilleggsutstyr. Dette kan være greit hvis man har behov for å skrive en del. Det er også mulig å få kjøpt sammenleggbart tastatur.

Figur 9 PCMCIA kort holder

Figur 10 Tastatur

2.4 Oversikt over forskjellige måter en PDA kan kommunisere med andre

Det finnes flere måter PDA'er kan kommunisere på. Det kommer litt an på hvem eller hva man ønsker å kommunisere med. Det er også forskjell på kommunikasjonsutrustning. Punktene under viser hvilke forskjellige måter en PDA kan kommunisere på. Dette er nærmere beskrevet i vedlegg A.

- IR
- Rs-232
- USB
- Bluetooth
- Wireless LAN
- HiperLAN/2
- GSM
- GPRS

2.5 Hva er begrensningene for hva PDA'er kan brukes til?

PDA'er åpner for mange nye muligheter og bruksområder, punktene under viser de faktorene som setter grenser for hva man kan bruke en PDA til:

- Kostnader
- Størrelse
- Prosessorkraft
- Minnekapasitet
- Overføringshastighet

2.5.1 Kostnader

For folk flest har pris mye å si for hvilken type PDA man kjøper. Prisen kan variere fra 2000-3000 for PDA'er som ikke har stort mer enn filofaks funksjonalitet, til de som koster 12000 – 13000 og har tilnærmet laptop-funksjonalitet.

2.5.2 Størrelse

Størrelse en viktig faktor for en som skal kjøpe seg en PDA. Punktene under viser noen faktorer som kan være med på å bestemme størrelsen på en PDA:

- Det er stor forskjell på størrelsen på en PDA med og uten tastatur.
- PDA'er med stor funksjonalitet, er gjerne tykkere og tyngre en de enkle PDA'er som ikke kan brukes til så mye. Dette fordi stor funksjonalitet krever større minne, mer prosessor- og batterikapasitet, mer kjøling og større batteri.
- Nye modeller er ofte tynnere enn de gamle.
- Dyre modeller er gjerne mindre og tynnere enn billige modeller. Chassiset er ofte laget av metall siden det er sterkere, tynnere og bedre til å lede bort varme.

2.5.3 Prosessorkraft/minnekapasitet

Det kan være stor forskjell på prosessor og minnekapasiteten på ulike PDA'er ut fra hvilke operativsystem de skal kjøre. PDA'er som bruker Pocket PC/Windows CE har større prosessor og minnekapasitet enn de som kjører et lettere system slik som for eksempel Palm Os. Et tyngre operativsystem krever ikke bare mer minne fordi det trenger mer plass for mellomlagring, men programmene er også mer avanserte og større. Økt funksjonelt krever mer minne til lagring av dokumenter og filer som programmene skal behandle. Et godt eksempel kan være en musikkspiller hvor musikkfiler tar mye lagringsplass.

2.5.4 Overføringshastighet

Overføringshastigheten på GSM mobilnettet varierer fra 9,6 kb/s standard GSM mobilnett til "High Speed Circuit Switched" som kan ha overføringer på 43,2 kb/s.
Med GPRS kan man teoretisk ha overføringer på 56 kb/s (4 av 8 mulige tidsluker á 14 kb/s). Telenor har GPRS-testnett på Sørlandet, her tillates bruk av 3 tidsluker til nedlasting og en til opplasting.
UMTS er 3. generasjon mobilnett. Dette nettet baserer seg på å kunne sende tekst, digitalisert stemme og video på overføringshastigheter kanskje høyere en 2 Mb/s.
Telenor åpner nettet i henhold til konsesjonsvilkårene i november i år. Deretter fortsetter utbyggingen, og innen desember 2005 skal alle tettsteder i Norge ha full dekning.

2.6 Hva brukes PDA'er til i dag

De fleste bruker PDA'en som en litt avansert filofaks selv om teknologien tillater langt større funksjonalitet. Punktene under viser hva man kan bruke PDA'en til:

- Agenda/kalender
- Kontaktliste
- Huskeliste
- Notatblokk
- Tekstbehandling
- Regneark
- Mobiltelefon WAP
- Tekstmeldinger
- E-post
- Tekstmeldinger
- WAP
- Internett
- Mp3 spiller
- Video avspilling
- Bildevisning
- Digitalkamra
- GPS
- Spill

Flere og flere bedrifter kjøper PDA'er til sine ansatte. Ledelsen ønsker at de ansatte skal være oppdatert på avtaler og hva som skjer i bedriften til en hver tid. De tror også at dette kan være med på å få de ansatte til å trives bedre i bedriften. De ser også viktigheten i å følge med på teknologien. Hvis de ansatte kan bruke enkle filofaks funksjoner, er steget ikke så stort når teknologien går videre og mer krevende oppgaver skal løses ved hjelp av PDA.

2.7 Hvilke faktorer kommer til å bety mest for bruken av PDA i den nærmeste fremtid?

Trenden i markedet viser at det ikke er lenge før de fleste PDA'er har mulighet for å kommunisere ved hjelp av Bluetooth. Det som imidlertid kommer til å forandre bruksområdet til PDA'er mest er høyhastighetsnett. Dette åpner for muligheter som folk for ikke lenge siden bare kunne drømme om.

2.7.1 Bluetooth

Bluetooth er en ny standard for kommunikasjon over korte avstander. Den tar over for mye av det IR har blitt brukt til før. Teknologien går ut på at mikroprosessor-basert radiosendere kommuniserer med hverandre.
Bluetooth versjon 1 kan gi overføringer på 1 M/sek. Versjon 2 kan gi overføringer på 2 M/sek. Rekkevidden for Bluetooth versjon 1 og 2 er på 10 eller 100 meter.

Punktene under viser noe av det man kan oppnå ved bruk av Bluetooth:

- Ved hjelp av Bluetooth blir PDA'en synkronisert med PC'en med en gang man kommer inn på kontoret.
- Er man i et møte, og ønsker å vise noe man har på PDA'en, er det lett å overføre og styre en framviser slik at man kan vise det man har på PDA'en på storskjerm. Hvis man ønsker å skrive ut noe som ligger på PDA'en kan man overføre dokumentet direkte til skriveren.
- Hvis man ønsker å gi et visittkort til en forretningsforbindelse kan man overføre dette mellom PDA'ene ved hjelp av Bluetooth.
- Man kan styre bilporten og husdøren slik at de åpnes automatisk når man står utenfor. Lyset kan styres slik at det slår seg på når man kommer inn i leiligheten.
- Man kan bruke PDA'en som en elektronisk billett. Man kan kjøpe og betale billetter ved hjelp av PDA'en. Når man kommer på flyet, bussen, kino osv er det bare å gå rett inn siden Bluetooth viser billetten.
- Trådløs betaling. Man slipper å betale når man går ut av supermarkedet ol. Det er bare å gå ut siden det er små sendere som er festet på varene som registrerer det du tar med deg. Betalingen skjer ved hjelp av et elektronisk betalingskort.
  (Ericsson samarbeider med Eurocard om ny betalingstjeneste. Ericsson vil i mai sette i gang et prøveprosjekt i Sverige hvor et antall testkunder utstyres med Ericsson telefonen R520 som inneholder Bluetooth og et virtuelt Eurocard. Identifisering skjer via PIN-kode på samme måte som ved vanlig kortbruk.
  Telefonen skal brukes som betalingsmiddel i vanlige butikker [2], nesten på samme måte som betalingskort.
  Det er nærliggende å tro at dette er en betalingsform som kommer til å bli overført til PDA'er.)
- Hvis man er på museum eller i en nasjonalpark, kan man bruke PDA'en som guide, Bluetooth overfører den aktuelle informasjonen til PDA'en når man nærmer seg det man ønsker å se på.
- Når man kommer bort til bilen åpner den seg automatisk, stiller in setet og setter på yndlings radiostasjonen.

Som man kan se ut av punktene over er det i grunnen bare fantasien som setter en stopper for hva man kan utrette ved bruk av Bluetooth og en PDA.

2.7.2 Høyhastighetsnett (UMTS)

I dag kan mangel på minne og prosessorkraft være et stort problem, men når høyhastighetsnettene (UMTS) kommer kan det hende at dette problemet er løst. Isteden for at all data skal lagres og behandles i PDA'en kommer dette til å skje på eksterne servere. Dette er samme trenden som skjer med nettverk. Brukeren kjører tynne klienter som kommuniserer med kraftige servere/databaser. Siden PDA'en bare viser et skjermbilde av de underliggende prosessene som blir kjørt på serveren, trenger ikke PDA'en ha mye minne eller prosessorkraft. Den omfattende utbygningen av mobilnettet har kostet mye så det er sannsynlig å tro at det kan være dyrt å bruke det nye mobilnettet til store dataoverføringer. HyperLAN/2 er definert i den UMTS standarden. Det virker slik at til vanlig er man tilkoplet UMTS men når man kommer innenfor dekningsområdet til et Hyperlan/2 koples PDA'en automatisk over. Hvis man er i nærheten av et åpent W-LAN nett går det også an og kople seg til automatisk. Det er sannsynlig å tro at prisen på overføringer som kommer til å avgjøre hvor mye tynne klient-løsningen kommer til å bli brukt

Høyhastighetsnett gjør at PDA'er kan brukes til:

- Å vise film. En selger kan f.eks. bruke PDA'en til å vise kundeproduktene med tv-kvalitet. (All informasjon ligger på bedriftens servere)
- Å gi tilgang til all slags informasjon som ligger på servere på jobben eller hjemme-PC
- Mulighet for videokonferanse. Hvis en byggingeniør skal vise en arbeider hvordan han skal sette opp f.eks. takstoler, kan dette gjøres ved hjelp videokonferanse på PDA. Dette kan gi store reisebesparelser for bedrifter.

2.7.3 Sikkerhet

I dag lagres all slags informasjon på PDA'en, noe som kan gi store konsekvenser hvis man mister den. Det kreves mye prosessorkraft for å kryptere/dekryptere data siden det må krypteres sterkt. Hvis en uønsket får tak i PDA'en har han god tid til å knekke krypteringen.

Hvis mesteparten av all sensitiv informasjon er lagret på en ekstern server, må fokuset på sikkerhet være:

- **Autentisering.** Det finnes flere metoder man kan bli autentisert på:
  - Pin-Kode.
  - Smartkort
  - Fingeravtrykkskanner
  - Stemmegjenkjenning
- **Tap av PDA som er autentisert.** Ved tap av en PDA, som fremdeles er oppkoplet på nett kan føre med seg store data tap, siden uønskede da har tilgang til den eksterne databasen.
- **Sikker overføring.** I tillegg til at mobilnettet krypterer det som sendes i luften, er det mulig å ha egen kryptering på data som skal sendes, mottakeren dekrypterer. Det trengs ikke brukes en så "tung" kryptering siden det er tidsbegrenset hvor lenge en nøkkel er gjeldene. Hvis en PDA blir mistet så kan man stenge databasen slik at den PDA'en som er kommet bort ikke kan kople seg på.

3 Nettverk

3.1 De mest vanlige sikkerhetsproblemene i et nettverk

De mest vanlige sikkerhetsproblemene i et nettverk er fiendtlige, eller mindre ønskede overtredelser fra brukere eller programmer. Det er forskjellige måter overtredelsene kan skje på. Denne rapporten er begrenset til å kun ta for seg de truslene nettverket kan bli utsatt for gjennom bruk av PDA.

