Den Sikre Mobile Medarbejder

Kenny Magnusson

Kongens Lyngby 2007
IMM-THESIS-2007-105

Technical University of Denmark
Informatics and Mathematical Modelling
Building 321, DK-2800 Kongens Lyngby, Denmark
Phone +45 45253351, Fax +45 45882673
reception@imm.dtu.dk
www.imm.dtu.dk

Abstract

The modern business trend is for employees to use a variety of mobile devices to assist them in a wide spectrum of activities. A typical executive, salesperson or engineer may, for example, travel round with a laptop PC, a PDA and a mobile smartphone, all of which may contain information that is important, perhaps even vital, for his or her company. These devices may be extensively used outside the company premises, for example at home, in conference rooms, at the airport, in hotels and so on - locations where security is not under the company's control and may be very poor.

In this thesis, the situation above has been analyzed by evaluating the security risks associated with employees whose work involves a degree of mobility. The thesis also involves an investigation of the level of security awareness among employees of a concrete company, evaluating the security risks which this form of working creates and making proposals for how the company can mitigate these security risks. As a part of this investigation, an internet-based survey regarding the use of wireless networks has been developed. The survey is designed as a combination of normal text-based questions and animated pictures which allows the respondents to interact on known scenarios and hopefully get a better understanding of the question even though it might be of a complex technological matter.

Resume

Det bliver i dag mere og mere almindeligt for virksomheder at udstyre deres medarbejdere med en række forskellige mobile apparater til at hjælpe dem med et bredt spektrum af aktiviteter. En typisk leder, salgsperson eller ingeniør kan for eksempel rejse rundt med en laptop, en PDA og en smartphone, der alle kan indeholde informationer som er vigtige, eller måske endda vitale for vedkomnes virksomhed. Disse apparater kan i stor udstrækning benyttes udenfor virksomhedens lokaliteter, for eksempel hjemme, i konferencerum, i lufthavnen, på hoteller osv. - alle steder hvor sikkerheden ikke er under virksomhedens kontrol og kan være ganske dårlig.

I denne afhandling analyseres denne situation ved at se på en række af de sikkerhedsproblemer der er forbundet med medarbejdere hvis arbejde involvere en hvis grad af mobilitet. Afhandlingen involverer også en undersøgelse af sikkerhedsbevidstheden blandt medarbejdere fra en konkret virksomhed, en evaluering af de sikkerhedsproblemer som opstår ved denne form for arbejde, samt udarbejder forslag til hvordan virksomheden kan undgå disse sikkerhedsproblemer. Som en del af undersøgelsen er der udarbejdet et internetbaseret spørgeskema omhandlende brugen af trådløst netværk. Spørgeskemaet er designet som en kombination af almindelige tekstbaserede spørgsmål og animerede billeder så svarpersonerne på mange af de mere komplekse teknologiske begreber får opstillet et velkendt scenarie og dermed sikre en forhåbentlig forøget forståelse af spørgsmålet.

Forord

Dette projekt er udført som afsluttende eksamensprojekt på civilingeniørstudiet på Danmarks Tekniske Universitet. Projektet er udført ved instituttet Informatik og Matematisk Modellering under vejledning af Robin Sharp. Projektet er udført i perioden mellem 1.Juni og 1.December 2007.

Jeg vil gerne rette en tak til Robin Sharp der i forbindelse med udarbejdelsen af dette projekt har været meget åben og hjælpsom.
Jeg vil også gerne rette en tak til de personer i virksomheden som jeg har haft kontakt med. Både til dem der har svaret på spørgeskemaet og til dem der har kunnet svare på spørgsmål af mere teknisk karakter.
Til sidst en stor tak til familie og venner for støtte og korrekturlæsning på rapporten.

Lyngby, December 2007
Kenny Magnusson

Indhold

Kapitel 1

Indledning

1.1 Motivation

At arbejde hjemmefra eller fra en anden lokalitet uden for virksomheden er i dag en stor del af hverdagen for mange mennesker. Den fortsatte stigende brug af IT systemer har ændret den måde vi opbevare, tilgår og kommunikere informationer. For mange mennesker er computeren og/eller mobiltelefonen i dag det vigtigste redskab i forbindelse med arbejdet og det er derfor også vigtigt at både virksomheden og medarbejderen kender de sikkerhedsmæssige risici der er forbundet med brugen af det mobile udstyr.

Det mobile udstyr som en medarbejder kan benytte sig af er i dette projekt defineret som en laptop (bærbar PC) og/eller en mobiltelefon med samme funktionaltitet som en smartphone. En sådan mobiltelefon er kendetegnet ved at være fysisk mindre og være mindre resourcekrævende end en laptop men ofte med de samme funktionaliteter. Derfor er det væsentligt at de begge som udgangspunkt bliver betragtet ens sikkerhedsmæssigt.

I forbindelse med mobile medarbejdere er udfordringen at få udstyret sikret så samme høje niveau af sikkerhed opnås, som på virksomheden øvrige udstyr. Da den mobile medarbejders udstyr ofte anvendes udenfor virksomheden, er den sjældent sikret fysisk på samme måde som stationære arbejdspladser i virksom-

heden. Den mobile medarbejder skal også have mulighed for på en sikker måde at kunne koble sig op på virksomhedens netværk også fra steder der ligger uden for virksomhedens kontrol.

Udover at udstyret skal være sikret, vil en øget sikkerhedsbevidsthed hos medarbejdere også kunne forhindre eller mindske risikoen for både eksterne og interne trusler mod virksomheden. Sikkerhedsbevidsthed, eller på engelsk 'Security Awareness', er en betegnelse for hvad man forstår ved sikkerhed og hvor højt man prioriterer det.

At fastlægge et niveau inden for IT sikkerhedsbevidsthed er ofte forbundet med nogen usikkerhed. For emner inden for IT er ofte komplekse teknologiske begreber og det kan være svært at afgøre om en person i en brugerundersøgelse, eksempelvis via spørgeskemaer, rent faktisk har forstået meningen med et spørgsmål.

At indbygge grafiske elementer i spørgeskemaerne kunne være en løsning. Det kunne eksempelvis være som animationer, interaktive billeder osv, alle elementer der vil opstille et velkendt scenarie for svarpersonen.

Fordelen ved at lave sikkerhedsbevidstheds kampagner i en virksomhed er, at her kan ledelsen påtvinge alle medarbejdere at deltage.

1.2 Problemformulering

Det primære formål med IT-sikkerhed er at sikre virksomhedens aktiver. Dette indebærer tre vigtige grundelementer - fortrolighed, integritet og tilgængelighed. Fortrolighed skal sikre, at aktiverne kun er tilgængelige for autoriserede personer. Integriteten sikrer, at et aktiv er hvad det ser ud til og ikke er ændret eller mangelfuldt. Til sidst skal tilgængelighed sikre, at aktivet er tilgængeligt når der er behov for det.[9]

Formålet med dette projekt er dels at analysere situationen, hvor en medarbejder i en virksomhed kan arbejde på en sikker og fortrolig måde udenfor virksomhedens lokaliteter, set fra den synsvinkel, at kunne tilbyde tilstrækkelige faciliteter på en sikker måde til de medarbejdere hvis arbejde involvere en hvis grad af mobilitet, samt sikre at medarbejderne er bevidste omkring de tilhørende risici.

Projektet udføres i samarbejde med en større virksomhed der stiller medarbejdere til rådighed, dels til at kunne spørgeskemaet men også til at kunne svare på spørgsmål omkring udformningen af eksempelvis fjernadgangsløsning og på hvilket grundlag de valgte løsninger i virksomheden bliver truffet.

For at kunne lave en vurdering af de risici der er forbundet med mobile medarbejdere, og det at opretholde et tilstrækkeligt højt sikkerhedsniveau i virksomheden, kræver det både dækkende informationssikkerhedspolitikker samt løbende foretaget risikoanalyser. Derfor gennemgåes hvordan udformningen af henholds-

vis risikoanalyse og informationssikkerhedspolitik for mobile medarbejdere, kan laves.

En række af de sikkerhedsproblemer, som etableringen af mobile medarbejdere kan medfører, skal også gennemgåes. Til mange af sikkerhedsproblemerne er givet forslag til hvordan disse afhjælpes. Relevante teknologier som VPN, firewalls, m.m. er også gennemgået. Dette er gjort som motivation for at kunne udarbejde en vurdering af virksomheden samt komme med forslag til forbedringer.

Næsten alle virksomheder er i dag så godt beskyttet, af netop VPN løsninger, firewalls, antivirus programmer, osv., at trusler udefra menes at udgøre en væsentlig mindre risiko end interne trusler fra medarbejdere og tidligere medarbejdere. Ofte ved medarbejderen måske slet ikke at hans/hendes adfærd udgør en reel trussel mod virksomheden. Virksomheder kan derfor med fordel forsøge at øge bevidstheden hos sine medarbejdere så mange af de interne trusler minimeres eller helt undgås. Udfordringen ligger i, for virksomheder, at lave sikkerhedsbevidstheds kampagner, programmer, brugerundersøgelser osv. så simple og enkle at forstå, trods det til tider omhandler komplekse teknologiske begreber, at budskabet går klart ind hos medarbejderen.
Der vil i projektet blive gennemgået eksempler på hvordan sikkerhedsbevidsthed programmer kan udformes.

Der vil i denne sammenhæng også udarbejdes et internetbaseret spørgeskema, der forsøger at kombinere almindelige tekstbaserede spørgsmål med interaktive animationer hvorved svarpersonen bliver udsat for et velkendt scenarie og derved gerne skulle forøge forståelsen af spørgsmålet, trods det at spørgsmålet kan omhandle et komplekst teknologisk begreb. Målet med dette spørgeskema er at fastlægge et sikkerhedsbevidstheds niveau hos medarbejderne.

1.3 Rapport struktur

Denne rapports struktur er som følger

Kapitel 2: beskriver hvordan man i henhold til (D)ansk (S)tandard,
DS 484:2005, kan udforme en risikoanalyse i en virksomhed. Kapitlet kommer med relevante forslag til risici der bør undersøges i forhold til mobile medarbejdere og deres udstyr. På baggrund af indledende risikoanalyse kan en informationssikkerhedspolitik udformes.

Kapitel 3: beskriver hvordan man i henhold til DS 484:2005 kan udforme en sikkerhedspolitik. Kapitlet giver eksempel på punkter der er relevante at få med i en informationssikkerhedspolitik i forbindelse med mobile medarbejdere, udstyr og opkobling til virksomhedens netværk. Sammen med kapitel 2 danner dette kapitel grundlaget for hvor niveauet af sikkerhed lægges i en virksomhed.

Kapitel 4: beskriver nogle af de sikkerhedsproblemer der er i forbindelse med mobile medarbejdere. Herunder generelle problemer(fysisk sikkerhed, password, social engineering, og phishing), problemer ved trådløse teknologier(Trådløst LAN) samt de mest udbredte teknologier(VPN, Autentificering, Kryptering, Firewall, osv.). Kapitlet danner grundlaget for den endelige vurdering af virksomheden.

Kapitel 5: I dette kapitel gives en vurdering af virksomhedens sikkerhedsniveau. Grundlaget herfor bygger på de foregående kapitler samt interviews af væsentlige personer i virksomheden.

Kapitel 6: beskriver lidt om vigtigheden af sikkerhedsbevidsthed samt hvilke muligheder for tiltag der er.

Kapitel 7: beskriver udviklingen af det internetbaserede spørgeskema samt de tilhørende resultater.

Kapitel 8: indeholder projektets konklusion. Kapitlet rundes af med en perspektivering, hvor der gives bud på fremtidig udvikling og viderudvikling af metoder til sikkerhedsbevidstheds brugerundersøgelser.

Mange af de anvendte fagudtryk og forkotelser i rapporten er forklaret i ordbogen der findes i appendix A.

I rapporten benyttes opløftede tal ([1]) som henviser til fodnoter, der vises nederst på siden. Tal i kantede paranteser [1] er kildehenvisninger til litteraturlisten bagerst i rapporten.

1.4 Beskrivelse af virksomheden

I dette afsnit gives en kort beskrivelse af virksomheden som projektet er udført i samarbejde med. Herunder lidt om virksomheden generelt, hvilken type personer der er konfereret med og lidt om situationen i virksomheden i forbindelse med mobile medarbejdere.

Generelt

Virksomheden er involveret i områder som udvikling, salg, marketing og rådgivning. Der er tale om en større international virksomhed der på verdensplan har mere end 10.000 ansatte primært i de nordiske lande.

Alle virksomhedens arbejdsstationer er Windows-baserede og ved udgangen af 2007 skulle alle gerne benytte Windows XP som operativ system.

[1] fodnote

Informationer om virksomheden er fået på baggrund af samtaler med forskellige væsentlige personer i virksomheden. Alle personer har en eller anden tilknytning til de mobile løsninger. Der har i forløbet været kontakt med virksomhedens IT-sikkerhedschef, forskellige IT udviklere og arkitekter som alle har haft en forbindelse til udviklingen af de sikkerhedsmæssige løsninger i forhold til mobile medarbejderes udstyr. Det er netop typisk udviklere og så sælgerne der benytter sig af mobile løsninger, det er også fra den målgruppe at besvarelserne på spørgeskemaet er kommet.

Virksomheden har ønsket at optræde anonymt i denne afhandling - hvilket naturligvis respekteres - og derfor er nogle af de specifikke tekniske løsninger i forbindelse med vurderingen af virksomheden, eksempelvis ved fjernadgang løsningen, udeladt eller kun meget overordnet beskrevet. Der vil f.eks. ikke blive nævnt hvilke porte firewall'en tillader eller blokerer, eller navn og model nummer på laptop's, VPN koncentrator, osv.

En mere teknisk beskrivelse af virksomheden findes i kapitel 5

Kapitel 2

Risikoanalyse

Dette kapitel giver en overordnet beskrivelse af hhv. risikoanalyse og risikovurdering. Risikoanalysen danner grundlaget for udarbejdelsen en risikovurdering. Risikovurderingen kan opfattes som et filter, som ordner information om sårbarheder efter, hvor kritisk sårbarheden er, og som giver ledelsen et grundlag for prioritering af indsatsen. Fremgangsmåden i denne risikoanalyse er bygget op i henhold til eksemplet fra DS484:2005, Anneks B [26], og er lavet for området omkring virksomheders brug af mobile medarbejdere og fjernadgang til virksomhedsnetværket. En risikoanalyse er en vigtig del af det samlede sikkerhedsoverblik, og den er samtidig med til på en let og overskuelig måde, at belyse den eller de mest kritiske risici der bør sættes ind overfor.

2.1 Risikoanalyse

I en risikoanalyse indgår en listning af potentielle trusler forbundet med virksomhedens anvendelse af IT, et estimat af konsekvenserne af uønskede hændelser samt en vurdering af sandsynligheden for forekomst af sådanne hændelser, og en angivelse af hvor sårbare de indgående IT ressourcer er.

Fremgangsmåden kan inddeles i følgende 6 trin:

Tabel 2.1: Fremgangsmåde

Trin	Aktivitet	Beskrivelse
1	Trusselliste	Der opstilles her en liste over alle sikkerhedstruende hændelser, der er forekommet eller kan tænkes at forekomme. Listen nummereres og grupperes under en række hovedoverskrifter.
2	Sandsynlighed og konsekvens	Ovennævnte trusselliste gennemgås, og der påføres en sandsynlighedsvurdering samt en vurdering af mulige forretningsmæssige konsekvenser. De mindst væsentlige elementer i listen, altså dem med lav sandsynlighed og lav konsekvens, kan elimineres. De resterende elementer skal beskrives så konkrete, at den forretningsmæssige konsekvens af sikkerhedsbristen vil være klar og tydelig for ledelsen. De forretningsmæssige konsekvenser opgøres oftest på en kvalitativ skala.
3	Trusselniveau	Trusselniveauet sammenfattes i et diagram "trusselbillede"(se figur 2.1) med skadevirkning/konsekvens og sandsynlighed som akser. Idet alle sikkerhedstrusler, markeret ved deres nummer i trussellisten, indplaceres på diagrammet skabes et fint overblik over hvilke trusler der udgør de største risici.
4	Sikkerhedsmiljø	Under gennemførelsen af trusselvurderingen har vi set bort fra virkningen af sikkerhedsmiljøet. Derfor skal nu alle eksisterende sikringsforanstaltninger og procedure relateres til den sikkerhedstruende hændelse identificeres og vurderes.
5	Samlet risikobillede	Her holdes trusselniveauet op imod sikkerhedsmiljøet/sårbarhederne med henblik på at nå frem til en vurdering af det samlede risikoniveau eller det der betegnes som det overordnede risikobillede. Det sker ved, at hver enkelt nummererede trussel markeres i diagrammet "risikobillede" (se figur 2.2) ved sit trusselniveau (fra figur 2.1) og ved niveauet af det til truslen modsvarende sikkerhedsmiljø.

Trin	Aktivitet	Beskrivelse
6	Risiko-begrænsning	Hvis risikoniveauet er for højt (mange i det røde og gule område), er det ideen herefter gradvist at introducere flere sikringsforanstaltninger og procedure med henblik på at kunne flytte markeringerne for sikkerhedstruende hændelser tilbage på "risikoniveau-skalaen. Dvs. fra rødt til gult til grønt område.

De efterfølgende afsnit viser den i tabel 2.1 beskrevne fremgangsmåde til udformningen af en risikoanalyse. Der tages i disse afsnit udgangspunkt i trusler ved det kritiske område omkring mobile medarbejdere og fjernadgang til virksomheden.

2.1.1 Trusselliste

Der medtages her trusler der er relateret til de tre hovedkategorier: fortrolighed, integritet og tilgængelighed.

Den nedenstående trusselliste er baseret på et scenarie uden hensyntagen til eventuelle sikkerhedsforanstaltninger implementeret på mobile medarbejderes udstyr. De sikkerhedsforanstaltninger der måtte være taget på virksomhedens interne netværk er ikke i fokus i denne rapport og derfor indeholder listen kun trusler mod virksomhedens netværk der opstår i forbindelse med fjernadgangløsninger og mobile medarbejdere.
Listen er inddelt i to hovedoverskrifter, trusler der kan forekomme på selve laptop'en og trusler der kan forekomme når medarbejderen har koblet sig op på virksomhedens netværk. Hver trussel er angivet med en sandsynlighed og en konsekvens der begge er givet en skala: LAV-MIDDEL-HØJ:

Tabel 2.2: Trusselliste

Nr	Trussel	Sandsynlighed	Konsekvens
På laptop			
1	Tyveri af laptop	MIDDEL	MIDDEL
2	Laptop'en bliver kompromitteret af en hacker via Internettet eller netværket (LAN / WLAN)	LAV	MIDDEL
3	Laptop'en bliver kompromitteret som et resultat af social engineering teknikker (Ondsindede web-sites, e-mail med vedhæftede trojansk hest,phishing, osv.)	MIDDEL	LAV
4	Ikke-ansatte benytter laptop'en (venner, familiemedlemmer, osv.)	MIDDEL	MIDDEL
5	Brugeren får ved en fejl gjort laptop'en tilgængelig (Windows fildeling, P2P fildeling, osv.)	MIDDEL	MIDDEL
6	Tyveri af gamle backup medier	LAV	LAV
7	Data bliver ikke fjernet når gamle laptops bliver kasseret eller solgt videre.	LAV	LAV
8	Brugeren sletter information ved en fejl	LAV	LAV
9	System software går ned.	MIDDEL	MIDDEL
10	System hardware går ned.	MIDDEL	MIDDEL
11	Laptop bliver inficeret med virus eller orm.	LAV	MIDDEL
12	Alle VBA makroer kan eksekveres og kan potentielt indeholde virus eller lign.	MIDDEL	HØJ
13	Det er muligt at gemme/åbne animerings-filer (.ani) - hvilket potentielt kan indeholde skadeligt kode.	LAV	HØJ
14	E-mail arkiver skal ligge lokalt på harddisken - en hacker der har fået fingre i en laptop, kan undgå windows logon skærmen og tilgå alle lokale filer - herunder også email arkiver! (kræver at laptop'en kun er låst og ikke slukket)	LAV	MIDDEL
15	USB-port er helt åben	MIDDEL	HØJ

Nr	Trussel	Sandsynlighed	Konsekvens
På virksomheds netværket			
16	Uautoriseret læse adgang til følsomme virksomheds informationer som kan medføre at disse bliver tilgængelige for konkurrerende virksomheder.	LAV	HØJ
17	Systemet er kompromiteret (VPN servere, firewall, osv.)	LAV	LAV
18	En kompromitteret laptop bliver brugt som back-door til at få adgang til virksomhedens netværk.	LAV	LAV
19	En stjålet laptop bruges til at få adgang til virksomhedens netværk.	MIDDEL	MIDDEL
20	En gammel laptop bruges til at få adgang til virksomhedens netværk.	LAV	LAV
21	Uautoriseret skrive adgang kan medføre at følsomme virksomheds informationer kan blive ændret og derved ikke længere er troværdige.	LAV	HØJ
22	Uautoriseret skrive adgang kan tillade at følsomme virksomheds informationer kan blive slettet.	LAV	HØJ
23	En inficeret laptop kobles direkte til virksomheden netværk.	MIDDEL	HØJ
24	Det er endnu ikke muligt at opdatere laptops via fjernadgang, via fx ADSL opkobling hjemmefra.	HØJ	HØJ
25	VPN autentificering sker via simpelt password(længde på 6 karakter - alle tal)	HØJ	LAV

2.1.2 Sandsynlighed og konsekvens

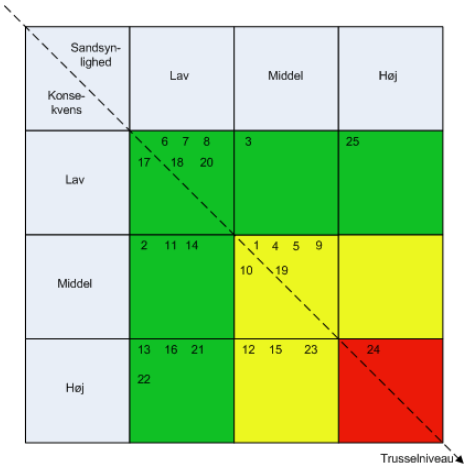
I tabel 2.1 står der beskrevet at sandsynligheden og de forretningsmæssige konsekvenser bør opgøres efter en kvalitativ skala. Disse vurderingsskalaer er bygget op på følgende måde:

- for sandsynlighed:
  1. indtræffer meget sjældent. Betragtes som en teoretisk mulighed(LAV)
  2. forekommer af og til. Sket mindst en gang (MIDDEL)
  3. forekommer hyppigt. Opserveret flere gange (HØJ)
- for forretningsmæssige konsekvenser:
  1. ingen signifikant skade (LAV)
  2. væsentlig skade (MIDDEL)
  3. yderst alvorlig skade (HØJ)

Sandsynligheder og konsekvens er inkluderet i trussellisten i tabel 2.2.

2.1.3 Trusselniveau

Trusselniveauet sammenfattes i et såkaldt trusselbillede-diagram. Til at beskrive trusselniveauet benyttes igen skalaen HØJ-MIDDEL-LAV som er synliggjort ved farverne rød-gul-grøn i diagrammet. Det vil for eksempel sige, at markeringer placeret i det røde område er kritiske. Dette giver et umiddelbart mere visuelt overblik over trusselniveauet.



Figur 2.1: Trusselbillede

I figur 2.1 er indsat alle markeringerne fra trussellisten ind i trusselbilledet.

2.1.4 Sikkerhedsmiljøet

Sikkerhedsmiljøet beskrives ved skalaen: STÆRK-MIDDEL-LAV og indsættes som en ekstra kolonne i trusselliste-tabellen 2.2. En samlet risikoanalyse skema kan derved udtrykkes ved følgende tabel:

Trusler der i trusseldiagramet, figur 2.1, er markeret i grønt område er i tabel 2.3 udeladt for overskuelighedens skyld.

2.1.5 Det samlede risikobillede

Her holdes trusselniveauet op imod sikkerhedsmiljøet og danner et samlet risikovurderingsdiagram. Skalaen vedrørende risikoniveauet er inddelt i følgende:

1. uacceptabel - rødt felt
2. delvis acceptabel - gult felt
3. acceptebel - grønt felt

Det vil sige, at markeringer placeret i det rødt område er kritiske mens markeringer i grønt område er uden væsentlig betydning. Et overblik over risikoniveauet vil man derfor umiddelbart kunne opnå på grundlag af hvor nummermarkeringerne er placeret henne i diagrammet.

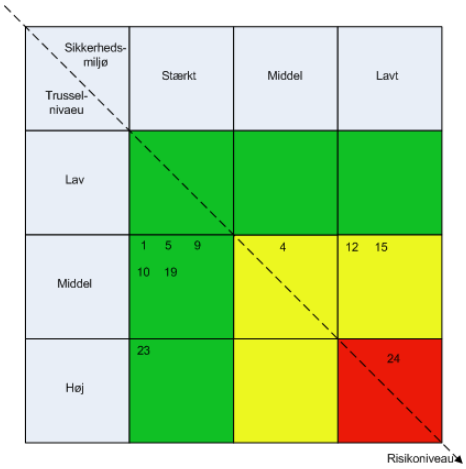
Tabel 2.3: Risikoanalyseskema

Nr	Trussel [Sandsynlighed/Konsekvens]	Sikkerhedsmiljø	Forbedring
På laptop			
1	Tyveri af laptop [MIDDEL/MIDDEL]	Laptop er beskyttet med stærk autentificering samt kryptering af harddisk. [STÆRK]	Ikke nødvendigt.
4	Ikke-ansatte benytter laptop'en (venner, familiemedlemmer, osv.) [MIDDEL/MIDDEL]	Laptop er beskyttet med firewall og antivirus program. [MIDDEL]	Der indføres regler for hvem der bennytter laptopen
5	Brugeren får ved en fejl gjort laptop'en tilgængelig (Windows fildeling, P2P fildeling, osv.) [MIDDEL/MIDDEL]	Ikke muligt for almindelig bruger kræver administrator rettigheder [STÆRK]	
9	System software går ned. [MIDDEL/MIDDEL]	Procedure findes. Ved adgang til virksomhedens netværk er det muligt at geninstallere alt nødvendigt software [STÆRK]	
10	System hardware går ned. [MIDDEL/MIDDEL]	Procedure findes. [STÆRK]	Mulighed for at låne udstyr under reperation
12	Alle VBA makroer kan eksekveres og kan potentielt indeholde virus eller lign. [MIDDEL/HØJ]	Antivirus program bruges. Men gennerelt kan alle makroer køres. [LAV]	Bør kun tillade signerede makroer. Sikkerhedsniveau ændres til 'Meget Høj'
15	USB-port er helt åben [MIDDEL/HØJ]	Ingen kontrol med USB-porte. [LAV]	

Nr	Trussel [Sandsynlighed/Konsekvens]	Sikkerhedsmiljø	Forbedring
På virksomheds netværket			
19	En stjålet laptop bruges til at få adgang til virksomhedens netværk. [MIDDEL/MIDDEL]	Procedure findes. [STÆRK]	
23	En inficeret laptop kobles direkte til virksomheden netværk. [MIDDEL/HØJ]	Procedure findes. [STÆRK]	
24	Det er endnu ikke muligt at opdatere laptops via fjernadgang, via fx ADSL opkobling hjemmefra. [HØJ/HØJ]	Ingen kontrol om software er opdateret. [LAV]	Der skal udarbejdes en løsning så laptop'en kan få installeret sikkerheds opdates via fjernadgang

I dette trin omsættes trusselsbilledet, figur 2.1, til et risikobillede, figur 2.2, ved en overføring af hver enkelt nummereret trussel fra trusselbilledet til risikobilledet, således at der sker en markering af trusselniveauet og af niveauet af de til truslen modsvarende sikkerhedsmiljø.

Det nye risikobillede kan ses i figur 2.2.



Figur 2.2: Risikobillede

2.1.6 Risikobegrænsning

Er nogle trusler markeret i rødt og gult område i risikobilledet er det alle trusler der bør tages stilling til om der skal foretages nogle nye eller ekstra foranstaltninger i virksomheden.

Ledelsen kan eksempelvis sætte sig det mål, at de vil have fjernet alle markeringer i det rødt område samt hovedparten af dem i gult område. Her er imidlertid andre vigtige overvejelse der gør sig gældende, f.eks. økonomiske. Virksomheden må her overveje de omkostninger der er forbundet med både det at få udbedret truslerne og derved flere sikkerhedsforanstaltninger i virksomheden op mod de omkostninger og konsekvenser det kan have ved ikke at ændre på nuværende niveau.

2.2 Risikovurdering

Når man skal vurdere informationssikkerheden i en virksomhed er det altid en god ide at starte med at lave en risikovurdering.
En risikovurdering skal gennemføres regelmæssigt og bør give information om:

- Hvilke aktiver, herunder data, der er kritiske for organisationens aktiviteter.
- Hvilke risici, der kan true organisationens aktiver.

- Hvilke risici, der kan påvirke omverdenens tillid til organisationens data.
- Hvad det vil koste at fastholde risikoen på et niveau, som ledelsen finder acceptabelt.
- Hvilke udækkede risici, som fortsat er til stede.

Mange danske virksomheder der foretager sådan en vurdering gør det i dag oftest i henhold til DS484:2005[26] men det er dog ikke et krav. Andre skrevne guides som ISO 27001:2005[15] kan også benyttes.

Risikovurdering anvendes til at undersøge hvilke forretningsmæssige risici en virksomhed er udsat for, når den benytter sig af informationsteknologi.
Herefter kan den resulterende vurdering, set i sammenhæng med eksempelvis lovgivningskrav og andre forretningsmæssige forhold, anvendes som grundlag for beslutning om hvilke sikkerhedsforanstaltninger og procedurer, der skal i-værksættes.

Den samlede vurdering af virksomheden kan ses i kapitel 5.

2.3 Opsummering

Brugen af risikovurderingen lægger op til, at man ikke skal have IT-sikkerhed for enhver pris, og at den sikkerhed man beslutter sig for skal lægges på et niveau, der modsvarer de trusler der realistisk set kan forekomme.

En indledende risikovurdering og risikoanalyse kan være en stor hjælp til udformningen af en sikkerhedspolitik.

Kapitlet lister en række trusler der alle er væsentlige i forbindelse med det at have mobile medarbejdere der skal kunne koble sig op på virksomhedens netværk også fra lokaliteter der ligger uden for virksomhedens kontrol. Nogle af truslerne kan mindskes ved tekniske foranstaltninge mens andre kræver en ændret adfær fra enten virksomheden eller medarbejderens side.

Kapitel 3

Sikkerhedspolitik

Dette kapitel beskriver først lidt omkring de gældende 'best practices' og standarder som virksomheder har mulighed for at benytte og hente vejledning fra, når informationssikkerhedspolitikken skal udformes. Herefter en beskrivelse af opbygning og indhold i en sikkerhedspolitik med eksempler på hvordan en sådan kan udformes i henhold til gældende standarder og/eller best practices. Sikkerhedspolitikken er en vigtig del af virksomheden og danner grundlag for virksomhedens datasikkerhed. Sikkerhedspolitikken fastlægges i høj grad på baggrund af viden om sårbarhederne i den pågældende virksomhed.

3.1 Best practices og Standarder

Informationssikkerhed bliver heldigvis stadig mere standardiseret og i forbindelse med implementering af mobile arbejdspladser har en række organisationer udarbejdet vejledninger og dokumenter med anbefalinger. Disse anbefalinger er ofte udarbejdet som en række krav til hvordan sikkerheden bør håndteres, de skal dog ikke ses som en komplet guide til sikker implementering af mobile arbejdspladser, men som det fremgår af navnet er de blot anbefalinger man kan tage udgangspunkt i.
Standarder bruges til at danne grundlaget for informationssikkerhedsarbejdet og til at hæve det generelle sikkerhedsniveau i virksomheden. I Europa benyttes primært ISO/IEC 27001:2005 [15] og i Danmark, Dansk Standard DS484:2005

[26]. Sidstnævnte skal idag efterleves af alle statens institutioner [19].

3.1.1 NIST

National Institute of Standards and Technology (NIST) er et føderalt agentur, der bl.a. leverer mange best practices og standarder i forbindelse med implementering af informationssikkerhed. NIST har en sikkerhedsafdeling, *Computer Security Division*(CSD), hvis formål er at:

> *"... provide standards and technology to protect information systems against threats to the confidentiality of information, integrity of information and processes, and availability of information and services in order to build trust and confidence in Information Technology (IT) systems."*[1]

I forbindelse med brugen af trådløse netværk samt opbygning af sikkerhedsbevidstheds programmer har NIST lavet en række vejledninger, 'Wireless Network Security for IEEE 802.11a/b/g and Bluetooth' [11] og 'Building an Information Technology Security Awareness and Training Program'[4].

3.1.2 ISO/IEC

27000 er ISO's ny nummerserie for internationale standarder om informationssikkerhed baseret på British Standard (BS) 7799 fra *British Standards Institute* (BSI).
ISO 27001 udkom som den første i den ny serie standarder i oktober 2005. [2]
Det er en standard som er et pendant til BS 7799-2. ISO 27001 beskriver de konkrete krav til it-sikkerhedsledelse.
ISO 27002 er tilsvarende en pendant til BS 7799-1 og beskriver en række af mere omfattende anbefalinger inden for it-sikkerhed, som ledelsen bør overveje.

3.1.3 DS484

DS484:2005, Dansk Standard for informationssikkerhed, blev kraftigt opdateret i 2005, hvor den som udgangspunkt blev lavet som en oversættelse af den internationale ISO17799:2005, med et antal ændringer eller tilføjelser. DS484 indeholder alle vejledningerne fra ISO17799 formuleret som krav og er udgivet til brug for etablering af IT-sikkerhed i danske virksomheder.
Forskellen mellem de to standarder, ISO og DS, kan overordnet beskrives med at ISO'en er mere omfattende på nogle punkter, DS484 er mere omfattende på

[1] Citatet er fra NIST's hjemmeside, se http://csrc.nist.gov/mission/index.html
[2] Information fundet på Neupart's hjemmeside: http://www.neupart.dk/

andre. Hvilken der er bedst egnet, afhænger af virksomhedens forhold og behov. Lidt populært kan man vel sige at i DS484 "slipper man for at tage stilling til sit behov", mens at ISO'en bedre kan tilpasses til et individuelt behov.

3.2 Informationssikkerhedspolitik

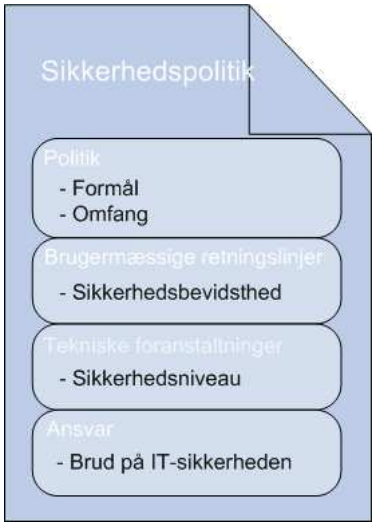
Informationssikkerhedspolitikken fastlægger ledelsens overordnede sikkerheds-målsætning og generelle retningslinjer, de organisatoriske rammer for it- sikkerhedsarbejdet og det organisatoriske ansvar. Politikken fastlægges i høj grad på baggrund af viden om sårbarhederne i den pågældende virksomhed.
Alle virksomheder bør have en informationssikkerhedspolitik, der løbende justeres, og som er godkendt af den øverste ledelse.
Sikkerhedspolitikken indeholder dels regler for overordnede tekniske foranstaltninger der kan anvendes til at beskytte virksomhedens data, virksomhedens retningslinjer, samt bruges til at regulere personers adfærd.
Ved at sikkerhedspolitikken indeholder virksomhedens retningslinjer opnås der en ensartet og kontrolleret håndtering af sikkerheden. I sikkerhedspolitikken bør der desuden også være opstillet regler for hvordan man praktisk sikre sig.
En sikkerhedspolitik formuleres i meget generelle termer, så den ikke behøver at blive ændret ofte. Sikkerhedspolitikken indeholder beskrivelser fra alle de informationssikkerheds områder, der er relevante for virksomheden. Den samlede sikkerhedspolitik består altså af flere politikker herunder f.eks. mobile arbejdspladser, fysisk sikkerhed, osv. Dermed kan hvert område uafhængigt reguleres, hvilket sikre større fleksibilitet overfor ændringer eller nye tilføjelser.

Selve politikken er bygget op så den først beskriver et formål, dernæst omfanget, hvilket sikkerhedsniveau der er valgt, hvilken grad af sikkerhedsbevidsthed man ønsker i virksomheden samt hvad der sker hvis der opstår et brud på informationssikkerheden. Dette er illustreret i figur 3.1.

Et eksempel på et område sikkerhedspolitikken kan ses i afsnit 3.2.1.

3.2.1 Eksempel på en sikkerhedspolitik for mobile medarbejdere

Formålet med dette afsnit er, at give et bud på hvad en virksomheds sikkerhedspolitik skal indeholde, hvis denne udvider sit eksisterende netværk til også at håndtere mobile medarbejdere der f.eks. kan koble sig op på virksomhedens netværk via et trådløst netværk og/eller via en fjernadgang(engelsk: 'remote access').
Indholdet i politikken er dannet på baggrund af dels anbefalinger i DS484[26], NIST 800-48 [11], eksempler på sikkerhedspolitikker fra *SysAdmin, Audit, Net-*



Figur 3.1: Opbygning af sikkerhedspolitik

work, Security Institute(SANS)[1][2], men også på baggrund i samtaler med personer i virksomheden.

3.2.1.1 Politik

Formål
Det er politikkens formål at definere standarder for forbindelse til virksomhedens netværk. Disse standarder er udarbejdet med henblik på at minimere potentielle eksponering af virksomheden, som kan føre til skader i form af uautoriseret anvendelse af virksomhedens ressourcer. Skader inkluderer tab af følsomt eller virksomhedsfortroligt data, intellektuel ejendom, skade på virksomhedens image, skade på virksomhedens interne systemer, osv. [1]
Medarbejderne skal så vidt muligt have adgang til det udstyr, software og andet materiale, der er nødvendigt for at kunne arbejde effektivt fra arbejdspladsen på en sikker og forsvarlig måde. Opkoblingen til virksomheden fra arbejdspladsen skal i videst muligt omfang være transparent for brugeren, ligesom brugervenligheden af systemet i sin helhed har høj prioritet.

Omfang
Politikken dækker alt udstyr der bruges ved fjernadgang til virksomheden, herunder laptops og smartphones, som inden eller uden for virksomhedens område, kan forbindes til virksomhedens netværk. Dette inkludere alle former for trådløst udstyr, som er i stand til at transmittere data pakker.
Trådløst udstyr og/eller netværk uden nogen form for forbindelse til virksom-

hedens netværk er ikke omfattet af denne politik. Alt eksisterende og fremtidigt udstyr, som falder inden for politikkens rammer skal konfigureres i henhold til politikken.

3.2.1.2 Brugermæssige sikkerhedsregler

Sikkerhedsbevidsthed
Mobile medarbejdere der ved en trådløs/fjernopkobling til virksomhedens netværk, fungerer som en forlængelse af virksomhedens netværk, og er derfor omfattet af de samme regler, som gælder ved en fast arbejdsstation i virksomheden [2].

Håndtering udenfor virksomhedens lokaliteter
Medarbejdere skal udvise ekstra forsigtighed, når de håndterer information udenfor virksomhedens lokaliteter. Det inkluderer håndtering af samtaler, dokumenter, Pc'er, Cd'er, USB-nøgler eller andre elektroniske medier eller fjernadgang til information, der er oplagret i IT-systemerne.

- Undgå at tale om eller fremvise information om kunder eller interne forretninger, når andre kan høre eller se det.
- Udstyr, information eller software bør ikke tages med eller sendes ud af huset, medmindre det er aftalt med din leder.
- Dokumenter, udstyr, og elektroniske medier skal overvåges eller låses forsvarligt inde, beskyttet mod uautoriseret brug og ødelæggelse. Efterlad ikke udstyr uovervåget på offentlige steder. Laptops bør bæres som håndbagage på rejser.
- USB-nøgler er små og kan let bortkomme eller tabes. Hvis der er behov for at anvende USB-nøgler til at gemme intern eller fortrolig information, skal du løbende fjerne information, der ikke længere behøver at være lagret på den måde. Hold altid USB-nøglen hæftet sammen med noget, helst dit nøglebundt. Hvis du bruger din USB-nøgle el.lign. i andres arbejdsstationer, skal du være opmærksom på, at der kan lejre sig virus på USB-nøglen uden din viden. Anvend kun din USB-nøgle på arbejdsstationer, der har tilstrækkelig virusbeskyttelse.
- Når du er uden for virksomhedens lokaliteter bør du kun printe på en direkte tilsluttet printer (ikke delt), som er fuldstændig under din kontrol og indenfor synsvidde.
- Rapportér altid tab eller misbrug af information eller udstyr uden forsinkelse til din leder.

Udstyr og systemer
Alle IT systemer, udstyr eller hukommelsesværktøjer, der anvendes, skal være godkendt af eller følge de standarder, der er udstedt af virksomhedens IT afdeling. Tilslut aldrig uautoriseret udstyr til arbejdsstationer eller netværk, og installér eller download kun programmer, hvis du er autoriseret til det.

- Du må ikke etablere din egen Internetforbindelse fra en arbejdsstation i virksomhedens interne netværk ved at bruge modem, telefonkort, trådløst netværk eller lignende. Skift aldrig sikkerhedsindstillingerne i browseren eller i din PC.

Idet arbejdspladsen er mobil samt kommunikerer vha. trådløs teknologi, skal medarbejderen udvise større opmærksomhed end normalt ved følgende:

- Arbejdspladsen er personlig og må kun benyttes af den pågældende medarbejder.
- Forbindelse til virksomhedens netværk må kun ske med det af virksomhedens udleverede udstyr.
- Arbejdspladsen må kun anvendes til arbejdsrelaterede formål. Visse private formål, såsom e-mail og web surfing tillades dog, så længe dette ikke er i konflikt med sikkerheden og virksomhedens øvrige politikker. [1]
- Arbejdspladsen må aldrig efterlades i en tilstand, med direkte adgang til virksomhedens netværk og skal være beskyttet mod uautoriseret adgang, når den ikke anvendes.
- Virksomhedens medarbejdere skal sikre at deres udstyr, når det er forbundet til virksomhedens netværk, ikke er forbundet til noget andet netværk. Dette gælder ikke personlige netværk, som er under medarbejderens fulde kontrol. [1]
- Passwords må ikke lagres på computeren, f.eks. ved autologin, men skal indtastes hver gang.
- Paaswords og andet, som anvendes i forbindelse med login, er personligt og må ikke videregives. [1]
- Arbejdspladsen skal altid have de nyeste opdateringer installeret.
- Medarbejderen må ikke udtrække fortrolig eller personfølsom information, f.eks. ved nedskrivning eller print uden for virksomhedens område.

3.2.1.3 Tekniske foranstaltninger

Sikkerhedsniveau

Almindeligt hardware

- Personal Data Assistants (PDA) understøttes ikke i virksomheden, men udvalgte mobiltelefoner understøttes.

Én pc pr. bruger
Hver medarbejder i virksomheden skal ikke have mere end én pc til brug i sit daglige arbejde.

- Virksomheden understøtter ikke pc-baserede hjemmearbejdspladser. Det er kun muligt at arbejde fra steder uden for virksomhedens kontorer med virksomhedens laptop-løsninger.

Fjernadgang
Beslutningen om en laptop-brugers fjernadgang, skal træffes på grundlag af arbejdssituationen og de forretningsmæssige behov.

Fjernadgang skal nedfældes i en aftale, der underskrives af en leder og en medarbejder for at sikre kendskabet til ansvar og regler om informationssikkerhed.

- Virksomhedens laptop-løsning indeholder en facilitet for fjernadgang og skal ses som en udvidelse af virksomheden uden for kontoret.
- Alle laptop-brugere, der forventes at arbejde uden for virksomhedens kontorer med fjernforbindelse til virksomhedens netværk, skal anvende den godkendte VPN-løsning (virtual private network) med henblik på sikker forbindelse til virksomhedens netværk. Den gives til trådløs, bredbånds- og opkaldsforbindelse.
- VPN-løsningen skal bestilles særskilt og inkluderer et sikkerheds-token (USB-token) og en PIN-kode. VPN-software er præinstalleret.
  VPN-løsningen understøtter ældre sikkerheds-token i virksomheden som fx PCMCIA chipkortlæsere, og eksterne USB-chipkortlæsere understøttes også.
- Laptop-brugere med et forretningsmæssigt behov for at arbejde hjemmefra skal bruge bredbåndsadgang eller opkaldsløsning. Funktionen til bredbåndsadgang er indeholdt i laptoppen. Opkaldsløsningen skal bestilles særskilt og inkluderer en opkaldskonto.
- Laptop-brugere med et forretningsmæssigt behov for ofte at arbejde fra hoteller eller andre kontorlignende steder, der ikke er nævnt ovenfor, skal bruge opkaldsløsninger eller en konto hos en offentlig bredbåndsudbyder.

- Laptop-brugere med et forretningsmæssigt behov for mobilforbindelser til virksomhedens netværk skal have en af virksomheden godkendt mobiltelefon (til GPRS-forbindelse), som skal godkendes af det pågældende forretningsområdes linjeledelse.

Applikation til fjernadgang og adgang til data.
Virksomheden giver laptop-brugere fjernadgang til: e-mail, intranet, internet og personligt drev efter anmodning.

Fjernadgang til information - fra steder, der er uden for virksomhedens kontrol - er begrænset. Enhver intern bruger, der har fjernadgang til it-systemer, har to roller: en rolle som fjernbruger og en rolle som intern bruger med særskilt autorisation til hver rolle.

Nogle lidt mere generelle krav:

- Forbindelse til virksomhedens interne netværk må kun ske med det af virksomheden udleverede udstyr.
- Der skal føres en log, der indeholder hændelser som brugernavne, tidspunkt for brugeres logon og logoff, hardware ID (MAC adresser) eller brugerlokation.
- Alle enheder med trådløs adgang til virksomhedens netværk skal anvende en krypteret forbindelse.
- Det må ikke være muligt at initiere en forbindelse til arbejdspladsen fra virksomheden.
- Så vidt muligt skal mobile enheder autentificeres inden netværksadgang gives.
- En VPN forbindelse må ikke være aktiv i mere end 12 timer. [2]
- Der skal indføres kontroller til opdagelse, forhindring og genetablering fra ondsindet kode sammen med et passende niveau af brugeropmærksomhed. Kontrollerne skal jævnligt opdateres.
- Der skal være en gateway, der filtrerer trafikken ud fra en liste med brugeres rettigheder til at tilgå tjenester på netværket.
- Når udstyret har været inaktivt i en periode, skal alle programmer og forbindelser lukkes, samtidig med at udstyret låses.
- Mobilt udstyr, der indeholder følsomme data, skal kryptere indholdet af deres diske.
- Det er ikke tilladt at anvende det trådløse udstyr i ad-hoc tilstand. Dette gælder ikke personlige netværk, som er under medarbejderens fulde kontrol. [11]

3.2.1.4 Ansvar

Medarbejderen har ansvaret for, at sikkerheden omkring arbejdspladsen som beskrevet ovenfor overholdes. Til enhver tid skal arbejdspladsen anvendes på en sådan måde, at virksomhedens data beskyttes. Endvidere skal usædvanlige hændelser, suspekte aktiviteter samt fejl og mangler indrapporteres til de netværksansvarlige.
Virksomheden har ansvaret for, at medarbejderen har læst og forstået sine forpligtelser, som er beskrevet ovenfor. Endvidere skal virksomheden informere medarbejderen om de sikkerhedsmæssige aspekter, som knytter sig til brug af mobilt udstyr.
Netværksafdelingen har ansvaret for, at medarbejderens udstyr fungere tilfredsstillende samt at udstyret løbende vedligeholdes og opdateres sådan, at maksimal sikkerhed kan opnås med det anvendte udstyr. Endvidere skal netværksafdelingen overvåge brugen af arbejdspladsen, samt reagere på suspekte aktiviteter i loggen.

3.3 Opsummering

Dette kapitel har genemgået hvordan man på baggrund af en risikoanalyse og i hehold til best practices og standarder, som ISO27001 og DS484, kan udforme en sikkerhedspolitik.

Sikkerhedspolitikkens i dette kapitel er opstillet specifikt med tanke for den pågældende virksomheds krav udfra det nuværende niveau af sikkerhed samt udformet med nogle generelle krav til det at have såkaldte mobile medarbejdere ansat i en virksomhed.

Grunden til at specifikke krav er medtaget, er dels at de kan bruges som inspiration for andre men også fordi de sammen med risikovurderingen er med til at fastlægge et passende sikkerhedsniveau i virksomheden.

Kapitel 4

Sikkerhedsproblemer ved mobile medarbejdere

Både i og udenfor virksomheden vil en mobil medarbejders udstyr være et udsat endepunkt. Dels i kraft af udstyrets mobilitet vil det være fysisk nem at miste, både ved tyveri men også i kraft af medarbejdernes egen glemsomhed. Det er velkendt at mange virksomheder oplever at mobilt udstyr som laptops og mobiltelefoner bliver stjålet eller glemt f.eks. i taxaen på vej til lufthavnen, på cafeer, restauranter, hotelværelser, i konferencerum, osv. Det mobile udstyr har ofte også adgang til virksomhedens interne netværk gennem mere eller mindre åbne netværk som Internettet, dette medfører en væsentlig forøgelse af angrebsfladen i forhold til interne arbejdsstationer. Dette kan for virksomheder der ønsker, at implementere fjernadgange og mobilt udstyr til sine medarbejdere, virke som en stor udfordring. Dette kapitel forsøger at afdækker de problemstillinger og teknologier der er forbundet med hvordan man på en sikker måde kan lade medarbejdere koble sig op på virksomhedens netværk fra steder der er uden for virksomhedens kontrol samt hvilke teknologier der gør det muligt på en sikker måde. Først kommer en beskrivelse af nogle af de generelle sikkerhedsproblemer der er knyttet til det at have mobile medarbejdere, efterfulgt af en beskrivelse af de mest udbredte typer trådløse netværk og deres sikkerhedsmæssige overvejelser. Til sidst gives en beskrivelse af nogle af de mest udbredte teknologier der bruges i forbindelse med at fjernadgange etableres i virksomheden.

4.1 Generelle problemer

I dette afsnit beskrives de sikkerhedsproblemer der kan opstå, men som ikke knytter sig til én bestemt teknologi. Det drejer sig her omkring den fysiske sikkerhed, passwordangreb, social engineering og phishing.

4.1.1 Fysisk sikkerhed

Den mobile medarbejder bruger i sagens natur udstyr der er småt og ikke vejer for meget, eksempelvis laptops, smartphones, osv. Det medfører en øget risiko for at udstyr bliver stjålet eller glemt. Der er flere måder man kan sikre udstyret mod at blive anvendt af fremmede på:

- Kabellåse - Ved at anvende kabellåse kan medarbejderens laptop låses fast, når den er uden for opsyn.
- Kryptering - Ved at kryptere følsomme data kan tabet som følge af tyveri begrænses til udstyrets værdi. Se mere omkring dette punkt i afsnit 4.3.3

4.1.2 Password angreb

Formålet med passwordangreb er for angriberen at komme i besiddelse af medarbejderens password. Hvis dette lykkes kan angriberen omgå sikkerheden og opnå adgang til virksomhedens netværk eller andre ressourcer. De største udfordringer ligger i antallet af password medarbejderen skal huske, deres konstruktion af password og selve omgangen med disse. Mange password til mange systemer gør at medarbejderen - om muligt - bruger samme password til dem alle hvilket gør at sikkerheden bestemmes ud fra det dårligst sikrede system. Der findes flere forskellige metoder til at beskytte sig mod passwordangreb på:

- Autentificering - Brugen af to-faktor autentificering baseret på certifikater eller engangspassword er den primære løsning. Se en nærmere beskrivelse i afsnit 4.3.2. Ved sådan autentificering undgås, at en angriber får adgang til virksomheden netværk blot ved et kompromitteret password.
- Passwordpolitik - Alle virksomheder bør have en passwordpolitik nedskrevet, der for alle dens systemer angiver nogle minimumskrav til konstruktion af "sikre"passwords (bestå af 8 tegn, bør indeholde både store og små bogstaver samt tal eller specialtegn [10]). Derudover bør det også være nedskrevet hvor ofte password skal udskiftes.
- Firewall og Antivirus programmer - Begge vil kunne forhindre angribere i at inficere medarbejderens udstyr med eksempelvis små programmer til at

aflure password og lignende. Yderligere beskrivelse af dette i afsnittende 4.3.5 og 4.3.6

For en angriber er der flere måder at tilegne sig en medarbejders password på. Oftest sker det gennem eksempelvis social engineering eller phishing.

4.1.3 Social engineering

Social engineering er en trussel der ofte overses men som regelmæssigt udnyttes af angribere. Der drages her fordel af det der længe er blevet betragtet som værende det svageste led i sikkerheden i en virksomhed, nemlig den menneskelige faktor. [6] Social engineering kan siges, at være en handling der får mennesker til at gøre ting de ellers ikke ville gøre, afsløre ting de ellers ikke ville afsløre. Andre gange til at undlade at gøre ting de ellers ville have gjort eller undlade at afsløre hvad de har opdaget, med andre ord, vi taler om forførelse af mennesker i alle ordets betydninger. Problemet med social engineering er at tekniske løsninger på næsten alle sikkerhedsproblemer ikke nødvendigvis er sikre, før end de også er løst i relation til social engineering. Med mobile medarbejdere der ofte bevæger sig uden for virksomhedens fysiske rammer øges også risikoen for at blive ramt af social engineering. Eksempelvis kan password og brugernavne blive afluret ved brug på offentlige steder. I [20] angives det, at social engineering benytter sig af en række egenskaber ved den menneskelige psyke for at opnå et mål:

- Autoritet - Mennesker har en tendens til at rette sig efter autoritetsfigurer. For eksempel vil en angriber med stor sandsynlighed have held til at overtale en, hvis han udgiver sig for at være en IT-ansat, medlem af ledelsen eller en ansat der hjælper bestyrelses medlemmer.
- Sympati - Mennesker vil gerne hjælpe dem de synes om, så en angriber kan forsøge at skabe venskabelige relationer med offeret, f.eks. ved at lade som om de har en eller flere fælles interesser.
- Gengældelse - Mennesker har en tendens til at hjælpe nogle der allerede har hjulpet dem. Derfor kan en angriber foregive at være en IT-medarbejder der netop har beskyttet eller forhindret tab af offerets data.
- Gennemførthed - Mennesker vil gerne samarbejde, når de har give et løfte herom. For eksempel vil en angriber der udnytter dette til, efter at have overtalt offeret til at følge en "ny"virksomheds politik, om at offeret bør ændre sit password til noget, der let kan gættes.
- Social anerkendelse - Mennesker har det med at gøre som de andre, hvis opførelsen synes at være acceptabel blandt ligemænd. Angriberen kan dermed lettere overtale et offer, hvis han fortæller at offerets kollegaer har gjort det samme.

