Undersøgelse af datasikkerhed i forbindelse med hjemmearbejdspladser i Danmark

Søren Maigaard

Kgs. Lyngby 2003
IMM-THESIS-2003-41

Undersøgelse af datasikkerhed i forbindelse med hjemmearbejdspladser i Danmark

Søren Maigaard

Kgs. Lyngby 2003

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

IMM-THESIS: ISSN 1601-233X

FORORD

Dette projekt er udført som afsluttende eksamensprojekt på civilingeniørstudiet på Danmarks Tekniske Universitet. Projektet er udført ved instituttet Informatik og Matematisk Modellering, Computer Science & Engineering - Safe and Secure IT-systems under vejledning af Robin Sharp og Steen Pedersen.
Projektets omfang repræsenter 30 ECTS-point og er udført mellem februar og august 2003.

Jeg ønsker at takke mine vejledere Robin Sharp og Steen Pedersen for hjælpsomme inputs og for at hjælpe mig til at holde fast på nogle af de idéer, som var gode, men virkede uoverskuelige i starten.

Jeg ønsker desuden at takke Trent Berghofer fra Microsoft Nordic for at dele ud af sine erfaringer med sikring af hjemmearbejdspladser i en stor, international virksomhed.
Derudover en tak til de personer fra teleselskaber, leverandører og offentlige instanser som har bidraget med information om danske forhold i forbindelse med hjemmearbejdspladser.

Til sidst en stor tak til familie, venner og kæreste for gentagne gange at læse korrektur på rapporten.

_____

Søren Maigaard
s971519

ENGLISH ABSTRACT

The purpose of the project has been to explore the possibilities of creating secure home offices in Denmark. As a foundation for the project, a security policy for home offices has been created based on the international standard ISO 17799, and on information from large, Danish organizations. The security policy functions not only as a basis for the rest of the project, but also as a guideline for the extension of the existing security policies of Danish corporations.

Several security problems that arise from the implementation of home offices have been analyzed. This includes descriptions of attack patterns, and suggestions on how to mitigate these attacks. These descriptions provide the motivation and goal for the project – the design of a secure implementation of home offices for Danish corporations.

A number of relevant technologies for securing home offices have been analyzed. As an example, VPN and firewalls have been analyzed in order for them to be used later in the design proposal. The implementations from the Danish telecommunications companies have also been analyzed. In this analysis, the focus has been on security and the ability to segment the home networks in an attempt to prevent private computers from posing an increased security risk.
Relevant laws, recommendations, best practices and standards have been reviewed in order to collect a number of requirements to be met by the design proposal. Information has been collected from, amongst others, "persondataloven" (law concerning personal data), "terrorloven" (anti-terror law), the "Ministry of Science, Technology and Innovation" and from standards such as DS 484.

The collection of this information has resulted in a design proposal which considers the home office computer in itself, the infrastructure in the home and the requirements for the corporate network. The design proposal solves the security problems described earlier in the report while maintaining focus on user friendliness to keep the home offices a positive experience for the users.
It is concluded that this project has resulted in a design proposal which can be used by Danish corporations and organizations as a foundation for their own implementations of home offices. CyberCity can, as the only Danish telecommunications company, deliver a combined solution which can replace the implementation in the homes otherwise carried out by the corporation.

Suggestions for further work are included such as writing an easier accessible booklet for Danish network administrators, and continued work on the model to ensure less dependency on the expertise of the network designers. Furthermore it is suggested that an implementation of the design and an analysis of the problems of including mobile devices be carried out.

RESUMÉ

Projektets formål har været at undersøge mulighederne for at etablere sikre hjemmearbejdspladser i Danmark. Som udgangspunkt for projektet er der udarbejdet en sikkerhedspolitik for hjemmearbejdspladser, baseret på den internationale standard ISO 17799 samt informationer fra større, danske organisationer. Sikkerhedspolitikken fungerer både som udgangspunkt for projektets videre forløb samt eventuelt som skabelon for danske virksomheders udvidelse af deres eksisterende sikkerhedspolitikker.

En række sikkerhedsproblemer, som implementeringen af hjemmearbejdspladser kan medføre, er gennemgået. Således er mange angrebstyper beskrevet og kommenteret, ligesom forslag til metoder til at forhindre disse er givet. Dermed er der også skabt motivation for projektets mål – at udarbejde et designforslag for en sikker implementering af hjemmearbejdspladser i en dansk virksomhed.

Adskillige relevante teknologier til sikring af hjemmearbejdspladser er blevet gennemgået. Således er fx VPN og firewalls gennemgået, så disse teknologier senere kan benyttes i designforslaget. Desuden er de danske teleselskabers løsninger blevet analyseret. Her er der lagt vægt på sikkerheden og muligheden for at kunne segmentere hjemmets netværk så eventuelle private computere ikke udgør en øget sikkerhedsrisiko.
De mest relevante love, anbefalinger, best practices og standarder er herefter blevet gennemgået, for at samle en række krav, som tilsammen danner grundlaget for udarbejdelsen af designforslaget. Således er der samlet information fra bl.a. persondataloven og terrorloven, fra Ministeriet for Videnskab, Teknologi og Udvikling samt fra standarder som DS 484.

Opsamlingen af disse informationer har resulteret i et designforslag, som inkluderer både hjemmearbejdspladsen i sig selv, infrastrukturen i hjemmet samt de krav, som stilles til virksomhedens netværk. Designforslaget løser de sikkerhedsproblemer, som rapporten tidligere har omtalt samt sikrer, at brugervenligheden holdes i fokus, så brugen af hjemmearbejdspladserne bliver en positiv oplevelse for brugerne.
Det konkluderes, at projektet har resulteret i et designforslag, som kan benyttes af danske virksomheder og organisationer som et udgangspunkt for deres egen implementering af hjemmearbejdspladser. CyberCity kan som det eneste, danske teleselskab levere en samlet løsning, som kan erstatte den implementering, virksomheden ellers skulle foretage i hjemmene.

Der gives forslag til videre arbejde med projektet. Således kan en lettere tilgængelig håndbog udfærdiges til danske administratorer, ligesom der kan arbejdes videre med en model, som skal sikre mindre afhængighed af den ekspertise, netværksdesigneren besidder. Desuden foreslås udvidelser til designet, et forsøg med implementering samt en analyse af problemstillingen ved brug af mobile enheder.

LÆSEVEJLEDNING

Rapporten kan overordnet opdeles i tre hoveddele: udarbejdelsen af en sikkerhedspolitik i kapitel 2, et litteraturstudie i kapitlerne 3, 4 og 5 samt en analysedel fra kapitel 6 og frem.

Rapporten er opdelt i kapitler med tilhørende underafsnit. Kapitel 1 indeholder projektets problemformulering, afgrænsning og en beskrivelse af arbejdsprocessen.
I kapitel 2 udfærdiges på baggrund af materiale fra danske og internationale virksomheder og organisationer en sikkerhedspolitik, som alene omhandler hjemmearbejdspladser. Sikkerhedspolitikken er forsøgt gjort så generel, at den kan integreres i en dansk virksomheds eksisterende sikkerhedspolitik.
Kapitel 3 beskriver nogle af de sikkerhedsproblemer, som hjemmearbejdspladser er udsat for. Desuden beskrives, hvordan disse problemer kan udnyttes i angrebseksempler, ligesom der gives forslag til, hvordan sikkerhedsproblemerne kan afhjælpes. Afsnittet fungerer desuden som motivation for, at sikkerhedsproblematikken i forbindelse med hjemmearbejdspladser bør tages særdeles alvorligt.
Kapitel 4 gennemgår på baggrund af de foregående afsnit de pakkeløsninger, som de danske teleselskaber tilbyder virksomheder til udrulning af hjemmearbejdspladser. Det forsøges undersøgt i hvilken grad teleselskaberne leverer en sikker løsning og hvor vidt denne kan integreres i en virksomheds eksisterende netværk.
I kapitel 5 bliver der gået mere i dybden med et udvalg af de mest udbredte teknologier, som kan benyttes til at sikre hjemmearbejdspladserne og virksomhedernes netværk. Disse teknologier vil senere blive benyttet til at udfærdige et designforslag til implementeringen af sikre hjemmearbejdspladser i en dansk virksomhed.
I kapitel 6 findes en samling af de i Danmark mest relevante lovgivninger, standarder, anbefalinger og best practices i forbindelse med hjemmearbejdspladser. Disse benyttes til – sammen med sikkerhedspolitikken, teleselskabernes løsninger samt de i kapitel 5 gennemgåede teknologier – at udfærdige en opsamling af de krav, som skal danne grundlag for det ønskede design.
Designet udfærdiges i kapitel 7, som ud over en grafisk præsentation af designforslaget indeholder en beskrivelse af den valgte modulopbygning. En vurdering af dette designforslag foretages i kapitel 8.
Projektets konklusion findes i kapitel 9. Herefter afsluttes rapporten med en perspektivering i kapitel 10, hvor der gives konkrete forslag til, hvordan arbejdet kan videreføres.

Mange af de fagudtryk og forkortelser, som benyttes, er forklaret i ordbogen, der er at finde sidst i rapporten. Når betegnelsen lag benyttes i forbindelse med netværk, henvises til OSI-modellen hvis ikke andet er nævnt.

I rapporten benyttes opløftede tal ([5]) som henvisninger til fodnoter, som vises nederst på den aktuelle side. Tal i kantede parenteser [5] er henvisninger til litteraturlisten.

Rapporten inkluderer desuden en CD-ROM, som indeholder både rapporten samt en samling log-filer, der henvises til, de relevante steder i rapporten.

God læselyst!

INDHOLDSFORTEGNELSE

FIGUROVERSIGT

1 INDLEDNING

Denne afhandling er en opsummering og beskrivelse af resultaterne fra seks måneders arbejde med sikring af hjemmearbejdspladser.
En hjemmearbejdsplads er i dette projekt defineret som en enhed placeret i hjemmet med opkobling til virksomhedens netværk og mulighed for at benytte de applikationer, informationer og ressourcer, som er nødvendige for effektivt at kunne arbejde fra hjemmet. Der er ikke krav om, at enheden er en PC, Mac, tynd klient eller bærbar enhed – blot er der tale om enheder, som alene tilsluttes netværket fra hjemmet.

Hjemmearbejdspladser kan øge medarbejdernes frihed og fleksibilitet. Samtidig kan de medføre øget produktivitet og dermed være en gevinst for både arbejdsgiveren og medarbejderen. Dette er bl.a. baggrunden for, at 417.000 danskere arbejder helt eller delvist fra hjemmet [101].
Ifølge Teknologisk Institut mener 83 % af adspurgte, danske ansatte, som benytter hjemmearbejdspladser, at hjemmearbejde øger deres performance [5]. Muligheden for at arbejde hjemmefra giver en frihed og muligheder for samvær med familien, som ellers ikke kan lade sig gøre. Samtidig opnår virksomheden fordele i form af mindre spildtid, øget effektivitet fra medarbejderne samt besparelser til lokaler mm.
Dog nævnes det bl.a. i diskussionsartiklen ”Teleworking in the UK” [4] at medarbejdere som arbejder hjemme kan blive holdt udenfor det sociale miljø og de uformelle møder. Samtidig kræver det motivation at holde sig i gang, ligesom det kan være svært at overbevise chefer og kolleger om, at man arbejder flittigt når man ikke er fysisk til stede. Derfor er hjemmearbejdspladser ikke nødvendigvis for alle. Men for de medarbejdere, som kan få glæde af ordningen, står virksomheden til at forbedre både fleksibiliteten og effektiviteten.

1.1 Problemformulering

En ny undersøgelse [3] viser, at mere end en tredjedel af alle finansielle institutioner er blevet hacket indenfor det forløbne år. To tredjedele af disse indbrud er sket fra eksterne arbejdsstationer. Sikkerhedsproblematikken ved hjemmearbejdspladser kan være så overvældende, at mange virksomheder vælger ikke at implementere muligheden på trods af ovennævnte fordele. Samtidig viser undersøgelser foretaget af Computer Economics, at computerkriminaliteten i verden vil vokse med mere end 230 % alene i år [6] hvorfor problemet må antages at eskalere de kommende år.

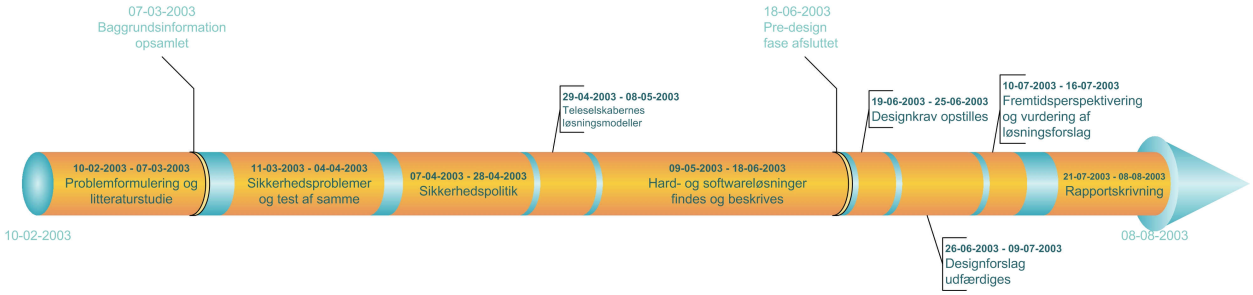
Det primære formål med IT-sikkerhed er at sikre virksomheders eller personers værdifulde aktiver. Dette indebærer tre fundamentale koncepter – konfidentialitet, integritet og tilgængelighed. Konfidentialitet skal sikre, at aktiverne ikke er tilgængelige for uautoriserede personer. Integritet skal sikre, at aktiverne kun kan modificeres af autoriserede personer og kun på autoriserede måder og til sidst skal tilgængelighed sikre, at aktiverne er tilgængelige for autoriserede personer.
I forbindelse med hjemmearbejdspladser er udfordringen at få enhederne i hjemmet beskyttet i lige så høj grad, som virksomhedens øvrige enheder. Da hjemmet sjældent er fysisk sikret på samme måde som virksomheden – og da et offentlige telenetværk benyttes til at overføre data – er det ikke let at etablere et sikkerhedsniveau, som kan fungere i et netværk med geografisk distribuerede enheder.
Det er denne problemstilling, der er baggrund for problemformuleringen for dette projekt:

Formålet med projektet er at undersøge mulighederne for at etablere sikre hjemmearbejdspladser i Danmark baseret på kendt teknologi og med brug af internettet som kommunikationsmedie mellem hjemmet og arbejdspladsen. Som et resultat af dette projekt skal opstilles et forslag til et løsningsdesign baseret på en udarbejdet sikkerhedspolitik.

1.2 Arbejdsproces

Projektet blev igangsat i februar 2003 og afsluttet i august samme år. I erkendelse, af at IT-sikkerhed er et stort område med utallige aspekter, har udgangspunktet for projektet været at afgrænse området for at levere et brugbart resultat som på en gang er omfangsrigt og fokuseret. Afgrænsningen er derfor sket for at analysen både blev grundig og brugbar for læsere på et højt teknisk niveau.

Efter fastsættelsen af projektets omfang og afgrænsninger – som dog enkelte gange i projektforløbet blev justeret efterhånden som ny viden blev tilgængelig – blev en tidsplan for projektet udfærdiget. Også denne er blevet justeret i løbet af projektet, idet nogle områder viste sig langt mere omfangsrige end andre ligesom nye områder kom til og andre fjernet efterhånden som overblikket over projektet blev bedre.
Nedenfor på figur 1 er vist en oversigt over denne tidsplan med tilhørende milepæle og hovedområder.



Figur 1 - Arbejdsprocessen

Som det ses har udgangspunktet for projektet været et litteraturstudie som kombineret med praktisk kendskab til og erfaring med IT-sikkerhed har dannet grundlaget for det videre forløb. Selvom det på figuren er vist, at litteraturstudiet er begrænset til projektets første uger har dette været en løbende proces, idet hvert nyt område har krævet en gennemgang af de relevante materialer.
Litteraturen og viden er hentet primært fra internettets mange portaler, diskussionsfora og artikler. Desuden har Danmarks Tekniske Videncenter (DTV) og adskillige bøger og artikler fra både danske og internationale forfattere leveret de nødvendige oplysninger. Den samlede litteraturliste kan ses bagest i rapporten.
Det skal i denne forbindelse nævnes, at mange af de kilder, som benyttes i projektet, kan være farvede af kommercielle interesser. Dette skyldes, at der i vidt omfang er benyttet white papers, manualer og teknisk dokumentation, som er skrevet af producenterne af det pågældende udstyr. Disse materialer er benyttet velvidende, at informationen er udarbejdet af personer indenfor samme virksomhed, som i sidste ende skal tjene penge på at sælge produkterne. Grunden til at materialerne alligevel er benyttet er, at meget af denne information ikke er tilgængelig på anden måde. Ideelt set ville alle disse informationer være leveret af uafhængige eksperter, men dette har desværre ikke været hverken tidsmæssigt eller ressourcemæssigt realistisk for dette projekt. For at kompensere så meget som muligt for dette, er det forsøgt enten at tage kontakt til leverandøren for at få opklaret eventuelle spørgsmål eller at finde information fra mere end en kilde.
Der knytter sig desuden nogle kommentarer til den måde, hvorpå information har været tilgængelig. Således har der været store problemer med at få virksomheder i tale, når det drejer sig om IT-sikkerhed. Mange virksomheder ønsker ikke at fortælle om deres interne strukturer, design og politikker, og specielt på dette sidste område – sikkerhedspolitik – har det været svært at få virksomhederne i tale. Offentlige instanser, som det har været forsøgt at få kontakt til, har med få undtagelser været langsomme til at behandle forespørgsler, hvilket har givet problemer med at få adgang til de relevante oplysninger i rette tid. Således har fx Rigspolitiet udvist stor interesse for at bidrage med informationer, men har efter to måneder endnu ikke leveret disse.
Selv producenterne har i visse tilfælde været tilbageholdende med at udlevere oplysninger når der er blevet gravet i, hvordan de grundlæggende design og konfigurationer af deres udstyr er opbygget. Således er der gået meget tid med at kommunikere med eksterne kontaktpersoner for at indsamle de nødvendige oplysninger. Dette har dog også været en spændende opgave, som har givet en god indsigt i den måde, virksomheder behandler information på.

Specifikt med hensyn til standarder for IT-sikkerhed (ISO 17799 samt Dansk Standard DS-484) har det været nødvendigt at basere både sikkerhedspolitikken samt andre dele af rapporten på ISO-standarden, idet den danske standard (DS 484) ikke har været tilgængelig før sidst i projektforløbet. Dansk Standard har ikke ønsket at udlevere en kopi af standarden og instituttet har ikke ønsket at indkøbe denne. Således har DTV i sidste øjeblik kunnet levere en kopi, som har gjort det muligt at inkludere de relevante hovedpunkter fra standarden.

Selve rapportskrivningen har foregået løbende under hele projektforløbet, samt koncentreret de sidste uger inden afleveringsdatoen. Desuden har der været ugentlige møder med vejlederne, hvor der er gjort status på projektforløbet samt diskuteret problemer og idéer. Specielt én problemstilling har været meget diskuteret ved disse møder. Det var oprindeligt et ønske at udvikle en metode eller model, så et netværksdesign ikke alene blev baseret på brugerens egen erfaring og ekspertise. Her har det dog vist sig, at en brugbar model til dette er så omfangsrig, at det ligger langt udenfor dette projekts rammer at udvikle den. Idéerne til modellen er dog præsenteret i perspektiveringsafsnittet og kan danne grundlaget for videre udvikling indenfor dette område.

2 SIKKERHEDSPOLITIK FOR HJEMMEARBEJDSPLADSER

En sikkerhedspolitik hjælper en virksomhed til at definere i hvilken grad og på hvilken måde udstyr, informationer og personer ønskes beskyttet. En sådan politik kan variere i størrelse fra en enkelt side til flere hundrede. Jo mere specifik politikken er, jo oftere skal den opdateres. Modsat, jo bredere politikken er formuleret, des flere krav stilles der til fortolkningen af den.
RFC 2196 [20] definerer en sikkerhedspolitik således:

"*A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide*"

Som udgangspunkt kan en sikkerhedspolitik baseres på enten reglen "tillad alt, som ikke forbydes" (som eksempel kan brugerne udføre enhver kommando på systemerne, som ikke specifikt er forbudt) eller "forbyd alt, som ikke tillades" (i samme eksempel kan brugerne kun udføre de kommandoer, som specifikt er tilladt). Begge regler kan bruges. Mens den førstnævnte er lettest at implementere, er den omvendt den sværeste at etablere sikkerhed omkring. Omvendt for den sidstnævnte.

En sikkerhedspolitik bør være uafhængig af specifikke hard- og softwareløsninger og i stedet basere sig på beskrivelser af, hvad virksomheden ønsker at opnå fra teknologien. På den måde begrænses politikken ikke, og nyudviklet udstyr og teknologier kan tages i brug uden at skulle ændre politikken hver gang en ny type udstyr kommer på markedet.

RFC 2196 skriver desuden om sikkerhedspolitikker, at:

"*[the purpose] is to provide a baseline from which to acquire, configure and audit computer systems and networks for compliance with the policy. Therefore an attempt to use a set of security tools in the absence of at least an implied security policy is meaningless.*"

Sikkerhedspolitikken er udgangspunktet for al videre sikkerhedsrelateret aktivitet. Den danner derfor også grundlag for denne rapport, og det kan undre, at kun halvdelen af de adspurgte virksomheder i en nylig undersøgelse [21] har endog en simpel sikkerhedspolitik.
Mange af de virksomheder, som det i løbet af projektet har været forsøgt at etablere samarbejde med, har afvist at udlevere deres sikkerhedspolitik. Samtidig har det været svært at få detaljer om, hvordan en sådan politik er blevet udfærdiget, implementeret og håndhævet. Enkelte virksomheder lever af at levere eksempler på færdige sikkerhedspolitikker, men disse giver ikke et godt billede af, hvordan en dansk sikkerhedspolitik om hjemmearbejdspladser kan udfærdiges. Et eksempel på et sådant firma er RUsecure.

En sikkerhedspolitik for hjemmearbejdspladser for en typisk, dansk virksomhed forsøges udarbejdet nedenfor. Dette er gjort for at give et eksempel på, hvordan en sådan politik kunne se ud. Sikkerhedspolitikken er forsøgt formuleret, så den så vidt muligt kan indlemmes i en virksomheds eksisterende sikkerhedspolitik.
Det antages, at virksomheden i forvejen har en sikkerhedspolitik som både dækker den såkaldte Acceptable Use Policy (AUP) som generelt beskriver hvordan brugerne bør opføre sig på netværket, men som også dækker det interne, eksterne og mellemliggende netværk, udstyr, informationer og personer.

Som baggrund for denne sikkerhedspolitik ligger materiale fra Forskningscenter Risø, Microsoft Nordic samt et større, unavngivet, dansk ministerium. Dette materiale består af anbefalinger, politikker og regler, som disse virksomheder har udarbejdet til internt brug. Materialet kan findes i litteraturlisten under [102], [103], [104], [105] samt [106]. Politikken dækker de tekniske minimumskrav hos både virksomheden og hjemmearbejdspladsen samt krav til brugeropførsel, overvågning og udstyrsbrug.
Hvor det har været muligt er der til sikkerhedspolitikken tilføjet referencer til relevante afsnit i ISO 17799-standarden fra 2000 ("Information technology – Code of practice for information security management") [83]. Denne standard giver anbefalinger omkring IT-sikkerhed både med hensyn til sikkerhedspolitik, design og implementering og er en meget anerkendt standardisering indenfor IT-sikkerhed. Referencer til standarden kan være relevant, idet uddybning eller fortolkning af sikkerhedspolitikken kan ske med baggrund i denne standard. Samtidig kan det af virksomheder benyttes til at argumentere for, at den egenudviklede sikkerhedspolitik har basis i en anerkendt standard. Referencerne er vist i tuborg-parenteser {}.
Visse dele af ISO 17799-standarden gennemgås desuden i afsnit 6.2.

2.1 Eksempel på en sikkerhedspolitik

Nedenfor følger et eksempel på en sikkerhedspolitik for hjemmearbejdspladser.

2.1.1 Definitioner og afgrænsninger

Med hjemmearbejdspladser forstås alle former for IT-arbejdspladser med fjernadgang til virksomhedens netværk.
Private hjemme-PC'er må ikke have opkobling til virksomhedens netværk og er derfor ikke omfattet.
Der differentieres ikke mellem hjemmearbejdspladser baseret på PC, Apple/Mac eller andre systemer, ligesom der ikke sondres mellem stationære og bærbare PC'er eller andre mobile enheder.

2.1.1.1 Formål

Brugerne skal så vidt muligt have adgang til det udstyr, software og andet materiale, som er nødvendigt for at kunne arbejde effektivt fra hjemmearbejdspladsen på en sikker og forsvarlig måde.
Opkoblingen til virksomheden fra hjemmearbejdspladsen skal i videst muligt omfang være transparent for brugeren, ligesom brugervenligheden af systemet i sin helhed har høj prioritet.

2.1.2 Sikkerhed

2.1.2.1 Brugermæssige sikkerhedsregler

Der gælder de samme regler omkring datasikkerhed, tavshedspligt og behandling af fortrolige eller personfølsomme oplysninger som er gældende ved normale arbejdspladser i virksomheden.
Idet de fysiske omgivelser i hjemmet ikke er beskyttet i samme grad som i virksomheden, skal medarbejderne udvise større opmærksomhed end normalt {7.2.5} ved specielt følgende:

- Computeren, som er stillet til rådighed i hjemmet, må aldrig efterlades i en tilstand, hvor den er forbundet til virksomhedens netværk {7.3.1.c samt 9.3.2.a+b}
- Brugeren må ikke nedskrive eller udskrive fortrolig information i hjemmet med det formål at gemme disse, herunder – men ikke begrænset til - logins og passwords {9.3.1.b}
- Hvis hjemmearbejdspladsen har tilsluttet en printer, må der ikke efterlades fortrolig information i denne, ligesom eventuel udskrevet information, som ikke skal benyttes, skal destrueres/makuleres {7.3.1.f samt 8.6.2.b}
- Hjemmearbejdspladsen må udelukkende anvendes til arbejdsrelaterede formål, samt i visse tilfælde til private formål som fx e-mails, så længe dette ikke konflikter med sikkerheden eller virksomhedens medarbejderpolitik
- Medarbejderen bærer ansvaret for, at hjemmearbejdspladsen til enhver tid anvendes på en sådan måde, at virksomhedens data sikres. Dette indebærer:
    - at følsomme data ikke må lagres lokalt, men kun på beskyttede, centrale servere i virksomheden {5.2.2}
    - at hjemmearbejdspladsen kun må benyttes af den pågældende medarbejder mens husstandens øvrige medlemmer er henvist til privat udstyr (som dog gerne må forbindes til den virksomhedsbetalte bredbåndslinie på en sikker og forsvarlig måde) {9.3.2.c}
    - at passwords ikke må gemmes i computeren, men skal tastes ved hvert login {9.3.1.g}
    - at login og password er personlige og ikke må videregives til andre {9.3.1.a}
    - at hjemmearbejdspladsen skal have nyeste opdateringer, service packs og anti-virus signaturer {8.3.1.c}

2.1.2.2 Tekniske sikkerhedsforanstaltninger

Følgende sikkerhedsforanstaltninger skal være gældende ved hjemmearbejdspladsen:

- Sikkerheden ved autentifikationen af forbindelsen til virksomhedens netværk må ikke alene være baseret på passwords {9.4.3 samt 9.5.3}
- Forbindelsen skal være beskyttet mod aflytning, genafspilning og ændring {9.4.9}
- Alle arbejdsstationer og brugere som kobles op mod virksomhedens netværk skal være unikt autentificeret. Routere og Network Address Translators (NATs) kan ikke alene udføre denne autentificering, da alle maskiner bag disse enheder dermed vil have uautentificeret adgang {9.5.1}
- Hjemmearbejdspladsen skal være beskyttet mod eksterne angreb med en enhed, som holdes centralt opdateret {9.8.2}
- Hjemmearbejdspladsen skal på bedst mulig måde sikres mod trojanske heste, keyloggers, virus og andre potentielle trusler {8.3.1}
- Hjemmearbejdspladsen skal holdes adskilt fra hjemmets private udstyr på bedst mulig måde {9.4.6}
- Det må ikke være muligt at installere software eller ændre på opsætningen af hjemmearbejdspladsen for andre end de netværksansvarlige i virksomheden {9.2.2.b}
- Hjemmearbejdspladsen skal så vidt muligt autentificeres før det er muligt at etablere forbindelse til virksomhedens netværk {9.4.4 samt 9.5.1}

For virksomhedens netværk skal følgende være gældende i forbindelse med etableringen af hjemmearbejdspladser:

- Autentificeringen af brugerne skal ske op mod en centraliseret valideringsdatabase, så synkroniseringen af brugerkonti er mulig {9.5.4}
- Passwords skal overholde regler for kompleksitet, længde og historik {9.3.1}
- Virksomhedens udstyr skal beskyttes mod angreb fra både eksterne, interne og hjemmearbejdsplads-brugere {9}
- Opkaldspunkterne må ikke fremstå som tydelige angrebsmål
- Hjemmearbejdspladsbrugernes adgang skal kunne begrænses til specifikke servere, serverparker, arbejdsstationer og lignende {9.6.1}
- En eller flere kompromitterede, offentlige maskiner må ikke kunne benyttes som base for yderligere angreb mod virksomheden eller hjemmearbejdspladsen {9.4.6}
- Trafikken til og fra hjemmearbejdspladsen skal være under virksomhedens kontrol og ikke kunne aflyttes af eksterne eller interne brugere {9.4.8}
- Aktiviteter foretaget fra en hjemmearbejdsplads skal kunne logges {9.7.2.1}
- Der må ikke kunne initieres forbindelse fra virksomheden til hjemmearbejdspladsen undtagen til administrative formål
- Suspekt aktivitet som fx etablering af forbindelse fra hjemmet mens medarbejderen befinder sig i virksomheden skal kunne overvåges og reageres på {9.7.2.3}

For infrastrukturen mellem hjemmet og virksomheden skal følgende være gældende:

- Det må ikke være muligt for 3. part at aflytte, genafspille eller ændre informationerne {8.5.1.c}
- Det må ikke være muligt at omdirigere trafikken

2.1.3 Øvrige forhold

2.1.3.1 IT-support

Som udgangspunkt ydes den samme support til hjemmearbejdspladser som til normale arbejdspladser. Enhver forespørgsel om support fra en hjemmearbejdsplads skal dog valideres ved at benytte dial-back til brugerens telefonnummer, ligesom brugeren skal identificeres ved hjælp af medarbejder-id-nummer.
Der må aldrig videregives fortrolig information over telefonen, e-mail eller andre usikre, elektroniske kommunikationsformer. Der skal derfor foreligge en grundig beskrivelse af, hvilke informationer, der, under supportopkald, må udleveres til medarbejdere, som ikke kan møde personligt op og fremvise billede-ID. {5.2.2}

2.1.3.2 Ansvar

Medarbejderen har ansvaret for, at sikkerheden omkring hjemmearbejdspladsen som beskrevet ovenfor overholdes, samt at eventuelle abnormaliteter, aktiviteter udenfor det normale samt fejl og mangler indrapporteres til de netværksansvarlige.
Det er ligeledes medarbejderens ansvar, at informere om stjålet eller tabt identifikationsmateriale, logins, passwords og dets lige.

Det er virksomhedsledelsens ansvar at sikre, at medarbejderen har læst og forstået sine forpligtelser samt at medarbejderen er informeret om de sikkerhedsmæssige aspekter i forbindelse med etableringen af hjemmearbejdspladsen.

Netværksafdelingen har ansvaret for, at udstyret hos både medarbejderen og i virksomheden fungerer tilfredsstillende samt at udstyret holdes løbende ved lige og opdateres, så det kan reflektere den maksimale sikkerhed, teknikken kan levere. Det er ligeledes netværksafdelingens ansvar, at reagere på suspekt aktivitet i loggen, samt at overvåge brugen af hjemmearbejdspladsens forbindelse til netværket. {4.1.3 samt 8.1.3}

3 HJEMMEARBEJDSPLADSERNES SIKKERHEDSPROBLEMER

Med implementeringen af hjemmearbejdspladser flytter virksomheden reelt den yderste forsvarsperimeter helt ud til hjemmene. Sikring af virksomhedens interne netværk fra internettet er ikke længere et problem som kan løses alene ved at se på virksomhedens forsvarsmekanismer.
En hjemmearbejdsplads bør betragtes som en enhed, der som udgangspunkt er ubeskyttet, har fast forbindelse til internettet og har direkte adgang til virksomhedens interne netværk. Umiddelbart det værst tænkelige scenarie, men med kendskab til de sikkerhedsproblemer implementeringen af hjemmearbejdspladser fører med sig, kan passende forsvarsmekanismer etableres. I dette kapitel gennemgås de mest udbredte sikkerhedsproblemer. Selvom mange af disse ikke er unikke for hjemmearbejdspladser, har hjemmearbejdspladserne medbragt nye aspekter af disse problemer, som bør overvejes.
Kapitlet fungerer således også som motivation for, at sikkerhedsproblematikken ved hjemmearbejdspladser bør tages alvorligt.

I visse tilfælde er det beskrevet, hvordan sikkerhedsproblemerne kan udnyttes, mens angrebene i andre tilfælde er udført i praksis. Disse angrebseksempler er indrammet og kræver i de fleste tilfælde, at læseren har kendskab til brugen og konfigurationen af forskelligt netværksudstyr. Hvert afsnit afsluttes med eksempler på, hvordan sikkerhedsproblemerne kan minimeres og på hvilke måder, hjemmearbejdspladserne kan sikres mod de gennemgåede angrebsmetoder.

Der er i Appendiks A angivet angrebstyper som retter sig mod data link laget og applikationslaget ligesom distributed denial-of-service (DDoS) angreb og netværksrekognoscering er beskrevet her. Disse angrebstyper er ligesom nedenstående relevante i forbindelse med implementeringen af hjemmearbejdspladser. De kræver dog et bedre kendskab til de anvendte teknologier. Besidder læseren ikke allerede denne viden, kan appendikset med fordel læses efter gennemgangen af teknologierne i kapitel 5.

Som tidligere nævnt vil der blive benyttet teknologier og udstyr i dette kapitel, som gennemgås senere i rapporten. I disse tilfælde er der indsat referencer til de relevante kapitler, hvor teknologierne gennemgås i detaljer ligesom ordbogen bagest i rapporten har forklaringer til de benyttede udtryk.

3.1 Aflytning

Aflytningen af netværkstrafik kan ske når dataene transporteres over et eller flere netværk hvor andre end afsender og modtager er tilkoblet. Dette vil næsten altid være tilfældet – både internt i virksomhedens LAN og eksternt på internettet. Der kan i så fald gøres brug af en såkaldt pakkesniffer, som fungerer ved at indstille netværkskortet i den enhed angriberen benytter til at operere i en såkaldt promiskuøs tilstand. I denne tilstand sender netkortet alle de netværkspakker der transmitteres på den del af netværket, kortet kan se, videre til en applikation (pakkesnifferen) i stedet for som normalt, at frasortere pakker, som ikke har en destinationsadresse der matcher netkortets.
Pakkesniffere benyttes normalt i forbindelse med fejlfinding på et netværk hvor opsamlingen af netværkspakker kan hjælpe til at danne et overblik over, hvordan enhederne på netværket udveksler information.
I et forsøg på at opfange brugernavne, passwords eller anden fortrolig information kan en angriber benytte pakkesniffere til at aflytte trafikken mellem hjemmearbejdspladsen og virksomheden. Dette er muligt fordi mange netværksapplikationer ikke i sig selv beskytter kommunikationen, men sender data i den form, som leveres til programmet. Derfor vil data ofte sendes ukrypteret med programmer som fx telnet, FTP, SMTP/POP3 og HTTP, med mindre brugeren selv aktivt har sørget for, at dataene er krypteret på anden vis.
Et stort problem i denne forbindelse er, at brugere ofte genbruger brugernavne og passwords på mange applikationer og systemer. Mange brugere benytter kun et enkelt password til alle deres applikationer, systemer og konti. Det er dermed et godt gæt, at hvis disse autorisationsinformationer kan aflyttes ét sted, kan de benyttes mange andre steder, hvor brugeren har en konto. Angriberen behøver dermed ikke aflytte det netværk han ønsker at bryde ind i, men blot aflytte det svageste af de netværk, som brugeren benytter.

Der er flere måder at beskytte sig mod denne form for angreb på:

- **Autentificering** – Brugen af en stærk autentificering er den primære løsning. Et eksempel på en sådan teknologi er to-faktor autentificering (se også afsnit 5.9). Engangspasswords (*One Time Passwords*, eller OTP) er et eksempel på et produkt, som benytter to-faktor autentificering. Brugeren er i besiddelse af en enhed, som producerer en ny kode hvert minut. Så snart koden er brugt eller tiden udløber, bliver den erklæret ugyldig. Selvom angriberen skulle opfange koden, er den alligevel ubrugelig. Aflytter angriberen trafikken for at opnå adgang til anden fortrolig information som fx indholdet af e-mails, vil stærk autentificering dog ikke have nogen effekt.
- **Infrastruktur baseret på switche** – Betegnelsen switch dækker over enten en bridge (lag 2) eller en router (lag 3). Fælles for dem er, at de i modsætning til hubs (som opererer på lag 1) dirigerer trafikken direkte fra punkt til punkt forstået sådan, at andre enheder på samme netværk ikke vil kunne se trafikken. Normalt vil trafikken fra hjemmearbejdspladsen gå igennem routere hos internetudbyderen og videre til virksomhedens

eget, switchede netværk. I sådanne tilfælde kan angriberen i princippet ikke aflytte trafikken.

Angrebseksempel

Der findes metoder, hvor selv switchede netværk kan aflyttes. I en artikel fra sommeren 2002 [99] beskrives, hvordan der kan brydes ind i stort set alle Cisco routere på markedet. Dette kan lade sig gøre fordi Cisco routere er bygget til at route pakker som højeste prioritet. Floodes routeren med pakker fra en eller flere maskiner vil den gå i en sikret tilstand, hvor kun de mest basale routerfunktioner opretholdes (dette kan fx gøres fra en Linux-maskine ved at udføre kommandoen *ping –s 65535 –f –c 1000000 cisco.host.name.net*). Det er herefter muligt at telnet'e til routeren fra en anden maskine og opnå administrative rettigheder på routeren ved at benytte standardpasswordet. Disse standardpasswords kan findes på internettet[1].
Når der er opnået administrative rettigheder over routeren udføres kommandoen *sh conf* hvorefter der kigges efter en linie som starter med "enable secret" eller "enable password". Dette gøres for at finde passwordet til administrationskontoen, som kommer i brug, når floodingen af routeren ophører. Hvis der kun er tre argumenter til en af disse linier er det tredje argument passwordet i klar tekst.
Er passwordet krypteret med Cisco Type 7 må det først brydes [7]. Ser linien derimod ud som "*enable secret md5 +949a8(%0xCV8*" er der tale om, at der er lagret en MD5 hashværdi i stedet for selve passwordet. I sådanne tilfælde benyttes fx programmet John the Ripper[2] til at finde passwordet.

Efter angriberen er kommet i besiddelse af passwordet til routeren er det oplagt at ændre routingtabellen så al trafik sendes igennem en maskine som kan opsamle de nødvendige data. Et program som TunnelX kan benyttes til dette og er omtalt i artiklen [8].

Andre uheldige design findes i produkter fra 3Com. I flere af deres produkter[3] findes et udokumenteret brugernavn – en såkaldt debugkonto – som har privilegier større end administratorens. Brugernavne og passwords til disse produkters debugkonti er kendt[4]. Ikke alene eksisterer disse bagdøre til systemerne, men det er muligt at ændre alle andre passwords til systemet uden at kende de eksisterende passwords. Således kan debugkontoen benyttes til at logge ind (via fx telnet) og ændre alle andre passwords, hvorved de legitime administratorer effektivt er udelukket fra at kommunikere med udstyret. Samtidig gives der adgang til enhedernes operativsystemer på et niveau, som selv administratorer ikke normalt har.

```
main menu:
==========
    [1] system          - Administer System level functions ->
    [2] ethernet        - Administer Ethernet ports ->
    [3] bridge          - Administer Bridging ->
    [4] atm             - Administer ATM resources ->
    [5] le              - Administer LAN Emulation Clients ->
    [6] vns             - Administer Virtual Networks configuration ->
    [7] management      - Administer IP and SNMP ->
    [8] quit            - Logout of the administration console
    [9] fast            - Fast Setup
   [10] tech            - Special technician options ->
```

Figur 2 – Hovedmenu fra en 3Com LanSwitch 2700

Benyttes de nævnte bagdøre til at logge ind på en 3Com LinkSwitch 2700 fås menuen som vist på figur 2. Der er desuden andre problemer med 3Com's backbone-produkter. Den enterprise MIB (Management Information Base) som 3Com leverer med produkterne, indeholder passwords og SNMP-nøgler til enhederne. Hvis SNMP-nøglen kan gættes (denne er ofte sat til fx "public") er det muligt at komme i besiddelse af administrationsnøglen og passwordet. Dette gøres via kommandoerne:

```
enterprises.synernetics.lanplex.lanplexSystemsMib.1.19.0 = "password"
enterprises.synernetics.lanplex.lanplexSystemsMib.6.7.0 = "public"
```

Dette trick kan udføres på fx CoreBuilder 3500 i softwareversioner 1.0 og 1.1 [9].
Idet mange af disse Cisco og 3Com-produkter er enheder, som benyttes af internetudbydere, teleselskaber og større virksomheder er det muligt for angribere at benytte disse sårbarheder til at aflytte forbindelserne til hjemmearbejdspladser og lignende, selvom udstyret i hjemmet og hos virksomheden ikke har disse svagheder.