PDA'en kan føre med seg følgende trusler til et nettverk:

1. Virus
2. Worm
3. Trojansk hest

Det er kun sikkerhetsmekanismene i selvet nettverket som kan stoppe disse overtredelsene. Det er ikke bare nettverksbasert angrep som forekommer. En bruker som har brukerkonto og som benytter seg av en lokal terminal kan være smittekilde til noe uønsket uten selv å vite det. Et virus, worm eller en Trojansk hest kan komme inn i nettverket gjennom en diskett. Disketten kan ha blitt smittet når brukeren hentet f.eks. informasjon fra hjemme PC'en. Når dataene på disketten skal overføres til PC'en på jobb, overføres også det uønskede som skjuler seg på disketten.

3.1.1 Virus

Antivirusprodusenten Norman ASA definerer et virus ved følgende kriterier:

- Evnen til å kopiere seg selv inn i andre filer.
- Virus trenger en vert for å spre seg.
- En hendelse som ikke er tilsiktet fra brukers side må inntreffe.

Et virus er noe lik en worm, men et virus er ikke et komplett program. Et virus er en kortere maskinkodedel som kan innpasse seg i andre komplette dataprogrammer og lage kopier av seg selv som innpasses i andre programmer det kommer i kontakt med. Virusene er ofte konstruert slik at de kan tre i aksjon når bestemte hendelser skjer, som at et spesielt (infisert) program kjøres eller en spesiell dag (dato) inntreffer. Virusproblemet ødelegger først og fremst for brukere av personlige datamaskiner.

3.1.2 Worm

De fleste operativsystemene er utstyrt med funksjoner som tillater at en prosess starter en eller flere avkomsprosesser. Med worm mener vi her en ulovlig prosess (et program) i systemet som bruker nettopp denne funksjonen for å redusere eller ødelegge systemets virkemåte. Worm'en skaper en kontinuerlig strøm av avkomsprosesser og søker gjerne å ta over tilgangen til alle ressursene i systemet.
Avkomsprosessene vil hver for seg gjøre det samme. Innen kort tid er all datakraften brukt til å holde worm'ene i virksomhet. I et nettverk er slike worm'er særdeles farlige siden de som regel vil kunne spre seg til alle datamaskiner.

Det har ennå ikke vært noen tilfeller av worm på PDA, men det kan virke som høyst sannsynlig at det kan komme om ikke lenge. Det skjer gjerne ikke på de enkleste operativsystemene slik som Palm, men Pocket PC kan være mer utsatt.

3.1.3 Trojanske hester

En trojansk hest kan i utgangspunktet gjøre hva som helst hvis operativsystemet tillater det. Mange operativsystemer inneholder mekanismer som gjør at programmer eid av noen brukere kan kjøres av andre brukere. Dersom slike dataprogrammer kjører i domener med tilgang, brukerrettigheter og gjennomføringsevner som egentlig er tildelt eieren, vil andre brukere få tilgang der de ikke skulle hatt det. En kodedel som tillater misbruk, eller i seg selv er en form for misbruk, kalles ofte for en trojansk hest.

En PDA har gjerne ikke et så "innviklet" operativsystem at trojanske hester kan virke på dem. Men PDA kan lett være en smittekilde. PDA'en kan på samme måte som en diskett overføre en uønsket trojansk hest fra f.eks. hjemmekontoret til nettverket på jobb.

Sett i sammenheng med nettverks- og PDA-sikkerhet, vil en trojansk hest vanligvis gjøre en av to ting:

- Utføre funksjoner som enten avslører vital og privilegert informasjon om et system eller kompromitterer systemet. Under denne kategorien har man sett eksempler på trojaner som avslører brukernavn, passord eller åpninger i brannmuren. Trojaneren sender informasjonen videre til inntrengeren. Dette gjøres ofte pr. mail, kommunikasjonsprogrammet ICQ, osv. Denne typen trojaner kan sies å ha en penetrerende hensikt.

- Gjemme noen funksjoner som enten avslører vital og privilegert informasjon om et system eller kompromitterer systemet. Denne type trojan kan sies å ha en innsamlede funksjon, og eksempel her kan være en trojan som i det skjulte logger alt som blir skrevet på tastaturet.

Noen trojanske hester gjør begge delene. I tillegg finnes det en tredje type trojansk hest som kun har til hensikt å forårsake skade. Eksempel på slik skade kan være å kryptere eller formatere harddisken.

Trojanske hester skiller seg fra virus ved at de ikke har evnen til å kopiere seg selv inn i andre filer og således spre seg på denne måten. En trojansk hest kan i og for seg inneholde et virus, men ifølge definisjonen er den ikke virus.

3.2 Forskjellige typer sikkerhetsmekanismer for bedriftsnettverk.

Bedrifter bruker forskjellige sikkerhetsmekanismer. De mest vanlige er:

- Brannmur
- Antivirusprogram
- Intrusion Detection Systems (IDS)
- Sikkerhetsarkitektur. Inndeling i soner (f.eks. 2 delt nettverk)
- Rutiner som setter begrensninger for hva som er tillatt

3.2.1 Brannmur

I dag har de fleste bedrifter brannmur. Den brukes for å filtrere ut nettverkstrafikk etter gitte regler. Brannmuren plasseres normalt ved en organisasjons tilkoblingspunkt til det offentlige nettet, og eventuelt ved de interne nettverkssegmenter som skal beskyttes ekstra. All trafikk som skal slippe gjennom blir vurdert opp mot brannmurens "policy-file", og pakker eller adresser som ikke tillates blir slettet. Jo flere protokoller som kan stoppes, desto bedre er det, men mange organisasjoner opererer servere som allmennheten skal ha tilgang til, som f.eks. webservere eller ftpservere. Dermed må en slippe gjennom noe trafikk, og systemet er utsatt for en risiko. Det er vanlig at brannmurer blir utsatt for angrep. Hackere sveiper hele tiden over svære IP-områder etter kjente svakheter på brannmuren til enkeltpersoner og bedrifter.

3.2.2 Antivirus programmer

Antivirusprogram har som hovedoppgave å verne et system mot virus, worm og trojanske hester. Antivirusprogrammer inneholder informasjon om kjente virus, worm og trojanske hester. Slik at når programmet leter/sjekker filer på maskinen, vet den hva den skal lete etter. Hvis det ikke ble laget flere virus, worm og trojanske hester kunne man stolt 100% på antivirusprogrammer. Problemet er at det hele tiden blir laget nye virus, worm og trojanske hester. Først blir viruset laget og så lager antivirusprodusentene antivirusprogrammer som kan verne mot viruset. Derfor er det viktig å oppdatere antivirusprogrammet med jevne mellomrom.

3.2.3 Intrusion Detection Systems (IDS)

IDS er litt i grenseland for hva man kan kalle en sikkerhetsmekanisme, siden den bare overvåker slik at feil i konfigurasjonen etc. kan rettes opp, eller at IDS'en viser at det er nødvendig å installere andre sikkerhetsmekanismer.
Utviklingen innen mobilkommunikasjon som har vært de siste årene har vært så eksplosiv at Internett og andre teknologier har gitt bedrifter og ansatte helt nye muligheter når det gjelder utveksling av informasjon som man for bare få år siden kunne drømme om.
Utbredelsen av Internett, og andre Internett-tjenester som elektronisk post og filoverføring har gjort sitt inntog stort sett overalt: i utdanningsinstitusjoner, næringsliv, statlige institusjoner og private husstander.

At datamaskiner koples sammen i større og større interne nettverk er avgjørende for å effektivisere bedrifter, institusjoner og organisasjoner. Flere og flere privatpersoner anskaffer seg PDA'er, det er til og med bedrifter som kjøper PDA'er til alle ansatte. Som en følge av disse truslene mot nettverket har det de senere årene blitt utviklet en rekke verktøy eller systemer for å oppdage slike innbrudd. Disse systemene kalles med en samlebetegnelse for IDS. Det er viktig å merke seg at IDS ikke er en erstatning for brannmur, men et supplement

3.2.3.1 Forskjellige typer IDS Systemer

Det finnes to hovedtyper IDS; "network based" og "host based" IDS. Hovedforskjellen på disse typene IDS, er hvor de er ment å virke i nettet. "Network based" IDS sjekker (eng. "sniff") nettverkstrafikken, mens "host based" IDS sjekker hver enkelt maskin, eksempelvis en kritisk server. Begge burde brukes slik at brukeren får et godt overblikk over hva som skjer både på nettverket og på servere.

3.2.3.2 Network Intrusion Detection Systems (NIDS)

NIDS overvåker datapakker som går gjennom nettverket og forsøker å oppdage om en hacker el. cracker forsøker å bryte seg inn i et system eller lamme hele eller deler av dette. (Såkalt "Denial of Service angrep"). Et NIDS kjøres på en uavhengig maskin som passivt overvåker all trafikk på nettverket.

3.2.3.3 Host-based Intrusion Detection

Dette er et type system som kjøres på hver enkelte maskin, og som benytter seg av informasjon fra operativsystemet for å overvåke alle operasjoner/hendelser som foregår på maskinen. Disse hendelser sammenliknes så med en predefinert sikkerhetsprofil for å oppdage innbrudd eller overtredelser av rettigheter.

3.2.3.4 System Integrity Verifiers (SIV)

SIV overvåker systemfiler for å oppdage når en inntrenger endrer dem, for eksempel for å etterlate seg en bakdør. Et SIV system kan også overvåke andre komponenter, ved at de leter etter kjente innbruddsignaturer.

3.2.3.5 Log File Monitors (LFM)

LFM overvåker loggfiler generert av nettverkstjenester. På en liknende måte som ved NIDS, analyserer disse systemmønstrene i loggfilene, som kan avsløre en angripende inntrenger. Et typisk eksempel vil være et program som kikker i Webserver loggfiler etter inntrengere som forsøker velkjente sikkerhetshull.

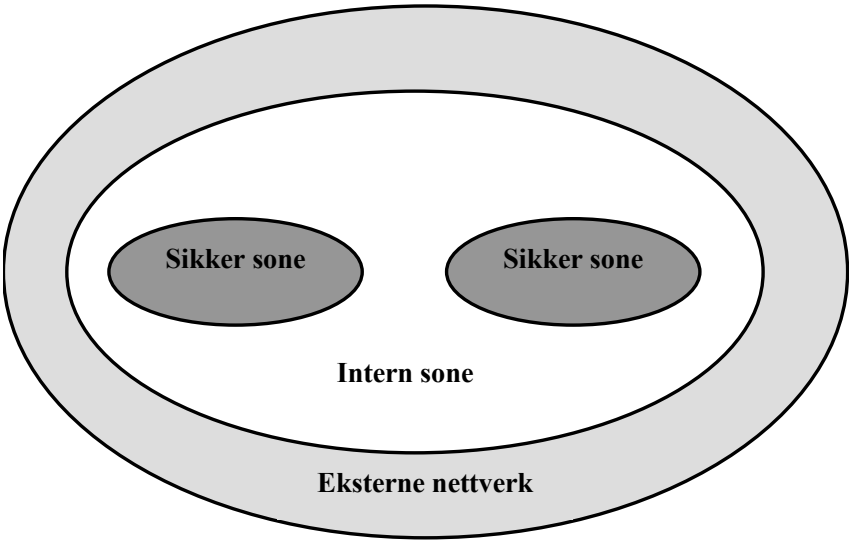
3.2.4 Sikkerhetsarkitektur. Inndeling i soner.