- Knaphed - Mennesker vil sjældent gå glip af noget og kan dermed lettere påvirkes for eksempel når noget kun er tilgængeligt i et kort tidsrum eller konkurrencer bliver udskrevet osv. Dette kan angriberen udnytte til for eksempel at få fat på login oplysninger fra medarbejderen, der har modtaget en mail, hvor der tilbydes præmier til de første registrerede på en hjemmeside styret af angriberen.

Et eksempel omhandlende et social engineering angreb, fundet på [1]
[...chefen der blev ringet op at en person som udgav sig for at komme fra at analyseinstitut der var i gang med en af de sædvanlige undersøgelser og spurgte om han måtte stille nogle spørgsmål. I løbet af spørgeækken kom der også en serie spørgsmål omkring IT sikkerheden i virksomheden og chefen afstod godt nok fra at opgive sit password, men ville gerne fortælle at han brugte din ældste datters navn. Lidt senere under spørgerækkens personlige spørgsmål fortalte han at han var gift med Jane og havde to døtre Sarah der var 11 og Stephanie der var 14.]

Der er flere ting virksomheder kan gøre for at beskytte sine medarbejdere mod social engineering. I [13] angives følgende måder:

- Sikkerhedspolitik - En sikkerhedspolitik kan tage højde for social engineering ved at give klare regler for hvilke handlinger der er tilladte. Medarbejderen vil derved også være mere opmærksom over for bedrag og angrebsforsøg.
- Sikkerhedsbevidsthed - Alle medarbejdere skal være bevidste om social engineering og hvad det betyder for dem. De skal kende værdien af de oplysninger de sidder med, hvordan et angreb kan identificeres og hvilke handlinger der vil være hensigtsmæssige hvis noget mistænkeligt sker. Alt dette skal være specificeret i sikkerhedspolitikken.
- Træning af nøglepersonale - Nøglepersonale skal yderligere trænes i at modstå social engineering angreb. Desuden skal de have deres egen modtagelighed over for angreb demonstreret. Dette giver en større motivation og bevågenhed.
- Løbende påmindelser - For at fastholde medarbejdernes opmærksomhed, skal de løbende påmindes om social engineering angreb. Dette kan gøres ved f.eks. at give eksempler på gennemførte social engineering angreb og hvad disse vil have af omkostninger for henholdsvis virksomheden og medarbejderne selv.
- Metodik - Opret metoder til eksponering og forhindring af angreb. Der er mange måder hvorpå dette kan gøres f.eks. ved at have en række spørgsmål, der kan bruges til autentificering af kollegaer.

[1] http://www.bufferzone.dk/hacking/hacking-social-engineering.htm

- Rapportering af hændelser - Hvert tilfælde af angreb skal registreres og kan bruges til at advare andre mulige mål. Dermed lærer virksomheden også af angrebet.

4.1.4 Phishing

Phishing er en form for svindel, der har til formål at stjæle personlige data, f.eks. kreditkortnumre, password, kontodata eller andre oplysninger. Phishing foregår ved at svindleren konstruerer et troværdigt scenarie, som eksempelvis en bank eller en anden velkendt virksomhed eller varemærke som offeret måtte have tillid til, hvorved han angiver sig for at være en anden, for derved at få lokket fortrolige informationer som brugernavn og adgangskode, ud af offeret. En af de mest udbredte phishing metoder er, hvor svindleren fabrikerer en falsk webside der næsten er identisk med en kendt side udadtil, og derved kan snyde brugere til at indtaste deres brugernavn og kodeord, der derpå bliver opsnappet af svindlerne. Det svarer næsten til at en svindler opstiller en falsk bank-automat, der hugger både kort og pinkode når en person bruger den. Da det på Internettet er det utrolig nemt at kopiere grafisk indhold fra en velkendt webside, finder der meget af denne type svindel sted. Ifølge Anti-Phishing Working Group (APWG) [14] var der fundet 32.079 falske websider på verdensplan i august 2007. Levetiden for disse sider er dog ikke særlig lang, i gennemsnit er sådan en side aktiv i 3,3 dage inden den bliver lukket ned igen.

Idet at en e-mail ikke koster noget at sende, er det en meget nem distributionskilde for uønskede reklamer og andet af mere alvorlig karakter som f.eks. phishing. Det meste phishingsvindel hænger sammen med e-mails, der udnytter den tillid offeret har til et respekteret varemærke ved at lokke offeret til at klikke på et hyperlink. Linket fører ofret frem til en lige så overbevisende (og lige så falsk) webside eller pop op-vindue, som er blevet oprettet til at imitere det virkelige firma. Her vil ofret blive anmodet om at røbe følsomme personlige oplysninger, f.eks. cpr-nummer, et bankkonto- eller kreditkortnummer, en bekræftelseskode, et password eller en pinkode. E-mails kan i nogle tilfælde også indeholde overdrevent alarmerende indhold. Svindlerne forsøger her at skabe en følelse af, at noget er meget vigtigt, så offeret svarer uden at tænke dig om.

Selvom årvågenhed og fornuft ofte er den bedste løsning, kan det være meget svært at skelne en veludført phishing webside fra den 'rigtige' webside. Der findes forskellige måder at beskytte sig mod phishing angreb på:

- Videregiv aldrig følsomme personlige oplysninger i en e-mail
  De fleste lovlige virksomheder anmoder aldrig om adgangskoder, konto- eller kreditkortnumre eller andre fortrolige oplysninger. Det er let for personer, som anvender phishing, at narre folk - f.eks. ved at forfalske 'Fra'-adressen i en e-mail-meddelelse.

- Vær varsom ved at klikke på et hyperlink i en meddelelse
  Hvis en e-mail anmoder om personlige oplysninger, fører hyperlinket sandsynligvis til en falsk webside, hvor oplysningerne sendes til svindleren, der oprettede websiden. Ved tvivl, om en meddelelse er ægte, kan virksomheden kontaktes på et telefonnummer, eksempelvis fundet i telefonbogen.

- Gem ofte besøgte websider i foretrukne
  Vær opmærksom på stavefejl og grammatiske fejl. En webadresse, der er ændret en smule vil kunne føre til en phishing webside. Eksempelvis vil siden, www.microsoft.com, kunne f.eks. blive vist som www.micosoft.com, www.mircosoft.com, eller www.microsoft.com. Det er derfor en god ide, når man befinder sig på den rigtige webside, at gemme siden i foretrukne.

- Kontroller, at webstedet beskytter personlige oplysninger og er ægte
  Personer, som anvender phishing, kan som tidligere nævnt forfalske adressen, der vises. Hvis der blot er en smule i tvivl om ægtheden af webstedet, skal der satses på sikkerheden og forlade det. Kontroller, om der er tegn på datakryptering, hvilket er en sikkerhedsforanstaltning, som hjælper med at sikre følsomme data, når de overføres på Internettet. Se efter "https"i webadressen og efter en lille lukket hængelås eller en hel nøgle (kan være placeret forskellige steder alt efter browsertype). Desværre kan både hængelåsen og nøglen forfalskes på nogle systemer, så det er en god ide at dobbeltklikke på den for at få vist sikkerhedscertifikatet til webstedet. Kontroller, om navnet på certifikatet stemmer overens med navnet i adresselinjen. Hvis navnet ikke stemmer overens, er webstedet sandsynligvis falsk.

- Sørg for at holde din computer opdateret
  Phishingsvindlere håber, at der ikke er anvendt de seneste sikkerhedsrettelser og vil måske forsøge at udnytte de svagheder, som ikke er blevet rettet.

4.1.5 Opsummering på generelle sikkerhedsproblemer

I dette afsnit er en række sikkerhedsproblemer, som ikke knytter sig til en bestemt teknologi, gennemgået. De fleste er ikke nye men i forbindelse med etableringen af mobile medarbejdere har dette medført nye aspekter af sikkerhedsproblematikken.
Der er ved hvert af de beskrevne sikkerhedsproblemer givet en række løsningsforslag. Følgende sikkerhedsproblemer er behandlet:

- Fysisk sikkerhed - tab og tyveri af mobilt udstyr er et stort problem for en virksomhed. Det er noget der må tages højde for, da tabt udstyr med

vigtige eller vitale informationer kan ende i andres besiddelse. En god måde at sikre udstyr på er ved brug af kryptering.

- Password - brugen af password skal foregå med omtanke, og en virksomhed bør ikke basere sine adgangskontrol på disse alene.
- Social engineering - her spiller mange menneskelige faktorer ind. Det er en hårfin balance for virksomheden med på den ene side at have service-mindede og hjælpsomme medarbejdere men samtidig at få oplært dem til ikke at udlevere følsomme informationer til selv personer der virker meget troværdige.
- Phishing - en metode der prøver at lokke følsomme informationer ud af personer på vellignende men falske websider eller emails. Medarbejdere bør her gøres opmærksomme på risikoen for sådanne angreb og hvilke forholdsregler man kan tage.

4.2 Sikkerhedsproblemer ved trådløse netværk

Den mobile medarbejders udstyr, bør af virksomheden, betragtes som værende et udsat angrebspunkt og derfor beskyttet som et sådan. Dette afsnit omhandler de forskellige trådløse teknologier og deres sikkerhedsproblemer i forhold til en virksomheds mobile udstyr. Der er valgt at se på teknologien trådløst LAN.

4.2.1 Trådløst LAN

Trådløst netværk er netværk baseret på IEEE 802.11 standarden og ofte kaldes disse også *Wireless LAN*(WLAN). For den mobile medarbejder vil WLAN spille en væsentlig rolle, idet teknologien er direkte implementeret i udstyret, og kan derfor anvendes af mange til at oprette forbindelse til virksomhedens netværk. Dette afsnit afdækker de største sikkerhedsproblemer i WLAN samt giver råd til hvordan man bedst beskytter sig mod disse.

4.2.1.1 WLAN kan ikke hemmeligholdes

Dette afsnit beskriver hvordan et trådløst netværk kan opdages, hvilket forudsætningen til alle de efterfølgende typer angreb beskrevet i dette kapitel.

Der er tale om to metoder til at opdage trådløse netværk: *Aktiv scanning* og brug af *pakkesniffer* [2].

[2]En pakkesniffer er et lille program der anvendes til at analysere netværkstrafik.

Aktiv scanning - er en metode der bruges når en person vil undersøge, om der findes et trådløst netværk inden for sin rækkevidde. Vedkomne sender en forespørgsel til alle Access Points (AP) om deres ServiceSetIdentifier (SSID). Ud fra de svar personen får tilbage er det muligt at se hvilke netværk der er i nærheden.

For at 'skjule' sit trådløse netværk så uvedkomne ikke kan se det er det muligt for en administrator at fravælge SSID-udsendelsen på netværkets AP. Derved vil AP kun svare på forespørgsler indeholdende deres specifikke SSID.

Netværket er dog ikke helt skjult. Med et såkaldt pakkesnifferprogram er det muligt at opsnappe pakker på netværket hvori netværkets SSID fremgår.
En *pakkesniffer* som f.eks. Ethereal[3] og WinDUMP[4] (til Windows) eller AirJack[5] og KisMet[6] (til Linux) virker på den måde at de omfanger 802.11-rammer indenfor rækkevidde, hvori netværkets SSID fremgår. Selv når netværket ikke anvendes aktivt udsendes periodevis såkaldte beacon-rammer fra AP for at gøre opmærksom på dets tilstedeværelse. Disse beacon-rammer indeholder blandt andet SSID, så hvis et af ovennævnte programmer lytter til disse beacon-rammer kan netværkets SSID også udledes.

Selvom det altså er altså relativt let at finde et WLAN om det er 'skjult' eller ej. Der er dog flere måder, at mindske sandsynligheden for at et WLAN opdages:

- Sluk for det trådløse netværk når det ikke anvendes - Et slukket AP vil ikke udsende pakker der kan opfanges af pakkesniffer programmer.
- Slå SSID-udsendelsen fra - Herved undgås det at netværket bliver fundet vha. aktiv scanning. Men vær opmærksom på at netværket altså ikke herved er 100 procent skjult.

4.2.1.2 Lytte til trafik

Da kommunikationen foregår trådløst er adgangen til trafikken mellem de kommunikerende parter åben og sårbar overfor aflytning. Ved aflytning kan virksomhedens fortrolige data og endda data anvendt til autentificering opsnappes ved brug af de såkaldte pakkesniffer-programmer.
Men for at kunne aflytte trafikken i begge retninger på et WLAN, skal pakkesnifferen være placeret inden for rækkevidde af såvel AP som klienten.
Dette kan være en alvorlig trussel mod datasikkerheden for en virksomhed. Der er dog en række måder at beskytte sig mod aflytning på:

[3]Information om programmet findes på: http://www.ethereal.com/
[4]Information om programmet findes på: http://windump.com/
[5]Information om programmet findes på: http://sourceforge.net/projects/airjack/
[6]Information om programmet findes på: http://www.kismetwireless.net/

- Kryptering - Den bedste beskyttelse mod at nogle lytter til trafikken er at sikre, at kommunikationen bliver uforståelig. Kryptering kan sørge for dette. Selve krypteringen kan foregå på mange forskellige lag i OSI-modellen, se appendix B, men jo lavere et lag det foregår på jo mindre information kan der opsnappes ved aflytning.
  Kryptering på lag 2, Data Link-laget, vil betyde at den trådløse del af netværket mellem klient og AP er krypteret, hvilket i de fleste tilfælde vil være nok.
  Ved fjernadgang til virksomheden er det nødvendigt at supplere med kryptering på lag 3 eller højere, da kommunikationen vil passere ubeskyttet over usikre netværk inden den når frem til virksomheden. Disse krypterings former er nærmere beskrevet i afsnittende 4.3.3 og 4.3.1

- Autentificering - Brugen af stærk autentificering vil sikre, at genafspilning af autentificeringsdata ikke kan forekomme. Det betyder at opsnappede autentificeringsdata reelt vil være ubrugelige. Autentificering er nærmere beskrevet i afsnit 4.3.2

4.2.1.3 Angreb mod udstyr

Selve det mobile udstyr kan også være mål for forskellige typer af angreb. Da udstyret ofte anvendes uden for virksomhedens kontrol og dermed uden for virksomhedens normale forsvarssystemer bør udstyret sikres særskilt.

Angreb fra Internettet er nærmest uundgåelige og ved anvendelse af trådløse klienter udvides angrebsfladen yderligere med ad-hoc netværk. Ad-hoc netværk er direkte forbindelser mellem to klienter uden om AP. Derved er der ikke kun tale om angreb gennem virksomhedens netværk og Internettet, men reelt fra alle trådløse enheder inden for rækkevidde. Så hvis en klient bliver inficeret med virus, orm eller lignende, vil den hurtigt kunne sprede sig til resten af netværket.

Der findes mange variationer af virus, orme og trojanske heste. De fleste er udviklet til at inficere PC'ere, men efterhånden som andet udstyr bliver lige så populært vil disse også være udsatte for disse angreb. Det drejer sig både om Personal Digital Assistant (PDA) og smartphones. Disse ondsindede programmer er heller ikke begrænset til kun at udbredes via WLAN, men også andre trådløse teknologier er her udsatte, f.eks. via Bluetooth eller 3G.

For at beskytte sig mod disse angreb anvendes:

- Ad-hoc netværk frakobles - I et ad-hoc netværk kan medarbejdere ikke kontrollere hvem der tilbyder tjenester over netværket. Derfor bør denne form for netværk ikke anvendes.

- Antivirusprogrammer - Antivirusprogrammer kan benyttes til at forhindre virus, orm, trojanske heste, osv. i at inficere udstyret. Se mere i afsnit 4.3.6

- Firewall - En firewall kan filtrere trafikken til og fra medarbejderens udstyr og derved forhindre angrebsforsøg. Se mere i afsnit 4.3.5
- IDS - Med et Intrusion Detection System (IDS) på medarbejderens udstyr, kan ondsindede programmer opdages ved at overvåge systemets opførsel.
- Flyt autentificerings certifikat til hardware - Hvis autentificeringen er baseret på certifikater kan disse med fordel flyttes til separat hardware. Dette vil mindske chancen for at ondsindede programmer som trojanske heste, osv. kan kopiere certifikatet som hvis det var gemt på selve klienten.
- Tjenester der ikke bliver brugt slukkes - De tjenester som medarbejderen ikke bruger, bør slås fra. Dette kan f.eks. være fildeling, fjernstyring, m.m. Derved mindskes angrebsfladen mest muligt.

4.2.2 Opsummering på sikkerhedsproblemer ved trådløse netværk

I dette afsnit er en række sikkerhedsproblemer ved WLAN gennemgået. Sikkerhedsproblemerne er en tussel mod både den mobile medarbejders udstyr men også virksomhedens netværk. Til sikkerhedsproblemerne er der udfærdiget en række løsningsforslag.
Afsnittet skal ikke betegnes som en komplet liste over hvilke typer angreb udstyret kan udsættes for og hvad en dertil hørende administrator kan gøre for at undgå dem. I stedet afspejler dette afsnit nogle få at tidens mest udbredte problemstillinger og løsningsmetoder.
Følgende sikkerhedsproblemer er afdækket:

- Skjult SSID - WLAN kan skjules så de ikke kan ses ved såkaldte aktive scanninger. Men med det rette udstyr kan en angriber alligevel finde det 'skjulte' udstyr. Rådet er derfor også altid at kryptere forbindelser.
- Lytte til traffik - om sniffere på både kablede og trådløse netværk. Udstrålingen øger risikoen for passive angreb, og en virksomhed må sikre at den trådløse forbindelse er både autentificeret og krypteret.
- Angreb mod udstyr - en mobil medarbejders udstyr er et særligt udsat angrebspunkt, og denne må derfor sikres i højere grad end f.eks. internt udstyr i virksomheden. Det være sig gennem firewalls, antivirusprogrammer, osv.

Afsnittet kan eventuelt udvides til også at omhandle sikkerhedsproblemer ved eksempelvis Bluetooth og 3G netværket.

4.3 Udbredte teknologier i forbindelse med fjernadgang

Opkobling til en virksomheds netværk kan i dag ske på mange forskellige måder og fra mange forskellige lokaliteter. Fælles for alle fjernadgangsløsninger er at det typisk sker gennem det åbne Internet.
Der findes en lang række teknologier og metoder der kan hjælpe virksomheder med at implementere fjernadgangsløsninger på en sikker måde.
Dette kapitel gennemgår nogle af de mest udbredte teknologier i forhold til fjernadgang og skal sammen med de tidligere beskrevne afsnit bruges til at danne grundlaget for en vurdering af den konkrete virksomhed.

4.3.1 VPN

Virtual Private Network(VPN) anvendes til at skabe sikre forbindelser over usikre offentlige netværk. [27] VPN skaber altså et privat netværk mellem to geografisk adskilte punkter også selvom forbindelsen etableres gennem det åbne Internet. Dette er en ganske attraktiv egenskab for virksomheder der ønsker at medarbejderne skal kunne etablere en sikker forbindelse til virksomhedsnetværket uden for virksomhedens område.

VPN kan blive brugt dels til at skabe sikker forbindelse mellem to af virksomhedens geografisk adskilte netværk, men også til at forbinde enkelte enheder til virksomhedens netværk. Dette afsnit vil fokusere på den sidste del.

VPN kan være baseret på flere forskellige protokoller. De mest udbredte er i denne forbindelse IP Security (IPSec) og Secure Socket Layer (SSL). Informationer herom er fundet i [5] samt [30].

4.3.1.1 IPSec

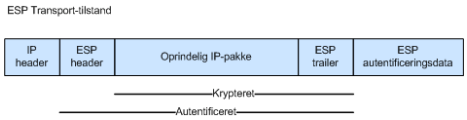
IPSec er en sikkerheds arkitektur for Internet Protocol (IP). Da den er udviklet specielt til IP opererer den på netværks laget (lag 3 i OSI-modellen).

IPSec benytter en række forskellige protokoller, hvoraf de tre vigtigste er IP Authentication Header (AH), IP Encapsulation Security Payload (ESP) hvilket er en kombineret autentificerings- og krypterings protokol samt en nøgleudvekslingsprotokol Internet Key Exchange (IKE).

AH og ESP protokollerne har to fungerende tilstande, Transport-tilstanden og Tunnel-tilstanden. **Transport-tilstand** - Heri beskyttes data i den sendte IP-pakke. I denne tilstand krypterer og autentificerer ESP dataene fra IP-pakkerne,

men ikke IP-headeren. AH autentificerer indholdet og enkelte dele af headeren på IP-pakken.

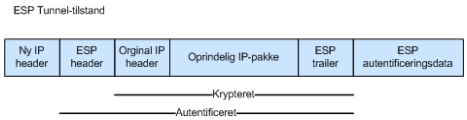
Figur 4.1 viser pakke formatet for IPSec med ESP i transport tilstand



Figur 4.1: Pakkeformat for IPSec ESP i transport tilstand

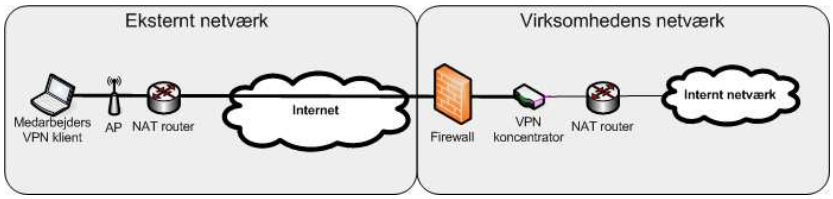
Tunnel-tilstand - Denne yder beskyttelse af hele IP-pakken ved at indkapsle denne i en anden IP-pakke. ESP krypterer og autentificerer i denne tilstand hele den indkapslede pakke. AH autentificerer den indkapslede pakke samt enkelte dele af headeren på den yderste IP pakke. Fordelen ved tunnel-tilstand er at hele den oprindelige pakke bevæger sig i en tunnel, hvorved ingen routere eller andet undervejs kan analysere den indre IP-header.

Figur 4.2 viser pakke formatet for IPSec med ESP i tunnel tilstand



Figur 4.2: Pakkeformat for IPSec ESP i tunnel tilstand

Ved etableringen af en VPN-forbindelse mellem den mobile medarbejders udstyr og virksomhedens netværk, anbefaler NIST [5] en såkaldt host-gateway arkitektur som vist i figur 4.3. Arkitekturen er hensigtsmæssig da virksomheden kan preinstallerer en software-klient på udstyret hvilket gør at alt medarbejderens trafik bliver indkapslet inden det forlader udstyret.



Figur 4.3: Host-gateway arkitektur med NAT

Den kraftige linje i figur 4.3 der går gennem det eksterne netværk og ind til virksomhedens netværk indikerer at kommunikationen er beskyttet af IPSec med ESP i tunnel-tilstand.

I forbindelse med opkobling til virksomhedens netværk fra usikre netværk, vil medarbejderen ofte skulle etablere forbindelsen gennem udbydere, som anvender Network Address Translation (NAT). Dette kan være et problem hvis IPSec anvendes, idet indholdet af den oprindelige IP-pakke er krypteret og dermed også dens portnummer (lag 4 i OSI-modellen). Da NAT-routeren ikke kan aflæse portnummeret kan pakkens modtager ikke bestemmes.
For at løse dette problem i et miljø, hvor virksomheden ikke selv har mulighed for at konfigurere NAT-routeren, anbefales det i NIST [5], at indkapsle IP-pakken i en User Datagram Protocol (UDP)- pakke i tunnel-tilstand i stedet for en IP-pakke som normalt anvendes. Derved får NAT-routeren tilgang til et ukrypteret portnummer. Selve UDP-indkapslingen laves ved oprettelsen af VPN-forbindelsen og udføres gennem IKE (der dog kræver en udvidelse til IKE kaldet IPSec NAT Traversal).

4.3.1.2 SSL

Trafikken mellem medarbejderens mobile udstyr og virksomheden kan også beskyttes af SSL-VPN der opererer et trin højere oppe i OSI-modellen, på transport laget (lag 4), end IPSec. SSL-VPN beskytter ved at autentificere og kryptere trafikken mellem udstyret og virksomheden. [30]

SSL bruges oftest til at tilbyde sikkerhed for Hypertext Transfer Protocol (HTTP) og tillade sikker kommunikation over Internettet. Dette kaldes HTTP over SSL eller Sikker HTTP (HTTPS) og understøttes i dag af næsten alle browsere.

Da mange standardapplikationer som f.eks. browser og emailklienter understøtter SSL, kan det være en attraktiv løsning for virksomheden at benytte denne form for VPN.

SSL-VPN kræver ikke en særligt VPN klient på medarbejderens udstyr, hvilket både har økonomiske og administrative fordele (hvis virksomhedens applikationer understøtter SSL). I forhold til IPSec vil der kunne spares mange penge i form af et væsentligt mindre behov for support, vedligeholdelse og installation. Dog kan det hurtigt blive ret dyrt for en virksomhed, hvis der opstår et behov for SSL understøttelse i specialsoftware, da der så skal udvikles specielle plugins.[24]

4.3.1.3 IPSec-VPN eller SSL-VPN?

En VPN forbindelse kan i værste fald udgøre en bagdør til virksomhedens netværk. *Split-tunneling* udgør her en væsentlig trussel, da klienten udover VPN forbindelsen også samtidig har en anden aktiv forbindelse åben. Fordelen herved er, at det kan øge forbindelseshastigheden da trafik som f.eks. genereres af en browser ikke behøver at gå gennem virksomhedens. Ulempen er blot at klienten

derved vil være tilgængelig direkte fra Internettet, og en kompromitteret klient kan fungere som en direkte vej fra Internettet og ind i virksomhedens interne netværk.

Forskellen mellem IPSec og SSL, ligger først og fremmest i hvilke lag de to VPN teknologier opererer på og derved hvilken sikkerhed de tilbyder. Da SSL operere på transport laget er IP headeren fra netværks laget ikke krypteret som ved IPSec. Generelt giver kryptering på et lavere lag en bedre beskyttelse af kommunikationen.

4.3.2 Autentificering

Det er vigtigt for en virksomhed at kunne autentificere sine medarbejdere, så alle uautoriserede forhindres adgang til eksempelvis netværket. Password regnes i denne forbindelse oftest for at være det svageste led i kæden også selvom der benyttes sikre password. Virksomheden kan ikke være sikker på at medarbejderne ikke skriver passwordet ned på papir eller at det måske bliver opfanget af en keylogger[7].

Autentificering er en proces hvor medarbejderen overfor systemet verificerer at det virkelig er vedkomne der vil have adgang og ikke en der bare udgiver sig for at være medarbejderen. Der er typisk tre måder en medarbejder kan autentificere sig på overfor systemet:

- Med noget medarbejderen ved - Typisk et password eller anden information som er sandsynlig at medarbejderen ved.
- Med noget medarbejderen har - Det kan f.eks. være et magnetkort, et smart-card, USB-token eller lignende.
- Med noget medarbejderen er - Det kan f.eks. være i form af fingeraftryk, stemmeaktivering, iris scanning, osv.

Hvis to, eller alle tre måder bliver brugt i en kombination, vil det være betydeligt sværere for en angriber at få adgang til systemet. For at autentificeringen kan betragtes som stærk, skal mindst to af de tre måder bruges i en kombination.

Nogle af de mest udbredte stærke autentificerings metoder vil blive beskrevet i dette afsnit.

[7] En keylogger opfanger i al hemmelighed, alle tastetryk der foretages på pågældendes udstyr. Kan forekomme enten i form af software eller som hardware.

4.3.2.1 Engangs-Password

En velkendt metode er brug af engangs-password eller på engelsk One-time password (OTP). Ved denne metode bliver hver medarbejder udstyret med en enhed der kan generere et password der kun er gyldigt i et begrænset tidsrum, f.eks. 1 minut. Det betyder at serveren er synkroniseret med denne enhed.

Denne metode kan betragtes som værende en stærk autentificering, da den kombinere et password (noget medarbejderen ved) med en enhed som medarbejderen må være i besiddelse af (noget som medarbejderen har), heraf en to-faktor autentificeringsmetode.

Et velkendt eksempel herpå er SecurID fra RSA Security [8]. Et eksempel på en autentificerings enhed fra RSA Security ses i figur 4.4

Figur 4.4: Billede af RSA SecurID autentificerings enheder

En ulempe ved OTP i forhold til den mobile medarbejder er dog at løsningen kræver at medarbejderen har forbindelse til virksomhedens OTP-server for at kunne gennemføre autentificeringen. Denne betingelse er kun opfyldt når medarbejderen opretter forbindelse til virksomhedens netværk og altså ikke når medarbejderen f.eks. forsøger at få adgang til selve udstyret.

Ved brug af certifikater, er der ikke den samme grad af afhængighed af synkronisering og derved opnås den fordel, at også adgangen til selve udstyret kan ske på med stærk autentificering.

4.3.2.2 Certifikater

Certifikater er en stærk autentificerings metode, hvor certifikatet (noget medarbejderen har) samt password til den private nøgle (noget medarbejderen ved) benyttes til at verificere medarbejderens identitet over for systemet.

Et certifikat og dets private nøgle kan hos medarbejderen være lagret på selve udstyret eller på en ekstern enhed. Fordelen ved at lagre det på en ekstern enhed

[8] Mere information kan findes på: http://www.rsa.com/node.aspx?id=1156

er, at den private nøgle ikke kan opsnappes hvis udstyret bliver kompromitteret.

Et eksempel på en ekstern enhed hvor certifikatet kunne lagres er, EToken PRO USB[9] fra Aladdin. Denne USB token understøtter 2048 bit RSA til autentificering og signering samt 3DES og SHA1. Enheden kan ses i figur 4.5

Figur 4.5: Aladdin EToken PRO USB

EToken generere selv nøgleparret til certifikatet, og dens private nøgle forlader derfor ikke det beskyttede miljø i enheden. Autentificeringen og signeringen udføres på selve enheden ved brug af de understøttede algoritmer.
En anden fordel med denne EToken er at en administrator kan bestemme, at maskinen skal låses hvis enheden tages ud af maskinen. En medarbejder behøver altså ikke logge ud men blot huske sin EToken når maskinen forlades.

4.3.3 Kryptering

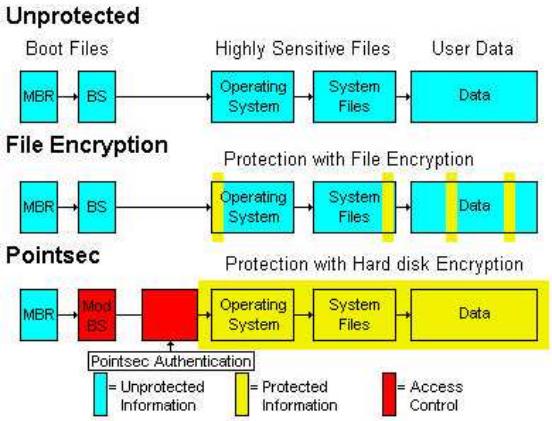
Da der er ringe fysisk sikkerhed forbundet med mobile medarbejders udstyr, må virksomheden overveje hvordan fortroligt data kan beskyttes i tilfælde af at udstyret bortkommer.
Enten må fortroligt data slet ikke lagres på udstyret og hvis det er nødvendigt kun tillade at kunne hente det frem og vise på skærmen, eller også skal udstyret sikres med diskkryptering. For en virksomhed vil diskkryptering altid være en god ide.

Der findes primært to typer af diskkryptering. Den ene opretter en krypteret folder som tilgås i form af et ekstra drev. Den anden type krypterer hele det fysiske drev inkl. operativ systemet(OS). En fuld kryptering af hele det fysiske drev har mange fordele i forhold til den fil- eller folder-baserede kryptering. En af fordelene er at mange applikationer opretter midlertidige filer og backups i andre foldere end der, hvor den benyttede fil åbnes. Det betyder, at ved brug af foldere kan almindelig anvendelse betyde at fortrolige data alligevel lagres ubeskyttet. Ved fuld disk kryptering vil samtlige data syne krypteret, inkl. backup og system filer. En anden fordel ved fuld diskkryptering er at krypteringen sker sektor for sektor, hvilket betyder at selv store filer kan dekrypteres relativt hurtigt i forhold til den folder baserede kryptering. [21]

[9] Mere information kan findes på: http://www.aladdin.com/etoken/devices/pro-usb.aspx

4.3.3.1 PointSec

CheckPoint's Pointsec PC 4.3 tilbyder denne form for fuld diskkryptering. Programmet anvender 3DES (168 bits) og AES (128, 192, 256 bits) kryptering. I forbindelse med adgang til enheden skal medarbejderen autentificeres inden OS startes. Derefter fungerer Pointsec transparent for brugeren ved at kryptere og dekryptere data, som skrives og læses.[22]
Autentificeringen kan baseres på certifikater placeret på smart-cards. Figur 4.6 viser hvordan Pointsec operere i forhold til andre krypteringsmetoder.



Figur 4.6: Pointsec. Figur fra [21]

4.3.4 Central administration

Som bekendt kører alt hardware og software i versioner, sådan at det fortløbende kan rettes ind og forbedres funktions- og sikkerhedsmæssigt. For at opretholde sikkerhedsniveauet på udstyret, er det nødvendigt at opdatere alle sikkerhedsrelevante programmer engang imellem.

Et generelt problem er specielt at visse ondsindede personer udnytter store producenters log til at finde huller i software. Da det typisk tager nogle dage for selv mere erfarne computerbrugere, fra en opdatering bliver udsendt til den bliver installeret på deres computere, kan disse personer udnytte denne tid til at lave et angreb specificeret ud fra den log der beskriver rettelsen af programmet. Dette taler især for automatiske opdateringer som de fleste programmer har, sådan at deres versioner kan blive opdateret så hurtigt som muligt.

Fordi den mobile medarbejders udstyr, i en virksomhed, er så udsat et angrebspunkt, må der stilles store krav til den løbende opdatering og konfiguration af

OS, VPN-klient, Antivirus programmer, osv. Dermed kan virksomheden sikre, at udstyret løbende efterlever sikkerhedspolitikken.

Med en centraliseret administration kan virksomheden konfigurere og opdatere medarbejderens udstyr uden medarbejderens indblanding. Dette har mange fordele blandt andet så behøver en administrator ikke fysisk adgang til udstyret, da det hele foregår over netværksforbindelsen. Dette sikre også at ændringer og opdateringer hurtigt kommer ud til samtlige medarbejderes udstyr og derved sikre ens sikkerhedsniveau på alt udstyr.

Central administration vil typisk foregå ved, at applikationen som skal styres, har tilknyttet en administrationsserver der kan indeholde konfigurationer, opdateringer, osv. som klienten skal imødekomme. Ændringen vil typisk blive installeret på medarbejderens udstyr sent om aftenen eller tidligt næste morgen, så medarbejderen ikke oplever forstyrrelser under det daglige arbejde. Er medarbejderens udstyr ikke forbundet til virksomhedens netværk på opdatering tidspunktet vil ændringen blot blive installeret næste gang medarbejderen forsøger at koble sig op på virksomhedens netværk.

4.3.5 Firewall

En firewall er et vigtigt redskab når netværk og udstyr skal sikres mod angreb. En firewall fungere som et filter, der tjekker både indgående og udgående trafik, og er beregnet til at blokere for alle de netværksporte der ikke benyttes.
Brugen af firewall forudsætter altså at virksomheden har kontrol over de tilgange der er til netværket.

Med etableringen af mobile medarbejdere er det ikke længere nok for virksomheden at opsætte en firewall mellem virksomhedens netværk og Internettet. Da det mobile udstyr er mere åbne overfor angreb, bl.a. på grund af deres trådløse teknologi kan tilgås direkte - både i og uden for virksomheden. Den eneste måde at håndtere det åbne scenarie er at etablere personlige firewalls på hver enkelt klient.

Der findes fire typer af firewalls.[30] De adskiller sig fra hinanden ved at operere på forskellige lag i OSI-modellen. Generelt kan man sige at jo højere lag firewall'en operere på desto bedre bliver beslutningsgrundlaget til filtreringen, i og med at en større del af trafikken kan analyseres.
Set fra et sikkerhedsmæssigt synspunkt er det bedre at sortere så meget uønsket trafik fra som muligt på lavest mulige lag, idet en pakke som stoppes på lag 3 aldrig vil komme til at angribe tjenester der operere på et højere lag. Det er dog heller ikke muligt at stoppe alt ondsindet trafik på de laveste lag og derfor nødvendigt også at have firewall's der operere på højere lag.
De fire forskellige typer firewall's er beskrevet i det følgende:

4.3.5.1 Packet filtering

Den mest basale type af firewall kaldes for en packet filtering firewall. Denne analyserer trafikken på netværkslaget (lag 3) i OSI-modellen. Her er det oplysninger som eksempelvis afsender, modtageradresse og portnummer der er tilgængelige. Typisk vil der være opstillet et sæt regler, som indkommende pakker scannes op imod. Disse regelsæt vil desuden være tilknyttet en standardregel. En standardregel kan være f.eks. 'forbyd alt som ikke tillades' eller en noget svagere 'tillad alt som ikke forbydes'. Den sidstnævnte kan, ved forglemmelser, fører til sikkerhedshuller der ikke nødvendigvis opdages mens den første er den sikreste af de to, for her vil eventuelle nye trusler der benytter andre porte automatisk blive stoppet.

4.3.5.2 Application-level filtering

En application-level firewall (ALF) (også kaldet en proxy) operere på applikationslaget (lag 7), hvor den i modsætning til packet filtering kan analysere hele indholdet af pakkerne. Det betyder at ALF'en kender applikationens protokol (eksempelvis HTTP, FTP, osv.) og kan derved bestemme hvilken type protokoltrafik der skal tillades og hvad der skal sorteres fra.
En anden fordel ved denne type firewall er at den kan forstå indholdet i den enkelte protokol, eksempelvis kender den forskellen mellem HTTP-get og HTTP-put, det betyder at ALF'en kan kontrollere at de data, som sendes tilbage, kun indeholder den type data som medarbejderen havde forespurgt.

4.3.5.3 Circuit-level gateway

Circuit-level gateways (CLG) operere på transportlaget (lag 4). Denne type firewall fungerer ved at den opretter forbindelse mellem den interne klient og CLG'en samt mellem CLG'en og den eksterne klient eller server. Når begge forbindelser er oprettet videresendes trafik mellem de to segmenter. Det betyder at det reelt kun er CLG'ens adresse der er tilgængelig på det eksterne netværk og selvom indholdet ikke bliver undersøgt bliver selve forbindelsen dog valideret ved at der kun tillades nogle trafiktyper at slippe igennem. Da det er på transportlaget filtreringen sker, kan det gøres på IP-adresser, portnumre og protokoltyper.

4.3.5.4 Stateful inspection firewall

Stateful inspection firewall er en kombination af de tre tidligere typer. Den opererer på flere lag, med filtrering på netværkslaget, validering på transportlaget samt inspicerer på sessionlaget.[3]

Denne type firewall holder desuden også styr på hvilke forbindelser pakkerne tilhører og hvilken tilstand de er i. Eksempelvis vil den første pakke i enhver ny forbindelse ved TCP-protokollen, have et SYN-flag sat og et ACK-flag fjernet. Firewall'en ved derved at denne type pakker er startpakker og alle pakker i samme serie er efterfølgende pakker. Kommer startpakken fra det interne netværk, må det altså betyde, at en klient indefra forsøger at etablere en forbindelse ud mod Internettet. Tillades dette vil firewall'en huske forbindelsesinformationerne (IP-adresse, portnummer, osv.). Skulle en efterfølgende pakke fra Internettet komme til firewall'en vil dennes forbindelsesinformationer blive sammenholdt med de informationer firewall'en har om eksisterende godkendte forbindelser. Matcher pakken en godkendt forbindelse for den derved lov at passere igennem og ellers bliver den stoppet her.

4.3.6 Antivirus

Virus er den hyppigst forekommende sikkerhedstrussel mod udstyr forbundet til Internettet. Udstyret bør derfor være ordentligt beskyttet herimod.
Antivirusprogrammer fungerer ved at holde de filer, der læses og skrives, op mod en database med virusdefinitioner. Hver indgang i databasen specificerer en række mønstre som kendetegner den pågældende virus, hvilket er nok til at programmet kan genkende virusen og få den stoppet.
Opdatering af definitionerne er vigtig, da der dagligt dukker nye vira op. Opdateringerne kan som regel foretages manuelt eller ske automatisk. Det vil her være en god ide for virksomheder at vælge antivirusprogrammer der kan opdateres fra centralt sted. Dette vil medfører at ansvaret for vedligeholdelsen bliver flyttet fra medarbejderen til virksomheden selv.

4.3.7 Adware og Spyware

Idet der findes så mange gratis programmer der kan hentes og installeres fra Internettet, er der også begyndt at komme megen Adware [28] og Spyware [29].

Disse er små ekstraprogrammer der følger med et installeret program og derved installerer uventet indhold ud over det brugeren har bedt om.

Ved Adware bliver et ekstra program installeret sammen med det der installeres, typisk som en slags annoncering, der tjener penge ind til det originale produkts ejere. Problemet med Adware er at det ofte tager sig i form af Spyware med hvilket brugerens informationer og aktioner bliver overvåget og optaget ulovligt.

Spyware's effekt minder om en virus, men adskiller sig ved ikke at være selvreplicerende. Hvor virus vil benytte alle tilgængelige medier (e-mail, WLAN, osv.) til at sprede sig selv, vil spyware ofte virke modsat og holde sig til den inficerede klient.

En anden forskel er at spyware forsøger at skjule sin tilstedeværelse, hvorimod en virus oftest hurtigt bliver opdaget, da den inficerede klient typisk vil begynde at opfører sig unormalt.

I forbindelse med mobilt udstyr er det vigtigt at have antispywareprogrammer installeret. Programmet fungerer ligesom med antivirusprogrammer ved at analysere data og holde det op imod en database med spywaredefinitioner. Mange antivirusprogrammer har i dag indbygget antispyware faciliteter.

4.3.8 Opsummering

I dette kapitel er der gennemgået en række af de mest udbredte teknologier, der kan hjælpe til at gøre den mobile medarbejders udstyr sikkert nok til at det på en sikker og forsvarlig måde kan anvendes uden for virksomhedens kontrol og herfra forbinde sig til virksomhedens netværk.
Kapitlet er ikke en komplet liste over de metoder og teknologier der kan anvendes til mobilt udstyr, listen skal ses som en række løsningsforslag til udbedringen af de tidligere beskrevne sikkerhedsmæssige problemer der er tilknyttet denne form for mobilt arbejde.

- VPN - Brugen af VPN leverer autentificering og kryptering på netværks laget (lag 3). Dette kan benyttes til fjernadgang fra det mobile udstyr til virksomhedens netværk.
- Autentificering - Stærk autentificering kan forhindre problemer med passwords, som opsnappes eller på anden måde brydes. Certifikater vurderes som den bedste løsning i forbindelse med fjernadgang.
- Kryptering - Brugen af diskkryptering er vigtig og kan forhindre, at data på mistet udstyr kan aflæses eller modificeres.
- Central administration - Antallet af mobile medarbejdere behøver ikke være særligt stort før det hurtigt kan blive uoverskueligt med en decentral styring. Det er i den forbindelse vigtigt at sammensætte produktporteføljen så alle væsentlige applikationer på det mobile udstyr kan administreres centralt.
- Firewall - Brugen af firewalls er et vigtigt supplement til sikkerheden. Der er gennemgået fire typer af firewalls og i forbindelse med implementering er det nødvendigt at overveje fordele og ulemper ved hver af de fire typer. I forbindelse med fjernadgang fra det mobile udstyr, er det vigtigt at der udover firewalls på virksomhedens hovedtilgange, også installeres personlige firewalls på selve udstyret.
- Antivirus - Beskyttelse mod antivirus er også en central del i sikkerheden, og antivirusprogrammer bør installeres på alle arbejdsstationer og servere.

- Adware og Spyware - Disse adskiller sig fra virus i deres virkemåde, og derfor må særlige programmer til beskyttelse mod disse anvendes.

Indtil nu er sikkerhedsproblemer i relation til specifikke angreb blevet beskrevet, men mange sikkerhedsproblemer har ofte rod i den måde medarbejderen benytter sit udstyr. Medarbejderne kan, hvis de ikke er bevidste nok, komme til at installere ondsindet software, eller på anden måde selv forårsage sikkerhedsproblemer. Dette gør at sikkerhedsforebyggende software ikke altid kan fange problemet.

På grund af Internettets store kommunikationsstyrke er det let at distribuere fælder, til f.eks. at lokke medarbejderne til at installere en virus på deres computer. Disse problemer skyldes til dels medarbejdernes egen uvidenhed, ved at de selv ubevidst kommer til at tillade ondsindet software på udstyret. I disse situationer vil sikkerhedsprogrammer som antivirusprogrammer ikke altid være i stand til at opdage truslen, da truslen så at sige selv er blevet 'lukket ind'. Netop derfor er det vigtigt at medarbejderne er bevidste overfor de trusler der findes og tager sig de forbehold der skal til for at bevare sikkerheden på sit udstyr.

Kapitel 5

Vurdering af virksomheden

I dette kapitel gives en vurdering af sikkerheden forbundet med brug af virksomhedens mobile udstyr samt forslag til eventuelle forbedringer. Der vil bl.a. blive set på beslutningsgrundlaget, sikkerheden i selve udstyret samt opkoblingsmuligheder til virksomhedens netværk.

Vurderingen sker på baggrund af samtaler med relevante medarbejdere, muligheden for selv at teste noget af udstyret (en laptop), samt i relation til de foregående kapitler.

Vurderingen af sikkerheden bygges udelukkende på baggrund af de tekniske løsninger der er valgt, holdt op i mod ledelsens beslutninger og udstukkede retningslinjer på området. En vurdering af medarbejdernes bevidsthed omkring relevante sikkerhedsmæssige problemstillinger er altså ikke inkluderet i denne vurdering. En nærmere behandling af dette område vil komme i de efterfølgende kapitler.

5.1 Beslutningsgrundlag

En mindst lige så interessant vinkel på valg af tekniske løsninger i en større virksomhed, er måden og det grundlag beslutningerne bliver truffet ud fra.

Idet størrelsen og kompleksiteten af tekniske løsninger kan være af større eller mindre grad er der ikke kun én bestemt proces for hvordan beslutningerne bliver

truffet.
Men generelt i virksomheden gælder, at der ønskes at strømline systemerne og ved valg af løsninger vil der derfor blive involveret en række 'arkitekter', som skal tilstræbe, at der over tid udformes løsninger der både er ensartede, effektive, sikre systemer der er billige i drift, og som virkelig understøtter (ensartede) forretningsprocesser.
Inden for de rammer som arkitekterne (og navnlig den forretningsmæssige sponsor) opstiller skal det til formålet nedsatte projekt vælge den rigtige tekniske løsning.

Som beskrevet indledningsvis har virksomheden valgt ikke at tillade hjemmearbejdspladser. Behovet for at kunne få adgang til virksomhedens netværk uden for virksomhedens område er der dog stadig. Derfor har virksomheden besluttet at lave en såkaldt fjernadgangsløsning.

De involverede parter i forbindelse med fjernadgangsløsningen i virksomheden listes her.

- Group Operational Risk Management (GORM)[1] har udstukket de helt overordnede regler for hvad der er tilladt i forbindelse med fjernadgang.
- IT Security definerer de tekniske kontroller, som skal tages i anvendelse, f.eks. VPN, logon baseret på USB-stick og password, kryptering af harddisk osv.
- Det nedsatte projekt finder de praktiske løsninger (i samarbejde med IT Security, Tekniske arkitekter, udviklere, osv.) og har også defineret og igangsat de nødvendige procedurer.

I en beslutningsproces er det naturligt også at overveje de økonomiske aspekter i løsningsmodellen. Som i alle andre virksomheder er det ikke altid lige nemt at få tildelt økonomiske ressourcer til nye projekter. Derfor sker det engang imellem at tiden og pengene til at undersøge markedet for de bedste produkter ikke er til stede. Derved vil beslutningerne ofte falde ud fra hvilke produkter der er billigst og stadig tilbyder den ønskede funktionalitet og sikkerhed. Dette kan medføre løsninger der er sammensat af mange forskellige produkter og derved er den samlede løsning ofte mindre fleksibel overfor nye udviklingsmuligheder, samtidig med at det giver et øget pres på eksempelvis supportere der skal kende mange forskellige produkter fremfor eventuelt ét stort produkt.

Virksomheden har valgt at de nedskrevne informationssikkerhedspolitikker samt sikkerhedshåndbøger skal være til rådighed for medarbejderne på virksomhedens

[1] Group Operational Risk Management har ansvaret for bl.a. at udvikle og vedligeholde en struktur til håndtering af operationellen risici, og sørge for strukturen bliver implementeret ud i alle forgreninger af virksomheden. GORM er også dem med ansvaret for at have kompetencer og support for informationssikkerheden i virksomheden. GORM rapporterer direkte til Group Executive Management og bestyrrelsen i virksomheden.

intranet. Da alt relevant information om sikkerheden er tilgængelig på intranettet har man besluttet, at det ikke er nødvendigt med eksempelvis uddannelsesforløb eller lignende for, at sikre medarbejdernes forståelse for sikkerheden.

5.2 Udstyr

I virksomheden udgør det tilladte mobile udstyr hhv. en laptop og en mobiltelefon. Alt andet udstyr (som eksempelvis PDA'er og smartphones) supporteres ikke af virksomheden.
En af udfordringerne med det mobile udstyr er, som tidligere beskrevet, at sikre udstyret mod at uautoriserede personer kan få adgang til evt. fortroligt data og samtidig ønskes udstyret også sikret mod eksempelvis at blive inficeret med virus eller på anden måde kunne blive kompromitteret.
I dette afsnit beskrives nogle af de væsentlige løsninger der er valgt til at sikre udstyret med.

5.2.1 Laptop

Medarbejderen har med laptop'en mulighed for at koble sig op på virksomhedens netværk både i og uden for virksomheden. Der er ved de to opkoblingsmuligheder tale om to meget forskellige sikkerhedsmæssige scenarier. Laptop'en har derfor ligeledes to forskellige tilstande: en 'Office'-tilstand og en 'Mobil'-tilstand . Laptop'en vil automatisk skifte tilstand alt efter om den er tilsluttet virksomhedens netværk. I 'Office'-tilstanden er laptop'en sikret på samme måde som en almindelig arbejdstation (dvs. beskyttet af virksomhedens firewalls, osv.). I 'Mobil'-tilstand vil en sikker VPN forbindelse forsøges oprettet til virksomhedens netværk. Samtidig vil VPN gateway'en mere eller mindre blokerer for alle servere på IP niveau. Det betyder reelt set at det er den eneste mulige kommunikation ud af laptop'en.

I det efterfølgende forudsættes det at laptop'en befinder sig i 'Mobil'-tilstand.

Laptop'en er beskyttet af fuld harddisk kryptering. Programmet Pointsec, se beskrivelse af programmet i afsnit 4.3.3.1, sørger for at alt data er krypteret og at medarbejderen autentificeres inden OS startes. Denne form for beskyttelse er den mest effektive hvis udstyret skulle blive stjålet.

Derudover er den også beskyttet med firewalls. Der benyttes to firewalls: Microsoft Windows XP's indbyggede firewall og Secgo Crypto IP[2] VPN firewall.

[2]For yderligere information om produktet se http://www.secgo.com/index.php?page=products/oem/ciptoolkit

Symantec Antivirus[3] beskytter laptop'en mod virus angreb. Programmet er styret via central administration der sørger for at holde programmet opdateret. I øjeblikket er det dog ikke muligt at opdatere via fjernadgang, så laptop'en får først opdateret antivirusprogrammet når denne forbindes i 'Office'-tilstanden, altså inde fra selve virksomheden. Dette gælder generelt for alle opdateringer til laptop'en.

Bluetooth driver og software er fjernet fra laptop'en. Hvis der skal oprettes forbindelse til et netværk gennem en mobiltelefon skal dette ske gennem den infrarøde port.

Som almindelig bruger, dvs. med begrænsede rettigheder, af laptop'en er der ikke mulighed for at installerer ting på laptop'en. Dette mindsker risikoen for at eventuelle ondsindede programmer vil blive installeret. Programmer der er godkendt af virksomheden og som den pågældende medarbejder har rettigheder til at kører, kan dog via en særskilt applikation hentes ned på laptop'en og installeres. Enkelte medarbejdere kan dog få tildelt lokal-administrator rettigheder[4] på laptop'en og er derved selv ansvarlige for at kunarbejdsrelevante programmer må installeres.

På grund af det store udbud af VBA makroer i virksomheden, har man besluttet at sænke makro-sikkerhedsniveauet til 'mellem', indtil alle virksomhedens VBA makroer er blevet signeret. Det er målet på sigt, at sætte makro-sikkerhedsniveauet på 'højest' og derved udelukke den potentielle risiko for at kendte VBA sårbarheder skal kunne blive udnyttet på maskinerne.

Der er ingen restriktioner ved brug af USB-porte. Alle former for USB-stick kan tilsluttes. Det åbner op for muligheden for at en medarbejder kan komme til, via et USB memory stick, at indlæse skadelig kode eller programfiler. Det er også uhensigtsmæssigt i forhold til at følsomme data kan lægges ned på et memory stick og tages med udenfor virksomhedens område.

En opsummering af sikkerhedsmiljøet på laptop'en:

- Laptop'en kan kører i to tilstande: Office-tilstand og Mobil-tilstand
- Fuld harddisk kryptering ved Pointsec - Kræver autentificering ved opstart inden OS indlæses.
- Lokale firewalls (Microsoft Windows XP + Secgo's VPN firewall)
- Antivirus (Symantec)
- Bluetooth ikke tilladt

[3] For yderligere information om produktet se http://www.symantec.com/en/uk/enterprise/products/index.jsp

[4] For at kunne blive tildelt lokal administrator rettigheder kræver det udover et relevant arbejdsmæssigt behov også godkendelse fra nærmeste leder.