Igen kan angriberen ændre routingtabellen for at sende al trafik gennem en maskine, som kan opsamle de nødvendige data og dermed aflytte den ønskede trafik.

Hvis ikke en sårbar Cisco eller 3Com router kan findes mellem hjemmearbejdspladsen og virksomheden, kan det forsøges at angribe en almindelig switch. Dette kan enten gøres ved at benytte den management port der ofte er at finde på disse (kræver fysisk adgang til switchen) eller ved at lave et overflow af adressetabellen med falske MAC adresser (eller ved blot at sende et kontinuerligt flow af tilfældige data). Dette vil ofte resultere i, at switchen skifter fra bridging mode til repeating mode, hvorved alle pakker

[1] Standardpasswords kan fx findes på adressen www.mksecure.com/defpw/
[2] Programmet John the Ripper kan findes på adressen http://www.freshmeat.net/projects/john/
[3] ATM switchene LanPlex 2500, 2500s og 2700, switchene SuperStack 2700 samt LinkSwitch 2000 og 2700, backbone ATM switchen CellPlex 7000, backbone routeren Corebuilder 3500 samt SuperStack II swtichene 1000 og 3000.
[4] For LANplex systemerne er det *debug/synnet* (loginnavn/password), for SuperStack og CellPlex produkterne er det *tech/tech* og for SuperStack-produkterne er det *monitor/monitor*

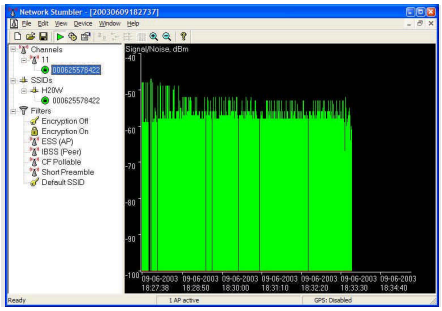
sendes ud på alle porte. Dette kaldes ”switch jamming” og kræver, at angriberen har adgang til mindst én maskine med opkobling til switchen [10]. Flere detaljer om denne problematik er gennemgået i Appendiks A.

- **Anti-sniffer udstyr** – En tredje metode for at undgå aflytning af trafikken er ved at benytte udstyr, som er designet til at detektere pakkesniffere. Teknologien virker ved at analysere responstiden for netværksenhederne og dermed afgøre, om de behandler mere trafik end blot den, der er adresseret til dem. Et eksempel på et sådant værktøj er AntiSniff som udvikles af Security Software Technologies[5].
- **Kryptering** – Den mest effektive måde at undgå aflytning af netværkstrafikken er ved at sikre at den trafik, som eventuelt aflyttes er ubrugelig. Hvis kommunikationen er sikret med kryptering kan en pakkesniffer kun opsamle cipher tekst. En mulig implementering af kryptering af kommunikationen er IP Security (IPSec), som operer på netværkslaget. Andre metoder er Secure Shell (SSH) samt Secure Sockets Layer (SSL), som opererer på applikationslaget[6].

Angrebseksempel

I visse tilfælde kan kryptering af netværkstrafikken ikke afhjælpe aflytningsproblememet. Specielle tilfælde i forbindelse med kryptering og aflytning af trådløse netværk, hvor denne undtagelse gælder, er kort nævnt nedenfor. Her er det muligt at aflytte trafikken på netværket selvom der benyttes kryptering. Det skyldes, at 802.11b netværk benytter et krypteringssystem kaldet Wired Equivalence Protection (WEP) som operer på lag 2. WEP benytter krypteringsstandarden RC4 med en bitlængde på enten 40, 64, 128 eller 256. Dette var aldrig ment som en stærk beskyttelse af netværket (”*wired equivalence*” antyder ”*så sikkert som et delt medie, kablet netværk*”) og der er fundet fejl i WEP som tillader nøgle-angreb mod datakrypteringen. Selvom disse fejl er rettet i det nyere udstyr, kræves der blot en enkelt sårbar klient eller access point på netværket for at tillade nøgle-angrebene. For at udtrække nøglen kræves tusindvis af svage nøgler, men da kun en eller to promille af pakkerne indeholder svage nøgler kan det tage lang tid at indsamle de nødvendige data.

Før disse data kan opsamles skal netværket findes. Et program som NetStumbler[7] kan – som det ses på figur 3 – fra en bærbar PC eller håndholdt enhed finde trådløse netværk i området. NetStumbler kan finde netværket uanset om SSID’en (Service Set Identififer) sendes eller ikke. Dette skyldes, at enhver klient, der forbinder sig til netværket, vil sende SSID’en i klar tekst (idet kun data-kanalerne kan krypteres via WEP). Der er altså meget ringe sikkerhedsforbedring forbundet med at slå SSID fra på access pointet.



Figur 3 - Netstumbler

Før trafikken kan aflyttes skal krypteringen som nævnt brydes. Dette arbejde kan gøres lettere ved at analysere kendte klar-tekst beskeder som fx DHCP discovery beskeder. Et program til at bryde WEP krypteringen er fx AirSnort[8]. Herefter kan programmer som NAI’s Wireless Sniffer[9], Ethereal[10] eller EtterCap[11] aflytte trafikken på netværket. Al trafik kan aflyttes, idet trådløse netværk fungerer som hubs og derfor udsender al den trafik der kan ses på netværket.

Selvom der ikke bevidst er opsat et trådløst access point, kan det være svært at undgå at ”udstråle” netværkstrafikken. Dette skyldes at mange nyere bærbare computere er udstyret med et indbygget trådløst netværkskort, som i visse tilfælde automatisk vil koble op mod andre trådløse enheder. En analyse af dette problem er dog udenfor dette projekts rammer, men mange spændende teknologier kan benyttes både til at udnytte og forhindre sådanne angreb[12].

Hvis trådløse netværk installeres i hjemmet, kan ovenstående angrebseksempel benyttes til at tilgå forbindelsen til virksomheden. Da trådløse netværk udstråler alle data som transmitteres på netværket, og hvis det benyttede netværk er sårbart som nævnt ovenfor kan der opnås adgang til hjemmets lokale netværk flere hundrede meter fra hjemmet. En mulig løsning på dette er at sikre, at hjemmets lokalnetværk er adskilt fra hjemmearbejdspladsen. Alternativt kan hjemmets lokale netværk med tilhørende hjemmearbejdsplads betragtes som et åbent netværk med tilhørende større krav til sikringen af hjemmearbejdspladsen.

---

[5] Information om produktet AntiSniff kan findes på adressen http://www.securitysoftwaretech.com/antisniff/
[6] Kryptering på applikationslaget krypterer kun dataene fra applikationerne. Således er alle routinginformationer og detaljer om netværksforbindelserne ukrypteret, idet dette foregår på underliggende lag.
[7] Programmet NetStumbler kan findes på adressen http://www.netstumbler.com/
[8] Programmet AirSnort kan findes på adressen http://airsnort.sourceforge.net/
[9] Information om programmet NAI Wireless Sniffer kan findes på adressen http://www.nai.com/
[10] Information om programmet Ethereal kan findes på adressen http://www.ethereal.com/
[11] Programmet Ettercap kan findes på adressen http://ettercap.sourceforge.net/
[12] Der er i angrebseksemplet brugt information fra [12]

3.2 Trust udnyttelse

Selvom der ikke er tale om et angreb i sig selv, refererer trust udnyttelse til det at angriberen misbruger de trustede forbindelser, som er etableret mellem enheder på et netværk. Dette kan fx være et segment af netværket, hvor virksomhedens eksternt tilgængelige servere er placeret – en såkaldt DMZ (demilitariseret zone). Fordi enhederne her tilhører samme netværkssegment, vil de ofte betragte hinanden som trustede systemer. Det samme kan gælde, hvis et eksternt system (som fx en hjemmearbejdsplads) er et trusted system overfor visse interne enheder. På den måde kan angriberen udnytte dette til at angribe det svageste led, hvorefter de trustede forbindelser giver adgang til andre enheder i systemet.

Det er muligt at begrænse denne type angreb ved at sætte strenge krav til, hvilke systemer, der kan betragtes som trustede i et netværk og nøje overveje, hvilke konsekvenser en etablering af trust mellem enhederne har. For at håndhæve sådanne regler kræver dog ofte specielt udstyr som fx brugen af PVLANs og VACLs (se afsnit 5.2). Samtidig bør trust ikke baseres alene på IP-adresser da det ovenfor er vist, hvordan disse kan forfalskes.

3.3 IP spoofing

Et angreb baseret på IP spoofing udnytter muligheden for at ændre afsender-IP-adressen på pakkerne. En angriber kan dermed sende pakker til netværket, som ser ud som om, de er sendt fra en anden maskine. Dette kan angriberen udnytte til at udgive sig for at være et system, som alene baseret på sin IP-adresse har specielle rettigheder i netværket (et *trusted* system). Et typisk eksempel er at spoofe interne IP numre i en virksomhed. Da disse adresser ofte er trustede af andre interne maskiner, kan den eksterne angriber dermed udgive sig for at være en intern maskine.
Spoofing kan desuden bruges til at sløre angriberens egen adresse ved fx Denial of Service (DoS) angreb (se Appendiks A).
Normalt kan IP spoofing kun benyttes til at indsætte data i en eksisterende kommunikationsstrøm. Hvis angriberen skal kunne etablere tovejskommunikation kræves det, at han er i stand til at ændre routingtabellerne i alle routere mellem ham selv og den enhed, der ønskes angrebet. Dette skyldes, at den IP-adresse, der spoofes, ikke tilhører ham, hvorfor svarene sendes tilbage til en anden enhed. Således vil svar som sendes til den spoofede adresse ikke nå frem til angriberen med mindre routingtabellerne er ændret, så trafik til den pågældende IP-adresse kan sendes tilbage til angriberen. Sker dette vil han således være i stand til at modtage og svare på kommunikation, som er sendt til den spoofede adresse.

Hjemmearbejdspladser udgør en stor risiko i forbindelse med denne angrebstype. Dette skyldes, at hjemmearbejdspladsens IP-adresse i visse tilfælde benyttes til at validere brugeren. Således kan en angriber udgive sig for at være den legitime hjemmearbejdspladsbruger ved at spoofe dennes IP-adresse.

Truslen fra IP spoofingangreb kan minimeres på følgende måder:

- **Adgangskontrol** – Ved at blokere al trafik fra det eksterne netværk, som har en afsenderadresse fra det interne netværk kan de fleste spoofingangreb forhindres. Men hvis virksomheden fx i forbindelse med hjemmearbejdspladser har eksterne, trustede adresser, vil denne adgangskontrol ikke forhindre spoofingangreb.
- **Autentificering** – IP spoofing er kun mulig, når enheder benytter IP-adressebaseret autentificering. Hvis andre autentificeringsmetoder tages i brug, kan IP spoofingangreb ikke gennemføres. Autentificering af enheder alene på basis af IP-adresser bør derfor ikke tildeles nogen sikkerhedsmæssig værdi.
- **RFC 2827 filtrering** – RFC 2827 [11] er et dokument som anbefaler, at alle netværk blokerer udgående trafik, som har en IP-adresse, der ikke er en del af organisationens eget IP-adresseområde. Dette afhjælper ikke direkte spoofingangreb, men forhindrer, at ens eget netværk kan være vært for spoofingangreb mod andre. Hvis alle netværksadministratorer og internetudbydere implementerede dette, ville spoofingangreb stort set ikke kunne forekomme.

3.4 Passwordangreb

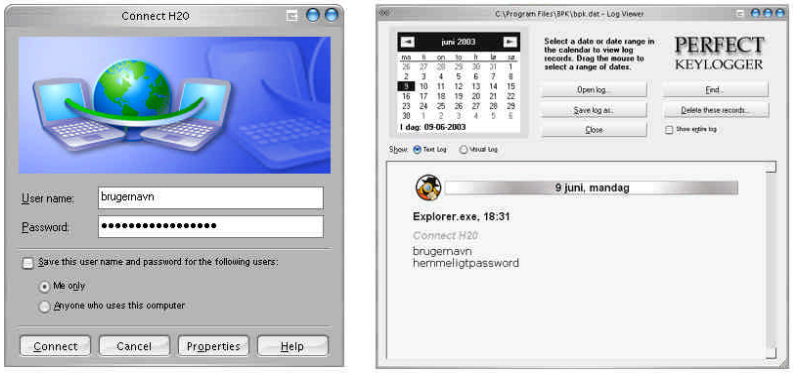
Passwordangreb er angreb, hvis formål det er at komme i besiddelse af brugernes passwords for på den måde at opnå adgang til netværket eller andre ressourcer. Der findes mange forskellige måder at udføre passwordangreb på. Det største, generelle problem i forbindelse med passwordangreb er brugeres valg af passwords samt vores tendens til at nedskrive disse og genbruge det samme password på alle systemer. Som tidligere nævnt gør dette arbejdet langt lettere for angriberen, som kun behøver angribe et svagt system for at opnå adgang til et stærkt beskyttet system.
Idet hjemmearbejdspladser ofte er ubeskyttet udenfor virksomhedens netværk er denne ofte et lettere offer end virksomhedens interne maskiner og kan dermed komme til at fungere som springbræt til virksomhedens interne net for en angriber. Ved fx at installere et program, som overvåger alle tastetryk (en såkaldt keylogger) på hjemmearbejdspladsen, kan angriberen afvente at brugeren benytter sit brugernavn og password og herefter selv benytte disse til at logge ind på virksomhedens net. Angriberen kan enten overtage hjemmearbejdspladsen via et

program, som gør angriberen i stand til at fjernstyre computeren (et eksempel er Back Orifice[13]) eller benytte en anden maskine til at koble på virksomhedens netværk ved at benytte de indhentede passwords. Hjemmearbejdspladsen kan også benyttes som base for videre passwordangreb mod systemet, idet maskinen ofte vil være en trusted adresse i virksomhedens netværk. På denne måde udnyttes samme svaghed som ved IP spoofing til at videreføre passwordangrebet.

Keyloggers kan fx installeres ved at opnå adgang til maskinen gennem kendte sårbarheder og derefter placere programmet i opstartssekvensen for maskinen. Programmer som kan benyttes til dette formål er det kommercielle Ghost Keylogger[14] eller gratis programmer som fx Home Keylogger[15]. Fælles for dem er, at de gemmer sig fra Windows' task liste og start menuer og kan sende de indtastede data via e-mail til angriberen. Alternativt kan angriberen forsøge sig med trojanske heste (se også afsnit 5.7), der er angrebsapplikationer, som er gemt i et andet program. Når brugeren udfører programmet, udføres samtidig den trojanske hest uden brugerens viden.

Angrebseksempel

Et eksempel på, hvordan det er muligt at benytte en keylogger til at få adgang til en VPN-forbindelse er vist nedenfor.
Brugeren vælger at oprette en VPN-forbindelse til sin arbejdsplads. Brugernavnet "brugernavn" og passwordet "hemmeligtpassword" benyttes til at oprette forbindelsen. Som det ses på figur 4 er passwordet skjult mens brugeren indtaster det.
Keyloggeren "Perfect Keylogger" fra BlazingTools er installeret på maskinen og afvikles skjult fra brugeren.
Installationen af keyloggeren kunne fx være sket via en e-mail eller social engineering (se også afsnit 3.8).



Figur 4 – Oprettelse af VPN-forbindelse og logfil fra Perfect Keylogger

Med jævne mellemrum sender keyloggeren informationer til angriberen om hvilke tastetryk, programmer og netværksaktiviteter der er sket på brugerens maskine. En sådan log ser ud som højre del af figur 4. Der kan desuden sendes skærmbilleder, billeder fra brugerens webkamera samt lyd, hvis brugeren har en mikrofon tilsluttet. Ud fra logfilen kan angriberen se at brugeren har oprettet en forbindelse til "H20" med brugernavnet "brugernavn" og passwordet "hemmeligtpassword". Bliver brugeren senere afkrævet yderligere identifikation når hun fx tilgår filer eller e-mails, vil også disse tastetryk blive aflæst og videresendt til angriberen. Det er dermed muligt at bruge disse informationer og tilgå virksomhedens netværk fra en anden lokation.

Andre eksempler er trojanske heste med keylogger-funktionalitet som fx den populære W32/Badtrans@MM, der distribueres via e-mail, lægger sig som gemte filer i Windows' systembiblioteker og sender information til angriberen. Der findes mange andre af denne slags trojanske heste som spredes via enten e-mail, spyware-programmer eller fildelingsprogrammer som fx Kazaa, eDonkey med flere.
Har man fysisk adgang til hjemmearbejdsplads-PC'en kan man installere en fysisk keylogger. Disse sælges af fx Amecisco[16] samt af ThinkGeek[17] for ganske få kroner. Et eksempel på en sådan kan ses på figur 5. De er populære hos bl.a. FBI som brugte dem i den meget omtalte Nicodemo Scarfo sag [13]. Et typisk eksempel hvor Scarfo benyttede en meget stærk kryptering igennem PGP[18] men hvor det svageste led i kæden gjorde det unødvendigt at bryde krypteringen.

Figur 5 - Keylogger fra ThinkGeek[20]

Hardware keyloggers kan være meget svære at beskytte sig imod, og da der sælges tastaturer som har en indbygget keylogger[19] er der ingen direkte mulighed for fysisk at afgøre om tastetrykkene aflyttes.

Der er dog flere forskellige måder at beskytte sig mod passwordangreb på:

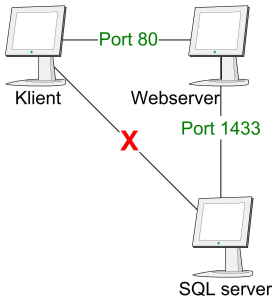
[13] Programmet BackOrifice kan findes på adressen http://www.cultdeadcow.com/tools/bo.html
[14] Information om Ghost Keylogger kan findes på adressen http://www.keylogger.net/
[15] Programmet Home Keylogger kan findes på adressen http://www.spyarsenal.com/
[16] Amecisco kan findes på adressen http://www.amecisco.com/
[17] ThinkGeek kan findes på adressen http://www.thinkgeek.com/
[18] PGP (Pretty Good Privacy) er et værktøj til kryptering af filer, e-mails m.m. Programmet blev i 2002 opkøbt af PGP Corp. og kan nu findes på adressen http://www.pgp.com/
[19] Produkterne kan findes på adressen http://www.keyghost.com/
[20] Billedet er fra ThinkGeek, http://www.thinkgeek.com/

- **Autentificering** – Ved at benytte kryptografiske autentificeringsmetoder eller ved at benytte engangspasswords (OTP) kan stort set alle passwordangreb forhindres. Desværre understøttes disse autentificeringsmetoder ikke af alle applikationer og enheder.
- **Scanningsværktøjer** – Brugen af antivirusprogrammer kan i et vist omfang begrænse passwordangreb. Programmerne kan ofte detektere trojanske heste og visse keyloggere. I mange tilfælde kræves der dog specielle scanningsværktøjer for at sikre sig mod dem med rimelig succes. Sådanne produkter (som fx TauScan[21]) fungerer ligesom antivirusprogrammer, men er lavet specielt til at identificere trojanske heste.
- **Egne passwordangreb** – Virksomhedens egne administratorer kan udføre passwordangreb mod de eksisterende brugerkonti i systemet for at sikre, at der ikke findes svage passwords i de tilfælde, hvor OTP eller kryptografiske metoder ikke kan tages i brug. Et program som LC4[22] kan på Windows-servere benyttes til at udføre brute-force angreb mod brugernes passwords.

3.5 Portomdirigering

Portomdirigering fungerer ved at en applikation lytter efter trafik på bestemte porte og videresender de rå (umodificerede) pakker til et andet, specificeret system. Således kan en applikation fx modtage trafik på port 80 fra ét system og videresende denne til et andet system på port 110. Samtidig kan afsenderporten ændres i de tilfælde dette er nødvendigt.

Formålet med portomdirigering er at omgå fx en firewalls restriktioner om, hvilken trafik der tillades fra den eksterne til den interne side af netværket. Dette kan gøres ved at kompromittere en maskine, som er tilgængelig offentligt, fx en webserver. En sådan server vil ofte være placeret i en DMZ. I visse tilfælde kan maskiner i dette segment kommunikere med det interne netværk. Grunden til dette kan være, at webservere placeret i dette segment skal kunne hente data fra en databaseserver, som af sikkerhedsmæssige årsager er placeret på det interne netværk. Således kan webserveren tilgås udefra på port 80, og kan tilgå en intern server med port 1433 (SQL). En firewall vil ofte sikre, at der ikke tillades trafik direkte fra det offentlige net til det private, interne net men kun til DMZ'en. En sådan opsætning er skitseret på figur 6.



Figur 6 - DMZ eksempel

Ved at kompromittere en webserver i dette segment, kan der installeres portomdirigeringssoftware på denne, som omdirigerer trafikken fra den eksterne maskine direkte ind til det interne netværk. Et eksempel på software som kan udføre denne portomdirigering er netcat[23].

Hjemmearbejdspladser kan være meget udsatte for denne type angreb. Det skyldes, at der i visse tilfælde åbnes for trafik ind til hjemmearbejdspladsens udstyr for at gøre det muligt at administrere dette fra virksomheden eller fra en ekstern udbyder. Som i eksemplet ovenfor etableres der regler for, hvilken type trafik der tillades ad denne vej, men med portomdirigering kan dette forsøges omgået. Samtidig kan portomdirigering bruges til at etablere forbindelse fra virksomhedens eksterne servere (som fx webserveren i eksemplet ovenfor) til hjemmearbejdspladserne igennem den forbindelse, som disse arbejdspladser har etableret til virksomheden. Dette vil ofte være mere kompliceret end vist ovenfor, men teknikken er den samme.

Truslen ved portomdirigering kan mindskes ved at etablere strenge krav til virksomhedens trust politik. Samtidig kan Host Intrusion Detection Systemer (HIDS'er) hjælpe til at detektere, hvornår en sådan omdirigering foregår samt eventuelt standse den ved at blokere for trafikken til og fra en angrebet enhed. Desuden bør der ved virksomhedens opkaldspunkter kontrolleres, hvilken type trafik, som går til og fra hjemmearbejdspladserne. Dette kan gøres ved at lade en firewall udføre trafikregulering – se også afsnit 5.4.

3.6 Angreb direkte på hjemmearbejdspladsen

Hjemmearbejdspladserne er et udsat angrebspunkt, idet de ikke direkte er beskyttet af virksomhedens forsvarssystemer men har adgang til at etablere forbindelser igennem disse systemer. De er ofte en overset sikkerhedsrisiko, hvilket er en del af baggrunden for dette projekt. Hvis en virksomhed placerede en arbejdsstation på ydersiden af deres sikkerhedssystemer og forbandt den både til internettet og direkte til de interne systemer ville alarmklokkerne ringe hos de fleste administratorer. Men blot fordi hjemmearbejdspladsen er flyttet flere kilometer væk, betyder det ikke, at denne situation ændres. Hjemmearbejdspladsen er ofte en arbejdsstation udenfor virksomhedens sikkerhedssystemer med mere eller mindre direkte forbindelse til det interne netværk og direkte forbindelse til internettet.

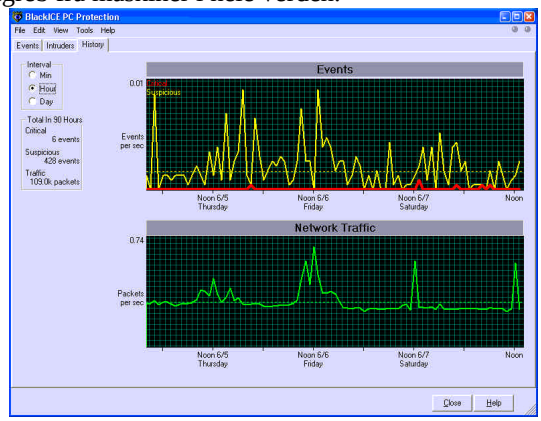
I det følgende udføres først to eksempler hvor det vises, hvor mange angreb der foretages mod ubeskyttede maskiner på internettet. Dernæst gives forslag til, hvordan hjemmearbejdspladsen kan sikres for at modstå disse, og andre, angreb.

Angrebseksempel

[21] Programmet TauScan kan findes på adressen http://www.tauscan.com/
[22] Programmet LC4 kan findes på adressen http://www.atstake.com/research/l3c/indx.html
[23] Programmet netcat kan findes på adressen http://insecure.org/tools.html

I et simpelt eksempel blev en ubeskyttet maskine med Windows 2000 uden servicepacks og patches sat til en ADSL-bredbåndsforbindelse fra Tiscali. Forsøget blev foretaget den 16. juli 2002. ISS' BlackICE system (version 3.5) blev benyttet til at overvåge trafikken til og fra maskinen, således at angrebene senere kunne analyseres. Efter 6 minutter var maskinen blevet angrebet første gang. 10 minutter senere var kendte sårbarheder blevet afprøvet, den indbyggede webserver var inficeret med ormen CodeRed og maskinen var begyndt at sende pakker ud – et tegn på, at den selv var aktivt i gang med at angribe andre maskiner. Efter yderligere en time var trafikken til og fra maskinen steget kraftigt og BlackICE viste et bredt spektrum af angreb fra maskiner i hele verden.

Et sekundært forsøg med Windows XP blev udført fra den 26. maj 2003 og otte uger frem. Ved at anbringe et fuldt opdateret system med McAfee antivirus, BlackICE firewall og IDS på en ubeskyttet del af DTU's netværk var det muligt at overvåge hvilken trafik der ramte maskinen. Efter 14 dage var antallet af angreb stilnet af og den daglige statistik så ud som på figur 7. På de 90 timer, som statistikken på figuren dækker over, var der i alt 428 angreb hvoraf de seks var alvorlige. Det skal understreges, at denne maskine ikke havde nogen porte åbne mod omverdenen.
Det bemærkes, at angreb mod SQL, web og mailservere også kan ses i loggen. Det tyder på, at angrebene udføres i blinde så snart et IP-nummer identificeres. Havde testmaskinen ikke været udstyret med nyeste opdateringer og beskyttelse af en firewall ville den med al sandsynlighed være blevet kompromitteret indenfor ganske kort tid.



Figur 7 - Angrebsstatistik fra BlackICE

Den samlede log over angrebet er vedlagt som bilag på CD-ROM. Det er interessant at observere, at selvom maskinen ikke havde nogen porte åbne, havde mere end 400.000 pakker fundet vej til maskinen på under 14 dage. De to forsøg understreger, at maskiner, som udsættes for direkte adgang til internettet, vil blive angrebet. Angrebene vil komme hurtigt og fra mange forskellige lande. Det første forsøg viser, hvordan en ubeskyttet maskine hurtigt bliver overtaget og selv aktivt tvinges til at angribe andre maskiner. Det andet forsøg viser det spektrum af angreb, som forsøges mod maskinerne, uanset om disse svarer på forespørgslerne eller ikke. Samtidig er det vist, at maskinerne bliver fundet på netværkene, selvom deres IP-numre eller navne ikke er offentliggjort, men blot er en del af den pulje af IP-numre som enten internetudbyderen (første forsøg) eller DTU (andet forsøg) er i besiddelse af.

Ofte vil trojanske heste blive benyttet i angreb mod hjemmearbejdspladserne. Disse kan enten benyttes til at samle informationer fra brugeren (som fx passwords – se også afsnit 3.4 ovenfor) eller til at muliggøre fjernstyring af maskinen fra angriberens enhed. Trojanske heste kan ofte kombineres med angreb mod kendte sårbarheder for på den måde at få mulighed for, at eksekvere den trojanske hest på offerets maskine.

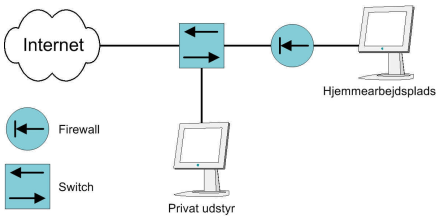
Der er flere måder at beskytte sig mod disse typer angreb:

- **Antivirus** – Brugen af antivirusprogrammer (se afsnit 5.6) og scannere mod trojanske heste (se afsnit 5.7) kan benyttes til at detektere og afværge angreb baseret på trojanske heste. Opdateringen af denne type programmer skal dog foregå jævnligt, hvilket i decentraliserede miljøer kan være et problem. Samtidig beskytter dette ikke mod angreb, som ikke benytter sig af trojanske heste.
- **Personlige firewalls** – Installationen af personlige firewalls på hjemmearbejdspladsmaskinerne kan i mange tilfælde forhindre angrebene. Ulempen ved denne type firewalls er dog, at de ofte kræver interaktion fra brugeren, som ikke altid vil være teknisk kvalificeret til at håndtere denne opgave. Samtidig træder beskyttelsen først i kraft det øjeblik trafikken når hjemmearbejdspladsens computer – en situation, som måske ikke er ønskværdig.
- **Hardware** – Flere forskellige typer hardware kan hjælpe til i opgaven med at beskytte hjemmearbejdspladserne. Ofte vil der af økonomiske og administrationsmæssige årsager ikke være tale om at kopiere sikkerhedsopsætningen i virksomheden, men der findes alternativer, som er designet til at håndtere beskyttelsen af mindre systemer. Firewalls og routere kan ofte leveres i udgaver, som er specielt velegnet til mindre båndbredder og de simplerere opsætninger, som kendetegner hjemmearbejdspladserne. Således er der sjældent brug for at kunne etablere egne offentligt tilgængelige servere eller levere e-mail services til mange brugere. I visse tilfælde kan disse firewalls og routere tilpasses virksomhedens udstyr, således at der kan etableres distribuerede opsætninger og konfigurationsændringer.
  VPN dialere kan også benyttes til at levere en øget sikkerhed og ydelse ved opkald til virksomhedens netværk. Fælles for dette udstyr er dog, at det kan være dyrt i anskaffelse, implementering og vedligeholdelse.

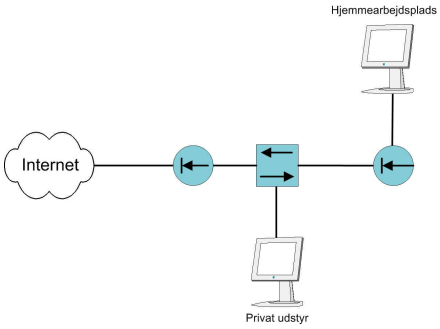
En anden type angreb mod hjemmearbejdspladsen er angreb fra hjemmets andre computere. Ofte vil bredbåndsforbindelsen i hjemmet også blive benyttet af de private computere, som hjemmets øvrige beboere benytter. Således kan fx spilkonsoller, printere, servere, bærbare og stationære computere samt trådløse netværk og

tilhørende enheder være tilsluttet forbindelsen. Da dette private udstyr ikke er under virksomhedens kontrol, kan det være meget udsat for eksterne angreb, vira, trojanske heste mm. Har angriberen først adgang til en af disse enheder, er der direkte adgang til både hjemmearbejdspladsen og det eventuelle udstyr, som benyttes til at etablere forbindelse til virksomheden. I det værst tænkelige tilfælde er der direkte adgang igennem en allerede etableret VPN-tunnel til virksomhedens interne netværk.
Det meget omtalte angreb mod Microsoft i oktober 2000, hvor angriberne stjal kildekode til forskellige produkter menes at stamme fra angreb mod en hjemmearbejdsplads' private netværk og derfra videre igennem hjemmearbejdspladsens opkobling til Microsoft [31].
For at beskytte sig mod sådanne angreb bør hjemmearbejdspladsen adskilles fra hjemmets resterende udstyr. Der er flere fremgangsmåder:

- Hjemmets øvrige udstyr kan forbindes til bredbåndslinien før hjemmearbejdspladsens firewall. Dermed er det private udstyr ubeskyttet mens hjemmearbejdspladsen er isoleret. Opsætning kan ses på figur 8. Ulemperne er den manglende beskyttelse af hjemmets private udstyr samt problemerne med at dele printere og andet fælles udstyr.
- Ved at benytte udstyr, som baseret på IP-adresser afgør hvilke computere der skal tildeles adgang igennem VPN-forbindelsen og hvilke der skal føres direkte til bredbåndsforbindelsen, kan det forhindres, at det private udstyr får adgang til VPN-forbindelsen. Denne løsning er dog meget sårbar overfor IP spoofing angreb. Fordelen er at alle maskiner beskyttes bag en eventuel firewall, ligesom printere og andet udstyr kan deles.
- Udstyr, som adskiller hjemmenes netværk med en firewall, kan benyttes som det ses på figur 9. Således beskytter én firewall alle maskiner i hjemmet mod angreb udefra, mens en anden firewall beskytter hjemmearbejdspladsen mod angreb fra det øvrige udstyr. Hvis det ønskes, kan der gives adgang til en fælles printer fra begge netværk. Udstyr af denne type leveres ofte integreret og ikke opdelt, som det er vist på figuren.



Figur 8 - Forbindelse før firewall



Figur 9 - Forbindelse med intern firewall

3.7 Angreb mod opkaldspunktet

Oftest vil virksomheden implementere opkaldspunkter af forskellig art for hjemmearbejdspladserne. Dette kan være modem, ISDN, VPN eller andre typer forbindelser. Forbindelserne benyttes til at åbne for adgang til virksomhedens interne netværk udefra.
Angribere kan benytte svagheder i disse systemer til at opnå adgang til virksomhedens interne netværk. For opkaldslinier (ISDN eller modem) benyttes ofte dial-back, hvor virksomheden ringer tilbage til brugeren og dermed bekræfter identiteten. Denne implementeringsform kan i visse tilfælde omgås – specielt hvis der er tale om et simpelt modem der ringer tilbage over samme linie som opkaldet kom ind på [15]. Princippet for angrebet er enkelt og består i, at modemet tvinges til ikke at "lægge på" hvorefter angriberens egen klartone afspilles over linien. Det får modemmet hos virksomheden til at tro, det har fået en ny linie og vil derfor forsøge at ringe tilbage til det forudbestemte nummer. Derefter laves en normal synkronisering af de to modems hvorved systemet vil tro, det succesfuldt har ringet tilbage.
VPN-porten kan også bruges som angrebspunkt. Den 26. september 2002 blev en sårbarhed i Microsoft's PPTP VPN protokol opdaget. Denne kan benyttes til afvikling af vilkårlig kode på VPN-serveren og har dermed potentiale for at give administrative rettigheder til angriberen [16]. Også ved brugen af hardwarebaserede VPN-enheder som fx en Cisco VPN Concentrator kan sårbarheder opstå. Den sidste blev fundet i 7. maj 2003 [17].

Selv hvis ingen sårbarheder eksisterer i produkterne der benyttes, er det stadig risikofyldt at åbne for adgangen. Benytter brugerne ukomplicerede passwords, kan en angriber forsøge at bryde disse ved at lave loginforsøg på de forskellige services som tilbydes. Brugernavnene kan ofte findes ved at se på de e-mailadresser, som virksomheden evt. oplyser om deres medarbejdere på hjemmesiden.

Forsvaret mod sådanne angreb kan bl.a. bestå af følgende:

- **Dedikerede dial-back enheder** – Specialudviklede dial-back enheder kan benyttes i stedet for almindelige modems eller ISDN-adaptere. Disse enheder er designet med henblik på at undgå den svaghed i systemet, som muliggør ovenstående angreb mod dial-back metoden. Enhederne benytter flere linier, hvoraf en andel er opsat til kun at kunne lave udgående opkald. Disse linier benyttes til at ringe tilbage til brugeren, så den samme linie aldrig kan bruges til indgående og udgående opkald.
- **Stærk autentificering** – Ved at benytte OTP eller andre typer stærk autentificering af brugerne og dermed ikke afhænge af brugen af passwords, kan mange af angrebene mod VPN-opkaldspunkterne afhjælpes. Samtidig kan andre teknologier benyttes til at autentificere opkaldsenhederne før brugerautentificeringen foregår (se også afsnit 5.3). Dermed kan kun ansatte med adgang til virksomhedsspecifikt udstyr forsøge at

angribe opkaldspunkterne fra disse enheder. Selvom noget sådant udstyr skulle blive stjålet fra hjemmearbejdspladserne, vil brugerautentificeringen baseret på OTP eller anden stærk autentificering beskytte adgangen.
Denne beskyttelse har dog ofte ingen effekt overfor sårbarheder i selve opkaldspunktets hardware eller software.

- **Vedligeholdelse** – Alle enheder bør vedligeholdes og holdes opdaterede med nyeste patches, service packs osv. fra de respektive producenter. Dette gælder specielt det udstyr, som benyttes til at håndtere opkaldspunkterne da udstyr af denne type oftest er direkte tilgængeligt fra internettet.
CERT oplyser, at 95 % af alle vellykkede angreb skyldes udnyttelse af kendte sårbarheder eller konfigurationsfejl, der allerede findes rettelser til. Det er derfor svært at overdrive vigtigheden af, at holde systemerne opdaterede.

3.8 Social Engineering

Figur 10 - Kevin Mitnick[24]

Social engineering er den menneskelige side af IT-sikkerhedsproblematikken. Den nu berømte hacker Kevin Mitnick gjorde denne form for angreb kendt ved blandt andet at bryde ind hos Novell og stjæle kildekoden til enkelte af deres produkter. Dette foregik uden at bryde firewalls, passwords og andre sikkerhedsforanstaltninger. I stedet for benyttede Mitnick det ofte svageste led i sikkerhedskæden: den menneskelige faktor.
Med lidt kendskab til virksomheden, imødekommende opførsel og charmerende personlighed er det ofte muligt at lokke næsten hvilken som helst oplysning ud af virksomhedens medarbejdere. I tilfældet med Novell ringede Mitnick blot til de rigtige medarbejdere og overbeviste dem om, at de skulle give ham den nødvendige adgang.
Risikoen i forbindelse med social engineering er endnu større når arbejdspladser flyttes udenfor virksomheden. Hvordan skal medarbejderen i hjemmet sikre sig, at den der ringer virkeligt er fra virksomheden? Og hvordan skal virksomheden sikre sig, at den der ringer virkeligt er medarbejderen i hjemmet?

Problemerne med social engineering kan relateres til stort set alle sikkerhedsproblemer. Hver gang et problem løses rent teknisk er der ingen garanti for, at det er løst i relation til social engineering.

Angrebseksempel

Et eksempel på, hvordan social engineering kan udnyttes er vist nedenfor.

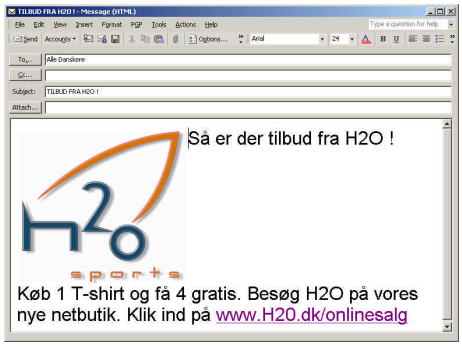
Der oprettes en hjemmeside, hvorpå det ser ud som om, der sælges tøj af mærket H_2O. En sådan side kunne fx se ud som på figur 11. Samtidig registreres domænenavnet H20.dk (i modsætning til H2O.dk, som antages registreret til ejeren af varemærket H_2O).
Angriberen har nu gode muligheder for at udnytte situationen. Dette foregår ved at sende en e-mail ud til enten en udvalgt gruppe af personer eller til så mange danskere som overhovedet muligt. I denne e-mail gælder det om at overbevise brugeren om, at der for det første er et godt tilbud og for det andet, at den hjemmeside der henvises til faktisk er den korrekte hjemmeside. Udformningen af en sådan e-mail kunne se ud som vist på figur 12. Mange brugere vil formentligt uden videre acceptere dette som en legal mail, specielt hvis afsenderadressen sættes til salgsnyt@H2O.dk hvilket også er gjort i det konkrete tilfælde.

Figur 11 - Falsk H2O hjemmeside

De vågne brugere vil dobbeltchecke, at linket i bunden af e-mailen faktisk peger på den adresse, som er skrevet – samt at denne adresse bærer navnet H2O. Da det næsten er umuligt at se forskel på et O og et 0, vil adressen formentligt blive accepteret.

[24] Billedet er fra Defensive Thinking som kan findes på adressen http://www.definsivethinking.com/

Når først brugeren er nået ind til hjemmesiden er det blot at sikre, at siden virker som en troværdig salgsbutik og gøre det muligt at handle online med sit kreditkort. Herefter stjæles disse data kombineret med brugerens navn, adresse og telefonnummer. Er angriberen specielt grundig sikres det, at brugeren senere modtager de bestilte varer (angriberen kan passende bestille varerne med brugerens kreditkort fra den rigtige H_2O-butik) så der ikke senere fattes mistanke mens Dankortet misbruges. Bemærk i øvrigt, at den på figur 12 viste adresse fungerer og kan afprøves af læseren.
FBI har netop udsendt en advarsel omkring ovenstående angrebsmetode [109].