Soner benyttes som et grunnleggende prinsipp i sikkerhetsarkitekturen. En sone er de deler av et informasjonssystem som tillates å kommunisere ved dataoverføring. Soner opprettes etter analyse av behovet for tilgang og dataoverføring. For å begrense tilgangen til sensitiv informasjon kan følgende soner benyttes internt i en bedrift (ref. Figur 12):

- Sikret sone hvor sensitive bedriftshemmeligheter og personopplysninger behandles (ved behov opprettes flere sikrede soner i virksomheten). Den enkelte sikrede sone er sikkerhetsmessig atskilt fra resten av det interne nettverket og eventuelle andre sikrede soner, foruten mot eksterne nettverk.

- Intern sone hvor ikke sensitiv informasjon behandles, denne kan også omfatte andre opplysninger i virksomheten som ikke skal eksponeres eksternt.

Eksterne nettverk som bedriften benytter, men som ikke kontrolleres av virksomheten er tegnet inn på figuren, da interne informasjonssystemer også kan kommunisere med slike.



Figur 12 Soneinndeling

Sikkerhetsarkitekturen skal ivareta følgende:

- Sensitive bedriftopplysninger skal behandles og lagres i sikrede soner hvor kun autoriserte brukere gis tilgang. En bedrift kan opprette flere sikrede soner avhengig av behovet.

- Skillet mellom sikret sone og det intern sone for øvrig skal gjennomføres slik at det ikke er mulig for brukere å overstyre innlagte begrensninger. Det må som minimum være en teknisk sikkerhetsbarriere mellom sikret sone og intern sone.

- Skillet mellom eksterne nettverk og sikret sone skal utgjøres av to tekniske sikkerhetsbarrierer.

- Ingen tjenester skal kunne initieres fra andre soner og inn i sikret sone.

Ved ekstern formidling av sensitive bedriftsopplysninger, samt informasjon om sikring av slike opplysninger må data krypteres.

4 Kjente trusler i forbindelse med bruk av PDA

4.1 Innledning

Pr. 06.05.01 er det bare to kjente trusler for selve PDA'en. Det er et virus(Phage) og en trojansk hest (Liberty).

4.1.1 Virus angrep på PDA

PalmOS/Phage.936 viruset [20] ble funnet 22.09.00. Dette er det første og eneste kjente virus som er oppdaget for noen type PDA. Phage er et virus som ikke er så farlig siden det er lett å oppdage.

Viruset ødelegger ved at det skriver over begynnelsen på Palmens utførelsestabell (executables). Hostfilene blir også ødelagt i prosessen.
Nå Palmens PRC først er infisert, så overfører Palmen viruset til andre Palm programmer helt til alle er infisert og ødelagt.

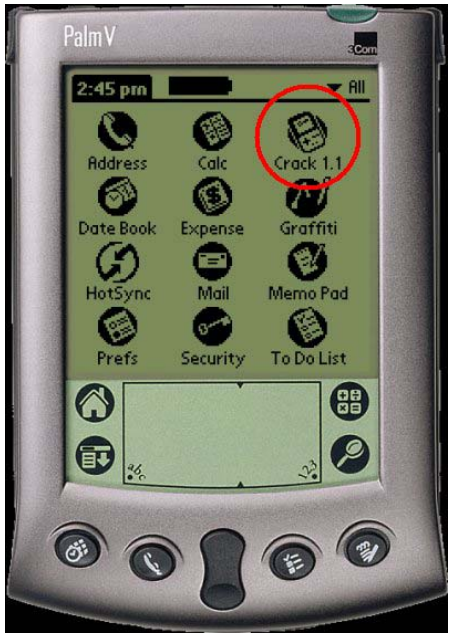
4.1.2 Trojansk hest angrep på PDA

Liberty (Palm) er den første og eneste kjente trojanske hesten som har angrepet en PDA. Den trojanske hesten er på 2,663 bytes, den ble oppdaget 30 August, 2000.

Liberty angriper bare PDA'er som bruker Palm som operativsystem.
Den trojanske hesten gjemte seg under det falske programnavnet: Gameboy emulator 1.1.

Bildet ved siden viser skjermen på en Palm V PDA. Crack 1.1 ikonet viser at "Gameboy" emulatoren er installert, men applikasjonen er enda ikke kjørt.

Når brukeren prøver å starte programmet med å dobbelt - trykke på ikonet. Startes den uønskede applikasjonen som sletter, utførelsestabell (executables) og rebooter maskinen.



Figur 13 Trojansk hest på Palm

4.1.3 En PDA kan være smittebærer av virus, worm eller trojanske hester

Når en PDA synkroniseres eller kommuniserer med andre kan den smitte eller bli smittet av noe uønsket. Grunnen til at et virus kan være farlig for en PC, men ikke en PDA er at de kjører på forskjellig operativsystem. En PDA kan overføre DLL og EXE filer uten å kunne lese dem.
Virusprodusenten McAffe lager antivirusprogrammer for å verne PC'er mot "smitte" fra PDA'er med Palm OS, EPOC og Pocket PC som operativsystem. Dette må bety at alle typer PDA'er kan smitte en PC med virus, worm eller trojanske hester.

4.2 Antivirusprogrammer ved bruk av PDA

4.2.1 Innledning

Alle typer PDA'er kan teoretisk være bærere av virus, worm eller trojanske hester.
I forbindelse med bruk av PDA finnes det to typer antivirusprogrammer, et som beskytter PDA'en og et som sjekker alt som synkroniseres mellom PDA og PC.

De to mest kjente produsentene av antivirusprogrammer er:

- F-Sesure [18]
- Mcafee [19]

Installasjon av antivirusprogrammer er nærmere beskrevet i vedlegg B.

4.2.2 Antivirusprogram som er ment for å beskytte PDA'en

Denne type antivirusprogram installeres på PDA'en. Programmet beskytter PDA'en mot kjente trusler.
Det har kun vært oppdaget angrep på PDA'er som bruker Palm OS. Det finnes flere antivirus produsenter på markedet som leverer denne type program.

Man bør installere denne type program på alle PDA'er som bruker Palm OS. Det er mulig å få kjøpt programmer som er ment å beskytte PDA'er med også andre operativsystemer.
Det er en kjent sak at man må ha et virus før man kan lage et antivirusprogram som kan være effektivt mot viruset. Den eneste fordelen jeg ser med installere å antivirusprogrammer for andre PDA operativsystemer, er at man kan bli oppdatert hvis det skulle komme noen nye trusler.

Teoretisk sett er det ingen grunn for at det ikke kan lages virus ol. som kan angripe PDA'er med andre operativsystem. Derfor er det sannsynlig å tro at det om ikke lenge finnes virus ol. som angriper PDA'er med også andre operativsystemer.

4.2.3 Antivirusprogram som sjekker overføring mellom PC og PDA under synkronisering

Denne typen antivirusprogram lagres på PC'en og brukes for å sjekke alt som sendes mellom PDA og PC under synkronisering. Antivirusprogrammet virker på samme måte som et vanlig antivirusprogram som folk flest er kjent med. Den sjekker alle filene mot kjente trusler.

Dette er et type program som effektivt kan stoppe virus som ellers ville blitt overført under synkronisering. Det virker på samme måte som et vanlig virusprogram for å sjekke innholdet på for eksempel en diskett før filene overføres til maskinen.

4.3 Hvilke trusler og sikkerhetsmekanismer kan man forvente kommer i den nærmest framtiden

Det er sannsynlig å tro at det ene viruset og den ene trojanske hesten som har blitt oppdaget på PDA bare er ”toppen av isfjellet” Hvis man i dag skal installere et program på PDA’en, må dette gjøres via PC. Etter hvert som overføringshastigheten på mobilnettet øker, er det sannsynlig å tro at det vil være mulig å installere programmer direkte fra Internett. PDA’er kommer til å bli mer sårbare etter hvert som de får flere funksjoner og blir mer avanserte.
En av grunnene til at PDA’er ikke har hatt så mange trusler til nå kan være at det er få som har kunnskapen om operativsystemene. Etter hvert som PDA’er blir mer utbrett, kommer det kanskje flere angrep?
Selv om det i dag finnes antivirusprogrammer for PDA’er, er det ikke så mange som benytter seg av dem. Etter hvert som det kommer flere trusler kommer trolig flere til å bruke dem.
Det er ikke mange som vet hvordan IDS kan være med å beskytte en bedrift, tror dette er en overvåkningsmekanisme som kommer til å bli mer vanlig. De å ha muligheten til å observere hva som skjer i bedriftsnettet er viktig for å vite hvilke sikkerhetstiltak som må utføres for å ha et tilfredsstillende sikkert bedriftsnett.

5 Bedriftscase

5.1 Innledning

Utgangspunktet var å analysere en konkret bedrift. Dette ble vanskelig siden rapporten er et offentlig dokument. Bedrifter ønsker ikke at uvedkommende skal vite hvilke sikkerhetsmekanismer som finnes i deres bedrift. Dette er imidlertid ikke et stort problem, siden en tenkt bedriftscase kan kartlegge hvilke sikkerhetstrusler som er tilstede i bedriftens nettverk, like godt som en virkelig case.
Casen er bygget opp på grunnlag av analysen i foregående kapitler.

5.2 Beskrivelse av bedriften

Sønderland AS er en stor bedrift som utvikler og selger XXXX. Bedriften har 3 avdelinger, utvikling, ledelse/økonomi og salgsavdeling. Salgsavdelingen har 40 selgere som reiser rundt i landet for å selge produkter både til bedrifter og privatkunder. Det jobber totalt 200 personer i bedriften. Flere av de ansatte har også hjemmekontor. Bedriften har en viktig samarbeidspartner og en hovedleverandør av råvarer.

5.3 Hvorfor ønsker bedriften bruk av PDA?

Ledelsen i Sønderland AS, ser på hvilke muligheter og besparelser bedriften kunne få hvis de kjøper PDA'er til de ansatte. I utgangspunktet kunne de tenke seg å gi en PDA til alle selgerne, men på sikt ser de for seg at alle ansatte i bedriften skal ha egen PDA.
Punktene under viser noen bruksområder ledelsen kan se for seg at selgerne kan bruke PDA'en til:

- PDA'en kan brukes som en elektronisk filofaks for å lagre avtaler ol. De ansatte kan spare tid på å synkronisere PDA'en med sine stasjonære PC'er.
- PDA'en kan inneholde informasjon slik som tlf, e-postadresse, adresse og kontaktperson osv (kundedatabase).
- PDA'en kan brukes for å finne fram til kunde, kartlesning (muligens med GPS).
- PDA'en kan brukes for å vise produktene fram til kunde:
    - Produktinformasjon
    - Bilder av produktene og små filmer av produktene

Når teknologien tillater det ønsker bedriften å ha en stasjonær produkt/kunde database, der den enkelte selger ved hjelp av raske mobile overføringslinjer kan overføre den informasjonen de trenger til en hver tid. Slik som:

- Avtaler ol.
- Produktinformasjon
- Bilder og små filmer av produktene
- Kundeinformasjon
- Informasjon om de andre selgere. Slik at de vet hvor de er og eventuelt hvilke kunder de har tenkt å besøke
- Bedriften kan på en enkel måte se hvor de ansatte er (GPS overføring). De kan også sende de ansatte den informasjonen de ønsker
- Selgeren kan enkelt sjekke om eventuelle nye kunder har finansiell troverdighet

5.4 Bedriftens nettverk

Alle avdelingene har egne nettverkssegmenter, bedriften har linje mot Internett og fast linje til samarbeidspartner og hovedleverandør. Hjemmekontorene bruker ISDN for å kommunisere med resten av bedriften.