- Begrænsede brugerrettigheder. Kan ikke installerer ikke-godkendte programmer selv.
- Sikkerhedsniveauet for VBA makroer er sat til 'mellem' - hvilket potentielt kan åbne op for eksekveringen af makroer der indeholder skadelig kode.
- Det er ikke muligt at opdatere applikationer centralt, dvs. at applikationer som eksempelvis antivirusprogrammet først kan blive opdateret når medarbejderen tager laptop'en med ind i virksomheden og tilslutter den det interne netværk derfra.
- Åbne USB-porte - kan udgøre en sikkerhedsmæssig risiko for virksomheden.

5.2.2 Mobiltelefon

Medarbejdere der har behov for at koble sig op til virksomhedens netværk fra steder hvor der ikke nødvendigvis er en bredbånds-forbindelse (LAN / WLAN) til rådighed, har muligheden for at få en mobiltelefon så forbindelsen kan oprettes via GPRS eller EDGE gennem denne.

Der er i virksomheden, af supportmæssige grunde, kun godkendt én mobiltelefon der kan opfylde de krav der er stillet fra GORM og IT Security. Mobiltelefonen skal kunne:

- Synkroniserer kalender, email, noter, osv. med MS Outlook.
- Kunne oprette infrarød forbindelse til andre enheder.
- Telefonen må ikke indeholde et kamera

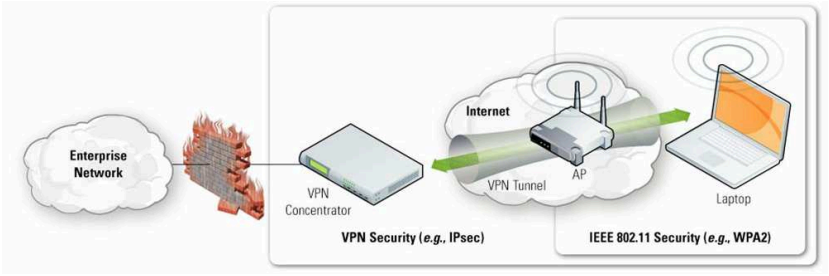
Tiltænker support for brug af 3G mobiltelefoner samt mulighed for brug af Bluetooth, hvilket vil gøre forbindelsen hurtigere (3G) og sikre en nemmere og mere stabil løsning i forbindelsen mellem mobiltelefonen og laptop'en.

Det har ikke været muligt at finde ud af om eller hvordan mobiltelefonen er sikret.

5.3 Opkobling til virksomhedens netværk

Virksomheden har som sagt valgt ikke at tillade såkaldte hjemmearbejdspladser, men har i stedet lavet en løsning hvor laptops har mulighed via et offentligt netværk at koble sig op på virksomhedens netværk og få en begrænset adgang

til enkelte applikationer; e-mail klient, Intranet, Internet gennem den sikrede VPN gateway, samt personlige drev på netværket.



Figur 5.1: Eksempel på opkobling via fjerndadgang

Der er altså tilladt adgang til virksomheden via en sikker VPN-klient ved brug af forskellige slags forbindelser over Internettet. Internet forbindelsen kan etableres på en af følgende måder:

- gennem en bredbåndsforbindelse som ADSL, gælder både for 'kablet' (Ethernet) og trådløst (WLAN) netværk.
- gennem Internet adgang på offentlige steder, såkaldte hot spots, som for eksempel konferencerum, lufthavne, hoteller, osv. Speciel applikation er udviklet til i et begrænset tidsrum at give tilladelse til via Internet Explorer at tilgå de tilhørende betalingssider.
- gennem GSM/GPRS/EDGE protokol, med den af virksomheden godkendte mobiltelefon.
- gennem 3G på sigt.

Virksomheden har ikke kontrol over sikkerheden ved f.eks. et privat opstillet trådløst netværk, der i princippet kan være helt uden beskyttelse og åbent for enhver eller ved offentlige netværk.
Der er derfor opstillet en række sikkerhedsforanstaltninger til at sikre, at forbindelsen til virksomhedens netværk kan ske på sikker vis.

Det er muligt via en sikker VPN forbindelse (gennem IPSec) at tilgå virksomhedens netværk. Secgo Crypto IP levere denne sikre VPN forbindelse, samtidig med at den benytter en to-faktor autentificering.
Så når laptop'en skifter til 'Mobil'-tilstand og forbindes til et af ovennævnte typer netværk, bliver medarbejderen bedt om at autentificere sig overfor Secgo Crypto IP så en sikker VPN forbindelse kan oprettes og alle andre forbindelses muligheder slås fra.

Selve to-faktor autentificeringen sker ved hjælp af et certifikat der er placeret på en Aladdin, EToken PRO USB enhed, der henvises til afsnit 4.3.2.2 for mere information om denne. Medarbejderen skal ved autentificeringen indsætte EToken i en USB-port og indtaste et password.

I og med at laptop'en er tilstrækkeligt beskyttet er der intet til hindrer for brug af trådløst netværk når fjernforbindelse til virksomheden skal etableres. Dette vil gøre laptop'en mere anvendelig i eksempelvis lufthavne, hoteller, osv. hvor offentlige trådløse netværk (Hot spots) kan benyttes.

En opsummering af de sikre forbindelses løsninger:

- Secgo Crypto IP - IPSec VPN forbindelse (Sikker VPN forbindelse)
- To-faktor autentificering (Certifikat + Password)
- Applikation til hot-spot logons (i et kort tisdrum tillades al Internet trafik)

5.4 Forslag til forbedringer

Selvom der generelt er tale om en meget sikker løsning for fjernadgang, er der alligevel en række punkter der kan forbedres, set fra et sikkerhedsmæssigt synspunkt.

- Det bør være muligt at opdatering applikationer gennem fjernadgangen.
- USB-porte bør lukkes, så kun tilladte medier kan tilsluttes der igennem.
- Sikkerhedsniveauet ved VBA macroer skal hurtigst muligt ændres til 'høj' - så medarbejderen ikke kommer til at eksekvere en makro indeholdende potentielt skadende kode.
- I stedet for mange forskellige produkter bør der tilstræbes én større samlet produktpakke (eksempelvis via en Cisco løsning eller andre). Mange forskellige produkter stiller store krav til de personer der skal udvikle, vedligeholde og supportere løsningerne samtidig med at der er risiko for mindre fleksibel udviklingsmuligheder fremover.
- Mulighed for at kunne bruge MS Outlook Web Access
- Bluetooth og 3G bør tillades til en hurtigere og bedre kommunikation dels mellem laptop og mobiltelefon men også mellem udstyret og virksomhedens netværk.
- Flere og flere benytter sig i dag af instant messenger programmer, som Live Messenger. Dette kan være et muligt behov på sigt og bør derfor overvejes når nye løsninger kommer frem.

Yderligere forbedringer kunne ske gennem sikkerhedsbevidstheds programmer. Jo mere opmærksomme medarbejderne er på problemer, jo mere vågne de er, jo svære er det for en angriber at udnytte eksempelvis Social Engineering uden at det opdages. Sikkerhedsbevidsthedsprogrammerne bør være en del af dagligdagen, metoderne bør ændre sig løbende hen over året, nye ting bør tages i drift for at medarbejderne ikke vender sig til budskaberne, så de blot bliver en del af den daglige støj.

5.5 Opsummering

Grunden til at der ikke er foreslået og beskrevet mange nye alternativer i forhold til det implementerede i virksomheden, er at jeg finder det grundlæggende sikkerheds niveau i virksomheden tilstrækkeligt. Fundamentet på den tekniske side synes at være ganske god.

Laptop'en er sikret med harddisk kryptering der kræver autentificering inden OS indlæses. Derudover er laptop'en sikret med både lokale firewalls og antivirusprogram. Bluetooth drivere og tilhørende software er fjernet fra laptop'en og kan derfor ikke benyttes.
Der påpeges dog en række uhensigtsmæssigheder, som at det helt er op til medarbejderen om en VBA makro skal køres (sikkerhedsniveauet er sat til 'mellem'), USB-porten er også helt åben hvorfra skadelige programmer/kode kan indlæses fra, samtidig med at det åbner op for at en medarbejder kan lægge følsomme data ned på et USB memory stick og uhindret tage det med uden for virksomheden.
En sidste vigtig uhensigtsmæssighed er at program opdateringer ikke er mulig gennem fjernadgangsløsningen.

Virksomheden har valgt at sikre udstyret med mange enkeltstående produkter til at løse et specifikt formål. En bedre løsning på sigt vil nok være at finde ét produkt der kan opfylde alle sikkerhedskravene.

Kapitel 6

Sikkerhedsbevidsthed

Formålet med dette kapitel er at sætte fokus på vindingen ved at bruge informationssikkerhedsbevidstheds kampagner og programmer i virksomheder.
Kapitlet beskriver først lidt generelt om IT sikkerhedsbevidsthed, hvad er det og hvorfor er det nødvendigt for en virksomhed at sætte fokus på det. Herefter beskrives nogle overordnede retningslinjer for udviklingen af et IT sikkerhedsbevidsthedsprogram hvortil der gives forslag til en række bevidsthedsfremmende tekniker der kan hjælpe med til at få et budskab ud til medarbejderne. Der introduceres også i kapitlet en ny type brugerundersøgelse, interaktive spørgeskemaer, ud fra hypotesen at mange svarpersoner til almindelige tekstbaserede spørgeskemaer, relateret til IT sikkerhedsbevidsthed, ikke forstår spørgsmål der til tider omhandler meget komplekse tekniske begreber og derved risikere den efterfølgende analyse at blive noget misvisende i forhold til det reelle niveau.

Som de foregående kapitler har beskrevet det, kan man benytte mange tekniske løsninger for at sikre virksomhedens udstyr bedst muligt. Dette er dog ikke i alle tilfælde nok. For i mere end 4 ud af 5 tilfælde er det medarbejderne selv eller tidligere medarbejdere der står bag virksomhedens sikkerhedsrelaterede hændelser. [23]

6.1 IT Sikkerhedsbevidsthed

IT sikkerhedsbevidsthed er lidt populært sagt den menneskelige side af IT sikkerhed.

For at en virksomhed fuldt ud kan bevarer fortrolighed, integritet og tilgængelighed af deres data er det nødvendigt at alle involverede parter dels forstår deres roller og ansvar relateret til virksomhedens mission og dels forstår virksomhedens IT sikkerhedspolitik og procedure. Det kræver også at de involverede parter har tilstrækkelig teknisk viden til at håndtere og beskytte de IT ressourcer de er ansvarlige for.
Det er almen kendt indenfor IT sikkerhed, at mennesket ofte er et af de svageste led når det kommer til at sikre systemer og netværk. Denne menneskelige faktor er nøglen til at sikre et passende og tilstrækkeligt niveau af sikkerhed.
Hvis mennesket både er et nøgle- men samtidig også det svageste led, er en bedre og mere målrettet opmærksomhed nødvendig.

6.1.1 Hvorfor introducere sikkerhedsbevidsthed i virksomheder?

IT sikkerhedsbevidsthed er et område af IT sikkerheden der i mange virksomheder ikke er særlig stor fokus på og det på trods af at flere offentliggjorte undersøgelser peger i retning af at medarbejderne i dag udgør en mindst lige så stor trussel mod virksomheden som eksempelvis eksterne virus- og hacker angreb.

I en ny sikkerhedsrapport, 'Global State og Information Security Study 2007', som blandt andet er udarbejdet af konsulentfirmaet PricewaterhouseCoopers, er konklusionen at det i dag er medarbejdere eller tidligere medarbejdere der er grunden til IT sikkerhedshændelser i hele 84% af tilfældene. I 2006 lå dette tal blot på 51%.
Mange virksomheder har teknologien, der skal sikre mod udefrakommende hændelser på plads, og derfor peger det nu i retning af at det er de interne forhold der skal sikres.
Rapporten påpeger også at løsningen skal findes i ledergruppen. For jo højere man er placeret i virksomheden, jo bedre mener man tilsyneladende, at sikkerheden er. Direktørerne har således en tydeligt større tro på, at sikkerheden er tilstrækkelig, end teknikkerne, som har sikkerhedsproblemerne inde på livet i det daglige arbejde. [23]

Et andet eksempel, er hvor de britiske told- og skattemyndigheder for nyligt mistede følsomme oplysninger på omkring 25 millioner briter. De mange millioner personlige oplysninger blev mistet, da en medarbejder brændte dem ned på to cd'er i toldmyndighedernes hovedkvarter. Den yngre medarbejder afsendte

dernæst, de to cd'er med posten, hvorfra de altså er forsvundet. Skandalen har blandt andet medført at direktøren har måtte trække sig fra sin post. [8]

Disse er blot få eksempler der viser et behov for at uddanne sine medarbejdere til at udvise en mere sikker adfærd når de har at gøre med følsomme data. Samtidig skal ledelsen anerkende at der er et problem, så der kan blive taget hånd om det fra højeste sted.

I den konkrete virksomhed anerkender man at en del sikkerhedshændelser skyldes medarbejdernes uvidenhed eller hensynsløse adfærd. Alligevel mener man i ledel- sen at den generelle sikkerhed er god nok og der derfor ikke behøves afsættes ressourcer til udvikling af for eksempel oplysningskampagner eller en undersøgelse af sikkerhedsbevidsthedsniveauet hos medarbejderne.
Mange retningslinjer for sikker adfærd er nedskrevet og lagt på Intranettet, men det er altså op til medarbejderne selv at finde dokumenterne og læse dem.

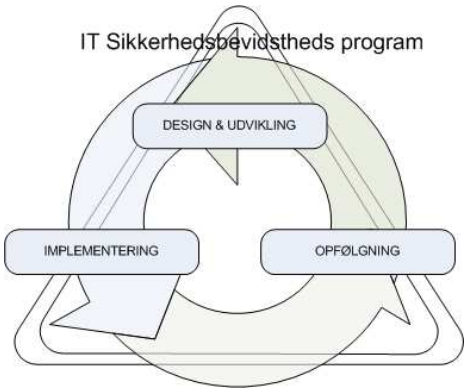
6.2 Udvikling af IT Sikkerhedsbevidstheds programmer

IT-sikkerhedsbevidsthed programmer bør være en integreret del af virksomhedens IT-sikkerheds politik. Afsnittet er baseret på kilderne: [4], [12], [16], [17] og [18].

En af forudsætningerne for at et IT sikkerhedsbevidsthedsprogram er velfungerende er, at der er fastlagt retningslinjer der afspejler f.eks. DS484:2005 samt at kravene til medarbejdere og andre parter, kommer herfra. Der bør løbende gennemføres behovsanalyser, så programmer og andre aktiviteter løbende kan prioriteres. Alle programmer bør gennemføres med synlig støtte og engagement fra virksomhedens ledelse.

Det er også vigtigt at gøre sig klart, hvem målgruppen for kampagner og/eller programmer er. Med en klart defineret målgruppe er det lettere at udvælge de budskaber der skal sættes fokus på. For at skabe størst mulig interesse for budskaberne er det vigtigt at emnerne er relevante for målgruppen, ligesom det er vigtigt at budskaberne opfattes som vigtige af medarbejderne. Her bør man gøre sig klart, om målet er at skabe øget kendskab, øget forståelse, øget efterlevelse eller en kombination. I praksis vil det sandsynligvis være svært og også uhensigtsmæssigt at forsøge at nå alle mål i samme kampagne/program.

Når der skal udvikles et sikkerhedsbevidsthedsprogram, er det vigtigt indledningsvis at udføre en behovsanalyse (eksempelvis gennem et spørgeskema) af alle virksomhedens medarbejdergrupper. Herefter kommer at der skal designes en strategi og fastlægge et passende omfang og indhold af budskaber til specifikke målgrupper. Hvert program skal målrettes de enkelte grupper.



Figur 6.1: Udviklingscyklus af IT sikkerhedsbevidsthedsprogrammer

Når materialet på denne baggrund er udviklet skal det implementeres. Der findes et utal af måder og tekniker til at implementere et sikkerhedsbevidsthedsprogram i en virksomhed, kun fantasien sætter grænser. Mange laver plakater, kampagne dage, undervisningsforløb alt efter hvilke budskaber og målgrupper materialet henvender sig til. En af fordelene ved et bevidsthedsprogram er at budskaberne gerne må gentages mange gange og gerne i form af forskellige implementeringer.
Næste vigtige skridt i udviklingscyklusen, se figur 6.1, er opfølgningen. De oplysninger der registreres ved program aktiviteter gemmes i en database til analyser af behov, opfølgninger, effektivitet og mulige forbedringstiltag.
Der bør periodisk udføres analyse af behov. Hvis denne viser at nye tiltag eller ændringer bør foretages starter udviklingsprocessen igen (design, budskab, strategi, udvikling, implementering opfølgning alle starter på ny igen).

6.2.1 Hvordan kan man øge folks bevidsthed

Et signifikant problem er at det ikke er let at undersøge menneskers attitude og opførselsmønstre i relation til mere komplekse teknologiske områder, såsom IT sikkerhed, idet der er en reel risiko for at svarpersonerne ved en undersøgelse rent faktisk ikke forstår det spørgsmål der er stillet dem. Et andet problem er at få formidlet budskaberne rigtigt ud.

Dette afsnit giver en beskrivelse af en ny metode til at forøge forståelsen ved brugerundersøgelser omhandlende IT sikkerhedsbevidsthed nemlig interaktive spørgeskemaer. Der gives også en række forslag på teknikker til at formidle de færdiglavede budskaber til medarbejderne på.

6.2.1.1 Interaktive spørgeskema

En måde at forøge forståelsen på kunne være at udvikle metoder der inkluderer grafiske illustrationer som eksempelvis animationer og simuleringer indlejret i spørgeskemaerne, for at kunne give svarpersonerne en mulighed for at svare gennem interaktive og valg, baseret på virkelige scenarier.
Formålet er altså at opbygge metoder til et spørgeskema der sikre en øget forståelse hos svarpersonerne. Ofte er svar-procenten relativ lav på rent tekstbaserede spørgeskemaer, mens brugen af visuelle effekter, animationer og simuleringer fører til en højere motivation for at deltage i sådanne undersøgelser.

Spørgeskemaet er en ofte benyttet metode ved brugeranalyser. Benyttet på Internettet er de nemme at distribuere og opsamling af svardata foregår her automatisk.
Normalt benyttes simpelt tekstbaseret spørgeskemaer, som består af en række tekstspørgsmål hvortil svarpersonen kan afkrydse sine svar. For at spørgeskemaet skal virke bedst muligt, er det vigtigt at alle svarpersoner nemt kan gå det igennem og svare på spørgsmålene, uden at synes at have spildt unødig tid på det. Det er derfor vigtigt at alle spørgsmålene er klart formuleret, og det skal være nemt for svarpersonen at finde det korrekte svar uden at tænke videre over det. Dette er også typisk situationen, da de fleste brugeranalyser omhandler brugsmønstre eller meninger som svarpersonen nemt kan relatere til. Dog kan der fremkomme komplikationer ved brugeranalyser der omhandler tekniske emner som ved sikkerhedsbevidsthed, da ikke alle svarpersoner nødvendigvis kan relatere til emnerne. Dermed kan man risikere at disse svarpersoner ikke forstår spørgsmålene og derfor ikke kan besvare spørgeskemaet rigtigt.

Programmer på en computer er ofte lavet med meget brugervenlige interfaces. De ellers til tider komplekse teknikker og mange lag af protokoller der ligger bag bliver omdannet til et enkelt grafisk interface, hvori brugeren med så få museklik som muligt, kan udføre den pågældende funktion.
Ideen med disse brugervenlige interfaces er, at brugeren ikke behøver bekymre sig om de bagvedliggende teknikker, eller forstå dem, og derved blot koncentrere sig om helheden i hvad programmet gør. En bruger behøver f.eks. ikke at vide hvordan en email-klient sender og modtager mails på det tekniske plan, men behøver blot vide hvad der skal gøres for at sende og modtage emails. På denne måde kræver computeren så lidt som muligt af brugeren sådan at flere brugere kan bruge den.
Derved risikerer man at brugerne til tider opbygger deres eget billede af hvad der egentlig sker i en funktion. For eksempel forstår brugeren ikke nødvendigvis at der udføres en synkroniserings transaktion med email-serveren, men blot at brugeren trykkede på send/modtag -knappen, hvorved emailen blev sendt til, eller modtaget fra en anden person. Nogle brugere kan endda blive forvirrede og usikre, hvis det grafiske design af deres program ændrer sig lidt ved en opdatering.

Denne forskel i forståelsen af computerens funktioner leder til hypotesen at mange brugere ikke forstår de mere tekniske begreber i forbindelse med IT sikkerhed, beskrevet med tekst i et spørgeskema og derved ikke vil kunne svare på det, eller måske bare vælger at svare ud fra et gæt. For at få så mange som muligt af brugerne til at forstå spørgsmålene korrekt, kan det blive nødvendigt at udvide spørgeskemaerne grafisk, således at brugerne eksempelvis får vist en grafisk repræsentation af de skærmbilleder de er vant til. Det gælder om at kunne relatere til det brugerne kender og få præsenteret/formuleret spørgsmålene på en nem og forståelig måde.

I kapitel 7 er udviklingen af et interaktivt spørgeskema beskrevet.

6.2.1.2 Liste over mulige bevidsthedsfremmende tekniker

Ud over metoden med et interaktivt spørgeskema listes her en række mulige bevidsthedsfremmende teknikker. Formidlingen af sikkerhedsbevidsthedsprogrammer og deres budskaber kan inddeles i 4 kategorier: personlig kommunikation, skriftlig kommunikation, kommunikation via systemer og andre kommunikationsformer.
Listen kan betragtes som et idékatalog, hvorfra der kan vælges et antal hensigtsmæssige aktiviteter/tekniker. Fordelen ved IT sikkerhedsbevidsthedsprogrammer er at de sagtens kan tåle gentagelser. Gentagelseseffekten er væsentlig og en kombination af de forskellige teknikker vil blot forstærker effekten. Gentagelser har samtidig den fordel at de overbeviser målgruppen om, at IT-sikkerhed er et emne, som tages alvorligt og har ledelsens opbakning.

Personlig kommunikation

- Gennemfør risikovurderinger med interviews o.a. metoder, som involverer personalet i processen.
- Integrer sikkerhedsrelaterede emner i de eksisterende og nye kursusforløb.
- Kræv af medarbejderne, at de gennemfører en online test, som dokumenterer deres kendskab til politikker og retningslinier. Kun hvis de opnår et tilfredsstillende resultat af denne test, vil de kunne tildeles (og evt. bevare) adgangsrettigheder til systemerne.
- Udnævn en dag til årlig 'Informations Sikkerheds Dag'. Gennemfør særlig uddannelse, kampagner o.a.
- Gennemfør (og markedsfør massivt internt) en undersøgelse af et brud på sikkerheden. Inddrag et antal relevante medarbejdere i denne undersøgelse.

Skriftlig kommunikation

- Tilføj spørgsmål om informationssikkerhed til eksisterende spørgeskemaer - Udvid evt. med grafiske elementer som animationer, interaktive billeder o.lign.
- Kræv at medarbejderne underskriver en erklæring om at overholde sikkerhedspolitik og relevante retningslinier før de får udleveret user ID.
- Placer klistermærker og lignende hvor de ses - f.eks. på kopimaskiner, fax, telefoner, o.a.
- Indlæg sikkerhedsfoldere i kuverter med lønsedler og flybilletter.
- Udarbejd funktions- og stillingsbeskrivelser som tydeliggør den enkeltes ansvar og opgaver i relation til sikkerheden.
- Udarbejd en arkitekturoversigt som viser/refererer til de etablerede sikkerhedsforanstaltninger (fysiske, logiske, administrative) - eller integrer sikkerheden i teknologibeskrivelserne på andre måder.
- Udgiv en IT sikkerheds håndbog indeholdende politikker, retningslinier, kontaktpersoner og en liste over godkendte applikationer, komponenter mv.
- Udarbejd rapporter om de seneste sikkerhedsmæssige hændelser sammen med evt. forslag til tiltag, som kan forbedre sikkerheden (eller beskrivelse af, hvad man efterfølgende allerede har gjort). Distribueres efter 'need to know' princippet.

Kommunikation via systemer

- Etabler online quiz som afdækker medarbejdernes kendskab til politik og retningslinier. Tilknyt evt. præmier/lodtrækning om præmier for korrekt besvarelse.
- Før brugerne får adgangsrettigheder til bestemte applikationer og services skal de gennemføre et online træningsprogram.
- Ændr startbilledet på de enkelte applikationer - herunder e-mail programmet - så der vises specifikke retningslinier for applikationens brug.
- Etabler interaktive spørgeskemaer eksempelvis via Intranet og test periodevis medarbejderne om forskellige emner.

Andre kommunikationsformer

- Skriv sikkerhedsslogans på krus, musemåtter, brevåbnere og andre ting, som udleveres til personalet.

- Etabler en hot-line med en automatisk telefonsvarer hvor man kan ind rapportere sikkerhedsproblemer - evt. anonymt.

Dette er blot nogle af de tekniker man kan benytte i forskellige kampagner og undersøgelser til at øge bevidstheden hos medarbejdere. En mere fyldestgørende liste kan ses i appendix C

6.3 Opsummering

I dette kapitel er gennemgået lidt om hvad IT-sikkerhedsbevidsthed er og hvorfor det bør introduceres i virksomheder.
Der er givet en kort beskrivelse af hvordan en udvikling af et IT sikkerhedsbevidsthedsprogram kan foregå i en virksomhed.

Der er i kapitlet også givet forslag til hvordan man kan øge bevidstheden hos folk både i forbindelse med de indledende spørgeskema undersøgelser og ved formidlingen af et sikkerhedsbevidsthedsprogram.
Brugerundersøgelser foregår ofte via tekstbaserede spørgeskemaer der gør det let at administrere og opsamle data. Men er data gode nok, forstår svarpersonerne spørgsmålene? Der gives i dette kapitel den påstand at mange svarpersoner simpelthen ikke forstår spørgsmål rigtigt og der må findes metoder til at forståelsen af mere tekniske begreber kan forøges. Dette kunne eksempelvis være ved at indlejre grafiske elementer i spørgeskemaerne, såsom animationer eller interaktive billeder hvorved svarpersonen grafisk for præsenteret en velkendt situation/scenarie og derved øger chancen for at det stillede spørgsmål forstås.
Til slut gives en liste med eksempler på bevidsthedsfremmende teknikker til hvordan man kan formidle budskaberne i et sikkerhedsbevidsthedsprogram til medarbejderne.

Kapitel 7

XAware - hjemmeside

I dette kapitel beskrives udviklingen af en online database-orienteret hjemmeside. Formålet med denne er at tilbyde spørgeskemaer inden for sikkerhedsbevidsthed målrettet til den konkrete virksomhed. Medarbejderne vil her kunne prøve et spørgeskema omhandlende primært trådløst netværk, som vil teste deres viden og samtidigt tilbyde indlæring inden for emnet, hvilket vil virke som sidens motiv. På denne måde vil medarbejdernes tendenser blive indsamlet gennem spørgeskemaet samtidigt med at medarbejderne føler de lærer noget af det.

Der skal igennem de indsamlede informationer vurderes hvor vidt et almindeligt tekstbaserede spørgeskemaer kombineret med en animeret interaktiv del indlejret er en forbedring over de simple og rene tekstbaserede spørgeskemaer og hvordan brugerne forholder sig til disse. Derudover undersøges også om et spørgsmål direkte efterfulgt at et svar med forklaring på hvorfor svaret enten var rigtig eller forkert, gør at brugeren senere hen i spørgeskemaet vil kunne svare rigtigt på næsten samme spørgsmål igen.

Kapitlet vil derudover analysere de indtil nu indsamlede resultater samt give en beskrivelse af de forbedringer der kan laves og eventuelt hvordan nye lignende spørgeskemaer kan udvikles.

7.1 Adobe Captivate

Adobe Captivate er et program designet til at lave indlæringsvideoer til Internettet. Programmet kan optage skærmbilleder af andre programmer, således at disse kan benyttes til at konstruere en interaktiv video der fremviser et program. Man kan dertil tilføje ekstra knapper, tekst felter og andre småting til at skræddersy indlæringsvideoen.[1]

Captivate er et af Adobe's mange webudviklings-programmer og bygger på deres populære flash-teknologi, som benyttes på Internettet til at konstruere vektorbaseret animeret grafik. Et Captivate projekt bliver udgivet som en swf-fil (shockwave flash) som så direkte kan indlejres i en web-side. I og med at flash er så udbredt på nettet, understøttes det af stort set alle browsere.

Adobe Captivate er især interessant da dets opbygning tillader optagelse af skærmbilleder, hvilket sammen med tilføjelser af f.eks. ekstra knapper, tekst felter, osv. kan benyttes til opbygning af animerede spørgeskemaer.

En ulempe med Captivate er dog det at opfange og videresende interaktionsdata til en eventuel database. Derfor er Captivate i dette projekt benyttet til at lave animationerne af velkendte skærmbilleder, hvor brugeren på samme vis kan manøvrere frit rundt - til en hvis grad, da fuld frihed ofte vil skabe meget store og tidskrævende projekter - og trykke på de forskellige knapper og indtaste tekst i tekstfelter osv. Mens selve besvarelsen af spørgsmålet så vil foregå på selve html-siden ved at afkrydse en af svarmulighederne der.

7.2 Udvikling af spørgeskema

7.2.1 Analyse

Der ønskes udviklet en online sikkerhedsbevidstheds hjemmeside, der skal gøre det muligt for medarbejderne i virksomheden, at teste deres viden om computersikkerhed gennem et animeret spørgeskema. På denne måde vil medarbejdernes tendenser blive opfanget og lagres for at kunne vises statistisk.

Spørgeskemaet skal omhandle brug af trådløst netværk, da det ofte er tilfældet for den mobile medarbejder, og nogle af de sikkerhedsaspekter der hører dertil.

Udover spørgeskemaet skal hjemmesiden tilbyde følgende funktionaliteter:

- Brugeroprettelse - for at undgå duplikeret data
- Logind og Logud funktioner

[1] For mere information om Adobe Captivate se på: http://www.adobe.com/products/captivate/

- Statistik - tilgængeligt for en administrator

For at kunne prøve spørgeskemaet skal man være oprettet som bruger af hjemmesiden og være logget ind. Ved brugeroprettelse ønskes følgende oplysninger:

- Brugernavn - skal bruges til at logge ind med
- Password
- Fornavn
- Efternavn
- Postnummer
- Alder
- Køn - (Kvinde/ Mand)
- Beskæftigelse - (Uden job/ Studerende/ Studerende m. arb./ Arbejder-deltid/ Arbejder-fuldtid)
- Virksomheden navn/ Uddannelsessted
- Job titel/ Uddannelses retning
- Computer færdighed - (Uerfaren/ Erfaren/ Super bruger/ Ekspert)

Der er her lagt op til at andre end virksomhedens ansatte også skal kunne afprøve spørgeskemaet.

7.2.1.1 Opbygning af spørgsmål

Opbygningen af de i alt 16 spørgsmål har tre formål:

1. Undersøge om animerede spørgeskemaer giver en øget forståelse af tekniske spørgsmål.
2. Undersøge om et spørgsmål direkte efterfulgt af et forklarende resultat kan give et forbedret svar på et lignende (og knapt så forklarende) spørgsmål senere i spørgeskemaet.
3. At give brugeren af hjemmesiden værktøjer til fremover at kunne færdes sikkert via trådløst netværk

De 16 spørgsmål eventuelt efterfulgt af en forklaring. De første 6 spørgsmål er forholdsvis generelle bruges til at finde i hvor stor udstrækning og hvor trådløst netværk bliver benyttet, blandet sammen med spørgsmål der kan bruges til at bestemme et generelt sikkerhedsbevidstheds niveau hos svarpersonerne. Derefter tages udgangspunkt i oprettelsen/opkoblingen til et trådløst netværk ved hjælp af Windows egne programmer til automatisk og manuelt at finde og oprette forbindelse. Både det manuelle oprettelses og det automatiske oprettelses program vil via Captivate blive animeret og indlejret i spørgsmålene så svarpersonen kan trykke sig frem til hvad der kunne være det rigtige svar på spørgsmålet.

1. **Hvor ofte benytter du trådløst netværk?**
2. **Benytter du dig af trådløst netværk derhjemme/ på arbejdet?**
3. **Føler du dig sikker, når du surfer på Internettet?**
4. **Ved du hvad du skal gøre eller hvem du skal henvende dig til hvis noget unormalt sker på din computer?** - Kender svarpersonen til virksomhedens retningslinjer hvis sikkerhedsrelaterede hændelser sker?
5. **Har du modtaget undervisning eller blevet oplært i de daglige programmer du benytter i forbindelse med arbejdet?** - dette er relevant i forhold til at svarpersonen ved hvordan væsentlige programmer skal håndteres herunder hvad man må og ikke må/ kan og ikke kan.
6. **Har du gjort dig bekendt med firmaets IT-sikkerhedspolitik?** - Ret så væsentlig, eftersom der ved ansættelsen bliver skrevet under på at denne er læst.
7. **Hvad betyder SSID?** - Her bliver svarpersonen for første gang introduceret til en Captivate animation. Der tages udgangspunkt i Windows eget program til oprettelse af manuelt trådløst netværk. Den opmærksomme svarperson kan se på animationen at SSID'et er netværkets navn.
8. **Kan det trådløse netværk skjules så uvedkomne ikke kan se det?** - En sikkerhedsforanstaltning der er god at kende når der opstilles trådløst netværk hjemme.
9. **Vælg den mest sikre netværksgodkendelsesmetode** - Igen vises animationen, så svarpersonen kan trykke sig frem og finde ud af hvilke muligheder for netværksgodkendelsesmetoder der tilbydes.
10. **Vælg den mest sikre datakrypteringsmetode** - Igen vises animationen, så svarpersonen kan trykke sig frem og finde ud af hvilke muligheder for datakrypteringsmetoder der tilbydes. Sammenholdt med foregående svar vil svarpersonen her blive præsenteret for en svar-side, der beskriver hvad der menes med de mest sikre metoder og hvad svaret evt. burde være.

11. **Vælg det mest sikre trådløse netværk** - Her præsenteres svarpersonen for den anden animation, af Windows' program til automatisk at finde og oprette forbindelse til et netværk. Svarpersonen kan trykke sig rundt og vælge mellem tre forskellige netværk der kan oprettes forbindelse til. Det ønskede svar, er det netværk der indeholder den stærkeste krypteringsmetode (i dette tilfælde WPA).

12. **Bør dit trådløse netværk være krypteret?** - Et væsentligt punkt ved brug af trådløst netværk er at få det krypteret. Der vises på svarsiden et eksempel med hvor let det er for en hacker at opfange og læse afsendte emails på et ikke-krypteret netværk. Skal bruges til at 'skræmme' svarpersonen hvis de ikke mener det er nødvendigt at krypterer.

13. **Når du benytter trådløst netværk med din arbejdscomputer hjemmefra eller fra et offentligt sted (eksempelvis i lufthavnen, toget, osv.), opretter du da en VPN forbindelse?** - Der bliver i virksomheden brugt en USB-EToken fra Aladdin til at autentificerer sig så en sikker VPN forbindelse kan oprettes. Dette vil fremgå af svar-siden til dette spørgsmål og der vil også være et billede af denne USB EToken.

14. **Hvad bruges denne EToken til?** - Billede af EToken findes sammen med dette spørgsmål. Ud fra sidste spørgsmåls svar-side skulle det her gerne være muligt for svarpersonen at genkende både ordet VPN-forbindelse og USB EToken.

15. **Vælge den sikreste af netværksgodkendelsesmetoder og datakrypteringsmetoder af nedenstående kombinationer?** - dette spørgsmål er tidligere blevet stillet i en lidt anden udformning. Tester her om svarpersonen kan huske hvad den sikreste kombination er. Gentagelse af begreber er en god ting.

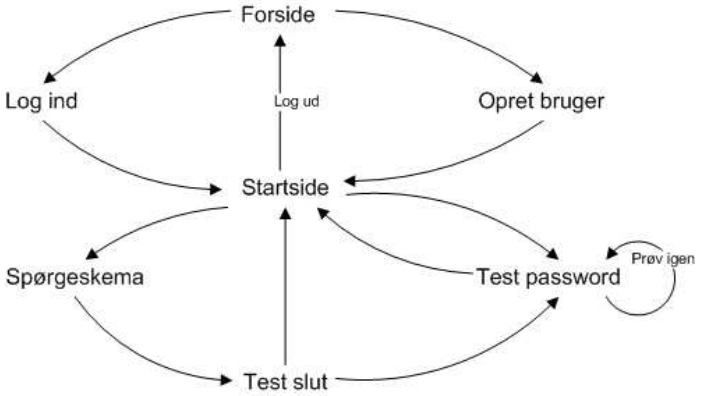
16. **Har du fået noget ud af dette spørgeskema?**

7.2.2 Design

De dele der skal bestemmes før implementeringen kan påbegyndes, er en opbygning af databasens struktur, samt et design af brugergrænsefladen.

Strukturen for hjemmesiden er overordnet vist på figur 7.1. Som det kan ses kommer man først frem til en forside med noget generelt info. Herfra kan man vælge at oprette sig som bruger eller logge ind. Oprettelsen af brugere er meget enkel, da dens formål er at opsamle nogle generelle personinformationer som alder, køn, beskæftigelse, computer færdighed, osv. Disse data kan være gavnlige ved brug af statistikker. Når en bruger er logget ind kommer han frem til en side hvorfra der kan vælges mellem at starte spørgeskemaet eller gå til siden hvor

man kan teste hvor robust sit password er.
Hvis spørgeskemaet bliver valgt, vises dette, og ved sidste side af spørgeskemaet vil brugeren have valgmuligheden at returnerer til startsiden for brugere der er logget ind eller gå videre til siden hvor test af password foregår.
På test af password-siden kan brugeren vælge at prøve igen med et nyt password eller at vende tilbage til startsiden.



Figur 7.1: Program struktur

Overordnet set skal det være nemt for en bruger at oprette sig samt prøve og lære af spørgeskemaet.

7.2.2.1 Designovervejelser

I forbindelse med udvikling af hjemmesiden er der brugt Apache HTTP server 2.2.4 til at håndterer PHP siderne og MySQL Server 5.0 som database løsning.

Til selve sideopbygningen er der valgt at benytte CSS's boksmodel. Brugen heraf gør det nemmere at ændre sidernes udseende radikalt uden at skulle rette i selve koden. Derudover sikrer det at alle sider får et ensformigt udseende.
Siden er bygget op på en hvid baggrund, sort tekst og understregede blå links. Herved opnår en god kontrast, der gør siden læsevenlig. Fejlmeddelelser udskrives med rødt.
Øverst på siden er XAwares logo placeret. Herunder er menuen placeret. Grunden hertil er at mange sider på Internettet er opbygget på denne måde, og den vil derfor ikke virke forvirrende på eventuelt uerfarne Internetbrugere. I højre side vises en loginformular samt når en bruger er logget ind vises her også de tilgængelige spørgeskemaer.
For at gøre det nemmere at opbygge siden er sidehovedet og menuen placeret i en ekstern fil.

På serversiden bruges PHP, til kommunikation mellem server og klient. Til udvikling af databasen benyttes MySQL. Udviklingen af siderne er foregået på en lokal Apache HTTP server.
Til afsendelsen af indholdet i formularer benyttes metoden POST, hvorved der undgås at indsætte følsomme data i adresselinjen. Til validering af de indtastede oplysninger benyttes Javascript funktioner.

Loginperioden(en session) er karakteriseret ved session-cookien xawareid, der indeholder brugerens medlemsnummer, samt session-cookien medlemstype, der indeholder medlemstypen. Der findes 2 medlemstyper, medlem eller administrator.
Sider der kræver medlemskab eller administratorrettigheder kan ikke tilgås af andre.
Ved afslutning af loginperiode, slettes gemte informationer om medlemmet. En loginperiode afsluttes automatisk efter 15 minutters inaktivitet eller hvis brugeren selv logger ud.

Til validering af formularer benyttes Javascript. Dette betyder at det er vigtigt, for at undgå fejl, at browseren har Javascript aktiveret.

7.2.2.2 Database struktur

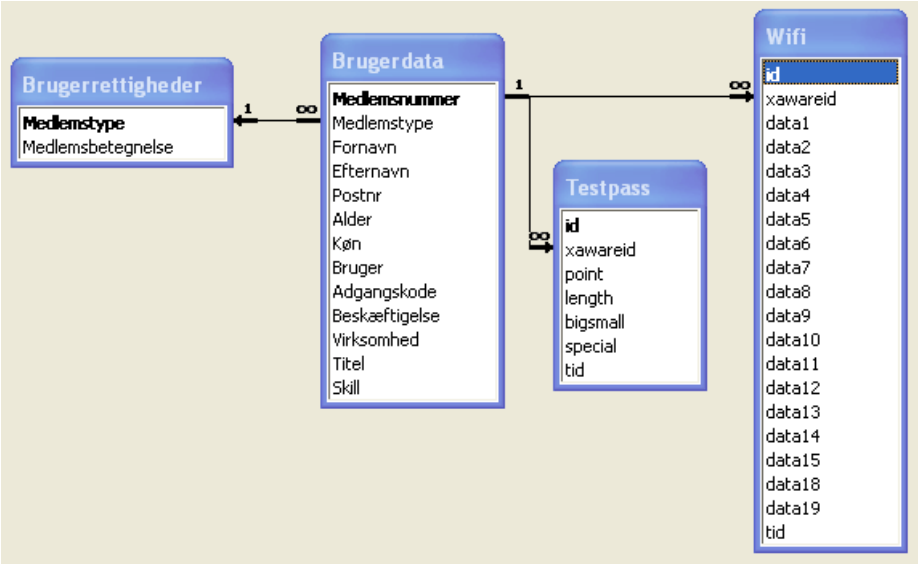
Systemets MySQL-database tager vare på de optagne data fra spørgeskemaerne og de oprettede brugere. For at beskrive denne er der lavet en relationsmodel, som er vist på figur 7.2.

Hele databasen er centreret omkring tabellen *brugerdata*, som indeholder alle data om de oprettede brugere. Brugerne får ved oprettelsen tildelt en medlemstype 'medlem'. De forskellige medlemstyper er gemt i tabellen *brugerrettigheder*. Der er som tidligere nævnt lavet to former for test, et spørgeskema omhandlende trådløst netværk og en test af password. Resultaterne fra de to test bliver gemt i henholdsvis *wifi* og *testPass*. Relationerne kan ses med forgreninger ved f.eks. at en *brugerdata* kan have mange rækker *testPass*, men en række i *testPass* skal have kun en tilknyttet *brugerdata*.

Modellen opfylder betingelserne for tredje normalform ved at alle tabeller har en primærnøgle og ingen gentagne felter. Der er desuden ingen sammensatte primærnøgler og ingen attributter der ikke er direkte afhængige af primærnøglen.

7.2.2.3 Layoutstruktur

Til selve sideopbygningen er der valgt at benytte CSS's boksmodel. Dette betyder at opsætningen af siden er baseret på et CSS stylesheet, *style.css* se evt. appendix D.1.2, der beskriver placeringen af sidens forskellige bokselementer



Figur 7.2: Database struktur

$<$ *span* $>$ og $<$ *div* $>$. Stylesheetet beskriver desuden udseendet, samt formateringen af sidens indhold. Figur 7.3 viser den overordnede layout struktur.

#title - indeholder XAwares logo

#datebox - placerer datoboksen placering.
#datebody - indeholder datoen.

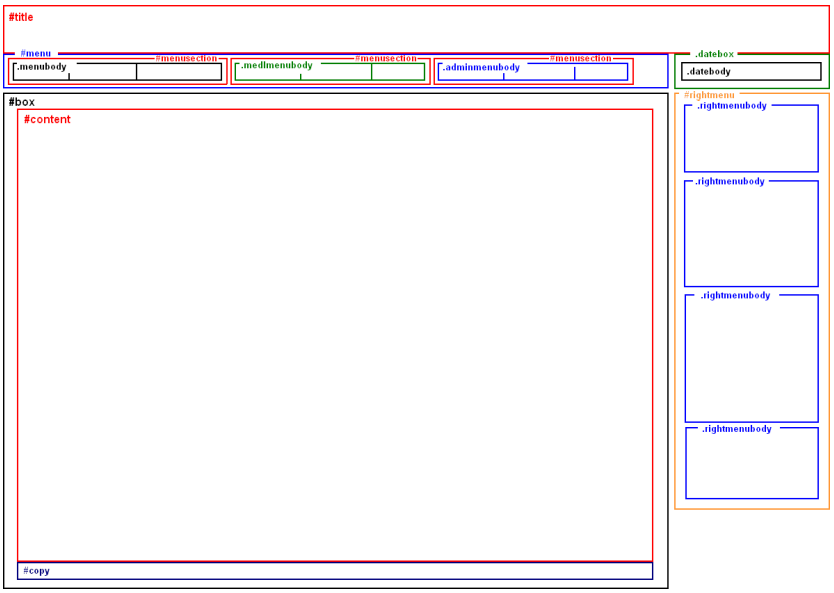
Menusystemet er placeret i en separat fil *menu.php* findes i appendix D.1.11 og er opdelt i følgende bokse:

#menu - specificerer placeringen af øverste menu.
.menusection - specificerer en sektion i den øverste menu.
.menubody - indeholder et menupunkt, der er synligt for alle brugere.
.medlmenubody - indeholder et menupunkt, der er synligt for medlemmer/administratorer.
.adminmenubody - indeholder et menupunkt, der er synligt for administratorer.

#rightmenu - specificerer placeringen af menuen i højre side.
.rightmenubody - indeholder en menudel i den højre menu.

#box - specificerer placeringen af sidens hovedindhold, hvilket er forskelligt fra side til side

#content - indeholder sidens hovedindhold, hvilket er forskelligt fra side til side



Figur 7.3: XAware Layout

7.2.2.4 Filstruktur

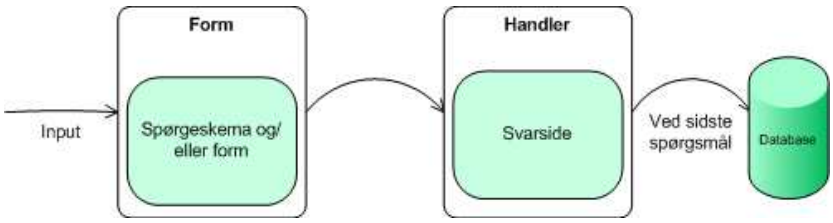
Siden vil blive opbygget som php-forbedret html, bygget op omkring en MySQL-database.

Siden består af 3 hoved sektioner, en sektion der er tilgængelig for alle besøgende, en sektion der er tilgængelig for medlemmer og administratorer og en sektion kun tilgængelig for administratorer.
Ved gyldigt login sættes $_SESSION['xawareid'], hvormed den besøgende får adgang til medlemssektionen. Hvis den besøgende har administratorrettigheder, dvs. $_SESSION['medlemstype'] = 2, gives yderligere adgang til administrator-sektionen.

Alle sider inkluderer header.php og menu.php.
header.php
XAwares sidehoved. Her erklæres at der benyttes XHTML 1.1. Indeholder derudover metatags og inkluderer en Javascript funktion der skriver dags dato i #datebody.
menu.php
Indeholder menuer for alle, for medlemmer (er medlem hvis '$_SESSION['xawareid'] <> " ') og for administrator (er administrator når '$_SESSION['xawareid'] <> " ' og '$_SESSION['medlemstype'] = 2').
Desuden indeholder filen også login boksen, i højre side af skærmen.

7.2.3 Implementering

Til denne hjemmeside benytte domænet www.dtu17.be, hvilket vil sige at siden kommer til at være tilgængelig fra http://dtu17.be eller http://www.dtu17.be/indeix.php. Siden tilbyder php samt database tilgang via mysql.
Siden er bygget med XHTML (af standarden transitional), JavaScript, Cascading Style Sheets (CSS) samt php til det mere dynamiske som bl.a. databasetilgangen.



Figur 7.4: Generel struktur mellem form og handler

Figur 7.4 viser sammenhængen mellem form og handler hvilket bliver benyttet i implementeringen. Form siden er den side hvor spørgeskemaet eller andet forminput er. Disse bliver så ved submit bliver sendt til en handler side som håndterer informationerne ved at vise et svar for brugeren og ved sidste spørgsmål i testen ligges oplysningerne op i databasen herfra. Implementeringsrækkefølgen er som følger:

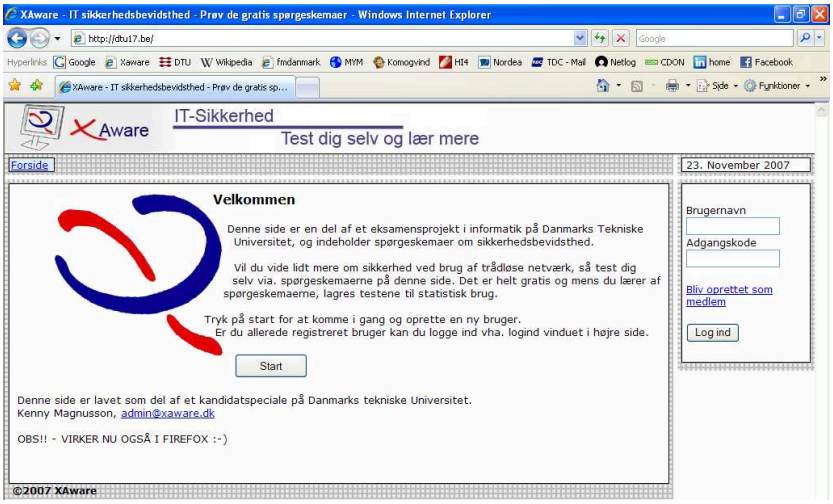
- Login
- Opret Bruger
- Afprøv Spørgeskema
- Afprøv Test af password

Implementeret af det scenarie hvor en brugeroprettelse finder sted vil blive beskrevet. Hvorefter henholdsvis afprøvningen af spørgeskemaet og test af password vil blive beskrevet.

Billede af forsiden kan ses i figur 7.5.

7.2.3.1 Logind

Logind kan foregå på to måder. Ved brugeroprettelse foretages logind automatisk hvis brugeren oprettes fejlfrit. Den anden måde at logge ind på er ved at skrive



Figur 7.5: Xaware forside

sit brugernavn og password ind i logindboksen i højreside og trykke på logind-knappen.

Alle spørgeskemaer på siden kan kun tilgås ved at oprette en bruger og logge ind på siden. En bruger bliver oprettet i databasens brugerdata-tabel og disse informationer bliver der sammenlignet med ved logind.

Det kodeord, der bliver indtastet i enten Opret Bruger formen eller ved logind boksen, bliver med det samme krypteret med MD5, hvilket er en envejs krypteringsalgoritme. Derved ligger alle kodeordene krypteret inde i databasen og ved logind bliver de krypterede strenge sammenlignet, for at validere brugeren.

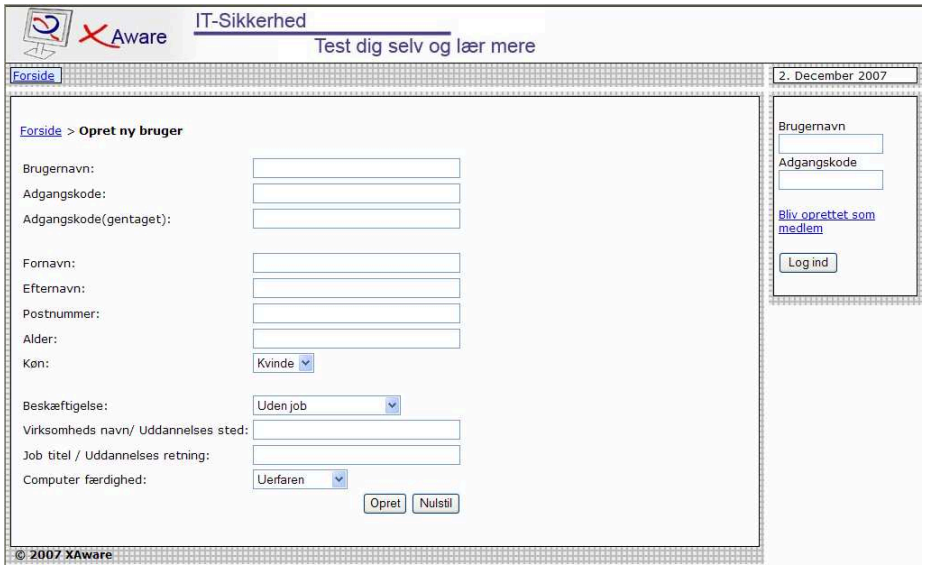
Når en bruger logger ind bliver der oprettet en browser session, hvilken indeholder medlemsnummeret på brugeren i databasen. Alle sider kontrollerer på denne sessionsnøgle i headeren hvorved der kan tages stilling til om brugeren har adgang til den pågældende side, eller skal redirectes videre til 'forsiden'.

Login håndteringen: logind.php kan findes i appendix D.1.9.

7.2.3.2 Opret Bruger

Sektionen til oprettelse af en ny bruger kan ses på figur 7.6. Denne er konstrueret til at være forholdsvis simpel sådan at brugere nemt kan oprette sig.

Som tidligere beskrevet skal specificere en række oplysninger om sig selv. Alle felter bliver javascript valideret, således at brugeren får en besked hvis han ind-



Figur 7.6: Opret bruger

taster ikke valide informationer. Dette sørger også for at holde data i databasen konsistente.
Html-formen på siden (opretbruger.php appendix D.1.12) sender informationerne videre til dens handler side (opretbrugerh.php appendix D.1.13) hvilken kontrollerer om det valgte brugernavn ikke allerede eksisterer og hvis det er tilfældet indsættes informationerne på en ny række i brugerdata-tabellen.

7.2.3.3 Afprøv Spørgeskema

Med brugeren logget ind kommer han ind på en side hvor han kan se de mulige spørgeskemaer og vælge mellem disse. Denne side hedder default.php (appendix D.1.5) og kan ses på figur 7.7.

På denne side bliver brugeren budt velkommen og den generelle målsætning for siden forklares igen. På siden kan brugeren i menuen oppe under logoet eller i den højre menuboks, vælge mellem de mulige spørgeskemaer se figurfig:forsideAdm.