Figur 12 - Falsk H2O salgsmail

En lignende teknik kan benyttes til at lokke brugernavne og passwords ud af brugerne i en virksomhed. Ved at lokke brugerne til at besøge, hvad der ligner en intern hjemmeside på virksomhedens servere er det formentligt muligt at få brugeren til at angive brugernavne og passwords. Det primære problem her er, at det som regel ikke som i det ovenstående tilfælde er muligt at registrere vellignende domænenavne. Løsningen er dog simpel.
En feature i både Internet Explorer, Netscape, Mozilla, Firebird[25] med flere gør det muligt at "formulere" en URL på en sådan måde, at mange brugere med stor sandsynlighed vil tro, at der er tale om en korrekt, intern adresse. Ønsker angriberen at få brugerne til at indtaste deres password på en side på den fiktive adresse http://n8kr.dk, kan URL'en formuleres således[26]:
http://FirmaServer.dk&item%3Dq209354@n8kr.dk/3Dquu5698/lo77/Q209354%20-%20LOGIN.htm
De fleste brugere vil formentligt antage, at denne side findes på FirmaServer.dk, som de er blevet meddelt af administratorer og kolleger er den korrekte side at besøge, hvis det drejer sig om virksomhedens interne vedligeholdelse af fx passwords, e-mail konti osv. Men faktisk peger denne URL på en side på n8kr.dk, som angriberen har kontrol over. Herefter benyttes samme trick som ovenfor, hvor angriberen designer en hjemmeside, som på troværdig vis afbilleder den interne servers hjemmeside med mulighed for ændring af passwords osv. I en e-mail, som ser ud til at komme fra virksomhedens IT-afdeling, anmodes de ansatte derefter om at besøge siden og skifte password grundet en opdatering af systemet. Har angriberen ikke mulighed for at finde ud af, hvordan virksomhedens interne hjemmeside ser ud, kan han blot i e-mailen meddele, at der er kommet nyt design, som webdesignerne i øvrigt meget gerne vil have feedback på.

Det interessante i disse eksempler er, at der ikke er tale om sårbarheder i produkter, brug af trojanske heste, vira eller andet. Der er udelukkende tale om at benytte social engineering til at få brugerne til at udføre kommandoer eller besøge hjemmesider, så informationer kan indhentes for på den måde at omgå den sikkerhed, som virksomheden ellers måtte have implementeret.
Det er værd at huske, at en angriber som regel vil angribe det svageste led i kæden. Hvis virksomheden har en velbeskyttet internetadgang som vedligeholdes af dygtige IT-sikkerhedseksperter, vil angriberen formentligt forsøge at omgå denne adgang. Og her kan både hjemmearbejdspladser og fx telefoner benyttes. Spørgsmålet der bør stilles er, om staben af IT-eksperter som håndterer virksomhedens internetadgang også overvåger hver eneste telefon og e-mailadresse for at sikre, at en uvidende ansat ikke afleverer de informationer, som de forsøger at beskytte.
En mulighed for at forebygge denne type angreb kan derfor være, at disse IT-eksperter træner de ansatte til at gennemskue, hvornår der er tale om social engineering-angreb[27].

3.9 Brugersabotage

I tilfælde, hvor virksomheden indfører restriktioner på, hvilke aktiviteter brugerne må foretage sig på netværket kan der forekomme situationer, hvor brugerne forsøger at omgå disse restriktioner. Dette er en væsentlig problemstilling, idet dyrt udstyr og gennemtænkte implementeringer hurtigt kommer til kort, hvis legitime brugere gennemfører handlinger, som omgå de implementerede sikkerhedsforanstaltninger.
Et produkt, som brugere i visse tilfælde benytter til dette er GoToMyPC[28]. Dette er et kommercielt produkt, som er meget udbredt i større virksomheder, hvor de ansatte installerer programmet for at kunne fjernstyre deres arbejds-PC fra en netcafé, hjemmet eller fra en vilkårlig anden maskine på internettet. Kun et password beskytter adgangen og virksomhedens øvrige sikkerhed kan ofte forbigås gennem dette program. Idet kommunikationen initieres indefra virksomhedens LAN (på port 80) vil en firewall normalt ikke blokere forbindelsen. Programmet er designet til at omgå næsten ethvert sikkerhedssystem.

---

[25] Denne feature findes i alle kendte versioner inkl. IE 6.0SP1, Mozilla 1.4 og Netscape 7.1 og betragtes ikke som en fejl i programmerne.
[26] Muligheden for at fomulere URLs på denne måde eksisterer fordi syntaksen http://brugernavn:password@adresse ofte benyttes til at angive ikke-anonyme URLs, hvor brugeren er logget på. Således kunne fx http://soren:secret@www.amazon.com/ benyttes til at logge på amazon.com med brugernavnet *soren* og passwordet *secret*.
[27] Der er i afsnittet brugt information fra [2].
[28] Programmet GoToMyPC kan findes på adressen http://www.gotomypc.com/

På trods af, at ExpertCity som opererer GoToMyPC har implementeret et omfattende sikkerhedssystem [14] som bl.a. forhindrer man-in-the-middle angreb og genafspilningsangreb er produktet farligt i den forstand, at det forbigår virksomhedens sikkerhedssystemer uden de netværksansvarliges viden. Har virksomheden fx implementeret to-faktor autentificering, kan denne forbigås hvis blot en enkelt bruger har installeret dette program. Og installeres programmet på hjemmearbejdspladserne kan disse enheder med forbindelse til virksomhedens interne netværk fjernstyres udelukkende ved brug af et password.
Det må antages sandsynligt, at der vil være mindst en enkelt bruger i en stor organisation, som har den nødvendige viden og vilje til at installere sådanne produkter. Derfor bør forsvaret mod dette ikke alene være brugeruddannelse, men også at sikre, at ingen brugere kan installere sådanne programmer – hverken i virksomheden eller på hjemmearbejdspladserne. Dette kan fx gøres ved at sørge for, at brugeren ikke har de nødvendige rettigheder på arbejdsstationerne. Det er desuden en mulighed at benytte en proxyserver, så udgående trafik skal autentificeres (se afsnit 5.4.3). Dette vil hjælpe til at sikre, at programmer, som omgår sikkerheden ved at etablere udgående forbindelser ikke vil fungere. Selv hvis programmet er designet til at benytte en sådan proxyserver, kan proxyserveren analysere datastrømmen og dermed i visse tilfælde detektere denne form for brugersabotage.

3.10 Opsummering

Der er i kapitlet gennemgået nogle af de sikkerhedsproblemer, som kan true sikkerheden omkring implementeringen af hjemmearbejdspladser og netværkssikkerhed generelt. Sammen med problemerne er der udarbejdet forslag til, hvordan disse kan løses. Det skal dog bemærkes, at hverken sikkerhedsproblemerne eller løsningerne udgør en komplet liste over de muligheder, som angribere og administratorer har. Der er tale om et udpluk af nogle af de mest aktuelle problemstillinger og løsningsmetoder. Således er der givet eksempler på følgende sikkerhedsproblemer:

- Aflytning
- Trust udnyttelse
- IP spoofing
- Passwordangreb
- Portomridigering
- Angreb direkte på hjemmearbejdspladsen
- Angreb mod opkaldspunktet
- Social Engineering
- Brugersabotage

De i kapitlet nævnte sikkerhedsproblemer skal sammen med de informationer, som gives i de følgende kapitler danne grundlaget for at etablere et netværksdesign til sikker implementering af hjemmearbejdspladser.

4 EKSISTERENDE PAKKELØSNINGER

For en virksomhed, som skal implementere hjemmearbejdspladser er det attraktivt at kunne lade en televirksomhed levere forbindelse og udstyr til hjemmene. Alternativet er, at virksomhedens IT-afdeling selv skal etablere udstyr, bestille forbindelser og levere service til hjemmearbejdspladserne. Således kan der være både administrative og økonomiske fordele i at benytte en pakkeløsning, hvis denne kan leve op til de krav, som virksomheden stiller til både sikkerhed og funktionalitet.
I dette afsnit undersøges, i hvor høj grad de tilbud televirksomhederne i Danmark tilbyder, kan leve op til de krav, der i denne rapport sættes til hjemmearbejdspladsernes sikkerhed.
Løsningerne er udvalgt ud fra de tilbud, som televirksomhederne tilbyder. Proceduren for udvælgelsen har bestået i at vælge den mest relevante løsning fra hvert teleselskab ud fra kravet om højst mulig sikkerhed samt muligheden for at segmentere hjemmets netværk.
Fra virksomhedens synspunkt vil det ofte være fordelagtigt, at IT-afdelingen har mulighed for at gennemføre ændringer til konfigurationerne, således at en beslutning som gælder for arbejdsstationerne også kan gennemføres for hjemmearbejdspladser. Samtidig kan det i visse tilfælde være en fordel, at den daglige vedligeholdelse af udstyret i hjemmene foretages af udbyderen. Denne slags overvejelser er medtaget i nedenstående gennemgang af de danske televirksomheders tilbud til hjemmearbejdspladser.

Der vil i afsnittet være henvisninger til teknologier, som beskrives senere i rapporten.

4.1 TDC Erhverv

TDC [22] sælger løsningen "Hjemmearbejdsplads VPN router" under lovning om, at man kan:

"[etablere hjemmearbejdspladser] uden at kompromittere sikkerheden på nogen måde".

Ifølge TDC er udbyttet af en sådan opsætning:

"Med denne hjemmearbejdsplads-løsning skabes således et virtuelt netværk mellem arbejdspladsen og hjemmet, som gør at medarbejderens oplevelse vil være den samme på kontoret som i hjemmet UDEN at sikkerheden kompromitteres"

Teknikken
Løsning er baseret på en SpeedStream 5781-router[29] i hjemmet, som leder trafikken igennem en L2TP eller IPSec VPN tunnel (se afsnit 5.1) til en SonicWall PRO100 enhed hos virksomheden. Sidstnævnte er en kombineret firewall og VPN koncentrator, som kan håndtere op til 50 samtidige VPN-forbindelser. Firewall'en understøtter brugen af en DMZ og kan lave stateful packet inspection (se afsnit 5.4.4) samt håndtere IPSec VPN-forbindelser med en samlet båndbredde på 20Mbit.

Figur 13 – SonicWall PRO100 [26]

SpeedStream-routeren i hjemmet kan p.t. ikke lave stateful packet inspection, og vil være en filterbaseret løsning indtil dette aktiveres i routeren (forventes 4. kvartal 2003 ifølge TDC). Dette er dog ikke et problem med selve routeren, men udelukkende et konfigurationsspørgsmål.

Figur 14 – SpeedStream 5781 [27]

SpeedStream 5781-routeren i hjemmet, som ses på figur 14, fungerer både som firewall og VPN dialer. Efficient Networks som producerer 5781-routeren fortæller [117], at når hjemmets private PC'er tilsluttes enheden foregår dette via en hub, som deles med internetforbindelsen. Således er trafikken til og fra hjemmearbejdspladsen også tilgængelig fra det private netværk. Den lidt dyrere 5800 router håndterer denne segmentering med brug af en switch, således at det private udstyr og hjemmearbejdspladsen også er adskilt i lag 2. Routeren har en maksimal VPN performance på 1Mbit.

Fordele
Både SpeedStream 5781 samt SonicWall PRO100 er ICSA-certificerede (se afsnit 6.3). Den hardwarebaserede VPN-dialer i hjemmet kan dog ikke benytte digitale certifikater til at autentificere enheden mod fx en VPN Concentrator.
TDC's løsning afhjælper problemer med aflytning af trafikken mellem hjemmet og virksomheden. Samtidig beskyttes hjemmearbejdspladsen mod angreb udefra ved hjælp af en hardwarebaseret, stateful packet inspection firewall – når TDC tillader, at denne funktionalitet implementeres. SpeedStream routeren kan logge aktiviteterne lokalt, hvorefter disse kan tilgås fra virksomheden via IPSec eller SSH forbindelser til routeren.

[29] Routeren er produceret af Efficient Networks, men sælges under SpeedStream-navnet i Danmark. Både Efficient Networks og SpeedStream er virksomheder under Siemens koncernen.

For mindre netværk kan det være en fordel, at der i løsningen medleveres en firewall og VPN-enhed til virksomheden. Enheden understøtter desuden mere avancerede features som blokering af URLs med mere.

Ulemper
Rent performancemæssigt udgør løsningen et problem. Med 50 mulige VPN-forbindelser til SonicWall PRO100-enheden og en maksimal båndbredde på 20Mbit/s gives kun 400kbit/s per forbindelse. Selv med færre brugere begrænser SpeedStream-produktet hastigheden til 1Mbit. Hurtige ADSL-forbindelser kan dermed ikke understøttes af løsningen, hvilket kan undre, da TDC bl.a. lever af at sælge disse forbindelser.
Segmentering af hjemmets private netværk og hjemmearbejdspladsens forbindelse er baseret på en hub, som dermed udsender al data på alle porte. Fra et sikkerhedsmæssigt synspunkt er dette risikabelt.
TDC's politik er ikke at tillade konfigurationsændringer i produkterne, hvilket kan være et problem for virksomheder med egen sikkerhedspolitik. Samtidig er TDC's implementering af nye features i produktet langsom, hvilket ses ud fra den manglende stateful packet inspection i SpeedStream routeren. Det er samtidig et problem, at virksomheden ikke selv kan opdatere udstyret. Kravene fra sikkerhedspolitikken omkring vedligeholdelse af udstyret kan dermed ikke imødekommes direkte, og en afhængighed af TDC's vilje til at opdatere udstyret kan for mange virksomheder repræsentere et problem.
Ifølge TDC Erhverv [118] vil en konfiguration af routeren med segmentering af nettene slet ikke være muligt, da en sådan konfiguration ikke supporteres af TDC. Da der samtidig ikke vil blive åbnet for muligheden for at ændre i routerens konfiguration efter levering, er der ikke mulighed for at benytte denne funktionalitet. Manglen på support for brugen af digitale certifikater bør også nævnes.
Løsningen indeholder ingen teknologi til at forhindre keyloggers, sniffere, trojanske heste eller virus på hjemmearbejdspladsen. Der er ikke support for One Time Passwords eller anden to-faktor autentificering i SonicWall VPN-enheden, ligesom der ikke implementeres begrænsninger på brugerens PC eller udstyr

Konklusion
Der er alene tale om sikring af kommunikationen mellem hjemmet og virksomheden i form af en hardwarebaseret IPSec VPN-forbindelse samt sikring af virksomhed med en stateful packet inspection firewall og hjemmet med et pakkefilter. Segmentering af hjemmets netværk er baseret på en hub, hvilket ikke er en optimal løsning, men da TDC ikke tillader brugen af segmenteringsfunktionen er dette mindre relevant.
Selvom løsningen kun skulle benyttes til alene at sikre kommunikationen mellem hjem og virksomhed er der svagheder i designet. Løsningen sælges sammen med ADSL-forbindelser på op til 2 Mbit/s, men udstyret understøtter maksimalt 1 Mbit/s.
SonicWall produktet skalerer ikke, da det er begrænset til 50 forbindelser. Generelt virker løsningen ufleksibel og udstyret får ikke lov til at leve op til dets potentiale pga. TDC's stramme politik om konfiguration og opdatering.

4.2 CyberCity Erhverv

CyberCity's [23] mest relevante løsning er deres Secure HomeOffice Pro. Denne beskrives som:

"Den meget sikre og altid opdaterede løsning". CyberCity skriver desuden at *"[løsningen] sikrer en hjemmearbejdsplads optimalt mod uautoriseret indtrængen fra internettet, samt at kommunikationen mellem hjemmearbejdspladsen og virksomhedens netværk forbliver fortrolig."*

Teknikken

Figur 15 - SonicWall Tele3TZ fra CyberCity [24]

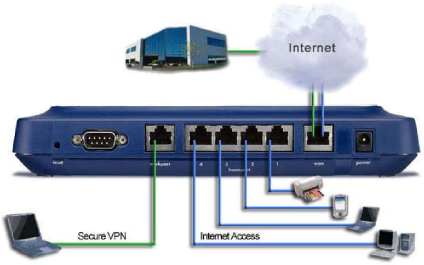
Denne løsning bygger på en firewall af mærket SonicWall Tele3TZ [24] som ses på figur 15. Firewall-enheden understøtter stateful packet inspection og kan desuden benyttes som VPN dialer – som standard dog kun til at tillade softwarebaserede dialere at passere enheden, men kan udvides til at fungere som VPN dialer uden brug af softwareklienter. Performancemæssigt understøtter enheden 20Mbit/s ved brug af 3DES kryptering til IPSec VPN. Den er ICSA certificeret og er udstyret med to 100Mbit porte til segmentering af hjemmets netværk.
Aktiviteterne fra hjemmearbejdspladsen kan logges i enheden, og SonicWall's Global Management System kan benyttes fra virksomheden til at sikre, at konfigurationsændringer distribueres til alle hjemmearbejdspladser.
SonicWall Tele3TZ er designet til at være kompatibel med IPSec VPN-produkter fra Cisco, CheckPoint, Nortel og Symantec – samt SonicWall's egne produkter. Som noget unikt understøtter SonicWall en række services, som skal sikre, at brugerens arbejdsstation overholder en række krav. Disse services er beskrevet nedenfor:

- **Anti-virus** – Gennem et samarbejde med McAfee kan SonicWall-enhederne sikre, at hjemmearbejdspladsen har de nyeste virussignaturer installeret og aktiveret før der gives adgang til netværket. Signaturfilerne kan automatisk påtvinges computeren hvis ikke de allerede eksisterer (så længe operativsystemet er Windows). Et omfattende management-interface kan distribuere politikker og indstillinger til enhederne.
- **Indholdsfiltrering** – URL-filtrering kan foretages indenfor 12 kategorier hvis det ønskes at begrænse, hvad brugeren må benytte arbejdspladsen til. Tidsafhængig filtrering kan foretages, så fx kun arbejdsrelaterede

sider kan besøges i arbejdstiden. Databasen over URLs leveres fra Cerberian's URL database, som er en liste over millioner af IP-adresser, URLs og domænenavne inddelt i kategorier, som fx "underholdning", "e-handelssteder" osv. Samme managementinterface som til ovenstående service kan benyttes til at håndtere dette.

- **Sårbarhedsscanning** – SonicWall tilbyder at scanne alle virksomhedens SonicWall-produkter (og i visse tilfælde andre produkter) for sårbarheder, fejlkonfigurationer og andet. Servicen fortæller desuden administratorerne hvis nye enheder dukker op eller nye porte åbnes i de eksisterende enheder. SonicWall beskriver i de tilfælde, hvor sårbarheder findes i de valgte produkter hvordan disse tilrettes – enten med opdateringer eller ændringer til konfigurationen.

Tele3TZ produktet adskiller hjemmets private netværk fra hjemmearbejdspladsen ved at inkludere en stateful packet inspection firewall mellem de to interne netværk. En switch (dvs. en bridge som opererer på lag 2) leverer internetadgang til fire enheder. Der tillades kun VPN-adgang fra hjemmearbejdspladsen, men gives internetadgang til det resterende udstyr. Den fysiske opsætning kan ses på figur 16.



Figur 16- SonicWall's måde at segmentere hjemmenetværk på [31]

Som udgangspunkt er der givet adgang til, at hjemmearbejdspladsen kan tilgå enheder på det private net. Dermed kan fx printere og filer deles mellem netværkene. Der er ingen adgang fra det private net til hjemmearbejdspladsen, men disse regler kan konfigureres.
De to porte kan konfigureres individuelt. På denne måde kan der åbnes for, at hjemmets private udstyr kan tilgås udefra (som webserver fx) mens hjemmearbejdspladsen holdes helt aflukket. På samme måde kan reglerne om antivirussoftware mm. konfigureres separat.
Der kan gives båndbredde prioritering til fx hjemmearbejdspladsen, så det private udstyr ikke kan forhindre, at medarbejderen kan arbejde effektivt fra hjemmet. Hvis Tele3TZ-enheden benyttes som hardwarebaseret VPN-dialer kan der benyttes autentificering på brugerniveau, så adgang til hjemmearbejdspladsen ikke er nok til at etablere forbindelsen til virksomheden.

Fordele
CyberCity's løsning er baseret på et standardprodukt, som er ICSA-certificeret. Kombinationen af stateful packet inspection, hardwarebaseret VPN dialer samt muligheden for at benytte services som antivirus-kontrol, indholdsfiltrering og sårbarhedsscanninger kan hjælpe til at sikre et højt sikkerhedsniveau. Den unikke måde at separere hjemmets private netværk med hjemmearbejdspladsen, mens der stadig gives mulighed for at printere og andet udstyr kan deles, virker gennemtænkt.
CyberCity's politik omkring konfiguration og opdatering af produkterne giver mulighed for at virksomheden selv foretager ændringer – eller vælger at lade CyberCity sikre, at den forudbestemte konfiguration holdes ved lige.
Performancemæssigt kan løsningen håndtere ti gange så stor båndbredde, som i dag er tilgængeligt for hjemmebrugere. Da løsningen er kompatibel med VPN-produkter fra de store leverandører kan den skalere og integreres i virksomhedens eventuelt eksisterende VPN-miljø.
Løsningen afhjælper problemet med aflytning af trafikken mellem hjemmet og virksomheden ved brug af IPSec VPN. Hjemmearbejdspladsen beskyttes via den indbyggede stateful packet inspection firewall samt via sårbarhedsscanninger som skal sikre, at udstyret ikke kan angribes ved brug af kendte sårbarheder. Aktiviteter kan logges lokalt i udstyret og både log og konfiguration kan håndteres centralt vha. IPSec og SSH-forbindelser til udstyret.

Ulemper
Understøttelsen af 802.1x til autentificering af udstyret inden opkaldet foretages er desværre ikke til stede. Der er heller intet der forhindrer, at brugeren installerer programmer på PC'en, ligesom hardwarebaserede keyloggere ikke forhindres.

Konklusion
CyberCity's løsning indeholder ligesom TDC's ikke teknologi, der skal forhindre keyloggere og sniffere (se afsnit 3.1). Der bliver til gengæld gjort en indsats for at forhindre trojanske heste og virus i form at den antivirus-service, som produktet kan leveres med.
Idet der er sikret kompatibilitet med bl.a. Cisco-udstyr, kan stærk autentificering som OTP benyttes. Samtidig understøttes en hardwarebaseret IPSec VPN-forbindelse mellem hjemmearbejdspladsen og virksomheden med en tilfredsstillende performance. Hjemmet beskyttes af en stateful packet inspection firewall som kan opdateres centralt og analyseres for sårbarheder af leverandøren.
CyberCity's store fordel er den liberale politik omkring opdatering og konfiguration af udstyret, ligesom metoden til at segmentere hjemmets netværk er konkurrenterne overlegen.
Løsningen kan være et godt udgangspunkt for en virksomheds sikring af hjemmearbejdspladser og kompatibiliteten med andet standardudstyr kan sikre, at løsningen kan skalere efter behov.

4.3 Tiscali

Tiscali [25] udtaler:

"Vi har udviklet den optimale hjemmearbejdspladsløsning, hvor sikkerhed er taget alvorligt." Løsningsmodel nummer 4 beskrives desuden som: *"... uanset kravene til sikkerhed [...], kan Tiscali tilbyde en løsning, der til fulde matcher virksomhedens behov"*.

Ud over selve den tekniske løsning beskrives det, at Tiscali har eget netværk i Europa, så de kan sikre, at forbindelsen fra udgangspunkt til slutpunkt kontrolleres af dem. Fordelene ved dette kan fx være, at chancen for man-in-the-middle angreb samt snifferangreb kan betragtes som mindre sandsynlige, hvis kunden stoler mere på Tiscalis netværk end andre teleudbyderes netværk.

Teknikken
Tiscali's løsning er baseret på en Cisco Concentrator 3000 i virksomhedens ende (placeret bag en udefineret firewall, som Tiscali desværre ikke har ønsket at kommentere). I hjemmet har Tiscali fem forskellige løsningsmuligheder, men kun 2 af disse kan tilbyde muligheden for at segmentere hjemmets netværk. Disse adskiller sig fra de resterende ved at tilbyde en firewall og VPN dialer samt segmentering af hjemmearbejdspladsen og de resterende PC'er i hjemmet.

Figur 17 - FilaNet InterJak 200 [28]

Dette gøres ved at benytte en FilaNet Interjak 200 [28] router med to netkort som ses på figur 17. For at undgå problemer med deling af printere kan routeren agere printserver og dermed tillade udprintninger fra begge netværk.
FilaNet InterJak 200 er en danskudviklet, Linux-baseret enhed (benytter Embedded Linux med en 2.0.33 kernel). Den har været ICSA certificeret, selvom FilaNet måtte rette adskillige fejl i produktet for at opnå denne certificering. Denne certificering er dog nu trukket tilbage [29]. Firewall'en er en stateful packet inspection firewall med URL filtrering.
Med to USB porte og en FireWire port kan enheden benyttes som mailserver (en harddisk kan tilsluttes FireWire-porten), som printserver (printeren tilsluttes USB-porten) samt som VPN Concentrator, idet enheden kan terminere VPN-forbindelser. Enheden kan desuden segmentere to netværk så hjemmearbejdspladsen isoleres.
Da FilaNet er blevet overtaget af en amerikansk virksomhed (Uroam), har det ikke været muligt at skaffe yderligere oplysninger om hvordan enheden segmenterer hjemmenetværket eller mere detaljerede oplysninger om firewall'en. Tiscali har ikke ønsket at levere information om produktet eller deres hjemmearbejdspladsløsninger generelt.
VPN-delen af FilaNet routeren beskrives ikke af Tiscali, men bliver andre steder betegnet som med "limited performance"[114]. Da enheden reelt er en Linux-server beskrives det, at datatab i routeren kan forekomme, hvis den ikke lukkes ned korrekt.

Fordele
Med en stateful packet inspection firewall, VPN dialer og indbygget printserver giver løsningen gode muligheder for at etablere velfungerende hjemmearbejdspladser.
Administrationen af enheden kan foregå via SSH, hvilket giver mulighed for at foretage konfigurationsændringer fra virksomheden.

Ulemper
På trods af flere henvendelser, har Tiscali ikke ønsket at diskutere løsningen. Det har ikke været muligt at komme telefonisk igennem til en tekniker og e-mails afventer efter flere måneder stadig svar. Denne manglende vilje til at videregive information om løsningen er et stort problem for virksomheder, som ønsker et overblik over, hvordan det benyttede udstyr fungerer. Segmenteringen af hjemmets netværk er således ikke beskrevet af Tiscali, men det må forventes, at FilaNet benytter Linux' indbyggede muligheder for at foretage denne segmentering.
Selvom enheden kan opdateres fra virksomheden, lader der ikke til at være support for, at sådanne ændringer kan foretages i større skala. Således skalerer løsningen dårligt.
Brugen af en Linux-server som router giver mulighed for en stor række features, men som beskyttelse af hjemmearbejdspladsen er muligheder som at etablere en e-mailserver næppe fordelagtige. Samtidig kræver brugen af enheden som printserver, at FilaNet har udviklet printerdrivere til netop den printer, som skal benyttes. Da FilaNet ikke længere understøtter produktet, er det svært at forestille sig, at der kan benyttes nyere printere.
FilaNet InterJak 2000 oplyses ikke til at være kompatibel med andet udstyr, men overholder IPSec standarden for VPN og kan dermed benyttes sammen med fx en Cisco Concentrator, som Tiscali foreslår. VPN-ydelsen lader dog ikke til at være optimal.

Konklusion
Tiscali's løsning har flere problemer og ubesvarede spørgsmål end fordele. Brugen af en Linuxserver som router virker uhensigtsmæssig og klodset i forhold til mere fokuserede implementeringer. Der understøttes mange features baseret på Linux' muligheder. Fra et sikkerhedsmæssigt synspunkt er dette ikke fordelagtigt, da der således også er langt flere muligheder for angribere at benytte sig af.

Ideen med printserveren er god, men driversupporten er et problem, som formentligt vil gøre denne feature nytteløs. Segmenteringen af hjemmets netværk er svær at udtale sig om grundet manglen på informationer om produktet. Tiscali's manglende kommunikationsvilje kan alene være grund nok til ikke at vælge denne løsning. Den manglende mulighed for at konfigurere og opdatere et større antal produkter samtidig er en alvorlig hæmsko for skaleringen af løsningen.
Der er ikke understøttelse for at sikre hjemmearbejdspladsen mod virus, trojanske heste, keyloggers eller andet.
VPN-dialeren i enheden er reelt Linux' mulighed for at etablere udgående VPN-forbindelser via software, og manglen på hardwareacceleration giver efter sigende performanceproblemer for enheden.
Påtænkes denne løsning implementeret bør det tages med i overvejelserne, at ICSA-certificeringen er trukket tilbage, samt at produktet hverken sælges eller supporteres af producenten længere.

4.4 UNI-C

Forskningsnettet og tilhørende universiteter og organisationer udgør en speciel gruppe af brugere, som i et vist omfang har specielle behov. UNI-C har derfor udarbejdet en model som beskriver hvordan hjemmearbejdspladser kan implementeres i Forskningsnettet [30]. Et af de overordnede mål med modellen er at tilbyde en facilitet, som ikke udbydes af nogen anden teleudbyder og som er skræddersyet til forskningsmiljøet.
Modellen er bygget op omkring en centraliseret struktur, hvor alle hjemmearbejdspladser forbindes via UNI-C. Således laves autentifikationen her, ligesom VPN-forbindelserne termineres her. Fra UNI-C fortsætter trafikken ukrypteret til de forskellige universiteter, organisationer og institutter, som er tilkoblet Forskningsnettet. Således antages det, at Forskningsnettet er et sikkert system.

Teknikken
Selvom det ikke står klart i dokumentationen, indikeres det, at det er planlagt at distribuere profiler til de for Forskningsnettet interne firewalls, således at hjemmearbejdspladsbrugerne tildeles adgang til de dele af nettet, de tilhører. Hele infrastrukturen bygges op omkring Cisco PIX firewalls (model 501), Cisco routere og Cisco VPN-udstyr af forskellig type. En Cisco server (Cisco Secure ACS 3.0 for Windows) benyttes til at udsende opdateringer samt til at distribuere profilerne til det pågældende udstyr og en Cisco VPN Concentrator 3000 terminerer VPN-forbindelserne.
Modellen tager udgangspunkt i et samarbejde med TDC, hvor denne internetudbyder opsætter en Cisco DSL SOHO71 router i hjemmet og konfigurerer denne efter forudbestemte specifikationer. En software VPN-klient fra Cisco benyttes til at foretage opkaldet til UNI-C.
Der er lagt op til en alternativ model, hvor der i hjemmet i stedet benyttes en Cisco PIX 501. Ud over firewallfunktionaliteten tilføjes en hardwarebaseret VPN-løsning, så brugeren ikke længere skal installere software på sin hjemmearbejdsplads.

Fordele
Ved at lade alle Forskningsnettets brugere benytte det samme system, kan der "roames" på netværket. Dvs. skal flere forskere arbejde sammen, kan der gives adgang på tværs af systemerne også fra deres hjemmearbejdspladser, da de alle benytter det samme centrale system. Centraliseringen betyder også, at der ikke skal indkøbes (og vedligeholdes) dyrt VPN-udstyr på hvert institut.
Brugen af Cisco-produkter sikrer, at alle de forskellige enheder er kompatible. Samtidig opnås formentligt en betragtelig mængderabat. TDC's Cisco-løsning (som dog koster ca. tre gange så meget pr. måned som en standard ADSL-opkobling med samme båndbredde) hjælper til at få løsningen ud til brugerne uden at skulle involvere administratorer fra de forskellige universiteter eller UNI-C.

Ulemper
Centraliseringen af VPN-forbindelserne betyder, at trafikken fra UNI-C til de forskellige institutioner foregår ukrypteret. Samtidig kræver dette, at institutionerne åbner adskillige porte i deres (eventuelle) firewalls, så alle de services som skal tilbydes brugerne er tilgængelige.
Da der ikke stilles nogen krav til hjemmearbejdspladserne, vil disse være sårbare overfor næsten alle typer angreb inkl. trojanske heste, keyloggere osv. Benyttes den hardwarebaserede løsning med en Cisco PIX i hjemmet kan enhver, som opnår fysisk adgang til denne enhed, koble sig på Forskningsnettets såkaldte "sikre system". Da der i dokumentet lægges op til, at brugerne selv må bestemme hvilken type udstyr de placerer i hjemmet, er der også åbnet for muligheden for, at hele hjemmets private netværk kobles til PIX'en og videre igennem Forskningsnettet.

Konklusion
Løsningsmodellen er naturligvis udelukkende tiltænkt Forskningsnettets brugere. Ideen med centralisering af tilgangen til netværket er god ud fra et økonomisk og administrationsmæssigt synspunkt, men giver anledning til sikkerhedsmæssige problemer. Den manglende sikkerhed i hjemmene gør disse til åbenlyse angrebspunkter – dvs. som springbræt til Forskningsnettet.
Betragtningen af Forskningsnettet som sikkert er en meget stor antagelse, ligesom deres afhængighed af Cisco-udstyr kan være et problem.

Alt i alt er løsningen et udmærket udgangspunkt til videre udvikling af ideen med en centraliseret struktur til Forskningsnettet. Der bør dog lægges langt mere arbejde i sikringen af hjemmearbejdspladserne samt håndteringen af trafikken, efter VPN-forbindelsen termineres. Da modellen ikke fortæller noget om autentificeringsmetoder vil disse overvejelser ikke blive medtaget her. Dog skal det nævnes, at hvis databasen over brugere benytter samme brugernavne og passwords for fx DTU's brugere som benyttes på universitets andre systemer, må disse betragtes som kompromitterede allerede inden de benyttes. Dette skyldes muligheden for at angriberen kan hente hele passwordlisten for (i DTU's tilfælde) ca. 11.000 brugere. Gennemgangen af, hvordan dette gøres er beskrevet i [10].

4.5 Opsummering

Teleselskaberne i Danmark leverer løsninger, som primært baseres på sikring af trafikken mellem hjemmet og virksomheden. TDC har en meget stram politik omkring konfiguration og opdatering af de valgte enheder. Samtidig virker produkterne underdimensionerede i forhold til de båndbredder, som TDC selv sælger.
CyberCity har en mere åben politik omkring konfiguration og opdatering, og tilbyder ekstra services, som ud over selve trafikken også beskytter brugerens PC i områder, som konkurrenterne ikke dækker. Samtidig benyttes produkter, som skalerer godt, kan håndtere store hastigheder og som er kompatible med det mest udbredte netværksudstyr.
Tiscali's løsning benytter et danskudviklet produkt, som er baseret på Linux. Mulighederne i produktet er mange, men det er klart, at produktet ikke er designet til at sikre hjemmearbejdspladser. Med features som e-mailserver og harddisktilslutning er det uklart, hvilket marked produktet er tiltænkt, når der samtidig tilbydes segmentering af netværk og printerdeling. Kombineret med Tiscali's uvilje til at kommentere løsningen og skaleringsproblemet, virker løsningen ikke realistisk for sikkerhedsbevidste virksomheder.
UNI-C's løsning er specifikt designet til Forskningsnettet kan derfor ikke direkte sammenlignes med de øvrige. Der er dog mange sikkerhedsmæssige problemer i konceptet, som bør adresseres før løsningen overvejes.

5 OVERSIGT OVER UDBREDTE TEKNOLOGIER

Der findes en mængde teknologier og metoder, som i den rigtige implementering kan hjælpe til at modstå bl.a. de sikkerhedsproblemer, som blev nævnt i afsnit 3. I dette afsnit er det forsøgt at gennemgå nogle af de mest udbredte teknologier med henblik på, at disse sammen med andre senere kan danne grundlag for de ønskede designforslag til sikring af hjemmearbejdspladser. Hvor det har været muligt, er teknologierne afprøvet i praksis med udstyr lånt af leverandørerne.

Der er i afsnittet ikke tale om en fuldstændig liste over anvendelige teknologier og produkter. Valget er taget ud fra overvejelser om, hvordan de tidligere beskrevne sikkerhedsproblemer kunne løses baseret på standardprodukter, som er i bred anvendelse i dag. Overvejelser omkring kompatibilitet mellem produkterne bliver behandlet senere, men er et vanskeligt problem at tackle uden direkte adgang til det pågældende udstyr.

Afsnittet behandler teknologierne VPN, VLAN og VACL, 802.1x, firewalls, integritetssoftware, antivirus og anti-trojan programmer, honeypots, to-faktor autentificering, Citrix-software samt fjernstyring af arbejdsstationer.

5.1 VPN

VPN (Virtual Private Network) kan benyttes til at etablere sikre forbindelser over offentlige netværk fra eksterne lokationer som fx hjemmearbejdspladser til virksomhedens netværk. Trafikken kan krypteres, ligesom autentificering af brugere og udstyr kan implementeres på forskellige måder. Alternativet til VPN vil ofte være at benytte dedikerede linier, dvs. kommunikationsforbindelser, som etableres af teleselskabet mellem virksomheden og hjemmearbejdspladsen. Dette er en meget dyr og ufleksibel løsning.

VPN er et virtuelt, privat netværk. Webster's ordbog definerer "private" som:

"*of, belonging to, or concerning a particular person or group; not common or general*." [115]

Et privat netværk kan altså siges at være et netværk, hvor man har eksklusive rettigheder over kommunikationslinierne. Dette står i kontrast til det offentlige netværk, hvor ejerskab og betaling er fordelt blandt alle netværkets "beboere".
"Virtual" defineres i Webster's som:

"*being such practically or in effect, although not in actual fact or name.*" [115]

Et virtuelt netværk skal altså opføre sig som et netværk uden at være det. Dette kan oversættes til, at virtuelle netværk er on-demand netværk i modsætning til de dedikerede netværk, som leveres af teleudbyderne. On-demand netværk vil næsten altid være bygget ovenpå netværkslaget (de dedikerede netværk) idet netværksadministratorer sjældent vil have kontrol over det fysiske netværk udenfor bygningen.
Et virtuelt, privat netværk vil dermed være et netværk, hvor man har ejerskab over kommunikationslinen i et on-demand design, som er bygget ovenpå de eksisterende, dedikerede netværk fra teleudbydere, internetudbydere m.m. Dvs. en enhed kan koble sig på netværket på ethvert givet tidspunkt, blive så længe det ønskes og derefter koble sig af igen.
Måden at etablere VPN-forbindelser på er oftest ved at tunnelere IP inden i IP med et lag mellem de to, som leverer den nødvendige on-demand management. De mest udbredte teknologier til VPN kaldes L2TP (Layer 2 Tunneling Protocol) [41] og IPSec (IP Security).

5.1.1 Layer 2 Tunneling Protocol (L2TP)

L2TP er en udvidelse af Point-to-Point protokollen (PPP) og opererer ligesom PPP på data link laget (lag 2). L2TP er en kombination af Microsoft's Point-to-Point Tunneling Protokol (PPTP) [42] samt Cisco's Layer 2 Forwarding (L2F) protokol [43]. L2TP kræver naturligvis at routere som skal behandle pakkerne, understøtter protokollen.

Figur 18 – Postbilen som illustration for tunnelering [44]

L2TP indkapsler PPP frames i IP-pakker i en såkaldt tunnel. En tunnel kan groft sammenlignes med det at have en computer leveret af posten. Computerleverandøren pakker computeren *(passagerprotokollen, fx IPX, NetBeui eller IP)* ned i en kasse *(den indkapslende protokol, L2TP i dette tilfælde)* som så læsses på en postbil *(carrier protokollen, dvs. den protokol som benyttes på transportmediet). For internettet vil det normalt være en del af TCP/IP, men kunne også være GSM for mobilnettet)* ved leverandørens varehus (tunneleringens startsted). Postbilen kører via vejene (internettet) til ens hjem (tunneleringens slutsted) og afleverer computeren. Man åbner kassen og tager computeren op *(og har nu passagerprotokollen tilbage).*

L2TP leverer ikke sikkerhed i sig selv; dette kan enten klares ved at benytte IPSec i transport mode (se afsnit 5.1.2), eller ved at benytte den noget svagere sikkerhed i PPP.
Som L2TP-navnet angiver, tunneleres en link-layer (lag 2) protokol over fx IP. Dette giver mulighed for at benytte adskillige protokoller over et IP-netværk som fx IPX eller AppleTalk. L2TP er udviklet til brug i routere udenfor virksomheden, men nogle servere, routere og gateways understøtter protokollen.
Som det beskrives nedenfor kan protokoller, som opererer på lag 3 ikke give samme fleksibilitet som L2TP. Til gengæld er der andre fordele[30].

5.1.2 IPSec

IPSec [45] leverer sikkerhed på netværks-niveau til IP. Protokollen kan kryptere og/eller autentificere al trafik på IP-plan og operer på lag 3.
IPSec har tre primære funktioner: en autentificeringsfunktion kaldet Authentication Header (AH), en kombineret autentificerings-/krypteringsfunktion kaldet Encapsulating Security Payload (ESP) samt en nøgleudvekslingsfunktion.
AH og ESP understøtter to modes – transport og tunnel mode.

- Transport mode leverer sikring af de øverste protokollag. Dvs. transport mode beskytter dataene af en IP-pakke. Eksempler på dette kan være TCP og UDP segmenter som opererer over IP. I denne mode krypterer og autentificerer ESP dataene fra IP-pakkerne, men ikke selve IP-headeren. AH autentificerer dataene samt enkelte dele af IP-headeren.
- Tunnel mode leverer beskyttelse af hele IP-pakken. Efter AH eller ESP-felterne er tilføjet til IP-pakken, bliver hele pakken (samt sikkerhedsfelter) til data for en ny IP-pakke med en ny, ydre IP-header. Hele den oprindelige, indre pakke bevæger sig således igennem en ”tunnel” fra et sted i IP-netværket til et andet. Ingen routere eller andet udstyr undervejs kan analysere den indre IP-header. Fordi hele den oprindelige pakke er indkapslet, kan den nye, ydre pakke have helt andre kilde- og destinationsadresser. Det betyder, at tunnel mode kan benyttes til at forbinde en gateway med en anden hvorefter alle maskiner på hver side af de to gateways kan etablere sikre forbindelser til hinanden uden at implementere IPSec.
  I tunnel mode krypterer og autentificerer ESP hele den indre IP-pakke inklusive headerinformationer. AH autentificerer hele den indre pakke samt enkelte dele af den ydre pakkes IP-header.