5.4.1 Sikkerhetssoner

De deler av informasjonssystemet som kan kommunisere ved hjelp av dataoverføring kan deles inn i sikkerhetssoner. Sonene opprettes etter analyse av behovet for tilgang og dataoverføring mellom enkelte enheter i informasjonssystemet. Tilgang til sone gis for en enhet identifisert eksempelvis ved hjelp av nettverksadresse.

Sønderland AS er delt opp i 3 ulike sikkerhetssoner (Figur 14):

1. Åpen sone eller demilitarisert sone (DMZ).
2. Intern sone.
3. Sikker sone.

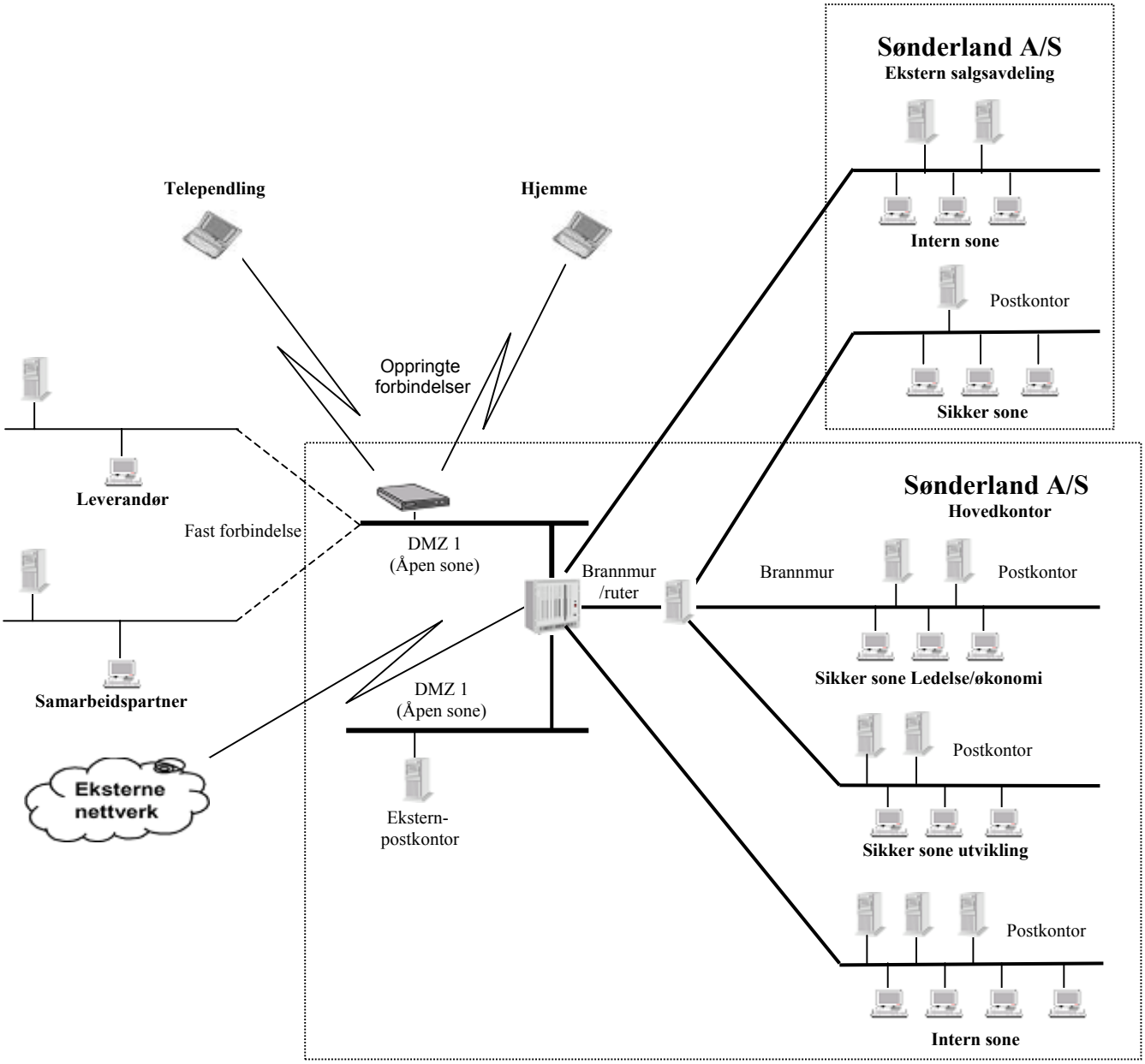
1. Åpen sone . En sone hvor brukere utenfor virksomheten kan gis tilgang, men som er skilt fra virksomhetens øvrige informasjonssystem ved hjelp av sikkerhetsbarrierer. Siden DMZ tillater kontrollerte eksterne forbindelser inn i åpen sone, må den ikke benyttes for tilgang mot Internett eller andre eksterne tjenester som ikke er underlagt virksomhetens sikkerhetsbestemmelser. Hvis noen skal kunne ringe og kople seg på DMZ skal:

- Telefonnummer være forhåndsdefinert. Dette begrenser mulige telefonnummer som kan ringe opp og kople seg på.
- Kjente mobiltelefonnummer tilbakeringes, hvor det er virksomhetens maskin som bryter forbindelsen.
- De som kopler seg på må autentisere seg.

2. Intern sone i Sønderland AS er en sone der de ansatte kan surfe på Internett. Både disketter og vedlegg kan leses, etter at de er sjekket for virus. Det skal ikke være lagret noen informasjon som ikke bør havne i ”uønskedes” hender her.

3. Sikker sone i Sønderland AS er en sikkerhetssone der de ansatte lagrer og jobber med produktutvikling, det er også lagret en del personopplysninger i denne sonen. Det er viktig at ikke uvedkommende får tak i data som ligger her. Det finnes derfor strenge restriksjoner for bruk av disketter, åpning av vedlegg osv. Hvis man får disketter eller vedlegg fra betrodde personer/bedrifter blir de sjekket med antivirusprogrammer.

Skissen under illustrerer bedriftens oppbygning.



Figur 14 Bedriftsnettverk

5.4.2 Hvilke sikkerhetsmekanismer finnes fra før?

Sønderland AS er en bedrift som har samlet behandling av sensitive opplysninger innenfor to fysisk kontrollerte områder (betegnet som Sønderland AS hovedkontor og Sønderland AS salgsavdeling på figur14, forrige side). De stiplede linjene indikerer hva som er innenfor og utenfor bedriftens fysisk kontrollerte lokaler. Sønderland AS har internt nettverk med 3 sikrede soner hvor all behandling og lagring av sensitive opplysninger skjer.

Bedriften har 2 nivåer av brannmurer hvor den indre brannmuren kontrollerer virksomhetens sikre soner, mens den ytre brannmuren kontrollerer alle øvrige eksterne forbindelser, inkludert mottak av ekstern e-post. Argumentet for å benytte to brannmurer er at ved bruk av bare en vil en kompromittering av denne kunne medføre full kompromittering av alle servere.

Tilgang mot eksterne forbindelser (figur 14) er kontrollert og begrenset via den ytre brannmuren. Denne brannmuren kontrollerer følgende soner og funksjoner:

- Tilgang til virksomhetens interne sone.
- Tilgang mot eksterne nettverk (f.eks. Internett).
- En demilitarisert sone (DMZ 1) for mottak og kontroll med bruk av modem for forbindelser mellom virksomheten og hjemmekontor, leverandør og samarbeidspartner. Siden DMZ 1 tillater ekstern tilgang fra kontrollerte eksterne forbindelser og inn i åpen sone, må den ikke benyttes for tilgang mot Internett eller andre eksterne tjenester som ikke er underlagt virksomhetens sikkerhetsbestemmelser.
- En annen demilitarisert sone (DMZ 2) for mottak og formidling av ekstern E- Post. Her står det en web server**.**

E-post som mottas med sensitive opplysninger, dekrypteres, sjekkes for virus og lagres på postkontor som er tilknyttet den aktuelle sikrede sonen. I Sønderland AS er det et postkontor i hver av de sikrede sonene, mens de øvrige interne nettverk har et felles postkontor.

Ekstern salgsavdeling
Salgsavdelingen holder til i et eget lokale, som har samme fysiske kontroll som det hovedkontoret har. Det benyttes faste forbindelser mellom salgsavdeling og hovedkontoret. Salgsavdeling er sikret sone kontrollert av samme brannmur som hovedkontorets sikrede soner, det er ikke behov for å initiere noe fra intern sone inn mot den sikre sonen. Alt som overføres mellom sikret sone i salgsavdelingen og hovedkontoret overføres kryptert gjerne ved bruk av en Viritual Private Network (VPN) løsning.

Hjemmekontoer
Hjemmekontorene koples til DMZ 1. Tilkopling tilfredsstiller følgene krav:

- Forhåndsdefinert valg av telefonnummer for oppringning som begrenser mulige telefonnummer som kan ringes.
- Tilbakeringing hvor det er virksomhetens maskin som bryter forbindelsen.

Telependling
Ekstern tilkopling gjøres via DMZ1. Tilkoplingen på Telependler-siden bruker:

- Forhåndsdefinert valg av telefonnummer for oppringning som begrenser mulige telefonnummer som kan ringes.
- Tilbakeringing til kjente mobiltelefonnummer hvor det er virksomhetens maskin som bryter forbindelsen. Eller bruk av smartkort med kode og engangspassord som identifiserer og autentiserer telependler.

Leverandør
Tilkopling til leverandør og samarbeidspartner skjer via DMZ 1. Tilkobling på leverandør og samarbeidspartner tilfredsstiller følgende:

- Tilbakeringing, hvor det er virksomhetens maskin som bryter forbindelsen
- Bruk av VPN-løsning i kommunikasjonen, slik at forbindelsen kun tillates gjennom krypterte og sterkt autentiserte VPN-klienter.

5.4.3 Vurdering av bedriftens sikkerhet

Sønderland AS har sikret seg med brannmurer og oppdaterte antivirusprogrammer. All informasjon som er viktig, blir det tatt sikkerhetskopi av. Bedriften har opparbeidet seg gode sikkerhetsrutiner. De ansatte må bruke adgangskort for å komme inn i bedriftens lokaler. Alle de ansatte har også egen påloggingsprofil som begrenser hvilke data/sikkerhetssone de har tilgang til. Bedriften har vært plaget av hackere noen ganger, det har vist seg at brannmuren var feil konfigurert. Bedriften har hatt mistanke om at det er utro tjenere blant de ansatte, de har ved flere anledninger oppdaget at hemmelig informasjon har lekket ut av bedriften.

Sikkerhetsløsningene til Sønderland AS er basert på Datatilsynets anbefalinger [21].

5.5 Hva er problemet med innføring av PDA i en bedrift

PDA er en av de nye teknologiene som vokser mest. Flere og flere ser hvilke muligheter som denne lille datamaskinen har. Men det er ikke så mange som ser hvilke nye sikkerhetstrusler som den bringer med seg. I forbindelse med denne oppgaven har jeg brukt mye tid på å søke etter informasjon om ulike sikkerhetstrusler og mottiltak. Det er lett å se at både brukere og produsenter bryr seg mer om brukervennlighet, design og muligheter, enn hvilke skader innføring av en PDA kan medføre. Spesielt bedrifter bør bruke mer tid på å få kartlagt hvilke farer som lurer ved å tillate ukritisk bruk av PDA i samspill med bedriftens eksisterende nettverk.