Brugerens svar bliver løbende via handler siden gemt i session-variable og efter det sidste spørgsmål i testen opsamles alle de gemte session-variable indeholdende alle svar og sendes til databasen hvor de sammen med brugerens medlemsnummer bliver gemt i den tilhørende tabel, se figur 7.4.

Figur 7.7: Forside for administrator der er logget på

7.2.3.4 Afprøv Test af password

Dette spørgeskema omhandler en enkelt side, hvori brugeren kan indtaste sit kodeord og få vurderet hvor sikkert det er. I kapitel 4.1.2 blev der nævnt nogle regler som et godt kodeord helst skal overholde.

Disse regler er at kodeordet skal[10]:

- Være på mindst 8 tegn
- Bruge både små og store bogstaver
- Bruge specieltegn og tal

Nedenstående vurderingsmekanisme bygger på den af Theo Andersens, master thesis om animerede spørgeskemaer [7], tilsvarende lavede vurderingsmekanisme.
Ud fra disse tre regler er der konstrueret en vurderingsmekanisme, så der kan vises en form for bedømmelse af hvor sikkert kodeordet er og hvad der eventuelt kan gøres for at forbedre det.

Vurderingsmekanismen benyttes altså til at bestemme hvor sikkert et kodeord er. Det vil blive bedømt ud fra en skala fra 0 til 100, hvor 0 er et dårligt sikrede kodeord og 100 er et godt sikret kodeord.
På denne skala vil 0-40 points repræsentere et dårligt kodeord, 41-70 et mellem,

Figur 7.8: Test af password - Resultat

og 71-100 et godt kodeord. Disse inddelinger vil grafisk blive repræsenteret af farverne rød, gul og grøn.

Dertil er der udviklet et pointsystem, som vil vurdere kodeordet på en enkel måde, hvor fokus er på at resultatet er forståeligt for brugerne.

Pointsystemet er bygget op af følgende trin:

1. Længden af kodeordet er det mest kritiske og bliver bedømt efter følgende ligning: $Point = (Length * 15) - 50$, hvor resultatet ikke kan blive større end 70 eller mindre end nul. Der opnås altså de maksimale 70 points hvis kodeordet har en længde på otte karakterer eller mere.

2. Hvis der er både små og store bogstaver i kodeordet tildeles der yderligere 15 points.

3. Findes der nogle specieltegn eller tal i kodeordet tildeles der også yderligere 15 point

Denne vurderingsmekanisme vurderer altså længden af kodeordet som vigtigere end specialtegn og forskel på store og små bogstaver.
Når spørgeskemaet har udført vurderingen, vil der præsenteres et svar for brugeren der på en skala fra 0 til 100 grafisk vil vise vurderingen af kodeordet. Samtidig vil de tre ovennævnte krav til et sikkert kodeord blive gentaget og et grønt flueben eller et rødt kryds placeret ud fra de krav alt efter om det indtastede kodeord indeholdte de anbefalede krav, se figur7.8.

7.3 Resultater

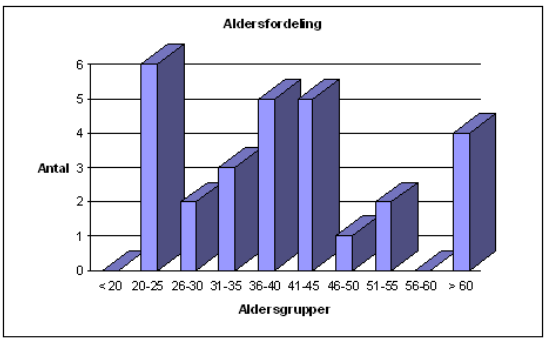
For at teste hjemmesiden og få brugerrespons har jeg udsendt den både til en række venner samt udsendt den til en række væsentlige afdelinger i den konkrete virksomhed. På en lille måned er der blevet oprettet 28 brugere, der alle har gennemført en eller flere af testene.
I dette afsnit vil svarene blive analyseret, for at få undersøgt hvorledes tendensen af brugernes viden inden for sikkerhedsbevidsthed er. Herudfra vil analysen også forsøge at give et svar på hvor godt de animerede spørgeskemaer virker.

7.3.1 Analyse af besvarelserne

I dette afsnit vil svarene fra de 28 svarpersoner blive analyseret, startende med brugerfordelingen.

7.3.1.1 Brugerfordeling

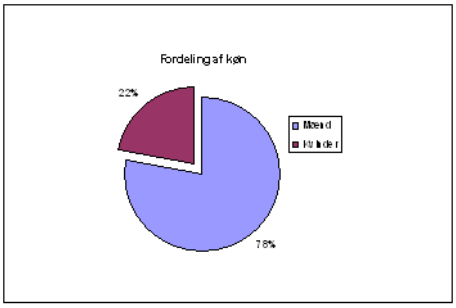
Idet størstedelen af brugerne er fra virksomheden, vil brugerne sandsynligt være mere teknisk kyndige end normale brugere, da de bruger computeren dagligt og mange af dem er udviklere. Figur 7.9 viser et diagram over aldersfordelingen for brugerne på hjemmesiden.



Figur 7.9: Aldersfordeling

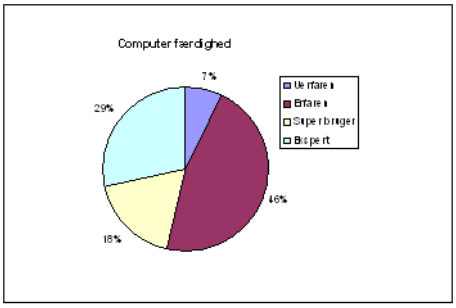
Som det kan ses er spænder brugernes alder vidt hvilket stemmer overens med den forventede bredde målgruppe i en virksomhed.

Kønsfordelingen fra figur 7.10, viser at en overvægt af brugerne er mænd, hvilket også passer sammen med fordelingen af køn i de afdelinger hjemmesiden er sendt ud til i virksomheden.
Dette behøver ikke have nogen stor indvirkning på besvarelserne, men mænd er



Figur 7.10: Fordeling af køn

normalt mere teknisk interesseret i computere end kvinder og har derved ofte mere erfaring med dem.

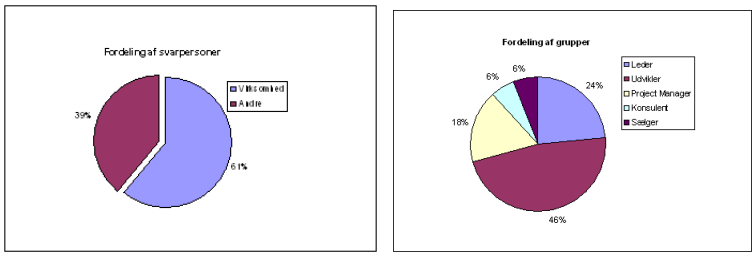


Figur 7.11: Computer færdigheder

Af fordelingen over computerfærdigheder som er vist på figur 7.11, er det vist at størstedelen af brugerne mener selv de har niveauet erfaren eller ekspert. Dette passer sammen med de tidligere beskrivelser, om at de oprettede brugere består af lidt mere teknisk orienterede brugere. Dog er der en del usikkerhed forbundet hermed, for ofte er der en tendens til at de dygtige brugere med stor viden om emnet ofte vil rangerer sig selv lavere, mens brugere der ikke besidder så meget viden på området ofte har en tendens til at klassificerer sig selv lidt højere.

Af figur 7.12 ses fordelingen af brugerne i forhold til virksomheden. Godt 2/3 af brugerne er fra virksomheden, se figur7.12(a) og deres indbyrdes gruppering viser at størstedelen af brugerne er udviklere og ledere, se figur 7.12(b).

Brugerfordelingen er ret snæver og består for det meste er mænd med hang til teknik, udviklere og andre IT folk. Dog må man så forvente at disse formodentlig vil vide mere om computersikkerhed end den gennemsnitlige bruger.



(a) Fordeling af brugerne

(b) Virksomhedens bruger inddelt i grupper

Figur 7.12: Fordeling i forhold til virksomhed

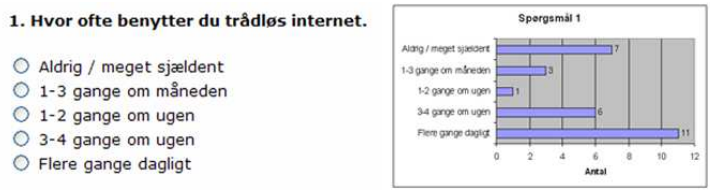
Den snævre brugergruppe gør at det ikke giver megen mening at benytte værktøjerne til brugerafgrænsning. Derfor vil analysen af spørgeskemastatistikkerne alle være for hele den opfangede brugergruppe. At der ikke er oprettet så mange personer gør at der er risiko for lidt tilfældigheder som kan være ødelæggende for statistikken.

De næste dele vil beskrive statistikkerne for spørgeskemaerne i detaljer. Til dette vil de forskellige dele af statistikerne blive delt op, vist og forklaret for sig.

7.3.1.2 Svar fra spørgeskema om trådløst netværk

De første spørgsmål, 1 til 6, omhandler generelle oplysninger omkring IT sikkerhed og trådløst netværk. De er alle rene tekstbaserede spørgsmål der skal bruges til at give en idé om hvilken type bruger og erfaringer brugeren har.

Spørgsmål 1 - Hvor ofte benytter du trådløst internet?

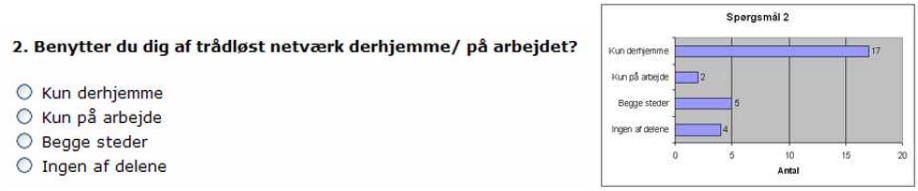


(a) Spørgsmål (b) Svar

Figur 7.13: Spørgsmål 1

Som det fremgår af figur 7.13 er gruppen af brugere delt i to, dem der ofte benytter trådløst netværk og dem der næsten aldrig benytter det.

Spørgsmål 2 - Benytter du dig af trådløst netværk derhjemme/ på arbejdet?



(a) Spørgsmål (b) Svar

Figur 7.14: Spørgsmål 2

Da det på selve virksomheden ikke er muligt eller tilladt at benytte trådløst netværk er der meget god overensstemmelse hermed, at hovedparten af brugerne der benytter trådløst netværk gør det hjemme. Se svarene i figur 7.14

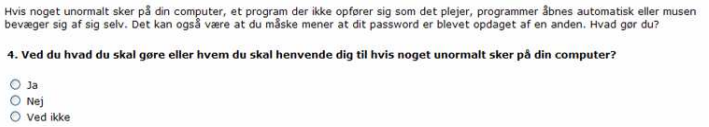
Spørgsmål 3 - Føler du dig sikker, når du surfer på Internettet?

(a) Spørgsmål (b) Svar

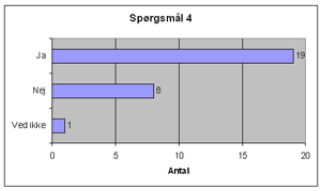
Figur 7.15: Spørgsmål 3

Som der konkluderes i brugerfordelingen er hovedparten af brugerne habile computer og Internet brugere, dette fremgår også af dette spørgsmål, se figur 7.15. Om end spørgsmålet er noget uklart defineret for menes der sikkert generelt eller sikkert ved benyttelse af trådløst netværk? - Meningen var at se om brugerne føler sig mere utrygge når de benytter sig af trådløst netværk.

Spørgsmål 4 - Ved du hvad du skal gøre eller hvem du skal henvende dig til hvis noget unormalt sker på din computer?



(a) Spørgsmål



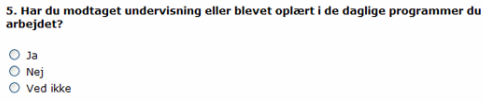
(b) Svar

Figur 7.16: Spørgsmål 4

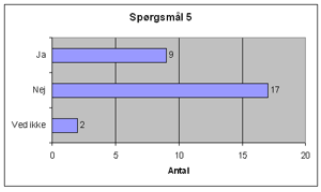
Ved dette spørgsmål, er der først en forklarende tekst til at præcisere hvad der forstås ved unormalt. En vigtig del af sikkerhedsbevidsthed i en virksomhed er også at medarbejderne præcis ved hvad de skal gøre og hvem de skal henvende

sig til hvis der opleves noget unormalt på computeren. Som det fremgår af figur 7.16 ved hovedparten af brugerne godt hvad de skal gøre eller hvem de skal henvende sig til.

Spørgsmål 5 - Har du modtaget undervisning eller blevet oplært i de daglige programmer du benytter i forbindelse med arbejdet?



(a) Spørgsmål

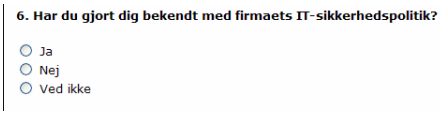


(b) Svar

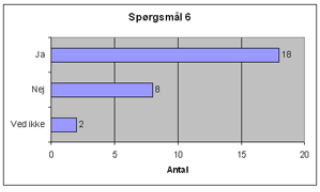
Figur 7.17: Spørgsmål 5

Af svarene til spørgsmål 5 fremgår det, at det er meget blandet om der er modtaget nogen form for undervisning i forbindelse med de dagligt brugte programmer. Ikke kun af forretningsmæssige grunde er det en god ide at medarbejdere bliver undervist i brugen af programmerne, for en bruger der ikke kender programmet ved måske heller ikke hvis der sker noget som ikke burde ske, og kan derved ikke rapportere det.

Spørgsmål 6 - Har du gjort dig bekendt med firmaets IT-sikkerhedspolitik?



(a) Spørgsmål



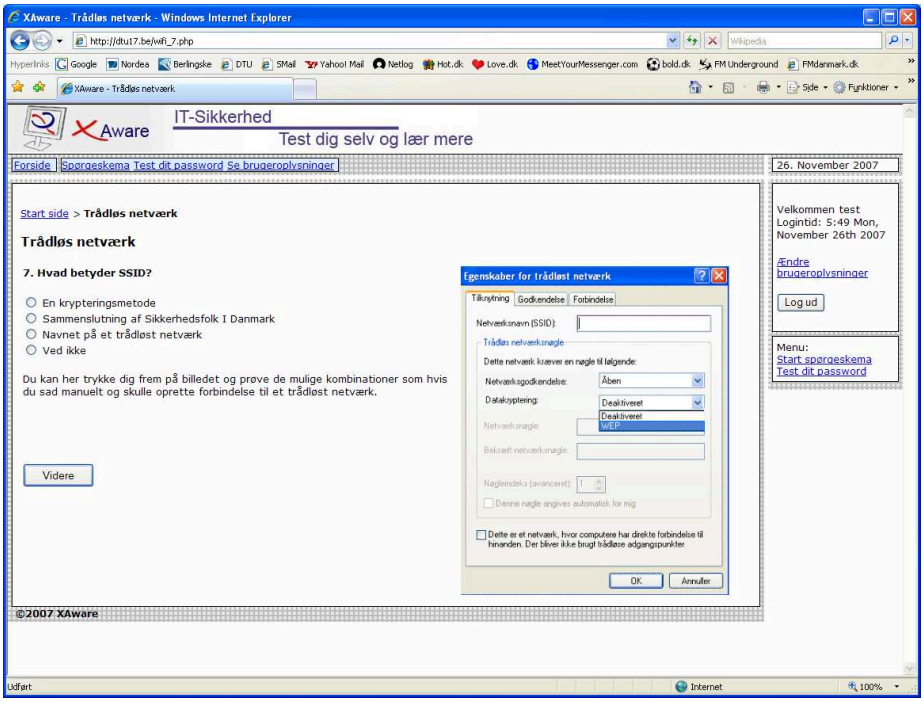
(b) Svar

Figur 7.18: Spørgsmål 6

Det sidste af de mere generelle spørgsmål, er ganske væsentligt i forhold til

sikkerhedsbevidsthed. Her svarer de fleste da også at de har gjort sig bekendt med IT sikkerhedspolitikken.

De efterfølgende spørgsmål inkluderer en interaktiv animation af Windows eget billede ved manuel oprettelse til trådløst netværk. Det er her muligt for svarpersonen, at vælge mellem de forskellige kombinationer af netværksgodkendelsesmetoder og datakrypteringsmetoder, samt mulighed for indtastning i de forskellige inputbokse herunder bl.a. netværksnavnet, se figur 7.19



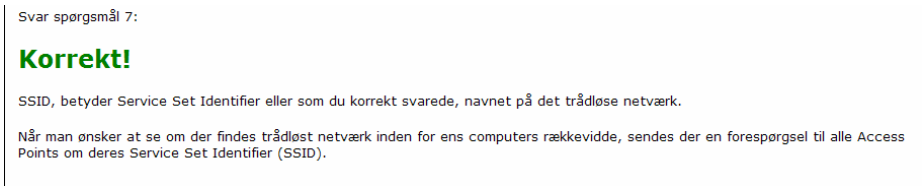
Figur 7.19: Spørgsmål 7 med interaktivt billede

Spørgsmål 7 - Hvad betyder SSID?

(a) Spørgsmål (b) Svar

Figur 7.20: Spørgsmål 7

Som det fremgår af figur 7.20 kunne næsten alle svare rigtigt på hvad SSID betyder. En stor hjælp til dette er også at svaret rent faktisk fremgår af den interaktive animation. Brugeren vil ved svar af dette spørgsmål blive præsenteret for en svar-side, se figur 7.21, hvor der forklares lidt om hvad SSID er.



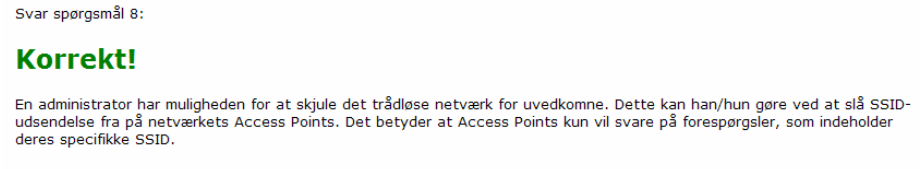
Figur 7.21: Svar på spørgsmål 7

Spørgsmål 8 - Kan det trådløse netværk skjules så uvedkomne ikke kan se det?

(a) Spørgsmål (b) Svar

Figur 7.22: Spørgsmål 8

Der er også generel enighed om at et trådløst netværk kan 'skjules' for andre. En angriber kan dog med rette værktøj altid finde det 'skjulte' netværk, men som udgangspunkt vil et skjult netværk ikke blive set når der blot foretages aktiv-scanning som for eksempel Windows eget program til dette. Brugeren vil også ved dette spørgsmål blive præsenteret for en svar-side som vist i figur 7.23



Figur 7.23: Svar på spørgsmål 8

Spørgsmål 9 og 10 omhandler valg af netværksgodkendelses- og datakrypteringsmetode. Her vil det være en stor fordel for brugeren at benytte det animerede billede, da brugeren derved kan afprøve de mulige kombinationer metoderne.

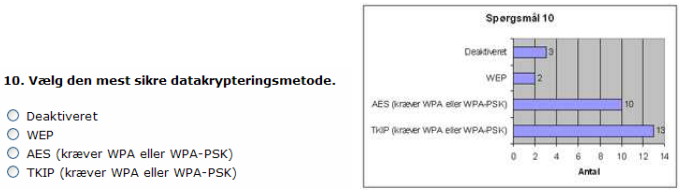
Spørgsmål 9 - Vælg den mest sikre netværksgodkendelsesmetode

(a) Spørgsmål (b) Svar

Figur 7.24: Spørgsmål 9

Som det fremgår af figur 7.24, ved brugerne godt at WPA eller WPA-PSK giver den bedste beskyttelse. Nogle enkelte har dog valgt et Åbent netværk som det sikreste. Dette kan eksempelvis skyldes at brugeren simpelthen ikke forstår begreberne brugt i spørgsmålet og derfor bare vælger det som Windows har som standard opsætning.

Spørgsmål 10 - Vælg den mest sikre datakrypteringmetode



(a) Spørgsmål (b) Svar

Figur 7.25: Spørgsmål 10

Igen er der ret stor enighed om at TKIP og AES giver det sikreste netværk. Enkelte har valgt at Deaktiveret eller WEP vil beskytte netværket nok. Dette kan igen hænge sammen med forståelsen af begreberne og valget af Windows standard opsætning. At så mange brugere har svaret på netop det nederste spørgsmål, kan dog også skyldes at brugerne blot mener at jo længere nede på listen jo mere sikkert er det.

Brugeren vil efter de to spørgsmål blive præsenteret for en svar-side, se figur

7.26.

Svar spørgsmål 9 & 10:

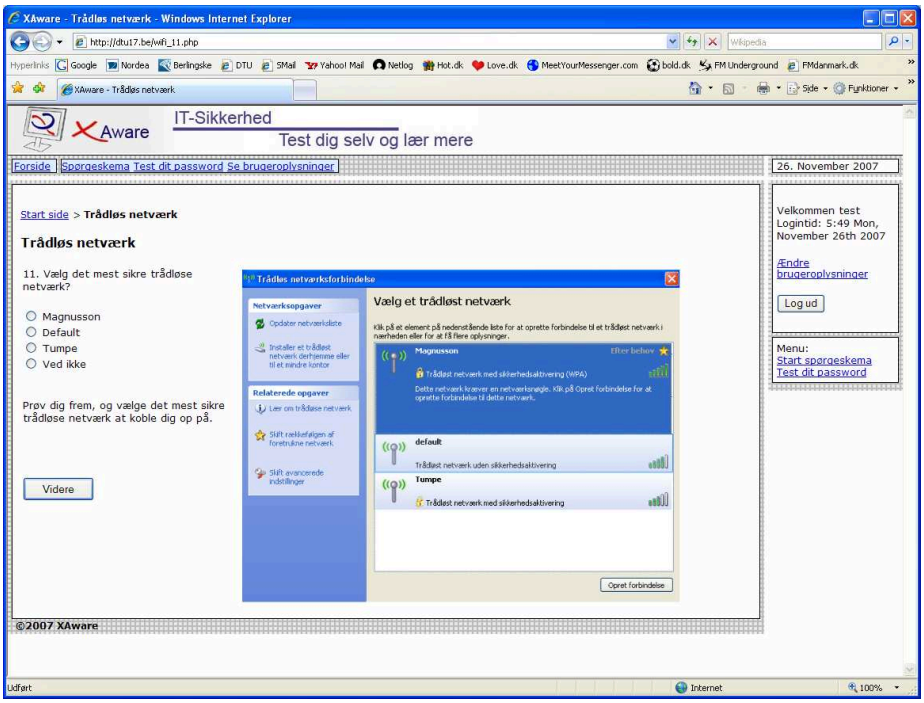
Korrekt!

En kombination af den stærkest tilgængelige krypterings- og netværksgodkendelsesmetode vil altid være at foretrække.

Den ønskede kombination er i dette tilfælde at der bliver valgt enten WPA eller WPA-PSK som de mest sikre netværksgodkendelsesmetoder samt, at der vælges AES eller TKIP som de mest sikre datakrypteringsmetoder.

Figur 7.26: Svar på spørgsmål 9 og 10

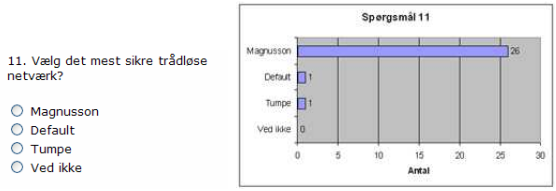
I det efterfølgende spørgsmål introduceres et nyt animeret billede. Denne gang er det af Windows eget program til automatisk oprettelse/forbindelse til trådløse netværk, se figur 7.27.



Figur 7.27: Animeret billede med automatisk oprettelse

Det er her muligt for brugeren at trykke sig rundt på billedet og se hvad de forskellige tilgængelige netværk indeholder. Brugeren skal herefter tage beslutning om hvilket der er det mest sikre at forbinde til.

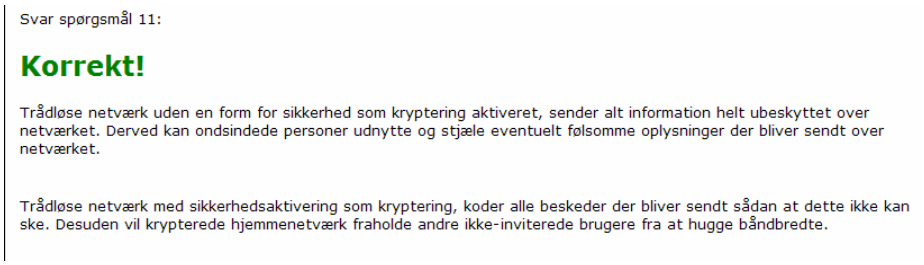
Spørgsmål 11 - Vælg det mest sikre trådløse netværk



(a) Spørgsmål (b) Svar

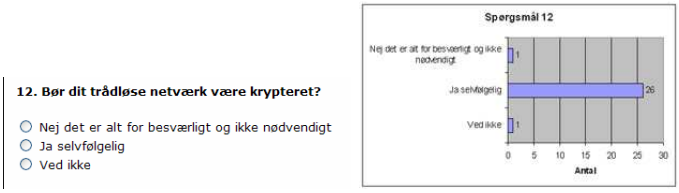
Figur 7.28: Spørgsmål 11

Som det fremgår af resultatet i figur 7.28, kunne de næsten alle brugere gennemskue at det var netværket med WPA-kryptering der var det sikreste. Brugeren blev efterfølgende præsenteret for denne svar-side med en beskrivelse af hvorfor det også netop var det sikreste, se figur 7.29



Figur 7.29: Svar på spørgsmål 11

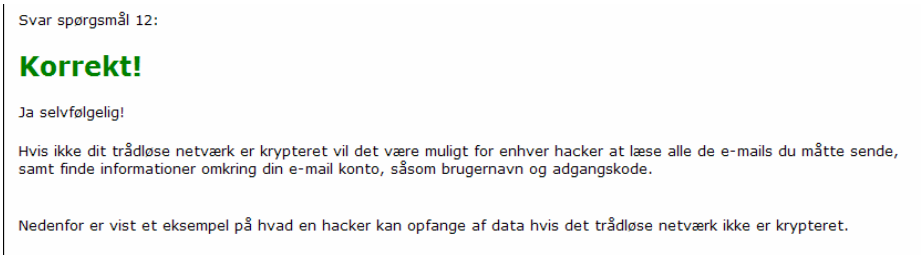
Spørgsmål 12 - Bør dit trådløse netværk være krypteret?



(a) Spørgsmål (b) Svar

Figur 7.30: Spørgsmål 12

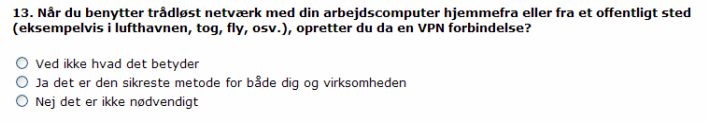
For at samle lidt op på de sidste par spørgsmål, stilles her et meget enkelt spørgsmål for at se om brugeren har set nødvendigheden af kryptering af trådløse netværk. Som det fremgår af figur 7.30, svarer næsten alle brugerne at et trådløst netværk bør være krypteret. Nedenfor i figur 7.31 er svar-siden til dette spørgsmål vist.



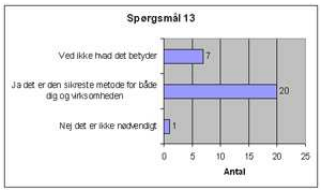
Figur 7.31: Svar til spørgsmål 12

Udover svaret, bliver brugeren på denne side præsenteret med et eksempel på hvor let det er for en angriber at opsnappe informationer på et ikke krypteret trådløst netværk, eksempelvis ved at kunne læse sendte og modtaget emails. Eksemplet bruges lidt som afskrækkelse, hvis brugeren endnu ikke er helt overbevist om krypteringens nødvendighed.

Spørgsmål 13 - Når du benytter trådløst netværk med din arbejdscomputer hjemmefra eller fra et offentligt sted (eksempelvis i lufthavnen, toget, osv.), opretter du da en VPN forbindelse?



(a) Spørgsmål



(b) Svar

Figur 7.32: Spørgsmål 13

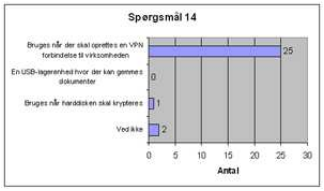
De teknisk kyndige brugere der har svaret på dette spørgeskema virker til at være klar over at den sikreste måde at oprette forbindelse til virksomhedens netværk er gennem en sikker VPN forbindelse. Se resultat i figur 7.32.
Brugeren vil også her blive præsenteret for en svar-side indeholdende information om VPN og hvilke hjælpemidler man kan bruge til det i form af en USB EToken, se figur 7.33

Figur 7.33: Svar på spørgsmål 13

Direkte afledt af foregående spørgsmål og svar stilles her et konkret spørgsmål om brugen af netop sådan en EToken.

Spørgsmål 14 - Hvad bruges denne EToken til?

(a) Spørgsmål

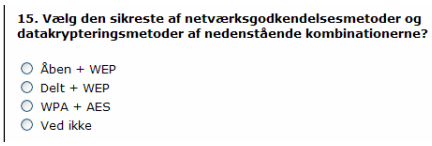


(b) Svar

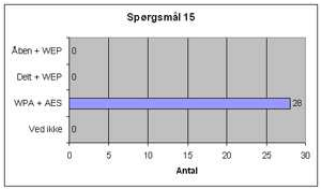
Figur 7.34: Spørgsmål 14

Dette var et spørgsmål næsten alle brugere har svaret rigtigt på, sandsynligvis godt hjulpet på vej af det foregående spørgsmål og svar. Brugeren skulle her gerne kunne genkende billedet af USB EToken og forbinde denne med oprettelse af sikker VPN forbindelse, som denne har af funktion i den konkrete virksomhed.

Spørgsmål 15 - Vælg den sikreste af netværksgodkendelsesmetoder og datakrypteringsmetoder af nedenstående kombinationer



(a) Spørgsmål



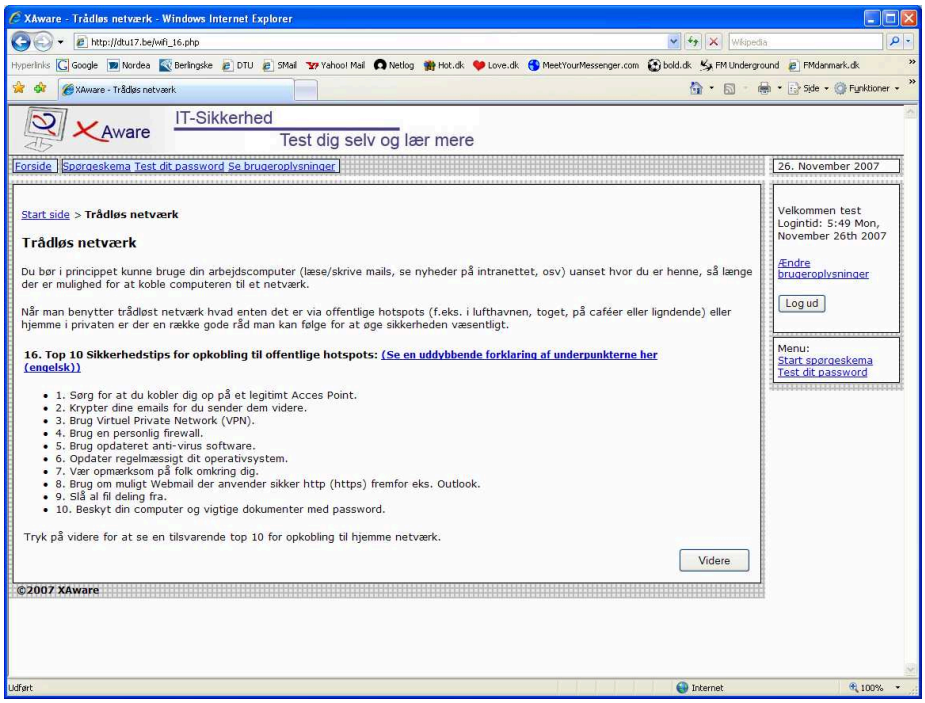
(b) Svar

Figur 7.35: Spørgsmål 15

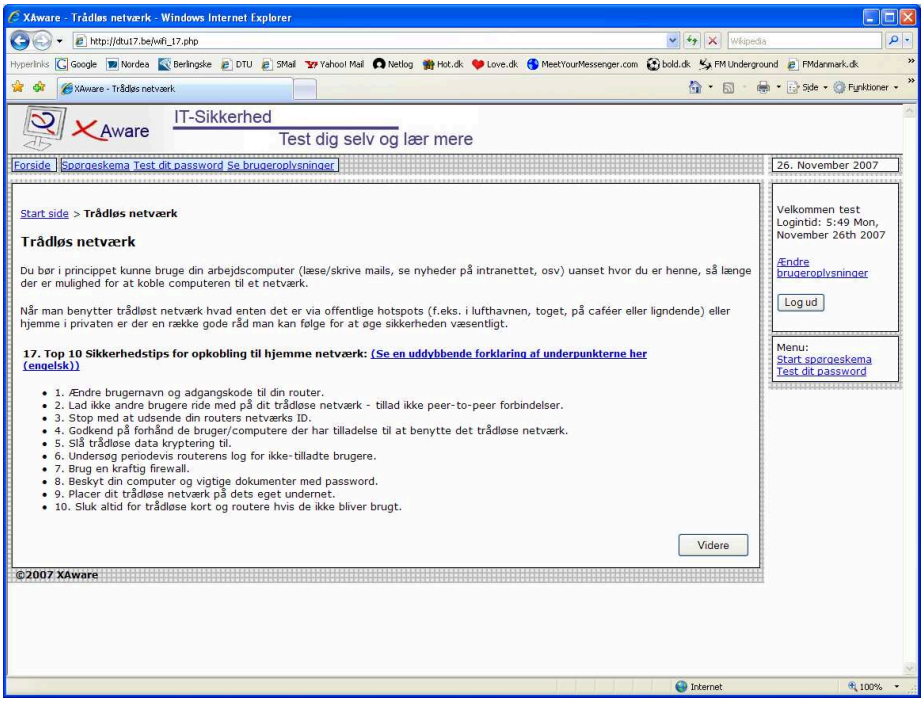
Disse begreber er tidligere i spørgeskemaet blevet gennemgået og er stillet lidt som en test af brugeren om de kan huske eller genkende begreberne og vælge det

rigtige svar. Dette synes at have en tydelig effekt, da alle brugerne har svaret rigtigt på dette spørgsmål, se figur 7.35

For at opsamle på nogle af de generelle råd i forbindelse med oprettelse til trådløse netværk, er spørgsmål 16 og 17 udformet som en top 10-liste med råd om sikre trådløse netværk i henholdsvis hjemmet og på offentlige steder. Se figur 7.36 og figur 7.37.



Figur 7.36: Top-10 råd ved offentlige trådløse netværk(Hot spot)

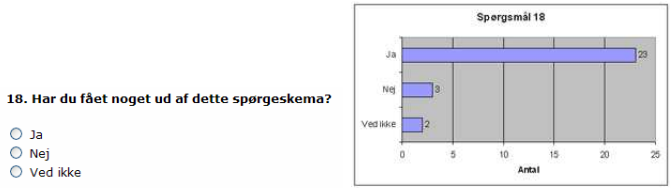


Figur 7.37: Top-10 råd ved private trådløse netværk

Det sidste spørgsmål i forbindelse med spørgeskemaet er om brugeren har fået noget ud af spørgeskemaet.

Spørgsmål 18 - Har du fået noget ud af dette spørgeskema?

De fleste har dertil svaret, at det har været et brugbart spørgeskema.



(a) Spørgsmål (b) Svar

Figur 7.38: Spørgsmål 18

7.3.2 Kommentarer

Fra virksomhedens medarbejdere har jeg fået en del respons i form af kommentarer om siden.
Langt de fleste af disse kommentarer har været positive og nogle også indeholdende kritik. I dette afsnit vil en del af kommentarerne blive gennemgået for at få indsigt i brugernes reaktion på spørgeskemaet.
Nedenfor er listet en række af de brugerreaktioner der er kommet fra svarpersonerne:

'Jeg synes, at kombinationen af spørgeskema og videns-formidling virker godt. Generelt ved jeg ikke specielt meget om trådløse netværk - men dette bidrog med, at jeg fik mere viden. Hjemmesiden virker godt gennemarbejdet...'

'Hvis man ikke kender noget til trådløst netværk, kan man gætte sig til at svare rigtigt på de fleste spørgsmål. Ellers fint spørgeskema.'

At en bruger mener at man kan gætte sig til de fleste spørgsmål, gør egentlig ikke noget. Meningen er mere at få brugerne til at kunne genkende situationer og begreber, og hvis brugeren kan gætte sig til det rigtige svar her, kan vedkomne også gætte sig til det rigtige svar i den virkelige situation.

'Til at beskytte sig mod en hacker, nytter hverken: - skjult SSID (netværket er stadig synligt) - MAC adresse filtrering (MAC adresser sendes som txt-streng og kan kopieres a f hacker). Kryptering, Lange passwords og skift af disse - er vigtiger'

'Prøv at forklar mig hvorfor det øger sikkerheden at man ikke udsender sit ssid. Min holdning er at hvis man benytter WPA så er det ligefrem bare besværligt at man ikke viser sit ssid. Dem der kunne tænkes at hacke dig vil alligevel finde dit trådløse'

Begge ovenstående kommentarer kommer med gode pointer og viser måske at der i spørgeskemaets udformning er lagt for stor vægt på områder som at skjule sit SSID i forhold til mindst lige så væsentlige punkter som kryptering og regelmæssige password skift.

'Ganske fornuftigt spørgeskema du har fået strikket sammen. Selvom jeg nok ikke lærte noget nyt, er det altid godt at få genopfrisket hukommelsen. Man har det jo ind imellem at springe over hvor gærdet er lavest, også selvom man ved bedre.'

'Jeg sys det er et rigtig godt skema, fordi man også får en masse svar med det samme...'

'Jeg har fundet ud af, at jeg ikke ved ret meget om trådløst netværk - uhyggelig oplevelse! Tak for testen...'

7.3.3 Test af kodeord

Det andet spørgeskema omhandlede en test af kodeord, hvor brugeren kunne teste et kodeord for at se hvor sikkert det er.

Antal test	29
Gennemsnitlige score	79.8
Gennemsnitlig længde	8.2
Længde > 7	25 (82.8%)

Tabel 7.1: Test af kodeord

Af tabel 7.1 fremgår det at 29 har prøvet denne test.
Generelt har brugerne ganske gode kodeord med en gennemsnitlig score på næsten 80 ud af 100. I virksomheden er der relativ stor opmærksomhed på at danne sikre kodeord, dette afspejles i denne test. En gennemsnitslængde for kodeordet på 8.2 og hele 82.8% af testene har kodeord med en længde større end 7, tyder på at der generelt er ret stor opmærksomhed på brug af sikre password og at brugerne rent faktisk også følger dette.

7.4 Forbedringer

Der er et par områder hvor spørgeskemaet godt kunne blive forbedret.
Dels ville en revidering af spørgsmålene være en god ide og måske tilføjelse af nye. Et andet område kunne være at give mere præcise instrukser om hvad de

animerede billeder kan og ikke kan, så brugerne ikke bliver forvirret over at nogle faneblade ikke virker når nu alt andet synes at virke normalt.

Der bør i forbindelse med revideringen af spørgsmålene lægges større vægt på emner som regelmæssige passwordskift og kryptering frem for eksempelvis det at skjule sit SSID.

Det ville også være værd at overveje om det layout og tidsmæssigt ville være muligt at lave spørgeskemaet fuldstændigt i Captivate og derved undgå at brugeren svarer '2' gange ved først at vælge det rigtige svar på det animerede billede og dernæst markere det rigtige svar i en html-form.

7.5 Udvikling af nye spørgeskemaer

Opbygningen af henholdsvis databasen og html-layoutet gør at det simpelt at tilføje nye spørgeskemaer.

Databasen
Et nyt spørgeskema skal blot have oprettet sin egen tabel i databasen med en fremmednøgle til medlemsnummeret i brugerdata-tabellen.

Header.php
For at bevare samme layout bør header.php importeres i de nye html/php-sider

Menu.php
For at et nyt spørgeskema vil fremgå i menuen øverst eller til højre, skal startsiden til spørgeskemaet tilføjes i denne.

Functions.php
Denne fil indeholder funktioner med kommunikation til databasen, her skal oprettes en ny funktion der sørger for at de indsamlede data ved nye spørgeskemaer bliver sendt til databasen.

Største udfordring ved oprettelse af nye spørgeskemaer vil blive at udvikle nye animerede billeder. Dette er en tidskrævende proces og man skal nok påregne en udviklingstid på omkring 2-3 uger per animering, alt efter hvor godt udvikleren kender Captivate og hvor omfattende animeringen skal være.

Et Captivate projekt udmønter sig som sagt i en swf-fil der kan indlejres i almindelige html-baserede sider. Derved kan et spørgeskema fuldt udviklet i Captivate relativt let indlejres på eksempelvis sider på virksomheden Intranet eller lignende.

7.6 Opsummering

Hjemmesiden om sikkerhedsbevidsthed opfylder de i analyse og design afsnittet opsatte krav ved at det gør det muligt for brugerne at teste deres viden inden for sikkerhedsbevidsthed samtidig med at deres reaktioner optages til at blive vist statistisk.

Resultaterne fra de 28 brugere viste at der generelt er stor opmærksomhed på de sikkerhedsproblemer der relaterer sig til det at benytte trådløse netværk og at brugerne også er bevidste om dem.

Generelt har brugerne reageret positivt på at det var et spørgeskema med animerede billeder hvor det var muligt at prøve sig frem på. Direkte adspurgt mener flere af brugerne at disse animationer har hjulpet til en øget forståelsen af spørgsmålet.
Også ud fra spørgsmålene synes det grafiske i de animerede spørgsmål at have en stor effekt på hvordan brugerne vurderer og svarer på spørgsmålene.

Resultaterne viste også at en metode, som det først at stille et spørgsmål og derefter direkte præsentere brugeren for et svar og en forklaring har en positiv effekt. Faktisk svarede samtlige brugere korrekt på det sidste spørgsmål om kombinationen af den sikreste netværksgodkendelsesmetode og datakrypteringsmetode, hvor der havde været noget usikkerhed om det første gang det blev præsenteret.

Om spørgeskemaerne fremover skal udvikles udelukkende i captivate som flash interaktive animationer vil have sine fordele og ulemper. Fordelen vil være et flottere og mere strømlinet layout. Ulempen vil være tiden det tager at udvikle i captivate op mod tiden det tager at udvikle en almindelig html-side. Der er også endnu lidt kompliceret hvordan opsamling og videresendelse af data skal ske fra captivate.

Kapitel 8

Konklusion

En række af de sikkerhedsproblemer der er i forbindelse med mobile medarbejdere er blevet undersøgt Potentielle risici er blevet fundet og mulige løsningsforslag givet.
På baggrund af en udarbejdet risikoanalyse er der givet forslag til udformningen af en sikkerhedspolitik for mobile medarbejdere. Begge kan hjælpe en virksomheds ledelse med at lægge et passende basisniveau af sikkerhed. Ved hjælp af risikoanalysen, informationssikkerhedspolitikken og undersøgelsen af sikkerhedsproblemer i forbindelse med mobile medarbejdere er en vurdering af sikkerheden i en konkret virksomhed udarbejdet.
Sikkerheden for de mobile medarbejderes udstyr var ganske god og kun mindre ting og uhensigtsmæssigheder er fundet.

Der er i forbindelse med undersøgelsen af virksomheden også forsøgt at måle et niveau af sikkerhedsbevidsthed hos relevante medarbejdere. Til det formål er der udviklet et Internetbaseret spørgeskema der indeholder animerede billeder som svarpersonen kan benytte interaktivt.
Det er kendt, at brugere er meget vaneprægede og bedst evner at forholde sig til scenarier, som direkte kan sammenlignes med situationer de er vant til.

Animerede spørgeskemaer er en stor fordel når det drejer sig om et emne så teknisk som sikkerhedsbevidsthed. Udfordringen ligger i at få det konstruerede scenarier som bedst muligt kan relateres til de visninger brugeren er vant til fra

sin egen computer. På den måde vil brugeren ikke behøve at overveje meningen af spørgsmålet, men blot svare som han ville i en normal situation.

Resultaterne af spørgeskemaet viste, at medarbejderne i virksomheden har et forholdsvis højt niveau af bevidsthed når det kommer til brug af trådløse netværk. Gruppen af medarbejdere der har svaret på spørgeskemaet er da også alle af en akademisk baggrund og arbejder dagligt med computere, mange af dem er udviklere. Så der er i forvejen en forholdsvis stor teknisk forståelse hos svarpersonerne.
Mange var dog meget positive over for muligheden, at kunne trykke sig rundt på de animerede billeder og derved blive sat i en kendt situation. Dette var helt klart med til at øge forståelsen af spørgsmålet.
En anden 'teknik' der blev afprøvet i spørgeskemaet var, at der først blev stillet et spørgsmål med nogle tekniske begreber hertil kom et svar og en uddybende forklaring. Senere i spørgeskemaet blev begrebet igen introduceret (i form af et andet spørgsmål) og her viste det sig faktisk at samtlige svarpersoner kunne svare rigtig på spørgsmålet. Konklusionen på det må være at denne teknik virker.

Adobe Captivate kan benyttes til udvikling af animerede spørgeskemaer da det gør det nemt at optage screenshots, til at danne animerede interaktive programsimulationer. Det skal dog gøres klart at programmet ikke er udviklet til at bygge animerede spørgeskemaer, og det kan dertil stærkt anbefales at man kun benytter Captivate til de dele som skal være animerede og holder al information udefra i et beskrivende sprog som html eller lignende.

8.1 Fremtidigt arbejde

Som det så ofte sker når noget undersøges, rejser det mindst lige så mange nye spørgsmål som det besvarer. Desværre kan ikke alle besvares indenfor projektets tidsfrist. Men nogle af spørgsmålene som står åbne beskrives her.

Det ville være en god ide også at se på sikkerhedsproblemer ved teknologier som Bluetooth og 3G, da de begge er teknologier som virksomheden inden for nærmeste fremtid ønsker at implementere.

En interessant vinkel kunne være at gentage spørgeskema undersøgelsen (i ny eller tilsvarende form) i virksomheden igen om 5-6 måneder og se på om medarbejderne kan huske noget af dette spørgeskema.

Bilag A

Ordbog

Ad-hoc netværk Et netværk uden infrastruktur, hvor enhederne på netværket bliver tilføjet, når de er indenfor rækkevidde. Ad-hoc netværk anvendes f.eks. i midlertidige netværk på konferencer og lignende. Pga. netværkets ukontrollerede natur anses denne netværksform for mindre sikker end netværk baseret på en fast og kontrolleret infrastruktur.

AH (Authentication Header) En protokol, der anvendes af IPSec, til autentificering af den beskyttede pakke.

Autentificering Den proces, hvor det valideres at en person eller noget andet rent faktisk er den, som han eller det påstår at være. I computer netværk er password den mest udbredte metode til autentificering. Ved at anvende autentificering kan identitetstyveri undgås.

Brute-force angreb. Et angreb på et kryptografisk sikkerhedssystem, hvor alle mulige værdier afprøves. Angrebet kan f.eks. udføres på kryptografiske nøgler. Brute-force angreb er ofte meget tidskrævende, men er en mulighed, når alt andet er afprøvet.

Certifikat En kryptografisk sammenbinding af identitet og en offentlig nøgle. Certifikater anvendes ofte til autentificering, hvor klienten præsenterer sit certifikat, og derefter beviser besiddelse af den til certifikatet tilhørende private nøgle.

DMZ (demilitariseret zone) En del af netværket, som ikke er beskyttet på samme måde som det interne net, og som er adskilt fra dette. DMZ markerer overgangen fra et sikkert netværk (det interne) til et usikkert netværk (eks. Internettet).

ESP (Encapsulated Security Payload) En protokol, der anvendes i IPSec, til kryptering og autentificering af den beskyttede pakke.

Fortrolighed Et grundprincip indenfor datasikkerhed. Fortrolighed omhandler begrænsningen af datas tilgængelighed til kun at indbefatte godkendte personer. Dette udføres ofte i praksis ved hjælp af kryptering, hvor fortroligheden er bevaret så længe data forbliver krypteret.

Gateway En gateway er en netværksenhed, som arbejdsstationer, servere og andre enheder benytter, for at komme fra et netværk til et andet (f.eks. fra virksomhedens interne netværk til Internettet). Således bør enhver netværksenhed vide, hvad adressen på den aktuelle gateway er, så trafik, som skal sendes ud af netværket, kan routes via denne gateway, som igen har information om, hvad den næste gateway er osv. Oftest vil en gateway i en virksomheds netværk være en router.

GPRS (General Packet Radio Service) En standard til dataoverførsel fra GSM-telefoner. Hastighederne i GPRS ligger alt efter typen mellem 14 til 58 kbit/s.

GSM (Global System for Mobile Communications) Den mest udbredte standard, der anvendes til mobiltelefoni.

Hardwarebaseret autentificering En form for autentificering, hvor en identifikator internt eller eksternt på den autentificerede enhed benyttes i autentificeringen. Eksempler herpå er USB-tokens til certifikater og tokens til engangskodeord.

HTTP (Hyper Text Transfer Protocol) En applikationslagsprotokol, der anvendes på Internettet til dataoverførsel, f.eks. af hjemmesider.

HTTPS (Hyper Text Transfer Protocol over SSL) En sikker version af HTTP, der anvender SSL/TLS til beskyttelse af trafikken.

IDS (Intrusion Detection System), der anvendes til at opdage angreb på enten en enhed eller et netværk.

IKE (Internet Key Exchange) En protokol, der anvendes til at oprette en IPSec VPN forbindelse. I protokollen forhandles om der skal anvendes NAT-traversal og hvilke algoritmer, der anvendes til beskyttelse af VPN forbindelsen.

Integritet Et grundprincip indenfor datasikkerhed. Integritet omhandler, at data kun kan ændres af godkendte personer på tilladte måder. Indenfor kommunikation er afsenderintegritet et meget anvendt begreb, der giver modtageren forvisning om, at det modtagne vitterlig stammer fra den opgivne afsender.

IPSec (Internet Protocol Security) En protokol til beskyttelse af IP pakker, hvilket benyttes til VPN. IPSec benytter AH og ESP til kryptering og autentificering af pakkerne, mens IKE anvendes til at forhandle VPN forbindelsens egenskaber mht. algoritmer osv.

MAC-adresse (Media Access Control- adresse) En MAC-adresse bruges til at identificere en netværksknude på datalinklaget i OSI-modellen.

NAT (Network Address Translation) NAT er en teknik til at skabe private, interne IP-adresser i en virksomhed. NAT-enheden, typisk en router, oversætter mellem en intern IP-adresse og portnummer til offentlige IP-adresser og portnumre. Da portnummeret skal være tilgængeligt for at kunne foretage NAT, anvendes NAT-Traversal til håndtering af IPSec VPN forbindelser. Derved indkapsles IPSec pakker i UDP, hvorved et portnummer bliver tilgængeligt.

Offentlig nøgle Se privat nøgle.

OSI reference model Se appendix B.

Pakke En betegnelse for enheder, der udgør netværkstrafikken på lag 3 i OSI modellen.

PDA (Personal Digital Assistent) En håndholdt lommecomputer, der bl.a. kombinerer kalender, e-mail, telefon/fax og netværksfunktionalitet. Forskellen mellem en PDA og en smartphone er, at en PDA funktionelt ligner en PC mere end smartphonen gør.

PKI (Public Key Infrastructure) En infrastruktur hvor alle parter besidder et privat/offentligt nøglepar. Denne infrastruktur kræves for at kunne anvende certifikater.

Port En benævnelse for en logisk forbindelse mellem PC'ere. En PC indeholder 65536 porte, der benyttes til transport af forskellige protokoller som defineret i Internet Assigned Number Authority (IANA).

Privat nøgle En krypteringsnøgle, der anvendes sammen med en offentlig nøgle til asymmetrisk kryptering. Kryptering med den private nøgle dekrypteres med den offentlige nøgle og omvendt. Dette bruges i digitale certifikater, hvor en offentlig nøgle knyttes sammen med en identitet gennem asymmetrisk kryptering.

Ramme En betegnelse for enheder, der udgør netværkstrafikken på lag 2. Således afsendes en besked opdelt i rammer af en bestemt størrelse, som når de modtages, samles igen så hele beskeden igen fremstår i sin helhed.

Sikkerhedspolitik En formel specifikation af de regler medarbejdere med adgang til virksomhedens teknologi- og informationsmæssige værdier skal overholde.

Smartphone En telefon med funktionaliteter, der ikke normalt forbindes med telefoner. Dette kan f.eks. være kalender, e-mail klient, osv.

Sniffer Et program, der anvendes til at opfange netværkstrafik. Der opfanges alle rammer, der er tilgængelige for snifferen, hvilket kan benyttes af administratorer til analyse af trafikken. Alternativt kan en angriber benytte en sniffer til aflytning.

Social engineering En proces hvor en angriber franarrer informationer ved overtalelse.

Split tunneling En måde at konfigurere VPN klienter som f.eks. på den mobile medarbejders udstyr, således at internettrafik ikke sendes via virksomhedens VPN koncentrator, men direkte via arbejdspladsens opkobling til Internettet. Dette sætter mindre krav til båndbredden i virksomheden, men sænker sikkerheden, idet virksomheden ikke har samme kontrol over den internettrafik, som udstyret udsender.

Spyware Ondsindede programmer, der tager helt eller delvist kontrol over et system uden ejerens samtykke.

SSID (Service Set Identifier) Navnet på et trådløst 802.11 netværk. Alle parter i netværket skal benytte dette navn for at kunne kommunikere med hinanden.

SSID-udsendelse Et trådløst 802.11 netværk kan opdages ved, at en klient udsender en forespørgsel til alle trådløse netværk om deres SSID. Hvis SSID-udsendelsen er slået fra på netværket, ignoreres forespørgslen. Ved deaktivering kræver at trådløse klienter skal kende netværkets SSID på forhånd, hvilket kan skjule netværket fra angribere. Med et sniffer program kan denne sikkerhed dog let omgås, da SSID fremgår af hver sendt ramme.