IPSec kan således benyttes til at lave sikrede, on-demand netværksforbindelser, men forskellen mellem L2TP og IPSec er væsentlig: L2TP leverer on-demand netværk som understøtter sikkerhed, mens IPSec leverer sikkerhed, som understøtter on-demand netværk.
Med mindre der er krav om understøttelse af andre protokoller, er IPSec i de fleste tilfælde den foretrukne løsning. Denne sikrer både konfidentialitet, integritet samt autentificering. Autentificeringen foregår enten ved en delt nøgle eller digitale certifikater.

Delte nøgler kan være såkaldte ”wildcard” nøgler, dvs. nøgler som er ens for alle enhederne i VPN-opsætningen. Dette er let at implementere, men giver anledning til sikkerhedsproblemer, idet en stjålet enhed kan benyttes til at koble på netværket fra en anden lokation. Det skyldes, at man ikke med wildcard nøgler kan identificere dem med specifikke IP numre eller andre lokationsspecifikke identifikationsnumre. Samtidig er det ikke muligt at lukke af for nøglen hvis en enhed er kompromitteret, idet der så samtidig lukkes for adgangen for alle andre VPN-enheder, som deler samme nøgle.
Det er også muligt at benytte unikke- og gruppenøgler. Unikke nøgler er tilknyttet en bestemt enhed, og muligheden for at kombinere dette med identifikationsnumre som fx IP-nummeret er dermed muligt.
Uanset hvilken nøgletype der benyttes kan denne metode udsættes for et man-in-the-middle angreb, idet en kompromitteret nøgle kan benyttes til at autentificere VPN-enheden mod en falsk enhed.
Ud over dette skalerer metoden med unikke nøgler af naturlige årsager meget dårligt.
Digitale certifikater skalerer derimod langt bedre. Certifikaterne er ikke knyttet til et IP nummer, men er en unik, signeret information på enheden som er valideret af virksomhedens Certificate Authority (CA). Hvis en enhed er kompromitteret eller stjålet, kan administratoren annullere certifikatet og gøre alle andre enheder opmærksom på dette ved at opdatere en Certificate Revocation List (CRL). CRL’en indeholder en af CA’en signeret liste over annullerede certifikater. Når en enhed modtager en anmodning om at etablere en tunnel, checker enheden det certifikat, som er brugt til at bevise identiteten af den ”opkaldende” enhed mod CRL’en.

Et problem ned VPN-forbindelser kan være, at forbindelsen ikke kan oprettes, hvis det adressesubnet, som den opkaldende enhed benytter overlapper de netværksadresser, som virksomheden benytter internt. Det skyldes, at det er umuligt at afgøre hvilken enhed trafikken skal sendes ud til, når den samme adresse eksisterer på flere enheder.
Den anbefalede metode til at undgå dette er, at lade de tilkoblede enheder benytte afgrænsede subnets af virksomhedens netværksadresser. Fx kan en tilkoblet enhed benytte 10.1.1.0/24 (i alt 254 brugbare adresser, eller et privat klasse C net), hvilket er indeholdt i virksomhedens 10.0.0.0/8 netværk (et privat klasse A net) [31].

[30] Der er i afsnittet brugt information fra [44].
[31] Der er i afsnittet brugt information fra [46] side 677-683 samt fra [11].

5.1.3 Sikkerhedsovervejelser ved VPN

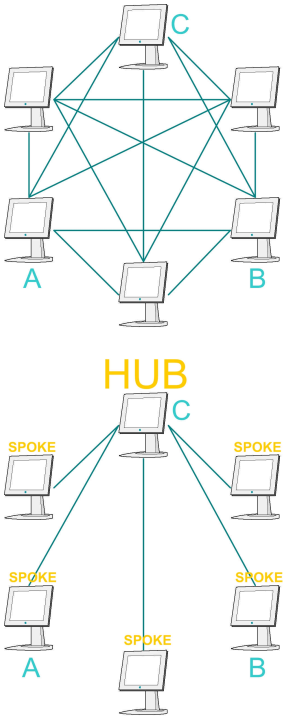
VPN kan levere autentificering og kryptering af private data over offentlige netværk som internettet. Sikkerheden baseres dermed på, at VPN-teknologien kan sikre dataene mod angreb, idet disse krypterede data sendes via offentligt tilgængelige netværk. Som det er vist i afsnit 5.1.6 nedenfor kan der være svagheder i implementeringen som kan sætte spørgsmålstegn ved den sikkerhed, som teknologien leverer.
Ved at tilkoble eksterne lokationer som hjemmearbejdspladser til virksomhedens netværk vha. VPN udvides antallet af mulige tilgangspunkter. Samtidig er disse nye tilgangspunkter ofte ikke fysisk sikret på samme måde som virksomhedens bygninger. Det vil derfor ofte være nødvendigt, at betragte VPN-forbindelsespunkterne som mindre sikre end virksomhedens centrale netværk – både fysisk, men også overfor angreb fra internettet.

Det kan være relevant at overvåge trafikken fra disse forbindelser med Network Intrusion Detection Systemer (NIDS'er). For det første kan en NIDS analysere trafikken, som kommer til og fra VPN-enheden. Dvs. den kan detektere angreb, som kommer fra de steder, som er tilkoblet virksomheden via VPN. For det andet kan en NIDS benyttes efter krypteringen til at validere, at kun krypteret trafik sendes og modtages af VPN-enhederne.

Ud over brugen af NIDS'er, bør Access Control Lists (ACLs) benyttes. På den offentlige side af VPN-enheden i virksomheden kan der med fordel placeres en router, som via filtre sikrer, at kun IPSec trafik slipper igennem. Der er ingen større fordel i at placere en firewall på dette sted, da stateful packet inspection og andre funktionaliteter ikke kan benyttes på krypteret trafik.
Firewall'en kan i stedet med fordel placeres bag VPN-enheden i virksomheden. Her kan den både benyttes til at lave brugerautentificering samt til at sikre, at kun tilladte protokoller passerer videre til virksomhedens netværk. Avancerede funktionaliteter i firewall'en kan benyttes, idet trafikken på dette punkt er dekrypteret.

En anden sikkerhedsovervejelse er fragmentering af VPN-pakkerne. Fragmenterede IPSec pakker skal samles før de kan checkes for integritet og dekrypteres. Dette betyder, at fragmenterede pakker kan eksistere på netværket uden at være blevet checket, ligesom det kræver store CPU- og hukommelsesressourcer at håndtere store mængder fragmenterede pakker. Dette bør derfor undgås.
Fragmentering opstår, når pakkerne er for store i forhold den mindste tilladte pakkestørrelse, der eksisterer i tunnelens rute igennem netværket. Dette undgås normalt ved at tillade ICMP (Internet Control Message Protocol) beskeder, som så vil benytte Path Maximum Transmission Unit Discovery (PMTUD) til at afgøre, hvad den største, tilladte pakkestørrelse er, og benytte denne.

5.1.4 Infrastruktur



Figur 19 - Fully og partially meshed (øverst) samt Hub and Spoke (nederst)

Der eksisterer typisk tre forskellige opbygninger af en VPN-infrastruktur. Disse er Fully Meshed, Partially Meshed og Hub and Spoke og er vist på figur 19. Fully Meshed netværk er opbygget, så alle VPN-enheder har forbindelse til alle andre VPN-enheder direkte. Et sådant net har den fordel, at trafik fra punkt A til B, ikke skal igennem C. Til gengæld skalerer netværket meget dårligt. Det kræver $\frac{n(n-1)}{2}$ tunneller, hvilket vil sige 1225 tunneler, hvis fx 50 enheder skal forbindes. Dette sætter enorme krav til VPN-enhedernes datakraft, ligesom kompleksiteten når en ny enhed skal tilføjes er meget stor.
Partially Meshed netværk skalerer bedre, idet forbindelser mellem enhederne kun oprettes, når der er behov for dem. Der er dog stadig store problemer ved at vedligeholde sådanne netværk, ligesom det er svært på forhånd at vide, hvor mange samtidige VPN-forbindelser enhederne skal kunne håndtere.
Hub and Spoke netværk skalerer bedst, idet kun virksomhedens "VPN-hub" skal udvides, når der tilføjes nye enheder. Ulempen er dog, at al trafik skal igennem denne hub, hvilket sætter meget store krav til båndbredden.

5.1.5 Hardware og software VPN klienter

Etableringen af en VPN-forbindelse kan ske enten via software eller via en dedikeret hardwareenhed, som fx en VPN dialer, en VPN firewall eller en VPN router. Softwareløsningen giver fleksibilitet, idet brugeren kan befinde sig hvor som helst og benytte VPN-forbindelsen fra sin bærbare computer. Til gengæld skal brugeren aktivt være involveret i etableringen af VPN-forbindelsen, ligesom det er muligt at benytte internetforbindelsen uden brug af VPN, hvilket set fra et sikkerhedsmæssigt synspunkt kan være et problem.

Ved at benytte en hardwarebaseret enhed til etableringen af forbindelsen, bliver denne transparent for brugeren. VPN-enheden autentificeres op mod virksomhedens VPN Concentrator fx ved hjælp af digitale certifikater. Er der tale om en sikker brugerlokation, kan yderligere autentificering undgås, men under normale omstændigheder vil

brugervalidering herefter foregå enten med passwords eller to-faktor autentificering. Dette kan desuden kombineres med brugen af autentificering på lag 2 (802.1x, se afsnit 5.3).

5.1.6 Svagheder

Kryptering af trafikken ved hjælp af VPN er ikke uden videre en garanti for datasikkerhed. I 1998 brød Bruce Schneier Microsoft's PPTP implementering [47]. Samtidig blev det vist, hvordan en PPTP server kan spoofes, hvorved autentificeringsinformationer kan opsamles.
Selvom disse angreb kun er beregnet på PPTP og ikke IPSec, er sidstnævnte heller ikke uden problemer. Schneier har sammen med Ferguson Weigh senere analyseret IPSec-standarden, og deres udtalelse var følgende:

"*In our opinion, IPSec is too complex to be secure*" [47]

De tilføjer dog, at standarden er bedre end nogen anden, som findes i dag.

Angreb mod selve implementeringen er dog ikke VPN's eneste svage punkt. Sikkerheden omkring VPN afhænger ikke kun af hvordan systemet sammensættes, men i høj grad også af, hvordan det bagefter benyttes af brugerne. Benyttes delte nøgler til autentificeringen og skriver brugerne deres passwords ned og hæfter sedlen til skærmen, er der kun en glasrude til at holde angriberne væk fra virksomhedens centrale servere.
Men selv ved mere gennemtænkte installationer med digitale certifikater og sikkerhedsbevidste brugere, kan VPN ikke stå alene for sikkerheden. Hvis en trojansk hest finder vej til en arbejdsstation, kan angribere i visse tilfælde se med "over skulderen" på den legitime bruger – og alene skærmbilleder kan være nok til, at virksomhedens vigtigste aktiver går tabt.[32]

5.2 VLAN

Nogle switche benytter en teknologi kaldet VLAN (Virtual LAN). VLANs tillader netværksadministratorer at opdele deres fysiske netværk i mindre, logiske netværk. Ligesom et fysisk netværk er hvert af disse logiske netværk (VLANs) adskilt fra de øvrige, så broadcasts ikke overlapper. Denne adskillelse foregår i lag 2 og fungerer ved, at hver pakke bliver tildelt en identifikationsheader, som sikrer, at pakkerne kun kan modtages på de porte, som er en del af det pågældende VLAN. De to mest udbredte metoder til at udføre dette er 802.1q og Cisco's Inter-Switch Link (ISL) header.
VLANs kan benyttes til at opdele store netværk i mindre for at håndtere mængden af broadcasts. Samtidig betyder opdelingen i VLANs, at trafik fra ét VLAN til et andet forhindres (med mindre routere tillader dette). Dette kan benyttes som et ekstra lag af sikkerhed, således af netværket kan opdeles i segmenter på hvert sit VLAN, som herefter kun kan kommunikere, hvis en router tillader dette. Men det bemærkes, at alle pakker mellem VLANs skal routes, hvilket kan give performanceproblemer. Samtidig kan VLAN-teknologien alene ikke kontrollere kommunikationen indenfor hvert VLAN.

I modsætning til VLANs, hvor alle maskiner på samme VLAN som nævnt kan tale med hinanden kan der indføres Private VLANs (PVLANs). PVLAN er en teknik som tillader portisolering indenfor samme VLAN. Kombineret med VACLs (se afsnit 5.2.2) kan PVLANs bl.a. benyttes til at etablere en trust model i et switchet netværk.

5.2.1 PVLAN

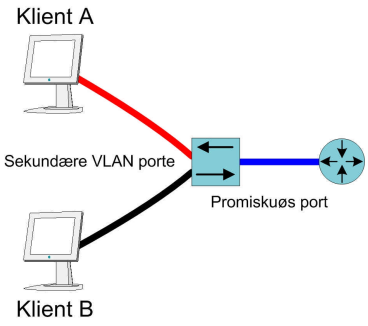
PVLANs er udviklet for at gøre det muligt at håndhæve regler om, at visse maskiner indenfor samme VLAN (samme broadcast domæne) ikke må kunne tale sammen. Baggrunden for dette kunne være en simpel DMZ-opsætning, hvor serverne er placeret på et DMZ-ben. Hvis en af disse servere kompromitteres kan denne server benyttes som base for angreb mod de andre servere. Lignende eksempler kan findes på selve LAN-delen af netværket, hvor det måske ikke er ønsket, at arbejdsstationerne kan etablere forbindelse mellem hinanden, men kun til routere, gateways og proxyservere. PVLANs kan her benyttes til at adskille maskinerne således at serverne i DMZ'en kun kan kommunikere med gateway'en men ikke med hinanden.

En port på en switch, som benytter PVLANs, kan konfigureres på tre måder:

- **Promiskuøs**. En promiskuøs port kan videresende trafik fra enhver port inkl. isolerede og kollektive porte indenfor et PVLAN.
- **Kollektiv**. En kollektiv port kan videresende trafik til en promiskuøs port eller en port tilhørende samme kollektiv og kan ligeledes modtage trafik fra samme.
- **Isoleret**. En isoleret port kan kun videresende trafik til promiskuøse porte og kan ligeledes kun modtage trafik fra promiskuøse porte.

[32] Der er i afsnittet om VPN benyttet informationer fra [1], [48] side 399 – 440 samt [47] side 383 til 389.

Disse typer går også under andre navne. Således kaldes promiskuøse porte for primære VLANs mens kollektive og isolerede porte kaldes sekundære VLANs. Normalt vil et PVLAN kun have ét primært VLAN men mange sekundære VLANs.
Generelt kan det siges, at en enhed sender trafik på sekundære VLANs og modtager trafik på primære VLANs samt (i forbindelse med kollektive VLANs) på sekundære VLANs.
I eksemplet med en DMZ ville gateway'en (fx en router eller firewall) være tilsluttet en promiskuøs port og serverne ville være tilsluttet isolerede porte. Dette ville tillade eksterne og interne arbejdsstationer at etablere forbindelse til serverne mens disse ikke indbyrdes ville kunne kommunikere. Hvis behovet opstår for, at fx en webserver skal kommunikere med en databaseserver i DMZ'en, kan disse to tildeles porte, som er en del af samme kollektiv. Så længe ingen andre maskiner tildeles porte tilhørende samme kollektiv kan disse to maskiner nu kommunikere uden at der kan kommunikeres til eller fra de resterende servere i DMZ'en.

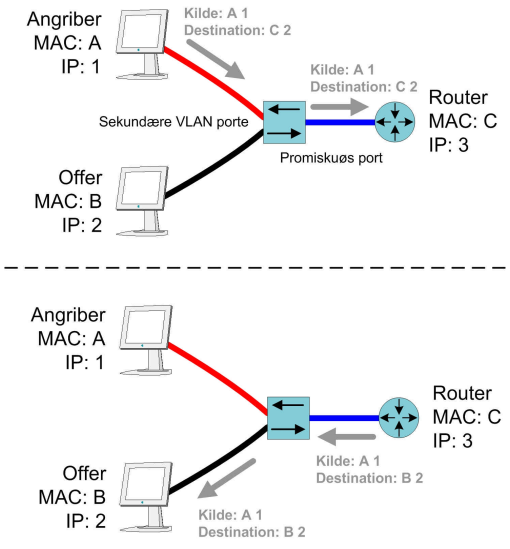


Figur 20 – PVLANs

Et eksempel på dette er vist på figur 20.
Her er den primære VLAN i blå og de sekundære VLANs er i rød og sort.
Klient A er tilsluttet en port på switchen som tilhører det sekundære VLAN i rød mens klient B er tilsluttet en port på switchen, som tilhører det sekundære VLAN i sort.
I dette eksempel vil man tilslutte routere og firewalls til promiskuøse porte, idet disse kan videresende trafik som kommer fra ethvert sekundært og primært VLAN. De porte som hver arbejdsstation er tilknyttet, kan kun videresende trafik, som kommer fra det primære VLAN eller fra det sekundære VLAN, som arbejdsstationen er tilknyttet.

Brugen af PVLANs kan hjælpe til at undgå den trust udnyttelse, som er beskrevet i afsnit 3.2. På samme måde kan PVLANs hjælpe til at sikre, at kompromitterede enheder ikke kan angribe andre enheder, ligesom det kan sikres, at legitime brugere med uhensigtsmæssige hensigter ikke kan tilgå andre enheder end dem, de bør have adgang til ifølge deres jobspecifikation.

Der er nogle problemer forbundet med brugen af PVLANs. For at distribuere VLAN informationer mellem Cisco switche benyttes VLAN Trunking Protocol (VTP). Formålet er at undgå at skulle konfigurere alle switche enkeltvist samt at sikre, at VLANs kan spænde over flere switche. Hvis PVLANs benyttes, skal switchen sættes i transparent VTP mode. Kort fortalt betyder dette, at switchen ikke kan modtage VTP-informationer og derfor ikke kan medvirke i et VTP domæne. Dette kan give nogle skaleringsproblemer i store netværk.
Der er desuden nogle sikkerhedsmæssige overvejelser forbundet med brugen af PVLANs. Ved at benytte en router kan sikkerheden i PVLANs til dels omgås. På figur 21 ses illustrationen af et sådant angreb. Angriberen afsender en pakke med korrekt afsenderadresse (både IP og MAC betegnet som A 1) samt korrekt modtager IP-adresser (2). Men i stedet for modtagerens MAC-adresse benyttes routerens MAC-adresse (C). Switchen vil videresende pakken til routerens port i switchen. Routeren vil så overskrive MAC-adressen med den korrekte MAC-adresse til modtageren og sende pakken tilbage til switchen. Switchen ser nu en pakke med det korrekte format, som kommer fra en promiskuøs port og sender pakken til modtageren, hvorved sikkerheden i PVLAN er brudt. Angrebet tillader dog kun envejskommunikation idet modtageren af pakken ikke kan svare tilbage da dette blokeres af switchens PVLAN-regler. Sikkerhedsproblematikken opstår, fordi PVLAN er en teknik som opererer på lag 2 og ikke lag 3. Dermed kigges der udelukkende på MAC-adresser, hvor en teknik på lag 3 ville kigge på IP-headeren.



Figur 21 - Sikkerhedsproblem med PVLANs

Forsvaret mod sådanne angreb kan baseres på brugen af Access Control Lists (ACLs) eller VLAN Access Control Lists (VACLs) på routeren. En beskrivelse af denne teknologi kan ses nedenfor, hvor PVLANs og VACLs relationen til hjemmearbejdspladser også vises[33].

5.2.2 VACL

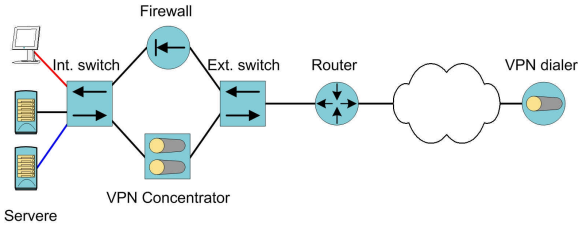
VACL (VLAN Access Control List) er en måde at filtrere trafik indenfor et VLAN. VACL udføres før almindelige ACLs og kontrollerer trafik på lag 2 (bridged trafik). Forskellen mellem ACL og VACL er, at ACL filtrerer pakker som går til routeren (fx inter-VLAN trafik) mens VACL filtrerer alle pakker som går gennem switchen, inkl. intra-VLAN trafik.

[33] Der er i afsnittet brugt information fra [32] og [34]

PVLANs kan udvides til at inkludere VACLs (VLAN Access Control Lists). Benyttes denne kombination, er det muligt at filtrere trafik på baggrund af trafikkens retning. Dette kan igen benyttes i situationen, hvor servere er placeret i en DMZ. Her skal serverne besvare indkomne forespørgsler, men serverne må ikke selv initiere forbindelser ud. Sidstnævnte kan være en indikation på et DoS-angreb. Ved at benytte PVLANs og VACLs kan man sikre, at disse serveres udgående pakker blokeres. Selvom dette allerede kan gøres i firewalls og i visse tilfælde i routere, er fordelen ved denne teknologi, at det foregår med wire speeds, dvs. uden hastighedstab.

Som tidligere omtalt kan problemet med at benytte en router til at omgås PVLAN-regler løses ved at benytte VACL. Ideen er, at det primære VLAN ignorerer trafik som kommer fra det samme subnet der ønskes routet tilbage til.

PVLANs og VACLs kan benyttes i forbindelse med hjemmearbejdspladser ved at kombinere disse teknologier med VPN. Et eksempel på dette kan ses på figur 22.



Figur 22 - PVLAN, VACL og VPN kombineret [35]

Her er en VPN Concentrator placeret parallelt med en firewall. Denne opsætning er populær, idet den er let at implementere og fordi den ikke kræver større ændringer til den eksisterende infrastruktur.
VPN-sessionerne ender i VPN koncentratoren, og normalt vil VPN-brugeren herefter have fuld adgang til det interne netværk. Der kan dog være situationer, hvor man kun ønsker at give VPN-brugerne adgang til en serverfarm eller andet. Det vil desuden i visse tilfælde være fordelagtigt at opdele VPN-trafikken og den normale internettrafik for fx at undgå, at VPN-brugerne tilgår internettet via virksomhedens firewall (split tunneling).

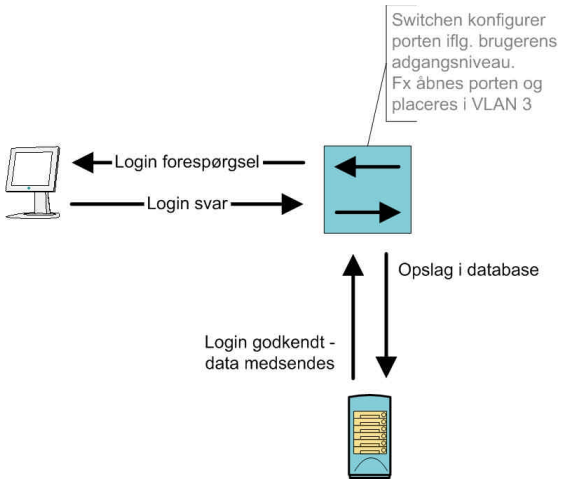
Ved at benytte PVLANs og VACLs kan der i denne opsætning laves regler som sikrer, at VPN-brugerne ikke kan tilgå internettet via virksomhedens firewall, mens man stadig sikrer, at de interne arbejdsstationer kan. Samtidig sørges for, at VPN-brugerne kun kan tilgå en bestemt serverfarm på det interne netværk, men forbydes adgang til det resterende LAN. Ud over tilgangen fra hjemmet via hardware VPN dialere, benyttes switche med VLAN, VPN koncentratorer og servere placeret på DMZ-ben. Ved at konfigurere switche, routere og firewalls kan brugernes adfærd kontrolleres, og regler for hvilke maskiner og brugere, der må tilgå hvilke ressourcer, kan håndhæves. Samtidig kan man sikre, at kompromitterede maskiner på det interne netværk eller i hjemmet ikke kan benyttes som springbræt til angreb mod hele virksomhedens resterende maskinpark[34].

5.3 802.1x

Det kan i visse netværksopsætninger være ønskeligt at sikre, at alle netværksporte er "låst" så det ikke er muligt at modtage eller sende trafik uden autentificering. Således vil et ledigt netværksstik i væggen (eller i hjemmene) ikke give adgang til netværket, før brugeren eller udstyret er autentificeret. På denne måde kan mange typer angreb modarbejdes allerede før angriberen får adgang til netværket. I forbindelse med hjemmearbejdspladser kan det i så fald sikres, at kun den godkendte arbejdsstation kan kobles til netværksudstyret i hjemmet.
En teknologi til at understøtte dette er 802.1x som opererer på lag 2. I udstyr hvor dette er implementeret og aktiveret overføres autentifikationsinformationer i form af Extensible Authentication Protocol (EAP). På denne måde bliver udstyret (som regel en switch) mellemmand for at videresende EAP modtaget i 802.1x pakker videre til en autentifikationsserver ved at benytte RADIUS (Remote Authentication Dial In User Service) til at overføre EAP informationerne. EAP kan bestå af følgende:

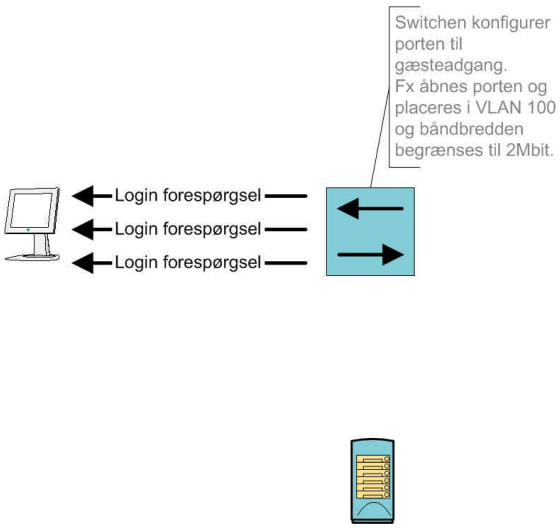
- EAP-MD5 som er MD5 hashede brugernavn/password informationer
- EAP-OTP som er One Time Passwords
- EAP-TLS som er PKI via SSL (TLS)

På figur 23 ses et eksempel på, hvordan 802.1x autentificering kan foregå. Brugeren har sat sin PC til et vilkårligt netværksstik i virksomheden. Switchen beder om identifikation via en af ovenstående EAP-metoder. Brugeren svarer tilbage og disse informationer kontrolleres via RADIUS. Sammen med godkendelsen af brugeren følger informationer om, hvilket VLAN brugeren skal tilkobles. Switchen konfigureres til dette på den pågældende port, hvorefter brugeren får den adgang til netværket, hans konto tillader.



Figur 23 - 802.1x autentificering af gyldig bruger

[34] Der er i afsnittet benyttet informationer fra [35]



Figur 24 - Gæsteadgang via 802.1x

Brugen af 802.1x kræver, at både netværksinfrastrukturen og arbejdsstationer, bærbare PC'ere osv. understøtter teknologien. Det kan derfor være et problem hvis en gæst eller udefrakommende ønsker at benytte netværket, men enten ikke har en konto eller ikke har udstyr, som understøtter 802.1x. I sådanne tilfælde kan virksomheden vælge at give en speciel gæsteadgang til netværket.

Et eksempel på, hvordan det kan foregå ses på figur 24. Brugeren tilslutter sin PC hvorefter switchen beder om identifikation. Da brugerens udstyr ikke genkender denne forespørgsel, ignoreres den. Efter en bestemt ventetid tildeler switchen en forudbestemt karantæneindstilling til porten. Denne kan fx inkludere et isoleret VLAN (i eksemplet med ID 100), båndbreddebegrænsninger med mere.
Ved en hjemmearbejdsplads kan denne teknologi benyttes til at foretage autentificering allerede inden der etableres forbindelse til virksomhedens netværk ved at udføre 802.1x autentificering på den router eller VPN dialer som benyttes i hjemmet. Dette giver et lag af sikkerhed, som beskytter virksomhedens opkaldspunkter yderligere da kun brugere som fra hjemmene allerede er autentificeret via 802.1x kan forsøge at angribe eventuelle VPN-systemer fra disse enheder[35].

5.4 Firewalls

Firewalls har fået ry for at være et universalmiddel for stort set alle sikkerhedsproblemer. Det er de ikke. De er blot endnu et værktøj til opbygning af sikkerhedssystemer. Cisco beskriver firewalls således:

"*The primary function of a firewall in a network is to prevent simple unauthorized access attacks*" [49].

Firewalls hjælper til at kontrollere den type og mængde trafik som passerer fra et netværkssegment til et andet. En firewall har således tre primære funktioner. Den skal sikre, at al trafik indefra og ud – samt omvendt – passerer igennem denne. Samtidig skal den sikre, at kun tilladt trafik passerer. Desuden skal firewall'en i sig selv være immun overfor de angreb, den beskytter imod.

Der er dem som mener, at en firewall giver en falsk sikkerhed og i princippet ikke bør benyttes [50]. Argumentationen er, at en firewall bygger på princippet om, at man har kontrol over de tilgange, der er til netværket. Dette er sjældent tilfældet. Er det fx sikret, at den telefonlinie, som hver medarbejder har, ikke er forbundet til et modem? Kan man være sikker på, at ingen uautoriserede personer (inkl. ansatte) kan opnå adgang til interne computere, netværksudstyr osv.? Er den fysiske sikkerhed på højde med den elektroniske – dvs. kan folk på nogen måde opnå fysisk adgang til nogen former for beskyttet data?
Blot fordi den primære, elektroniske fordør til virksomheden er beskyttet, bør dette ikke give anledning til at tro, at netværket er sikret.
Med dette i baghovedet kan der dog alligevel være mange gode grunde til at implementere firewalls i virksomheden. En kendt metafor siger, at en firewall er som at have et hegn rundt om sit hus med en låge i forhaven mens en indbrudstyv står udenfor og rusker i tremmerne. Det kan godt være han kan komme over hegnet eller gennem lågen, men det ville være dumt ikke i det mindste at *have* hegnet og lågen.

En firewall vil ofte findes i forskellige varianter alt efter hvilken funktion den skal udfylde. De fire mest udbredte varianter er vist nedenfor:

- Packet-filtering router (pakkefiltre)
- Circuit-level gateway
- Application-level gateway
- Stateful, multi-layer inspection firewall

Fælles for de fire typer er, at de som regel vil benytte et hærdet operativsystem, som ikke umiddelbart er sårbart overfor de angreb, som enheden er designet til at beskytte imod.

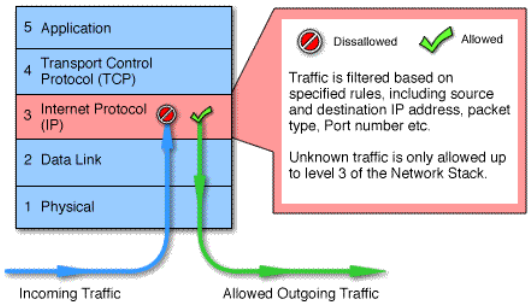
I forbindelse med afsnittet som firewalls anvendes TCP/IP-modellen i stedet for OSI-modellen til at beskrive, på hvilke lag de forskellige typer fungerer. Den tætte forbindelse til de forskellige TCP/IP-protokoller gør, at TCP/IP-modellen giver et bedre overblik over sammenhængen mellem de fire typer. I ordbogen er gennemgået sammenhængen mellem OSI- og TCP/IP-modellerne.

[35] Der er i afsnittet brugt information fra [36].

De fire typer fungerer alle på forskellige lag. Således fungerer et pakkefilter på lag 3 (netværkslaget), en circuit-level gateway på lag 4 (transportlaget) og en application-level gateway på lag 5 (applikationslaget). En stateful, multi-layer inspection firewall fungerer – som navnet siger – på mange lag, ofte alle lag fra 3 til 5.
På lag 3 kan en firewall afgøre om en pakke er fra en bestemt afsender, men den kan ikke afgøre hvad pakken indeholder eller hvordan den er relateret til andre pakker. På lag 4 kendes er lidt mere til pakken og denne kan afvises eller godkendes afhængigt af fx protokoltypen. På lag 5 kan firewall'en se på hele indholdet af pakken og dermed foretage en mere detaljeret analyse af denne før det afgøres, om den skal godkendes eller ikke.
Det kan dog ikke fra ovenstående uden videre antages, at jo højere lag firewall'en opererer på, jo bedre. Faktisk er firewall'en sikrere jo lavere et lag pakkerne stoppes på. Dette skyldes, at hvis en pakke kan stoppes på lag 3, er der ingen chance for, at pakken kan angribe de services, som afvikles på de højere lag. Problemet er naturligvis, at det det ikke er muligt at stoppe alle ondsindede pakker på de laveste lag, hvorfor application-level gateways har deres eksistensberettigelse. Hellere stoppe pakken på lag 5 end slet ikke at stoppe den.

I nedenstående gennemgang af de fire typer firewalls er for hver vist en figur, som indikerer hvilket lag enhederne arbejder på, samt hvordan det afgøres, om pakkerne skal tillades eller afvises. Disse figurer kan benyttes til at få et overblik over, hvordan de fire typer adskiller sig fra hinanden. Figurerne er fra [107].

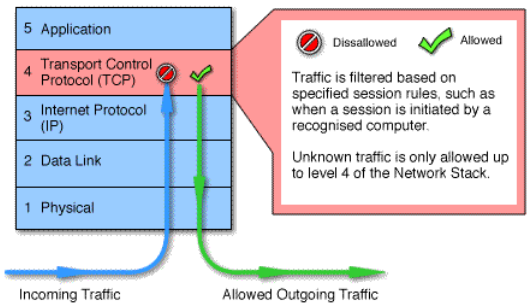
5.4.1 Packet-filtering router



Figur 25 - Packet-filtering router

En packet-filtering router har som minimum mulighed for at opstille et sæt regler, som indkommende (og i visse tilfælde udgående) IP pakker stilles overfor. Reglerne baseres typisk på felter i IP pakkerne som fx afsender og modtagerinformation, portnumre med mere. Der vil desuden være en standardregel som følges, hvis ikke en pakke hører under andre regelsæt. Her kan administratoren vælge mellem "alt hvad der ikke er tilladt afvises" eller "alt hvad der ikke afvises er tilladt". Førstnævnte er den sikreste metode, idet nye trusler, som fx benytter hidtil ubenyttede porte, automatisk afvises. Til gengæld er den sidste metode den absolut letteste at implementere, idet man er sikret, at alle funktioner i netværket fungerer allerede før konfigurationen påbegyndes.
Der er mange faldgruber i implementeringen af filtersystemer. Fx kan spoofing af afsenderadresser ofte medføre, at udefrakommende pakker, som skulle have været afvist, alligevel bliver tilladt. Dette sker fordi et filter tillader alle pakker med en afsenderadresse fra det interne netværk at passere. Løsningen er et checke, hvor pakken kommer fra – dvs. kontrollere, om pakken kommer fra det eksterne eller interne netværk. Herefter krydscheckes dette med de godkendte adresser. På den måde vil pakker med en intern adresse ikke tillades, hvis de kommer fra det eksterne netværk.
Et andet problem med pakkefiltreringen kan være angribere, som vælger at specificere hvilken rute pakkerne skal tage på vej mod firewall'en. På den måde kan de vælge det sidste hop til at være et sted på det offentlige net, som firewall'en stoler på. Dette kan fx være en ekstern afdeling af virksomheden eller en hjemmearbejdsplads. Dette kan løses ved at afvise alle pakker, hvor ruten er forudspecificeret.
Packet-filtering routere kigger udelukkende på headerinformationer og ikke på de data, som er indeholdt i pakkerne. Idet pakkefiltrering alene foregår på lag 3, kan ondsindet kode gemme sig i de øvre lag uden at blive detekteret. Da der samtidig er tale om, at hver pakke som passerer routeren skal checkes mod de filtre, som routeren indeholder, kan der i større netværk være et skaleringsproblem.
Packet-filtering er en 20 år gammel, men velafprøvet teknologi. Et produkteksempel er en Cisco 2500 serie router.

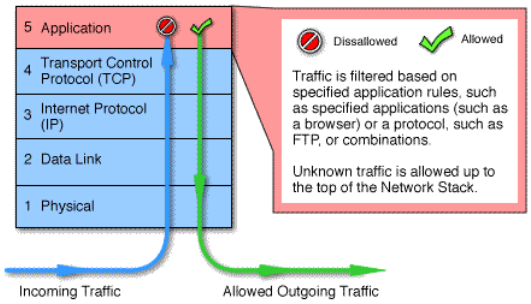
5.4.2 Circuit-level gateway



Figur 26 - Circuit-level gateway

En circuit-level gateway opererer på lag 4 og tillader ikke direkte end-to-end forbindelser. I stedet for oprettes to forbindelser – en mellem gateway'en og brugeren på det indre netværk og en mellem gateway'en og den eksterne bruger eller maskine. Når disse to forbindelser er etableret, videresender gateway'en segmenter fra den ene forbindelse til den anden uden at undersøge indholdet. Forbindelsen bliver dog valideret i den forstand, at kun tilladte trafiktyper slippes igennem. Idet gateway'en oprerer på lag 4 kan der ud over IP-adresse og portnumre også checkes for protokoltype.
Den store ulempe med circiut-level gateways er, at det kræver speciel opsætning af brugernes software. Samtidig er der de samme svagheder som ved en packet-filtering gateway, idet ondsindet data kan gemmes i de højere lag (fx applikationslaget).
Et eksempel på en circuit-level gateway er en SOCKS-baseret gateway [51].

5.4.3 Application-level gateway (ALG)

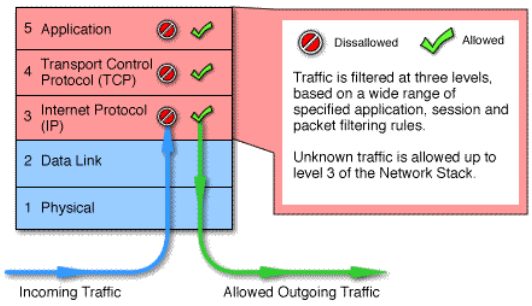


Figur 27 - Application-level gateway

En application-level gateway (også kendt som en proxy) undersøger i modsætning til packet-filtering routere al data i en pakke. Den opererer i applikationslaget og overvåger de informationer, som føres igennem den for at sikre, at denne information er acceptabel i henhold til virksomhedens politik om tilladt trafik samt applikationernes specifikationer.
Forskellen på en circuit-level gateway og en ALG er, at ALG'en forstår applikationens protokol, mens circuit-level gateway'en forstår IP-protokollen.

Der er tale om, at applikationstrafikken videresendes. Dette fungerer ved at brugeren kontakter gateway'en via en applikation som fx et FTP-program. Gateway'en beder applikationen om adressen på den server, som skal kontaktes og beder dernæst brugeren om autentificering. Gateway'en kontakter serveren og videresender TCP segmenter som indeholder applikationsdata mellem serveren og brugeren. Det er dermed muligt for administratoren at bestemme, hvilke applikationer, der kan benyttes eller hvilke dele af en applikation, som må få adgang til internettet. Samtidig kan gateway'en kontrollere, at de data, som sendes tilbage, kun indeholder den type data, som brugeren har bedt om.
Den store ulempe ved denne type beskyttelse er, at alle applikationer skal være designet til – og sat op til – at bruge systemet. Det er dermed ikke transparent for brugeren, ligesom løsningen skalerer dårligt, idet der kræves store ressourcer for at behandle trafikken.
Oftest vil en application-level gateway være applikationsspecifik. Et eksempel er derfor en web (http) proxy. Fordelen ved ALGs er, at det er muligt for enheden at forstå specifikke protokoller. Således kan fx en ALG designet til FTP forstå forskellen på "put" og "get" kommandoer. En virksomhed kan derfor tillade, at brugerne henter filer via FTP, men ikke at de sender filer ud af huset via denne protokol. Denne type sikkerhed kan ikke opnås ved brug af packet-filtering routere eller circuit level gateways.

5.4.4 Stateful, multi-layer inspection firewall



Figur 28 - Stateful, multi-layer inspection firewall

Stateful packet inspection blev opfundet af CheckPoint Software Technologies Ltd. i 1993. Groft sagt holder en stateful packet inspection firewall styr på, hvilke forbindelser pakkerne tilhører og i hvilken tilstand (state), de er.
Disse firewalls ser på den tilstandsinformation, som er inkluderet i TCP pakkerne. Den første pakke i enhver ny forbindelse har et SYN flag sat og et ACK flag fjernet. Disse pakker kaldes startpakker. Alle pakker i samme serie, som ikke har denne struktur, er "efterfølgende" pakker.
Hvis en startpakke kommer fra det ydre net, betyder det, at en maskine udefra forsøger at lave en forbindelse ind mod firewall'en. Med mindre dette specifikt tillades (fx hvis der er tale om en forbindelse til virksomhedens webserver), vil sådanne pakker blive stoppet.
Hvis startpakken kommer fra det interne net (LAN), betyder det, at en maskine indefra forsøger at lave en forbindelse ud mod internettet. Dette vil som regel blive tilladt, og firewall'en vil huske forbindelsesinformationer som IP adressen, TCP porten med mere.
Hvis en efterfølgende pakke rammer firewall'en (enten fra internettet eller fra det interne net), vil dennes forbindelsesinformationer blive checket op imod de informationer, som firewall'en har om eksisterende, godkendte forbindelser. Pakken får dermed kun lov til at slippe igennem, hvis den passer til en godkendt forbindelse.