5.5.1 Hvilke faktorer er med å bestemme risikoen

Punktene under viser faktorer som er med å bestemme risikoen:

- Bedriftens størrelse:
  - Antall ansatte
  - Antall og avstand mellom avdelingene
  - Hvilken type bedriftsnett som benyttes
- Hvilke sikkerhetsmekanismer blir brukt i bedriftsnettverket.
  - Oppdaterte antivirusprogrammer
  - Riktig konfigurerte brannmurer
  - IDS
  - Sikkerhetsrutiner
- Hvilke sikkerhetsmekanismer blir benyttet på PDA'en:
  - Kryptering
  - Autentisering
  - Antivirusprogrammer
- Hvilken informasjon som blir behandlet i bedriften og på PDA'en.
- Hva som er lagret på PDA'en

5.6 Bruk av PDA i et bedriftsnettverk gir en inntrenger to nye måter å bryte seg inn i nettverket

1. En kanal inn i et nettverk
2. En uønsket inntrenger kan tappe PDA'en for informasjon, hvis han får tak i den

5.6.1.1 PDA'er kan brukes som en kanal for å få uønskede ting inn i et nettverk.

PDA'er kan brukes som en kanal for å få uønskede ting inn i et nettverk.
De ansatte tar med seg PDA'en ut av bedriften. Den smittes mens den f.eks. brukes hjemme. Når PDA'en igjen synkroniseres med den stasjonere PC'en på jobb overføres også virus, worm eller trojanske hester. Siden PC'en står i nettverk kan smitten bli overført til hele nettverket.

5.6.1.2 Uønskede kan få informasjonen ut av PDA'en.

Informasjon som ligger i en PDA er ikke sikker hvis en uønsket stjeler eller får tak i PDA'en på annet vis. En bedrift kan risikere å miste sensitiv informasjon som ligger på PDA'en, men også informasjon om hvordan man f.eks. kan komme gjennom brannmuren.
Det er viktig at de ansatte bruker passordbeskyttelse. Selv om informasjonen på PDA'en er passordbeskyttet er den ikke sikker.

Det finnes flere måter å komme rundt passordsperra:

- **Fysiske inngrep.** Det er mulig å åpne PDA'en og fjerne/bytte komponenter slik at man kommer seg rundt sperra. Dette er ganske komplisert og ikke en veldig aktuell måte å få tak på informasjonen, siden det går an å komme rundt sperra på de fleste PDA'er, ved hjelp av enklere metoder.

- **Tappes gjennom seriellkabel.** Det er ikke lett å få oversikt over alle crack programmer som er på markedet. I massemedia er det spesielt Palm som har fått dårlig omtale. Chris Wysopal jobber i firmaet @Stake. Han hevder at hvem som helst med en bærbar PC og en seriellkabel kan komme seg rundt passordsperra, man bruker visstnok en såkalt "bakdør" for å komme seg inn i en PDA, og eventuelt lese det som måtte være der av sensitive informasjon. Bakdøren er tiltenkt program- og applikasjonsutviklere og er tilgjengelig for alle med standard utviklingsprogrammer installert på PC-en sin. Dette sikkerhetshullet er blitt tettet i Palm's nyeste operativsystem, Palm OS 4.0.

- **Tappes gjennom IR.** [3] Firmaet @stake har skrevet et program som heter NotSync, og det kan kommunisere med PalmOS-enhet gjennom IR-porten, mens det gir seg ut for å være ditt HotSync-program. Dette gjør at man ved hjelp av NotSync kan få tak i brukerens passord og få tilgang til brukerens personlige data. Den eneste måten å finne ut om du har blitt hacket på denne måten, er hvis man er svært observant og sjekker når PDA'en ble synkronisert sist, før du setter i gang neste synkronisering.
  I følge @stake kan et program som NotSync lett lages av de fleste hackere, og det gjør at sensitive opplysninger som er lagret på PDA'en lett kan overføres hvis du f.eks. legger PDA'en ned på kafébordet. Firmaet har utviklet et program som løser dette problemet, det ligger ute på @stakes nettsted.

- **Tappes gjennom dockingstasjonen.** Hvis en uønsket har tilgang til dockingstasjonen, og synkroniseringssperren ikke er iverksatt, kan inntrengeren sette en PDA i dockingstasjoen å få maskinen til å synkronisere. Da overføres all den info som sist ble synkronisert med PC'en.

PDA utviklere og hackere driver en stadig kamp. Hackere prøver å finne svakheter ved produktene, og utnytte dem. Mens PDA utviklerne prøver å tette igjen så godt de kan.

5.6.2 Kryptering av sensitiv informasjon som er lagret på PDA'en

Det finnes mange forskjellige krypteringsprogram som kan brukes til å kryptere det som er sensitivt på PDA'en. Det er bare små program som installeres på PDA'en. Det er vanlig at man må ha en krypteringskode for å få dekryptert det man har kryptert.

5.7 Sikkerhetstiltak ved innføring av PDA hos Sønderland A/S

Det er viktig, men vanskelig å få identifisert alle typer sikkerhetsangrep bedriften kan bli utsatt for hvis de tillater de ansatte å bruke PDA. Bedriften foretok en risikoanalyse [5] som var med på å kartlegge hvor de kunne sette in sikkerhetstiltakene.

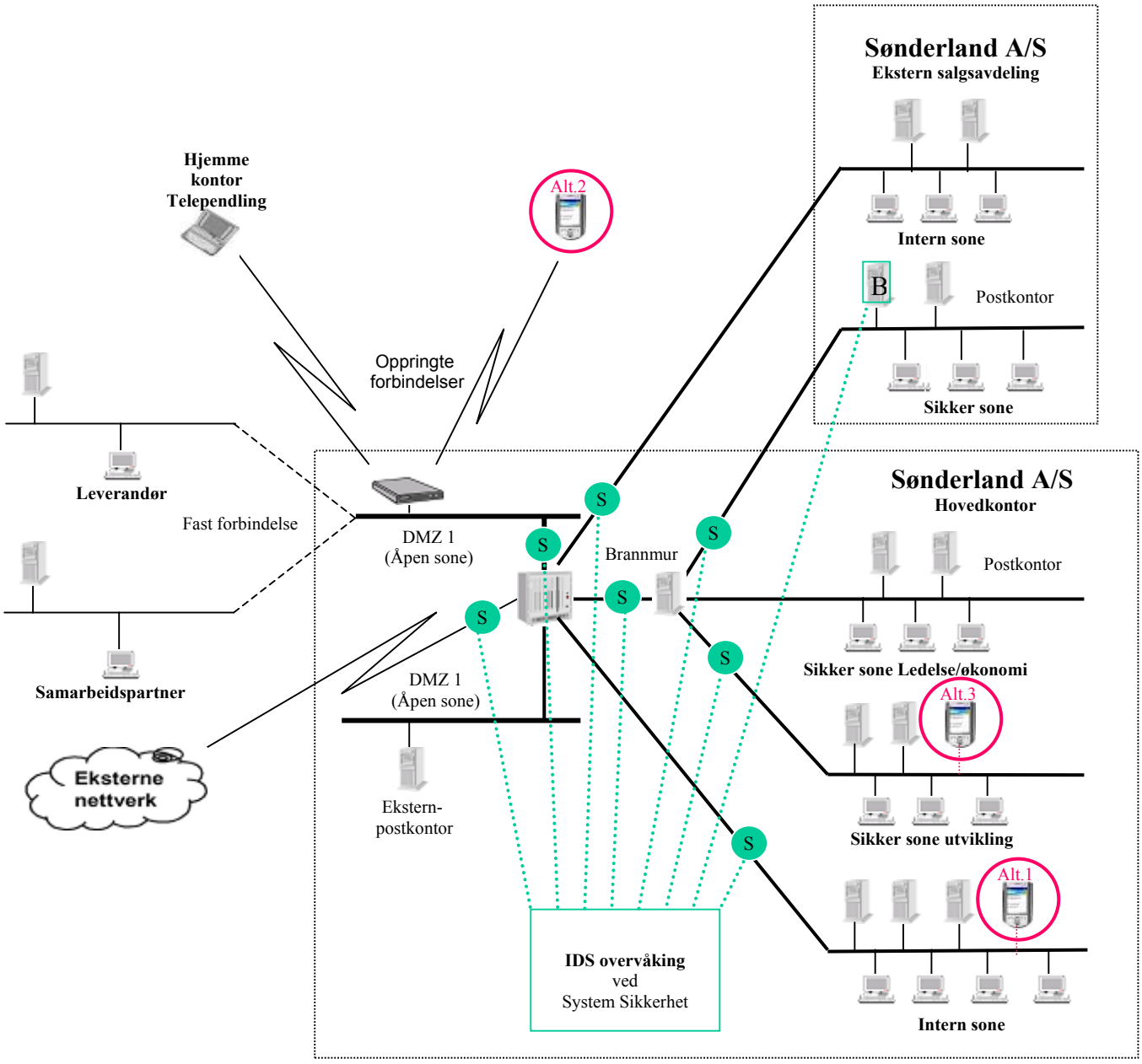
Sønderland A/S gjennomførte en risikoanalyse med følgende faser:

- Planlegging og oppstart.
- Beskrivelse og avgrensing for bruk av PDA.
  - Identifisering av hvor forskjellig type informasjon befinner seg i i bedriftsnettverket.
  - Identifisering av tiltak for sikring av sensitiv informasjon.
- Beskrivelse av trusler mot informasjonssikkerheten mhp.
  - Konfidensialitet.
  - Tilgjengelighet.
  - Integritet.
- Årsaksanalyse dvs. vurdering av hvordan en uønsket hendelse kan inntreffe.
- Konsekvensanalyse dvs. vurdering av de følger en uønsket hendelse kan medføre.
- Frekvensanalyse dvs. vurdering av sannsynlighet for at en uønsket hendelse kan inntreffe.
- Vurdering av sikkerhetstiltak.

Risikoanalysen gav følgende resultat:

- Oversikt over hvilke trusler bedriften står ovenfor.
- Angivelse av sannsynlighet for at en uønsket hendelse kan inntreffe.
- Angivelse av konsekvenser av en uønsket hendelse.
- Resultat fra analyse av sikkerhetstiltakenes effekt i forhold til risiko.

Slik jeg ser det har bedriftsledelsen 3 alternativer for hvordan de ansatte kan kople seg til bedriftsnettet med PDA'ene.
Bildet under viser de forskjellige alternativene:



Figur 15 Bedriftsnett med forskjellige alternativer.

5.8 Hva kan være med på å bedre sikkerheten i bedriften?

5.8.1 Sikkerhetsrutiner

Det er viktig å se på bedriftens sikkerhetsrutiner før man tillater de ansatte å bruke PDA. Man bør se på hvordan de ansatte bruker disketter, åpner post, surfer på nettet eller sikkerhetsfaktorer rundt bruken av hjemmekontorer ol.
Disse faktorene bør være med i vurderingen av om man velger at de ansatte skal kunne bruke PDA. Hvis de ansatte ikke har noen spesielle restriksjoner i f.eks. intern sone, er det ikke noe poeng å lage strenge restriksjoner for bruken av PDA i denne sonen.

Hvis det blir lagret informasjon på PDA'en som er sensitive er det viktig at den blir kryptert. Kapittel 5.6.1.2 beskriver faren ved tap av PDA'en.