SSL (Secure Socket Layer) Se TLS.

Tilgængelighed Et grundprincip indenfor datasikkerhed. Princippet omhandler at data skal være tilgængelige, når de skal anvendes af autoriserede personer.

TKIP (Temporal Key Integrity Protocol) En lag 2 kryptering, der anvendes i 802.12. TKIP anses for en midlertidig udbedring af problemet med WEP.

TLS (Transport Layer Security) En sikkerhedsprotokol der beskytter applikationsprotokoller inden de indkapsles i en transportprotokol. TLS er afløseren til SSL, og anvender kryptering og autentisering af endepunkterne til f.eks. en sikker forbindelse til netbank. TLS anvender et handshake til autentificering af endepunkterne.

To-faktor autentificering Autentificering, hvor der benyttes to faktorer til at fastslå klientens identitet. Password, certifikater og biometriske data er eksempler på faktorer der kan sammensætte to-faktor autentificering.

Trojansk hest Et nyttigt eller tilsyneladende nyttigt program, der indeholder en skjult kode med ondsindet funktion.

Udsendelse Udsending af en ramme med en generel adresse, hvorved den modtages af alle indenfor afsenderens udsendelsesdomæne. Udsendelse anvendes ofte i forbindelse med oprettelsen af en forbindelse til en enhed, hvor adressen ikke på forhånd er kendt.

Virus Et program, som kan 'smitte' andre programmer ved at modificerer dem. Denne modifikation inkluderer en kopi af virussen, som så igen kan smitte andre programmer. Vira indeholder som regel ondsindet kode, der er til gene for anvendelsen af en inficeret maskine.

VPN (Virtual Private Network) VPN kan benyttes til at forbinde enheder på tværs af usikre medier, f.eks. Internettet. Dermed sikres forbindelser over offentlige netværk fra eksterne lokaliteter til virksomhedens netværk. Ofte vil trafikken blive krypteret bl.a. for at undgå, at data kan aflyttes. VPN fungerer ved at lave en tunnel, hvor en protokol beskyttes og indkapsles i en anden protokol.

VPN-klient En software- eller hardware enhed, som typisk etablerer forbindelse til en VPN koncentrator. På den mobile medarbejders udstyr vil VPN klienten være softwarebaseret.

VPN Koncentrator En hardware enhed anvendt til at terminere VPN forbindelser. Ved at implementere koncentratoren i hardware opnås en bedre ydeevne i forhold til software. Dette er relevant, da kryptering og dekryptering af mange VPN forbindelser kan være ressourcekrævende.

Bilag B

OSI-modellen

OSI-modellen eller OSI-reference model er en lagdelt, abstrakt beskrivelse af kommunikation og netværks protokol design.[25]
OSI modellen er et hierakisk system af syv lag, der definerer kravene for al kommunikation mellem to computere:

OSI modellen deler protokol-funktionerne ind i en række lag. Hvert lag har den funktion, at det kun benytter det underliggende lags funktioner, og kun tilbyder funktioner til laget over.

Lag 7: Applikationslaget
Applikationslaget danner grundlag for at brugeren har adgang til information på netværket via programmel. Dette lag er brugergrænsefladen, eller brugerinterfacet til programmet, og derigennem til netværket. Eksempler på applikationslag-protokoller kunne være Telnet, File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP) and Hypertext Transfer Protocol (HTTP).

Lag 6: Præsentationslaget
Præsentationslaget omdanner data til en (af programmet) kendt standard grænseflade, og/eller andre data strukturer. F.eks. til og fra XML.

Lag 5: Sessionslaget
Sessionslaget er det lag der er ansvarlige for "Terminated gracefully"der er en del af TCP og for session checkpointing og recovery, hvis anvendelse ikke er særlig udbredt på internettet.

Nr	Lag	Beskrivelse
7	Applikation	Direkte support til applikations processer for forskellige typer af distribueret aktivitet
6	Præsentation	Formatering af data, så de kan præsenteres for applikationslaget.
5	Session	Håndterer forbindelser (sessions) mellem applikationerne.
4	Transport	Sikrer at data leveres fejlfrit i korrekt sekvens og uden tab eller duplikeringer.
3	Netværk	Kontrollerer driften af subnettet og afgør hvilken fysisk vej data skal tage baseret på netværks-tilstanden.
2	Data Link	Sikrer fejlfri transmission af data rammer fra en enhed til en anden over den fysiske linje.
1	Fysisk	Dækker over det fysiske interface mellem comuteren og netværket.

Tabel B.1: OSI-Model

Lag 4: Transportlaget
Transportlaget tillader umærkeligt dataoverførsler mellem brugere, og aflaster således de øvre lag for bekymringer, mens de giver pålidelige dataoverførsler. Transportlaget tjekker pålideligheden af an given forbindelse via flowkontrol, "indpakning"/"udpakning"og fejlkontrol. Nogle protokoller er "state-"og "connection-"orienterede. Dette betyder at transportlaget holder styr på pakkerne og gensender dem der aldrig kom frem. Det bedst kendte eksempel på en transportlagsprotokol, er Transmission Control Protocol (TCP). Transportlaget er det lag der omdanner data til til TCP pakker eller User Datagram Protocol (UDP), Stream Control Transmission Protocol (SCTP), osv. til pakker.

Lag 3: Netværkslaget
Netværkslaget tilbyder de rutiner der skal til, for at sende en variabel størrelse datablok, fra kilde til endestation, via et eller flere netværk. Dette lag holder også styr på QoS som "Transportlaget"lever højt på. Netværkslaget udfører routing-funktioner (sender pakkerne til deres rette modtager), kan udføre ind- og udpakning og rapportere om leveringsfejl. Routere arbejder i dette lag, sender data gennem det udvidede netværk og gør internettet muligt (der eksisterer også 3. lags (eller IP) Switche). Dette er et logisk adresseringssystem, hvor værdier er valgt af netværksadministratoren. Adressesystemet er struktureret hierakisk. Det bedste eksempel på en layer 3 protokol er IP

Lag 2: Data Link-laget
Data Link-laget giver mulighed for at overføre data mellem netværks-moduler og finde, muligvis rette, fejl der måtte optræde i det fysiske lag. Adresserings-

metoden er fysisk, d.v.s. MAC-adressen, der i de fleste tilfælde er "hard-coded"inde i netkortet. Nogle netværks-kort understøtter at administratoren specificerer en anden MAC-adresse, men som regel er det ikke muligt at ændre den. Adresseringen er ikke hierakisk opdelt. Det bedst kendte eksempel på dette lag er Ethernet. Andre eksempler på data link protokoller er HDLC og ADCCP for point-to-point eller packet-switched netværk, og Aloha for lokale netværk. På IEEE 802 netværk, og nogle andre netværk, som FDDI, kan dette lag være opdelt i et MAC lag og selve Logical Link Control eller LLC-laget. Det arrangerer bits fra det fysiske lag til frames (brugt af Netværks-laget).

I dette lag arbejder Netværksbroer og Switche. Forbindelse foregår mellem lokalt tilsluttede netværk der danner "Data link"domæner til unicast- eller broadcast-forwarding. Andre protokoller kan blive pålagt frames til at danne tunneller og logisk adskilte "Data link"domæner.

Lag 1: Det fysiske lag
Det fysiske lag definerer alle elektriske og fysiske rammer for netværks-elementerne. Dette lag dækker stik-type, spændinger og kabel-specificationerne. Netværks-hubs, repeatere, netværks-kort og Host Bus Adaptere (HBA'er brugt i Storage Area Networks) er fysisk-lags enhederare. De mest fremtrædende funktioner af laget er:

- Oprettelse og afslutning a elektrisk forbindelse til overførsels-mediet.
- Deltager i effektivisering af kommunikation mellem flere brugere. F.eks. contention ("vente på stilhed, før man blander sig") og flow-styring.
- Modulering eller oversættelse mellem repræsentationen af digitale data til tilsluttet udstyr og tilsvarende signaler sendt via kommunikations kanalen. Det betyder at de skal omdannes så de kan sendes v.h.a. enten kabel (som kobber eller fiber) eller radio.

I dette lag findes SCSI "busser"og diverse fysisk definerede Ethernet standarder; Ethernet indeholder både dette lag og "data link laget"(lag 2). Det samme gælder andre lokale netværks typer, som Token ring, FDDI og Wireless LAN.

Bilag C

Liste over mulige bevidsthedsfremmende tekniker

Listen kan betragtes som et idékatalog, hvorfra der kan vælges hensigtsmæssige aktiviteter/tekniker. Vælg ikke blot én eller to metoder - men 10 eller 20. Gentagelseseffekten er som nævnt væsentlig og en kombination vil blot forstærker effekten. Gentagelser overbeviser også målgruppen om, at IT-sikkerhed er et emne, som tages alvorligt og har ledelsens opbakning.

Personlig kommunikation

- Planlæg og gennemfør specielle kurser hvert år for brugere, systemadministratorer, sikkerhedskoordinatorer, nyansatte og andre grupper med udgangspunkt i behovsanalyser.
- Engager foredragsholdere udefra med ekspertviden om sikkerhedsforhold til at holde indlæg på virksomhedskonferencer, afdelingsmøder eller ved andre lejligheder, hvor personalet i forvejen er samlet.
- Udlever materiale og drøft sikkerhedsspørgsmål ved orienteringsmøder for nyansatte.
- Send toneangivende IT-medarbejdere til eksterne konferencer omkring sik-

kerhedsforhold.

- Hold videokonferencer, hvor man diskuterer sikkerhedsspørgsmål på tværs af lokaliteter.
- Arranger demonstrationer, hvor man tydeliggør sårbarheder (f.eks. tigerteam og penetrationstests).
- Etabler en dedikeret demonstrationscomputer/et isoleret netværk og demonstrer hvad der kan ske når en ondskabsfuld virus angriber en pc.
- Gennemfør risikovurderinger med interviews o.a. metoder, som involverer personalet i processen.
- Gennemfør undersøgelser hvor I fokuserer på overholdelsen af regelsættene om ophavsret.
- Indfør sanktioner overført fra Færdselsloven eller sportsverdenen, som afspejler graden af brud på politik og retningslinier.
- Gennemfør interne audits, hvor I checker for graden af overensstemmelse mellem krav og praksis.
- Gennemfør eksterne audits, hvor I lader en sikkerhedskonsulent checke for graden af overensstemmelse.
- Gennemgå computerne for at identificere ulovligt kopieret/installeret software.
- Installer et management system, som registrerer al installeret software og muliggør licensstyring og drøftelser med brugere, som anvender uautoriseret software.
- Integrer sikkerhedsrelaterede emner i de eksisterende og nye kursusforløb.
- Kræv af medarbejderne, at de gennemfører en online quiz, som dokumenterer deres kendskab til politikker og retningslinier. Kun hvis de opnår et tilfredsstillende resultat af denne quiz, vil de kunne tildeles (og evt. bevare) adgangsrettigheder til systemerne.
- Etabler et tværgående IT sikkerhedsudvalg på ledelsesniveau - og markedsfør begrundelsen herfor.
- Etabler en komite bestående af systemadministratorer og andre, som skal beskæftige sig med sikkerhedsrelaterede emner.
- Afhold kvartalsvise frokostmøder for systemadministratorer hvor der med udgangspunkt i en struktureret dagsorden diskuteres sikkerhedsrelaterede emner.

- Igangsæt strategisk planlægning, udvikling af nye produkter og andre initiativer hvor information og IT er en væsentlig forudsætning for konkurrencemæssige fordele.
- Udskyd idriftsættelse af nye og ønskede services (f.eks. Internetadgang eller hjemmearbejdspladser) indtil det ønskede sikkerhedsniveau er etableret (firewalls, segmentering, VPN).
- Nedlæg forbud mod at nye eller ændrede applikationer flyttes i produktion før det ønskede sikkerhedsniveau er dokumenteret og etableret. Inddrag den forretningsmæssige ledelse i drøftelserne.
- Implementer en ny og mere restriktiv forretningsgang omkring godkendelse af ændringer (Change Management).
- Giv amnesti i et begrænset tidsrum til medarbejdere, som er blevet bevidst om, at de overtræder politik eller retningslinier, så disse kan få assistance til at få forholdene bragt i orden.
- Test backuprutiner og backups som evt. gennemføres på afdelingsniveau eller på adskilte lokaliteter af systemadministratorer der. Diskuter evt. problemstillinger med de relevante ledere.
- Udnævn en dag til årlig 'Informations Sikkerheds Dag'. Gennemfør særlig uddannelse, kampagner o.a.
- Gennemfør (og markedsfør massivt internt) en undersøgelse af et brud på sikkerheden. Inddrag et antal relevante medarbejdere i denne undersøgelse.
- Planlæg orienteringsmøder med topledelsen mhp. drøftelse af de overordnede forudsætninger for at gennemføre en ændring af virksomhedskulturen, således at denne i højere grad understøtter IT sikkerheden.
- Gennemfør en gap analyse, hvor det eksisterende trænings og orienteringsmateriale omkring sikkerhedsforhold sammenholdes med de budskaber, som ledelsen ønsker at kommunikere ud. Såfremt der er afvigelser skal ledelsen foranledige igangsat afhjælpning.

Skriftlig kommunikation

- Gennemfør en spørgeskemaundersøgelse hos mellemlederne hvor disse spørges om, hvad man kunne gøre for at højne sikkerheden. De vil herved formodentligt reflektere over forhold, som de ellers ikke har fokus på.
- Gennemfør en spørgeskemaundersøgelse hos kunder, leverandører og andre samarbejdspartnere hvor disse spørges om, hvad man kunne gøre for yderligere at sikre kommunikationen.

- Tilføj spørgsmål om informationssikkerhed til eksisterende spørgeskemaer til Balanced Scorecards o.a.
- Kræv underskrift på en erklæring om personligt ansvar/ ansættelseskontrakten hvor medarbejderen erklærer sig indforstået med at overholdelse af politik og retningslinier er en forudsætning for et fortsat ansættelsesforhold.
- Kræv underskrift på en formular, hvor medarbejderen bekræfter at have modtaget en kopi af IT-sikkerhedshåndbogen samt læst og forstået indholdet.
- Kræv årligt en underskrift på en formular, hvor medarbejderen bekræfter at være ajour med indholdet af IT-sikkerhedshåndbogen og have forstået indholdet.
- Kræv at medarbejderne underskriver en erklæring om at overholde sikkerhedspolitik og relevante retningslinier før de får udleveret user ID.
- Skriv artikler om sikkerhedsforhold til interne personaleblade o.l.
- Udgiv periodevist skriftlige procedurer, standarder og statusrapporter - eller referencelister til de gældende.
- Udgiv små brochurer til slutbrugerne omkring hensigtsmæssig/sikker adfærd.
- Udgiv et lær-selv hæfte, som introducerer brugerne til de basale sikkerhedsemner.
- Udarbejd memoer, som topledelsens løbende kan udsende, hvor brugerne mindes om korrekt og sikker adfærd.
- Rundsend udklip fra aviser og fagblade, hvor sikkerhedsproblemer bliver omtalt.
- Ophæng plakater og skilte i lokalerne med: "Har du husket, at..."og lignende sikkerhedsrelaterede påmindelser.
- Placer klistermærker og lignende hvor de ses - f.eks. på kopimaskiner, fax, telefoner, o.a.
- Lav specielle labels til flytbare aktiver/medier som muliggør mærkning med følsomhed, håndteringsanvisning og ejerskab.
- Send sikkerhedsopråb til interne nyhedsgrupper m.v.
- Indlæg sikkerhedsfoldere i kuverter med lønsedler og flybilletter.

- Indarbejd forslag og ideer til sikkerhedsforanstaltninger i ramme-/fasemodellen for systemudvikling.
- Vær opmærksom på områder hvor der kan være uklar ansvarsplacering på sikkerhedsområdet - og udsend løbende afklarende memoer.
- Udarbejd funktions- og stillingsbeskrivelser som tydeliggør den enkeltes ansvar og opgaver i relation til sikkerheden.
- Udarbejd målbeskrivelser for de enkelte organisatoriske enheder hvor sikkerhedsforhold tydeliggøres som målområde.
- Udarbejd en arkitekturoversigt som viser/refererer til de etablerede sikkerhedsforanstaltninger (fysiske, logiske, administrative) - eller integrer sikkerheden i teknologibeskrivelserne på andre måder.
- Udgiv en IT sikkerheds håndbog indeholdende politikker, retningslinier, kontaktpersoner og en liste over godkendte applikationer, komponenter mv.
- Udarbejd checklister som forholder sig til hvordan man implementerer en IT sikkerhedspolitik
- Skriv detaljerede instruktioner for backup og insister på at de bliver fulgt.
- Udvikl og test en beredskabs-/katastrofeplan.
- Kræv at de ansvarlige ledere udfylder en standardiseret erklæring om accept af risikoen i de situationer hvor de inden for ansvarsområdet ikke er i overensstemmelse med politik og retningslinier og hvor der ikke er iværksat aktiviteter, som hurtigt kan sikre en sådan overensstemmelse.
- Udarbejd tavshedserklærings-blanketter og uddan personalet i hvornår de skal anvendes.
- Udarbejd konkurrenceklausuls-blanketter og uddan personalet i hvornår de skal anvendes.
- Udarbejd orienteringsmateriale, som kan udleveres til alle de, som kommer i kontakt med forretningshemmeligheder, hvor der henvises til specifikke regler og retningslinier.
- Udarbejd rapporter om de seneste sikkerhedsmæssige hændelser sammen med evt. forslag til tiltag, som kan forbedre sikkerheden (eller beskrivelse af, hvad man efterfølgende allerede har gjort). Distribueres efter 'need to know' princippet.
- Udarbejd en oversigt over og et resume af relevant lovgivning m.v. af betydning for organisationens sikkerhedsniveau.

Kommunikation via systemer

- Tilføj sikkerhedsinstruktioner til hjælpeskærmbilleder i applikationer og hjælpeprogrammer.
- Køb træningssoftware om IT-sikkerhed og kræv at personalet kører forløbet igennem. Ideelt set skal der ske automatisk rapportering til en central log, hvor der registreres tidspunkter o.a. og anvendes digital signatur - dette sikrer bevis for, at medarbejderne har læst politik, retningslinier m.v. i tilfælde af tvistigheder.
- Etabler online quiz som afdækker medarbejdernes kendskab til politik og retningslinier. Tilknyt evt. præmier/lodtrækning om præmier for korrekt besvarelse.
- Før brugerne får adgangsrettigheder til bestemte applikationer og services skal de gennemføre et online træningsprogram.
- Fremstil en cd med relevant sikkerhedsmateriale - herunder værktøjer til kryptering, password generering/kontrol, overskrivningsværktøjer og en spørgeramme til personligt brug til afklaring af viden på sikkerhedsområdet.
- Brug testværktøjer til kontrol af den faktiske sikkerhed - f.eks. penetrationstests. Sikkerhedspersonalet bliver herved opmærksom på problemerne - forkert installation/opsætning, svage passwords o.a.
- Installer IDS for at afsløre evt. indbrudsforsøg.
- Etabler en intranet-server (velbeskyttet) og placer al sikkerhedsdokumentation inkl. formularer på denne.
- Etabler en FAQ-liste vedr. sikkerhedsspørgsmål på intranettet - kan reducere belastningen af sikkerhedsfunktionen.
- Etabler søgefaciliteter på førnævnte servere - muliggør, at man hurtigere kan finde relevant materiale.
- Etabler filtre på førnævnte servere - muliggør, at den enkelte kun gives adgang til den information, som er relevant for hans/hendes arbejdsfunktion.
- Etabler filtre på firewall'en, som muliggør at man kan blokere for adgang indefra til visse servere. Udsend memo hvor man forklarer årsag og virkemåde.
- Etabler indholdsscanning. Udsend memo hvor man forklarer årsag og virkemåde.

- Kræv, at alle bærbare computere som kobles til jeres systemer overholder visse minimumskrav til opsætning (virus scan, personlig firewall, pauseskærm, ...).
- Udvælg et produkt som kan håndtere krypterings opgaven som jeres standard/platform og orienter intern om hvordan dette produkt kan understøtte organisationens implementering af PKI.
- Etabler et log-system som kan afdække sikkerhedsbrud og implementer samtidig en forretningsgang/procedure til orientering af brugere og deres leder (afhængig af bruddet).
- Tilpas logon meddelelsen så det fremgår, at systembrug kræver autorisation, at systemet kun må bruges til forretningsmæssigt brug og at alle aktiviteter logges.
- Placer en besked i forbindelse med logon til firewalls og modempuljer (og ved fysisk tilgang) - hvor man henvises til relevante retningslinier og konfigurationsbeskrivelser.
- Udvikl pop-up's eller hints, som skifter indhold løbende, hvor man gøres opmærksom på specifikke sikkerhedsforhold. Der skal kvitteres (trykkes 'Ok') for at lukke vinduet.
- Kræv at brugerne hver gang de foretager pålogning aktivt skal bekræfte, at de kender sikkerhedspolitikken og at de vil overholde retningslinierne.
- Ændr startbilledet på de enkelte applikationer - herunder e-mail programmet - så der vises specifikke retningslinier for applikationens brug.

Andre kommunikationsformer

- Skriv sikkerhedsslogans på krus, musemåtter, brevåbnere og andre ting, som udleveres til personalet.
- Påtryk sikkerhedsslogans på 'Post-it"s og tilsvarende.
- Påtryk slogans på T-shirts og sweatshirts og giv disse til medarbejdere, som i særlig grad understøtter sikkerhedsarbejdet.
- Fremstil videobånd/DVD med sikkerhedsindslag, som kan distribueres til afdelinger og fjernarbejdspladser.
- Etabler en hot-line med en automatisk telefonsvarer hvor man kan ind rapportere sikkerhedsproblemer - evt. anonymt.
- Vis sikkerhedsindslag på internt tv placeret i f.eks. frokostrum.
- Udlever "Wunderbaums"med sikkerhedsslogans til medarbejderne med henblik på ophængning i bakspejl.

Bilag D

Xaware

D.1 Kildekode

D.1.1 SQL-db

```
CREATE DATABASE xaware
GO

USE xaware
GO

CREATE TABLE Brugerdata (
  Medlemsnummer INT NOT NULL AUTO_INCREMENT PRIMARY KEY,
  Medlemstype int NOT NULL,
  Fornavn varchar(50) NOT NULL,
  Efternavn varchar(50),
  Postnr int,
  Alder int,
  Køn int,
  Bruger varchar(50) NOT NULL,
  Adgangskode varchar(50) NOT NULL,
```

```
  Beskæftigelse int,
  Virksomhed varchar(50),
  Titel varchar(50),
  Skill int
)
GO

CREATE TABLE Brugerrettigheder (
  Medlemstype INT NOT NULL PRIMARY KEY,
  Medlemsbetegnelse VARCHAR(20) NOT NULL,
  FOREIGN KEY (Medlemstype) REFERENCES brugerdata(Medlemstype)
)
GO

INSERT INTO Brugerrettigheder (Medlemstype, Medlemsbetegnelse)
VALUES (1, "Bruger")
GO

INSERT INTO Brugerrettigheder (Medlemstype, Medlemsbetegnelse)
VALUES (2, "Admin")
GO

CREATE TABLE wifi (
id INT NOT NULL AUTO_INCREMENT PRIMARY KEY,
xawareid INT NOT NULL,
data1 VARCHAR(50) NOT NULL, data2 VARCHAR(50) NOT NULL,
data3 VARCHAR(50) NOT NULL, data4 VARCHAR(50) NOT NULL,
data5 VARCHAR(50) NOT NULL, data6 VARCHAR(50) NOT NULL,
data7 VARCHAR(50) NOT NULL, data8 VARCHAR(50) NOT NULL,
data9 VARCHAR(50) NOT NULL, data10 VARCHAR(50) NOT NULL,
data11 VARCHAR(50) NOT NULL, data12 VARCHAR(50) NOT NULL,
data13 VARCHAR(50) NOT NULL, data14 VARCHAR(50) NOT NULL,
data15 VARCHAR(50) NOT NULL, data18 VARCHAR(50) NOT NULL,
data19 VARCHAR(250), tid TIMESTAMP NOT NULL,
FOREIGN KEY (xawareid) REFERENCES brugerdata(medlemsnummer)
)
GO

CREATE TABLE testPass (
id INT NOT NULL AUTO_INCREMENT PRIMARY KEY,
xawareid INT NOT NULL,
point VARCHAR(50) NOT NULL, length VARCHAR(50) NOT NULL,
bigsmall VARCHAR(50) NOT NULL, special VARCHAR(50) NOT NULL,
tid TIMESTAMP NOT NULL,
```

```
FOREIGN KEY (xawareid) REFERENCES brugerdata(medlemsnummer)
)
GO

ALTER Brugerdata (Medlemstype)
SET Medlemstype = 2
WHERE Bruger = Admin

GO
```

D.1.2 Style.css

```
/*-------------------------------------------------------------------------*/
/* Grundlæggende layout                                                    */
/*-------------------------------------------------------------------------*/
body {
 margin:0px;
 padding:0px;
 background-color: #fefefe;
 font-family: verdana, arial, sans-serif;
 font-size:0.8em;
 color: #000000;
}

/* -------- Sidehoved/Titel ----------*/
#title {
 margin:0px;
 padding:0px;
 vertical-align: middle;
 background-image: url(images/xaware.jpg);
 background-repeat: no-repeat;
 height:62px;
 border-top: 1px solid;
 border-bottom: 1px solid;
}

/* -------- Dagens Dato --------------*/
/* Datoboks */
#datebox {
 position: absolute;
 top: 64px;
 right: 0px;
 background-image: url(images/fane.jpg);
 background-color: #999999;
 padding: 4px 5px 5px 5px;
 margin: 0px 0px 5px 0px;
 width:160px;
}

/* Dato */
#datebody {
 padding: 0px 5px 0px 5px;
 background-color: #fefefe;
 border: 1px solid;
```

```
}


/* -------- Menu System --------------*/
/* Top menu */
#menu {
 background-image: url(images/fane.jpg);
 background-color: #999999;
 margin: 0px 175px 5px 0px;
 padding: 5px;
}

/* Top menu sektion */
.menusection {
 background-color: #ddeeff;
  margin: 0px 5px 0px 0px;
 border: 1px solid;
}

/* Top menu element */
.menubody {
 background-color:  #ddeeff;
 padding: 0px 2px 0px 2px;
}

/* Top menu medlem element */
/*.medlmenubody {
 background-color: #ddffee;
 padding: 0px 2px 0px 2px;
}

/* Top menu admin element */
.adminmenubody {
 background-color: #ccffff;
 padding: 0px 2px 0px 2px;
}

/* Højre menu */
#rightmenu {
 position: absolute;
 top: 95px;
 right: 0px;
 background-image: url(images/fane.jpg);
 background-color: #999999;
```

```
 padding: 5px;
 width:160px;
}

/* Højre menu element */
.rightmenubody {
 background-color: #fefefe;
 margin: 0px 0px 5px 0px;
 padding: 5px;
 border: 1px solid;
}

/* -------- Sideindhold --------------*/
#box {
 margin:0px 175px 0px 0px;
 padding:5px;
 background-image: url(images/fane.jpg);
}

#content {
 vertical-align: top;
 padding: 10px 10px 10px 10px;
 border: 1px solid;
 background-color: #fefefe;
}

/* ----------------------------------------*/
/* default.asp                            */
/*----------------------------------------*/
#sidetekst {
 position:relative;
 margin: 0px 40px 0px 10px;
 text-align:left;
 height: 350px;
}

/* ----------------------------------------*/
/* nyheder.asp                            */
/*----------------------------------------*/
/* X logo */
img.curve {
 position:relative;
 float: left;
 clear: left;
```

```
 margin: 0 1em 0 1em;
}

/* Kolonne 1 */
#kol1 {
  float: left;
  width: 70%;
  padding: 5px;
  /*border-right: 1px solid #000;*/
}

/* Kolonne 2 */
#kol2 {
  float: left;
  padding: 5px;
  width: 25%; /* kun 25% så kolonnerne virker i Mozilla/Netscape */
}

/* Stop flydende kolonner */
.stopflyd { clear: both }

/* Nyhedspunkt */
.nyhed {margin:0em 0em 2em 0em;}


/* ----------------------------------------*/
/* Sidefod                                 */
/*----------------------------------------*/
/* Copyright */
#copy {
 position: relative;
 top: 1px;
 left: 0px;
 padding: 0px 0px 0px 5px;
 font-size: 0.9em;
 font-weight: bold;
}

/* ----------------------------------------*/
/* Deltagerlister                   */
/*----------------------------------------*/
/* Listelink */
#deltagerlister a {
 text-decoration: underline;
```

```
}


/* ----------------------------------------*/
/* Blandet                                 */
/*-----------------------------------------*/
.lightgray { background-color: #eeeeee }
.gray { background-color: #cccccc }
/*.blackborder { border: 2px ridge;  border-color: #000000;}*/
.required { color: #ff6500} /* opretbruger.asp - påkrævede formularfelter */
.formhelp { color: #ff0000} /* Fejlbeskeder ved submit af formular */
#nyeang { font-weight: bold } /* Nye arrangementer overskrift */
.nye { font-size:0.8em;} /* Nye arrangementer */
small { font-size: 0.8em; }
caption { text-align: left; }

/* Links */
a { font-size:0.9em;}
a:link { color: #0000cc }
a:visited { color: #0000cc }
a:active { color: #0000cc }
```

D.1.3 brugerprofil.php

```
<?php include("header.php"); require_once("functions.php");?>

  <? if ($_SESSION["xawareid"] == "") { ?>
  <script type="text/javascript"> window.location="index.php"</script>
  <? } ?>

  <script type="text/javascript">
   function validateBrugerprofil()
   {
    if (
     (document.profil.txtBruger.value.length > 0) &&
     (document.profil.txtFornavn.value.length > 0) &&
     (document.profil.txtEfternavn.value.length > 0) &&
     (document.profil.txtPostnr.value.length > 0) &&
     (document.profil.txtAar.value.length > 0) &&
     (document.profil.txtBeskæftigelse.value.length > 0) &&
     (document.profil.txtVirksomhed.value.length > 0) &&
     (document.profil.txtTitel.value.length > 0) &&
     (document.profil.txtSkill.value.length > 0)
    ) {
     return true;
    }
    else {
     alert("Et eller flere af felterne er ikke udfyldt!");
     return false;
    }
   }
  </script>

  <title>XAware - Brugerprofil</title>
 </head>
 <body onload="Tid();">
  <? include ("menu.php"); ?>
  <div id="box">
   <div id="content">
   <p><a href="default.php">Forside</a> > <b>Ændre brugeroplysninger</b></p>
    <? brugerProfil($_SESSION["xawareid"]) ?>
    <div>
     <form id="profil" method="post" onsubmit="return validateBrugerprofil();"
      action="brugerprofilh.php">
     <table summary="brugerprofil">
      <tr>
```

```
 <td><label>Brugernavn</label></td>
 <td>
  <input name="txtBruger" type="text" size="34"
   value="<? echo $_SESSION["bruger"] ?>" />
 </td>
 <td></td>
</tr>

<tr>
 <td><label>Fornavn</label></td>
 <td>
  <input name="txtFornavn" type="text" size="34"
   value="<? echo $_SESSION["fornavn"] ?>" />
 </td>
 <td></td>
</tr>
<tr>
 <td><label>Efternavn</label></td>
 <td>
  <input name="txtEfternavn" type="text" size="34"
   value="<? echo $_SESSION["efternavn"] ?>" />
 </td>
<td></td>
</tr>
<tr>
 <td><label>Postnummer</label></td>
 <td>
  <input name="txtPostnr" type="text" size="34" maxlength="4"
   value="<? echo $_SESSION["postnr"] ?>" /></td>
 <td></td>
</tr>
<tr>
 <td><label>Alder</label></td>
 <td>
  <input name="txtAar" type="text" size="34" maxlength="4"
   value="<? echo $_SESSION["aar"] ?>" /></td>
 <td></td>
</tr>

<tr>
 <td><label>Beskæftigelse</label></td>
 <td>
 <? if ($_SESSION["beskæftigelse"] == 0) { ?>
 <select name="txtBeskæftigelse"/>
```

```
 <option value="0" selected="selected">Uden job</option>
 <option value="1">Studerende</option>
 <option value="2">Studerende m. arbejde</option>
 <option value="3">Arbejder - deltid</option>
 <option value="4">Arbejder - fuldtid</option>
 <? }
 if ($_SESSION["beskæftigelse"] == 1) { ?>
 <select name="txtBeskæftigelse"/>
 <option value="0">Uden job</option>
 <option value="1" selected="selected">Studerende</option>
 <option value="2">Studerende m. arbejde</option>
 <option value="3">Arbejder - deltid</option>
 <option value="4">Arbejder - fuldtid</option>
 <? }
 if ($_SESSION["beskæftigelse"] == 2) { ?>
 <select name="txtBeskæftigelse"/>
 <option value="0">Uden job</option>
 <option value="1">Studerende</option>
 <option value="2" selected="selected">Studerende m. arbejde</option>
 <option value="3">Arbejder - deltid</option>
 <option value="4">Arbejder - fuldtid</option>
 <? }
 if ($_SESSION["beskæftigelse"] == 3) { ?>
 <select name="txtBeskæftigelse"/>
 <option value="0">Uden job</option>
 <option value="1">Studerende</option>
 <option value="2">Studerende m. arbejde</option>
 <option value="3" selected="selected">Arbejder - deltid</option>
 <option value="4">Arbejder - fuldtid</option>
 <? }
 if ($_SESSION["beskæftigelse"] == 4) { ?>
 <select name="txtBeskæftigelse"/>
 <option value="0">Uden job</option>
 <option value="1">Studerende</option>
 <option value="2">Studerende m. arbejde</option>
 <option value="3">Arbejder - deltid</option>
 <option value="4" selected="selected">Arbejder - fuldtid</option>
 <? } ?>
 </td>
 <td></td>
</tr>

<tr>
 <td><label>Virksomheds navn/ Uddannelses sted:</label></td>
```

```
 <td><input name="txtVirksomhed" type="text" size="34" value="<? echo $_SESSION["virksomhed"] ?>"
 <td></td>
</tr>

<tr>
 <td><label>Job titel / Uddannelses retning:</label></td>
 <td><input name="txtTitel" type="text" size="34" value="<? echo $_SESSION["titel"] ?>" /></td>
 <td></td>
</tr>

<tr>
 <td><label>Computer færdighed:</label></td>
 <td>
 <? if($_SESSION["skill"] == 0){ ?>
 <select name="txtSkill"/>
 <option value="0" selected="selected">Uerfaren</option>
 <option value="1">Erfaren</option>
 <option value="2">Super bruger</option>
 <option value="3">Ekspert</option>
 <? }
 if ($_SESSION["skill"] == 1) { ?>
 <select name="txtSkill"/>
 <option value="0">Uerfaren</option>
 <option value="1" selected="selected">Erfaren</option>
 <option value="2">Super bruger</option>
 <option value="3">Ekspert</option>
 <? }
 if ($_SESSION["skill"] == 2) { ?>
 <select name="txtSkill"/>
 <option value="0">Uerfaren</option>
 <option value="1">Erfaren</option>
 <option value="2" selected="selected">Super bruger</option>
 <option value="3">Ekspert</option>
 <? }
 if ($_SESSION["skill"] == 3) { ?>
 <select name="txtSkill"/>
 <option value="0">Uerfaren</option>
 <option value="1">Erfaren</option>
 <option value="2">Super bruger</option>
 <option value="3" selected="selected">Ekspert</option>
 <? } ?>
 </td>
 <td></td>
</tr>
```

```
      <tr>
       <td colspan="2" style="text-align:right">
        <input type="submit" value="Send" />
        <input type="reset" value="Nulstil" />
       </td>
       <td></td>
      </tr>
     </table>
     </form>
    </div>
   </div>
   <div id="copy">&copy; 2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.4 brugerprofilh.php

```
<?php include("header.php"); require_once("functions.php");?>

  <? if ($_SESSION["xawareid"] == "") { ?>
  <script type="text/javascript"> window.location="index.php"</script>
  <? } ?>

  <title>XAware - Brugerprofil</title>
 </head>
 <body onload="Tid();">
  <? include ("menu.php"); ?>
  <div id="box">
   <div id="content">
   <p><a href="default.php">Forside</a> > <b>Ændre brugeroplysninger</b></p>
    <? brugerProfil($_SESSION["xawareid"]) ?>
    <div>
     <?php
      require_once ("functions.php");

      $result = updateBruger( $_POST["txtFornavn"],$_POST["txtEfternavn"], $_POST["txtPostnr"], $_POST[
       if($result) //Logger brugeren på direkte efter oprettelsen
       {
        $xawareid = xaware_id($_POST["txtBruger"]);
        echo "<h2>Brugerinformation til, ".stripslashes($_POST["txtBruger"])." blev opdateret!</h2>";
        echo "<a href=\"default.php\">Tilbage til startsiden!</a>";
       }
       else
       {
        echo "<h2>Fejl! Det er sket en fejl.";
        echo "<h2>Kontakt <a href=\"mailto:kenny.magnusson@gmail.com\">Webmasteren</a>".
        " om denne fejl og prøv lidt senere igen!";
       }

     ?>
    </div>
   </div>
   <div id="copy">&copy; 2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.5 default.php

```
<?php include("header.php"); ?>

 <title>XAware - IT sikkerhedsbevidsthed - Prøv de gratis spørgeskemaer</title>

 </head>
 <body onload="Tid()">

 <?php include ("menu.php") ?>

  <div id="box">
   <div id="content">
    <div id="sidetekst">
     <img src="images/logo1.gif" width="216" height="19" class="curve" alt="Del 1 af X" />
     <img src="images/logo2.gif" width="234" height="23" class="curve" alt="Del 2 af X" />
     <img src="images/logo3.gif" width="242" height="22" class="curve" alt="Del 3 af X" />
     <img src="images/logo4.gif" width="242" height="24" class="curve" alt="Del 4 af X" />
     <img src="images/logo5.gif" width="240" height="25" class="curve" alt="Del 5 af X" />
     <img src="images/logo6.gif" width="229" height="24" class="curve" alt="Del 6 af X" />
     <img src="images/logo7.gif" width="205" height="22" class="curve" alt="Del 7 af X" />
     <img src="images/logo8.gif" width="219" height="18" class="curve" alt="Del 8 af X" />
     <img src="images/logo9.gif" width="243" height="25" class="curve" alt="Del 9 af X" />

      <h4>Velkommen, <?php echo getusername($_SESSION["xawareid"]); ?></h4>
      <p>
       Du har nu mulighed for at prøve et spørgeskema, designet til at teste din viden om forskellig
       <br /><br />
       Tryk på start for at komme i gang og teste din viden.
       <br /><br /><br /><br />
      </p>
      <td align="center">
      <form name="form" action="wifi_1.php" method="post">
       <input type="submit" value="Start" style="width: 90px; height: 30px;" />
      </form>
      </td>
     <br /><br />
     <p>
      Denne side er lavet som del af et kandidatspeciale
      på Danmarks tekniske Universitet.<br /><br />
      Kenny Magnusson, <a href="mailto:kenny.magnusson@gmail.com">admin@xaware.dk</a>
     </p>
    </div>
   </div>
```

```
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.6 functions.php

```
<?php

function connect()
{
 //http://dtu17.be
 mysql_connect("localhost", "dtu17_be", "S011236DB") or die(mysql_error());

 //Udvikling lokalt
 //mysql_connect("localhost", "root", "Kenny-0104") or die(mysql_error());

 mysql_select_db("dtu17_be") or die(mysql_error());
}


// Kontroller om en bruger er logget ind
function check()
{
 return $_SESSION["xawareid"];
}

// Bruger Login
function loginuser($username, $password)
{
 if(brugerauth($username, $password))
 {
  $_SESSION["xawareid"] = xaware_id($username);
  $_SESSION["medlemstype"] = brugerRettighed($username);
  $_SESSION["logindtid"] = time();
  $_SESSION["bruger"] = $username;
  return true;
 }
 else
 { return false; }
}

function brugerauth($username, $password)
{
 connect();
 $result = mysql_query("SELECT * FROM Brugerdata WHERE bruger = '".$username."' AND adgangskode = '
 $password."';") or die(mysql_error());
 $row = mysql_fetch_array( $result );
 if ( $row )
```

```
 { return true; }
 else
 { return false; }
 mysql_close();
}

function xaware_id($username)
{
 connect();
 $result = mysql_query("SELECT medlemsnummer FROM Brugerdata WHERE bruger = '".
 $username."';") or die(mysql_error());
 $row = mysql_fetch_row($result);
 if ( $row )
 { return $row[0]; }
 else
 { return false; }
 mysql_close();
}

function brugerRettighed($username)
{
 connect();
 $result = mysql_query("SELECT medlemstype FROM Brugerdata WHERE bruger = '".
 $username."';") or die(mysql_error());
 $row = mysql_fetch_row($result);
 if ( $row )
 { return $row[0]; }
 else
 { return false; }
 mysql_close();
}

function brugerFindes($username)
{
 connect();
 $result = mysql_query("SELECT * FROM Brugerdata WHERE bruger = '".
 $username."';") or die(mysql_error());
 $row = mysql_fetch_array( $result );
 if ( $row )
 { return true; }
 else
 { return false; }
 mysql_close();
}
```

```
// Bruger oprettelse
function opretBruger($bruger, $adgang, $fornavn, $efternavn, $postnr, $aar, $sex, $besk, $virk, $tit
{
 connect();
 $result = mysql_query("INSERT INTO Brugerdata (Medlemstype, Fornavn, Efternavn, Postnr,".
 "Alder, Køn, Bruger, Adgangskode, Beskæftigelse, Virksomhed, Titel, Skill)".
 "VALUES (1, '".$fornavn."', '".$efternavn."', ".$postnr.", ".
 "".$aar.", ".$sex.", '".$bruger."', '".$adgang."', ".$besk.", '".$virk."', '".$titel."', ".$skill."
 or die(mysql_error());
 if ( $result )
 { return true; }
 else
 { return false; }
 mysql_close();
}

// Bruger Logout
function logout()
{
 if($_SESSION["xawareid"])
 {
  $_SESSION = array();
  session_destroy();
  return true;
 }
}


function getusername($id)
{
 connect();
 $result = mysql_query("SELECT bruger FROM Brugerdata WHERE medlemsnummer = ".$id.";") or die(mysql_
 $row = mysql_fetch_row($result);
 if ( $row )
 { return $row[0]; }
 else
 { return false; }
 mysql_close();
}

function brugerProfil($id)
{
 connect();
```

```
 $result = mysql_query("SELECT Fornavn, Efternavn, Postnr, Alder, Bruger, Beskæftigelse, Virksomhed, Ti

 $row = mysql_fetch_row($result);
 if ( $row )
 {
  $_SESSION["fornavn"] = $row[0];
  $_SESSION["efternavn"] = $row[1];
  $_SESSION["postnr"] = $row[2];
  $_SESSION["aar"] = $row[3];
  $_SESSION["bruger"] = $row[4];
  $_SESSION["beskæftigelse"] = $row[5];
  $_SESSION["virksomhed"] = $row[6];
  $_SESSION["titel"] = $row[7];
  $_SESSION["skill"] = $row[8];
  return true;
 }
 else
 { return false; }
 mysql_close();
}

function updateBruger($fornavn, $efternavn, $postnr, $aar, $bruger, $besk, $virk, $titel, $skill, $id)
{
 connect();
 $result = mysql_query("UPDATE Brugerdata SET Fornavn = '".$fornavn."', Efternavn = '".$efternavn."', "
  "Postnr = ".$postnr.", Alder = ".$aar.", Bruger = '".$bruger."', Beskæftigelse = '".$besk."', ".
  "Virksomhed = '".$virk."',  Titel = '".$titel."', Skill = ".$skill." ".
     "WHERE Medlemsnummer=".$id.";") or die(mysql_error());
 if ( $result )
 { return true; }
 else
 { return false; }
 mysql_close();
}

// Indsæt resultater fra spørgeskema
function wifiDB($id, $data1, $data2, $data3, $data4, $data5, $data6, $data7, $data8, $data9, $data10, $
{
 connect();
 $result = mysql_query("INSERT INTO wifi (xawareid, data1, data2, data3,".
 "data4, data5, data6, data7, data8, data9, data10, data11, data12, data13,".
 "data14, data15, data18, data19, tid)".
 "VALUES ('".$id."', '".$data1."', '".$data2."', '".$data3."', ".
 "'".$data4."', '".$data5."', '".$data6."', '".$data7."', '".$data8."', '".$data9."', '".$data10."', ".
```

```
 "'".$data11."', '".$data12."', '".$data13."', '".$data14."', '".$data15."', '".$data18."', '".$data
 or die(mysql_error());
 if ( $result )
 { return true; }
 else
 { return false; }
 mysql_close();
}

// Indsæt resultater fra spørgeskema
function testPass($id, $point, $length, $bigsmall, $special )
{
 connect();
 $result = mysql_query("INSERT INTO testPass (xawareid, point, length, bigsmall,".
 "special, tid)".
 "VALUES ('".$id."', '".$point."', '".$length."', '".$bigsmall."', ".
 "'".$special."', Now());")
 or die(mysql_error());
 if ( $result )
 { return true; }
 else
 { return false; }
 mysql_close();
}

?>
```

D.1.7 header.php

```
<?php
session_start();
header("Cache-control: private"); // IE 6 Fix.
require_once ("functions.php");
$validuser = check();
?>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">

<head>
 <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
 <meta name="Keywords" content="XAware, IT-sikkerhed, sikkerhedsbevidsthed, spørgeskema, interaktiv" />
 <meta name="Author" content="Kenny Magnusson" />
 <meta name="Description" content="Spørgeskema omhandlende sikkerhed ved trådløse netværk." />
 <meta name="Robots" content="ALL" />
 <meta name="Rating" content="General" />
 <meta name="Revisit" content="1" />

 <link href="style.css" rel="stylesheet" type="text/css" />

 <script type="text/javascript">
 function Tid()
 {
   var tid = new Date();
   var mdr=new Array("Januar","Februar","Marts","April","Maj","Juni","Juli","August","September","Oktob
   document.getElementById("datebody").innerHTML = tid.getDate() + ". " + mdr[tid.getMonth()] + " " + t
 }
 </script>
```

D.1.8 index.php

```
<?php include("header.php"); ?>

 <title>XAware - IT sikkerhedsbevidsthed - Prøv de gratis spørgeskemaer</title>

 </head>
 <body onload="Tid()">

 <?php include ("menu.php") ?>

  <div id="box">
   <div id="content">
    <div id="sidetekst">
     <img src="images/logo1.gif" width="216" height="19" class="curve" alt="Del 1 af X" />
     <img src="images/logo2.gif" width="234" height="23" class="curve" alt="Del 2 af X" />
     <img src="images/logo3.gif" width="242" height="22" class="curve" alt="Del 3 af X" />
     <img src="images/logo4.gif" width="242" height="24" class="curve" alt="Del 4 af X" />
     <img src="images/logo5.gif" width="240" height="25" class="curve" alt="Del 5 af X" />
     <img src="images/logo6.gif" width="229" height="24" class="curve" alt="Del 6 af X" />
     <img src="images/logo7.gif" width="205" height="22" class="curve" alt="Del 7 af X" />
     <img src="images/logo8.gif" width="219" height="18" class="curve" alt="Del 8 af X" />
     <img src="images/logo9.gif" width="243" height="25" class="curve" alt="Del 9 af X" />

      <h4>Velkommen </h4>
      <p>
       Denne side er en del af et eksamensprojekt i informatik på Danmarks Tekniske Universitet, og
       <br /><br />
       Vil du vide lidt mere om sikkerhed ved brug af trådløse netværk, så test dig selv via. spørge
       Det er helt gratis og mens du lærer af spørgeskemaerne, lagres testene til statistisk brug.
       <br /><br />
       Tryk på start for at komme i gang og oprette en ny bruger.<br />
       Er du allerede registreret bruger kan du logge ind vha. logind vinduet i højre side.
       <br /><br />
      </p>

      <td align="center">
       <form name="form" action="opretbruger.php" method="post">
        <input type="submit" value="Start" style="width: 90px; height: 30px;" />
       </form>
      </td>

     <p>
      Denne side er lavet som del af et kandidatspeciale på Danmarks tekniske Universitet.
```

```
      <br />
      Kenny Magnusson, <a href="mailto:kenny.magnusson@gmail.com">admin@xaware.dk</a>
      <br /><br />
      OBS!! - VIRKER NU OGSÅ I FIREFOX :-)
     </p>
    </div>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.9 logind.php

```
<?php include("header.php"); ?>

 <title>XAware - IT sikkerhedsbevidsthed - Prøv de gratis spørgeskemaer</title>

 </head>
 <body onload="Tid()">

 <?php include ("menu.php") ?>

  <div id="box">
   <div id="content">
    <div id="sidetekst">
     <?php
      require_once ("functions.php");

      if($_POST["txtBruger"])
      {
       if(loginuser($_POST["txtBruger"], MD5($_POST["txtAdgang"])))
       {
        echo "<b>Velkommen, ".check().".</h2>";
        echo "Du bliver nu omdirigeret til hovedsiden <br />";
        echo $_SESSION["medlemstype"];
     ?>
     <script type="text/javascript"> window.location="default.php"</script>
     <?php
       }
       else
       {
        echo "<b>Brugernavn eller kodeord forkert, <a href=\"index.php\">tilbage!</a></b>";
       }
      }
     ?>
    </div>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.10 logud.php

```
<?php $page = "i"; include("header.php"); ?>

 <title>XAware - IT sikkerhedsbevidsthed - Prøv de gratis spørgeskemaer</title>

 </head>
 <body onload="Tid()">

 <?php include ("menu.php") ?>

  <div id="box">
   <div id="content">
    <div id="sidetekst">
     <?php
      require_once 'functions.php';
      logout();
     ?>
     <script type="text/javascript"> window.location="index.php"</script>
    </div>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.11 menu.php

```
<?php // Menuer for alle, medlemmer, administrator, samt
  // boksen med nyeste oprettede arrangementer
  // og login boksen, i højre side af skærmen

 require_once "functions.php";

?>
   <script type="text/javascript">
    function validateLogind()
    {
     if((document.frmLogind.txtBruger.value.length > 0) ||
      (document.frmLogind.txtAdgang.value.length > 0))
     { return true; }
     else
     { alert("Et af felterne er ikke udfyldt!"); return false; }
    }
   </script>

   <div id="title"></div>
   <div id="datebox">
    <div id="datebody">
     <a href="nojavascript.php">
      <span class="formhelp">JavaScript er ikke aktiveret</span>
     </a>
    </div>
   </div>
   <div id="menu">
    <span class="menusection">
     <?// Vis menu hvis brugeren er logget ind.
     If ( $_SESSION["xawareid"] <> "" ) { ?>
      <span class="menubody"><a href="default.php">Forside</a></span>
     <? } else { ?>
      <span class="menubody"><a href="index.php">Forside</a></span>
     <? } ?>
    </span>

    <?//Vis menu hvis brugeren er logget ind
      If ($_SESSION["xawareid"] <> "") { ?>

    <span class='menusection'>
     <span class="medlmenubody" >
      <a href='wifi_1.php'>Spørgeskema</a>
```

```
 </span>
 <span class="medlmenubody" >
  <a href='testPassword.php'>Test dit password</a>
 </span>
 <span class="medlmenubody" >
  <a href='brugerprofil.php'>Se brugeroplysninger</a>
 </span>
</span>

<? } ?>

<? //Vis menu hvis brugeren er logget ind og har admin-rettigheder.
 If ($_SESSION["xawareid"] <> "" AND $_SESSION["medlemstype"] == 2) { ?>

<span class='menusection'>
 <span class="adminmenubody" >
  <a href='/Rapport/index.php'>Rapport filer</a>
  <a href='statistik.php'>Statistik</a>
 </span>
</span>

<? } ?>

</div>
<div id="rightmenu">
 <?// Vis menu hvis brugeren er logget ind.
  If ( $_SESSION["xawareid"] <> "" ) { ?>
 <div class="rightmenubody">
  <p>
   Velkommen <? echo $_SESSION["bruger"] ?><br />
   Logintid: <? echo date("g:i D, F jS Y",$_SESSION["logindtid"]) ?>
  </p>
  <p><a href="brugerprofil.php">Ændre brugeroplysninger</a></p>
  <form method="post" action="logud.php">
   <div><input type="submit" value="Log ud" /></div>
  </form>
 </div>
 <div class="rightmenubody">
  <div id="startmenu">Menu:</div>
   <a href="wifi_1.php">Start spørgeskema</a><br />
   <a href="testPassword.php">Test dit password</a>
 </div>

 <? //Vis menu hvis brugeren er logget ind og har admin-rettigheder.
```

```
 If ($_SESSION["xawareid"] <> "" AND $_SESSION["medlemstype"] == 2) { ?>
 <div class="rightmenubody">
  <div id="startmenu">Statistik:</div>
   <a href="statistik.php">Oversigt</a> <br \>
   <a href="statBruger.php">Bruger oplysninger</a> <br \>
   <a href="statSpm.php">Svar på spørgsmål</a><br \>
   <a href="statKommentar.php">Kommentarer</a><br \>
   <a href="statPass.php">Test af password</a>
 </div>
<? } ?>

<? } Else { ?>

<div class="rightmenubody">
 <form id="xawarelogin" name="frmLogind" method="post" action="logind.php"
  onsubmit="return validateLogind();">
  <div>
   <label>Brugernavn</label><br />
   <input name="txtBruger" type="text" size="15" />
  </div>
  <div>
   <label>Adgangskode</label><br />
   <input name="txtAdgang" type="password" size="15" />
  </div>
  <div><input type="hidden" name="jsaktiveret" value="false" /></div>
  <p>
   <a href="opretbruger.php">Bliv oprettet som medlem</a>
  </p>
  <div><input class="button" type="submit" value="Log ind" /></div>
 </form>
</div>
<? } ?>

</div>
```