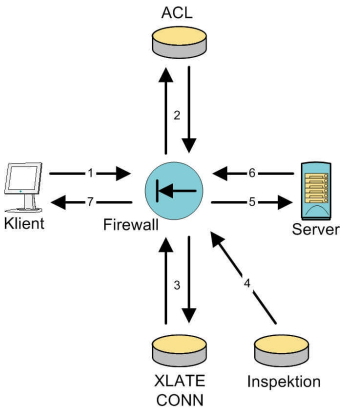
Hvis der er tale om UDP eller ICMP pakker i stedet for TCP pakker, er der ikke samme mængde forbindelsesinformation tilgængelig. Der vil dog som minimum være IP adresse-par. Ved UDP er der desuden port-par og ICMP har et type-ID tilknyttet. I sådanne tilfælde vil denne type information blive brugt til at matche pakkerne.
Ved ICMP vil en firewall ofte kun tillade echoes og echo svar, address mask forespørgsler og svar samt timestamp forespørgsler og svar. Dette skyldes, at andre former for ICMP-forespørgsler indeholder så lidt information, at det er svært at matche pakkerne.

Visse protokoller så som FTP benytter adskillige netværksforbindelser samtidig. Ofte vil der være tale om en kontrolforbindelse og efterfølgende dataforbindelser. Ved FTP vil en bruger på det interne net åbne en kontrolforbindelse og anmode om en fil. Derefter vil serveren på internettet åbne en dataforbindelse tilbage til brugeren. Hvis FTP skal fungere, skal denne forbindelse have lov til at passere firewall'en, selvom en sådan forbindelse normalt vil blive afvist.

For at klare dette, bliver FTP-dataene analyseret. Der søges efter udgående ”PORT” kommandoer. Når disse findes, gemmes informationen om dem i firewall’en, hvorefter dataforbindelsen afventes. Dette kan gøres, idet PORT-kommandoen indeholder information om IP-numre og portinformation, som senere kan benyttes til at identificere den indkommende dataforbindelse.

Stateful, multi-layer inspection firewalls er en videreudvikling af stateful packet inspection, hvor flere lag undersøges i én enhed. Således operer disse ofte på alle lag fra 2 til 5. Filtrering foregår i lag 2-3, validering i lag 4 og inspektion i lag 5. Et eksempel på en sådan enhed er CheckPoint’s Firewall-1 produkt.

For at lave inspektion i de øvre lag uden at benytte samme proxyteknik som en ALG, benyttes specielt software i udstyret, som tager et øjebliksbillede af de data som passerer. Således inspiceres pakkerne i stedet for – som ved en ALG – at blive processeret. Resultatet er, at firewall’en er transparent for de legitime brugere ligesom den hastighedsforringelse, som ALG medfører ikke opleves i samme grad.
Visse af Cisco’s større stateful, multi-layer inspection firewalls benytter på denne måde applikationsbevidste services i operativsystemet, som analyserer pakkestrømmene i applikationslaget.
Et eksempel på dette ses på figur 29. ACL er Access Control Lists, dvs. en liste over hvilke netværk, enheder og services (TCP/UDP port numre) som tillades. ”Inspektion” på figuren henviser til et sæt af statiske, predefinerede funktioner mens ”XLATE CONN” er en database med de statusinformationer med mere, som er gemt for hver etableret forbindelse igennem enheden.



Figur 29 - Cisco's Adaptive Security Algorithm

Numrene på figuren er den rækkefølge, som operationerne foregår i.

1. En TCP SYN pakke ankommer til firewall’en for at etablere en ny forbindelse.
2. Firewall’en checker ACL’en for at se, om denne forbindelse kan godkendes.
3. Der laves en ny post i databasen (XLATE CONN).
4. Firewall’en checker inspektionsdatabasen (”Inspektion”) for at afgøre, om forbindelsen kræver applikationsbevidste inspektionsservices.
5. Efter denne operation er færdig og eventuelle operationer på pakkerne er foretaget videresendes pakken til sin destination.
6. Destinationen besvarer forespørgslen.
7. Firewall’en modtager svarpakken, slår op i forbindelsesdatabasen (XLATE CONN) og videresender pakken fordi den tilhører en allerede etableret forbindelse.

Nogle af de applikationer, som kræver denne behandling, er fx H.323, DNS, FTP, HTTP, SMTP med flere.

Desuden kan der i enkelte tilfælde benyttes specielle forsvarsmekanismer ud over ovennævnte. For Cisco’s vedkommende kan dette indbefatte fx funktionerne FragGuard og Virtual Packet Assembly. Disse beskytter firewall’en mod IP fragmenteringsangreb. Fragmenteringsangreb udnytter, at mange firewalls ikke udfører samling af pakkerne. Derved kan angreb gemmes i mange pakker, som forbigår firewall’en og først samles ved den server som angribes. Modsat kan fragmenteringsangreb også benyttes mod firewalls som udfører pakkesamling. Dette foregår ved at sende store mængder fragmenterede pakkeserier med ukomplette fragmentreringssekvenser. På denne måde overbelastes enheden i et forsøg på at samle pakkerne fra de mange pakkeserier. FragGuard og Virtual Packet Assembly beskytter udstyret mod overbelastning ved kun at samle pakker for ICMP fejlbeskeder idet disse beskeder ofte benyttes til at angribe servere ved brug af fragmenteringsteknikken. Samtidig laves en virtuel samling af pakkerne for den resterende trafik for at lede efter andre former for angreb, som er fordelt over en serie af fragmenterede pakker[36]. En anden funktion som benyttes er TCP Intercept, som beskytter TCP servere fra TCP SYN flood-angreb. Dette foregår ved at opfange TCP SYN pakker. Firewall’en etablerer en forbindelse tilbage til afsenderen på vegne af den server, som pakken var sendt til. Hvis dette lykkedes etablerer firewall’en en forbindelse til serveren og fletter de to forbindelser sammen. På denne måde modtager serveren aldrig SYN pakker, som ikke har en valid afsender.

Også CheckPoint har udviklet beskyttelse på applikationsniveau til deres Firewall-1 produktserie under navnet Application Intelligence. Dette sker ud fra fire grundlæggende principper: validering af overensstemmelse med standarder, validering af forventet brug af protokollerne, begrænsning af applikationernes mulighed for at medbringe ondsindet data samt kontrol over applikationslagets operationer. Eksempler på hvad disse udtryk dækker over kan være følgende:

- Validering af overensstemmelse med standarder kan fx sikre, at der ikke benyttes binære data i HTTP headere. Dette er ikke tilladt ifølge den officielle HTTP standard, men checkes normalt ikke af firewall’en. Angribere kan dermed udføre angreb ved at inkludere eksekverbar kode i HTTP headeren.
- Validering af forventet brug af protokollerne kan give mulighed for at begrænse eller stoppe brugen af Peer-to-Peer (P2P) kommunikation. Idet mange udbredte programmer af denne type benytter port 80 og

[36] Pakkefragmenteringsproblemet hænger sammen med IP protokollens opbygning og er forklaret i RFC 791 og 815

gemmer sig i legitim HTTP-trafik, kan det være et stort problem at stoppe denne type trafik. Ved at kontrollere, om protokollen (HTTP) benyttes til webtrafik som forventet, kan P2P-programmerne blokeres.

- Begrænsning af applikationers mulighed for at medbringe ondsindet data kan fx udføres ved at kontrollere URLs eller ved at blokere for cross site scripts.
- Kontrol over applikationslagets operationer kan fx ske ved at blokere for bestemte filtyper ved FTP-overførsler. Selvom der her benyttes en godkendt protokol, som overholder standarder og benyttes på den ønskede måde, kan skadelige filer eller uønskede informationer overføres via programmet. Dette kan analyseres i firewall'en og blokeres hvis det ønskes.

CheckPoint var de første til at levere denne type firewalls, og produktet har kun været på markedet siden maj 2003. Der er derfor endnu ikke meget tilgængeligt materiale omkring hvor effektiv denne teknologi er mod disse typer af angreb, ligesom det ikke er klart, hvordan produktet skalerer i større virksomheder. En samlet oversigt over de applikationslags-angreb, som teknologien ifølge CheckPoint kan modstå, er vist i Appendiks B.

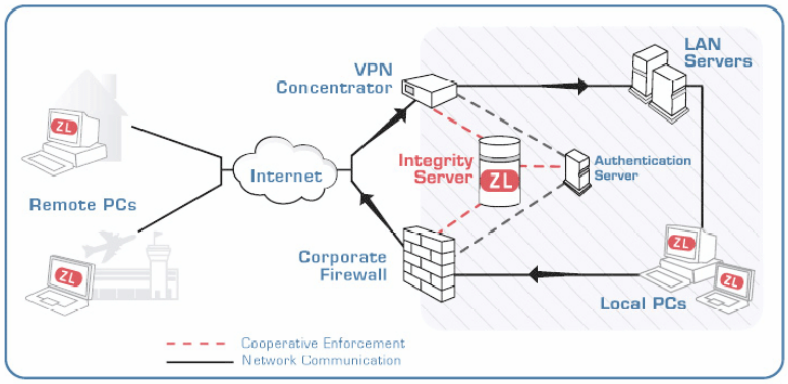
Både Cisco og CheckPoint's mere avancerede features går under betegnelsen Dynamic Network Firewalling. Typisk sker blokeringen ud fra signaturbaserede algoritmer. Der er tale om en kombination af Intrusion Detection Systemer (IDS), firewalls og realtime intrusion prevention. På denne måde kan en sådan enhed fx nægte adgang til klienter som udfører SQL slammer-angreb, mens der stadig tillades adgang til standard SQL trafik[37].

5.4.5 Personlige/softwarebaserede firewalls

Selv med en firewall, som beskytter virksomheden mod angreb udefra, kan det være nødvendigt yderligere at beskytte hver enkelt arbejdsstation og hjemmearbejdsplads. Dette kan være relevant, hvis den ydre firewall svigter, ligesom firewalls installeret på arbejdsstationerne kan sikre maskinerne mod angreb fra hinanden, hvis fx en enkelt af dem bliver inficeret med en trojansk hest via et program, som brugeren har hentet fra internettet. For hjemmearbejdspladserne og mobile enheder kan grunden være, at man ønsker en beskyttelse af maskinen uanset hvor den befinder sig.
Personlige firewalls har ofte tre funktioner. Disse er:

- Protokoldriverblokering – det sikres, at ikke-standard protokoldrivere ikke indlæses og benyttes af programmer
- Blokering på applikationsniveau – kun bestemte applikationer tillades netadgang
- Signatur-baseret blokering – konstant overvågning af netværkstrafikken for at undgå, at kendte angrebsmetoder kan udføres mod systemet.

Problemet med de softwarebaserede firewalls er ofte, at de sætter store krav til brugerens kunnen og forståelse for sikkerhedsproblemerne. Samtidig skalerer løsninger som oftest dårligt, idet installationen, vedligeholdelsen og konfigurationen af tusindvis af arbejdsstationer med firewalls er meget tidskrævende.
Zone Labs, som er kendt for udviklingen af den personlige firewall ZoneAlarm, har udviklet et distribueret firewallsystem til arbejdsstationer og hjemmearbejdspladser. Dette kaldes Zone Labs Integrity (ZLI). Ideen er, at små agentprogrammer installeres på arbejdsstationer og hjemmearbejdspladser samt mobile enheder, mens en central server holder styr på konfigurationer, regelsæt og opdateringer. På den måde kan bestemte grupper af medarbejdere få påtvunget et sæt regler, mens andre får et andet sæt. Administratorerne kan til enhver tid ændre i regelsættene ligesom agentprogrammerne kan holdes opdateret fra central side.

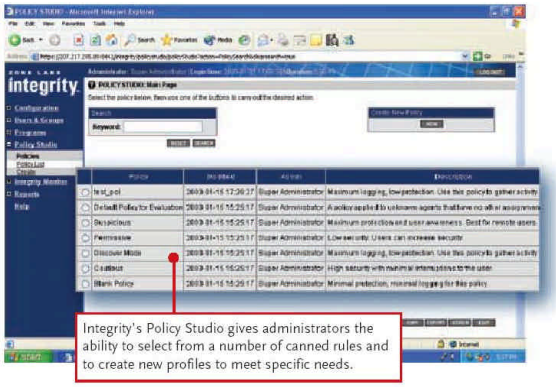


Figur 30 - ZoneLabs' distribuerede firewallprogram [54]

For at undgå problemet med uddannelsen af brugeren, er programmerne usynlige for brugerne, som heller ikke vil blive bedt om at tage stilling til sikkerhedsspørgsmål hvis deres maskine angribes. Der vil på forhånd være udfærdiget en politik om, hvordan programmerne skal reagere på bestemte trusler.
ZLI kan arbejde sammen med fx Cisco's VPN Concentrator-serie for at verificere, at brugere som ønsker at koble op med VPN til virksomheden overholder fastsatte standarder for sikkerhed på deres hjemmearbejdsplads. Dette er vist på figur 30. Samtidig checkes, at nyeste versioner af antivirusprogrammerne er installeret, aktiveret og opdateret. Kun hvis både firewall- og antivirusprogrammet overholder de fastsatte krav får brugeren lov til at benytte netværket. Et lignende kontrolsystem kan benyttes, når arbejdspladsen på kontoret ønsker at benytte netværket for fx at sikre, at bærbare computere, som tages med på kontoret, er sikret efter de fastsatte krav.

[37] Der er i afsnittet brugt information fra [52], [73] og [74].

ZLI kan konfigureres til at være helt transparent for brugeren og rapportere tilbage til et centralt managementprogram i virksomheden. Det er således muligt for administratorerne at få overblik over, hvilke aktiviteter der foregår og afgøre, om der skal ændres på den måde programmerne reagerer mod disse som vist på figur 31.



Figur 31 - ZLI's administrationsinterface [55]

Ulempen med ZLI er, at det udelukkendes findes til Windows-klienter. Til gengæld er det en afprøvet teknologi, som benyttes på mere end 20 millioner arbejdsstationer.

Et lignende system findes fra McAfee under navnet Personal Firewall. Her er der dog ikke mulighed for integration med VPN eller antivirusprogrammer, så brugernes konfigurationer kan valideres inden de tillades adgang til netværket.

Internet Security Systems (ISS) har ligeledes lanceret et produkt efter deres køb af Network ICE. ISS RealSecure Desktop Protector tilbyder ligesom Zone Labs og McAfee at lave gruppeindstillinger, opdateringer mm. og kan installeres transparent på brugernes arbejdsstationer. Samtidig laves der cheksums af alle filer på maskinen, og hver gang en fil eksekveres eller åbnes sammenlignes dens checksum med den gemte. Dette princip kan sammenlignes med Tripwire, som er beskrevet i afsnit 5.5. Hvis disse ikke stemmer overens kan programmet eller filen ikke åbnes. Dette sikrer, at der ikke sker ændringer til systemet, installerede programmer mm. uden administratorernes tilladelse. ISS har ligesom Zone Labs lavet integrering med VPN og antivirusprogrammer, så brugerens indstillinger kan verificeres, inden der tillades adgang til netværket.
ISS har desuden mulighed for automatisk at distribuere information om angribere til hele netværket. Har en angriber dermed én gang forsøgt sig mod en arbejdsstation, hjemmearbejdsplads, mobil enhed eller en honeypot (se også afsnit 5.8) distribueres information om angriberen til alle andre enheder på netværket. Ligesom med Zone Labs tilbyder ISS udelukkende agentprogrammerne til Windowsplatformen[38].

5.4.6 Svagheder ved brug af firewalls

Installationen af en firewall er ikke i sig selv en sikkerhed mod angreb. Fejlkonfigurerede firewalls leverer blot en falsk tryghedsfornemmelse. Samtidig findes der hvert år adskillige sikkerhedshuller i stort set alle firewallprodukter, hvilket kræver en kontinuerlig vedligeholdelse af udstyret. Dermed skal ikke forstås, at en veldesignet, velkonfigureret og vedligeholdt firewall ikke er stort set umuligt at bryde igennem. Dette ved angriberne også, og de vil i sådanne tilfælde forsøge at arbejde sig rundt om enheden. Dvs. udnytte eventuelle forbindelser, som pga. tillid til en virksomhed eller person får lov at passere firewall'en. Eller de vil forsøge at angribe hjemmearbejdspladser eller afdelinger af virksomheden og derfra koble op ved hjælp af opkaldsforbindelser, VPN eller andet. Angriberne vil altså søge udenom en stærk firewall, og det er derfor essentielt at denne holdes så stærk som mulig hvorefter der kan fokuseres på de resterende sårbare forbindelser.

Benyttes en packet-filtering router, som ikke kan opretholde status på forbindelserne (som fx en Cisco IOS router), kan en angriber ved brug af et program som nMap[39] scanne interne maskiner igennem firewall'en. Dette gøres ved at udnytte, at en packet-filtering router, som ikke er udstyret med stateful packet inspection, er nødt til at lade trafik fra bestemte portnumre passere. I det tidligere eksempel med FTP betyder dette, at så længe trafikken har en kildeport på 20 vil den blive tilladt igennem firewall'en. Dette skyldes, at når den legitime, interne bruger har lavet en FTP-forbindelse ud igennem firewall'en, vil FTP-serveren på den eksterne side svare tilbage med en kildeport på 20 og en destinationsport, som er større end 1024. Ved at benytte en port "redirector" som fx Fpipe, kan angriberen sætte kildeporten til 20, mens destinationsporten er variabel. Den eneste måde at undgå dette på, er ved at benytte firewalls med stateful packet inspection eller ved at benytte en application-level gateway.
Selv med stateful packet inspection kan en sløset konfiguration åbne for scanninger ind bag firewall'en. Hvis virksomheden fx ønsker, at internetudbyderen kan foretage DNS zonetransfers kan dette ske ved at der laves en post i Access Control Listen (ACL) med "tillad aktivitet med TCP kildeport 53", mens der burde have stået "tillad aktivitet fra internetudbyderens IP-adresse med TCP kildeport 53 og destinationsport 53 til DNS serverens IP-adresse" [76].
Faren for fejlkonfigurationer eksisterer også ved application-level gateways. Hvis administratoren ikke har lukket for ekstern adgang til proxyserveren, kan denne benyttes af eksterne brugere til enten at videresende angreb til andre maskiner eller til at få adgang til virksomhedens intranet. Sidstnævnte kan ske selvom der er implementeret Network Address Translation (NAT), idet selv ikke-routebare adresser kan tastes ind i en browser, som benytter proxyserveren. Dette skyldes, at proxyserveren selv er i stand til at kontakte de interne servere.

Det er værd at bemærke, at de fleste dygtige angribere næsten øjeblikkeligt kan vurdere, om det er forsøget værd at angribe virksomhedens primære sikkerhedssystemer. Det er ikke kompliceret at identificere den type udstyr, og de

[38] Der er i afsnittet brugt information fra [54], [55] samt [75].
[39] Programmet nMap kan findes på adressen http://www.insecure.org/

konfigurationer som beskytter "hovedindgangen" til virksomheden. Ofte vil de målrettede angreb derfor ikke ske direkte mod kædens ofte stærkeste led, men derimod mod andre svage led i forsvaret. Et eksempel på disse svage led er brugen af bagdøre.

Bagdøre
Det er ofte langt lettere at få en bruger til at åbne en vedhæftet fil end at konstruere det angreb, som er nødvendigt for at lave en buffer overflow i en CheckPoint firewall. Sidstnævnte skal formentligt gennemgås flere gange med forskellige systemer for at nå igennem det primære forsvar. Brugen af bagdøre kan være langt lettere. Disse kan typisk opdeles i tre kategorier – passive, aktive og angrebsbaserede bagdøre. Nogle eksempler på aktuelle bagdøre er vist nedenfor:

- **Passiv bagdør**. Programmet BindShell[40] kan lytte på en vilkårlig TCP port og afvente telnet-adgang til denne port.
  For at opdage bagdøren kan fx nMap benyttes til at scanne alle maskiner i et netværk og sammenligne resultatet med et lignende resultat fra en "ren" maskine.

- **Aktiv bagdør**. Programmet Sneakin[41] afventer to specielle ICMP-pakker før det aktiveres. Herefter udføres en telnet-session mellem maskinen og en foruddefineret maskine udenfor netværket.
  Sneakin kan ikke opdages med nMap, da programmet ikke er aktivt før ICMP-pakkerne er modtaget. Benyttes i stedet for et program til at liste alle åbne filer kan man med baggrund i, hvordan systemet så ud før kompromitteringen se, at programmet er aktivt.

- **Angrebsbaseret bagdør**. GIFtpD[42] er navnet på en bagdør, som benytter en sårbar FTP-server. Ved at udnytte sårbarheden i FTP-serveren placeres og afvikles bagdøren automatisk.

BindShell og Sneakin er klassiske eksempler på, hvordan en svag politik omkring indgående trafik kan udnyttes. Men selv en meget stærk begrænsning på indgående trafik kan forbigås ved at benytte aktive bagdøre som benytter tunneleringsmetoder. På denne måde etableres en udgående forbindelse, som ikke stoppes af en typisk firewallopsætning.
Circuit-level gateways kan benyttes til at minimere denne form for udgående trafik. Ved at benytte en SOCKS gateway på denne måde, skal en bagdør kontakte gateway'en og bede om lov til at lave en udgående forbindelse før dette kan ske. Dette sker dog ikke uden en omkostning i administration og brugervenlighed.
Et alternativ er at lave en meget restriktiv politik for udgående trafik kombineret med web- og andre applikationsspecifikke proxy-servere som kræver autentifikation før adgangen gives. På denne måde skal bagdørene ikke alene tale det rigtige sprog for at kommunikere med proxy'en, men bagdøren (og dermed angriberen) skal også være i besiddelse af et login og password. Dermed er det muligt at identificere en bruger til alle forbindelser. Man er altså nu i stand til at afvise, observere og afsløre bagdøre.
Ulempen ved et system af den type er naturligvis en markant nedsættelse af brugervenlighed og muligheder for legitimt at benytte netværket effektivt[43].

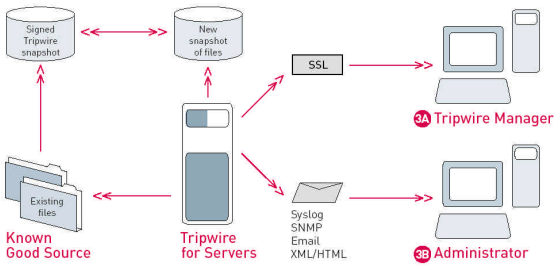
5.4.7 Opsummering

Firewalls kan benyttes til at mindske risikoen for flere af de i kapitel 3 samt Appendiks A nævnte sikkerhedsproblemer. Dette inkluderer IP spoofing, angreb på applikationslaget samt netværksrekognoscering og angreb på hjemmearbejdspladserne samt opkaldspunktet. Dog kan firewalls ikke alene modvirke disse angreb og fungere som virksomhedens eneste beskyttelse, men kan med fordel bruges som hovedingrediens i et forsvarssystem, baseret på mange lag af beskyttelse.
Anvendelsen af softwarebaserede, distribuerede firewalls på brugernes arbejdsstationer, hjemmearbejdspladser og mobile enheder kan være en stor fordel i situationer hvor adgangen til det interne net ikke er 100 % blokeret, eller hvor man ønsker et ekstra sikkerhedslag. Det kan dog ikke erstatte brugen af en hardwarebaseret firewall til adskillelse af virksomhedens interne net og internettet.
Muligheden for at validere brugernes antivirus- og firewallindstillinger inden de tillades adgang til netværket kan være en stor fordel for mobile brugere og i visse tilfælde for hjemmearbejdspladser. Denne teknik benyttes bl.a. af Microsoft for at sikre, at bærbare computere ikke poserer en al for stor risiko, når de benyttes på det interne netværk [119].

[40] Programmet BindShell kan findes på adressen http://hysteria.sk/sd/f/junk/bindshell/bindshell.c
[41] Programmet Sneakin kan findes på adressen http://packetstormsecurity.org/Exploit_Code_Archive/sneakin.tgz
[42] Beskrivelsen af GIFtpD kan findes på adressen http://www.security-express.com/archives/bugtraq/1999-q4/0443.html
[43] Der er i afsnittet om firewalls benyttet information fra [56], [48] side 517-527 og fra [47] side 482-502

5.5 Integritet

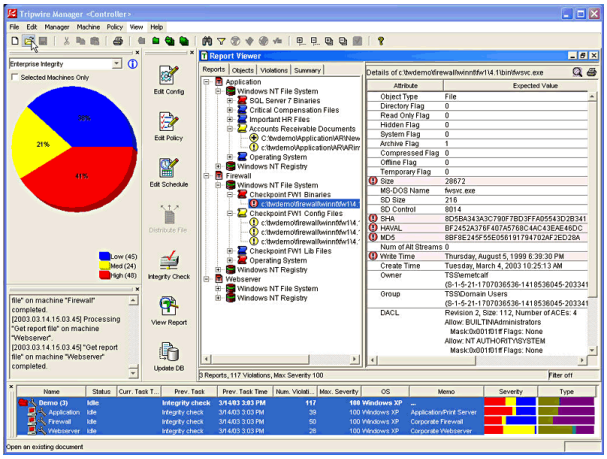
For at sikre, at uautoriserede ændringer til konfigurationer af netværksudstyr, operativsystemer på servere, web-serveres hjemmesider og virksomhedens statiske information kan detekteres, kan integritetsbekræftelse integreres i netværket.
Integritetsbekræftelse detekterer alle ændringer af udvalgte filer på netværksenheder, servere, databaser med mere. Desuden overvåges oprettelsen af nye og sletningen af eksisterende filer. Et populært eksempel på et sådant produkt er Tripwire[44].



Figur 32- Grundlæggende funktionalitet af Tripwire [57]

Tripwire starter med at opbygge en basisprofil – en database over den nuværende tilstand af filer, biblioteker, konfigurationer med mere. Herefter checkes med jævne mellemrum om disse informationer ændres, hvem der ændrer dem og hvad de ændres til. Dette er skitseret på figur 32. Tripwire holder på denne måde øje med filernes tilstand. For at undgå, at der kan ændres i filerne uden det opdages, benytter programmet hash-algoritmer som SHA eller MD5. Programmets primære egenskab er at kunne spore, hvilke ændringer der er foretaget til udstyret, som overvåges. Dette kan benyttes til at få netværket genoprettet efter et angreb eller til at fejlsøge netværket efter legale ændringer er foretaget. Visse ændringer kan godkendes automatisk mens andre vises på en oversigt, som administratorer kan tage stilling til. Administrationsinterfacet kan ses på figur 33.

Tripwire kan overvåge netværksprodukter såvel som routere, firewalls og VPN-udstyr samt servere, arbejdsstationer og databaser. Overvågningen af netværksudstyr foretages primært for at have en historik over, hvem der har foretaget hvilke ændringer og hvornår, samt for at kunne identificere, hvad en eventuel angriber har ændret. Overvågningen af servere og arbejdsstationer kan udføres for at kunne sikre at opdateringer er installeret til operativsystemerne, samt at brugerne (eller andre) ikke har ændret i opsætningen af programmer og lignende.

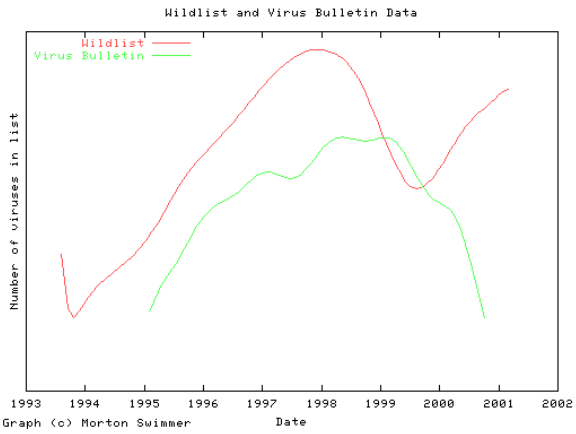


Figur 33 - Tripwires administrationsmodul

Programmer som Tripwire har altså ikke som direkte formål at forhindre angreb, men derimod at detektere ændringer i netværket for senere at kunne genoprette systemet samt spore aktiviteten. For administratorer kan værktøjet være en stor hjælp specielt i distribuerede netværksopsætninger som fx ved brug af hjemmearbejdspladser. Her kan der fra et centralt sted dannes et overblik over alle ændringer til alt udstyr, som benyttes både indenfor og udenfor virksomheden. Da programmer som Tripwire kan registrere alle ændringer til et system, kan angrebstyper fra kapitel 3 som fx portomdirigering, der kræver installation af software på virksomhedens enheder, detekteres.

[44] Information om produktet Tripwire kan findes på adressen http://www.tripwire.com/

5.6 Antivirus



Figur 34 - Virusstatistik baseret på Virus Bulletin og WildList [61]

Brugen af antivirusprogrammer burde efterhånden være en selvfølge indenfor erhvervslivet. Alligevel har over halvdelen af danske virksomheder været udsat for virusangreb, og 41 % af de britiske virksomheder har været udsat for "alvorlige virusangreb" [58]. I det offentlige ser situationen endnu mere alvorlig ud. Her har ca. 80 % af amterne oplevet virusangreb [59]. 51 % af amerikanske virksomheder udtaler, de har haft "virus katastrofer" indenfor de sidste 12 måneder [60].
Det er interessant at se på, hvordan udviklingen er gået de sidste 10 år. En måde at afgøre, om antivirusproducenterne og administratorerne har situationen under kontrol, er ved at se på, hvor mange vira, der aktivt er i omløb – dvs. dagligt inficerer computere i større skala. På figur 34 ses antallet af vira i omløb mellem 1993 og 2002 beregnet ud fra to forskellige statistiske datasæt.
Y-aksen på grafen (antallet af vira i omløb) er normaliseret for at følge udviklingen, men antallet af vira varierer fra ca. 100 til 500.
Som det ses er mængden af vira i omløb, som aktivt inficerer computere, relativt stabil. Da den samlede mængde af vira er steget kraftigt (fra ca. 1000 i 1993 til ca. 70.000 i januar 2002 [62]) er grafen et udtryk for, at antivirusprogrammerne holder mængden af vira nede, men samtidig et udtryk for, at situationen ikke forbedres. Det sidste skal formentligt forklares ud fra, at brugerne ikke bliver bedre til at installere opdateringerne. Og med 1200 nyfundne vira hver måned [62] er opdateringerne kritiske, specielt set i lyset af de nye viras hurtige spredning. Som eksempel spredte Sapphire virussen sig til alle, internetaktive lande i verden på ca. 10 minutter. Efter tre minutter var den i stand til at lede efter sårbare maskiner med en hastighed på 55 millioner IP-adresser i sekundet.
For virksomheden handler det om at sørge for, at samtlige sårbare enheder sikres mod virusangreb. Dette indebærer både installation af et antivirusprogram, men også opdateringen af dette. Som det beskrives nedenfor, findes der mange mulige løsninger på problemet.

5.6.1 Beskyttelse af arbejdsstationen

Produkter som Norton AntiVirus eller McAfee's VirusScan kan installeres på hver enkelt arbejdsstation og i baggrunden overvåge de filer, som læses og skrives. Opdateringen af produkterne kan enten ske automatisk eller ved at brugeren henter opdateringerne fra en hjemmeside og selv installerer disse.
Som beskyttelse af private PC'ere fungerer disse produkter udmærket. Dog vælger mange at slå overvågningen af filerne fra, fordi det nedsætter hastigheden af maskinen. Gøres dette har programmet udelukkende en funktion, hvis brugeren selv iværksætter en scanning af alle nye filer og e-mails, som hentes. Og da kun hvis brugeren samtidig har sikret, at programmet er opdateret.
I en virksomhed kan specielle versioner af disse programmer benyttes, som tillader administratorerne at kontrollere indstillinger, opdateringer osv. Dette kræver dog en del overvejelse, idet brugere stillet overfor spørgsmålet om en inficeret fil skal slettes, ofte vil svare nej, idet sletning af filerne som regel er noget, der skal undgås. Derfor skal alt konfigureres på forhånd, så farlige filer fx kan placeres i karantæne på en server, hvor administratorer kan finde dem frem, hvis brugerne føler det nødvendigt.
Specielt til hjemmearbejdspladser findes distribuerede versioner af antivirusprogrammerne. Disse arbejder ud fra en central struktur, hvor administratorerne i virksomheden kan styre distributionen og opdateringen af tusindvis af disse programmer. Da der ikke er noget brugerinterface til programmet på hjemmearbejdspladsen, kan man sikre, at indstillinger, rapportering mm. er centraliseret, ligesom ansvaret for opdateringer og vedligeholdelse er flyttet fra brugeren til virksomheden. For mobile brugere kan man kræve, at antivirusprogrammet opdateres inden maskinen tillades adgang til netværket. Et eksempel på et sådant program er McAfee's VirusScan Thin Client[45].

5.6.2 Beskyttelse af e-mails og internettrafik

Selvom programmerne, som installeres på arbejdsstationen, kan give beskyttelse mod vira i e-mails, vil det ofte være en fordel at scanne e-mails før de når ud til brugerne ud fra en filosofi om, at jo længere fra brugerne og deres data vira stoppes jo bedre. Dette kan ske med antivirusprogrammer, som installeres på virksomhedens mailservere. Derved har man også sikret, at e-mails som læses udenfor virksomhedens netværk (fx via en internetside) allerede er scannet.
I en virksomhed som Microsoft sendes der dagligt ca. 4,5 millioner e-mails internt i virksomheden [119]. Dette svarer til ca. 50 e-mails pr. sekund. Der stilles derfor relativt store krav til det udstyr, som skal scanne alle e-mails centralt i en større virksomhed.

[45] Produktet VirusScan Thin Client kan findes på adressen http://www.mcafeeb2b.com/products/virusscan-tc/default-virusscan-tc.asp

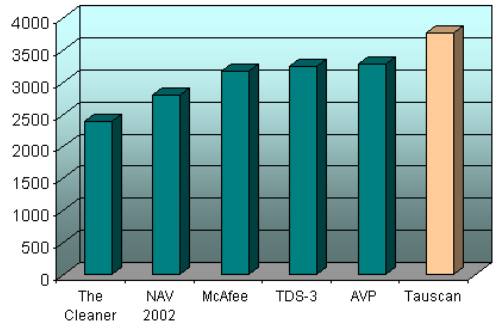
Ud over e-mails kommer den største virustrussel fra de filer, som medarbejderne henter via internettet. I en virksomhed vil internettrafikken ofte gå igennem en gateway på vejen ud mod internettet, og på denne gateway vil der derfor være mulighed for at scanne trafikken for virus. Dette medfører dog adskillige problemer, idet det kræver, at gateway'en er i stand til at opsamle brugernes trafik indtil hele programmer er færdighentede før selve scanningen kan begynde. I større netværk kan det kræve meget store ressourcer, ligesom metoden ikke kan sikre alle downloads. Benyttes fx en SSL-forbindelse, vil gateway'en ikke kunne analysere denne trafik.

Figur 35 - WebShield e500 fra McAfee[46]

McAfee har udviklet specielt hardware til at håndtere scanning af internettrafik på den måde. Serien hedder WebShield og scanner POP, HTTP, FTP og SMTP trafik. Den største model (e1000) kan scanne ca. 40 e-mails eller 2Mb internettrafik pr. sekund. Lillebroderen e500 er vist på figur 35[47].

5.7 Beskyttelse mod trojanske heste

Selvom antivirusprogrammerne leverer en udmærket beskyttelse mod virus og virusrelaterede problemer kan det være fordelagtigt at benytte et værktøj, som specifikt beskytter mod trojanske heste.



Figur 36 - Anti-Trojan vs. AntiVirus programmer. Grafen viser hvor mange trojanske heste de forskellige produkter kan identificere[48]

Bl.a. Kevin Mitnick anbefaler [2] brugen af disse produkter og henviser til programmer som The Cleaner[49] og Trojan Defence Suite[50]. Et andet anbefalelsesværdigt produkt er TauScan fra Agnitum[51] som påstår at have verdens største database over trojanske heste og metoder til at fjerne disse.
Sidstnævnte har fået udført en analyse af, i hvor høj grad antivirusprogrammer finder og fjerner trojanske heste i et forsøg på at retfærdiggøre brugen af Anti-Trojan produkter. Grafen fra analysen kan ses på figur 36. Der er ifølge denne undersøgelse 964 trojanske heste, som Norton AntiVirus 2002 ikke kan finde.
Det skal dog bemærkes, at der ved brugen af et Anti-Trojan program tilføjes endnu et ressourcekrævende produkt til PC'en, og at programmerne samtidig – ligesom med antivirusvarianterne – kræver jævnlig opdatering af signaturfilerne.

5.8 Honeypots

Honeypots kan defineres som:

"*[...] an information system resource whose value lies in unauthorized or illicit use of that resource*" [91].

En honeypot er en computer, som udgiver sig for at være en del af netværket i et forsøg på at tiltrække uautoriseret trafik. En honeypot vil således simulere en netværksenhed for at lokke angribere til at tro, de angriber et rigtigt system. Ideelt set burde en honeypot aldrig se noget trafik. Det kan derfor antages, at al trafik honeypot'en kan opfange er fjendtlige angreb. I modsætning til et IDS logger honeypots kun aktivitet, som med sikkerhed ikke er legitim brugeraktivitet, da ingen legitime brugere burde opsøge andre maskiner på netværket end dem, de har rettigheder til at benytte. Dette gør at de data, som opsamles, har større værdi og er mindre tidskrævende at gennemse for administratorerne. Samtidig kræves der relativt få ressourcer for at håndtere dem. En stor fordel ved honeypots er at de kan håndtere nye hidtil ukendte angreb, idet de tager imod al trafik der sendes til dem.

Det er vigtigt at understrege, at en honeypot kun logger den aktivitet, som er rettet mod de IP-adresser som overvåges af honeypot'en[52]. Angreb på legitimt netværksudstyr bliver ikke opdaget af honeypot'en. Her må firewalls, IDS'er og andet udstyr håndtere indsamlingen af værdifuld data. Samtidig løbes der en risiko, når honeypots benyttes. Hvis angriberen er dygtig nok, kan han overtage maskinen og anvende denne til at angribe legitime netværkssystemer. Denne risiko kan minimeres ved at omringe honeypot'en med firewalls, routerfiltre og eksterne overvågningssystemer, men det er stadig en risiko.

---

[46] Billedet er fra McAfee's hjemmeside på adressen http://www.mcafee2b.com/
[47] Der er i afsnittet om antivirus benyttet informationer fra [48] side 501-513.
[48] Billedet stammer fra Agnitum's hjemmeside på adressen http://www.agnitum.com/products/tauscan/compare.html
[49] Programmet The Cleaner kan findes på adressen http://www.moosoft.com/
[50] Programmet Trojan Defense Suite kan findes på adressen http://www.diamondcs.com.au/
[51] Programmet TauScan kan findes på adressen http://www.agnitum.com/
[52] Dette vil være IP-adresser, som ikke benyttes af andet udstyr på netværket. Honeypot'en kan således få tildelt et enkelt eller en række IP-adresser, som herefter overvåges.

Der findes to forskellige funktioner, honeypots kan udføre – beskyttelse og indlæring. Som beskyttelse er honeypots opsat for at spore angrebsaktivitet og benytte informationen om angribere til at omkonfigurere det primære netværk. Således kan angribere som forsøger sig mod en af virksomhedens honeypots, blive blokeret fra det reelle netværk. Som indlæring benyttes en honeypot af administratorer for at lære fra angriberne. Logfilerne gennemgås, de brugte værktøjer undersøges og de kommandoer, som angriberen har udført afprøves på andre test-systemer for at se resultatet. På denne måde kan administratorer lære om nye angrebsmetoder før de bliver benyttet mod virksomhedens primære netværk.

Honeypots er typisk opdelt i to typer: høj-interaktionssystemer og lav-interaktionssystemer. honeyd er et eksempel på sidstnævnte og er en OpenSource honeypot[53]. Der findes desuden et kommercielt produkt til Windows-maskiner, Specter[54].

honeyd
honeyd kan simulere mere end 400 operativsystemer og tusindvis af services og programmer. Dette emuleres primært ved applikationslaget, men også netværkslaget benyttes. Op til 65.000 virtuelle maskiner kan emuleres på én enkelt Pentium-baseret PC.
honeyd fungerer ved at overvåge alle netværksadresser på et netværk, som ikke har nogen enhed tilknyttet. Når en angriber forsøger at scanne eller angribe en af disse adresser overtager honeyd adressen via ARP spoofing (se Appendiks A) og interakterer med angriberen via de emulerede services.
De emulerede services, programmer og operativsystemer er blot scripts, som reagerer på forudbestemte hændelser. Fx findes et script som emulerer telnet servicen på en Cisco router. Her leveres et Cisco IOS telnet login billede, hvorefter honeyd forsøger at interaktere med angriberen så længe som muligt. Samtidig overvåges alle andre porte på samtlige IP-numre maskinen er i besiddelse af for at se hvilken type angreb, der foretages. Hvis scriptet er godt nok, kan det måske køre længe nok til, at det er muligt at få information om, hvad angriberen leder efter eller måske endda hans brugernavn, password eller en form for identifikation af, hvem der var tale om.