5.8.2 IDS

Bedriften har vært utsatt for at brannmuren har vært feilkonfigurert noe som har ført til at uønskede har brutt seg inn i bedriftsnettverket. IDS er et hjelpemiddel som kan være med å oppdage slike feil. Network Based IDS (mer beskrevet i kapittel 3.2.3) kan oppdage om noen uønskede prøver eller har klart å hacke seg gjennom brannmuren eller oppdage unormal trafikk på nettverket. En PDA kan overføre en trojansk hest til nettverket under synkronisering. Den trojanske hesten kan sende viktig informasjon ut av bedriften uten at noen oppdager det. IDS er et nyttig hjelpemiddel for å finne slik uønsket nettverkstrafikk. På figur 15 er IDS systemet tegnet med grønt. Det plasseres ut sensorer som registrerer trafikken på utsatte stedene i bedriftsnettet. På tegningen er disse sensorene tegnet som grønne punkter med en S inni. Siden det er viktige data på post-serveren på sikker avdeling, kan det være lurt å bruke IDS der også. På figur 15 er denne merket med en grønn firkantramme med en B inni. Isteden for å bruke føler, så brukes det host based IDS (nærmere beskrevet i kapittel 3.2.3) som registrerer aktiviteten på serveren.
Siden det trengs spesiell kunnskap for å lese loggene som IDS systemet logger kan denne tjenesten settes bort til System Sikkerhet ASA. Logg info overføres til System Sikkerhets kontor der de blir gjennomgått. Ved unormal trafikk blir det gitt tilbakemelding til bedriften.

5.8.3 Sette signatur på dokumentene.

En av de verste truslene for en bedrift er at hemmelige dokumenter blir sendt ut av bedriften til mottakere som ikke skulle ha hatt dem. Dokumentene kan bli sendt ved en feiltagelse eller at det er noen utrotjenere. Det finnes blant annet metoder for å sjekke at dette ikke skjer [4]. Det er mulig å "merke" dokumenter slik at de blir stoppet hvis de ikke blir sendt til mottakere som er klarert for å motta dem. Det er mulig å lage forskjellige graderinger slik at for eksempel dokumenter til et prosjekt kun kan sendes til de som er involverte.
Dette er en type overvåkning av de ansatte som krever at de ansatte opplyses om at dokumenter som sendes sjekkes.

Bedriften bør sjekke om det også er mulig å bruke denne type mekanisme for å kontrollere at de ansatte ikke overfører sensitive data til PDA'en, eventuelt før dataene er krypterte.

Figur 15 viser 3 alternativer for hvor det kan være hensiktsmessig å kople på en PDA:

5.8.4 Alt 1: Kople PDA'en direkte til en maskin i intern sone

Dette alternativet går ut på at PDA'en skal kunne kommunisere inne i intern sone i bedriften. PDA'er koples på de enkelte ansattes maskiner. En PDA kan som nevnt tidligere i oppgaven, synkroniseres med PC på følgende måter:

- Rs-232
- USB-kabel
- IR

Intern sonen i Sønderland AS er en sone hvor de ansatte kan surfe på Internett og hvor både disketter og vedlegg kan åpnes etter at de er sjekket for virus. Det skal ikke være lagret noen informasjon i denne sonen som "uønskede" ikke må få tak i.
Innføring av PDA i intern sone kan være en ny kanal for virus, worm, trojanske hester eller at data kan bli stjålet eller forandret.

Det er ikke et stort problem at de ansatte kan kople seg på intern sone med PDA'er, siden dette ikke fører med seg en ny type sikkerhetstrussel. Selv om det ikke er krise at man mister data på intern sone, så koster det penger å få nettet opp igjen. Derfor er det viktig med oppdaterte antivirusprogrammer som er beregnet på PDA bruk. Det kan være med på å stoppe de fleste fiendtlige angrep. Rapporten tar i kapittel 4.2.1 for seg forskjellige antivirusprogrammer som skal brukes i forbindelse med bruk av PDA. Vedlegg B tar for seg installasjon av disse programmene.

5.8.5 Alt 2. Kople PDA'en til DMZ 1 ved hjelp av mobiltelefonnettet

Dette alternativet går ut på at PDA'en skal kunne kommunisere med bedriften ved hjelp av mobilnettet. En PDA kommuniserer på følgende måter:

- PDA'en sender dataen til en mobiltelefon ved hjelp av:
  - IR
  - Bluetooth
  - Kabel
- PDA'en kan sende data direkte hvis den har innebygget modem eller at man kan kople til en PCMCIA kort holder. Det finnes flere typer PCMCIA kort som kan kommunisere med mobiltelefonnettet:
  - GSM-kort
  - GPRS-kort
  - Bluetooth-kort (Sender da dataen videre til mobiltelefonen)

Tilkobling hos bedriftsnettet gjøres via DMZ 1. Tilkobling er en type telependling, som bør tilfredsstille følgende:

- Forhåndsdefinert valg av telefonnummer for oppringning som begrenser mulige telefonnummer som kan ringes.
- Tilbakeringing til kjente mobiltelefonnummer, hvor det er virksomhetens maskin som bryter forbindelsen.
- PDA brukeren må autentiseres

Siden DMZ 1 tillater ekstern tilgang fra kontrollerte eksterne forbindelser og inn i åpen sone, må den ikke benyttes for tilgang mot Internett eller andre eksterne tjenester som ikke er underlagt virksomhetens sikkerhetsbestemmelser.

Bruk av PDA gjennom oppringteforbindelser, resulterer i at bedriften får en ny kanal hvor de kan få virus, worm, og trojanske hester inn i bedriftens åpne sone, deretter inn i intern sone og eventuelt inn i sikker sone, hvis bedriften åpner for at de ansatte kan kommunisere forbi den siste brannmuren.
Ved bruk av oppringte forbindelser er det to sikkerhets perspektiv:

- Kommunikasjon mellom PDA og bedrift ved hjelp av mobilnettet, vil indirekte si at man får de samme truslene som man ellers ville fått ved synkronisering av PDA i de ulike sikkerhetssonene:
  - Intern sone. Dette er nærmere beskrevet i alt 1.
  - Sikker sone. Dette er nærmere beskrevet i alt 3.
- Sikker overføring mellom PDA'en og bedriften. Det er viktig at overføringen mellom PDA'en og DMZ 1 skjer på en sikker måte, slik at uønskede ikke kan klare å avlytte eller endre data. I utgangspunktet er overføringen kryptert fra telefonoperatørens side. Men i senere tid har det blitt konstatert at det er mulig å avlytte/endre disse (GSM) overføringene. Det kan derfor være lurt å kryptere data som skal sende og mottas med PDA'en.

5.8.6 Alt 3:Kople PDA'en direkte til en maskin i sikker sone

Dette alternativet går ut på at PDA'en skal kunne kommunisere inne i sikker sone i bedriften. Bedriften bør se på behovet de ansatte har før de lar de ansatte bruke PDA i denne sonen. Alle ansatte har tilgang til intern sone.
En PDA kan, som nevnt tidligere i oppgaven, synkroniseres med PC på følgende måter:

- Rs-232
- USB-kabel
- IR

Sikker sone i Sønderland AS er en sikkerhetssone der de ansatte lagrer og jobber med produktutvikling og hvor det også er lagret en del personopplysninger. Det er viktig at ikke uvedkommende får tak i data som ligger her. Det finnes derfor strenge restriksjoner for bruk av disketter, åpning av vedlegg osv. Hvis man får disketter eller vedlegg fra betrodde personer/bedrifter blir de sjekket med antivirusprogrammer.

Bedriftens sikre sone har ikke blitt smittet av virus ol. Innføring av PDA i sikker sone vil være en ny kanal for virus, worm og trojanske hester.
En innføring kan medføre at data blir mistet, stjålet eller forandret.
Konsekvensene ved at en trojansk hest åpner brannmurene slik at bedriften mister data, kan være veldig store. Derfor er det viktig at alle rutiner og regler holdes slik at de ansatte ikke slippe inn noe "uønsket".

Slik bedriftsnettet er bygget opp bør ikke bedriften tillate de ansatte å bruke PDA inne i sikker sone. Det er ikke nok med gode antivirusprogrammer. Problemet er at PDA'en kan bringe inn trojanske hester som åpner brannmuren fra innsiden.

For at det skal være forsvarlig å bruke PDA inne i sikker sone må det innføres brukerretningslinjer og/eller helst forandre på nettverksstrukturen:

- Brukerretningslinjer. Her er noen punkt man bør vurdere nøye:
  - Hvor PDA'en kan brukes
  - Hva som skal være lov å lagre
  - Hva som må krypteres
  - At alle sikkerhetsfunksjonene er rett konfigurert på PDA'en

- Nettverksstruktur. Hvis man fjerner den fysiske forbindelsen mellom sikker sone og resten av nettverket, kan man være ganske* sikker på at man ikke kan miste data selv om man får trojanske hester inn i nettverket. Forbindelsen er merket med en blå stiplet linje i figur 15.
  All overføring må da skje gjennom diskett, CD eller andre fysiske overføringsmekanismer.
  Selv om nettet er "sikkert" så må man være sikker på at ikke uønskede kan få tak i informasjonen som ligger lagret i PDA'en hvis de ansatte skulle miste den. Dette kan kun gjøres ved å kryptere sensitive data, slik at uønskede ikke får tak i informasjon selv om de får tak i en PDA.

* (Grunnen til at jeg skriver ganske sikker, er at det fremdeles er mulig å plante en trojansk hest i PDA'en. Når PDA'en synkroniseres med nettet i sikker sone (uten fysisk forbindelse til omverdenen) kan den trojanske hesten samle inn informasjon og lagre den i PDA'en. Når PDA'en kommer utenfor sikker sone igjen, sender den informasjonen videre til inntrengeren.)

6 Drøfting av funksjonalitet/sikkerhetsaspekter

6.1 PDA'er

Det er stadig flere som ser hvilke mulighetene en PDA har. Denne trenden viser seg også ellers i verden. I tabell 3 kan man se at tallet på solgte PDA'er i Norge var 32124 i1999, mens det i 2000 ble solgt 76335. Det er mer enn en dobling på et år. Man kan også se at Compaq som nå bruker Pocket PC som OS er den PDA produsenten som stjeler flest markedsandeler. Hvis de rette sikkerhetstiltakene ikke blir iverksatt, kan flere PDA brukere få store problemer i tiden framover.

De mest brukte operativsystemene er; Palm OS, EPOC og Pocket PC/Windows CE.
Palm har per februar 2001 en markedsandel på ca 60 %, men det er ventet at blant annet Microsoft med Pocket PC i større grad kommer til å ta markedsandeler fra Palm OS. Operativsystem er avgjørende for hvilken funksjonalitet en PDA har.
PDA'er som bruker Palm OS er små og brukervennlige. De har små prosessorer og lite minne. De støtter kun enkle programmer. Palm PDA'er ikke mye mer enn en litt avansert elektronisk filofaks. Operativsystemet Pocket PC/Windows CE er en miniutgave av Windows. De inneholder miniutgaver av de mest vanlige Windows programmene. Denne type PDA har forholdsvis store prosessorer og mye minne, det er mulig å vise både film, bilde og spille MP3. PDA'er med EPOC ligger nok et sted midt mellom Palm OS og Pocket PC i funksjonalitet. EPOC har støtte for at flere programmer kan gå samtidig og er et velfungerende operativsystem uten støtte for de tyngste multimedieapplikasjoner. De fleste rene PDA'er som kjører på EPOC operativsystem har tastatur
Noen av de mest kjente mobiltelefonprodusentene; Ericsson, Nokia og Motorola har mobiltelefoner med PDA egenskaper, disse bruker EPOC til operativsystem.