D.1.12 opretbruger.php

```
<?php include("header.php"); ?>

 <script type="text/javascript">
 function validateOpretbruger()
 {
  if((document.frmOpretbruger.txtBruger.value.length > 0) &&
   (document.frmOpretbruger.txtAdgang.value.length > 0) &&
   (document.frmOpretbruger.txtAdgang2.value.length > 0) &&

   (document.frmOpretbruger.txtFornavn.value.length > 0) &&
   (document.frmOpretbruger.txtEfternavn.value.length > 0) &&
   (document.frmOpretbruger.txtPostnr.value.length > 0) &&
   (document.frmOpretbruger.txtAar.value.length > 0) &&

   (document.frmOpretbruger.txtVirksomhed.value.length > 0) &&
   (document.frmOpretbruger.txtTitel.value.length > 0))
  {
   // Test af gentagent kodeord er ens
   if(document.frmOpretbruger.txtAdgang.value != document.frmOpretbruger.txtAdgang2.value)
   { alert("De to kodeord er ikke ens!"); return false; }

   return true;
  }
  else
  {
   alert("Et fornødent tekstfelt er ikke udfyldt!");
   return false;
  }
 }
 </script>

 <?php $_SESSION["cookietjek"] = True; ?>

  <title>XAware - Opret ny bruger</title>

 </head>
 <body onload="Tid()">
  <? include("menu.php") ?>
  <div id="box">
   <div id="content">
    <p> <!-- breadcrumbs -->
   <a href="index.php">Forside</a> >
```

```
 <b>Opret ny bruger</b>
</p>

  <div id="tilmeld">
<form name="frmOpretbruger" method="post" onsubmit="return validateOpretbruger();" action="opretbr
 <table summary="tilmeld">
  <tr>
   <td><label>Brugernavn:</label></td>
   <td><input name="txtBruger" type="text" size="34" /></td>
   <td></td>
  </tr>
  <tr>
   <td><label>Adgangskode:</label></td>
   <td><input name="txtAdgang" type="password" size="34" /></td>
   <td></td>
  </tr>
  <tr>
   <td><label>Adgangskode(gentaget):</label></td>
   <td><input name="txtAdgang2" type="password" size="34" /></td>
   <td><input type="hidden" name="jsaktiveret" value="false" /></td>
  </tr>
  <tr><td></td><td></td><td></td></tr>
  <tr><td></td><td></td><td></td></tr>
  <tr><td></td><td></td><td></td></tr>
  <tr><td></td><td></td><td></td></tr>
  <tr><td></td><td></td><td></td></tr>
  <tr><td></td><td></td><td></td></tr>
  <tr><td></td><td></td><td></td></tr>
  <tr>
     <td><label>Fornavn:</label></td>
     <td><input name="txtFornavn" type="text" size="34" /></td>
     <td></td>
  </tr>
  <tr>
   <td><label>Efternavn:</label></td>
   <td><input name="txtEfternavn" type="text" size="34" /></td>
   <td></td>
  </tr>
  <tr>
   <td><label>Postnummer:</label></td>
   <td><input name="txtPostnr" type="text" size="34" maxlength="4" /></td>
   <td></td>
  </tr>
  <tr>
```

```
 <td><label>Alder:</label></td>
 <td><input name="txtAar" type="text" size="34" maxlength="4" /></td>
 <td></td>
</tr>
<tr>
 <td><label>Køn:</label></td>
 <td>
  <select name="txtSex">
  <option value="0">Kvinde</option>
  <option value="1">Mand</option>
  </select>
 </td>
 <td></td>
</tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr>
 <td><label>Beskæftigelse:</label></td>
 <td>
 <select name="txtBeskæftigelse" />
 <option value="0">Uden job</option>
 <option value="1">Studerende</option>
 <option value="2">Studerende m. arbejde</option>
 <option value="3">Arbejder - deltid</option>
 <option value="4">Arbejder - fuldtid</option>
 </td>
 <td></td>
</tr>
<tr>
 <td><label>Virksomheds navn/ Uddannelses sted:</label></td>
 <td><input name="txtVirksomhed" type="text" size="34" /></td>
 <td></td>
</tr>
<tr>
 <td><label>Job titel / Uddannelses retning:</label></td>
 <td><input name="txtTitel" type="text" size="34" /></td>
 <td></td>
</tr>
<tr>
```

```
     <td><label>Computer færdighed:</label></td>
     <td>
     <select name="txtSkill" />
     <option value="0">Uerfaren</option>
     <option value="1">Erfaren</option>
     <option value="2">Super bruger</option>
     <option value="3">Ekspert</option>
     </td>
     <td></td>
    </tr>

    <tr>
     <td colspan="2" style="text-align:right">
     <input type="submit" name="submit" value="Opret" />
     <input type="reset" value="Nulstil" /></td>
     <td></td>
    </tr>
  </table>
     </form>
    </div>
   </div>
   <div id="copy">
  &copy; 2007 XAware
   </div>
  </div>
 </body>
</html>
```

D.1.13 opretbrugerh.php

```
<?php include("header.php"); ?>

 <title>XAware - IT sikkerhedsbevidsthed - Prøv de gratis spørgeskemaer</title>

 </head>
 <body onload="Tid()">

 <?php include ("menu.php") ?>

  <div id="box">
   <div id="content">
    <div id="sidetekst">
     <?php
      require_once ("functions.php");
      if(brugerFindes($_POST["txtBruger"]))
      {
       echo "<h2>Brugernavnet: '".stripslashes($_POST["txtBruger"])."' er allerede i brug.</h2>";
       echo "<a href=\"javascript:history.go(-1)\">".
       "Klik her for at komme tilbage og vælge et andet.</a>";
      }
      else
      {
       $result = opretBruger($_POST["txtBruger"], MD5($_POST["txtAdgang"]),   $_POST["txtFornavn"],$_PO
       if($result) //Logger brugeren på direkte efter oprettelsen
       {
        $xawareid = xaware_id($_POST["txtBruger"]);
        echo "<form name=\"form\" action=\"logind.php\" method=\"post\">";
        echo "<h2>Tak, ".stripslashes($_POST["txtBruger"])." blev oprettet!</h2>";
        echo "<a href=\"javascript:document.form.submit();\">Videre!</a>";

        echo "<input name=\"txtBruger\" type=\"hidden\" value=\"".        stripslashes($_POST["txtBruge
        echo "<input name=\"txtAdgang\" type=\"hidden\" value=\"".$_POST["txtAdgang"]."\">";
        echo "</form>";
       }
       else
       {
        echo "<h2>Fejl! Det er sket en fejl.";
        echo "<h2>Kontakt <a href=\"mailto:kenny.magnusson@gmail.com\">Webmasteren</a>".
        " om denne fejl og prøv lidt senere igen!";
       }
      }
     ?>
```

```
    </div>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.14 statBruger.php

```
<?php include("header.php"); ?>

 <title>XAware - IT sikkerhedsbevidsthed - Prøv de gratis spørgeskemaer</title>

 </head>
 <body onload="Tid()">

 <?php include ("menu.php") ?>

  <div id="box">
   <div id="content">
    <div id="sidetekst">
     <h4>Statistik side - Medlemsoplysninger </h4>
     <?php require_once ("functions.php"); ?>
     <?php require_once ("statfunc.php"); ?>

     <table border="1" cellpadding="5">
     <tr><th colspan="9">Bruger oplysning </th></tr>
     <? brugerOplysning(); ?>
     </table>

     <p>Øvrige statistikker:</p>

     <a href="statistik.php">Oversigt</a>  

     <a href="statSpm.php">Svar på spørgsmål</a>  
     <a href="statKommentar.php">Kommentarer</a>  
     <a href="statPass.php">Test af password</a>

    </div>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.15 statfunc.php

```
<?php

// Statistik modul
function antalMedlemmer()
{
 connect();
 $result = mysql_query("SELECT count(*) FROM Brugerdata WHERE medlemstype=1;") or die(mysql_error()
 $row = mysql_fetch_row($result);
 if ( $row )
 { return $row[0]; }
 else
 { return false; }
 mysql_close();
}

function antalAdmin()
{
 connect();
 $result = mysql_query("SELECT count(*) FROM Brugerdata WHERE medlemstype=2;") or die(mysql_error()
 $row = mysql_fetch_row($result);
 if ( $row )
 { return $row[0]; }
 else
 { return false; }
 mysql_close();
}

function antalSvar($spm, $mulighed)
{
 connect();
 $select = ' SELECT ';
 $column = ' count(a.data'.$spm.') ';
 $from = ' FROM ';
 $tables = ' wifi a, (select Medlemsnummer from Brugerdata where Medlemstype=1) b ';
 $where = ' WHERE (a.xawareid = b.Medlemsnummer AND data'.$spm.'='.$mulighed.')';
 $query = $select.$column.$from.$tables.$where;

 $result = mysql_query( $query );
 if (!$result)
 {
 die ("Could not query the database: <br />". mysql_error());
 }
```

```
 while ($result_row = mysql_fetch_row($result)){
    echo "<td>".$result_row[0] . '<br />';
 }

}

function brugerOplysning()
{
 connect();
 $select = ' SELECT ';
 $column = ' Medlemsnummer, Fornavn, Efternavn, Alder, Køn, Beskæftigelse, Virksomhed, Titel, Skill ';
 $from = ' FROM ';
 $tables = ' Brugerdata ';
 $where = ' WHERE Medlemstype=1 ';
 $query = $select.$column.$from.$tables.$where;

 $result = mysql_query( $query );
 if (!$result)
 {
 die ("Could not query the database: <br />". mysql_error());
 }

 echo "<tr><td>Medlemsnummer</td><td>Fornavn</td><td>Efternavn</td><td>Alder</td><td>Køn</td><td>Beskæf
 while ($result_row = mysql_fetch_row($result)){
    echo "<tr><td>".$result_row[0] ."</td><td>".$result_row[1] ."</td><td>".$result_row[2] ."</td><td>"
 }
}

function svarKommentar()
{
 connect();
 $select = ' SELECT ';
 $column = ' a.xawareid, a.data19 ';
 $from = ' FROM ';
 $tables = ' wifi a, (select Medlemsnummer from Brugerdata where Medlemstype=1) b ';
 $where = ' WHERE (a.xawareid = b.Medlemsnummer)';
 $query = $select.$column.$from.$tables.$where;

 $result = mysql_query( $query );
 if (!$result)
 {
 die ("Could not query the database: <br />". mysql_error());
 }
```

```
 echo "<tr><td>Medlemsnummer</td><td>Kommentar</td></tr>";
 while ($result_row = mysql_fetch_row($result)){
    echo "<tr><td>".$result_row[0] ."</td><td>".$result_row[1] ."</td></tr>";
 }

}

function statPassword()
{
 connect();
 $select = ' SELECT ';
 $column = ' a.xawareid, a.point, a.length, a.bigsmall, a.special ';
 $from = ' FROM ';
 $tables = ' testPass a, (select Medlemsnummer from Brugerdata where Medlemstype=1) b ';
 $where = ' WHERE b.Medlemsnummer=a.xawareid ';
 $query = $select.$column.$from.$tables.$where;

 $result = mysql_query( $query );
 if (!$result)
 {
 die ("Could not query the database: <br />". mysql_error());
 }

 echo "<tr><td>Medlemsnummer</td><td>Point</td><td>Længde</td><td>StoreSmåBogstaver</td><td>Specialt
 while ($result_row = mysql_fetch_row($result)){
    echo "<tr><td>".$result_row[0] ."</td><td>".$result_row[1] ."</td><td>".$result_row[2] ."</td><t
 }
}

?>
```

D.1.16 statistik.php

```
<?php include("header.php"); ?>

 <title>XAware - IT sikkerhedsbevidsthed - Prøv de gratis spørgeskemaer</title>

 </head>
 <body onload="Tid()">

 <?php include ("menu.php") ?>

  <div id="box">
   <div id="content">
    <div id="sidetekst">
     <h4>Statistik side</h4>
     <?php require_once ("functions.php"); ?>
     <?php require_once ("statfunc.php"); ?>

     <table border="1">
     <tr><th colspan="2">Antal registrede på denne side:</th></tr>
     <tr>
      <td>Admin</td><td>Medlemmer</td>
     </tr>
     <tr>
      <td><? echo antalAdmin(); ?></td><td><? echo antalMedlemmer(); ?></td>
     </tr>
     </table>

     <p>Øvrige statistikker:</p>

     <a href="statBruger.php">Bruger oplysninger</a>  
     <a href="statSpm.php">Svar på spørgsmål</a>  
     <a href="statKommentar.php">Kommentarer</a>  
     <a href="statPass.php">Test af password</a>

    </div>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.17 statKommentar.php

```
<?php include("header.php"); ?>

 <title>XAware - IT sikkerhedsbevidsthed - Prøv de gratis spørgeskemaer</title>

 </head>
 <body onload="Tid()">

 <?php include ("menu.php") ?>

  <div id="box">
   <div id="content">
    <div id="sidetekst">
     <h4>Statistik side - Svar på spørgsmål 19 - Kommentarer </h4>
     <?php require_once ("functions.php"); ?>
     <?php require_once ("statfunc.php"); ?>

     <table border="1" cellpadding="5">
     <tr><th colspan="2">Spørgsmål 19:</th></tr>
     <tr><th colspan="2">Kommentarer</th></tr>
     <? svarKommentar(); ?>
     </table>

     <p>Øvrige statistikker:</p>

     <a href="statistik.php">Oversigt</a>  
     <a href="statBruger.php">Bruger oplysninger</a>  
     <a href="statSpm.php">Svar på spørgsmål</a>  

     <a href="statPass.php">Test af password</a>

    </div>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.18 statPass.php

```
<?php include("header.php"); ?>

 <title>XAware - IT sikkerhedsbevidsthed - Prøv de gratis spørgeskemaer</title>

 </head>
 <body onload="Tid()">

 <?php include ("menu.php") ?>

  <div id="box">
   <div id="content">
    <div id="sidetekst">
     <h4>Statistik side - Test af password </h4>
     <?php require_once ("functions.php"); ?>
     <?php require_once ("statfunc.php"); ?>

     <table border="1" cellpadding="5">
     <tr><th colspan="5">Test af password </th></tr>
     <? statPassword(); ?>
     </table>

     <p>Øvrige statistikker:</p>

     <a href="statistik.php">Oversigt</a>  
     <a href="statBruger.php">Bruger oplysninger</a>  
     <a href="statSpm.php">Svar på spørgsmål</a>  
     <a href="statKommentar.php">Kommentarer</a>

    </div>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.19 statSpm.php

```
<?php include("header.php"); ?>

 <title>XAware - IT sikkerhedsbevidsthed - Prøv de gratis spørgeskemaer</title>

 </head>
 <body onload="Tid()">

 <?php include ("menu.php") ?>

  <div id="box">
   <div id="content">
    <div id="sidetekst">
     <h4>Statistik side - Svar på spørgsmål 1 - 18 </h4>

     <?php require_once ("functions.php"); ?>
     <?php require_once ("statfunc.php"); ?>

     <table border="1" cellpadding="5">
     <tr><th colspan="2">Spørgsmål 1:</th></tr>
     <tr><th colspan="2">Hvor ofte benytter du trådløs internet.</th></tr>
     <tr><td>Aldrig / meget sjældent </td><? antalSvar(1,0); ?></tr>
     <tr><td>1-3 gange om måneden </td><? antalSvar(1,1); ?></tr>
     <tr><td>1-2 gange om ugen </td> <? antalSvar(1,2); ?> </tr>
     <tr><td>3-4 gange om ugen </td> <? antalSvar(1,3); ?> </tr>
     <tr><td>Flere gange dagligt </td> <? antalSvar(1,4); ?> </tr>
     </table>
     <br \>
     <table border="1" cellpadding="5">
     <tr><th colspan="2">Spørgsmål 2:</th></tr>
     <tr><th colspan="2">Benytter du dig af trådløst netværk derhjemme/ på arbejdet?</th></tr>
     <tr><td>Kun derhjemme </td><? antalSvar(2,0); ?></tr>
     <tr><td>Kun på arbejde </td><? antalSvar(2,1); ?></tr>
     <tr><td>Begge steder </td> <? antalSvar(2,2); ?> </tr>
     <tr><td>Ingen af delene </td> <? antalSvar(2,3); ?> </tr>
     </table>
     <br \>
     <table border="1" cellpadding="5">
     <tr><th colspan="2">Spørgsmål 3:</th></tr>
     <tr><th colspan="2">Føler du dig sikker, når du surfer på Internettet?</th></tr>
     <tr><td>Ja </td><? antalSvar(3,0); ?></tr>
     <tr><td>Nej </td><? antalSvar(3,1); ?></tr>
     <tr><td>Ved ikke </td> <? antalSvar(3,2); ?> </tr>
```

```
</table>
<br \>
<table border="1" cellpadding="5">
<tr><th colspan="2">Spørgsmål 4:</th></tr>
<tr><th colspan="2">Ved du hvad du skal gøre eller hvem du skal henvende dig til hvis noget unorma
<tr><td>Ja </td><? antalSvar(4,0); ?></tr>
<tr><td>Nej </td><? antalSvar(4,1); ?></tr>
<tr><td>Ved ikke </td> <? antalSvar(4,2); ?> </tr>
</table>
<br \>
<table border="1" cellpadding="5">
<tr><th colspan="2">Spørgsmål 5:</th></tr>
<tr><th colspan="2">Har du modtaget undervisning eller blevet oplært i de daglige programmer du be
<tr><td>Ja </td><? antalSvar(5,0); ?></tr>
<tr><td>Nej </td><? antalSvar(5,1); ?></tr>
<tr><td>Ved ikke </td> <? antalSvar(5,2); ?> </tr>
</table>
<br \>
<table border="1" cellpadding="5">
<tr><th colspan="2">Spørgsmål 6:</th></tr>
<tr><th colspan="2">Har du gjort dig bekendt med firmaets IT-sikkerhedspolitik?</th></tr>
<tr><td>Ja </td><? antalSvar(6,0); ?></tr>
<tr><td>Nej </td><? antalSvar(6,1); ?></tr>
<tr><td>Ved ikke </td> <? antalSvar(6,2); ?> </tr>
</table>
<br \>
<table border="1" cellpadding="5">
<tr><th colspan="2">Spørgsmål 7:</th></tr>
<tr><th colspan="2">Hvad betyder SSID?</th></tr>
<tr><td>En krypteringsmetode </td><? antalSvar(7,0); ?></tr>
<tr><td>Sammenslutning af Sikkerhedsfolk I Danmark </td><? antalSvar(7,1); ?></tr>
<tr><td>Navnet på et trådløst netværk </td> <? antalSvar(7,2); ?> </tr>
<tr><td>Ved ikke </td> <? antalSvar(7,3); ?> </tr>
</table>
<br \>
<table border="1" cellpadding="5">
<tr><th colspan="2">Spørgsmål 8:</th></tr>
<tr><th colspan="2">Kan det trådløse netværk skjules så uvedkomne ikke kan se det?</th></tr>
<tr><td>Ja </td><? antalSvar(8,0); ?></tr>
<tr><td>Nej </td><? antalSvar(8,1); ?></tr>
<tr><td>Ved ikke </td> <? antalSvar(8,2); ?> </tr>
</table>
<br \>
<table border="1" cellpadding="5">
```

```
<tr><th colspan="2">Spørgsmål 9:</th></tr>
<tr><th colspan="2">Vælg den mest sikre netværksgodkendelsesmetode.</th></tr>
<tr><td>Åben </td><? antalSvar(9,0); ?></tr>
<tr><td>Delt </td><? antalSvar(9,1); ?></tr>
<tr><td>WPA </td> <? antalSvar(9,2); ?> </tr>
<tr><td>WPA-PSK </td> <? antalSvar(9,3); ?> </tr>
</table>
<br \>
<table border="1" cellpadding="5">
<tr><th colspan="2">Spørgsmål 10:</th></tr>
<tr><th colspan="2">Vælg den mest sikre datakrypteringsmetode.</th></tr>
<tr><td>Deaktiveret </td><? antalSvar(10,0); ?></tr>
<tr><td>WEP </td><? antalSvar(10,1); ?></tr>
<tr><td>AES (kræver WPA eller WPA-PSK) </td> <? antalSvar(10,2); ?> </tr>
<tr><td>TKIP (kræver WPA eller WPA-PSK) </td> <? antalSvar(10,3); ?> </tr>
</table>
<br \>
<table border="1" cellpadding="5">
<tr><th colspan="2">Spørgsmål 11:</th></tr>
<tr><th colspan="2">Vælg det mest sikre trådløse netværk?</th></tr>
<tr><td>Magnusson </td><? antalSvar(11,0); ?></tr>
<tr><td>Default </td><? antalSvar(11,1); ?></tr>
<tr><td>Tumpe </td> <? antalSvar(11,2); ?> </tr>
<tr><td>Ved ikke </td> <? antalSvar(11,3); ?> </tr>
</table>
<br \>
<table border="1" cellpadding="5">
<tr><th colspan="2">Spørgsmål 12:</th></tr>
<tr><th colspan="2">Bør dit trådløse netværk være krypteret?</th></tr>
<tr><td>Nej det er alt for besværligt og ikke nødvendigt </td><? antalSvar(12,0); ?></tr>
<tr><td>Ja selvfølgelig </td><? antalSvar(12,1); ?></tr>
<tr><td>Ved ikke </td> <? antalSvar(12,2); ?> </tr>
</table>
<br \>
<table border="1" cellpadding="5">
<tr><th colspan="2">Spørgsmål 13:</th></tr>
<tr><th colspan="2">Når du benytter trådløst netværk med din arbejdscomputer hjemmefra eller fr
<tr><td>Ved ikke hvad det betyder </td><? antalSvar(13,0); ?></tr>
<tr><td>Ja det er den sikreste metode for både dig og virksomheden </td><? antalSvar(13,1); ?><
<tr><td>Nej det er ikke nødvendigt </td><? antalSvar(13,2); ?> </tr>
</table>
<br \>
<table border="1" cellpadding="5">
<tr><th colspan="2">Spørgsmål 14:</th></tr>
```

```
    <tr><th colspan="2">Hvad bruges denne eToken til?</th></tr>
    <tr><td>Bruges når der skal oprettes en VPN forbindelse til virksomheden </td><? antalSvar(14,0);
    <tr><td>En USB-lagerenhed hvor der kan gemmes dokumenter </td><? antalSvar(14,1); ?></tr>
    <tr><td>Bruges når harddisken skal krypteres </td> <? antalSvar(14,2); ?> </tr>
    <tr><td>Ved ikke </td> <? antalSvar(14,3); ?> </tr>
    </table>
    <br \>
    <table border="1" cellpadding="5">
    <tr><th colspan="2">Spørgsmål 15:</th></tr>
    <tr><th colspan="2">Vælg den sikreste af netværksgodkendelsesmetoder og datakrypteringsmetoder af
    <tr><td>Åben + WEP </td><? antalSvar(15,0); ?></tr>
    <tr><td>Delt + WEP </td><? antalSvar(15,1); ?></tr>
    <tr><td>WPA + AES </td> <? antalSvar(15,2); ?> </tr>
    <tr><td>Ved ikke </td> <? antalSvar(15,3); ?> </tr>
    </table>
    <br \>
    <table border="1" cellpadding="5">
    <tr><th colspan="2">Spørgsmål 18:</th></tr>
    <tr><th colspan="2">Har du fået noget ud af dette spørgeskema?</th></tr>
    <tr><td>Ja </td><? antalSvar(18,0); ?></tr>
    <tr><td>Nej </td><? antalSvar(18,1); ?></tr>
    <tr><td>Ved ikke </td> <? antalSvar(18,2); ?> </tr>
    </table>
    <br \>
    <p>Øvrige statistikker:</p>

    <a href="statistik.php">Oversigt</a>  
    <a href="statBruger.php">Bruger oplysninger</a>  

    <a href="statKommentar.php">Kommentarer</a>  
    <a href="statPass.php">Test af password</a>

   </div>
  </div>
  <div id="copy">&copy;2007 XAware</div>
 </div>
</body>
</html>
```

D.1.20 testPassword.php

D.1.21 testPasswordh.php

```
<?php include("header.php"); require_once("functions.php"); ?>

 <title>XAware - IT sikkerhedsbevidsthed - Prøv de gratis spørgeskemaer</title>

 </head>


 <body onload="Tid()">

 <?php include ("menu.php") ?>

  <div id="box">
   <div id="content">
    <div id="sidetekst">

     <b>Vurdering af kodeord</b>

     <table width="340" cellpadding="0" cellspacing="0">
     <?
      testPass($_SESSION['xawareid'], $_POST['points'], $_POST['length'], $_POST['bigsmall'], $_POST['s
     ?>
     <tr><td></td><td style="padding-bottom: 2px;">Dit kodeord blev vurderet som:
     <?php
     if($_POST['points'] <= 40) { echo "Dårligt sikret"; }
     if($_POST['points'] > 70) { echo "Godt sikret"; }
     if(($_POST['points'] <= 70) && ($_POST['points'] > 40)) { echo "Mellem sikret"; }
     //echo " -".$_POST['points'];
     ?></td><td></td>

     <tr><td width="20"></td>
     <td style=" width:300px; border: 1px solid black;" align="left">
     <div style="width:
     <?php
     echo ($_POST['points'] * 3)."px; ";
     //Point <= 40 vises med en rød farve
     if($_POST['points'] <= 40) { echo "background-color: #ff0000;"; }
     //Point > 70 vises med en grøn farve
     if($_POST['points'] > 70) { echo "background-color: #00ff00;"; }
     //Point <= 70 og > 40 vises med en gul farve
     if(($_POST['points'] <= 70) && ($_POST['points'] > 40)){echo "background-color: #ffff00;"; }
     ?>"> </div>
     </td>
```

```
<td width="20"></td>
</tr>
<tr>
<td align="left" colspan="3">
<div style="display:inline;padding: 0px; margin: 0px; padding-right: 12px"> </div>0
<div style="display:inline;padding: 0px; margin: 0px;padding-right: 132px; "> </div>50
<div style="display:inline;padding: 0px; margin: 0px;padding-right: 120px; "> </div>100
</td>
</table>
<br /><br />

Et sikkert kodeord skal:<br /><br />
<?php
 if($_POST['length'] < 8)
 { echo "<img src=\"../images/cross.jpg\" />"; }
 else
 { echo "<img src=\"../images/check.jpg\" />"; }
 echo " - være mindst otte karakterer langt.<br />\n";

 if($_POST['bigsmall'] == "false")
 { echo "<img src=\"../images/cross.jpg\" />"; }
 else
 { echo "<img src=\"../images/check.jpg\" />"; }
 echo " - indeholde både små og store bogstaver<br />\n";

 if($_POST['specialnumber'] == "false")
 { echo "<img src=\"../images/cross.jpg\" />"; }
 else
 { echo "<img src=\"../images/check.jpg\" />"; }
 echo " - indeholde specielle tegn eller tal<br />\n";
?>
<br />
Kodeordet må ikke indeholde elementer af det brugernavn det bliver benyttet sammen med.
Hvis det gør er det meget nemt at gætte. Kodeord der er dannet af et rigtigt ord er
nemmere at gætte. Så dan ikke kodeord af rigtige ord.<br />
<br />
Forsøg at overholde så mange af reglerne her så dit kodeord bliver vurderet "godt sikret"
(grøn). Men sørg stadigvæk for at kodeordet ikke bliver så kompliceret at du ikke
kan huske det.
<br />
Prøv igen? Klik <a href="testPassword.php">her</a>
<br /><br />
Klik <a href="default.php">her</a> for at vende tilbage til startsiden.
```

```
    </div>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.22 top10_home.php

```
<?php include("header.php"); ?>

  <? if ($_SESSION["xawareid"] == "") { ?>
  <script type="text/javascript"> window.location="index.php"</script>
  <? } ?>

  <title>XAware - Trådløs netværk</title>
 </head>
 <body onload="Tid();">

 <? include ("menu.php") ?>

  <div id="box">
   <div id="content">
    <p><a href="default.php">Start side</a> > <b>Trådløs netværk</b></p>
    <h4>Trådløs netværk</h4>

    <h5>Top 10 Sikkerhedstips for opkobling til hjemme netværk: </h5>
    <table width="100%">
      <tr>
       <td align="left">
        <form id="wifi" method="post" action="wifi_17.php" >

         <ul>
         <li><h5>1. Ændre brugernavn og adgangskode til din router.</h5>
         <p>This is always the first line of defense. It's easy for attackers to find out what the d
         </li>

         <li><h5>2. Lad ikke andre brugere ride med på dit trådløse netværk - tillad ikke peer-to-pe
         <p>on all access points and clients on the network. Disable the "ad-hoc" mode, which lets d
         </li>

         <li><h5>3. Stop med at udsende din routers netværks ID.</h5>
         <p>The SSID (Service Set Identifier) is essentially the network name for the wireless porti
         <p>For home networks, this broadcast information is not necessary. You can simply type in t
         <p>In public-access hotspots or large company Wi-Fi nets, SSID broadcasting may be required
         </li>

         <li><h5>4. Godkend på forhånd de bruger/computere der har tilladelse til at benytte det tra
         <p>in your wireless router. Most Wi-Fi gateways let you restrict access to known MAC (Media
         <p>Sound foolproof? Not quite. Even if your SSID isn't broadcast and you restrict access to
         </li>
```

```
    <li><h5>5. Slå trådløse data kryptering til.</h5>
    <p>Encryption is the next step in the wireless security ladder. WEP (wireless equivalency prot
    <p>While WEP is better than nothing, it will only keep out the neighbors and opportunistic hac
    <p>WPA builds on WEP encryption by scrambling the key and integrity-checking it to ensure it h
    <p>Note that WPA and WPA2 require that ALL devices on the wireless net be set to them -- clien
    <p>No matter which encryption type you use, change your passkey regularly. It takes recording
    <p>For more on WPA encryption check out Network World's primer Explaining WPA2. The Wi-Fi Alli
    </li>

    <li><h5>6. Undersøg periodevis routerens log for ikke-tilladte brugere.</h5>
    <p>attached to the network. Most Wi-Fi gateways have a status screen that shows the MAC addres
    <p>Another way to monitor your network is with a packet sniffer like the free Wireshark. Packe
    <p>Rogue clients aren't the only thing to look for, however. Rogue access points are dangerous
    </li>

    <li><h5>7. Brug en kraftig firewall.</h5>
    <p>The steps we've discussed so far focus on securing the wireless network, but once your wire
    <p>Most home networking routers come with built-in firewall capabilities. The firewall is usua
    <p>Unless you are running a Web or FTP server you shouldn't need any of the ports open, but so
    <p>You can also use a personal firewall like Zone Alarm Pro or Norton Personal Firewall (part
    </li>

    <li><h5>8. Beskyt din computer og vigtige dokumenter med password.</h5>
    <p>Often overlooked in a home environment, passwords provide another layer of security for you
    <p>Whenever possible, try to place private, confidential or otherwise sensitive documents in s
    <p>In general, the longer the password the longer it will take someone to find it using passwo
    </li>

    <li><h5>9. Placer dit trådløse netværk på dets eget undernet.</h5>
    <p>If you're a network pro and have a small office network, consider doing a couple more thing
    </li>

    <li><h5>10. Sluk altid for trådløse kort og routere hvis de ikke bliver brugt.</h5>
    <p>The final word of advice for home wireless networks is "Turn it off!" While it may seem lik
    </li>

    </ul>

  </td>
  <td rowspan="2">

  </td>
 </tr>
```

```
      <tr>
       <td>

       </td>
      </tr>

      <tr>
       <td align="right">


       </td>
       <td align="left">

         <input type="submit" name="submit" value="Tilbage"
         style="width: 90px; height: 30px;" />

       </td>
      </tr>


    </table>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.23 top10_hot.php

```
<?php include("header.php"); ?>

  <? if ($_SESSION["xawareid"] == "") { ?>
  <script type="text/javascript"> window.location="index.php"</script>
  <? } ?>

  <title>XAware - Trådløs netværk</title>
 </head>
 <body onload="Tid();">

 <? include ("menu.php") ?>

  <div id="box">
   <div id="content">
    <p><a href="default.php">Start side</a> > <b>Trådløs netværk</b></p>
    <h4>Trådløs netværk</h4>

    <h5>Top 10 Sikkerhedstips for opkobling til offentlige hotspots </h5>

    <table width="100%">
      <tr>
       <td align="left">
        <form id="wifi" method="post" action="wifi_16.php" >

         <ul>
         <li><h5>1. Sørg for at du kobler dig op på et legitimt Acces Point.</h5>
         <p>This first step is probably the least obvious, but one of the most important. Rogue access
         <p>So don't connect in places where there is no sign for a legitimate provider, and check the
         </li>

         <li><h5>2. Krypter dine emails for du sender dem videre.</h5>
         <p>As you beam emails from your laptop to the wireless access point and back, or as you enter
         <p>While data sent to and from secure Web sites (those starting with https:) is generally prot
         </li>

         <li><h5>3. Brug Virtuel Private Network (VPN).</h5>
         <p>One of the best ways to protect your data when using a public wireless network or hotspot i
         <p>If you don't have a corporate VPN, you can be secure at any hotspot using JiWire Hotspot He
         </li>

         <li><h5>4. Brug en personlig firewall.</h5>
         <p>When you connect to a public wireless network you are joining a local network with other un
```

```
    <p>To protect your computer you should run a personal firewall program. There are many exce
    <p>A personal firewall will help you restrict the traffic allowed in and out of your comput
    </li>

    <li><h5>5. Brug opdateret anti-virus software.</h5>
    <p>When you are on your home network or even on your company network you can operate with a
    <p>Of course, antivirus software is only as good as its last update. If you updated your an
    </li>

    <li><h5>6. Opdater regelmæssigt dit operativsystem.</h5>
    <p>It seems that almost every week there's a new "security patch" for various parts of the
    <p>Windows users should enable Automatic Updates or visit the Windows Update site to scan y
    </li>

    <li><h5>7. Vær opmærksom på folk omkring dig.</h5>
    <p>When you're at an ATM, you make sure noone can see you type your PIN. Be just as careful
    </li>

    <li><h5>8. Brug om muligt Webmail der anvender sikker http (https) fremfor eks. Outlook.</h
    <p>when you're connecting at a public hotspot, instead of Outlook or Apple Mail. Most ISPs
    </li>

    <li><h5>9. Slå al fil deling fra.</h5>
    <p>On home networks, file sharing is frequently used to copy files back and forth between c
    </li>

    <li><h5>10. Beskyt din computer og vigtige dokumenter med password.</h5>
    <p>Our final tip: use strong passwords for sensitive files and folders, as well as for acce
    </li>

    </ul>

  </td>
  <td rowspan="2">

  </td>
 </tr>
 <tr>
  <td>

  </td>
 </tr>

 <tr>
```

```
       <td align="right">


       </td>
       <td align="left">

         <input type="submit" name="submit" value="Tilbage"
         style="width: 90px; height: 30px;" />

       </td>
      </tr>


    </table>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.24 wifi_1.php

```
<?php include('header.php'); ?>

  <? if ($_SESSION["xawareid"] == "") { ?>
  <script type="text/javascript"> window.location="index.php"</script>
  <? } ?>

  <script type="text/javascript">
   function validateResult()
   {
    if((document.wifi1.wifi_1[0].checked == true) ||
       (document.wifi1.wifi_1[1].checked == true) ||
       (document.wifi1.wifi_1[2].checked == true) ||
       (document.wifi1.wifi_1[3].checked == true) ||
       (document.wifi1.wifi_1[4].checked == true))
    {
     getValue();
     return true;
    }
    else
    {
     alert("Der er ikke svaret på spørgsmålet! Vælg venligst en af svarmulighederne!");
     return false;
    }
   }

   function getValue()
   {
    var thisValue;
    thisValue = 0;

    if (document.wifi1.wifi_1[0].checked)
     thisValue = 0;
    else if (document.wifi1.wifi_1[1].checked)
     thisValue = 1;
    else if (document.wifi1.wifi_1[2].checked)
     thisValue = 2;
    else if (document.wifi1.wifi_1[3].checked)
     thisValue = 3;
    else if (document.wifi1.wifi_1[4].checked)
     thisValue = 4;

    document.wifi1.svar.value = thisValue;
```

```
  }
 </script>

 <title>XAware - Trådløs netværk</title>
</head>
<body onload="Tid();">

<?php include("menu.php"); ?>

 <div id="box">
  <div id="content">
   <p><a href="default.php">Start side</a> > <b>Trådløs netværk</b></p>
   <!--  -->
   <table colspan="2" width="100%">
    <h4>Trådløs netværk</h4>
    <tr>
     <td align="left">
      <form name="wifi1" method="post" onsubmit="return validateResult();" action="wifi_handler.php">
       <p><h5>1. Hvor ofte benytter du trådløs internet.</h5></p>
       <input type="radio" name="wifi_1" value="0"> Aldrig / meget sjældent
       <br>
       <input type="radio" name="wifi_1" value="1"> 1-3 gange om måneden
       <br>
       <input type="radio" name="wifi_1" value="2"> 1-2 gange om ugen
       <br>
       <input type="radio" name="wifi_1" value="3"> 3-4 gange om ugen
       <br>
       <input type="radio" name="wifi_1" value="4"> Flere gange dagligt
       <input type="hidden" name="svar" value= "" />

       <? $_SESSION["wifiside"] = 1; ?>

     </td>
    </tr>
    <tr>
     <td align="right">

     </td>
     <td align="left">

       <input type="submit" name="submit" value="Videre"
       style="width: 90px; height: 30px;" />

     </td>
```

```
     </tr>
    </table>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.25 wifi_2.php

```
<?php include("header.php"); ?>

  <? if ($_SESSION["xawareid"] == "") { ?>
  <script type="text/javascript"> window.location="index.php"</script>
  <? } ?>

  <script type="text/javascript">
   function validateResult()
   {
    if((document.wifi2.wifi_2[0].checked == true) ||
       (document.wifi2.wifi_2[1].checked == true) ||
       (document.wifi2.wifi_2[2].checked == true) ||
       (document.wifi2.wifi_2[3].checked == true))
    {
     getValue();
     return true;
    }
    else
    {
     alert("Der er ikke svaret på spørgsmålet! Vælg venligst en af svarmulighederne!");
     return false;
    }
   }

   function getValue()
   {
    var thisValue1;
    thisValue1 = 0;

    if (document.wifi2.wifi_2[0].checked)
     thisValue1 = 0;
    else if (document.wifi2.wifi_2[1].checked)
     thisValue1 = 1;
    else if (document.wifi2.wifi_2[2].checked)
     thisValue1 = 2;
    else if (document.wifi2.wifi_2[3].checked)
     thisValue1 = 3;

    document.wifi2.svar.value = thisValue1;
   }
  </script>
```

```
 <title>XAware - Trådløs netværk</title>
</head>
<body onload="Tid();">

<? include ("menu.php") ?>

 <div id="box">
  <div id="content">
   <p><a href="default.php">Start side</a> > <b>Trådløs netværk</b></p>
   <h4>Trådløs netværk</h4>

   <table width="100%">
     <tr>
      <td align="left">
       <form name="wifi2" method="post" action="wifi_handler.php"
       onsubmit="return validateResult();">
        <p><h5>2. Benytter du dig af trådløst netværk derhjemme/ på arbejdet?</h5></p>
        <input type="radio" name="wifi_2" value="0"> Kun derhjemme
        <br>
        <input type="radio" name="wifi_2" value="1"> Kun på arbejde
        <br>
        <input type="radio" name="wifi_2" value="2"> Begge steder
        <br>
        <input type="radio" name="wifi_2" value="3"> Ingen af delene
        <input type="hidden" name="svar" value="">

      </td>
      <td rowspan="2">

      </td>
     </tr>
     <tr>
      <td>

        <? $_SESSION["wifiside"] = 2; ?>

      </td>
     </tr>

     <tr>
      <td align="right">


      </td>
```

```
       <td align="left">

         <input type="submit" name="submit" value="Videre"
         style="width: 90px; height: 30px;" />

       </td>
      </tr>


    </table>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.26 wifi_3.php

```
<?php include("header.php"); ?>

  <? if ($_SESSION["xawareid"] == "") { ?>
  <script type="text/javascript"> window.location="index.php"</script>
  <? } ?>

  <script type="text/javascript">
   function validateResult()
   {
    if((document.wifi3.wifi_3[0].checked == true) ||
       (document.wifi3.wifi_3[1].checked == true) ||
       (document.wifi3.wifi_3[2].checked == true))
    {
     getValue();
     return true;
    }
    else
    {
     alert("Der er ikke svaret på spørgsmålet! Vælg venligst en af svarmulighederne!");
     return false;
    }
   }

   function getValue()
   {
    var thisValue2;
    thisValue2 = 0;

    if (document.wifi3.wifi_3[0].checked)
     thisValue2 = 0;
    else if (document.wifi3.wifi_3[1].checked)
     thisValue2 = 1;
    else if (document.wifi3.wifi_3[2].checked)
     thisValue2 = 2;

    document.wifi3.svar.value = thisValue2;
   }
  </script>

  <title>XAware - Trådløs netværk</title>
 </head>
 <body onload="Tid();">
```

```
<? include ("menu.php") ?>

 <div id="box">
  <div id="content">
   <p><a href="default.php">Start side</a> > <b>Trådløs netværk</b></p>
   <h4>Trådløs netværk</h4>

   <table width="100%">
     <tr>
      <td align="left">
       <form name="wifi3" method="post" action="wifi_handler.php"
       onsubmit="return validateResult();">
        <p><h5>3. Føler du dig sikker, når du surfer på Internettet?</h5></p>
        <input type="radio" name="wifi_3" value="0"> Ja
        <br>
        <input type="radio" name="wifi_3" value="1"> Nej
        <br>
        <input type="radio" name="wifi_3" value="2"> Ved ikke
        <input type="hidden" name="svar" value="">

      </td>
      <td rowspan="2">

      </td>
     </tr>
     <tr>
      <td>

        <? $_SESSION["wifiside"] = 3; ?>

      </td>
     </tr>

     <tr>
      <td align="right">


      </td>
      <td align="left">

        <input type="submit" name="submit" value="Videre"
        style="width: 90px; height: 30px;" />
```

```
       </td>
      </tr>


    </table>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.27 wifi_4.php

```
<?php include("header.php"); ?>

  <? if ($_SESSION["xawareid"] == "") { ?>
  <script type="text/javascript"> window.location="index.php"</script>
  <? } ?>

  <script type="text/javascript">
   function validateResult()
   {
    if((document.wifi4.wifi_4[0].checked == true) ||
       (document.wifi4.wifi_4[1].checked == true) ||
       (document.wifi4.wifi_4[2].checked == true))
    {
     getValue();
     return true;
    }
    else
    {
     alert("Der er ikke svaret på spørgsmålet! Vælg venligst en af svarmulighederne!");
     return false;
    }
   }

   function getValue()
   {
    var thisValue;
    thisValue = 0;

    if (document.wifi4.wifi_4[0].checked)
     thisValue = 0;
    else if (document.wifi4.wifi_4[1].checked)
     thisValue = 1;
    else if (document.wifi4.wifi_4[2].checked)
     thisValue = 2;


    document.wifi4.svar.value = thisValue;
   }
  </script>

  <title>XAware - Trådløs netværk</title>
 </head>
```

```
<body onload="Tid();">

<? include ("menu.php") ?>

 <div id="box">
  <div id="content">
   <p><a href="default.php">Start side</a> > <b>Trådløs netværk</b></p>
   <h4>Trådløs netværk</h4>
   <p>Hvis noget unormalt sker på din computer, et program der ikke opfører sig som det plejer, pr

   <table width="100%">
     <tr>
      <td align="left">
       <form name="wifi4" method="post" action="wifi_handler.php"
       onsubmit="return validateResult();">
        <p><h5>4. Ved du hvad du skal gøre eller hvem du skal henvende dig til hvis noget unormalt
        <input type="radio" name="wifi_4" value="0"> Ja
        <br>
        <input type="radio" name="wifi_4" value="1"> Nej
        <br>
        <input type="radio" name="wifi_4" value="2"> Ved ikke
        <input type="hidden" name="svar" value="">

      </td>
      <td rowspan="2">

      </td>
     </tr>
     <tr>
      <td>

        <? $_SESSION["wifiside"] = 4; ?>

      </td>
     </tr>

     <tr>
      <td align="right">

      </td>
      <td align="left">

        <input type="submit" name="submit" value="Videre"
        style="width: 90px; height: 30px;" />
```

```
       </td>
      </tr>


    </table>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.28 wifi_4_svar.php

```
<?php include("header.php"); ?>

  <? if ($_SESSION["xawareid"] == "") { ?>
  <script type="text/javascript"> window.location="index.php"</script>
  <? } ?>

  <title>XAware - Trådløs netværk</title>
 </head>
 <body onload="Tid();">

 <? include ("menu.php") ?>

  <div id="box">
   <div id="content">
    <p><a href="default.php">Start side</a> > <b>Trådløs netværk</b></p>
    <h4>Trådløs netværk</h4>

    <table width="100%">
      <tr>
       <td align="left">
        <form id="wifi4_svar" method="post" action="wifi_5.php" >

         <? If ($_SESSION["wifi_4"] == 0){ ?>
         <h2 style="color: green">Godt!</h2>
         <? } ?>
         <br />
         <p>Ifølge firmaets sikkerhedspolitik bør du i disse tilfælde gøre mindst én af følgende:</p
         <br />
         <ul>
         <li>Sluk din computer</li>
         <li>Kontakte din nærmeste leder</li>
         <li>Ringe til HelpDesk Security og beskrive problemet </li>
         <!-- <li><a href="https://intservices.sed1.root4.net/portal/internalportal/appmanager/norde
         </ul>



       <td rowspan="2">

       </td>
      </tr>
      <tr>
```

```
       <td>

         <? $_SESSION["wifiside"] = 4; ?>

       </td>
      </tr>

      <tr>
       <td align="right">

       </td>
       <td align="left">

         <input type="submit" name="submit" value="Videre"
         style="width: 90px; height: 30px;" />

       </td>
      </tr>


    </table>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.29 wifi_5.php

```
<?php include("header.php"); ?>

  <? if ($_SESSION["xawareid"] == "") { ?>
  <script type="text/javascript"> window.location="index.php"</script>
  <? } ?>

  <script type="text/javascript">
   function validateResult()
   {
    if((document.wifi5.wifi_5[0].checked == true) ||
       (document.wifi5.wifi_5[1].checked == true) ||
       (document.wifi5.wifi_5[2].checked == true))
    {
     getValue();
     return true;
    }
    else
    {
     alert("Der er ikke svaret på spørgsmålet! Vælg venligst en af svarmulighederne!");
     return false;
    }
   }

   function getValue()
   {
    var thisValue;
    thisValue = 0;

    if (document.wifi5.wifi_5[0].checked)
     thisValue = 0;
    else if (document.wifi5.wifi_5[1].checked)
     thisValue = 1;
    else if (document.wifi5.wifi_5[2].checked)
     thisValue = 2;

    document.wifi5.svar.value = thisValue;
   }
  </script>

  <title>XAware - Trådløs netværk</title>
 </head>
 <body onload="Tid();">
```

```
<? include ("menu.php") ?>

 <div id="box">
  <div id="content">
   <p><a href="default.php">Start side</a> > <b>Trådløs netværk</b></p>
   <h4>Trådløs netværk</h4>

   <table width="100%">
     <tr>
      <td align="left">
       <form name="wifi5" method="post" action="wifi_handler.php"
       onsubmit="return validateResult();">
        <p><h5>5. Har du modtaget undervisning eller blevet oplært i de daglige programmer du benytter
        <input type="radio" name="wifi_5" value="0"> Ja
        <br>
        <input type="radio" name="wifi_5" value="1"> Nej
        <br>
        <input type="radio" name="wifi_5" value="2"> Ved ikke
        <input type="hidden" name="svar" value="">

      </td>
      <td rowspan="2">

      </td>
     </tr>
     <tr>
      <td>

        <? $_SESSION["wifiside"] = 5; ?>

      </td>
     </tr>

     <tr>
      <td align="right">

      </td>
      <td align="left">

        <input type="submit" name="submit" value="Videre"
        style="width: 90px; height: 30px;" />

      </td>
```

```
      </tr>


    </table>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.30 wifi_5_svar.php

```
<?php include("header.php"); ?>

  <? if ($_SESSION["xawareid"] == "") { ?>
  <script type="text/javascript"> window.location="index.php"</script>
  <? } ?>

  <title>XAware - Trådløs netværk</title>
 </head>
 <body onload="Tid();">

 <? include ("menu.php") ?>

  <div id="box">
   <div id="content">
    <p><a href="default.php">Start side</a> > <b>Trådløs netværk</b></p>
    <h4>Trådløs netværk</h4>

    <table width="100%">
      <tr>
       <td align="left">
        <form id="wifi5_svar" method="post" action="wifi_6.php" >

         <? If ($_SESSION["wifi_5"] <> 0){ ?>
         <p>Svar spørgsmål 5: </p><h2 style="color: red">Forkert!</h2>

         <? } else { ?>
         <p>Svar spørgsmål 5: </p><h2 style="color: green">Korrekt!</h2>

         <? } ?>
         <p>En administrator har muligheden for at skjule det trådløse netværk for uvedkomne. Dette kan
         </p>
         <br />
         <br />
       <td rowspan="2">

       </td>
      </tr>
      <tr>
       <td>

         <? $_SESSION["wifiside"] = 5; ?>
```

```
       </td>
      </tr>

      <tr>
       <td align="right">

       </td>
       <td align="left">

         <input type="submit" name="submit" value="Videre"
         style="width: 90px; height: 30px;" />

       </td>
      </tr>


    </table>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.31 wifi_6.php

```
<?php include("header.php"); ?>

  <? if ($_SESSION["xawareid"] == "") { ?>
  <script type="text/javascript"> window.location="index.php"</script>
  <? } ?>

  <script type="text/javascript">
   function validateResult()
   {
    if((document.wifi.wifi_1[0].checked == true) ||
       (document.wifi.wifi_1[1].checked == true) ||
       (document.wifi.wifi_1[2].checked == true))
    {
     getValue();
     return true;
    }
    else
    {
     alert("Der er ikke svaret på spørgsmålet! Vælg venligst en af svarmulighederne!");
     return false;
    }
   }

   function getValue()
   {
    var thisValue;
    thisValue = 0;

    if (document.wifi.wifi_1[0].checked)
     thisValue = 0;
    else if (document.wifi.wifi_1[1].checked)
     thisValue = 1;
    else if (document.wifi.wifi_1[2].checked)
     thisValue = 2;

    document.wifi.svar.value = thisValue;
   }
  </script>

  <title>XAware - Trådløs netværk</title>
 </head>
 <body onload="Tid();">
```

```
<? include ("menu.php") ?>

 <div id="box">
  <div id="content">
   <p><a href="default.php">Start side</a> > <b>Trådløs netværk</b></p>
   <h4>Trådløs netværk</h4>

   <table width="100%">
     <tr>
      <td align="left">
       <form name="wifi" method="post" action="wifi_handler.php"
       onsubmit="return validateResult();">
        <p><h5>6. Har du gjort dig bekendt med firmaets IT-sikkerhedspolitik?</h5></p>
        <input type="radio" name="wifi_1" value="0"> Ja
        <br>
        <input type="radio" name="wifi_1" value="1"> Nej
        <br>
        <input type="radio" name="wifi_1" value="2"> Ved ikke
        <input type="hidden" name="svar" value="">

      </td>
      <td rowspan="2">

      </td>
     </tr>
     <tr>
      <td>

        <? $_SESSION["wifiside"] = 6; ?>

      </td>
     </tr>

     <tr>
      <td align="right">

      </td>
      <td align="left">

        <input type="submit" name="submit" value="Videre"
        style="width: 90px; height: 30px;" />

      </td>
```

```
      </tr>


    </table>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.32 wifi_7.php

```
<?php include("header.php"); ?>

  <? if ($_SESSION["xawareid"] == "") { ?>
  <script type="text/javascript"> window.location="index.php"</script>
  <? } ?>

  <script type="text/javascript">
   function validateResult()
   {
    if((document.wifi.wifi_1[0].checked == true) ||
       (document.wifi.wifi_1[1].checked == true) ||
       (document.wifi.wifi_1[2].checked == true) ||
       (document.wifi.wifi_1[3].checked == true))
    {
     getValue();
     return true;
    }
    else
    {
     alert("Der er ikke svaret på spørgsmålet! Vælg venligst en af svarmulighederne!");
     return false;
    }
   }

   function getValue()
   {
    var thisValue;
    thisValue = 0;

    if (document.wifi.wifi_1[0].checked)
     thisValue = 0;
    else if (document.wifi.wifi_1[1].checked)
     thisValue = 1;
    else if (document.wifi.wifi_1[2].checked)
     thisValue = 2;
    else if (document.wifi.wifi_1[3].checked)
     thisValue = 3;

    document.wifi.svar.value = thisValue;
   }
  </script>
```

```
 <title>XAware - Trådløs netværk</title>
</head>
<body onload="Tid();">

<? include ("menu.php") ?>

 <div id="box">
  <div id="content">
   <p><a href="default.php">Start side</a> > <b>Trådløs netværk</b></p>
   <h4>Trådløs netværk</h4>

   <table width="100%">
     <tr>
      <td align="left" width="60%" valign="top">
       <form name="wifi" method="post" action="wifi_handler.php"
       onsubmit="return validateResult();">
        <p><h5>7. Hvad betyder SSID?</h5></p>
        <input type="radio" name="wifi_1" value="0"> En krypteringsmetode
        <br>
        <input type="radio" name="wifi_1" value="1"> Sammenslutning af Sikkerhedsfolk I Danmark
        <br>
        <input type="radio" name="wifi_1" value="2"> Navnet på et trådløst netværk
        <br>
        <input type="radio" name="wifi_1" value="3"> Ved ikke
        <input type="hidden" name="svar" value="">
        <br />
        <br />
        <p>Du kan her trykke dig frem på billedet og prøve de mulige kombinationer som hvis du sad man
        <br /><br /><br /><br />
        <input type="submit" name="submit" value="Videre"
        style="width: 90px; height: 30px;" />

      </td>
      <td rowspan="2" align="left" valign="top">

       <object classid="clsid:d27cdb6e-ae6d-11cf-96b8-444553540000"    codebase="http://fpdownload.mac
        <param name="movie" value="Wireless_Manuel_custom.swf">
        <param name="quality" value="high">
        <param name="loop" value="0">
        <embed src="Wireless_Manuel_custom.swf" width="343" height="416" loop="0" quality="high" plugi
       </object>
      </td>
     </tr>
     <tr>
```

```
       <td>

         <? $_SESSION["wifiside"] = 7; ?>

       </td>
      </tr>

    </table>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.33 wifi_7_svar.php

```
<?php include("header.php"); ?>

  <? if ($_SESSION["xawareid"] == "") { ?>
  <script type="text/javascript"> window.location="index.php"</script>
  <? } ?>