Der er med honeyd tale om et lav-interaktionssystem, idet systemer er opbygget af scripts. Uanset hvor gode disse scripts er lavet, vil angriberen på et tidspunkt opdage, at der ikke er tale om de virkelige services og programmer. Fordelen med disse systemer er, at de er meget simple og dermed lette at administrere og vedligeholde. De fungerer ofte godt i en beskyttelsesfunktion.

Honeypots af høj-interaktionstypen er som oftest komplette systemer med rigtige operativsystemer, services og programmer. Hvis et Windows 2000 system med IIS 5 ønskes simuleret, installeres Windows 2000 samt IIS5 i de fulde versioner. Ved at give angriberne et ægte system at interaktere med, fås bedre data og længerevarende angreb. Måske overtages maskinen og et hidtil ukendt root-kit installeres. Denne type information kan være meget værdifuld for administratorerne. Et eksempel på en høj-interaktionshoneypot er Symantec's Decoy Server [92] og Honeynets[55].

Honeynets
Honeynets er ikke et produkt eller et stykke software, men et komplet netværk af maskiner med komplette operativsystemer, programmer og services. Hele nettet er designet til at blive angrebet. Når en angriber finder vej til netværket overvåges al aktivitet fra fx krypterede SSH sessioner til fileroverførsler på ubenyttede portnumre. Dette foregår ved at indsætte moduler på maskinerne som fanger al trafik der sendes fra og til dem. Samtidig kontrolleres angribernes aktivitet ved at benytte en såkaldt Honeywall gateway. Denne gateway tillader indkommende trafik til systemerne, men holder øje med den udgående trafik ved at benytte intrusion detection-teknikker. Formålet er at undgå, at kompromitterede honeypots kan benyttes som angrebsbase mod andre maskiner.

Opsummering
Ofte vil lav-interaktionshoneypots blive benyttet til beskyttelse, mens høj-interaktionshoneypots benyttes til indlæring pga. kompleksiteten og vedligeholdelsesomkostningerne ved høj-interaktionstypen.
Honeypots kan hjælpe virksomheden til at hæve sikkerheden på flere forskellige måder hvoraf nogle af disse er nævnt nedenfor.

- Da honeypots kan overvåge tusindvis af IP-numre kan automatiske angreb, som scanner hele netværk og angriber alle maskiner sløves kraftigt ned. Ved at lade en honeypot besvare alle forespørgsler på ubenyttede IP-numre kan angrebet sløves ned ved at levere langsomme svar og fejlagtige oplysninger. Med lidt held kan angrebet stoppes helt med denne metode. Dette kan ofte bruges internt i virksomheden, hvor sådanne automatiske angreb ikke burde kunne finde sted.
- Honeypots kan også benyttes til at forvirre en angriber ved at camouflere de rigtige netværksenheder mellem honeypots. Således ved angriberen ikke hvilke enheder der er reelle netværksenheder og hvilke, der er honeypots. Vælges en honeypot alarmeres administratorerne og angriberens aktiviteter kan stoppes, før der udføres skade på andre enheder.

[53] Programmet honeyd kan findes på adressen http://www.citi.umich.edu/u/provos/honeyd/
[54] Programmet Spector kan findes på adressen http://www.specter.com/
[55] Honeynets er beskrevet på adressen http://www.honeynet.org/

- Installationen af honeypots i et netværk kan også hjælpe til at detektere angreb, som ellers ikke ville være fanget af IDS'er eller firewalls. Ofte giver IDS'er mange falske positiver og firewalls kan have svært ved at detektere nye angrebstyper. Honeypots internt i virksomheden kan dermed hjælpe til at detektere nye angrebstyper.
- Når et angreb er detekteret kan honeypots som er blevet udsat for angrebene, fjernes fra netværket og analyseres for at finde frem til de metoder, angriberen har benyttet. Resultatet fra analysen kan derefter benyttes til at sikre de øvrige systemer på netværket eller til at omkonfigurere firewalls og IDS'er til at blokere angrebene.
  Denne måde at analysere angrebne enheder på kan være svært uden brugen af honeypots. Det kan være vanskeligt at fjerne kritisk udstyr fra netværket for at analysere angreb mod det og endnu sværere at finde frem til de rigtige data på udstyret. Da en honeypot kun logger uautoriseret adfærd og ingen øvrig netværksfunktion har, vil stort set al data på disse enheder være værdifulde for administratorerne.

Generelt kan honeypots levere en værdifuld tilføjelse til virksomhedens sikkerhed. Brugen af en enkelt PC til emulering af tusindvis af forskellige enheder holder omkostningerne nede samtidig med, at administratorerne kan lære om nye angrebsmetoder før de primære systemer udsættes for samme[56].

5.9 To-faktor autentificering

Passwords er ofte det svageste led i sikkerheden. Det kan være svært at få brugerne til at vælge sikre passwords, og hvis det lykkes er det ikke unormalt at se, at disse nedskrives på notesblokke, i punge eller andre steder.
Selv med en god passwordpolitik og sikkerhedsbevidste brugere kan passwords være et problem for virksomhedens sikkerhed. Angribere kan benytte en keylogger (enten som software eller hardware) eller sniffer (se også afsnit 3.1) til at aflytte passwordet når det sendes over netværket eller fysisk observere brugeren, mens denne indtaster sit password.
En løsning på dette problem kan være to-faktor autentificering. De to faktorer vil oftest være noget brugeren har kombineret med noget brugeren ved. Dvs. fx kombinationen af en fysisk genstand og et password. Et velkendt eksempel er dankortet, som består af en pin kode (noget brugeren ved) og et fysisk kort (noget brugeren har).
Til dette formål er der udviklet utallige produkter. Disse spænder fra biometriske enheder som irisscannere og fingeraftrykslæsere til krypterede filer, som brugeren opbevarer enten på sin PC eller på en flytbar enhed. Fordelene ved begge disse yderligheder er klar. Biometriske identifikationssystemer benytter fysiske "enheder" som brugeren altid har på sig (øjne, fingre). Det har den fordel, at brugeren ikke skal bære rundt på – og huske – elektroniske enheder for at benytte systemet. Samtidig kan enhederne ikke uden videre stjæles. De krypterede filer sætter til gengæld ingen krav om investering af ekstra udstyr, men kræver, at brugeren har adgang til disse filer og dermed bærer rundt på dem eller har dem installeret på sin arbejdsstation. Sidstnævnte benyttes af de danske banker.
Der er naturligvis også ulemper ved metoderne. Det mest omdiskuterede problem med biometriske enheder er, at databasen med identifikationsmønstrene kan stjæles. Hvis denne kompromitteres, er det ikke umiddelbart muligt at udstede nye fingeraftryk eller irismønstre til brugerne ligesom man ellers ville kunne gøre med andre autentifikationssystemer. Problemet med filerne er, at disse ofte installeres stationært på arbejdsstationerne, hvilket betyder, at en kompromitteret arbejdsstation ikke får forbedret sikkerheden ved brug af denne metode.

To af de mest udbredte to-faktor autentificeringssystemer er engangspasswords, eller OTP (One Time Passwords) samt digitale certifikater. Første metode har den fordel at benytte dedikeret hardware uden at kræve specielt udstyr på de arbejdsstationer, det skal benyttes. Anden metode benytter USB-baserede enheder til opbevaring og generering af digitale certifikater.
I det følgende gennemgås to produkter af disse typer to-faktor autentifikationssytemer. Det ene er RSA's SecurID system som er baseret på OTP-teknikken, mens det andet er Rainbow Technologies' iKey system, som er baseret på digitale certifikater.

5.9.1 RSA SecurID

Figur 37 - RSA SecurID[57]

RSA Security's SecurID system er baseret på unikke, tidssynkroniserede enheder som ses på figur 37. Disse enheder beregner ved hjælp af en krypteringsalgoritme (128bit AES), en initieringskode samt klokkeslættet en sekscifret kode, som vises på et display på enheden. Da enhederne er unikke, kan en bestemt enhed knyttes til en bestemt bruger på systemet. Det er dermed muligt at sikre, at brugeren er i besiddelse af den korrekte enhed (der er dog undtagelser til dette hvilket er beskrevet nedenfor).
Initieringskoden er på forhånd lagt ind i hardwareenheden når denne leveres, og leveres desuden på en diskette, som efter ibrugtagning beskyttes eller destrueres. Denne kode installeres på serveren, som dermed i lighed med enheden kan beregne den forventede sekscifrede kode til sammenligning. Dette kræver naturligvis at servere og enheder er tidssynkroniserede, hvilket klares ved at lade serveren synkronisere med en

[56] Der er i afsnittet brugt information fra [91].
[57] Billedet er fra RSA Security's hjemmeside på adressen http://www.rsa.com/

præcis tidskilde (fx atomuret i Frankfurt) samt ved at benytte et præcist urværk i enheden, som forventes at holde præcisionen i en årrække, hvorefter brugeren udstyres med en ny enhed.
Hvert 60. sekund udregnes en ny kode. For at undgå, at brugeren bliver fanget i at indtaste en kode mens denne skifter, accepteres den kode, som tilhører det nuværende klokkeslæt samt koden et minut før og efter. Dette benyttes samtidig til at kontrollere om enheden og serveren skulle være ude af synkronisering, hvilket i så fald huskes, så systemet kompenserer for dette ved de efterfølgende logins.
Har brugeren ikke logget ind i en længere periode (flere måneder) kan enheden og serveren være længere fra hinanden end det tilladte treminutters vindue. I sådanne tilfælde checkes, om brugerens kode passer i et 20-minutters vindue. Hvis dette er tilfældet, bliver brugeren bedt om at vente 60 sekunder og fortælle hvad den nye kode er. Stemmer dette, vil serveren huske tidsforskellen og kompensere ved de efterfølgende logins.
Den ekstra kode benyttes til at sikre, at en angriber ikke blot har set enheden på et bord indenfor 20 minutter, men faktisk er i besiddelse af enheden.

Der udføres desuden kontrol af genafspilningsangreb. Dette sker ved, at serveren låser brugerens enhed i systemet, når denne er i brug under logins ligesom den aktuelle kode blokeres i samtlige servere på systemet når den først er taget i brug. Dette undgår desuden, at en angriber kan benytte en sniffer (se afsnit 3.1) til at observere en kode og derefter benytte den indenfor det tilladte vindue. Har koden først været i brug på netværket (hvilket den skal have været før angriberen kan observere den), kan den ikke længere benyttes. Af denne grund har teknologien fået navnet One Time Passwords (OTP).

Figur 38 - RSA SecurID med PIN-kode[58]

For at hæve sikkerheden yderligere er det muligt at benytte en anden type enhed, hvor brugeren skal benytte en PIN-kode for at aflæse den sekscifrede kode. Dette hæver sikkerheden yderligere, men besværliggør brugen af systemet, ligesom brugerne skal huske endnu en pin kode i deres hverdag.

RSA har mere end 10 millioner brugere af SecurID-systemet hvilket gør det til det mest populære to-faktor autentificeringssystem i verden. En styrke ved systemet er, at det fungerer uden ekstra krav om hardware på de maskiner, som brugerne kobler sig op med. Fordi brugeren kun skal indtaste en kode, er der ikke behov for at kunne aflæse certifikater, biometriske data eller andet. Samtidig er det et udbredt og anerkendt system, som bakkes op af mange fabrikanter af sikkerhedsudstyr. Der er desuden ingen problemer forbundet i at miste enheder, da disse let kan erstattes. Så snart en enhed er anmeldt stjålet eller på anden måde tabt kan administratorer blokere den i samtlige systemer fra en central applikation.
Understøttelsen af systemet fra andre fabrikanter gør det muligt at benytte fx Cisco Concentrators til VPN, CheckPoint Firewalls, Citrix-systemer og SUN ONE servere.
Samtidig kan de fysiske enheder erstattes af software-enheder, som installeres på fx PocketPC'er eller Palm PDA'er som det ses på figur 39. På den måde skal brugerne ikke bære rundt på flere enheder end normalt. Også visse Nokia og Ericsson mobiltelefoner kan benyttes til dette formål.
RSA SecurID er et utrolig fleksibelt værktøj til implementering af to-faktor autentificering. Dokumentation og brugervenlighed efterlader en del at ønske, men dette opvejes af support for produktet fra stort set alle større leverandører af netværksudstyr[59].

Figur 39 – RSA på en iPaq PDA

Det har været muligt at have SecurID-systemet til afprøvning. En gennemgang af produktets egenskaber i et testmiljø er vist i Appendiks C.

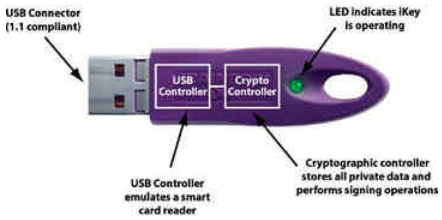
5.9.2 Rainbow Technologies' iKey

Rainbow Technologies iKey-system er bygget op omkring digitale certifikater til sikker identifikation af brugeren. Der benyttes en USB-enhed til generering og opbevaring af certifikaterne, og ud over formfaktoren er enheden teknisk identisk med et smart card. Enheden kan ses på figur 40.

Figur 40 - iKey[60]

[58] Billedet er fra RSA Security's hjemmeside på adressen http://www.rsa.com/
[59] Der er i afsnittet om RSA SecurID benyttet informationer fra [63].
[60] Billedet er fra Rainbow Technologies hjemmeside på adressen http://www.rainbow.com/

Denne enhed består af en Philips 5032 kontrolchip som understøtter brugen af algoritmer som DES, triple-DES, RC5 samt lagring af X.509 certifikater og private nøgler. Systemet kan desuden benyttes sammen med krypteringsprogrammet PGP.
På figur 41 ses opbygningen af en iKey 2000. Ud over USB-delen består den af en 8-bit kontrolchip, en processor til at håndtere de kryptografiske funktioner samt en hardwareaccelerator primært til triple-DES kryptering. Desuden en programmerbar hukommelse til opbevaring af certifikater og nøgler.
iKey-systemet er designet til at håndtere kryptografiske funktioner som nøglegenerering, digital underskrift, brugervalidering med mere.



Figur 41 - Opbygningen af en iKey 2000[61]

Brugervalidering kan foregå på to måder:

- Når en iKey eller et smart card initialiseres lægges en fælles, hemmelig kode på både enheden og på den server, som senere skal validere brugeren. Denne kode er ikke kendt af brugeren, og kan ikke udtrækkes af enheden. Samtidig tildeles enheden en PIN-kode. To-faktor autentificeringen består herefter af den delte kode samt brugerens PIN-kode.
  Når brugeren skal valideres, indsættes enheden i en USB-port hvorefter PIN-koden indtastes. Serveren aflæser enhedens unikke serienummer og afgør, om det er en valid enhed. Herefter sender serveren en streng af tilfældige data til brugeren, hvis enhed ud fra en hash funktion og den delte kode genererer en unik responsstreng. Serveren bruger enhedens serienummer til at slå op hvilken kode enheden har og beregner herefter selv den samme hash funktion. Hvis disse to funktioner er ens, er brugeren valideret. Det er værd at bemærke, at den hemmelige kode aldrig udtrækkes fra enheden eller sendes over netværket.
- Alternativt benyttes digitale signaturer i et PKI-system. Brugeren tildeles her et digitalt certifikat som genereres direkte på nøglen. Dermed eksisterer den private nøgle udelukkende her.
  Systemet fungerer herefter ved at klienten kontakter serveren, hvorefter en streng af tilfældige data genereres. Klienten signerer dataene (dvs. beregner en hash funktion og krypterer denne med sin egen private nøgle) og krypterer de resulterende data med serverens offentlige nøgle. Serveren modtager denne signerede og krypterede besked og dekrypterer den med sin egen private nøgle hvorefter klientens digitale signatur valideres ud fra dennes offentlige nøgle. Serveren kontakter en CA for at modtage brugerens digitale certifikat og checker så sin egen database for at se om dette certifikat er godkendt til denne brug. Hvis dette er tilfældet er brugeren valideret.

Hvis virksomheden har egen CA kan den private nøgle genereres direkte på iKey-enheden således at den ikke eksisterer andre steder.

iKey-systemet kan benyttes til at autentificere brugere i forbindelse med VPN samt ved normal tilgang til en netværksserver. Med systemet er det desuden muligt at sikre hjemmesider, WebMail osv. idet certifikater understøttes direkte i de fleste webservere som fx Apache og Microsofts IIS. En af fordelene ved at benytte en USB-nøgle som iKey er desuden, at administratorerne kan bestemme, hvad der skal ske, når nøglen fjernes fra USB-porten. Den typiske konfiguration er at maskinen låses og kun kan låses op ved brug af nøglen. På den måde behøver medarbejderne ikke tænke på at logge ud, når de forlader arbejdsstationen eller hjemmearbejdspladsen, så længe de tager USB-nøglen med sig.

Rainbow Technologies' iKey-system er understøttet af fx Check Point i deres VPN-1 og Firewall-1 produkter, samt af flere andre producenter. Der er dog ikke tale om lige så bred en support som ved RSA's SecurID.
Det har også været muligt at have dette system til afprøvning. Denne er udført og beskrevet i Appendiks C.

5.9.3 Svagheder

Brugen af to-faktor autentificeringssystemer er ikke uden problemer. Ud over de administrationsmæssige og implementeringsmæssige problemer, er der nogle sikkerhedsproblemer med produkterne, som kræver overvejelse. Som nævnt i Appendiks C er problemet med RSA SecurID at en enkelt kompromitteret enhed i visse tilfælde kan gøre hele to-faktor autentificeringen værdiløs for alle brugere. Selvom dette problem nu er blevet bekræftet af producenten og vil blive rettet i produktet er det vigtigt at overveje, at der kan eksistere denne type sikkerhedsproblemer i autentificeringsmetoderne. For iKey-produktet er der også sikkerhedsproblemer. @stake Inc. (tidligere l0pht Research Labs) offentliggjorde den 20. juli 2000 et dokument [64] hvori de beskriver en svaghed ved iKey 1000-nøglen. Ved at have fysisk adgang til enheden i ca. 30 sekunder er det muligt at omkode den administrative kode (MKEY) til en valgfri værdi udelukkende ved brug af standardværktøjer (artiklen inkluderer desuden en opskrift på hvordan dette værktøj kan laves for $10). Det er uklart, om denne sårbarhed også eksisterer i iKey-2000 systemet som normalt benyttes til sikre installationer (grundet en indbygget krypteringschip). Der er dog umiddelbart ingen grund til at tro, at systemet skulle være anderledes i denne version. Da sårbarheden kræver fysisk

[61] Billedet er fra Rainbow Technologies hjemmeside på adressen http://www.rainbow.com/

åbning af enheden – og disse kun har været til udlån – er det ikke blevet forsøgt at afprøve om dette er muligt med en iKey 2000.

Der findes andre typer fysiske sårbarheder ved to-faktor autentificeringsudstyr. Forskeren Sudhakar Govindavajhala fra Princeton University har ved at tænde en elektrisk lampe tæt ved en hukommelseschip fremprovokeret en fejl, hvor en bit får ændret sin værdi [67]. Ved at lade et Java-program køre samtidig, kunne den ændrede bit sørge for, at dette program fik lov til at udføre kommandoer, som normalt ikke er tilladt for programmet. Succesraten var ca. 70 %. Forskeren har derefter kommenteret [68], at idet mange smartcards benytter Java, skulle der ikke være noget i vejen for at bruge denne metode til at bryde sikkerhed på disse kort.

Generelt giver brugen af to-faktor udstyr stærkt forbedret sikkerhed ved autentificering af brugerne. Men teknologien bør ikke stå alene, og sikkerhedsfejl i udstyret bør ikke i sig selv være nok til at kompromittere systemet. Der bør – som altid – være adskillige lag af sikkerhed, så svagheder på et lag ikke alene er nok til at bryde sikkerheden[62].

5.10 Terminal Services / Citrix

Brugen af tynde klienter er kendt fra ældre UNIX-systemer, hvor en enkelt maskine servicerede mange klienter, som ikke i sig selv var i stand til at afvikle programmer. I grove træk var der i de tynde klienter blot tale om skærme, tastaturer og netkort mens serverne afviklede programmer, gemte filer osv. Da prisen for personlige computere senere faldt til et prisleje, hvor det var muligt at placere en komplet maskine på hvert skrivebord, blev ideen om den serverbaserede struktur stort set lagt til side.
I de senere år er den dog dukket op igen. Vedligeholdelsesudgifterne til de mange individuelle maskiner kan i mange tilfælde være høj, ligesom sikkerhedsaspektet i en centraliseret struktur er lettere både at overskue og administrere. Samtidig har udviklingen af hurtige netværk, grafiske operativsystemer og stor datakraft gjort det muligt at centralisere afviklingen af også grafiske applikationer og operativsystemer. Således kan fx Windows 2000 i dag afvikles via tynde klienter fra centrale servere stort set uden brugeren er klar over, at det ikke afvikles lokalt. Fra et administrativt synspunkt er det langt lettere at udskifte en tynd klient, som herefter fortsat viser brugerens personlige applikationer, indstillinger og filer end at servicere en komplet arbejdsstation. Samtidig kan brugeren slukke for sin klient for næste dag at fortsætte præcist hvor hun slap, idet serveren fortsætter med at afvikle programmerne selvom brugeren ikke længere er aktiv på systemet.

Terminal Services (TS) er indbygget i Microsoft's server-operativsystemer fra Windows 2000 og frem og er en metode til at etablere den ovenfor beskrevne serverbaserede struktur. Citrix har i samarbejde med Microsoft bygget videre på dette koncept, og tilbyder en række produkter, som bygger på samme princip. Citrix-systemer kan køre på både UNIX, Solaris og Windows og klienterne kan være af næsten hvilken som helst type inklusive håndholdte enheder, tynde klienter, Mac, Linux og naturligvis Windows. Ud over platformssupporten tilbyder Citrixprodukterne opbyggelsen af serverfarme, web-portaler og sikkerhedsstyring samt integration med mange tredjeparts produkter, som ikke umiddelbart understøttes af TS.

For hjemmearbejdspladser kan en Citrix-løsning være et alternativt bud på, hvordan medarbejdere kan tilgå information og applikationer på virksomhedens netværk. Ved at etablere tynde klienter (eller komplette arbejdsstationer, som delvist udnytter den serverbaserede struktur) i hjemmene, kan mange sikkerhedsproblemer undgås. Tynde klienter kan ikke i sig selv blive inficeret med vira, trojanske heste eller keyloggere. Opsætningen kan ikke ændres lokalt, ligesom det ikke er muligt at benytte maskinen til andet end at oprette forbindelse til virksomhedens netværk. Til gengæld fungerer enheden kun, hvis netværksforbindelsen kan etableres. Løsningen er derfor primært interessant i situationer, hvor en bredbåndsforbindelse i hjemmet kan sikre "always on" forbindelse til virksomheden og ikke i tilfælde, hvor telefonlinien benyttes til at ringe op til virksomheden.

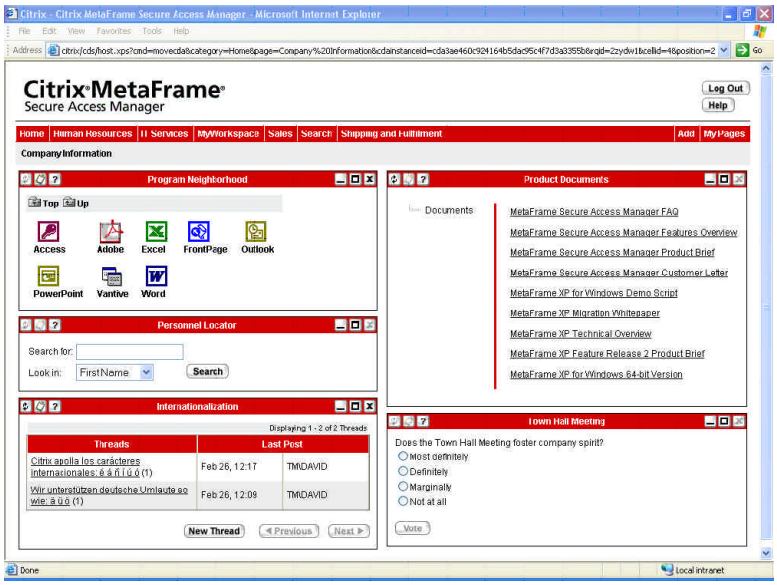
Nedenfor gennemgås de teknologier og produkter, som tilsammen udgør et bud på, hvordan hjemmearbejdspladser kan kobles op mod en Citrix-baseret løsning i virksomheden på en sikker og brugervenlig måde.
En sådan løsning vil bestå af produkterne MetaFrame XP Presentation Server, MetaFrame Secure Access Manager samt Secure Gateway for MetaFrame. Kombineret og implementeret korrekt kan disse tre produkter levere sikker, web-baseret adgang til virksomhedens interne dokumenter og applikationer. Denne adgang kan udbygges med et brugervenligt interface. Løsningen vil bygge på en Windows 2000 eller 2003 Server-platform, men kan også udvides til at inkludere UNIX- og Solaris-maskiner. De tre produkters funktioner er beskrevet nedenfor:

- MetaFrame XP Presentation Server (PS) er Citrix' primære produkt og danner grundlaget for enhver Citrix-løsning. PS afvikler de valgte applikationer og leverer skærmbilleder på baggrund af brugerens tilsendte muse- og tastetryk. Til forskel fra Microsoft's TS understøttes load balancing, bedre skalering (op til 100.000 samtidige brugere) og mulighed for at administrere serverparken og brugernes opsætninger

[62] Der er i afsnittet om iKey benyttet information fra Rainbow Technologies hjemmeside på adressen http://www.rainbow.com/ samt fra [65], [66] og [78].

centralt. Citrix tillader desuden såkaldte seamless vinduer, som muliggør afviklingen af applikationer fra en server på almindelige arbejdsstationer uden at brugeren ved, at applikationen ikke afvikles lokalt.

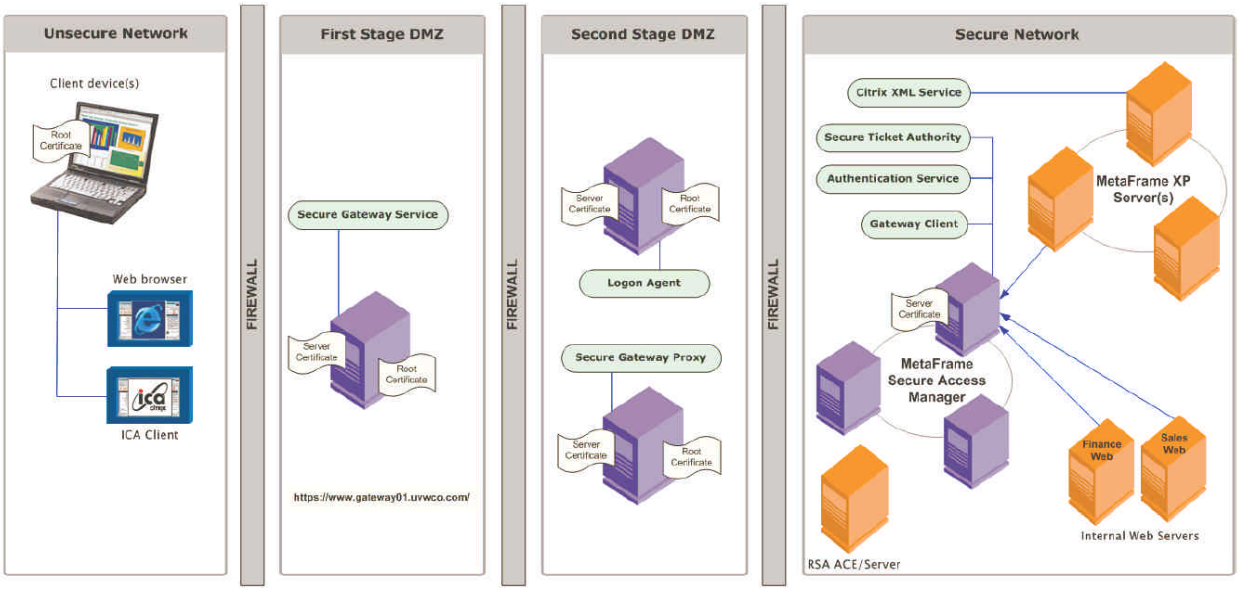
- MetaFrame Secure Access Manager (SAM) leverer sammen med PS en web-baseret adgang til både applikationer og filer samt til interne webservere i virksomheden. Disse informationer og applikationer samles i en browserbaseret brugergrænseflade, som præsenteres for brugeren. Samtidig gøres brugen af systemet uafhængigt af brugerens udstyr. Dette sker ved at levere en ActiveX eller Java-baseret Citrix-klient til brugeren, hvis ikke denne allerede er i besiddelse af en "ægte" klient. Et eksempel på, hvordan SAM samler informationer fra PS-farme, web-servere samt dokumenter og databaser, kan ses på figur 42.



Figur 42 - Citrix Secure Access Manager

- Secure Gateway for MetaFrame (SG) er en udvidelse til SAM som gør det muligt at publicere informationer og applikationer til medarbejdere, som befinder sig udenfor virksomheden. Produktets primære opgave er at sikre kommunikationen mellem brugeren og de benyttede servere. Ved at placere serveren i en DMZ er der ikke behov for at åbne adgang direkte fra internettet til det interne netværk. SG er transparent for brugeren og understøtter både brugen af ActiveX/Java-klienter samt "ægte" ICA-klienter på alle platforme.
  SG består desuden af en logon agent som reelt er de ASP-sider, brugeren benytter ved web-baseret logon.

I en opsætning til brug ved hjemmearbejdspladser vil de tre produkter benyttes til at levere information og programmer over internettet til brugere af mobile eller stationære enheder. Ved brug af SG er det muligt at undgå brugen af VPN for at sikre trafikken. Dette sker ved at benytte digitale certifikater via en SSL-forbindelse mellem brugeren og SG-serveren. Idet al trafik herefter vil gå igennem denne forbindelse, skal kun port 443 (SSL) være åben. Fra denne server etableres en ny forbindelse enten direkte til de interne servere eller via en dobbel-hop DMZ til en sekundær SG-server, som håndterer logons og kommunikerer med de interne servere. Ved kun at åbne port 443 er der ikke direkte adgang til ICA-protokollen udefra (benytter port 1494). Samtidig er der ingen følsomme oplysninger på SG-serveren, og selv en kompromitteret SG-server kan kun lave opslag i den efterfølgende SG-server. Fra denne er der adgang til de interne servere igennem port 1494 via ICA-protokollen, men disse kontaktes via SAM-serverne. Skulle man opnå direkte adgang til SAM-serverne fra en kompromitteret SG-server, skal sikkerheden i både SAM og de øvrige servere brydes, før der kan opnås adgang til virksomhedens interne informationer.
Dette princip kan ses på figur 43 nedenfor. Forbindelsen mellem klienten og SG-serveren i den første DMZ etableres via SSL enten via en webbrowser eller en ICA-klient. Autentifikation til serveren foregår via digitale certifikater, og det er desuden muligt at lade serveren autentificere brugeren på samme måde. Trafikken er herefter krypteret samt sikret mod modifikation (sidstnævnte via hash funktioner). Selve adgangen til Citrix-systemet sker via den logon agent, som er placeret i anden DMZ. Accepteres brugeren tillades adgang videre i systemet til SAM.



Figur 43 - Dobbel-hop DMZ opsætning af Citrix Secure Gateway [69]

Som det ses på figur 43 er det muligt at benytte RSA's SecurID system sammen med Citrix. I dette tilfælde integreres SecurID i logon agenten, og brugeren vil blive valideret via både brugernavn og SecurID-systemet. RSA ACE/Serveren kan placeres i det interne netværk og fungere sammen med øvrige systemer, som benytter SecurID-autentificering.

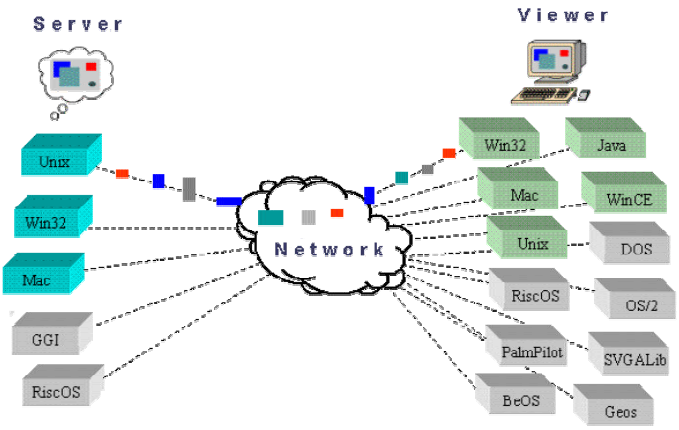
I en opsætning som ovenstående kan enhver klient med en browser benyttes til at tilgå virksomhedens interne systemer, idet de nødvendige programmer leveres i form af ActiveX eller Java. Der kræves ingen opsætning af klienten og brugeren kan frit flytte sig mellem Unix, Windows, tynde klienter og bærbare enheder. Trafikken beskyttes med SSL og to-faktor autentificering understøttes i form af SecurID. Det er også muligt at benytte Citrix-systemet ovenfor igennem en VPN-forbindelse fra hjemmearbejdspladserne.

En serverbaseret struktur er ikke altid en god løsning, idet visse applikationer ikke kan afvikles via systemet ligesom det kræver, at brugerne altid er tilkoblet serverne. Men i de tilfælde, hvor brugen tillader det, kan det være et værdifuldt værktøj til både at etablere forbedret sikkerhed samt forenklet administration. Som det er vist ovenfor, kræver det dog omtanke at etablere en fornuftig sikkerhed for systemet. Samtidig bør klienterne stadig beskyttes, idet direkte fysisk adgang til en klient stadig udgør en betragtelig sikkerhedsrisiko. Adgang til netværksudstyret, som forbinder klienter, er også fortsat et problem, som ikke bliver løst af brugen af tynde klienter.
Det skal også nævnes, at meget grafiktunge applikationer som CAD og desktop publishing ikke er velegnede til brug i Citrix-miljøer. De meget tunge grafiske billeder tager tid at overføre over selv hurtige netværk, og da datakraften for at behandle billederne ofte er meget stor, vil det kræve meget store ressourcer på de servere, som skal afvikle applikationerne. Benyttes et stort antal specielle applikationer kan det desuden være problematisk at få disse afviklet på serverne, idet der i visse tilfælde kan være problemer med servebaseret afvikling af programmer, som ikke understøtter dette[63].

5.11 Fjernstyring af arbejdsstationer

I visse tilfælde kan det være nødvendigt at tillade direkte fjernstyring af specifikke arbejdsstationer eller servere. Dette kan fx være tilfældet i udviklingsmiljøer, hvor programmerne udelukkende kan afvikles på bestemt hardware. Forskellen mellem serverbaseret afvikling af programmer og fjernstying af maskiner er, at mens den serverbaserede afvikling leverer applikationsskærmbilleder til klienten, viser fjernstyringssoftwaren det billede, som maskinen sender til sin egen skærm. Samtidig giver serverbaseret afvikling mulighed for at mange brugere benytter samme server, mens fjernstyring normalt kun tillader én bruger per maskine.

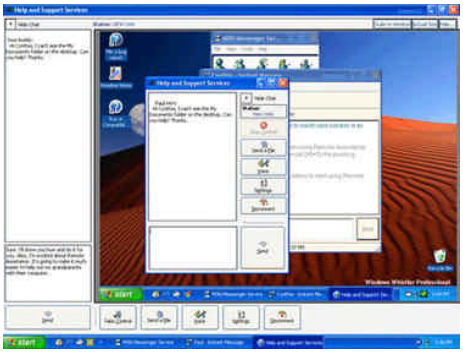
[63] Der er i afsnittet brugt information fra [69], [70], [71], [72] samt fra Citrix' hjemmeside på http://www.citrix.com/



Figur 44 - Understøttede platforme med VNC[64]

For at tillade hjemmearbejdspladser at få adgang til bestemte arbejdsstationer kræves fjernstyringssoftware, som kan overføre skærmbilleder og tastetryk mellem hjemmearbejdspladsen og arbejdsstationen i virksomheden. Denne overførsel af informationer bør sikres på bedst mulige måde, ligesom sikkerheden omkring tilgangen til arbejdsstationen skal sikres.
Der findes adskillige produkter til fjernstying af arbejdsstationer. Et af dem er VNC, og som det ses på figur 44 er programmet udviklet til at understøtte en næsten vilkårlig kombination af platforme. VNC autentificerer brugeren ved hjælp af et password, som sendes krypteret mellem arbejdsstationen som skal fjernstyres og brugeren. Den resterende VNC-trafik (overførsel af skærmbilleder, tastetryk og musebevægelser) sendes ukrypteret, og det er derfor nødvendigt enten at sikre denne trafik eller at benytte VNC igennem en VPN-tunnel. Mere sikre versioner af VNC er under udvikling, bl.a. Secure VNC[65].
VNC virker kort fortalt ved at lade en server opdatere en klients framebuffer. Det sætter dermed meget små krav til klienten, som kan være en næsten hvilken som helst enhed, som kan kommunikere og vise grafiske skærmbilleder. Opdateringerne foregår ud fra simple kommandoer, som ”placer et rektangel med disse pixeldata ved position x,y”. Hvis både server og klient understøtter mere avancerede metoder, vil disse blive brugt. Dette kan fx være JPEG-komprimering af still-billeder eller MPEG-komprimering af levende billeder.
Når skærmbilledet skal opdateres, sender serveren ændringerne fra det foregående skærmbillede. Da dette ofte er meget få data, kan billedet virke flydende selv med meget små båndbredder.

Kører arbejdsstationen, som skal fjernstyres, Windows XP Professional kan Microsoft’s Remote Desktop system benyttes. Dette er i princippet en terminal service-baseret funktion, men fungerer mere som VNC idet kun én bruger kan benytte systemet ad gangen. Protokollen er langt mere kompleks end VNC og har indbyggede komprimeringsalgoritmer. Der kræves, at både klienten og den arbejdsstation som fjernstyres kører Windows hvilket har den fordel, at de dermed deler store dele af den metodik, som benyttes i den grafiske opbygning af vinduer. Dermed fås en betydeligt bedre responstid end ved fx VNC. Samtidig understøtter Remote Desktop ligesom Terminal Services og Citrix, at lyd, udprintninger og filer flyttes igennem forbindelsen, således at fx diskettedrevet i den lokale maskine vil blive til A:-drevet på den maskine, som fjernstyres. Remote Desktop-trafikken er desuden krypteret ligesom der kan benyttes smartcards til autentificering.



Figur 45 - Remote Desktop som supportværktøj[66]

Remote Desktop kan ud over muligheden for fjernstying af maskinen benyttes til support af brugerne, idet brugerens skærmbillede kan ses fra supportcenteret når brugeren ønsker hjælp. Dette er vist på figur 45. I modsætning til VNC findes Remote Desktop udelukkende til Windows-platformen, men dog inkl. Windows CE og PocketPC.

Der er store sikkerhedsovervejelser, som skal gennemtænkes før der tillades fjernstyingsadgang til en arbejdsstation. Arbejdsstationen bør beskyttes så kun enkelte enheder har mulighed for at kontakte maskinen. Selv hvis trafikken kommer fra disse enheder bør det sikres, at kun den korrekte trafik får lov at passere. Desuden bør brugeren der forsøger at opnå adgang autentificeres inden der tillades adgang. Hvis ikke applikationen selv kan håndtere dette tilfredsstillende, kan autentificeringen eventuelt udføres på en firewall, som placeres foran maskinen. Trafikken bør herefter fortsat være krypteret for at undgå, at denne kan aflyttes eller modificeres.
Der bør i det hele taget kun gives fjernstyringsadgang til arbejdsstationer, hvor det er absolut nødvendigt og hvor det er muligt at etablere en betydelig sikkerhedsstruktur rundt om maskinen.