Det er fordeler og ulemper med å ha mobiltelefon og PDA i samme enhet. Det er kjekt med en liten telefon mens en PDA bør ha litt størrelse på skjermen.
Det finnes i dag telefoner som også inneholder PDA funksjoner. De mest kjente er beskrevet i kapittel 2.3.5. Dette er telefoner som er forholdsvis store og tunge. De har ikke den samme funksjonaliteten som en mer avansert ren PDA, har. Dette skyldes at operativsystemet, minne, prosessoren og skjermen er mindre. Men de er fullt brukbare som enkle elektroniske filofakser. Prisen er forholdsvis høy på disse telefonene.
PDA'er med tilleggsutstyr for å lese PCMCIA kort gir mulighet for å ringe. Ved å putte inn et modemkort er det mulig å bruke den som telefon. Dette er ikke noen god løsning siden PDA'en med alt utstyret er forholdsvis stor og tung. Batterikapasiteten er heller ikke så god at man kan ha PDA'en på hele tiden. Dette er også en dyr løsning.

6.2 Sikkerhetstrusler og mulige mottiltak ved bruk av PDA i et nettverk

En PDA, uansett operativsystem, kan smitte en PC med; virus, worm eller trojanske hester under synkronisering. Det har blitt oppdaget et virus og en trojansk hest som angriper PDA'er som bruker Palm OS. En trojansk hest kan åpne en brannmur fra innsiden slik at uønskede kan komme gjennom brannmurer og hente, endre eller ødelegge data.

Det finnes forskjellige måter å håndtere disse nye truslene på. Det er viktig at det blir laget retningslinjer/restriksjoner ved bruk av PDA'er, som er tilpasset den enkelte bedrift. Det finnes forskjellige antivirusprogrammer som sjekker synkroniseringen mellom PDA og PC. Det finnes også antivirusprogram som beskytter mot denne type trusler. Programmet installeres på PDA'en.

Det er vanlig å dele en bedrift inn i flere sikkerhetssoner. Hver sone er deler av et større informasjonssystem som kommuniserer med andre soner eller omverdenen ved hjelp av dataoverføring. Sonene opprettes ut fra behovet de ansatte har for å kommunisere. Målet er å begrense tilgangen til sensitiv informasjon. Det er vanlig å ta backup på viktig informasjon i alle soner, derfor behøver det ikke å ha noen store konsekvenser om virus kommer inn i bedriftens nettverk, og ødelegger data, selv om det koster penger å få nettet opp å gå igjen. Det som derimot er farlig er hvis f.eks. en PDA fører med seg en trojansk hest inn i en sone der det er sensitiv informasjon under synkronisering. En trojansk hest kan åpne en brannmur og sende informasjon ut at bedriften.

Intrusion Detection System (IDS) er en sikkerhetsmekanisme som kan overvåke bedrifters nettverkstrafikk. IDS kan derfor brukes for å finne trojanske hester som har klart å lure seg inn i nettverket ved å analysere trafikkmønstre.

6.3 Hvordan PDA'er kommer til å bli brukt i bedrifter i den nærmeste framtid.

Det er ikke så mange måneder til høyhastighetsnettet (UMTS) kommer i drift.
Dette kan være med å endre bruken av PDA. I dag kan det være et problem at PDA'er har lite minne og prosessorkapasitet. Ved bruk av høyhastighetsnett kan dette problemet være løst. Hvis mesteparten av dataene blir lagret i en database, som kan nås ved hjelp av mobilnettet, er det mulig å kjøre programmene fra serveren. Det er bare skjermbilde og manøvreringsfunksjoner som overføres. Citrin har allerede kommet med en slik "tynn klient" løsning. Hvis all data ligger i en database er det lettere å holde ansatte oppdaterte, selv om de er ute og reiser. Denne løsningen kan også brukes for å holde oversikt over for eksempel hvilke kunder som har blitt besøkt, osv. Sikker autentisering og overføring av informasjon mellom PDA'er og database er viktig, men prosessor krevende kryptering kan gjøres noe enklere. Hvis PDA'en kommer bort er det mulig å sperre PDA'en ute fra databasen. Selv om uønskede klarer å bryte krypteringen på det som er lagret på PDA'en, er det i hovedsak bare autentiseringsopplysninger som mistes.

Det er knyttet usikkerhet til når UMTS nettet kommer. Det kan også ta tid før den mobile enheten kan benytte seg av stor overføringskapasitet. Dette kan skyldes batterikapasitet og det, settes krav til kjøling av den mobile senderen hvis en telefon skal sende mye informasjon.

Utbygningen av det nye mobiltelefonnettet har kostet mye, og det er derfor sannsynlig at overføringer kommer til å prises ganske høyt, iallfall i den første tiden. Det er en ulempe at man må ha en mobilforbindelse for å bruke PDA'en, i mange betongbygninger er det ikke mobildekning. Utviklingen av PDA'er skjer så fort at det er ikke sikkert at prosessor og minnekapasitet kommer til å være et stort problem i framtiden?

7 Konklusjon

Det er sannsynlig å tro at trenden som ses i Norge og andre steder i verden med at det blir solgt flere og flere PDA'er kommer til å forsette. Hvis de rette sikkerhetstiltakene ikke blir iverksatt kan flere PDA-brukere få store problemer i tiden framover.
Det ene viruset og den ene trojanske hesten som har blitt oppdaget på PDA , er bare "toppen av isfjellet". En av grunnene til at PDA'er ikke har hatt så mange trusler til nå kan være at det er "få" som har kunnskap om operativsystemene.

Hvis en PDA brukes utenfor en bedrift kan den bli smittet av virus, worm eller trojanske hester. Noen av truslene er farlige for PDA'en mens andre angriper PC'en som PDA'en synkroniseres med.

Hvis en PDA kommer i hendene på uønskede så er det en risiko for at de kan tappe den for informasjon selv om passordssperren er på. Kryptering er den eneste måten å sikre dataene på. Bedrifter som tillater bruk av PDA bør installere antivirusprogrammer som beskytter både PDA'en og PC'en den synkroniseres med. I dag er det forholdsvis få som benytter seg av slike program, men etter hvert som det dukker opp flere trusler kommer sikkert flere til å se nytten av dem.

Det er ikke mange som vet hvordan IDS kan være med å beskytte et bedriftsnett, men jeg tror dette er en overvåkningsmekanisme som kommer til å bli mer vanlig. IDS er et godt hjelpemiddel for å finne unormal nettverkstrafikk. En PDA kan under synkroniseringen føre med seg en trojansk hest inn i bedriftsnettet, som kan sende informasjon ut av bedriften. Bedrifter som ønsker å innføre PDA'er bør ta en risikoanalyse slik at de kan få laget seg en sikkerhetsagenda som omhandler bruk av PDA.

Det kan være hensiktsmessig å dele et bedriftsnett inn i flere sikkerhetssoner. Hver sone er en del av et større informasjonssystem som kommuniserer med andre soner eller omverdenen ved hjelp av dataoverføring. Sonene bør opprettes ut fra behovet de ansatte har for å kommunisere. Målet er å begrense tilgangen til sensitiv informasjon. Man bør ta backup av viktig informasjon i alle soner. Selv om et virus ødelegger data i en sone, behøver dette ikke å ha noen stor konsekvens, annet enn at det koster penger å få nettet opp å gå igjen. Det som derimot er farlig, er hvis for eksempel en PDA fører med seg en trojansk hest inn i en sone som har sensitiv informasjon. En trojansk hest kan åpne en brannmur og sende data ut av bedriften til uønskede.

Når høyhastighets mobilnettet kommer vil flere bedrifter ønske å utnytte PDA'en på en mer effektiv måte, hvis overføringskostnadene ikke blir for store. Da blir det mulig å overføre dataene som er lagret på PDA'en til en ekstern database der de ansatte ved hjelp av et mobil høyhastighetsnett kan logge seg på og hente dataene etter at de har autentisert seg. PDA'en skal da bare kjøre tynne klienter Denne løsningen vil øke sikkerheten og gjøre PDA'en til et mer effektivt arbeidsverktøy.
En telefon bør være liten og lett mens en PDA bør ha en skjerm som er så stor at den er grei å bruke. Isteden for å ha to enheter er det kanskje enklere og billigere å bruke en enhet som inneholder både PDA- og mobiltelefon- funksjoner. Det finnes i dag slike enheter, men jeg mener de ikke tilfredsstiller det behovet man ellers får dekket med to atskilte enheter. Jeg tror det bare er et tidsspørsmål før det kommer en enhet på markedet som kan klare dette på en tilfredsstillende måte.

8 Referanser

Artikler/dokumenter:

[1] Ynge Bjørlykke; Dagensnæringsliv. 05.03.2001.

[2] Finn Halvoren; Teknisk ukeblad NR.15. 19.04.2001.

[3] Sindre Lia; Infosync. 07.02.2001
http://www.infosync.no/nyheter/visnyhet.asp?Link=633

[4] Datatilsynet; Retningslinjer for informasjonssikkerhet. TR-100:1998.

[5] Datatilsynet; Veiledning i risikoanalyse av informasjonssystem. TV-201:1998

Forskjellige PDA'er og operativsystem:

[6] Michael Morrison; Pocket PC. Forlaget Quepublishing, . ISBN 0-7897-2472-3. 2000. Oversikt over PDA'er som bruker Pocket PC som OS.

[7] Craig Peacock, "Pocket PC clear & simple". Forlaget Digital Press. ISBN 0-7506-7354-0. 2001. Oversikt over PDA'er som bruker Pocket PC som OS.

[8] Nokia; Nokia Communicator 9210 og 9110i. 27.03.2001.
http://www.nokia.no/mobiltelefoner/

[9] Motorola; Oversikt over Motorolas modeller. 02.04.2001.
http://www0.motorola.com/developers/wireless/products/matrix/index.html?view=full&order=desc&sort=avail_ysn

[10] Psion; Oversikt over de forskjellige modellene til Psion. 25.03.2001.
http://www.psion.com/

[11] Ericsson; Ericsson R380 mobiltelefon. 02.04.2001.
http://www.ericsson.no/products/r380.shtml

[12] Palm; Oversikt over de forskjellige Palm modellene. 02.04.2001.
http://www.palm.com/products/

[13] Oversikt over Compaq IPAQ 19.05.2001.
http://athome.compaq.com/showroom/static/iPaq/handheld.asp

[14] Michael Morrison, "Pocket PC". Forlaget Quepublishing, 2000. ISBN 0-7897-2472-3 (Oversikt over Pocket PC)

Microsoft; Forteller om hva en PDA er. 02.04.2001.
http://www.microsoft.com/mobile/pocketpc/pdainfo.asp

[15] Magcom; Norsk PDA Mobiltelefonprodusent. 04.05.2001.
http://www.magcom.no

[16] Symbian; EPOC. 02.04.2001.
http://www.symbian.com/About/investorinfo.html

[17] Epoccity; EPOC, 02.04.2001
http://www.epoccity.com/new/public/ (EPOC)

Pda2day; Oversikt over operativsystemer 02.06.2001.
http://www.pda2day.com/

Idedata; Oversikt over forskjellige PDA'er.02.04.2001.
http://www.idedata.no/

Sikkerhet/virus referanser

[18] F-secure; Forskjellige antivirusprogrammer. 03.06.2001.
http://www.f-secure.com/wireless/palm/

[19] McAffe; Forskjellige antivirus programmer. 04.04.2001.
http://www.mcafee.com/wireless/default.asp

[20] F-Secure; Beskrivelse av det første PDA viruset på Palm. 03.06.2001.
http://www.europe.f-secure.com/v-descs/phage.shtml

[21] Datatilsynet; Veiledning kommuner. TV-202:1999. 17.04.2001
http://www.datatilsynet.no/infosik/veiledn/kommune/Kommuneveiledning.pdf

Vedlegg A *Oversikt over hvordan PDA'er kan kommunisere:*

1. Rs-232 og USB

Rs-232/USB brukes til å overføre informasjon mellom to enheter. Brukes blant annet til å synkronisere informasjon mellom PDA og PC. USB kabel erstatter serie kabel og er en mye sikrere og raskere måte å overføre data på.