  <title>XAware - Trådløs netværk</title>
 </head>
 <body onload="Tid();">

 <? include ("menu.php") ?>

  <div id="box">
   <div id="content">
    <p><a href="default.php">Start side</a> > <b>Trådløs netværk</b></p>
    <h4>Trådløs netværk</h4>

    <table width="100%">
      <tr>
       <td align="left">
        <form id="wifi_svar" method="post" action="wifi_8.php" >

         <? If ($_SESSION["wifi_7"] <> 2){ ?>
         <p>Svar spørgsmål 7: </p><h2 style="color: red">Forkert!</h2>
         <p>SSID, betyder Service Set Identifier eller som i daglig tale, navnet på det trådløse netvær
         <? } else { ?>
         <p>Svar spørgsmål 7: </p><h2 style="color: green">Korrekt!</h2>
         <p>SSID, betyder Service Set Identifier eller som du korrekt svarede, navnet på det trådløse n
         <? } ?>
         <p>Når man ønsker at se om der findes trådløst netværk inden for ens computers rækkevidde, sen
         </p>
         <br />
         <br />
       <td rowspan="2">

       </td>
      </tr>
      <tr>
       <td>

         <? $_SESSION["wifiside"] = 7; ?>
```

```
       </td>
      </tr>

      <tr>

       <td align="left">

         <input type="submit" name="submit" value="Videre"
         style="width: 90px; height: 30px;" />

       </td>
      </tr>


    </table>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.34 wifi_8.php

```
<?php include("header.php"); ?>

  <? if ($_SESSION["xawareid"] == "") { ?>
  <script type="text/javascript"> window.location="index.php"</script>
  <? } ?>

  <script type="text/javascript">
   function validateResult()
   {
    if((document.wifi.wifi_1[0].checked == true) ||
       (document.wifi.wifi_1[1].checked == true) ||
       (document.wifi.wifi_1[2].checked == true))
    {
     getValue();
     return true;
    }
    else
    {
     alert("Der er ikke svaret på spørgsmålet! Vælg venligst en af svarmulighederne!");
     return false;
    }
   }

   function getValue()
   {
    var thisValue;
    thisValue = 0;

    if (document.wifi.wifi_1[0].checked)
     thisValue = 0;
    else if (document.wifi.wifi_1[1].checked)
     thisValue = 1;
    else if (document.wifi.wifi_1[2].checked)
     thisValue = 2;

    document.wifi.svar.value = thisValue;
   }
  </script>

  <title>XAware - Trådløs netværk</title>
 </head>
 <body onload="Tid();">
```

```
<? include ("menu.php") ?>

 <div id="box">
  <div id="content">
   <p><a href="default.php">Start side</a> > <b>Trådløs netværk</b></p>
   <h4>Trådløs netværk</h4>
   <table width="100%">
     <tr>
      <td align="left" width="60%" valign="top">
       <form name="wifi" method="post" action="wifi_handler.php"
       onsubmit="return validateResult();">
        <p><h5>8. Kan det trådløse netværk skjules så uvedkomne ikke kan se det?</h5></p>
        <input type="radio" name="wifi_1" value="0"> Ja
        <br>
        <input type="radio" name="wifi_1" value="1"> Nej
        <br>
        <input type="radio" name="wifi_1" value="2"> Ved ikke
        <input type="hidden" name="svar" value="">
        <br />
        <br />
        <p>Du kan her trykke dig frem på billedet og prøve de mulige kombinationer som hvis du sad
        <br /><br /><br /><br />
        <input type="submit" name="submit" value="Videre"
        style="width: 90px; height: 30px;" />

      </td>
      <td rowspan="2" align="left" valign="top">

       <object classid="clsid:d27cdb6e-ae6d-11cf-96b8-444553540000"    codebase="http://fpdownload
        <param name="movie" value="Wireless_Manuel_custom.swf">
        <param name="quality" value="high">
        <param name="loop" value="0">
        <embed src="Wireless_Manuel_custom.swf" width="343" height="416" loop="0" quality="high" pl
       </object>
      </td>
     </tr>
     <tr>
      <td>

        <? $_SESSION["wifiside"] = 8; ?>

      </td>
     </tr>
```

```
    </table>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.35 wifi_8_svar.php

```
<?php include("header.php"); ?>

  <? if ($_SESSION["xawareid"] == "") { ?>
  <script type="text/javascript"> window.location="index.php"</script>
  <? } ?>

  <title>XAware - Trådløs netværk</title>
 </head>
 <body onload="Tid();">

 <? include ("menu.php") ?>

  <div id="box">
   <div id="content">
    <p><a href="default.php">Start side</a> > <b>Trådløs netværk</b></p>
    <h4>Trådløs netværk</h4>

    <table width="100%">
      <tr>
       <td align="left">
        <form id="wifi8_svar" method="post" action="wifi_9.php" >

         <? If ($_SESSION["wifi_8"] <> 0){ ?>
         <p>Svar spørgsmål 8: </p><h2 style="color: red">Forkert!</h2>

         <? } else { ?>
         <p>Svar spørgsmål 8: </p><h2 style="color: green">Korrekt!</h2>

         <? } ?>
         <p>En administrator har muligheden for at skjule det trådløse netværk for uvedkomne. Dette
         </p>
         <br />
         <br />
       <td rowspan="2">

       </td>
      </tr>
      <tr>
       <td>

         <? $_SESSION["wifiside"] = 8; ?>
```

```
       </td>
      </tr>

      <tr>
       <td align="right">


       </td>
       <td align="left">

         <input type="submit" name="submit" value="Videre"
         style="width: 90px; height: 30px;" />

       </td>
      </tr>


    </table>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.36 wifi_9.php

```
<?php include("header.php"); ?>

  <? if ($_SESSION["xawareid"] == "") { ?>
  <script type="text/javascript"> window.location="index.php"</script>
  <? } ?>

  <script type="text/javascript">
   function validateResult()
   {
    if((document.wifi.wifi_1[0].checked == true) ||
       (document.wifi.wifi_1[1].checked == true) ||
       (document.wifi.wifi_1[2].checked == true) ||
       (document.wifi.wifi_1[3].checked == true))
    {
     getValue();
     return true;
    }
    else
    {
     alert("Der er ikke svaret på spørgsmålet! Vælg venligst en af svarmulighederne!");
     return false;
    }
   }

   function getValue()
   {
    var thisValue;
    thisValue = 0;

    if (document.wifi.wifi_1[0].checked)
     thisValue = 0;
    else if (document.wifi.wifi_1[1].checked)
     thisValue = 1;
    else if (document.wifi.wifi_1[2].checked)
     thisValue = 2;
    else if (document.wifi.wifi_1[3].checked)
     thisValue = 3;

    document.wifi.svar.value = thisValue;
   }
  </script>
```

```
 <title>XAware - Trådløs netværk</title>
</head>
<body onload="Tid();">

<? include ("menu.php") ?>

 <div id="box">
  <div id="content">
   <p><a href="default.php">Start side</a> > <b>Trådløs netværk</b></p>
   <h4>Trådløs netværk</h4>

   <table width="100%">
     <tr>
      <td align="left" width="60%" valign="top">
       <form name="wifi" method="post" action="wifi_handler.php"
       onsubmit="return validateResult();">
        <p><h5>9. Vælg den mest sikre netværksgodkendelsesmetode.</h5></p>
        <input type="radio" name="wifi_1" value="0"> Åben
        <br>
        <input type="radio" name="wifi_1" value="1"> Delt
        <br>
        <input type="radio" name="wifi_1" value="2"> WPA
        <br>
        <input type="radio" name="wifi_1" value="3"> WPA-PSK
        <input type="hidden" name="svar" value="">
        <br />
        <br />
        <p>Du kan her trykke dig frem på billedet og prøve de mulige kombinationer som hvis du sad man
        <br /><br /><br /><br />
        <input type="submit" name="submit" value="Videre"
        style="width: 90px; height: 30px;" />

      </td>
      <td rowspan="2" align="left" valign="top">

       <object classid="clsid:d27cdb6e-ae6d-11cf-96b8-444553540000"    codebase="http://fpdownload.mac
        <param name="movie" value="Wireless_Manuel_custom.swf">
        <param name="quality" value="high">
        <param name="loop" value="0">
        <embed src="Wireless_Manuel_custom.swf" width="343" height="416" loop="0" quality="high" plugi
       </object>
      </td>
     </tr>
     <tr>
```

```
       <td>

         <? $_SESSION["wifiside"] = 9; ?>

       </td>
      </tr>
    </table>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.37 wifi_10.php

```
<?php include("header.php"); ?>

  <? if ($_SESSION["xawareid"] == "") { ?>
  <script type="text/javascript"> window.location="index.php"</script>
  <? } ?>

  <script type="text/javascript">
   function validateResult()
   {
    if((document.wifi.wifi_1[0].checked == true) ||
       (document.wifi.wifi_1[1].checked == true) ||
       (document.wifi.wifi_1[2].checked == true) ||
       (document.wifi.wifi_1[3].checked == true))
    {
     getValue();
     return true;
    }
    else
    {
     alert("Der er ikke svaret på spørgsmålet! Vælg venligst en af svarmulighederne!");
     return false;
    }
   }

   function getValue()
   {
    var thisValue;
    thisValue = 0;

    if (document.wifi.wifi_1[0].checked)
     thisValue = 0;
    else if (document.wifi.wifi_1[1].checked)
     thisValue = 1;
    else if (document.wifi.wifi_1[2].checked)
     thisValue = 2;
    else if (document.wifi.wifi_1[3].checked)
     thisValue = 3;

    document.wifi.svar.value = thisValue;
   }
  </script>
```

```
 <title>XAware - Trådløs netværk</title>
</head>
<body onload="Tid();">

<? include ("menu.php") ?>

 <div id="box">
  <div id="content">
   <p><a href="default.php">Start side</a> > <b>Trådløs netværk</b></p>
   <h4>Trådløs netværk</h4>

   <table width="100%">
     <tr>
      <td align="left" width="60%" valign="top">
       <form name="wifi" method="post" action="wifi_handler.php"
       onsubmit="return validateResult();">
        <p><h5>10. Vælg den mest sikre datakrypteringsmetode.</h5></p>
        <input type="radio" name="wifi_1" value="0"> Deaktiveret
        <br>
        <input type="radio" name="wifi_1" value="1"> WEP
        <br>
        <input type="radio" name="wifi_1" value="2"> AES (kræver WPA eller WPA-PSK)
        <br>
        <input type="radio" name="wifi_1" value="3"> TKIP (kræver WPA eller WPA-PSK)
        <input type="hidden" name="svar" value="">
        <br />
        <br />
        <p>Du kan her trykke dig frem på billedet og prøve de mulige kombinationer som hvis du sad
        <br /><br /><br /><br />
        <input type="submit" name="submit" value="Videre"
        style="width: 90px; height: 30px;" />

      </td>
      <td rowspan="2" align="left" valign="top">

       <object classid="clsid:d27cdb6e-ae6d-11cf-96b8-444553540000"    codebase="http://fpdownload
        <param name="movie" value="Wireless_Manuel_custom.swf">
        <param name="quality" value="high">
        <param name="loop" value="0">
        <embed src="Wireless_Manuel_custom.swf" width="343" height="416" loop="0" quality="high" pl
       </object>
      </td>
     </tr>
     <tr>
```

```
       <td>

         <? $_SESSION["wifiside"] = 10; ?>

       </td>
      </tr>
    </table>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.38 wifi_10_svar.php

```
<?php include("header.php"); ?>

  <? if ($_SESSION["xawareid"] == "") { ?>
  <script type="text/javascript"> window.location="index.php"</script>
  <? } ?>

  <title>XAware - Trådløs netværk</title>
 </head>
 <body onload="Tid();">

 <? include ("menu.php") ?>

  <div id="box">
   <div id="content">
    <p><a href="default.php">Start side</a> > <b>Trådløs netværk</b></p>
    <h4>Trådløs netværk</h4>

    <table width="100%">
      <tr>
       <td align="left">
        <form id="wifi_svar" method="post" action="wifi_11.php" >

         <? If (($_SESSION["wifi_9"] < 2) OR ($_SESSION["wifi_10"] < 2) ){ ?>
         <p>Svar spørgsmål 9 & 10: </p><h2 style="color: red">Forkert!</h2>

         <? } else { ?>
         <p>Svar spørgsmål 9 & 10: </p><h2 style="color: green">Korrekt!</h2>

         <? } ?>
         <p>En kombination af den stærkest tilgængelige krypterings- og netværksgodkendelsesmetode v

         <p>Den ønskede kombination er i dette tilfælde at der bliver valgt enten WPA eller WPA-PSK

         <p> </p>
       <td rowspan="2">

       </td>
      </tr>
      <tr>
       <td>

         <? $_SESSION["wifiside"] = 10; ?>
```

```
       </td>
      </tr>

      <tr>
       <td align="right">

       </td>
       <td align="left">

         <input type="submit" name="submit" value="Videre"
         style="width: 90px; height: 30px;" />

       </td>
      </tr>


    </table>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.39 wifi_11.php

```
<?php include("header.php"); ?>

  <? if ($_SESSION["xawareid"] == "") { ?>
  <script type="text/javascript"> window.location="index.php"</script>
  <? } ?>

  <script type="text/javascript">
   function validateResult()
   {
    if((document.wifi.wifi_1[0].checked == true) ||
       (document.wifi.wifi_1[1].checked == true) ||
       (document.wifi.wifi_1[2].checked == true) ||
       (document.wifi.wifi_1[3].checked == true))
    {
     getValue();
     return true;
    }
    else
    {
     alert("Der er ikke svaret på spørgsmålet! Vælg venligst en af svarmulighederne!");
     return false;
    }
   }

   function getValue()
   {
    var thisValue;
    thisValue = 0;

    if (document.wifi.wifi_1[0].checked)
     thisValue = 0;
    else if (document.wifi.wifi_1[1].checked)
     thisValue = 1;
    else if (document.wifi.wifi_1[2].checked)
     thisValue = 2;
    else if (document.wifi.wifi_1[3].checked)
     thisValue = 3;

    document.wifi.svar.value = thisValue;
   }
  </script>
```

```
 <title>XAware - Trådløs netværk</title>
</head>
<body onload="Tid();">

<? include ("menu.php") ?>

 <div id="box">
  <div id="content">
   <p><a href="default.php">Start side</a> > <b>Trådløs netværk</b></p>
   <h4>Trådløs netværk</h4>
   <p></p>
   <table width="100%">
     <tr>
      <td align="left" valign="top" width="30%">
       <form name="wifi" method="post" action="wifi_handler.php"
       onsubmit="return validateResult();">
        <p>11. Vælg det mest sikre trådløse netværk?</p>
        <input type="radio" name="wifi_1" value="0"> Magnusson
        <br>
        <input type="radio" name="wifi_1" value="1"> Default
        <br>
        <input type="radio" name="wifi_1" value="2"> Tumpe
        <br>
        <input type="radio" name="wifi_1" value="3"> Ved ikke
        <input type="hidden" name="svar" value="">
        <br /><br /><br />
        <p>Prøv dig frem, og vælge det mest sikre trådløse netværk at koble dig op på.</p>
        <br /><br /><br />
        <input type="submit" name="submit" value="Videre"
        style="width: 90px; height: 30px;" />

      </td>
      <td rowspan="2">
       <object classid="clsid:d27cdb6e-ae6d-11cf-96b8-444553540000" codebase="http://fpdownload.macrom
        <param name="movie" value="wifi_new.swf">
        <param name="quality" value="high">
        <param name="loop" value="0">
        <embed src="wifi_new.swf" width="553" height="427" loop="0" quality="high" pluginspage="http:/
       </object>

       <? $_SESSION["wifiside"] = 11; ?>

      </td>
     </tr>
```

```
    </table>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.40 wifi_11_svar.php

```
<?php include("header.php"); ?>

  <? if ($_SESSION["xawareid"] == "") { ?>
  <script type="text/javascript"> window.location="index.php"</script>
  <? } ?>

  <title>XAware - Trådløs netværk</title>
 </head>
 <body onload="Tid();">

 <? include ("menu.php") ?>

  <div id="box">
   <div id="content">
    <p><a href="default.php">Start side</a> > <b>Trådløs netværk</b></p>
    <h4>Trådløs netværk</h4>

    <table width="100%">
      <tr>
       <td align="left">
        <form id="wifi_svar" method="post" action="wifi_12.php" >

         <? If ($_SESSION["wifi_11"] <> 0) { ?>
         <p>Svar spørgsmål 11: </p><h2 style="color: red">Forkert!</h2>

         <? } else { ?>
         <p>Svar spørgsmål 11: </p><h2 style="color: green">Korrekt!</h2>
         <? } ?>
         <p>Trådløse netværk uden en form for sikkerhed som kryptering aktiveret, sender alt informatio
         <br />
         <p>Trådløse netværk med sikkerhedsaktivering som kryptering, koder alle beskeder der bliver se
         <br />
         <br />

       <td rowspan="2">

       </td>
      </tr>
      <tr>
       <td>

         <? $_SESSION["wifiside"] = 11; ?>
```

```
       </td>
      </tr>

      <tr>
       <td align="right">

       </td>
       <td align="left">

         <input type="submit" name="submit" value="Videre"
         style="width: 90px; height: 30px;" />

       </td>
      </tr>


    </table>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.41 wifi_12.php

```
<?php include("header.php"); ?>

  <? if ($_SESSION["xawareid"] == "") { ?>
  <script type="text/javascript"> window.location="index.php"</script>
  <? } ?>

  <script type="text/javascript">
   function validateResult()
   {
    if((document.wifi.wifi_1[0].checked == true) ||
       (document.wifi.wifi_1[1].checked == true) ||
       (document.wifi.wifi_1[2].checked == true))
    {
     getValue();
     return true;
    }
    else
    {
     alert("Der er ikke svaret på spørgsmålet! Vælg venligst en af svarmulighederne!");
     return false;
    }
   }

   function getValue()
   {
    var thisValue;
    thisValue = 0;

    if (document.wifi.wifi_1[0].checked)
     thisValue = 0;
    else if (document.wifi.wifi_1[1].checked)
     thisValue = 1;
    else if (document.wifi.wifi_1[2].checked)
     thisValue = 2;

    document.wifi.svar.value = thisValue;
   }
  </script>

  <title>XAware - Trådløs netværk</title>
 </head>
 <body onload="Tid();">
```

```
<? include ("menu.php") ?>

 <div id="box">
  <div id="content">
   <p><a href="default.php">Start side</a> > <b>Trådløs netværk</b></p>
   <h4>Trådløs netværk</h4>

   <table width="100%">
     <tr>
      <td align="left">
       <form name="wifi" method="post" action="wifi_handler.php"
       onsubmit="return validateResult();">
        <p><h5>12. Bør dit trådløse netværk være krypteret?</h5></p>
        <input type="radio" name="wifi_1" value="0"> Nej det er alt for besværligt og ikke nødvendi
        <br>
        <input type="radio" name="wifi_1" value="1"> Ja selvfølgelig
        <br>
        <input type="radio" name="wifi_1" value="2"> Ved ikke
        <input type="hidden" name="svar" value="">

      </td>
      <td rowspan="2">

      </td>
     </tr>
     <tr>
      <td>

        <? $_SESSION["wifiside"] = 12; ?>

      </td>
     </tr>

     <tr>
      <td align="right">

      </td>
      <td align="left">

        <input type="submit" name="submit" value="Videre"
        style="width: 90px; height: 30px;" />

      </td>
```

```
      </tr>


    </table>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.42 wifi_12_svar.php

```
<?php include("header.php"); ?>

  <? if ($_SESSION["xawareid"] == "") { ?>
  <script type="text/javascript"> window.location="index.php"</script>
  <? } ?>

  <title>XAware - Trådløs netværk</title>
 </head>
 <body onload="Tid();">

 <? include ("menu.php") ?>

  <div id="box">
   <div id="content">
    <p><a href="default.php">Start side</a> > <b>Trådløs netværk</b></p>
    <h4>Trådløs netværk</h4>

    <table width="100%">
      <tr>
       <td align="left">
        <form id="wifi_svar" method="post" action="wifi_13.php" >

         <? If ($_SESSION["wifi_12"] <> 1) { ?>
         <p>Svar spørgsmål 12: </p><h2 style="color: red">Forkert!</h2>

         <? } else { ?>
         <p>Svar spørgsmål 12: </p><h2 style="color: green">Korrekt!</h2>
         <p> Ja selvfølgelig! </p>
         <? } ?>
         <p>Hvis ikke dit trådløse netværk er krypteret vil det være muligt for enhver hacker at læs
         <br />
         <p>Nedenfor er vist et eksempel på hvad en hacker kan opfange af data hvis det trådløse net
         <br />
         <br />
         <H3>Et ukrypteret trådløst netværk set fra en hacker. (engelsk)</H3>
         <P>First, let&#146;s take a look at what a Wi-Fi eavesdropper can see when you send an e-ma

         <P><IMG style="WIDTH: 323px; HEIGHT: 276px" border="1" alt="Security Email " src="images/se
         <P>At the same time, I captured packets from the network on my laptop using a free tool cal
         <P><IMG style="WIDTH: 731px; HEIGHT: 523px" alt=Ethereal src="images/securityissues02.gif"
         <P>If that isn&#146;t bad enough, see what I captured in the packet trace shown in Figure 3
         <P><IMG style="WIDTH: 689px; HEIGHT: 482px" alt="Ethereal shows POP3 info" src="images/secu
```

```
        <P>To clarify, the administrator of this wireless network could have changed the default SSID,
        <P>You should also note that I did capture these packets in Ethereal via an Ethernet connectio
       <td rowspan="2">

       </td>
      </tr>
      <tr>
       <td>

        <? $_SESSION["wifiside"] = 12; ?>

       </td>
       <td align="left">

        <input type="submit" name="submit" value="Videre"
        style="width: 90px; height: 30px;" />

       </td>
      </tr>
    </table>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.43 wifi_13.php

```
<?php include("header.php"); ?>

  <? if ($_SESSION["xawareid"] == "") { ?>
  <script type="text/javascript"> window.location="index.php"</script>
  <? } ?>

  <script type="text/javascript">
   function validateResult()
   {
    if((document.wifi.wifi_1[0].checked == true) ||
       (document.wifi.wifi_1[1].checked == true) ||
       (document.wifi.wifi_1[2].checked == true))
    {
     getValue();
     return true;
    }
    else
    {
     alert("Der er ikke svaret på spørgsmålet! Vælg venligst en af svarmulighederne!");
     return false;
    }
   }

   function getValue()
   {
    var thisValue;
    thisValue = 0;

    if (document.wifi.wifi_1[0].checked)
     thisValue = 0;
    else if (document.wifi.wifi_1[1].checked)
     thisValue = 1;
    else if (document.wifi.wifi_1[2].checked)
     thisValue = 2;

    document.wifi.svar.value = thisValue;
   }
  </script>

  <title>XAware - Trådløs netværk</title>
 </head>
 <body onload="Tid();">
```

```
<? include ("menu.php") ?>

 <div id="box">
  <div id="content">
   <p><a href="default.php">Start side</a> > <b>Trådløs netværk</b></p>
   <h4>Trådløs netværk</h4>

   <table width="100%">
     <tr>
      <td align="left">
       <form name="wifi" method="post" action="wifi_handler.php"
       onsubmit="return validateResult();">
        <p><h5>13. Når du benytter trådløst netværk med din arbejdscomputer hjemmefra eller fra et off
        <input type="radio" name="wifi_1" value="0"> Ved ikke hvad det betyder
        <br>
        <input type="radio" name="wifi_1" value="1"> Ja det er den sikreste metode for både dig og vir
        <br>
        <input type="radio" name="wifi_1" value="2"> Nej det er ikke nødvendigt
        <input type="hidden" name="svar" value="">

      </td>
      <td rowspan="2">

      </td>
     </tr>
     <tr>
      <td>

        <? $_SESSION["wifiside"] = 13; ?>

      </td>
     </tr>

     <tr>
      <td align="right">

      </td>
      <td align="left">

        <input type="submit" name="submit" value="Videre"
        style="width: 90px; height: 30px;" />

      </td>
```

```
      </tr>


    </table>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.44 wifi_13_svar.php

```
<?php include("header.php"); ?>

  <? if ($_SESSION["xawareid"] == "") { ?>
  <script type="text/javascript"> window.location="index.php"</script>
  <? } ?>

  <title>XAware - Trådløs netværk</title>
 </head>
 <body onload="Tid();">

 <? include ("menu.php") ?>

  <div id="box">
   <div id="content">
    <p><a href="default.php">Start side</a> > <b>Trådløs netværk</b></p>
    <h4>Trådløs netværk</h4>

    <table width="100%">
      <tr>
       <td align="left" width="60%" valign="top">
        <form id="wifi_svar" method="post" action="wifi_14.php" >

         <? If ($_SESSION["wifi_13"] <> 1) { ?>
         <p>Svar spørgsmål 13: </p><h2 style="color: red">Forkert!</h2>
         <p> Det er altid en god idé at oprette forbindelsen igennem VPN og i mange tilfælde er det et

         <? } else { ?>
         <p>Svar spørgsmål 13: </p><h2 style="color: green">Korrekt!</h2>
         <p> Ja det er altid en god idé at oprette forbindelsen igennem VPN og i mange tilfælde er det
         <? } ?>
         <br />
         <p>VPN eller Virtual Private Network, på dansk "virtuelt privat datanet", er betegnelsen på en
         <p>Formålet med VPN er at gøre det lettere at få tilgang til virksomhedens services på LANet e
         Med en krypteret VPN kan man skabe en sikker privat forbindelse over f.eks. et offentligt data
         <br />
         <br />
       </td>
       <td rowspan="2">
         <img src="images/etoken.jpg" width="192" height="144" class="curve" />
       </td>
      </tr>
      <tr>
```

```
       <td>

         <? $_SESSION["wifiside"] = 13; ?>

       </td>
       <td align="rigth" width="40%">
        <p>Det er f.eks. muligt at oprette en sikker VPN forbindelse til et virksomhedsnetværk ved b
       </td>
      </tr>

      <tr>
       <td align="right">

       </td>
       <td align="left">

         <input type="submit" name="submit" value="Videre"
         style="width: 90px; height: 30px;" />

       </td>
      </tr>


    </table>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.45 wifi_14.php

```
<?php include("header.php"); ?>

  <? if ($_SESSION["xawareid"] == "") { ?>
  <script type="text/javascript"> window.location="index.php"</script>
  <? } ?>

  <script type="text/javascript">
   function validateResult()
   {
    if((document.wifi.wifi_1[0].checked == true) ||
       (document.wifi.wifi_1[1].checked == true) ||
       (document.wifi.wifi_1[2].checked == true) ||
       (document.wifi.wifi_1[3].checked == true))
    {
     getValue();
     return true;
    }
    else
    {
     alert("Der er ikke svaret på spørgsmålet! Vælg venligst en af svarmulighederne!");
     return false;
    }
   }

   function getValue()
   {
    var thisValue;
    thisValue = 0;

    if (document.wifi.wifi_1[0].checked)
     thisValue = 0;
    else if (document.wifi.wifi_1[1].checked)
     thisValue = 1;
    else if (document.wifi.wifi_1[2].checked)
     thisValue = 2;
    else if (document.wifi.wifi_1[3].checked)
     thisValue = 3;

    document.wifi.svar.value = thisValue;
   }
  </script>
```

```
 <title>XAware - Trådløs netværk</title>
</head>
<body onload="Tid();">

<? include ("menu.php") ?>

 <div id="box">
  <div id="content">
   <p><a href="default.php">Start side</a> > <b>Trådløs netværk</b></p>
   <h4>Trådløs netværk</h4>

   <table width="100%">
     <tr>
      <td align="left" valign="top">
       <form name="wifi" method="post" action="wifi_handler.php"
       onsubmit="return validateResult();">
        <p><h5>14. Hvad bruges denne eToken til?</h5></p>
        <input type="radio" name="wifi_1" value="0"> Bruges når der skal oprettes en VPN forbindels
        <br>
        <input type="radio" name="wifi_1" value="1"> En USB-lagerenhed hvor der kan gemmes dokument
        <br>
        <input type="radio" name="wifi_1" value="2"> Bruges når harddisken skal krypteres
        <br>
        <input type="radio" name="wifi_1" value="3"> Ved ikke
        <input type="hidden" name="svar" value="">

      </td>
      <td rowspan="2">
       <img src="images/etoken.jpg" width="192" height="144" class="curve" />
      </td>
     </tr>
     <tr>
      <td>

        <? $_SESSION["wifiside"] = 14; ?>

      </td>
     </tr>

     <tr>
      <td align="right">

      </td>
      <td align="left">
```

```
        <input type="submit" name="submit" value="Videre"
        style="width: 90px; height: 30px;" />

       </td>
      </tr>


    </table>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.46 wifi_15.php

```
<?php include("header.php"); ?>

  <? if ($_SESSION["xawareid"] == "") { ?>
  <script type="text/javascript"> window.location="index.php"</script>
  <? } ?>

  <script type="text/javascript">
   function validateResult()
   {
    if((document.wifi.wifi_1[0].checked == true) ||
       (document.wifi.wifi_1[1].checked == true) ||
       (document.wifi.wifi_1[2].checked == true))
    {
     getValue();
     return true;
    }
    else
    {
     alert("Der er ikke svaret på spørgsmålet! Vælg venligst en af svarmulighederne!");
     return false;
    }
   }

   function getValue()
   {
    var thisValue;
    thisValue = 0;

    if (document.wifi.wifi_1[0].checked)
     thisValue = 0;
    else if (document.wifi.wifi_1[1].checked)
     thisValue = 1;
    else if (document.wifi.wifi_1[2].checked)
     thisValue = 2;

    document.wifi.svar.value = thisValue;
   }
  </script>

  <title>XAware - Trådløs netværk</title>
 </head>
 <body onload="Tid();">
```

```
<? include ("menu.php") ?>

 <div id="box">
  <div id="content">
   <p><a href="default.php">Start side</a> > <b>Trådløs netværk</b></p>
   <h4>Trådløs netværk</h4>

   <table width="100%">
     <tr>
      <td align="left" valign="top">
       <form name="wifi" method="post" action="wifi_handler.php"
       onsubmit="return validateResult();">
        <p><h5>15. Vælg den sikreste af netværksgodkendelsesmetoder og datakrypteringsmetoder af neden
        <input type="radio" name="wifi_1" value="0"> Åben + WEP
        <br>
        <input type="radio" name="wifi_1" value="1"> Delt + WEP
        <br>
        <input type="radio" name="wifi_1" value="2"> WPA + AES
        <br>
        <input type="radio" name="wifi_1" value="3"> Ved ikke
        <input type="hidden" name="svar" value="">
        <br />
        <br />
        <p>Du kan her trykke dig frem på billedet og prøve de mulige kombinationer som hvis du sad man
        <br /><br /><br /><br />
        <input type="submit" name="submit" value="Videre"
        style="width: 90px; height: 30px;" />

      </td>
      <td rowspan="2" align="left" valign="top">

       <object classid="clsid:d27cdb6e-ae6d-11cf-96b8-444553540000"    codebase="http://fpdownload.mac
        <param name="movie" value="Wireless_Manuel_custom.swf">
        <param name="quality" value="high">
        <param name="loop" value="0">
        <embed src="Wireless_Manuel_custom.swf" width="343" height="416" loop="0" quality="high" plugi
       </object>
      </td>
     </tr>
     <tr>
      <td>

        <? $_SESSION["wifiside"] = 15; ?>
```

```
       </td>
      </tr>



    </table>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.47 wifi_16.php

```
<?php include("header.php"); ?>

  <? if ($_SESSION["xawareid"] == "") { ?>
  <script type="text/javascript"> window.location="index.php"</script>
  <? } ?>

  <title>XAware - Trådløs netværk</title>
 </head>
 <body onload="Tid();">

 <? include ("menu.php") ?>

  <div id="box">
   <div id="content">
    <p><a href="default.php">Start side</a> > <b>Trådløs netværk</b></p>
    <h4>Trådløs netværk</h4>
    <p>Du bør i princippet kunne bruge din arbejdscomputer (læse/skrive mails, se nyheder på intranette
    <p>Når man benytter trådløst netværk hvad enten det er via offentlige hotspots (f.eks. i lufthavnen

    <table width="100%">
      <tr>
       <td align="left">
        <form id="wifi" method="post" action="wifi_17.php" >
         <h5>16. Top 10 Sikkerhedstips for opkobling til offentlige hotspots: <a href="top10_hot.php">(
         <ul>
         <li>1. Sørg for at du kobler dig op på et legitimt Acces Point.</li>
         <li>2. Krypter dine emails for du sender dem videre.</li>
         <li>3. Brug Virtuel Private Network (VPN).</li>
         <li>4. Brug en personlig firewall. </li>
         <li>5. Brug opdateret anti-virus software. </li>
         <li>6. Opdater regelmæssigt dit operativsystem. </li>
         <li>7. Vær opmærksom på folk omkring dig. </li>
         <li>8. Brug om muligt Webmail der anvender sikker http (https) fremfor eks. Outlook.</li>
         <li>9. Slå al fil deling fra. </li>
         <li>10. Beskyt din computer og vigtige dokumenter med password.</li>
         </ul>

         <p>Tryk på videre for at se en tilsvarende top 10 for opkobling til hjemme netværk.</p>
       </td>
       <td rowspan="2">

       </td>
```

```
      </tr>
      <tr>
       <td>

       </td>
      </tr>

      <tr>
       <td align="right">

       </td>
       <td align="left">

         <input type="submit" name="submit" value="Videre"
         style="width: 90px; height: 30px;" />

       </td>
      </tr>


    </table>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.48 wifi_17.php

```
<?php include("header.php"); ?>

  <? if ($_SESSION["xawareid"] == "") { ?>
  <script type="text/javascript"> window.location="index.php"</script>
  <? } ?>

  <title>XAware - Trådløs netværk</title>
 </head>
 <body onload="Tid();">

 <? include ("menu.php") ?>

  <div id="box">
   <div id="content">
    <p><a href="default.php">Start side</a> > <b>Trådløs netværk</b></p>
    <h4>Trådløs netværk</h4>
    <p>Du bør i princippet kunne bruge din arbejdscomputer (læse/skrive mails, se nyheder på intranette
    <p>Når man benytter trådløst netværk hvad enten det er via offentlige hotspots (f.eks. i lufthavnen

    <table width="100%">
      <tr>
       <td align="left">
        <form id="wifi" method="post" action="wifi_18.php" >
         <h5>17. Top 10 Sikkerhedstips for opkobling til hjemme netværk: <a href="top10_home.php">(Se e
         <ul>
         <li>1. Ændre brugernavn og adgangskode til din router.</li>
         <li>2. Lad ikke andre brugere ride med på dit trådløse netværk - tillad ikke peer-to-peer forb
         <li>3. Stop med at udsende din routers netværks ID.</li>
         <li>4. Godkend på forhånd de bruger/computere der har tilladelse til at benytte det trådløse n
         <li>5. Slå trådløse data kryptering til.</li>
         <li>6. Undersøg periodevis routerens log for ikke-tilladte brugere.</li>
         <li>7. Brug en kraftig firewall.</li>
         <li>8. Beskyt din computer og vigtige dokumenter med password.</li>
         <li>9. Placer dit trådløse netværk på dets eget undernet.</li>
         <li>10. Sluk altid for trådløse kort og routere hvis de ikke bliver brugt.</li>
         </ul>

       </td>
       <td rowspan="2">

       </td>
      </tr>
```

```
      <tr>
       <td>

       </td>
      </tr>

      <tr>
       <td align="right">

       </td>
       <td align="left">

         <input type="submit" name="submit" value="Videre"
         style="width: 90px; height: 30px;" />

       </td>
      </tr>


    </table>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.49 wifi_18.php

```
<?php include("header.php"); ?>

  <? if ($_SESSION["xawareid"] == "") { ?>
  <script type="text/javascript"> window.location="index.php"</script>
  <? } ?>

  <script type="text/javascript">
   function validateResult()
   {
    if((document.wifi.wifi_1[0].checked == true) ||
       (document.wifi.wifi_1[1].checked == true) ||
       (document.wifi.wifi_1[2].checked == true))
    {
     getValue();
     return true;
    }
    else
    {
     alert("Der er ikke svaret på spørgsmålet! Vælg venligst en af svarmulighederne!");
     return false;
    }
   }

   function getValue()
   {
    var thisValue;
    thisValue = 0;

    if (document.wifi.wifi_1[0].checked)
     thisValue = 0;
    else if (document.wifi.wifi_1[1].checked)
     thisValue = 1;
    else if (document.wifi.wifi_1[2].checked)
     thisValue = 2;

    document.wifi.svar.value = thisValue;
   }
  </script>

  <title>XAware - Trådløs netværk</title>
 </head>
 <body onload="Tid();">
```

```
<? include ("menu.php") ?>

 <div id="box">
  <div id="content">
   <p><a href="default.php">Start side</a> > <b>Trådløs netværk</b></p>
   <h4>Trådløs netværk</h4>

   <table width="100%">
     <tr>
      <td align="left">
       <form name="wifi" method="post" action="wifi_handler.php"
       onsubmit="return validateResult();">
        <p><h5>18. Har du fået noget ud af dette spørgeskema?</h5></p>
        <input type="radio" name="wifi_1" value="0"> Ja
        <br>
        <input type="radio" name="wifi_1" value="1"> Nej
        <br>
        <input type="radio" name="wifi_1" value="2"> Ved ikke
        <input type="hidden" name="svar" value="">

      </td>
      <td rowspan="2">

      </td>
     </tr>
     <tr>
      <td>

        <? $_SESSION["wifiside"] = 18; ?>

      </td>
     </tr>

     <tr>
      <td align="right">

      </td>
      <td align="left">

        <input type="submit" name="submit" value="Videre"
        style="width: 90px; height: 30px;" />

      </td>
```

```
      </tr>


    </table>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.50 wifi_19.php

```
<?php include("header.php"); ?>

  <? if ($_SESSION["xawareid"] == "") { ?>
  <script type="text/javascript"> window.location="index.php"</script>
  <? } ?>

  <title>XAware - Trådløs netværk</title>
 </head>
 <body onload="Tid();">

 <? include ("menu.php") ?>

  <div id="box">
   <div id="content">
    <p><a href="default.php">Start side</a> > <b>Trådløs netværk</b></p>
    <h4>Trådløs netværk</h4>

    <table width="100%">
      <tr>
       <td align="left">
        <form id="wifi" method="post" action="wifi_db.php">
         <p><h5>19. Yderligere kommentarer, ris og ros?</h5></p>
         <textarea name="kritik" rows="5" cols="30">
         </textarea>
         <input type="hidden" name="svar" value="">
       </td>
       <td rowspan="2">

       </td>
      </tr>
      <tr>
       <td>


       </td>
      </tr>

      <tr>
       <td align="right">

       </td>
       <td align="left">
```

```
        <input type="submit" name="submit" value="Videre"
        style="width: 90px; height: 30px;" />

       </td>
      </tr>


    </table>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.51 wifi_db.php

```
<?php include("header.php"); ?>

 <title>XAware - IT sikkerhedsbevidsthed - Prøv de gratis spørgeskemaer</title>

 </head>
 <body onload="Tid()">

 <?php include ("menu.php") ?>

  <div id="box">
   <div id="content">
    <div id="sidetekst">
     <?php
      require_once ("functions.php");

      $result = wifiDB($_SESSION["xawareid"], $_SESSION["wifi_1"], $_SESSION["wifi_2"], $_SESSION["w

      if($result) //Ved success gå til afsluttende side
      {
       echo "<h2>Data indsat i DB!</h2>";
       ?>
       <script type="text/javascript"> window.location="wifi_end.php"</script>
       <?
      }
      else
      {
       echo "<h2>Fejl! Det er sket en fejl.";
       echo "<h2>Kontakt <a href=\"mailto:kenny.magnusson@gmail.com\">Webmasteren</a>".
       " om denne fejl og prøv lidt senere igen!";
      }

     ?>
    </div>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

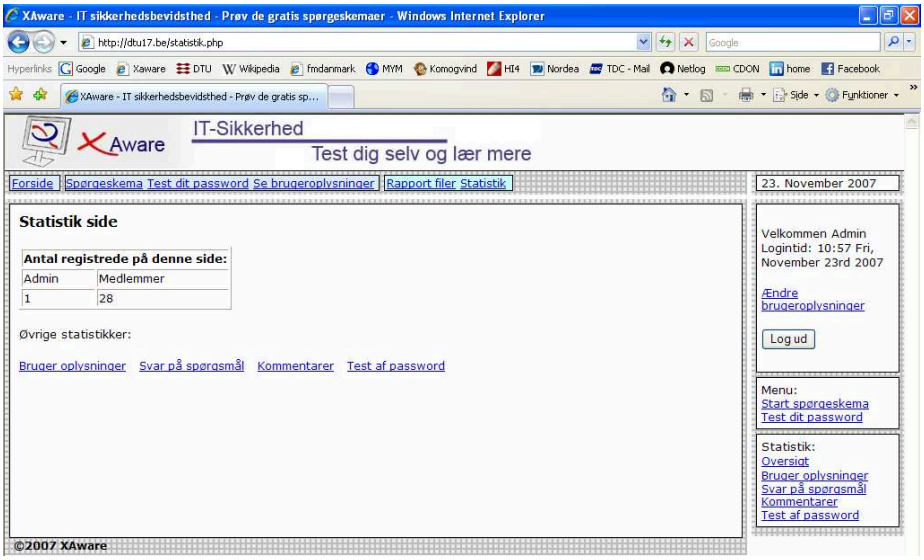
D.1.52 wifi_end.php

```
<?php include("header.php"); ?>

  <? if ($_SESSION["xawareid"] == "") { ?>
  <script type="text/javascript"> window.location="index.php"</script>
  <? } ?>

  <title>XAware - Trådløs netværk</title>
 </head>
 <body onload="Tid();">

 <? include ("menu.php") ?>

  <div id="box">
   <div id="content">
    <p><a href="default.php">Start side</a> > <b>Trådløs netværk</b></p>
    <h4>Trådløs netværk</h4>

    <table width="100%">
      <tr>
       <td align="left">
        <form id="wifi_end" method="post" action="default.php" >

         <p>Tak for din deltagelse!</p>
         <p> Håber det har været udbytterigt!</p>
         <br />
         <p>Prøv eventuelt at få testet hvor sikkert dit password til denne hjemmeside er. Klik på 'Tes
         <br />
         <br /><br />
         <p>Tryk på Afslut for at komme tilbage til startsiden</p>
       <td rowspan="2">

       </td>
      </tr>
      <tr>
       <td>



       </td>
      </tr>

      <tr>
```

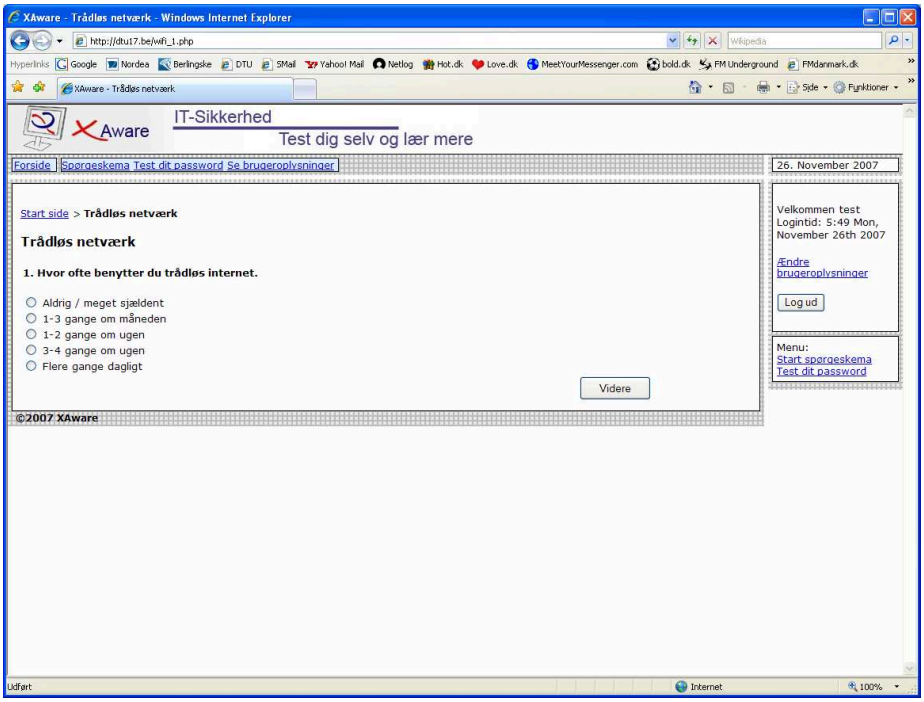
```
       <td align="right">


       </td>
       <td align="left">

         <input type="submit" name="submit" value="Afslut" style="width: 90px; height: 30px;" />

       </td>
      </tr>


    </table>
   </div>
   <div id="copy">&copy;2007 XAware</div>
  </div>
 </body>
</html>
```