5.12 Opsummering

De beskrevne teknologier kan hjælpe til at danne grundlaget for et design til implementering af sikre hjemmearbejdspladser. Samtidig har gennemgangen af teknologierne givet mulighed for at få et indblik i de netværksspecifikke problemstillinger. Nedenfor er kort opsummeret de nævnte teknologier:

[64] Billedet er fra RealVNC’s hjemmeside på adressen http://www.realvnc.com/
[65] Udviklingen af Secure VNC kan følges på adressen http://evilsecurity.com/vnc/
[66] Billedet er fra Microsoft’s hjemmeside på adressen
http://www.microsoft.com/windowsxp/pro/techinfo/planning/techoverview/helpandsupport.asp

- **VPN** – Brugen af VPN kan hjælpe til at forhindre aflytning af trafikken samt til at begrænse de nødvendige åbne adgange til virksomhedens netværk. Det kræver nøje overvejelser at implementere VPN-systemer korrekt, så de ikke giver anledning til flere sikkerhedsproblemer end de løser. Men de rige muligheder for autentificering, kryptering samt brugen af hard- og softwareløsninger kan i den rette kombination levere en velfungerende infrastruktur til sikring af trafikken til og fra hjemmearbejdspladsen.
- **VLAN og VACL** – Brugen af VLANs og VACLs er ikke direkte en hjemmearbejdspladsspecifik teknologi, men har alligevel stærke bånd til brugen af hjemmearbejdspladser. PVLANs kan segregere det fysiske netværk og sammen med VACLs sikre, at kun de enheder, som er nødvendige kan tilgås fra fx hjemmene. Dette virker begge veje – således modvirker teknologien også at enheder i virksomheden kan angribe hjemmearbejdspladserne.
- **802.1x** – 802.1x er en ny teknologi, som kan levere autentificering på lag 2 og dermed gøre det langt sværere for angribere at få adgang til netværket. I hjemmene kan dette bl.a. bruges til at sikre at opkaldsudstyret ikke kan benyttes af uautoriserede enheder.
- **Firewalls** – Selvom firewalls ikke nødvendigvis er det mirakelmiddel, de ofte anses for at være, kan de være et godt værktøj når de implementeres korrekt. Der er gennemgået packet filtering routers, circuit level gateways, application level gateways og stateful multi-layer inspection firewalls. De forskellige typers fordele og ulemper må overvejes i forbindelse med den aktuelle implementering, men det er vigtigt, at hverken virksomhedens eller hjemmets sikkerhed alene afhænger af firewalls da der ikke er tale om en ubrydelig barriere. Brugen af personlige firewalls kan hjælpe til at etablere et ekstra sikkerhedslag på enhedsniveau. I visse tilfælde kan det være en fordel at kunne håndhæve brugen af personlige firewalls samt være i stand til at distribuere konfigurationsopdateringer fra centralt sted.
- **Integritet** – Brugen af et integritetsværktøj kan gøre det muligt at overvåge hvilke ændringer der foretages til konfigurationer, filer og enheder. Dette kan både hjælpe til at opdage angreb, men også til at reetablere systemet, hvis angrebet er succesfuldt. Samtidig er det et godt værktøj til at modvirke menneskelige fejl.
- **Antivirus** – Beskyttelse mod virus og trojanske heste kan være en af de vigtigste forsvarsmekanismer. Beskyttelsen bør foregå på både arbejdsstationer, servere, hjemmearbejdspladser og ved tilgange til netværket som gateways, e-mail relays og eventuelt andet relevant udstyr. Kombinationen af hardware, antivirusprogrammel samt specielt software til detektion af trojanske heste kan samlet give en god beskyttelse af netværket.
- **Honeypots** – Honeypots og honeynets kan benyttes til at aflede angriberen og observere, hvordan angrebene udføres i et kontrolleret miljø. Således kan de både benyttes til at isolere angriberen for at beskytte værdifulde aktiver samt til at observere nye angrebsmetoder – en viden som kan være brugbar for de administratorer, som skal beskytte netværket mod disse.
- **To-faktor autentificering** – Brugen af to-faktor autentificeringsmetoder kan afhjælpe problemer med passwords som enten kan gættes, aflyttes eller brydes på anden vis. RSA leverer en løsning, som er kompatibel med meget andet udstyr, mens Rainbow Technologies kan benytte digitale certifikater, som ud over autentificering også kan benyttes til signering af dokumenter, e-mails osv. Begge metoder har dog sine ulemper, og udrulningen af to-faktor autentificering kan være både kostbar og administrationskrævende. Spørgsmålet er, om det er sikkerhedsmæssigt forsvarligt ikke at benytte teknologien.
- **Citrix** – Terminal services og Citrix-løsninger kan benyttes til at give adgang til netværksressourcer for både mobile enheder og hjemmearbejdspladser. Da der kort fortalt er tale om overførsel af skærmbilleder, vil ingen data blive gemt i hjemmet, ligesom der kan laves per bruger-regler for, hvilke informationer der er tilgængelige og hvordan de vises.
- **Fjernstyring** – Der kan være brug for at fjernstyre enheder på virksomhedens netværk fra hjemmet. Programmer som VNC og Remote Desktop kan benyttes til dette, men der kræves specielle forholdsregler for at sikre, at fjernstyringen sker på en sikkerhedsmæssig forsvarlig måde.

De ovenfor nævnte teknologier er på ingen måde en komplet liste over de metoder, som kan benyttes til at sikre hjemmearbejdspladser. Det er en gennemgang af nogle af de mest udbredte metoder til at løse nogle af de sikkerhedsproblemer, som blev nævnt i kapitel 3.

6 DESIGNKRAV

Inden et netværksdesign baseret på sikkerhedspolitikken fra kapitel 2 samt sikkerhedsproblemer og mulige sikkerhedsløsninger fra kapitel 3 udformes, gennemgås nedenfor en række vejledninger, gode råd, lovmæssige krav og best practices fra primært danske, men også udenlandske organisationer og virksomheder.
Denne gennemgang har til formål at give et bredere perspektiv af sikkerhedsproblematikken og løsningsmetoder samt samle de oplysninger, som i Danmark er væsentlige i forbindelse med etableringen af hjemmearbejdspladser. Således giver lovgivningen, danske organisationer som DK•CERT, standarder som DS 484 samt internationale certificeringer alle indirekte råd og vejledning til, hvordan sikring af hjemmearbejdspladser kan gennemføres. Kombineret med sikkerhedspolitikken, beskrivelsen af sikkerhedsproblemerne samt de tekniske løsninger vil disse informationer danne grundlag for det designforslag, som udfærdiges i kapitel 7.

Til sidst i kapitlet opsamles og konkretiseres alle de krav og forslag, som er gennemgået i rapporten. Den tabel, som herefter udfærdiges, vil danne grundlaget for det egentlige designforslag.

6.1 Best Practices

En række organisationer og virksomheder har udgivet forskellige dokumenter med anbefalinger og gode råd til implementering af hjemmearbejdspladser. Disse er samlet under betegnelsen ”Best Practices” i dette afsnit.
Der er i ingen tilfælde tale om en definitiv guide til en sikker implementering af hjemmearbejdspladser. Ofte fokuseres der på enkelte dele af problematikken, og i de fleste tilfælde er dokumenterne meget utekniske med fokus på primært de ledelsesmæssige problemer.
Det kan undre, at der i Danmark ikke er udfærdiget en guide eller et sæt af anbefalinger, som kan hjælpe administratorer, udviklere og systemdesignere til at etablere sikre hjemmearbejdspladser. Forhåbentligt kan samlingen af disse best practices sammen med beskrivelsen af standarder, certificeringer og lovgivninger give et samlet overblik over nogle af de tilgængelige ressourcer, som kan benyttes til dette formål.

6.1.1 DK•CERT

Danmarks Computer Emergency Response Team (CERT) blev oprettet i 1991 i forbindelse med en af Danmarks første hackersager[67]. DK•CERT’s formål er at:

”[...] opbygge en samlet viden, der sætter DK•CERT i stand til at offentliggøre og udsende advarsler, og anden information om potentielle risici og begyndende problemer” samt at ”*modtage henvendelser om sikkerhedsrelaterede hændelser og koordinere indsatsen på området*”[68].

Desuden offentliggøres løbende artikler med bl.a. rådgivning samt forebyggelse af sikkerhedshændelser.
Ud fra ovenstående ville det være forventet, at DK•CERT har udformet et omfangsrigt dokument, som fortæller om potentielle risici samt forebyggende handlinger i forbindelse med hjemmearbejdspladser. Dette er dog ikke tilfældet. DK•CERT’s journalist Torben B. Sørensen [120] har dog udarbejdet en kort artikel om sikring af hjemmearbejdspladser.
Hovedpunkterne i denne artikel er listet nedenfor:

- Adskillelse af private netværk og hjemmearbejdspladsen i hjemmet
- Virusbeskyttelse
- Sikring af kommunikationen mellem hjemmet og virksomheden. Her foreslås enten brug af telefonnettet eller VPN. Førstnævnte foreslås sikret ved at sikre, at kun de valgte telefonnumre kan oprette forbindelsen. En sikkerhed baseret på denne type identifikation er dog langt fra umulig at omgå. Benyttes et privat telefonsystem (en PBX) kan det udgående CLID (Caller Line Identifier) ofte sættes valgfrit for hvert lokalnummer. En anden metode er at få oplysningen til at ringe et nummer op for dig. Herefter sendes dit eget nummer ikke længere med[69]. Der findes flere andre metoder til at omgås CLID sikkerheden [79].
- Brugen af en personlig eller hardwarebaseret firewall i hjemmet for at beskytte forbindelsen mod eksterne angreb. Her nævnes desuden skaleringsproblematikken med visse typer udstyr.

[67] Her er formentligt tale om sagen med de danske hackere JubJub Bird og Sprocket. Via hjemmecomputere og modems brød de ind i computere hos Danmarks Tekniske Højskole og angreb herfra maskiner i primært USA og Sydafrika. De blev opdaget af NASA som tog kontakt til UNI-C i slutningen af 1990.
[68] Citaterne er fra DK•CERT’s hjemmeside, se https://www.cert.dk/kontakt/
[69] Dette er mere kompliceret end som så. CLID er ikke den eneste identifikation af opkaldene. Der findes en mere grundlæggende identifikation, som kaldes ANI (Automatic Number Identification). Der er ingen måde at undgå, at dette nummer sendes sammen med egne samtaler. Men hvis oplysningen foretager opkaldet for dig, videresendes ANI ikke. Ved at bede oplysningen ringe nummeret på et telefonkortselskab (ikke testet på danske selskaber dog) vil en automatiseret procedure anmode om, hvilket nummer der ringes fra. Det nummer som indtastes her, vil blive benyttet som CLID for det videre opkald.

Der gives ikke bud på de konkrete tekniske løsninger, men opfordres blot til, at disse sikkerhedsproblemer overvejes.

6.1.2 CSIRT

CSIRT (Computer Security Incident Response Team) er TDC Internets sikkerhedsafdeling som tager sig af sikkerhedsrelaterede hændelser på internettet. Det erklærede formål er [80]:

"*at assistere Tele Danmarks kunder i håndtering af IT sikkerhedsrelaterede hændelser*".

CSIRT har den 29/8-2000 nedskrevet ti overvejelser [81], som bør gennemgås, før der etableres hjemmearbejdspladser. Disse er beskrevet nedenfor:

- Hvilke datasystemer skal medarbejderen have adgang til? Fx e-mail, lønsystemet osv.
- Skal det være samme system, som medarbejderen har adgang til fra virksomheden?
- Hvordan klassificeres data? Fx opdelt som offentlige, fortrolige og hemmelige dokumenter.
- Fortroligheden af data over usikre netværk bør sikres, ligesom data der lagres lokalt på hjemmearbejdspladsen bør krypteres.
- Fysisk sikkerhed i hjemmet bør overvejes. Fx hvem der har adgang til hjemmearbejdspladsen, samt en vurdering af risikoen for tyveri.
- Udskrivning i hjemmet, opbevaring af fortrolige udskrifter og eventuelt tilintetgørelse af disse bør overvejes.
- Der bør udarbejdes en sikkerhedspolitik, der bestemmer hvordan udstyret må anvendes samt hvordan ansvaret er fordelt.
- Logisk sikring af udstyret, dvs. sikring mod trojanske heste, vira, eksterne angreb og lignende skal etableres. Ligeledes skal en sådan beskyttelse holdes ved lige.
- Virksomheden bør overveje, om der kun skal tilbydes faste hjemmearbejdspladser, eller om mobile enheder også tillades.
- Hvilken "Access-mode" skal anvendes – dvs. om der skal benyttes direkte linier eller om internettet (med eller uden VPN) skal benyttes.
- Autentifikationsmekanismer. Hvis der benyttes opkaldslinier kan A-nummer verificering og dial-back overvejes. Stærk brugerautentifikation (OTP, smartcards osv.) kan også overvejes.

CSIRT har desuden udfærdiget en kort rapport omkring sikring af hjemmearbejdspladser [90]. Denne rapport beskriver, hvordan dial-back, VPN og tynde klienter kan benyttes til at levere sikkerhed for hjemmearbejdspladserne. Anbefalingen er, at der uanset valg af metode benyttes stærk autentifikation.

6.1.3 Ministeriet for Videnskab, Teknologi og Udvikling

Ministeriet har bl.a. udarbejdet en vejledning om hjemmearbejdspladser, som skal:

"*være en støtte for ledelse og medarbejdere i både private virksomheder og offentlige myndigheder, inden pc-arbejdspladser etableres i privatboligerne*" [82].

Rapporten omhandler primært de ledelsesmæssige og økonomiske aspekter af indførelsen af hjemmearbejdspladser. Således fortælles det, at der ressourcemæssigt kræves en IT-medarbejder pr. 35-50 hjemmearbejdspladser. Mere praktisk gennemgås de overvejelser, der skal gøres, før indkøbet af udstyr foretages. Der er vejledning til mængden af RAM, skærmens genopfriskningsfrekvens og hvilken type farveprinter, der har den bedste sidepris.
Der gives gode råd til udformningen af en sikkerhedspolitik, og der skrives, at:

"*opkoblingen af en hjemme-PC til virksomhedens netværk [...] ikke i sig selv[udgør] en større risiko, end når andre arbejdsstationer kobles til virksomhedens netværk*" [82].

Denne udtalelse synes dog ikke at være i overensstemmelse med tanken om, at virksomhedens systemer ofte vil være langt bedre beskyttede end hjemmets.
Vejledningen fra ministeriet opstiller en række konkrete sikkerhedskrav og råd til hjemmearbejdspladser. Disse er nævnt nedenfor:

- Arbejdet med sikkerhed bør anskues som en kontinuerlig proces
- Der bør stilles krav til kvaliteten af passwords, udskiftningsfrekvens og forbud mod genbrug af passwords på mindre sikre systemer.
- Hvis der foretages lokal lagring af oplysninger på hjemmearbejdspladsen bør disse krypteres.
- Hvis der udskrives information på en printer i hjemmet skal det overvejes, hvordan disse informationer beskyttes og eventuelt destrueres. Ifølge arkivloven skal færdigbehandlede dokumenter opbevares betryggende.

- Privat brug af hjemmearbejdspladsen bør overvejes nøje og et ansvar for denne eventuelle brug placeres. Benyttes hjemmearbejdspladsen privat, bør en firewall og antivirusprogrammel installeres.
- Overvejelser omkring problemer med den fysiske sikkerhed bør gennemføres.
- Hvis der benyttes opkaldslinier (som fx ISDN) skal der trækkes foranstaltninger, som forhindrer uautoriserede opkald til det centrale system. Eksempler kan være brugen af dial-back, passwords, OTP osv.
- Der bør foretages en registrering (logning) af brugen af opkaldslinierne.
- Hvis der overføres personlige oplysninger, skal forbindelsen mellem hjemmet og virksomheden anvende kryptering.
- Virksomhedens firewall, der beskytter mod eksterne angreb, bør sættes op, så den også dækker hjemmearbejdspladserne. Hvis ikke dette er muligt, bør hjemmearbejdspladserne udstyres med egne firewalls (enten software- eller hardwarebaserede). Det understreges, at datatilsynet stiller krav om, at personoplysninger beskyttes ved opsætning af en firewall.
- Da mange angreb forekommer internt i virksomheden kan det være relevant at opsætte et IDS.
- Hjemmearbejdspladserne skal forsynes med antivirusprogrammel, og dette programmel skal holdes opdateret.
- Ved salg og reparation af udstyret, bør alle virksomhedsrelevante data destrueres.
- Benyttes digitale signaturer bør det overvejes, om den private signaturnøgle skal opbevares på et chip-kort.
- Det næves desuden, at Datatilsynet kan kræve adgang til lokaler hvoraf behandling af personoplysninger foregår. Dette inkluderer dermed også hjemmearbejdspladser. Inspektionsadgangen giver altså adgang til medarbejderens hjem.

Vejledningen indeholder primært krav og råd, som allerede er indeholdt i enten lovgivninger eller andre best practices. Den er mest fokuseret på administrative og ledelsesmæssige forhold og er derfor ikke teknisk grundig i forbindelse med sikkerhedsaspekterne.

6.2 Standarder

Standardernes overordnede funktion er at fastlægge et fornuftigt udgangspunkt for IT-sikkerhedsarbejdet. Dvs. standarderne samler det, en virksomhed bør gøre for at opnå optimal balance i IT-sikkerheden. Ofte vil standarden indeholde en liste over de generelle sikkerhedsproblemstillinger, som alle virksomheder bør forholde sig til. Værdien ved at overholde en standard kan være større troværdighed, bedre image og et mere gennemskueligt sikkerhedsniveau. Standardiseringer giver også mulighed for at have et sæt standarder at trække på, både når virksomhedens sikkerhedspolitik udformes, samt når selve netværksdesignet skal laves. Samtidig kan en virksomhed opnå en certificering efter disse standarder som for potentielle kunder og samarbejdspartnere kan give et indtryk af, at virksomheden tager IT-sikkerhed alvorligt.
I Danmark benyttes primært to standarder for IT-sikkerhed, ISO 17799 samt Dansk Standard DS-484. Disse er beskrevet nedenfor.

6.2.1 ISO 17799

ISO 17799:2000 standarden [83] er baseret på British Standard 7799-1:2000. Dokumentet har titlen ”Information Technology – Code of practice for information security management”. Som titlen angiver, er der tale om en række anbefalinger indenfor IT-sikkerhed, som primært er rettet mod ledelsen. Der er dermed ikke tale om et teknisk dokument, som går i dybden med specifikke sikkerhedsproblemer og –løsninger, men derimod en samling af overvejelser.
Standarden er meget bred og gør som eksempel opmærksom på, at der kan være problemer med støv på netværksudstyr. Samtidig er der konkrete forslag til, hvordan virksomheden sikrer systemer mod ondsindet software. ISO 17799 har tidligere været brugt i denne rapport i forbindelse med sikkerhedspolitikken. Nedenfor forsøges det at udtrække de konkrete forslag og råd, som undertegnede mener, kan være behjælpelige i forbindelse med udarbejdelsen af et netværksdesign. Dette skal ikke ses som en komplet liste over konkrete tiltag i standarden og ej heller som en indikation af, at standardens yderligere afsnit og information ikke har værdi i forbindelse med netværksdesign. Det er alene et forsøg på at udtrække konkrete elementer, som senere vil blive benyttet til – sammen med den øvrige information i bl.a. dette afsnit – at danne grundlag for det netværksdesign, som i denne rapport forsøges udført.
I standardens introduktion foreslås det, at der udvælges metoder fra standarden ud fra en overvejelse om omkostninger vs. den risiko, som virksomheden mener, kan reduceres. Sådanne økonomiske overvejelser er ikke direkte udført nedenfor. Dette skyldes, at det er forsøgt at gøre denne del af rapporten så generel som mulig.
Listen nedenfor benævner det relevante afsnit fra standarden i parentes hvorefter en kort beskrivelse gives.

- **(8.3.1)** Beskyttelse mod ondsindet software som vira, trojanske heste osv. Der anbefales brug af antivirussoftware med jævnlige opdateringer. Antivirussoftwaren bør benyttes både på arbejdsstationer, servere, e-mail gateways osv. Brugen af integritetsudstyr til at sikre, at uautoriseret data eller uautoriserede ændringer til eksisterende data opdages foreslås også.

- **(8.4.1)** I forbindelse med hjemmearbejdspladser bør det overvejes, hvordan data som eventuelt opbevares udenfor virksomheden kan undergå jævnlig backup.
- **(8.5.1.c)** Integriteten og fortroligheden af data, som transmitteres over offentlige netværk, bør sikres. Samtidig skal systemer, som er koblet på disse forbindelser (fx hjemmearbejdspladser) sikres.
- **(8.7.4.1)** Sikkerhedsproblemerne med offentliggørelse af e-mailadresser og ekstern adgang til e-mailkonti bør overvejes.
- **(8.7.6)** Adgangen til offentligt tilgængelige systemer (fx placeret i en DMZ) må ikke tillade utilsigtet adgang til interne netværks
- **(9.1.1.2)** Brugen af reglen ”forbyd alt, som ikke tillades” i stedet for ”tillad alt, som ikke forbydes” når der udvikles regelbaserede adgangssystemer bør vælges.
- **(9.2.1)** Det bør sikres, at alle brugere har unikke brugernavne og ikke deler ”gruppekonti”
- **(9.2.3)** Passwords skal ændres jævnligt, være sikre og kun udleveres til brugeren efter denne er identificeret. Brugen af to-faktor autentificering bør overvejes.
- **(9.3.1)** Passwords bør overholde krav om kompleksitet, længde og levetid. Det bør desuden sikres, at passwords ikke gemmes på computeren.
- **(9.4.2)** Kontrol af den rute, trafikken følger mellem brugerens arbejdsstation og den service, som brugeren forsøger at kontrollere bør udføres. Dette kan fx indebære sikring af, at netværksportes adgang er begrænset, at bestemte applikations-gateways benyttes eller at adgangen til visse destinationer ledes gennem gateways, som analyserer informationen. Det næves desuden, at virtuelle netværk bør benyttes til at opdele virksomhedens netværk og dermed begrænse tvær-adgangen mellem netværk.
- **(9.4.3)** Adgangskontrol for eksterne brugere. Afhængigt af det påkrævede sikkerhedsniveau bør kryptografiske teknikker, hardware enheder eller challenge/response protokoller benyttes. Benyttes opkaldslinier skal det sikres, at de sårbarheder, som eksisterer ved sådanne systemer behandles – fx det tidligere nævnte problem, hvor en angriber kan få virksomhedens modems til at tro, at forbindelsen er afbrudt selvom dette ikke er tilfældet.
- **(9.4.5)** Diagnosticeringsporte på netværksudstyr bør være enten slået fra eller beskyttet. Disse porte giver adgang til administrationen af netværksudstyret.
- **(9.4.6)** Segregering af de interne netværk bør ske for at undgå, at visse brugergrupper kan få adgang til andre gruppers informationer. Denne opdeling kan fx ske ved brugen af logiske netværk separeret med en firewall, som kontrollerer adgangen mellem netværkene.
- **(9.4.7)** Kontrol med udgående trafik, fx e-mails og filoverførsel bør udføres, for at sikre, at brugerne ikke sender konfidentielle data til eksterne maskiner hvis ikke dette ønskes.
- **(9.4.8)** Routingkontrol med trafik, som krydser grænsen mellem virksomhedens net og det offentlige net bør baseres på en sikker identifikationsmetode for afsender- og modtageradresser (IP numre).
- **(9.5.1)** Der kan benyttes automatisk terminalidentificering til at sikre, at bestemte forbindelser kun kan initieres fra bestemte arbejdsstationer. Herefter bør brugerne autentificeres.
- **(9.5.2)** Gode logonprocedurer bør bl.a. indeholde logning af usuccesfulde forsøg samt tidsforsinkelse før yderlige forsøg kan udføres.
- **(9.5.3)** Brugen af tokens, smart cards og biometriske enheder kan benyttes til at styrke autentifikationen af brugere.
- **(9.5.4)** Standardpasswords som benyttes til administration af udstyr og software bør ændres.
- **(9.5.8)** Begrænsning af tidspunkter for etablering af forbindelser samt forbindelsestid kan etableres. Dette gælder specielt for terminaler eller arbejdsstationer, som er placeret udenfor virksomheden som fx hjemmearbejdspladser.
- **(9.7.2)** Virksomheden bør logge alle aktiviteter, hvor brugere skal benytte deres konto eller password. Dette gælder også usuccesfulde forsøg på at logge på systemet, samt information fra eventuelle IDS’er og andre netværksenheder. Der bør samtidig benyttes et system, som kan finde de relevante informationer i logfilerne, når disse eventuelt skal benyttes. Disse logfiler bør sikres mod uautoriseret ændring eller sletning, ligesom logfilerne bør gennemgås jævnligt.
- **(9.7.3)** Urene på alle netværksenheder, computere, terminaler osv. bør være synkroniserede så informationer fra logfilerne tidsstemples korrekt
- **(9.8.2)** Hjemmearbejdspladserne bør sikres med hensyn til fysisk sikkerhed, sikkerhed i forhold til brugen fra familiemedlemmer eller besøgende, beskyttelse af kommunikationsudstyret samt overvågning i form af logning.
- **(10.5.1)** Når operativsystemer, programmer, konfigurationer eller andet ændres bør disse ændringer logges og godkendes af autoriserede personer.
- **(10.5.4)** Når nye programmer indkøbes bør det sikres, at der ikke er bagdøre eller trojansk kode i produktet. Dette kan ske ved at benytte programmer fra anerkendte leverandører, benytte open source (hvis der er ressourcer til at se kildekoden igennem), kontrollere, at der ikke ændres i koden efter implementering samt eventuelt benytte evaluerede produkter.
- **(12.1)** Virksomheden bør sikre, at gældende love og indgåede aftaler overholdes.

- **(12.2.2)** Det bør regelmæssigt sikres, at de benyttede systemer er korrekt implementeret. Dette bør som regel foretages af eksperter. Samtidig bør systemerne testes for muligheder for ulovlig indtrængen og kendte sårbarheder. Igen bør eksperter benyttes til dette.

De nævnte afsnit udgør de anbefalinger fra ISO 17799 standarden, som er fundet relevante i forbindelse med sikring af hjemmearbejdspladser. I afsnit 6.7 vil disse dermed være med til at danne grundlaget for valget af udstyr samt design.

Nedenfor gennemgås på samme måde Dansk Standard DS-484.

6.2.2 Dansk Standard

Dansk Standard har udarbejdet en standard for IT-sikkerhedsprocesser, DS-484 med titlen ”Norm for edb-sikkerhed”. DS 484 er delt i to dele. Første del rummer de krav, som skal overholdes for at en virksomhed med rimelig kan hævde at have et forsvarligt IT-sikkerhedsniveau. Anden del er skærpede krav, som finder anvendelse, når der sættes større krav til IT-sikkerheden.
Standarden indeholder i alt ca. 260 krav i første del, som primært omhandler personalesikkerhed, fysisk sikring, lovbestemmelser, risikovurderinger og sikkerhedspolitik.
DS 484 vedligeholdes, så den i videst muligt omfang er i overensstemmelse med ISO 17799-standarden. Således er den væsentligste forskel på ISO 17799 og DS 484, at sidstnævnte indeholder flere aspekter af IT-sikkerheden end ISO 17799. ISO 17799 er dermed en delmængde af DS 484. De steder, hvor DS går ud over ISO standarden er typisk hvor denne tilføjer specifikke danske krav. Anden del af DS 484 ligger delvist ud over, hvad ISO 17799 indeholder.
Mens ISO 17799 er en meget udbredt standard i mange lande, er der endnu ingen virksomheder, der er blevet certificeret efter DS 484 [122].

Ligesom for ISO 17799 ovenfor gennemgås her, de dele af DS 484, som kan være behjælpelige i forbindelse med udarbejdelsen af et netværksdesign til hjemmearbejdspladser. Kun de dele af DS 484 som ikke er inkluderet i ISO 17799 er medtaget nedenfor.

Del 1

- **(8.2.2)** Edb-systemer og netværk, der benyttes af flere brugere, skal beskyttes mod uautoriseret adgang og kontrolleres ved hjælp af formelle autorisationsprocedurer.
- **(8.3)** Uautoriseret brugeradgang må ikke kunne forekomme.
- **(8.4)** Det skal være muligt at fastslå og verificere identiteten af hver enkelt autoriseret bruger eller udstyr fra hver arbejdsstation eller lokation, hvorfra brugeren søger adgang.
- **(8.4.1)** Logon-proceduren skal afsløre så lidt som muligt om de edb-systemer, der forsøges opnået adgang til.
- **(8.4.2)** Al edb-anvendelse skal kunne spores til rette vedkommende.
- **(8.4.3)** Adgang fra en uautoriseret arbejdsstation via netværk skal forhindres.
- **(8.5)** For edb-netværk skal der findes kontroller, som sikrer imod, at tilsluttede brugere og edb-anlæg kompromitterer sikkerheden i netværket. Dette skal omfatte veldefinerede grænseflader mellem servicemuligheder i netværket, tilstrækkelige valideringsmekanismer for tilkoblede brugere og udstyrs autenticitet samt kontrol af brugeradgang til netværkets serviceydelser.
- **(8.5.2)** Opkobling af et netværk til et andet netværk og forbindelsesvejene mellem disse skal registreres og kontrolleres. Det skal begrænses, hvilke former for kommunikation, der må anvendes mellem forskelligt edb-udstyr og den edb-service, brugeren har autorisation til at anvende.
  Datakommunikation, der sker fra et lokalt netværk til ressourcer, som befinder sig på et åbent net eller vice versa, skal kontrolleres med skærpet overvågning og anvendelse af logiske filtre (firewalls) skal overvejes.
- **(8.5.4)** Der skal træffes foranstaltninger for at hindre skadepåvirkninger fra en ukontrolleret opkoblingsforbindelse fra et eksternt edb-anlæg, en arbejdsstation eller andet edb-udstyr.
- **(8.5.6)** Adgangskontrol for brugersystemer skal forebygge uautoriseret adgang til de informationer, der er lagret på dem.
- **(8.7.1)** Uønskede hændelser skal kunne spores.
- **(9.2.5)** Identiteten af afsender og modtager skal sikres. Hvis kodeord benyttes skal de beskyttes ved hjælp af kryptografering. Alternativt kan engangskodeord benyttes.
- **(9.2.6)** Uafviselighed kan benyttes ved at kombinere autenticitetssikring, integritetssikring og sikret kvitteringsprocedure.
- **(9.2.7)** Der skal etableres kontrol, så det sikres, at data ikke uautoriseret bliver transmitteret mere end én gang (replay)
- **(9.3.1)** Der skal udføres kontrol med overførsel af alle programmer for at sikre disse mod uautoriseret modifikation.
- **(11.3)** Loven om personoplysninger skal overholdes.

Del 2

- **(S7.2.6)** Enhver netværksmeddelelse eller dataenhed skal indeholde koder, som identificerer afsender og modtager.
- **(S7.2.7)** Der skal anvendes automatiske overvågningssystemer, som foretager logning og alarmering af uhensigtsmæssigheder og fejl på netværket. Al netværkstrafik skal logges.
- **(S7.3)** Der skal etableres et logisk filter (firewall) mellem virksomhedens LAN og eksterne netværk, som sikrer mod uautoriseret adgang og utilsigtet anvendelse af ressourcer eller programmer.
  Kritiske programmer skal beskyttes med en kontrol som sikrer, at de ikke kan eksekveres, hvis der er foretaget uautoriserede ændringer til programmerne. Denne kontrol skal være automatisk.
- **(S7.4.2)** Logning skal være automatisk og må ikke kunne afbrydes uforsætligt.
- **(S7.6.4)** Vedhæftede filer, som modtages via e-mail skal kontrolleres for ondsindede programmer og virus. Der kan stilles yderligere krav om e-mails' hemmeligholdelse, uafviselighed og integritet samt afsenders og modtagers autenticitet.
- **(S8.2.4)** Kodeord skal krypteres under transmission på eksterne netværk. I visse tilfælde skal engangskodeord også benyttes på interne netværk.
- **(S8.4.1)** Logon-proceduren skal vise en advarselsinformation om, at anlægget kun må benyttes af autoriserede brugere. Der må ikke gives information, som kan hjælpe uautoriserede brugere. Ved logon-fejl må det ikke indikeres, hvilke datadele der er korrekte eller ukorrekte.
- **(S8.4.3)** Alle eksterne enheder skal autentificeres (ud over brugerautentificeringen).
- **(S8.5.2)** Der skal etableres en overvåget, kontrollerende grænsepassage (fx firewall) mellem lokale og eksterne netværk. Dette system skal understøtte bl.a. følgende:
  - Logisk adgangskontrol.
  - Autentificering.
  - Overvågning og eventuel afvisning af eksekverbare programmer inkl. Java, Cookies mm.
  - Virusbeskyttelse.
  - Beskyttelse mod spoofing.
  - Alarmering af uautoriseret aktivitet.
  - Kontrol af datakommunikationsretning.
  - Proxy-support.
  - Begrænsning af protokoller og services.
  - Logning.
  - Enheden som udfører dette skal være godkendt af et anerkendt certificeringsorgan.
- **(S8.5.6)** Den hardware som benyttes til rutekontrol skal være certificeret.
- **(S9.2.3)** I visse tilfælde skal følsomme og fortrolige data beskyttes med et anerkendt kryptograferingssystem eller baseret på anerkendte og certificerede hardware-sikkerhedsmoduler.
- **(S9.2.4)** I visse tilfælde skal følsomme og fortrolige data beskyttes med en digital signatur baseret på et anerkendt kryptograferingssystem eller baseret på anerkendt og certificerede hardware-sikkerhedsmoduler.
- **(S9.2.5)** I visse tilfælde skal autenticitetssikringen baseres på en asymmetrisk kryptograferingsteknik og evt. kombineres med en biometrisk verifikationsmetode.
- **(S9.2.7)** Identifikation og tidsstempler på datameddelelser må ikke kunne manipuleres uden at det afsløres for dermed at undgå replay.

Som det ses er de i del 2 beskrevne retningslinier i mange tilfælde meget specifikke og sætter store krav til både selve udstyret, men specielt implementeringen af det. Dette kan i mange tilfælde kræve meget store ressourcer og er kun i et vist omfang medtaget i det design, som kan ses i kapitel 7.

6.3 Certificering og evaluering

Mens en virksomhed kan blive certificeret efter en standard som fx ISO 17799, kan udstyr også certificeres og evalueres. Dette giver potentielle brugere af udstyret bedre mulighed for at vurdere den sikkerhed, som udstyret kan levere. En certificering kan således give en indikation af, at udstyret overholder nogle fastsatte standarder, mens en officiel evaluering kan levere en analyse af udstyrets kunnen og design, som brugerne af udstyret kan gennemse inden beslutningen om valget af udstyr træffes.
Certificering er en verificering af, at et produkt lever op til en specificeret standard eller efterkommer bestemte minimumskrav. ICSA er et eksempel på en certificering.
Evaluering er på den anden side en metodologi til at verificere, at et produkts påståede funktionaliteter lever op til etablerede sikkerhedskrav. Common Criteria er et eksempel på en evaluring.

Certificering og evaluering af sikkerhedsprodukter kan være en hjælp i designfasen. De giver en indikation af, i hvilket omfang udstyret overholder fastsatte standarder for IT-sikkerhed.

6.3.1 ICSA

ICSA (International Computer Security Association) Labs officielle målsætning er:

"*to achieve major risk reduction within certified products and systems"* [84]

ICSA certificerer stort set alle sikkerhedsrelaterede produkter fra antivirussoftware til firewalls. Certificeringen er baseret på udstyrets evne til at modstå angreb og er ikke baseret på bestemte designprincipper eller teknologier. Dette afspejler en "black box" måde at udføre tests på.
ICSA certificeringer udføres på en bestemt version af et produkt (både hardware og software). Producenten forpligter sig herefter til at sikre, at alle fremtidige versioner og opdateringer til produktet foretages, så disse stadig følger kravene fra certificeringen – og samtidig udføres så ofte, at opdateringer til certificeringskravene til stadighed overholdes. For at sikre, at dette overholdes af producenterne udfører ICSA Labs tilfældige kontrolchecks, ligesom hele certificeringsproceduren skal gentages årligt for de certificerede produkter.

Selve certificeringskriterierne udarbejdes af ICSA Labs ud fra input fra sikkerhedseksperter, organisationer, udviklere, brugere, universiteter og mange andre. De endelige kriterier godkendes af et udvalg, som primært består af et bredt spektrum af offentligt anerkendte sikkerhedseksperter.
Testen af produkterne er baseret på både automatiserede og manuelle procedurer. Disse er reproducérbare og så vidt muligt objektive.

Motivationen for at få certificeret et produkt er at brugerne får en sikkerhed for, at produktet overholder krav, som et bredt spektrum af eksperter har besluttet er nødvendige. Fra brugerens synspunkt fås en sikkerhed, som ikke alene er baseret på egne erfaringer og viden, men på et stort antal eksperters vurderinger.
Antallet af certificerede produkter er svært at opgøre direkte. Således er der fx 39 hardwarebaserede firewallprodukter, som er certificerede. Dette dækker dog over firewall-serier. Fx er Cisco's serie af PIX produkter samlet under et i denne optælling. Alene for Cisco's vedkommende dækker dette over fem modeller i PIX 500 serien. Den samme problematik for optælling gør sig gældende ved routere, antivirusprogrammel osv.

Det er vigtigt at understrege, at ICSA certificeringen ikke betyder, at produktet er modstandsdygtigt overfor alle sårbarheder og angreb. Som eksempel findes der 16 kendte sårbarheder i de ICSA certificerede Cisco PIX firewalls[70]. I samme omgang skal dog nævnes, at Cisco har forpligtet sig til løbende at opdatere de certificerede produkter og sikre overholdelse af ICSA-standarden til alle gældende tider. Således opdateres de pågældende produkter løbende, og Cisco's sidste opdatering af PIX serien skete den 7. maj 2003[71]. En fuldt opdateret Cisco PIX har ingen kendte sårbarheder ifølge SecurityFocus og Cisco[72].[73]

6.3.2 Common Criteria

Common Criteria (CC) er resultatet af mange års forsøg på at udvikle internationalt anerkendte kriterier for evalueringen af IT sikkerhed [85]. Således er Trusted Computer System Evaluation Criteria (TCSEC), Information Technology Security Evaluation Criteria (ITSEC), Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) og Federal Criteria for Information Technology Security (FC) alle forløbere for CC.
I oktober 1998 underskrev regeringer fra USA, Canada, Frankrig, Tyskland og England en aftale om brugen af CC. Formålet var at sikre, at produkter kun skal evalueres én gang hvorefter denne evaluering kan genbruges på tværs af landegrænser. Senere er andre landet kommet på listen, men det bør understreges, at Danmark ikke er på listen over lande, som accepterer CC ("The Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security") eller som kan udføre CC evalueringer[74].
For at sikre, at CC forbliver uafhængig af kommercielle interesser sendes resultaterne fra enhver evaluering til det respektive lands Common Criteria Organization. Disse offentlige instanser foretager en uafhængig validering af evalueringen. Det er denne uafhængighed der adskiller CC fra andre evalueringssystemer og sikrer, at evalueringsprocessen er homogen og konsekvent på tværs af evalueringslaboratorierne.

CC består af følgende elementer:

- **Protection Profile (PP)** – en model som specificerer generelle sikkerhedskrav til produktklasser og –systemer (fx Intrusion Detection Systemer). Disse modeller genbruges og er ikke produktspecifikke.
- **Security Target (ST)** – definerer sikkerhedskrav til det specifikke produkt.
- **Target Of Evaluation (TOE)** – definerer det specifikke produkt (eller dele af et produkt), som skal evalueres.

[70] Sårbarhederne er hentet fra SecurityFocus.com
[71] Cisco advisories og sikkerhedsopdateringer kan ses på adressen http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/prod_security_advisories_list.html
[72] Gældende for juni 2003.
[73] Der er i afsnittet benyttet information fra ICSA Labs hjemmeside på adressen http://www.icsalabs.com/
[74] Medlemslandene og de ansvarlige dele af regeringerne kan ses på adressen http://www.commoncriteria.org/registry/NatScheme.html

CC evalueringer er inddelt i en række adskilte niveauer afhængigt af den mængde detaljer og de teknikker, som bruges under evalueringen. Der findes syv definerede niveauer – EAL 1 (laveste bekræftelse) til EAL 7 (højeste bekræftelse). EAL står for Evaluation Assurance Level. Typiske kommercielle produkter er evalueret efter EAL 1 til EAL 4 idet de højere bekræftelsesniveauer specificerer krav, som kun er nødvendige i de mest restriktive regeringsmiljøer. Ifølge Cisco er EAL 4 det højeste universelle evalueringsniveau, der endnu er implementeret af CC[75]. Dog er der på CC's hjemmeside et enkelt produkt, som har opnået EAL 5. Det kan også med rimelighed antages, at produkter, som har opnået en meget høj EAL måske af sikkerhedsmæssige årsager ikke er at finde på en officiel liste over evaluerede produkter. Ofte vil produkter med så høje EALs være til militært brug.
De forskellige EAL niveauer gennemgås kort nedenfor.

- **EAL1** – evaluering på dette niveau burde bevise, at produktet fungerer på en måde, som er konsistent med dokumentationen.
- **EAL2** – benyttes, hvis brugere eller udviklere ønsker et lav til moderat niveau af uafhængig sikret sikkerhed – ofte i tilfælde, hvor producenten ikke kan eller vil medhjælpe.
- **EAL3** – her bekræftes enkelte tests, som oprindeligt er foretaget af producenten af produktet. Samtidig bekræftes det, at producenten har ledt efter åbenlyse sikkerhedshuller i produktet.
- **EAL4** – dette er det højeste niveau, det menes at være kommercielt realistisk at tilføje til et eksisterende produkt. Der kræves stadig ingen specialister, specifik viden eller store ressourcer for at gennemføre evalueringen. Der foretages en analyse af de grundlæggende designprincipper for TOE'en, ligesom en mindre del af implementeringen gennemgås. En uafhængig søgning efter åbenlyse sikkerhedshuller gennemføres.
- **EAL5** – produkter, som ønsker dette evalueringsniveau bliver formentligt designet efter dette formål. Hele implementeringen af produktet analyseres. Der foretages en uafhængig søgning efter sårbarheder, som sikrer modstandsdygtighed overfor angribere med et moderat angrebspotentiale.
- **EAL6** – der stilles her meget store krav til design- og implementeringsprocessen. Den uafhængige søgning efter sårbarheder skal sikre modstandsdygtighed overfor angribere med et stort angrebspotentiale.
- **EAL7** – kun stærkt fokuserede sikkerhedsprodukter, som skal benyttes i ekstreme højrisikosituationer bør overveje dette niveau. En fuldstændig, uafhængig analyse af samtlige tests udført af producenten gennemføres. Der stilles meget store krav til design- og implementeringsarbejdet. Evalueringen kan kun gennemføres på produkter, som har et meget simpelt design.