2. IR og Bluetooth

IR (eng. Infra Red) og Bluetooth er teknologier som i hovedsak brukes for kommunisere trådløs mellom PDA og mobil eller PDA og PC/laptop. De fleste PDA'er er i dag utstyrt med IR. Teknologien går ut på at man overfører data med hjelp av lys. Siden lys er retningsbestemt er det begrenset hvordan PDA'er kan kommunisere med andre. Det er viktig at lyssender og lysmottaker har fri sikt til hverandre.
PDA'er med IR gir også andre muligheter. Flere nye skrivere har IR mottaker, dette gjør det mulig å sende det som ligger på PDA direkte til skriver.
PDA'er med IR kan også brukes som fjernkontroll. Det ligger gratis programmer på Internett som gjør det mulig å lagre fjernkontroll funksjoner i PDA'en.
IR er en forholdsvis gammel teknologi. Det er mye som tyder på at Bluetooth mer og mer kommer til å ta over. Dette er en teknologi som er mer anvendelig siden det er radiosignaler som sendes, isteden for lys. PDA'er har ikke foreløpig innebygd Bluetooth, men det er bare et tidsspørsmål. Men det er mulig å få kjøpt det som tilleggsutstyr til noen PDA'er. Til Compaq kan man få kjøpt PCMCIA kort med Bluetooth.
Bluetooth er cirka fire år gammel. Det var Ericsson som henvendte seg til IBM, Nokia, Intel og Toshiba, med ideen om at enhver elektronisk maskin skulle kunne kommunisere med enhver annen maskin ved hjelp av en mikroprosessorbasert radiosender. Siden har hele industrien kastet seg over dette; nær sagt alt som kan krype og gå innen data, tele og forbrukerelektronikk arbeider for å utvikle en felles standard.
Enheten bruker det tidligere ubrukte 2,45 GHz båndet som er globalt tilgjengelig med enkelte variasjoner i båndbredden i enkelte land
Maksimal rekkevidde for Bluetooth er 10 meter, og data kan utveksles med 1Mbit pr sekund i versjon en og opp til 100meter med 2Mbit i versjon to.
(ref. http://bluetooth.ericsson.se/bluetooth/ www.bluetooth.com)

3. Wireless LAN og HiperLAN/2

Wireless LAN og HiperLAN/2 (High Performance Radio Local Area Network type 2) er teknologier som brukes for trådløsoverføring. HiperLAN/2 er en videreføring av Wireless LAN. Hovedforskjellen er at den sender på en litt annen måte, slik at overføringen kan gå raskere og sikrere. Kan brukes for å kople maskiner sammen i et radio basert nettverk. IEEE 802.11 er standard for trådløse nettverk. Selv om utstyr er levert av forskjellige leverandører er dette ikke noe problem å kople sammen, så lenge det støtter den felles standen.

Man får ikke kjøpt PDA'er med innebygd Wireless LAN/HiperLAN/2. Men man får PCMCIA kort som har det. Det blir mer og mer vanlig at man kan kjøpe tilleggsutstyr til PDA'en slik at det er mulig å bruke disse kortene.

4. GSM og GPRS

GSM (Global System for Mobile communication) og GPRS (General Packet Radio Service) er overføringsmetoder som ligger i mobiltelefoner. Hvis man i dag ønsker å kommunisere med f.eks. Internett. Da oppretter man først kontakt mellom PDA'en og Mobiltelefonen, gjennom IR, Bluetooth eller kabel. Derfra går kommunikasjonen ved hjelp av GSM eller GPRS.

For å kunne oppnå høyere ytelse blir det i GPRS benyttet pakkesvitsjet overføring. En metode som på en dynamisk og fleksibel måte deler de tilgjengelige ressursene med andre GSM tjenester. For å kunne overføre data ved høyere hastighet blir det brukt flere tidsluker i stedet for en tidsluke per mobilstasjon som dagens GSM gjør. Antall tidsluker som blir benyttet blir regulert dynamisk ut i fra trafikkmengde, ledig kapasitet, og hva slags tjeneste brukeren ønsker og er villig til å betale for. Med GPRS kan en oppnå hastigheter opp mot 115kb/s, i motsetning til dagens tjeneste i GSM hvor en kun har linjesvitsjet dataoverføring med ytelse på 9,6kbit/s.

Det finnes i dag GSM PCMCIA kort og man kan forvente at det ikke er lenge før det også går an å skaffe GPRS PCMCIA kort. Ved bruk av slike kort kan kommunikasjonen gå direkte fra PCMCIA kortet som er festet på PDA'en til Internett via mobiltelefon/GPRS/GSM modul (Ref. Jian Cai David J. Goodman, Rugers University:
General Packed Service in GSM, IEEE Communications MagaZine Page 122-131 Oktober 1997)

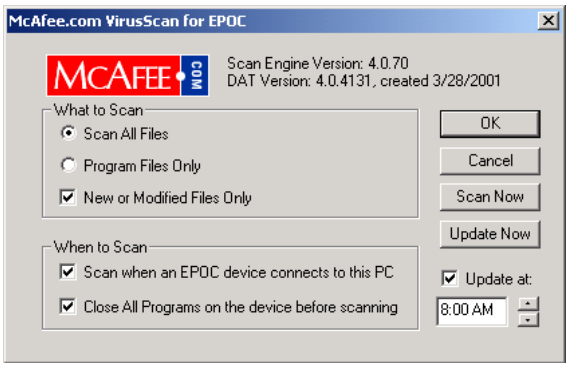
Vedlegg B *Installasjon av antivirusprogrammer*

Virusprogram er et av de beste virkemidlene man har for å bekjempe virus, worm og trojanske hester. Rapporten tar for seg installasjon av virusprogrammer for de 3 mest vanlige operativsystemene. Det var ingen mulighet for å teste om virusprogrammene virkelig virker, til det trenger man et virus. Tabellen under viser de tre PDA'ene og hvilke operativsystem de benytter. Det ble valgte å bruke antivirusprogram som er levert av McAffe.

Forskjellige PDA'er	Operativsystem
Psion Series 5	EPOC
Compaq IPAQ	Pocket PC
Palm VX	Palm OS

1. Installasjon av antivirusprogram på Psion Series 5

McAffe Scan Engine er et antivirusprogrammet er lagd får å sjekke overføringen mellom PDA'er som bruker EPOC som operativsystem, og PC.
Bildet under viser skjermbildet, som kommer opp når man har installert og kjører virus programmet.



Antivirusprogrammet gir forskjellige valg. Man stiller programmet inn for hvordan man ønsker det skal lete etter virus. Det er i hovedsak 3 måter:

- Skanne alle filene på PDA'en.
- Skanne programfilene
- Skanne kun nye eller modifiserte filer

Antivirusprogrammet oppdaterer seg selv automatisk hvis man ønsker det. Hvis programmet skal virke som ønsket er det viktig at det kan stå imot de nyeste virusene ol.

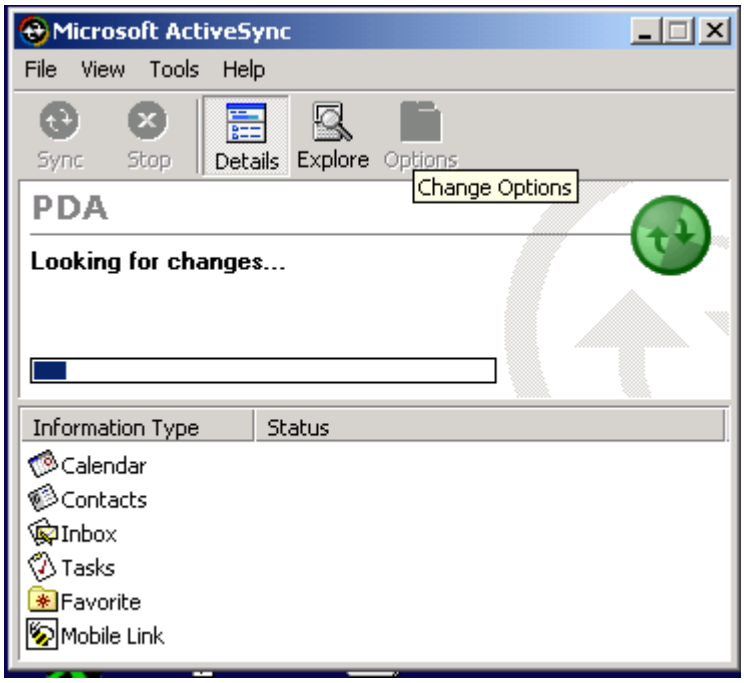
Antivirusprogrammet aktiviseres hver gang PC og PDA synkroniseres. Programmet verner mot:

- Virus under synkroniseringen.
- Trådløse transaksjoner
- Infrarøde overføringer

Dette program verner kun PC og nettverket den er tilkoplet. Hvis det dukker opp virus ol. som er skadelige for PDA'er med EPOC som operativsystem, bør det også installeres antivirus program som kan verne PDA'en den mot angrepene.

2. Installasjon av antivirusprogram på Compaq IPAQ

McAffe har et antivirusprogram som skal verne PDA'er med Pocket PC som operativsystem. Når man kjøper programmet for ca $25 får man gratis oppdatering i et år. Når man har lastet ned programmet, går installasjon av seg selv.
Hver gang man synkroniserer IPAQ'en med PC, kommer framene som er vist under opp. Framen til venstre viser vanlig synkronisering, mens framen til høyre viser at antivirusprogrammet virker som det skal.



Dette program verner kun PC og nettverket den er tilkoplet. Hvis det dukker opp virus ol. som er skadelige for PDA'er med Pocket PC som operativsystem bør det også installeres antivirus program som kan verne PDA'en mot angrepene.

3. Installasjon av antivirusprogram på Palm Vx

Det bør installeres to typer antivirusprogrammer på PDA'er som bruker Palm OS. Et for å verne PDA'en og et for å verne PC'en den blir synkronisert med.
Installasjonen av antivirusprogrammene gjøres på samme måte som alle andre programmer. Det ene antivirusprogrammet brukes for å verne PC'en under synkronisering. Programmet starter installasjonen av seg selv, etter at det var blitt lastet ned.

Kjente produsenter av antivirusprogrammer for PDA
Det finnes i dag flere produsenter av antivirus programmer som også er beregnet for PDA. Noen av de mest vanlige er:

http://www.f-secure.com/wireless
http://www.mcafee.com/wireless