D.1.53 wifi_handler.php

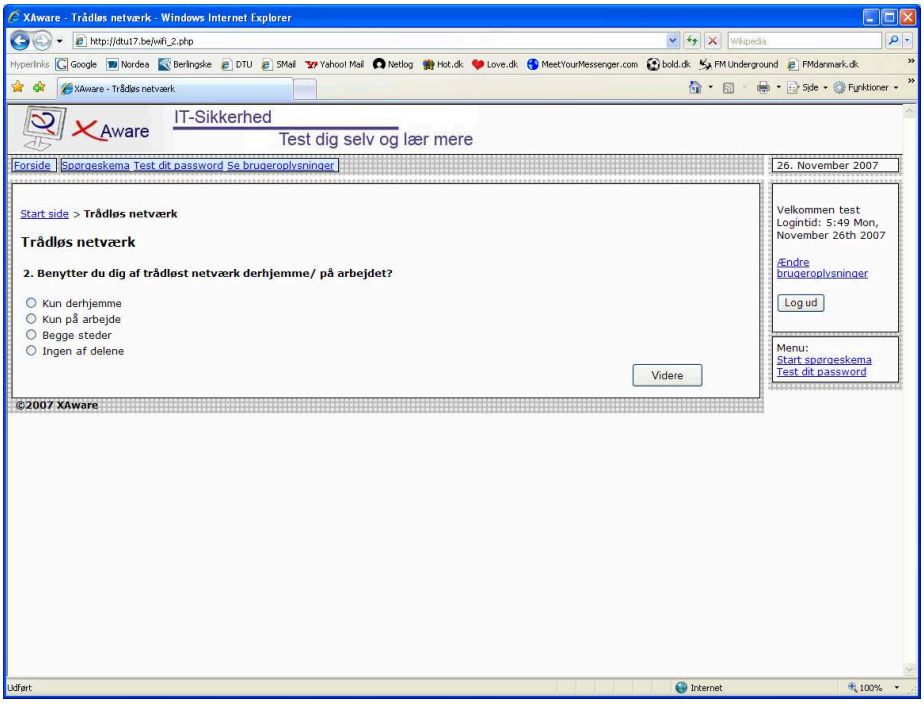
D.2 Skærmbilleder af XAware



Figur D.1: XAware forside

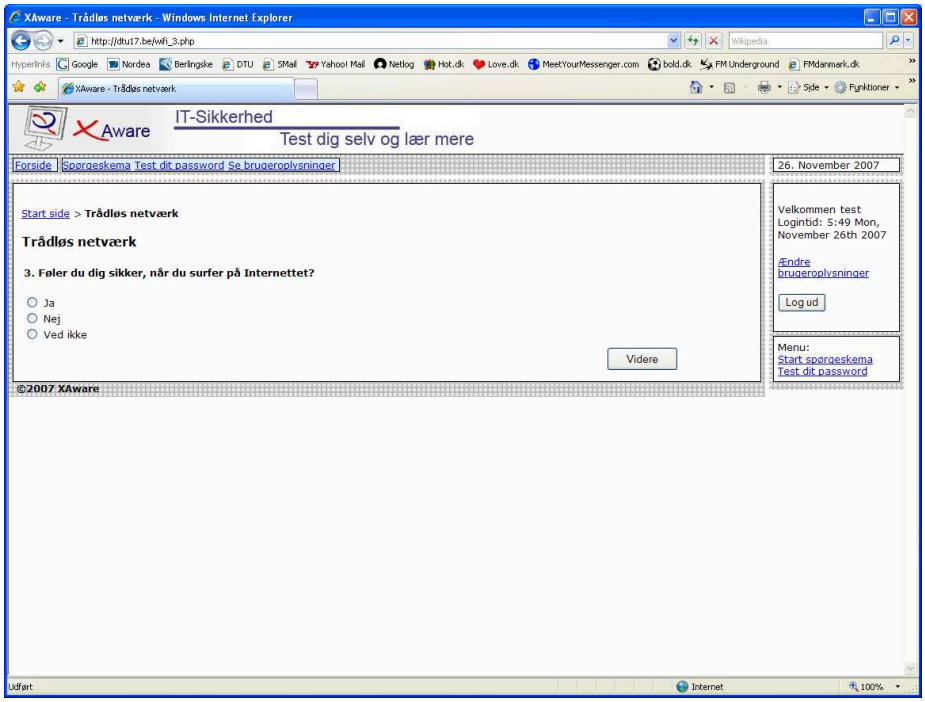


(a) Wifi1

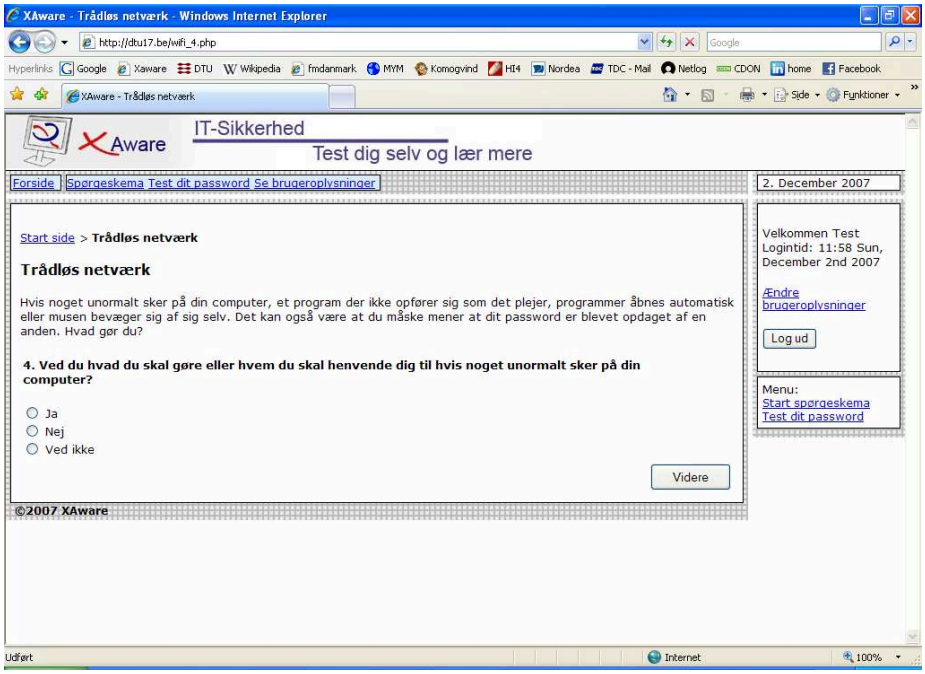


(b) Wifi2

Figur D.2: Trådløst netværk spørgeskema

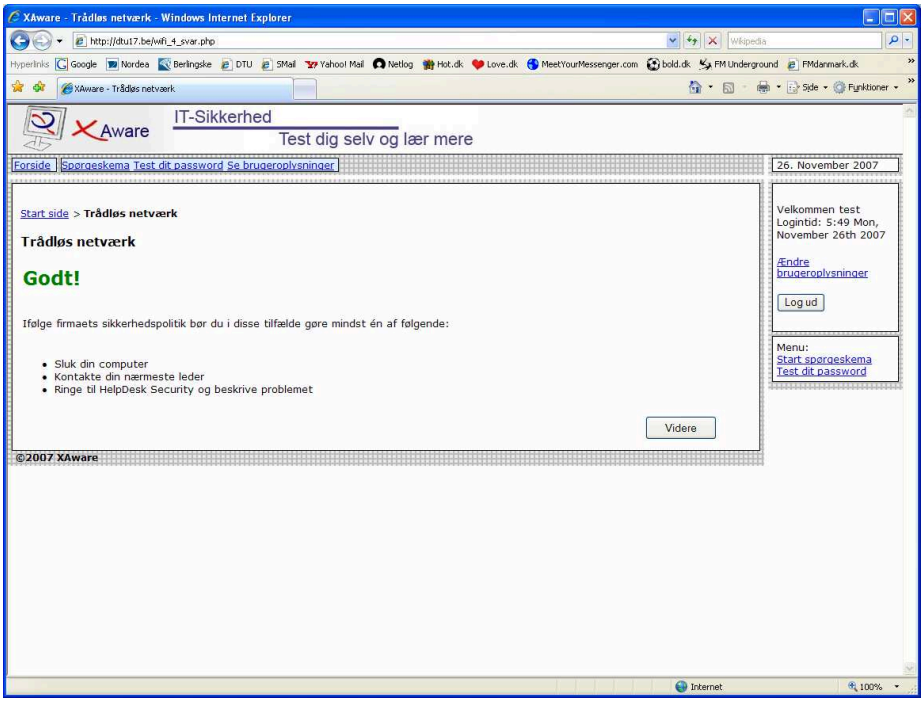


(a) Wifi3

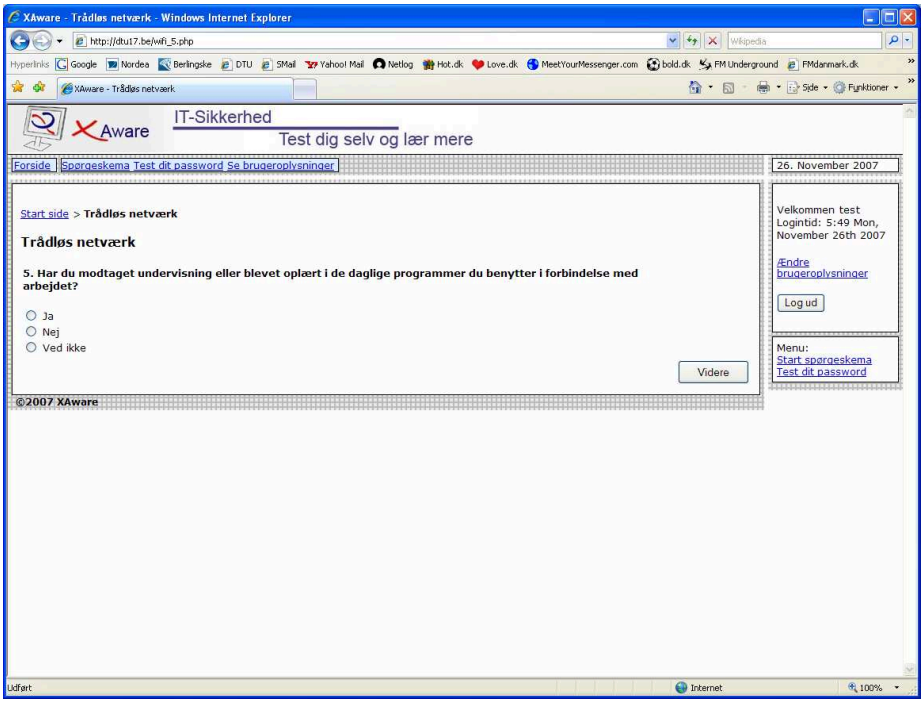


(b) Wifi4

Figur D.3: Trådløst netværk spørgeskema

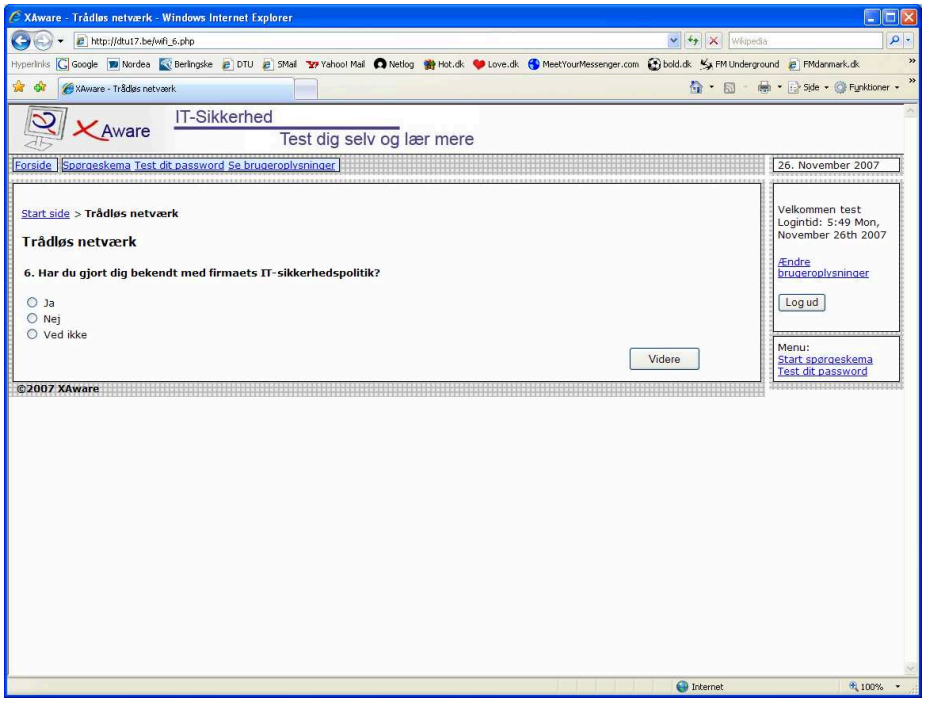


(a) Wifi4svar

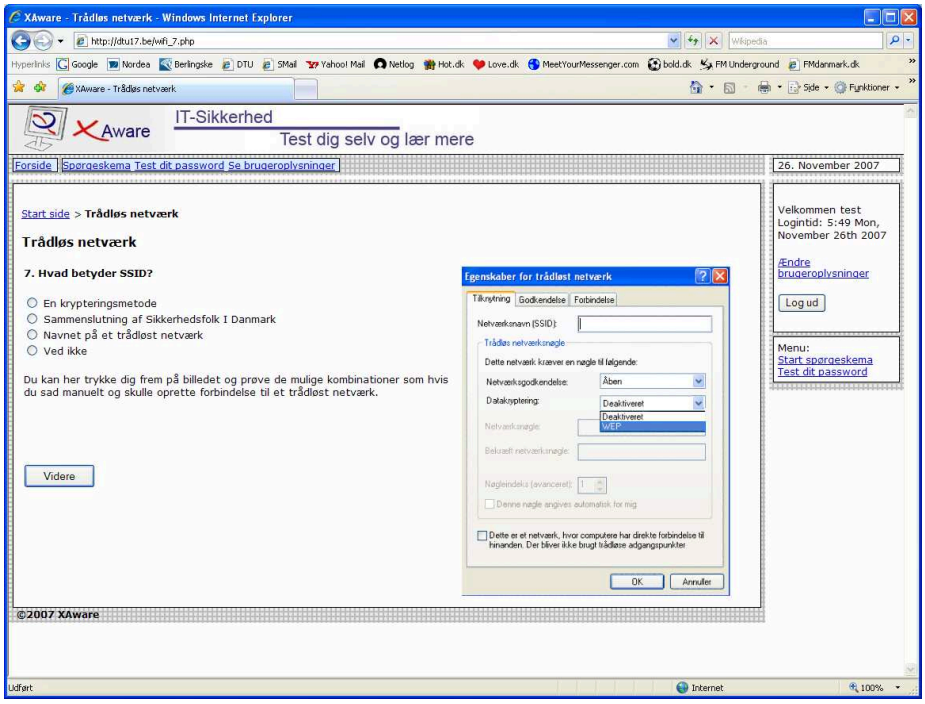


(b) Wifi5

Figur D.4: Trådløst netværk spørgeskema

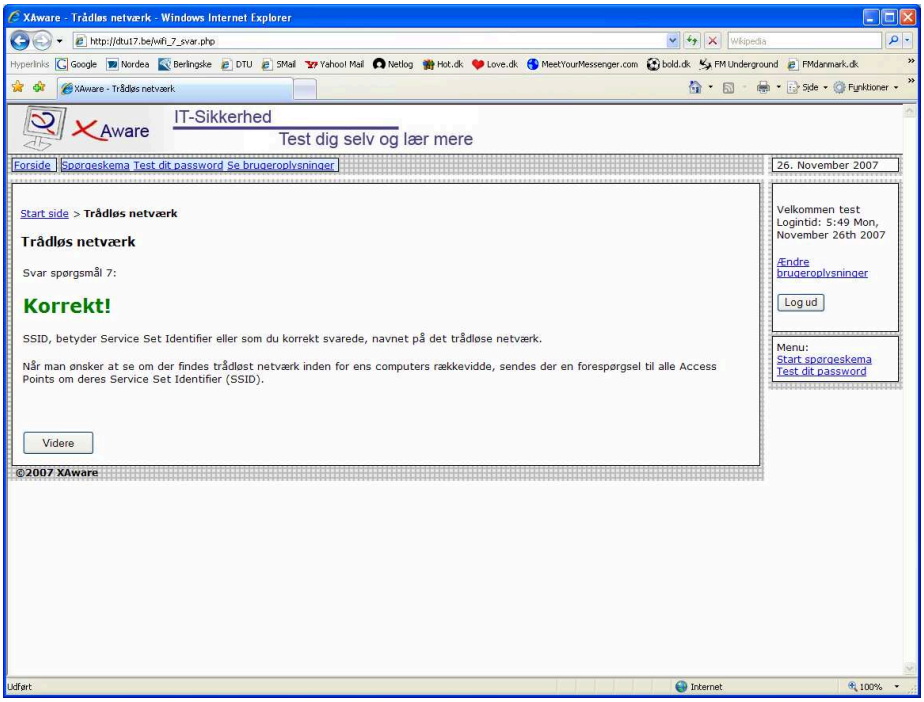


(a) Wifi6

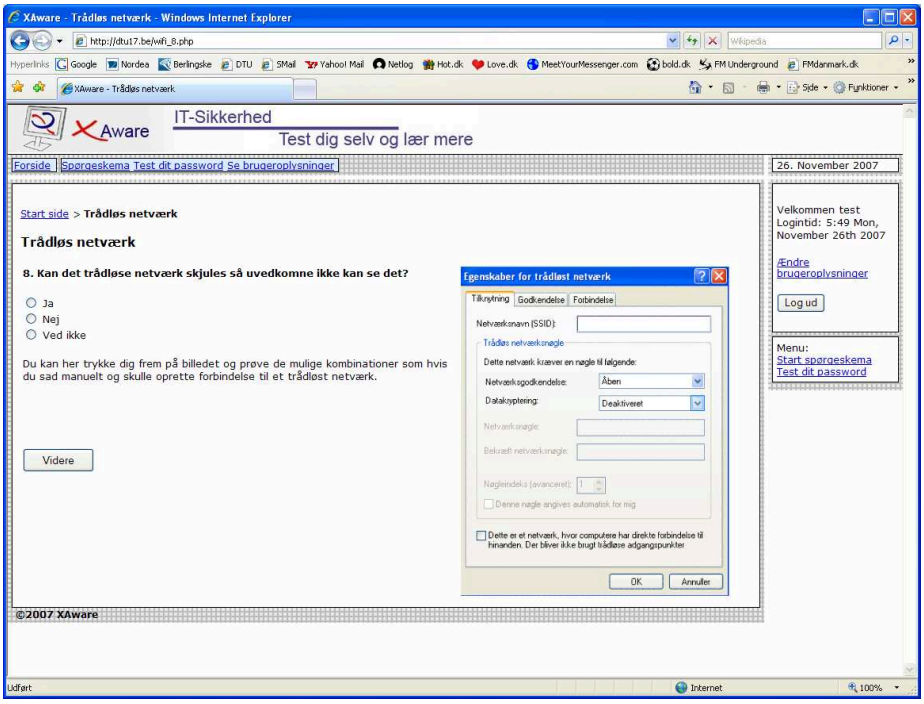


(b) Wifi7

Figur D.5: Trådløst netværk spørgeskema

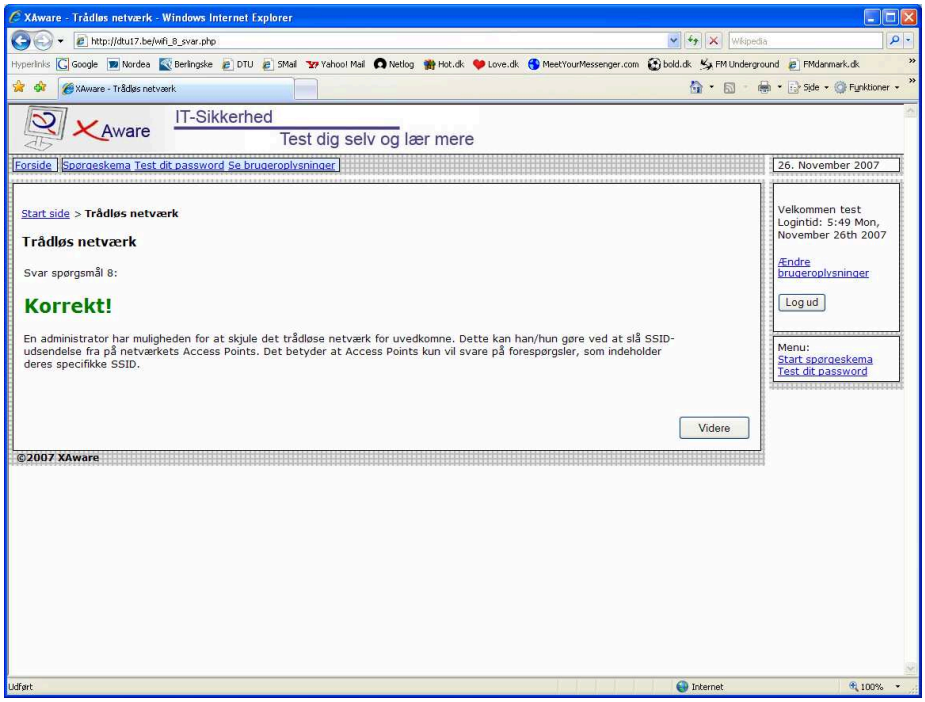


(a) Wifi7svar

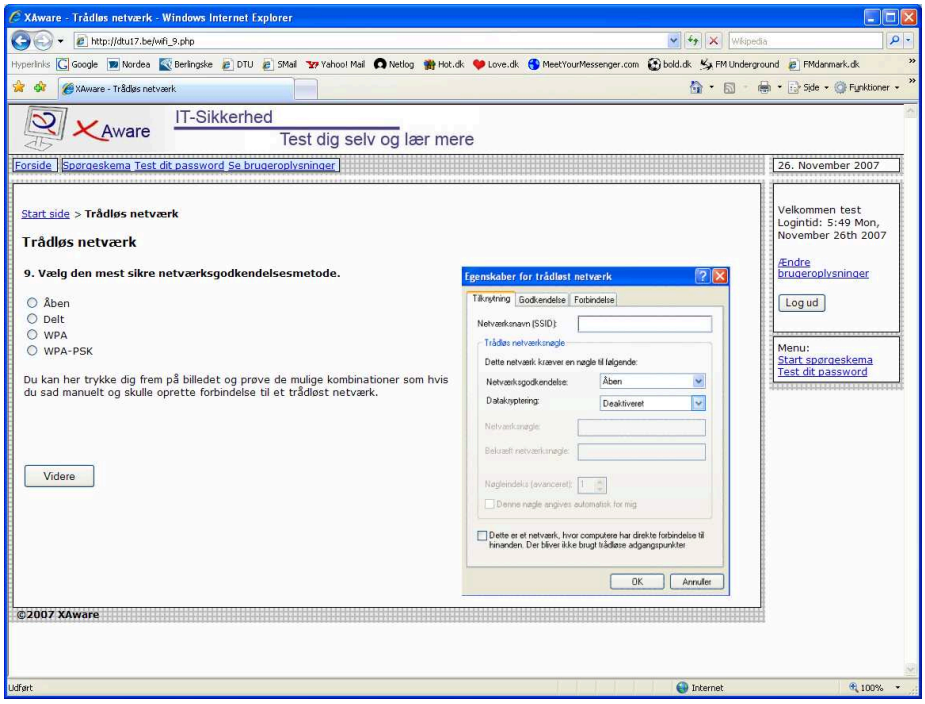


(b) Wifi8

Figur D.6: Trådløst netværk spørgeskema

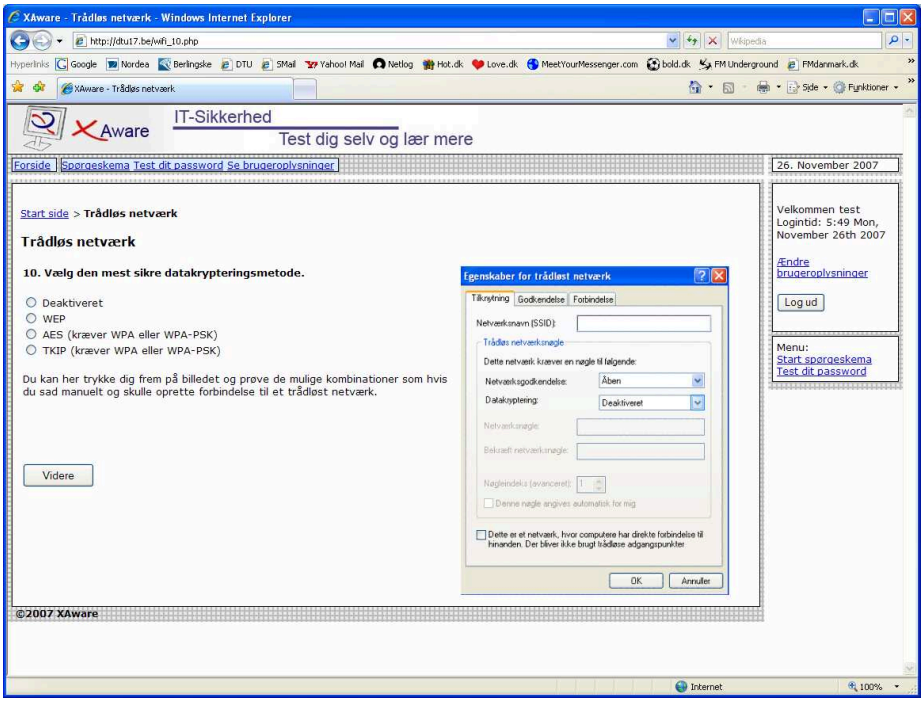


(a) Wifi8svar

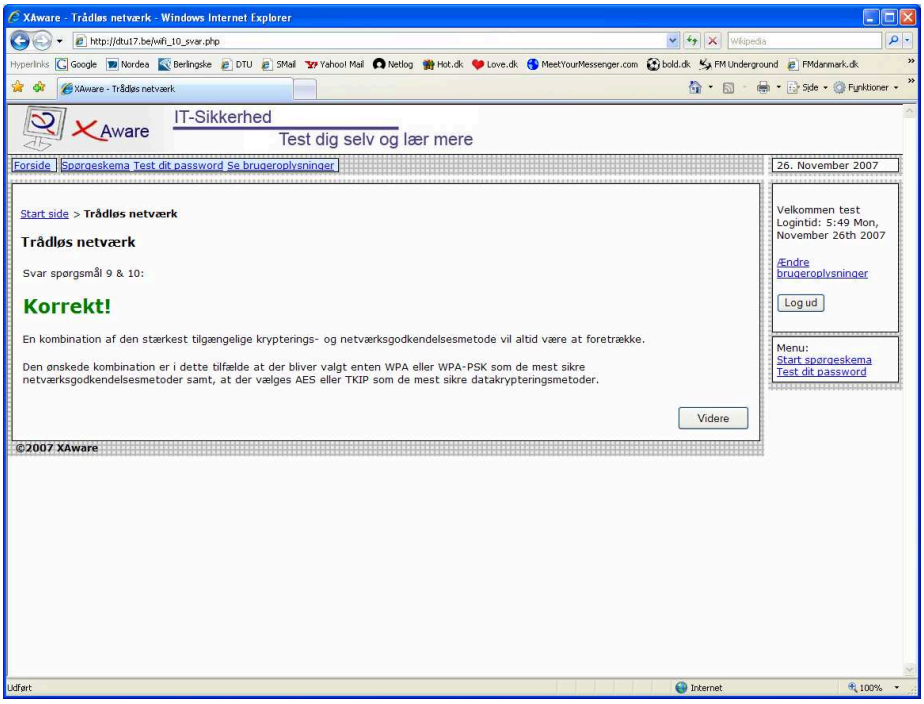


(b) Wifi9

Figur D.7: Trådløst netværk spørgeskema

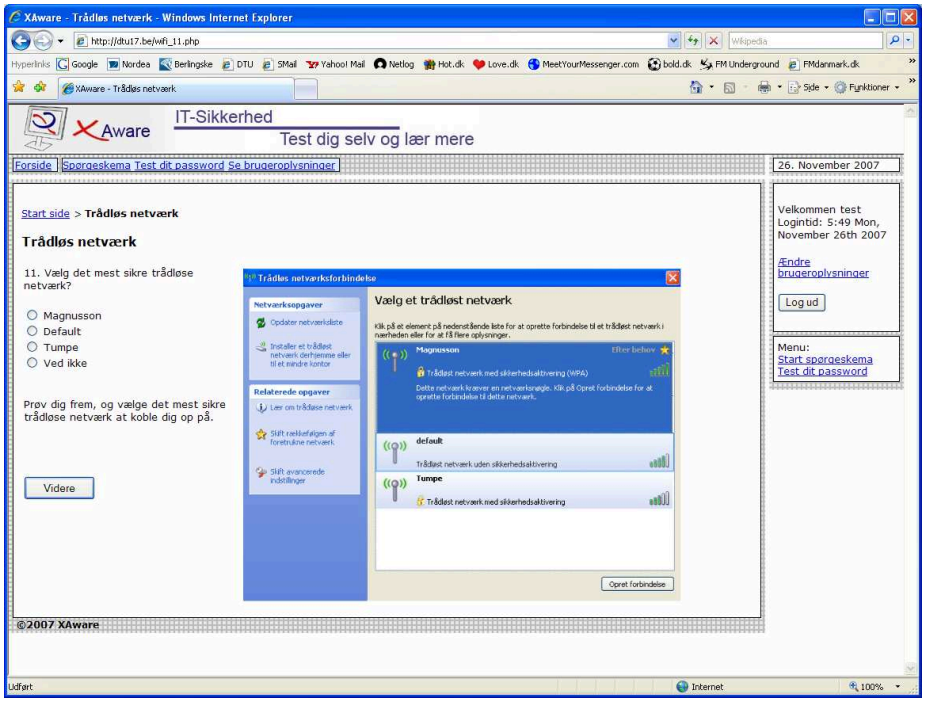


(a) Wifi10

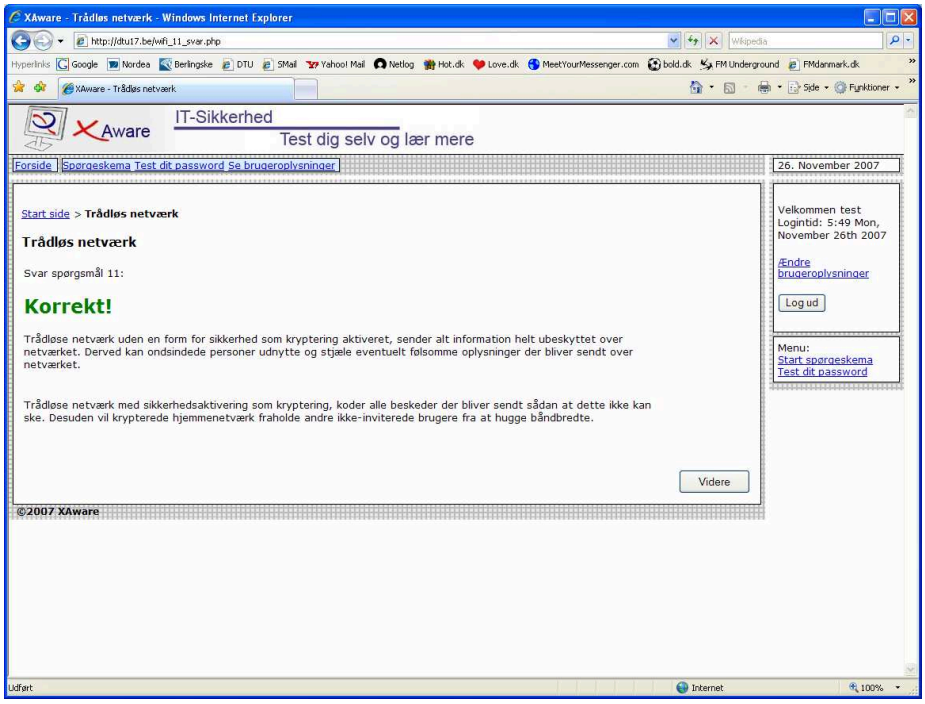


(b) Wifi10svar

Figur D.8: Trådløst netværk spørgeskema

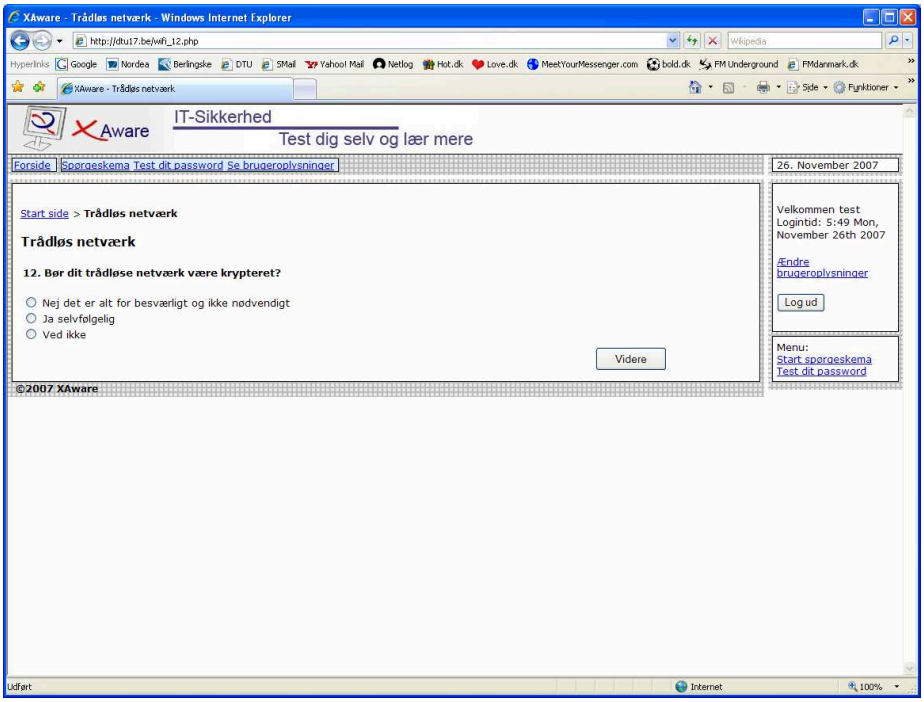


(a) Wifi11

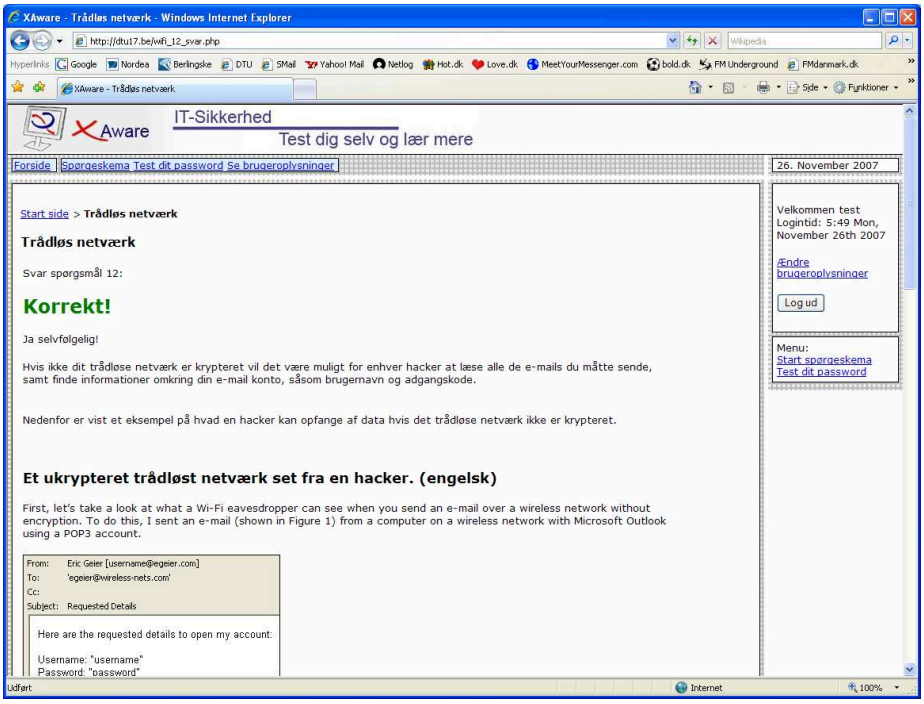


(b) Wifi11svar

Figur D.9: Trådløst netværk spørgeskema

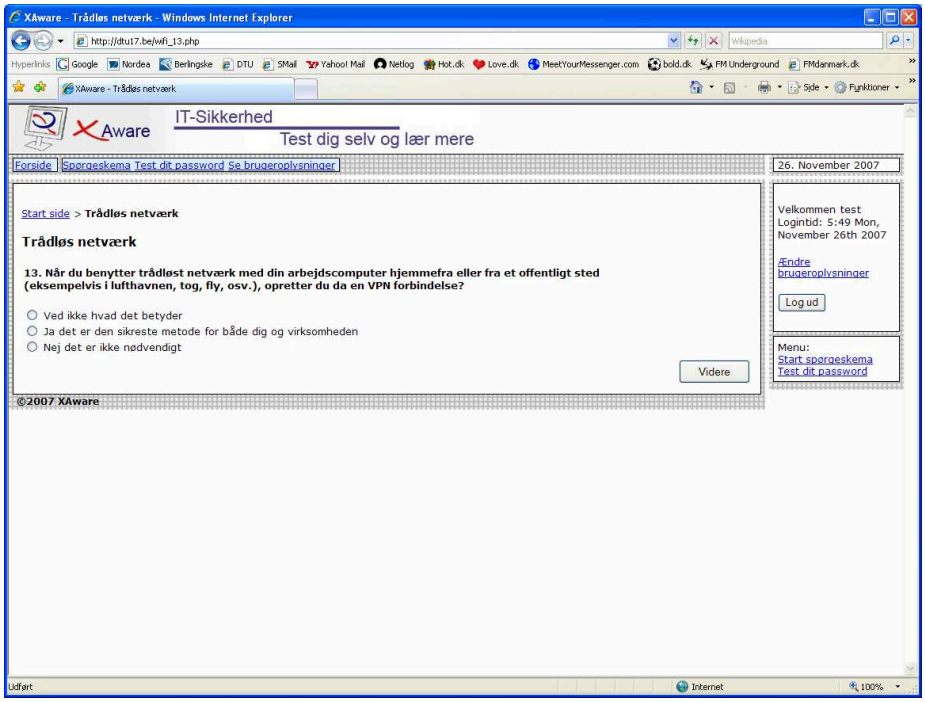


(a) Wifi12

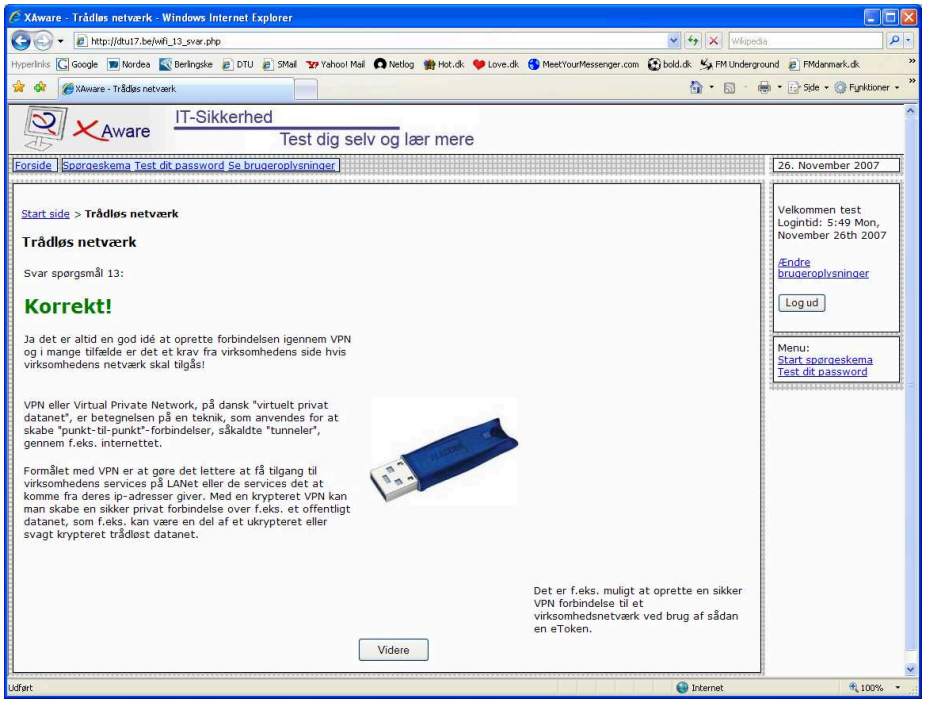


(b) Wifi12svar

Figur D.10: Trådløst netværk spørgeskema

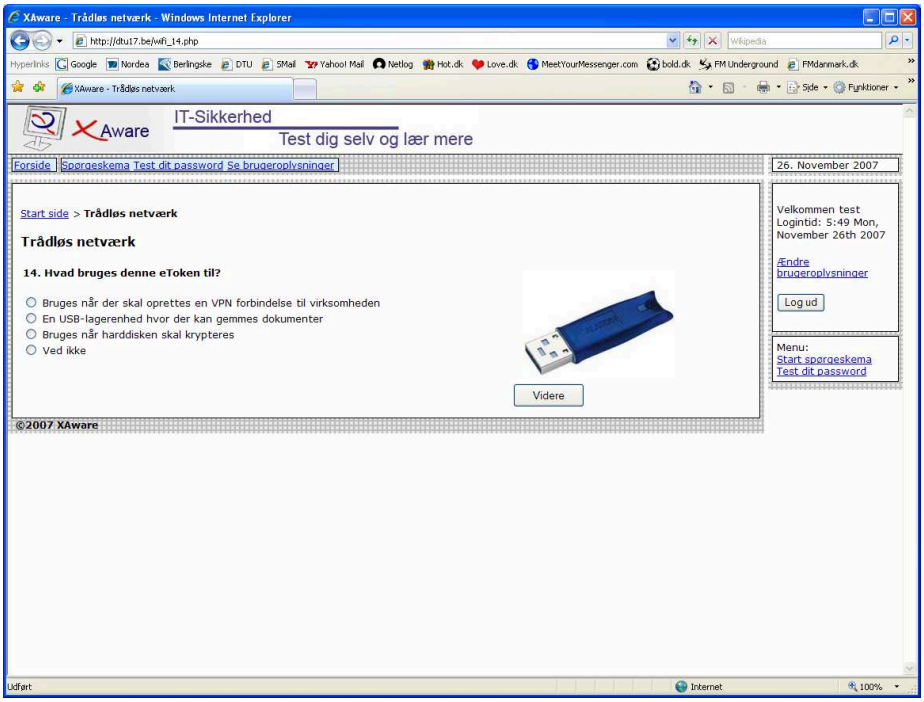


(a) Wifi13

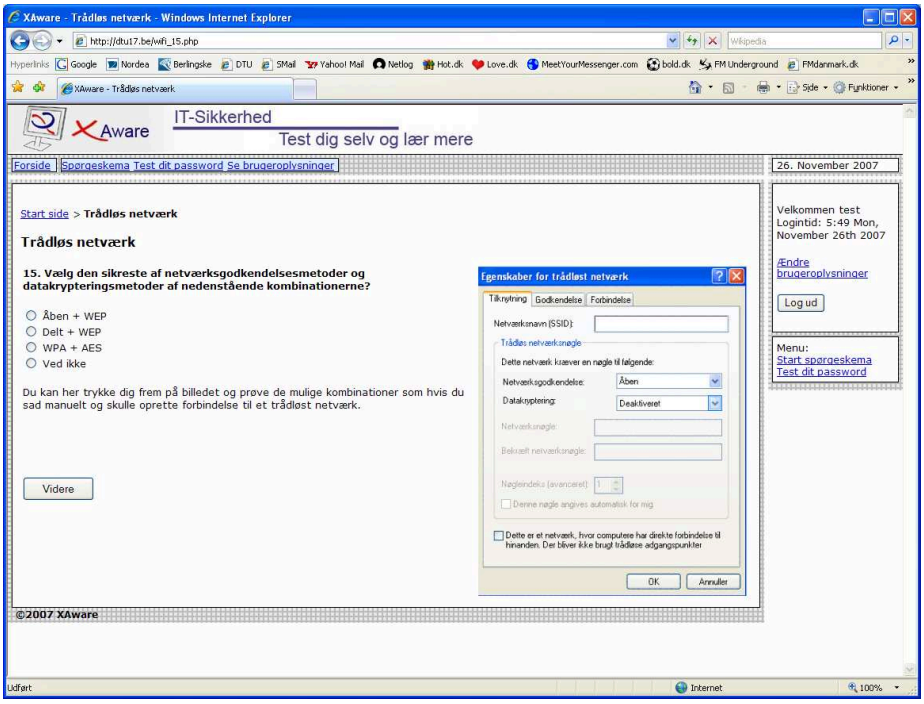


(b) Wifi13svar

Figur D.11: Trådløst netværk spørgeskema

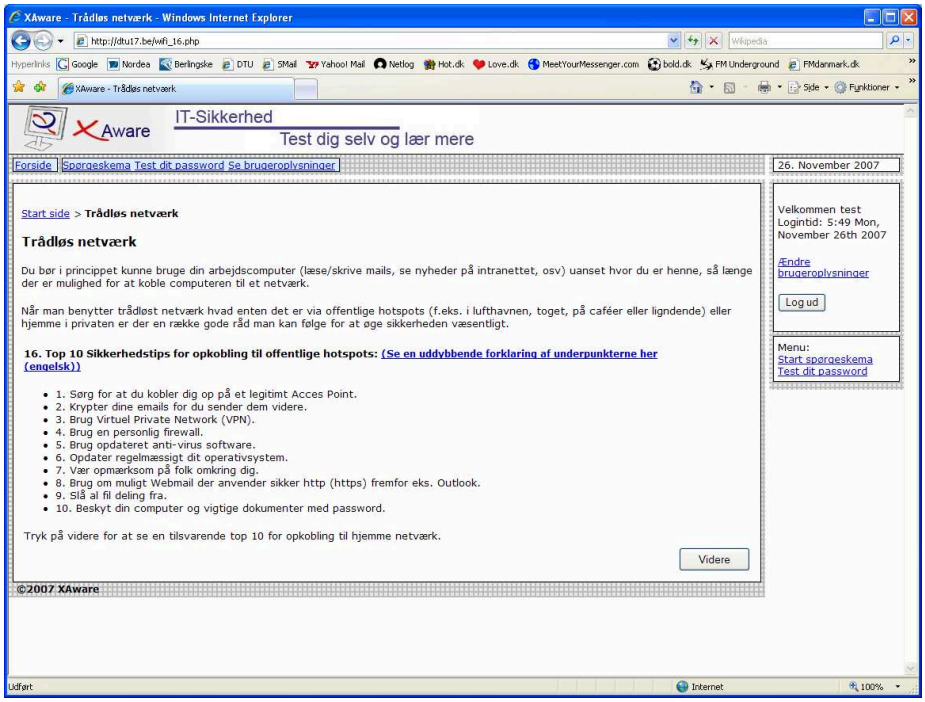


(a) Wifi14

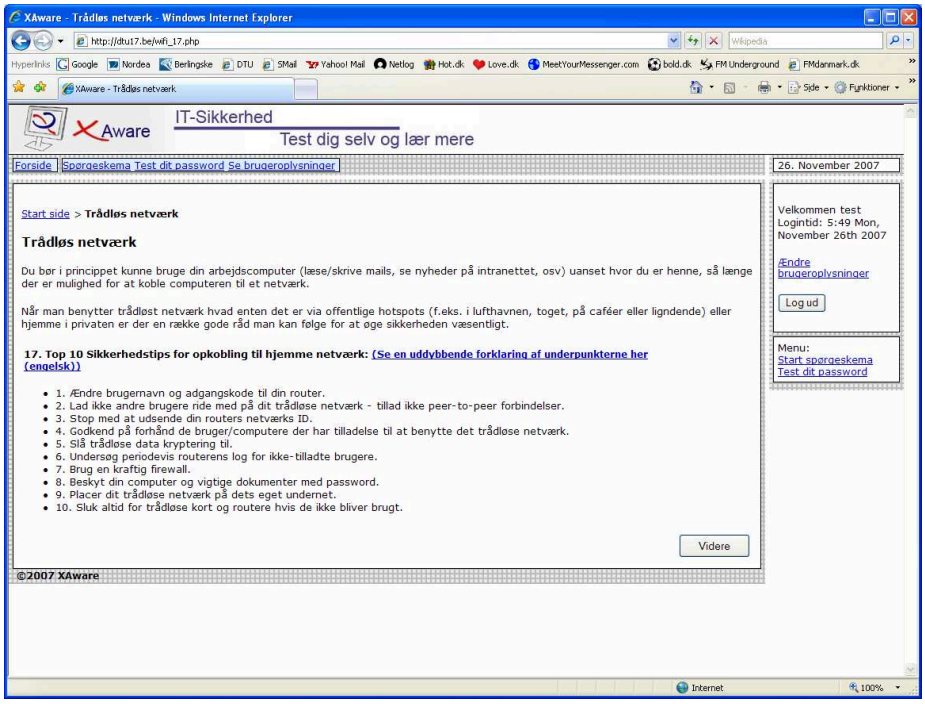


(b) Wifi15

Figur D.12: Trådløst netværk spørgeskema

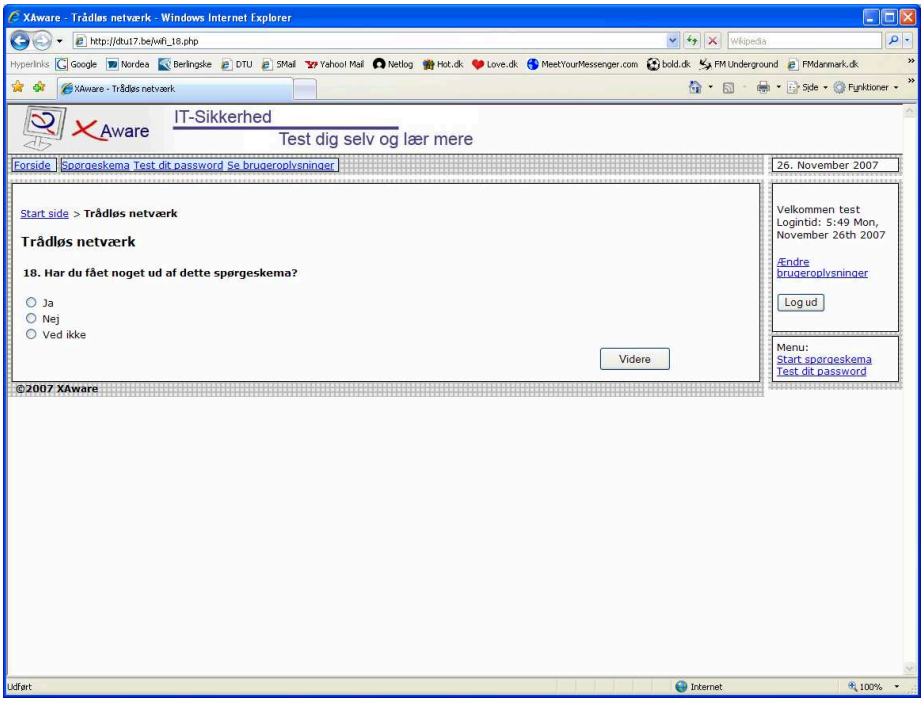


(a) Wifi16

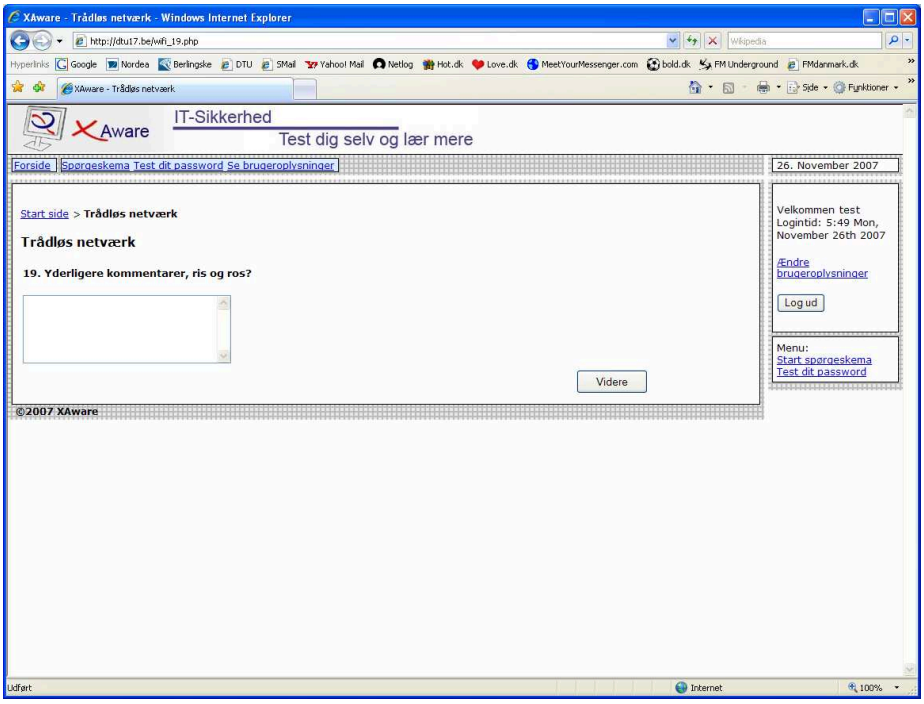


(b) Wifi17

Figur D.13: Trådløst netværk spørgeskema

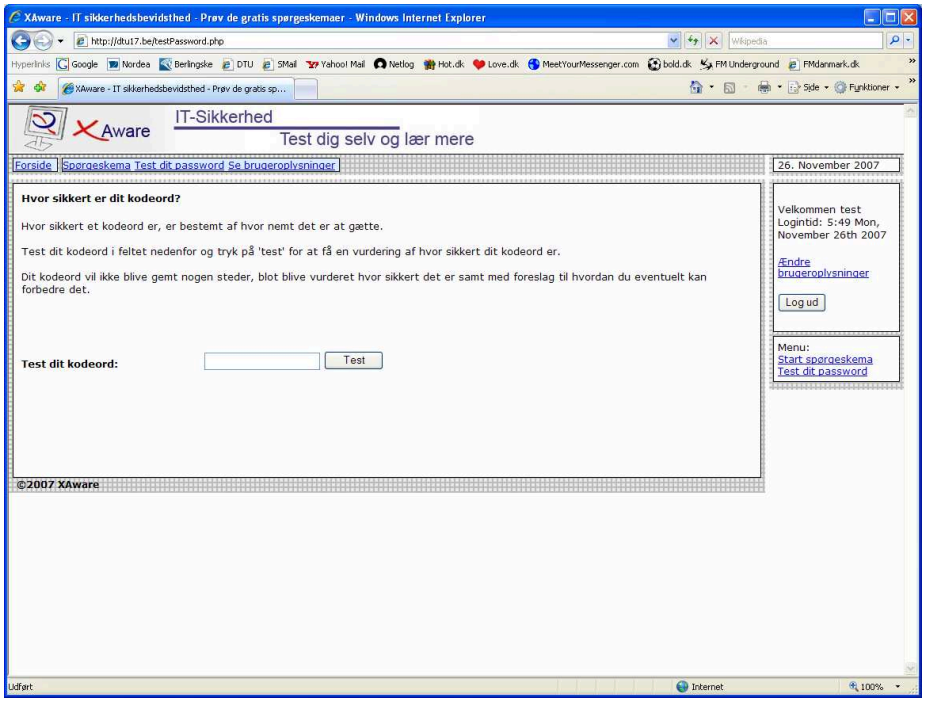


(a) Wifi18

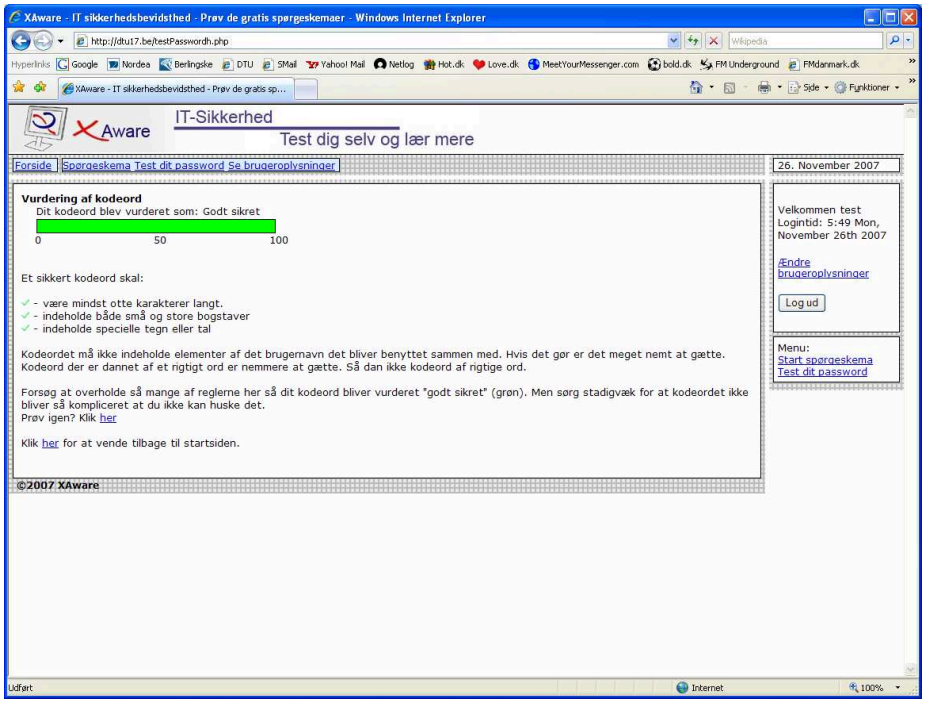


(b) Wifi19

Figur D.14: Trådløst netværk spørgeskema



(a) Test af kodeord



(b) Resultat

Figur D.15: Test af kodeord

Litteratur

[1] *SANS* - remote access policy. Fundet på World Wide Web, d. 11/11-2007: http://www.sans.org/resources/policies/Remote_Access_Policy.pdf.

[2] *SANS* - virtual private network (vpn) policy. Fundet på World Wide Web, d. 11/11-2007: http://www.sans.org/resources/policies/Virtual_Private_Network.pdf.

[3] NIST Special Publication 800-41. National institute of standards and technology - guidelines on firewalls and firewall policy, Januar 2002. Fundet på: http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf.

[4] NIST Special Publication 800-50. National institute of standards and technology - building an information technology security awareness and training program, Oktober 2003. Fundet på: http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.

[5] NIST Special Publication 800-77. National institute of standards and technology - guide to ipsec vpns, December 2005. Fundet på: http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf.

[6] Malcolm Allen. Social engineering - a means to violate a computer system, Juni 2006. Fundet på: http://www.sans.org/reading_room/whitepapers/engineering/.

[7] Theo Andersen. Animerede spørgeskemaer. Master's thesis, The Technical University of Denmark (DTU), Juli 2007.

[8] Siobhan Chapman. Toldmyndighed mister data på 25 millioner personer. 21. november 2007. Fundet på: http://www.computerworld.dk/art/42768?a=related\&i=42791.

[9] Shari Lawrence Pfleeger Charles P. Pfleeger. Security in computing, third edition, 2003. ISBN: 0-13-035548-8.

[10] DK-CERT. Gode rÅd om it-sikkerhed. 2005. Fundet på: https://www.cert.dk/vejled/10raad.shtml.

[11] NIST Special Publication 800-48 Revision 1 (Draft). National institute of standards and technology
- wireless network security for ieee 802.11a/b/g and bluetooth (draft), August 2007. Fundet på:
http://csrc.nist.gov/publications/drafts/800-48-rev1/Draft-SP800-48r1.pdf.

[12] ENISA. A users' guide: How to raise information security awareness, Juni 2006. Fundet på:
http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_a_users_guide%_how_to_raise_IS_awareness.pdf.

[13] David Gragg. A multi-level defense against social engineering, Oktober 2003. Fundet på:
http://www.sans.org/reading_room/whitepapers/engineering/.

[14] Anti-Phishing Working Group(APWG). Phishing activity trends - report for the month of july, 2007, Oktober 2007. Fundet på:
http://www.antiphishing.org/reports/apwg_report_july_2007.pdf.

[15] ISO/IEC. *ISO/IEC* 27001:2005 – information technology - security techniques - information security management systems - requirements, Oktober 2005.

[16] Ministeriet for Videnskabs Teknologi og Udvikling IT og Telestyrelsen. Checkliste for systemejerskab, December 2006. Fundet på:
http://it-sikkerhedsportalen.dk/portal/page/pr06/IT_SIKKERHED/Awareness/Checkliste%20for%20systemejere.pdf.

[17] Ministeriet for Videnskabs Teknologi og Udvikling IT og Telestyrelsen. Vejledning om uddannelse, træning og oplysning, Juni 2006. Fundet på:
http://it-sikkerhedsportalen.dk/portal/page/pr06/IT_SIKKERHED/Materiale%20og%20vaerktoejer/Vejledninger/Link%2

[18] Ministeriet for Videnskabs Teknologi og Udvikling IT og Telestyrelsen. Drejebog for ledelsesinvolvering, Januar 2007. Fundet på:
http://it-sikkerhedsportalen.dk/portal/page/pr06/IT_SIKKERHED/Awareness/Drejebog%20for%20ledelsesinvolvering.z

[19] IT-sikkerhedsportalen. It-sikkerhedsportalen. Fundet på:
http://www.it-sikkerhedsportalen.dk/portal/page/pr06/IT_SIKKERHED.

[20] Heather Kratt. The inside story: A disgruntled employee gets his revenge, December 2004. Fundet på:
http://www.sans.org/reading_room/whitepapers/engineering/.

[21] Pointsec. Enterprise encryption and access control for laptops and workstations, 2000. Fundet på:
http://www.securiteinfo.com/ebooks/pdf/pointsec_overview083100.pdf.

[22] Pointsec. Pointsec pc 4.3 - security target, st-version 1.08, Januar 2004. Fundet på:
http://www.dsd.gov.au/library/pdfdocs/EPL_Listings_ST_CRs/pc_security_pdf/PointSec/pointsecST.pdf.

[23] CSO Magazine PricewaterhouseCoopers, CIO Magazine. Global state of information security 2007, 2007. Fundet på: http://www.pwc.com/nz/security/pwc_GISS2007.pdf.

[24] Schlumberger. Virtual private networks solutions for remote access - comparison of ipsec and ssl, 2004. Fundet på: http://www.slb.com/media/services/software/whitepaper/whitepaper%_vpnsra.pdf.

[25] Robin Sharp. Principles of protocol design, 2004. Draft 2. edition, IMM Kgs. Lyngby.

[26] Dansk Standard. *DS* 484:2005 - dansk standard for informationssikkerhed, 2005.

[27] Wikipedia. Vpn. Fundet på: http://en.wikipedia.org/wiki/Vpn.

[28] Wikipedia. Vpn. Fundet på: http://da.wikipedia.org/wiki/Adware.

[29] Wikipedia. Vpn. Fundet på: http://da.wikipedia.org/wiki/Spyware.

[30] Aviel D. Rubin William R. Cheswick, Steven N. Bellovin. Firewalls and internet security - repelling the wily hacker, second edition, Feb 2003. ISBN: 0-201-63466-X.