Det er vigtigt at understrege, at evalueringsniveauerne foretages ud fra et af producenten fastsat Security Target. Dette er en beskrivelse af krav, som producenten ønsker den del af produktet TOE'en udgør, evalueret mod. Det giver derfor ikke umiddelbart mening at angive, at et produkt har opnået et EAL4-niveau, hvis ikke også ST'en og TOE'en gengives, så brugeren kan se, hvilke dele af produktet, der med en "vishedsgrad" på EAL4 lever op til hvilke krav.
Op til og med EAL4 er der ikke krav om, at selve udstyret testes. Der er alene tale om, at en stor mængde dokumentation i samarbejde med producenten gennemgås og valideres.

CC er betragtet som den "højeste" standard indenfor sikkerhedsevalueringer. Dette er primært fordi der er tale om en internationalt anerkendt, uafhængig evaluering, som er godkendt af en lang række lande og som valideres af offentlige instanser uden kommercielle interesser.

Under 100 produktserier er blevet evalueret i henhold til CC[76]. Dette spænder over software som Microsoft's Windows 2000 til firewalls som Cisco's PIX serie. Det er som ved ICSA svært at få et komplet overblik over, hvor mange produkter der faktisk er tale om. Dette skyldes, at der i visse tilfælde er tale om hele serier af produkter, mens der er i andre tilfælde er tale om et enkelt produkt baseret på en bestemt softwareversion. Generelt er CC mindre fleksibel end ICSA i den forstand, at produkterne skal genevalueres for hver software og hardwareversion. Således er en Cisco PIX model 535 med software version 6.2.2 evalueret efter et EAL4-niveau. Opgraderes denne software senere, mister produktet sin EAL.

Som med ICSA giver en CC-evaluering ingen garanti for, at udstyret er modstandsdygtigt overfor ethvert angreb eller ikke indeholder sårbarheder, som kan benyttes til at forbigå sikkerheden. Samme eksempel, som blev beskrevet ovenfor med en Cisco PIX i forbindelse med ICSA gør sig gældende for CC – bortset fra, at det ikke er muligt at opdatere udstyret når nye sikkerhedshuller opdages, hvis evalueringsbekræftelsen skal beholdes[77].

[75] Cisco's påstand kan ses på adressen
http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a00800b0d87.html
[76] Dette tal er kun delvist korrekt idet der er tale om 93 produkter, hvis sikkerhedsprofil er offentliggjort. I enkelte tilfælde kan der anmodes om ikke at blive medtaget på denne liste. Dette kan fx ske ud fra overvejelser om national sikkerhed og lignende.
[77] Der er i afsnittet brugt information fra [85] og [86].

6.4 Persondataloven

Persondataloven er navnet på lov nr. 429 af 31. maj 2000 og gælder for offentlige myndigheder, private virksomheder, foreninger osv., men dog ikke for privatpersoner. Den erstatter de to tidligere registerlove. I modsætning til registerlovene gælder persondataloven ved enhver form for behandling af personoplysninger og ikke blot registrering eller videregivelse. Persondataloven dækker dermed også behandling af personoplysninger, som finder sted fra hjemmearbejdspladsen. Personoplysninger defineres som enhver form for information om en identificeret eller identificerbar fysisk person. Eksempler på dette kan være navn, adresse, e-mailadresse og lignende.

I forhold til hjemmearbejdspladser er der flere dele af loven, som er relevante. De vigtigste forhold er beskrevet nedenfor:

Transmission af følsomme oplysninger – Fra §41 stk. 3 fremgår det, at:

"den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger [...] kommer til uvedkommendes kendskab". Bekendtgørelse nr. 528 af 15. juni beskriver, *at "der kun må etableres eksterne kommunikationsforbindelser, hvis der træffes særlige foranstaltninger for at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger"*.

Når virksomhedens netværk tilsluttes internettet eller andre åbne net, skal der ifølge Datatilsynet træffes foranstaltninger, som sikrer imod uvedkommende trafik og forhindrer adgang fra det åbne net til den det interne net. Konkret har Datatilsynet udtalt, at tilstrækkelig sikkerhed kan opnås ved etablering af en firewall så længe denne opsættes korrekt, løbende kontrolleres og ajourføres. Dette betyder, at hvis virksomheden er i besiddelse af personoplysninger, (dette vil stort set altid være tilfældet, da alene navne på ansatte betragtes som personoplysninger) er der lovmæssige krav om, at virksomheden tager hånd om sikkerheden, når denne forbindes til internettet. Datatilsynet klargør, at arbejdet med sikkerhed er en kontinuerlig proces og lægger op til, at etablerede sikkerhedssystemer løbende revideres.
Minimumskravene når personfølsomme data transmitteres over internettet omfatter, at data ikke kan læses eller ændres. Datatilsynets opfattelse er, at hvis der er tale om oplysninger af følsom karakter (dvs. omfattet af §7 stk. 1 og §8 stk. 1), skal der benyttes stærk kryptering baseret på en kendt algoritme. Dette er defineret som symmetrisk kryptering med en nøglelængde på 128 bit eller mere. Algoritmen bør være certificeret i overensstemmelse med ITSEC (Information Technology Security Evaluation and Certification). Dette kan fx være DES, Triple-DES eller AES.
Sikkerhed for autenticitet og integritet skal sikres i fornødent omfang fx via elektronisk signatur eller fortrolige adgangskoder. Datatilsynet anbefaler brugen af såkaldte challenged passwords eller OTP.

Hjemmearbejdspladsen – For at sikre forsvarlig behandling af persondata i hjemmet har Datatilsynet listet en række forhold, der skal tages stilling til. Dette omfatter lokal lagring af oplysninger, lokal udskrivning af oplysninger, fysisk sikkerhed, beskyttelse af opkaldslinier og sikkerhedsforanstaltninger ved privat brug af maskinen.
I henhold til §59 og §60 kan Datatilsynet give virksomheden påbud med hensyn til behandling af persondata. Ifølge §62 har Datatilsynet ret til – uden retskendelse – at få adgang til lokaler, hvorfra behandlingen sker. Dette gælder dermed også medarbejdernes hjem, hvis der her behandles personfølsomme oplysninger.

Logning – Det er ikke tilladt at indsamle oplysninger, hvis man ikke aktuelt har noget at bruge dem til, men blot forventer, at der senere viser sig et formål. Samtidig må der ikke indsamles flere oplysninger, end hvad der er nødvendigt, ligesom indsamlingen af oplysninger generelt skal ske til specifikke og saglige formål.
Generelt skal den registrerede afgive sit udtrykkelige samtykke før registreringen finder sted. Rent praktisk er Datatilsynets anbefaling i forbindelse med automatisk logning, at der gives information om denne, inden den finder sted. Som eksempel skal brugeren informeres, *inden* en cookie sendes til hende fra en hjemmeside. Information om, hvem der indsamler oplysninger, hvad der indsamles og til hvilke formål, skal desuden være tilgængeligt.
Der er specielle regler for offentlige myndigheder som fx sætter krav om, at der foretages registrering af alle afviste adgangsforsøg fra samme arbejdsstation. Selvom disse krav ikke direkte gælder for private virksomheder, er det Datatilsynets opfattelse, at der som udgangspunkt stilles samme krav til datasikkerheden i private virksomheder som i den offentlige forvaltning, såfremt forholdene er sammenlignelige[78].

Opsummering
Da en virksomhed næppe kan garantere, at der aldrig vil blive behandlet personlige oplysninger fra en hjemmearbejdsplads, skal denne sikre, at både hjemmearbejdspladsen og transmissionen af data sikres efter nogle af Datatilsynet fastsatte standarder og anbefalinger. Ønsker virksomheden desuden at logge data på forskellig måde, fx

[78] Der er i afsnittet om persondataloven anvendt oplysninger fra [87], fra Datatilsynets hjemmeside på adressen http://www.datatilsynet.dk/ samt fra [82].

i forbindelse med IDS, oplyser Datatilsynet, at denne form for logning godt kan godkendes, selvom den i princippet vil indeholde information, som ikke må logges. Dette godkendes, fordi det ikke er muligt at undgå rent teknisk. Samtidig går denne type logning under oplysninger, der ikke aktuelt er noget at bruge til, men som det blot forventes, at der senere viser sig et formål med – altså en type, som Datatilsynet som udgangspunkt ikke tillader. Men igen gælder, at hvis formålet med logningen er fx et IDS – og hvis der samtidig etableres procedurer for, hvordan disse data slettes efter fx 30 dage – kan Datatilsynet godt godkende, at disse data opsamles[79].

6.5 Terrorpakken

Terrorpakken er navnet på en dansk lovændring der trådte i kraft efter terrorangrebet på New York City den 11. september 2001. De for hjemmearbejdspladser relevante dele af terrorpakken (som officielt hedder Anti-terrorpakken) er primært fokuseret på §786 stk. 4 og 5 [88]. Stk. 4 siger, at udbydere af telenet eller teletjenester skal foretage registrering og opbevaring i et år af oplysninger om teletrafik. Dette skal senere kunne bruges til efterforskning og retsforfølgning. De praktiske forhold omkring dette samt hvordan samarbejdet med politiet skal foregå (stk. 5), fastsættes senere af justitsministeren sammen med ministeriet for videnskab, teknologi og udvikling. Normalt vil ovenstående ikke påvirke virksomheder, idet disse som udgangspunkt er undtaget fra loven. Kun internetudbydere vil blive pålagt at foretage den omtalte registrering. Kristina Tranders fra IT Sikkerhedskontoret i IT & Telestyrelsen [116] fortæller dog, at situationen hvor datatrafikken er krypteret mellem hjemmet og virksomheden, endnu ikke har været behandlet. Problemet er, at internetudbyderne i dette tilfælde ikke har mulighed for at foretage den krævede registrering. Denne problemstilling vil derfor nu blive taget op i den arbejdsgruppe, som behandler sagen. Kristina Tranders ville ikke udelukke, at det kan blive påkrævet virksomhederne at foretage denne registrering i tilfælde, hvor virksomhedens brug af hjemmearbejdspladser forhindrer internetudbyderne i at udføre registreringen.
Samtidig kan politiet altid kræve indsigt i trafikken, hvis en retskendelse giver dem ret til dette. Dette sker udenom terrorloven, og det må derfor antages, at virksomheden i sådanne tilfælde skal kunne levere disse data. Der sættes dermed indirekte krav om, at virksomheden er i stand til at opsamle data på denne måde.

Terrorpakken giver ligeledes politiet ret til (§791b) i visse tilfælde, at ”aflæse ikke offentligt tilgængelige oplysninger i et informationssystem ved hjælp af programmer eller andet udstyr (dataaflæsning)”. Dette vil normalt kunne oversættes til, at politiet får mulighed for at benytte keyloggere. I visse tilfælde vil brugen af softwarebaserede keyloggere ikke være mulig. Det er dog ikke besluttet, i hvor stort omfang virksomheden i sådanne tilfælde skal kunne være i stand til at levere denne adgang til politiet.

6.6 Fremtidssikring

Det bør overvejes, i hvor vid udstrækning det udstyr som designet baseres på skal være fremtidssikret. I hvilket omfang forventes antallet af brugere og båndbredde at stige? Planlægger virksomheden implementering af IPv6 indenfor en årrække? Er der ønsker om at benytte IP-telefoni, selvom dette ikke implementeres i første omgang? Sådanne spørgsmål kan danne grundlaget for nogle overvejelser omkring valg af udstyr. Besparelserne ved indkøbet kan blive til større udgifter senere, hvis ikke der tages højde for virksomhedens fremtidsplaner. Antallet af hjemmearbejdspladser bestemmer til en vis grad kapaciteten af det udstyr, som skal håndtere disse forbindelser. Men forventer virksomheden, at antallet stiger fremover, bør det overvejes, om denne dimensionering af udstyret skal medtages ved første implementering for at undgå senere udgifter til udskiftning af udstyret med dertil knyttede omkostninger.
Det er dog ikke kun båndbredde og antal forbindelser der bør overvejes. Hvis virksomheden kan forvente en øget angrebsaktivitet eller kan se frem til at arbejde med mere følsomme oplysninger, bør det overvejes, om de sikkerhedskrav dette medfører, skal tages med i overvejelserne.

6.7 Opsamling af krav

Sikkerhedspolitikken fra kapitel 2 betragtes som et udgangspunkt, der indeholder rammerne for det ønskede netværksdesign. Kombineret med ovenstående anbefalinger, lovkrav og best practices er nedenfor udarbejdet en tabel over mange af de egenskaber, som netværket bør opfylde. Denne tabel benyttes som en kravspecifikation for designforslaget, og vil blive gennemgået igen i kapitel 8 hvor designforslaget vurderes. I tabellen gives nogle produktforslag, som primært har baggrund i de i kapitel 5 gennemgåede teknologier. Det undersøges desuden om produkterne er certificerede eller evaluerede af de ovenfornævnte organisationer. Specielt angående CC evaluering skal det understreges, at et EAL-niveau ikke i sig selv er udtryk for en brugbar information. I tilfælde hvor dette er af væsentlig betydning for beslutningen bør Security Target som minimum gennemlæses.

Som beskrevet af SANS [89] kan de sikkerhedsmæssige krav, som beskriver forskellige forhold omkring beskyttelse af netværket, opdeles i følgende kategorier:

[79] Ifølge samtale med forskellige medarbejdere hos Datatilsynet den 1/7-2003.

- **Prevention** (forebyggelse)
  Passivt forsvar.
  Gennemtænkt design, implementering og konfigurering af netværket. Routerfiltre, firewalls og andre passive forsvarsmekanismer indgår her.
- **Pre-emption** (tiltag som foretages for at komme fjenden i forkøbet)
  Aktivt forsvar.
  Brugeruddannelse, kontrol med brugernes opførsel samt infiltrering af angribernes verden for at få et forhåndskendskab til nyeste angrebsmetoder. Desuden forebyggende scanninger mod eget netværk.
- **Deterrence** (afskrækkelse)
  Sikkerhedens PR-afdeling.
  Camouflage af de kritiske systemer samt fremhævelse af styrken af sikkerhed, som omringer systemet kan hjælpe til at afskrække angribere.
- **Deflection** (afbøjning)
  Afledningsmanøvrer.
  Oprettelse af honeypots, honeynets og lignende systemer for at få angribere til at fokusere på falske systemer.
- **Detection** (detektering)
  Detektivarbejdet.
  På baggrund af data fra logfiler og kendte angrebssignaturer kan systemet advare administratorer om, at et angreb er undervejs eller har været foretaget. Bestemte aktiviteter kan af systemerne markeres som mistænkelige og senere efterforskes.
- **Countermeasures** (modtræk)
  Netværkets indsatsstyrke.
  Proaktive intrusion detection systemer kan reagere på angreb ved lukke dele af netværket, begrænse brugerens adgang eller lukke helt af for angriberens adresser.

Disse kategorier er beskrevet nærmere i ordbogen. Formålet med opdelingen er at få en anerkendt kategorisering af udstyret, hvilket kan hjælpe til at give overblik over dets funktionalitet. Således er ovenstående kategorier anerkendte betegnelser i litteraturen, og ud fra nedenstående tabel kan det dermed ses, hvilke forholdsregler virksomheden tager i forbindelse med fx detektering eller forebyggelse af angreb.

Nedenfor er vist tabellen over de samlede krav, deres kategorisering, hvor kravene kommer fra samt produktforslag. I de tilfælde hvor de foreslåede produkter har opnået en ICSA eller CC certificering/evaluering er dette angivet. Følgende forkortelser benyttes i tabellen:

- **PR, PE, DE, DF, DT, CM** er forkortelserne for Prevention, Pre-emption, Deterrence, Deflection, Detection og Countermeasures.
- Kilderne er forkortet med **SP** (sikkerhedspolitik), **CSIRT** (Computer Security Incident Response Team i Danmark), **CERT** (Computer Emergency Response Team i Danmark), **ISO** (ISO 17799-standarden), **DS** (Dansk Standard DS-484), **PL** (persondataloven), **TL** (terrorloven) samt **MVTU** (rapporten fra Ministeriet for Videnskab, Teknologi og Udvikling).
  DS benyttes, når dette ikke er inkluderet i **ISO**.

Et eksempel kunne således være følgende:
Kravet om at data ikke må lagres lokalt, stammer fra sikkerhedspolitikken (SP). Dette hører under kategorien prevention (forebyggelse, PR) idet det er en forebyggende handling at undlade at gemme data lokalt, så eventuelle angribere ikke kan tilgå data direkte på hjemmearbejdspladsen. Kilden er som nævnt sikkerhedspolitikken, og et produktforslag kan være brugen af Citrix-systemer. Da Citrix-systemet ikke er certificeret af ICSA eller CC, er dette felt ikke udfyldt.

Tabellen kan ses som en opsummering af de i rapporten relevante og konkrete tiltag, som et netværksdesign bør overholde. Den benyttes til at konkretisere kravene fra rapportens tidligere afsnit og tilknytte produkteksempler til disse krav. Tabellen gennemgås igen i kapitel 8 hvor hvert krav gennemgås for at undersøge, hvorvidt designforslaget overholder de nævnte krav – samt hvordan disse i så fald overholdes.

Krav	PR	PE	DE	DF	DT	CM	Kilder	Produktforslag	Certificering
Computer må ikke efterlades forbundet til netværket							SP	• BluePosition bluetooth positionsudstyr • Passwordbeskyttet screen saver	
Data må ikke lagres lokalt							SP, CSIRT, MVTU, PL	• Citrix • Windows 2000/XP med Group Policies	CC EAL4 (Windows 2000)
Bredbåndsforbindelsen i hjemmet må deles med privat udstyr / privat udstyr skal holdes adskilt fra hjemmearbejdspladsen							SP / SP, CERT /, ISO /, PL /	• Adskillelse med firewalls, fx Cisco PIX 501 og Nokia IP130 • Alternativt CyberCity's løsning baseret på SonicWall Tele3TZ	ICSA, CC EAL 4 (begge) ICSA
Passwords må ikke gemmes i PC							SP	• Citrix • Windows 2000/XP med Group Policies	CC EAL 4 (Windows 2000)
Hjemmearbejdspladsen skal opdateres med nyeste service packs, patches, antivirus-signaturer, konfigurationsopdateringer mm.							SP, CSIRT, MVTU, PL	• Citrix • Windows 2000/XP med Group Policies • Cisco VPN Concentrator samt RealSecure server eller Zone Labs Integrity server • CyberCity's opdateringsservice	CC EAL 4 (Windows 2000)
Autentifikation må ikke alene baseres på passwords							SP, CSIRT, ISO, PL	• RSA SecurID • Digitale certifikater via Cisco VPN 3002+VPN Concentrator	
Data i transit mellem hjemmet og virksomheden skal beskyttes mod aflytning, genafspilning og ændring							SP, CSIRT, MVTU, ISO, DS, PL	• IPSec VPN via Cisco VPN 3002 og VPN Concentrator	
Krypteringsalgoritmer skal baseres på fx DES, Triple-DES eller AES							PL, DS	• IPSec VPN via Cisco VPN 3002 og VPN Concentrator	
Alle arbejdsstationer og brugere skal være unikt autentificeret							SP, DS	• 802.1x via fx Cisco Catalyst switche • Digitale certifikater via Cisco VPN 3002 og VPN Concentrator • RSA SecurID	

Krav	PR	PE	DE	DF	DT	CM	Kilder	Produktforslag	Certificering
Hjemmearbejdspladsen skal være beskyttet mod eksterne angreb							SP, CERT, CSIRT, MVTU, ISO, PL	• Cisco PIX 501 • Nokia IP130 • SonicWall Tele3 TZ	ICSA, CC EAL 4 ICSA, CC EAL 4 ICSA
Den enhed, som beskytter hjemmet mod eksterne angreb skal opdateres centralt							SP, CSIRT	• Cisco PIX 501 • Nokia IP130 • SonicWall Tele3 TZ	ICSA, CC EAL 4 ICSA, CC EAL 4 ICSA
Hjemmearbejdspladsen skal sikres mod trojanske heste							SP, CSIRT, ISO	• Tauscan • McAfee VirusScan Thin Client	
Hjemmearbejdspladsen skal sikres mod virus							SP, CERT, CSIRT, MVTU, ISO	• McAfee VirusScan Thin Client • McAfee WebShield • McAfee GroupShield • Norton AntiVirus Corporate Edition	ICSA
Hjemmearbejdspladsen skal sikres mod keyloggers							SP	• Citrix • Tauscan • McAfee VirusScan Thin Client • Tripwire • RealSecure Desktop Protector • Zone Labs Integrity	CC EAL 1
Hjemmearbejdspladsen skal sikres mod andre potentielle trusler							SP, DS	• Cisco PIX 501 • Nokia IP130 • SonicWall Tele3 TZ • Tripwire • RealSecure Desktop Protector • Zone Labs Integrity	ICSA, CC EAL 4 ICSA, CC EAL 4 ICSA CC EAL 1
Installationer og ændringer af konfigurationer på hjemmearbejdspladsen må ikke være mulig for brugere eller angribere							SP	• Citrix • Windows 2000/XP med Group Policies • Tripwire • RealSecure Desktop Protector	CC EAL 4 (Windows 2000) CC EAL 1

Krav	PR	PE	DE	DF	DT	CM	Kilder	Produktforslag	Certificering
Så vidt muligt skal hjemmearbejdspladsbrugeren autentificeres før der etableres forbindelse til virksomheden							SP, DS		
Hjemmearbejdspladsens bør sikres fysisk							CSIRT, MVTU, ISO, PL	• Kensington-låse til netværksudstyr og computer	
Autentificering skal ske mod centraliseret valideringsdatabase							SP	• RADIUS-server, fx Cisco ACS	
Passwordregler om kompleksitet mm. skal overholdes							SP, MVTU, ISO	• RADIUS-server fx Cisco ACS	
Virksomhedens udstyr skal beskyttes mod eksterne, interne og hjemmearbejdsplads-brugere							SP, ISO, PL	• Cisco PIX 515E • CheckPoint Firewall-1 NG • Cisco Catalyst switche med VLAN, PVLAN, VACL • Cisco NIDS som fx IDSM-2 • Honeynet	ICSA, CC EAL 4 CC EAL 4
Virksomhedens opkaldspunkter må ikke fremstå som tydelige angrebsmål							SP	• Honeynet og en honeypot som fx honeyd	
Logon proceduren skal afsløre så lidt som muligt							DS	• Cisco VPN Concentrator • Citrix Secure Gateway • Webservere, e-mail servere	
Hjemmearbejdspladsbrugernes adgang skal kunne begrænses							SP, DS, CSIRT	• Cisco Catalyst switche med VLAN, PVLAN og VACL • Cisco PIX 515E • CheckPoint Firewall-1 NG • Citrix Secure Access Manager	ICSA, CC EAL 4 CC EAL 4
En offentlig maskine må ikke kunne angribe andre (inkl. hjemmearbejdspladsen)							SP, ISO	• Cisco Catalyst switche med PVLAN, VACL • HIDS'er på alle servere • CheckPoint Firewall-1 NG • Cisco NIDS som fx IDSM-2	CC EAL 4
Trafikken til og fra hjemmearbejdspladsen må ikke kunne aflyttes af eksterne eller interne brugere i virksomheden							SP	• Cisco Catalyst switche med VLAN, PVLAN, VACL • CheckPoint Firewall-1 NG	CC EAL 4

Krav	PR	PE	DE	DF	DT	CM	Kilder	Produktforslag	Certificering
Der må ikke kunne initieres forbindelse fra virksomhed til hjemmearbejdsplads							SP	• CheckPoint Firewall-1 NG • Cisco Catalyst switche med PVLAN, VACL	CC EAL 4
Der skal (og må) foretages overvågning af brugen af hjemmearbejdspladserne (logning)							SP, MVTU, ISO, PL, (TL)	• Cisco NIDS som fx IDSM-2 • Cisco PIX 515E • Cisco PIX 501 • Cisco VPN 3002 • CheckPoint Firewall-1 NG • SonicWall Tele3 TZ • HIDS-enheder • Nokia IP130 • Tripwire • RealSecure Desktop Protector • Zone Labs Integrity • Citrix-systemer • Event logs fra Windows-klienter	ICSA, CC EAL 4 CC EAL 4 ICSA ICSA, CC EAL 4 CC EAL 1
Alle loginforsøg skal (og må) overvåges							ISO, DS, PL, TL	• Honeypot som honeyd • IDS-enheder • Cisco VPN Concentrator • Citrix Secure Gateway • RADIUS-server som Cisco ACS	
Det må ikke være muligt at omdirigere trafikken fra hjemmet til virksomheden							SP	• Cisco VPN 3002 eller SonicWall Tele3 TZ med digitale certifikater	ICSA
Opstilling af IDS i virksomheden anbefales							MVTU, ISO	• Cisco Catalyst switche med NIDS som fx IDSM-2 • HIDS på alle servere • RealSecure Desktop Protector eller Zone Labs Integrity på alle arbejdsstationer og hjemmearbejdspladser	
Benyttes digitale signaturer, bør den private nøgle opbevares på et chipkort							MVTU	• Rainbow iKey	

Krav	PR	PE	DE	DF	DT	CM	Kilder	Produktforslag	Certificering
E-mail gateways, servere og lignende bør sikres mod virus							ISO	• McAfee NetShield, GroupShield, WebShield • Norton AntiVirus Corporate Edition	ICSA
Integritetsudstyr bør benyttes på data, servere, netværksudstyr og lignende.							ISO	• Tripwire • RealSecure Desktop Protector	CC EAL 1
Ved adgangssystemer bør ”forbyd alt som ikke tillades” benyttes i stedet for ”tillad alt, som ikke forbydes”							ISO	• Alle routere (fx Cisco 3700), switche (fx Cisco Catalyst) og firewalls • Cisco PIX 501, 515 • CheckPoint Firewall-1 NG • Nokia IP130	ICSA, CC EAL 4 CC EAL 4 ICSA, CC EAL 4
Der skal etableres beskyttelse af portene på netværksudstyret							ISO	• 802.1x • Alle ubenyttede porte samles i ubrugt VLAN og slås fra • Brugen af VLAN, PVLAN og VACL • Smarte CAM-tabeller • Begrænsning af antallet af MAC-adresser pr. port	
Der skal udføres kontrol med udgående trafik for at sikre, at konfidentielle e-mails og data ikke sendes ud af virksomheden							DS	• CheckPoint Firewall-1 NG • McAfee GroupShield • E-mail gateways som fx McAfee WebShield	CC EAL 4
Kritiske programmer skal under en kontrol, som sikrer, at de ikke kan eksekveres, hvis der er foretaget uautoriserede ændringer							DS	• RealSecure Desktop Protector	
Logon-systemer skal beskrive, at uautoriseret adgang ikke tillades							DS	• Cisco VPN Concentrator • Citrix Secure Gateway • Webservere, e-mail servere	
Der skal være kontrol med datakommunikationsretningen							DS	• Cisco PIX 501, 515E • CheckPoint Firewall-1 NG • Nokia IP130 • PVLAN og VACL	ICSA, CC EAL 4 CC EAL 4 ICSA, CC EAL 4

Krav	PR	PE	DE	DF	DT	CM	Kilder	Produktforslag	Certificering
Alle enheder skal tidssynkroniseres							ISO	• Citrix • Group Policies til Windows 2000/XP • NTP-server til netværksenheder	CC EAL 4 (Windows 2000)
Adgang til nødvendigt udstyr, software, filer mm. skal være til stede							SP, CSIRT	• Citrix-baserede arbejdsstationer • Kopi af fulde arbejdsstationer fra virksomheden	
Transparent opkobling							SP	• Hardwarebaseret VPN-dialer fx Cisco VPN 3002	
Brugervenlighed							SP	• Citrix • Cisco VPN 3002 • McAfee VirusScan Thin Client antivirus og RealSecure Desktop Protector eller Zone Labs Integrity kræver ingen brugerinvolvering	

Som det ses, er der primært lagt vægt på forebyggelse (prevention). Dette er forventet, idet et godt design og grundlæggende konfigurering af netværket er fundamentet for ethvert sikkert netværk Der er desuden enkelte krav, som ikke falder ind under de angivne kategorier (vist på denne side).

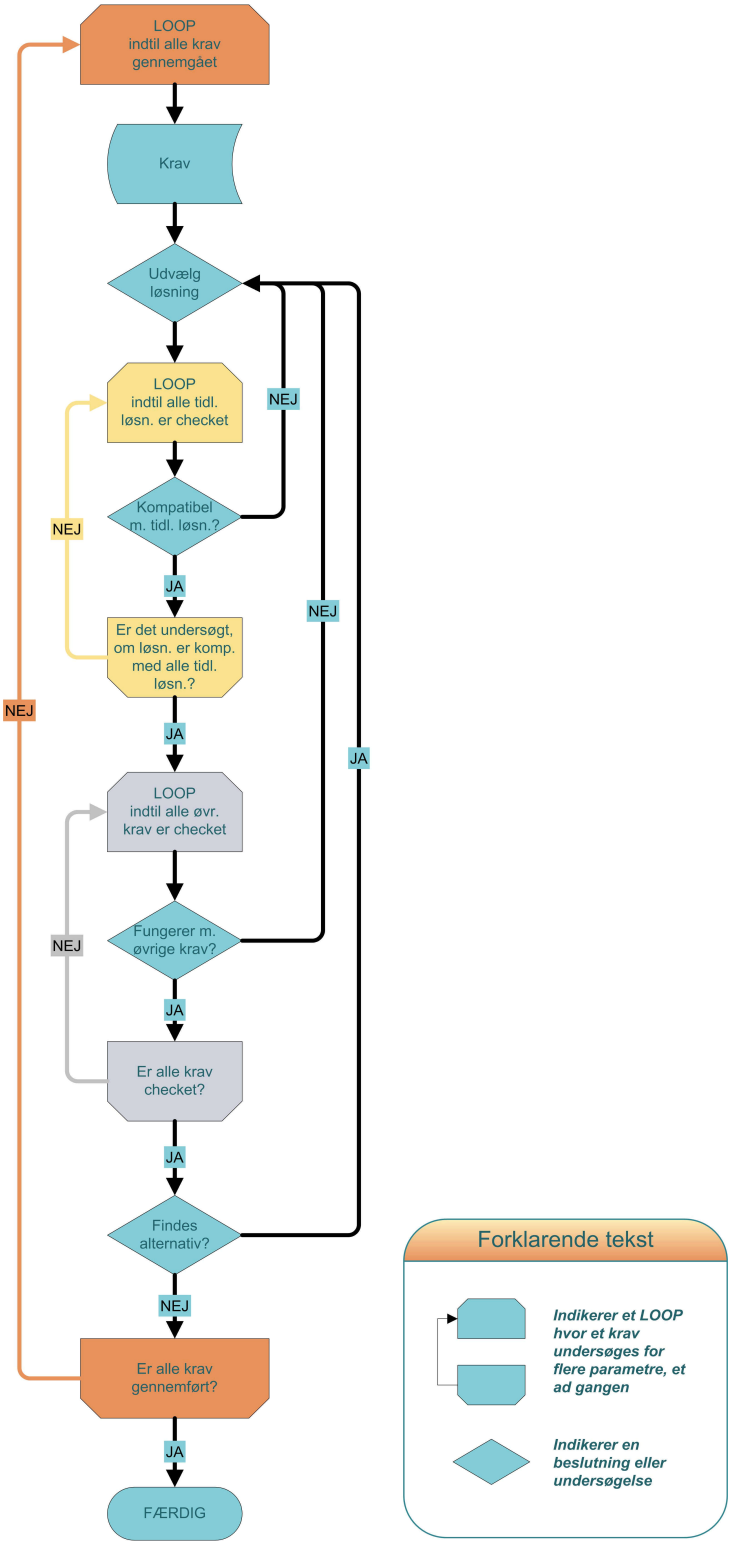
Kompatibilitet mellem de foreslåede produkter i tabellen – samt med det udstyr, som allerede eksisterer på netværket – kan i princippet være umuligt at afgøre uden at udføre tests på de valgte produktkonfigurationer. For mindre og mellemstore virksomheder er dette formentligt ikke en realistisk opgave, men med bred opbakning fra producenterne kan der være baggrund for sådanne tests i større virksomheder.

Det er også en mulighed at fokusere på en enkelt, stor leverandør af det centrale udstyr som fx Cisco idet mange produkter garanterer kompatibilitet med dette. Et alternativ er OPSEC (Open Platform for Security), som med baggrund i CheckPoint udstyr er en sammenslutning af en række leverandører af sikkerheds- og netværksudstyr. Med et ”OPSEC” logo på udstyret garanterer CheckPoint, at der er fuld kompatibilitet mellem produkterne.

Vælges der ikke en enkelt leverandør er en metode til at drive kompatibilitetsprocessen udarbejdet nedenfor. Metodens eneste funktion er at sikre, at alle produkter gennemgås og at der i tvivlstilfælde kan udvælges alternative produkter. Samtidig sikres det, at de valgte produkter overholder de ovennævnte krav. Da der hverken har været vilje (fra producenterne), tid eller ressourcer til at gennemføre en sådan kompatibilitetstest af de ovennævnte produkter, er dette ikke foretaget. Kombineret med en implementering af udstyret i et testmiljø ville dette dog være et oplagt sted at koncentrere det videre arbejde med dette projekt (se også kapitel 10).

6.7.1 Model

Modellen viser, hvordan der opnås en interkompatibel, produktspecifik løsning med tilhørende alternativer.
Baseret på kravet udvælges en valgfri løsning til opfyldelse af dette. Denne løsning undersøges for kompatibilitet med de tidligere fundne løsninger for andre krav (dette skridt er naturligvis ikke nødvendigt under første kørsel). Findes det, at løsningen er kompatibel med alle tidligere fundne løsninger, undersøges det, om løsningen samtidig opfylder alle øvrige – dvs. om løsningen af et krav skaber konflikt med de øvrige krav. Er dette ikke tilfældet er løsningen godkendt, men der spørges til, om der findes alternativer. Er dette tilfældet gennemgås proceduren igen for disse alternativer indtil der ikke findes (eller ønskes at finde) flere alternative løsninger til det aktuelle krav. Kørslen fortsættes derefter med det næste krav fra sikkerhedspolitikken indtil alle krav er gennemgået.
Hvad modellen ikke tager højde for er, i hvilken rækkefølge kravene skal udvælges og gennemgås, samt hvordan de alternative løsningsforslag skal benyttes ved eventuelle konflikter. Dette er en begrænsning i modellen, hvis kompleksitet ellers ville være vokset betragteligt.



Figur 46 - Model til sikring af kompatibilitet

Det er klart, at denne metode vil resultere i et design, som udelukkende er baseret på brugerens erfaring og evner. Selvom metoden hjælper til at sikre, at de valgte systemer kan arbejde sammen og overholder de valgte krav, er selve udvælgelsen af systemerne alene pålagt brugeren af modellen.
En bedre løsning kunne være at basere denne udvælgelse på et ekspertsystem. Ved at fodre systemet med regelsæt, fysiske begrænsninger og et generelt kendskab til netværksteknologi, kan der dannes grundlag for en indlæring af systemet. En sådan indlæring kunne komme fra et bredt spektrum af eksperter, som hver især giver deres bud på, hvordan en aktuel problemstilling kan løses. Systemet lærer af disse erfaringer, og er antallet af problemstillinger og løsninger stort nok, vil muligheden for at løse nye problemstillinger tilfredsstillende formentligt være høj. Kombineret med en fyldestgørende database over tilgængeligt udstyr, og dettes specifikationer vil der være grundlag for et bedre valg, end det, det er muligt at lave med de nuværende metoder. Udviklingen af et ekspertsystem og indlæringen af dette er dog udenfor dette projekts rammer. Der henvises i øvrigt til kapitel 10 (Perspektivering).

7 DESIGNFORSLAG

Designforslaget bygger på de i kapitel 6 nævnte krav, anbefalinger, love, best practices og standarder. Grundprincippet har været brugen af lagdelt beskyttelse forstået på den måde, at der så vidt muligt er flere lag, som skal gennembrydes, før den samlede sikkerhed er brudt. Således vil der i designet være redundante systemer fx når funktioner, som kunne være samlet i en enkelt enhed, splittes op i flere. Dette hjælper til at distribuere sikkerheden, så en enkelt enheds sårbarheder ikke kan sætte hele netværkets sikkerhed på spil.

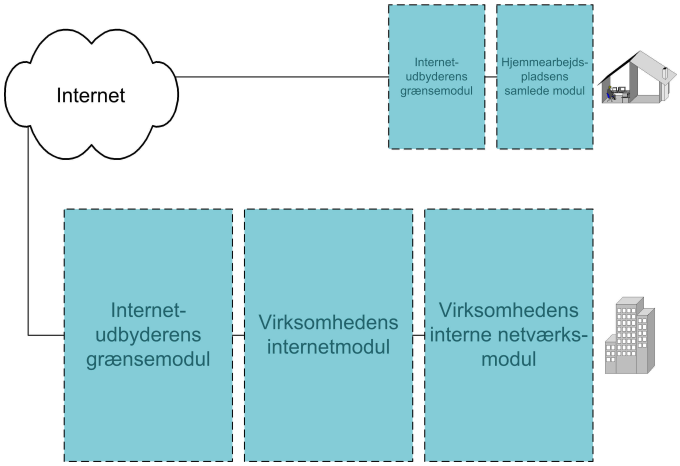
Det har været væsentligt at sikre både brugervenlighed og standardisering. Sidstnævnte for at sikre, at løsningen skalerer og kan udvides med tiden, samt integreres i virksomhedens nuværende netværksstruktur. På samme måde er det forsøgt at understøtte forskellige brugergrupper, så hjemmearbejdspladserne kan tilpasses brugerens behov.

Der er hentet inspiration til designet fra både leverandører af netværksudstyr [1][19][34][49][73][112][113], SANS [110][111], information fra nyhedsgrupper på internettet samt egen erfaring og kendskab til eksisterende netværk i diverse virksomheder. Det er interessant at observere, at der generelt er enighed om det grundlæggende netværksdesign i selve virksomheden, mens der er langt større spredning i den måde, netværket i hjemmet opbygges på. I ingen af de tilgængelige ressourcer har der være fokuseret på en samlet beskyttelse, som spænder fra det interne netværk i virksomheden til den valgte software på hjemmearbejdspladsen. Dette er forsøgt her.

I kapitel 8 laves en vurdering af designforslaget med baggrund i rapportens øvrige kapitler.

7.1 Modulopbygning

Det kan være en fordel at opdele netværksdesignet i moduler. Både fordi det letter overskueligheden, men også fordi det gør det nemmere at placere udstyr efter funktionalitet. En sådan modulopbygning kunne se ud som på figur 47. Opbygningen sker ud fra en betragtning om, at de funktioner, som hvert modul indeholder, er afgrænsede i forhold til nabomodulerne.



Figur 47 - Modulopbygning

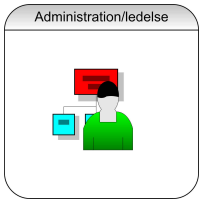
Internetudbyderens grænsemoduler indeholder udelukkende internetudbyderens eget udstyr og er medtaget, idet dette er den først mulige forsvarsmekanisme, der kan benyttes.

Virksomhedens internetmodul håndterer virksomhedens forbindelse til internettet og terminerer ekstern tilgang som fx VPN samt offentlige services som DNS, HTTP, SMTP osv. Virksomhedens interne netværksmodul indeholder den interne infrastruktur, interne servere og arbejdsstationer.

For hjemmearbejdspladsen er der tale om et samlet modul, som tilsvarer virksomhedens internetmodul og interne netværksmodul. Dette skyldes, at denne forbindelse ikke benyttes til at servicere andre, hvorved mængden af udstyr er kraftigt reduceret. Normalt vil udstyret her bestå af en ADSL-router eller tilsvarende, opkaldsudstyr, beskyttelse mod eksterne angreb samt evt. en række software til den eller de arbejdsstationer, som skal benyttes fra hjemmet.

7.2 Opdeling i brugerkategorier

Større virksomheder forventes at have brugere med forskellige krav til hjemmearbejdspladsens funktionalitet. Mens nogle brugere vil ønske adgang til deres filer, e-mails og Office-applikationer, vil andre måske ønske direkte adgang til deres arbejdsstation i virksomheden – måske fordi denne maskine er unik på den ene eller anden måde. Det er derfor relevant at opdele brugerne i kategorier, så adgangen kan skræddersys til de forskellige behov. Samtidig er det dog værd at overveje, om en for minutiøs opdeling vil skabe en uforholdsmæssig stor administrations- og implementeringsbyrde. Et kompromis mellem antallet af opdelinger og den administrative byrde er derfor nødvendig.
I dette designforslag indgår to brugergrupper. Der er ikke tale om opdeling af rettigheder, men forskel i den måde, grupperne tilgår virksomhedens ressourcer på. Disse grupper er beskrevet nedenfor og består af en administrationsgruppe samt en udviklergruppe.



Administrationsgruppen er den gruppe af ansatte, som har behov for at have adgang til standardapplikationer, filer og e-mails. Typisk vil denne gruppe indeholde HR-afdelingen (Human Resources), salgsafdelingen, produktionsafdelingen samt sekretærer og andet administrativt personale. Dette er samtidig den gruppe, som må antages sætte størst pris på brugervenligheden. Det er derfor væsentligt, at tilgangen til de nødvendige værktøjer og materialer sker så let og intuitivt som muligt.

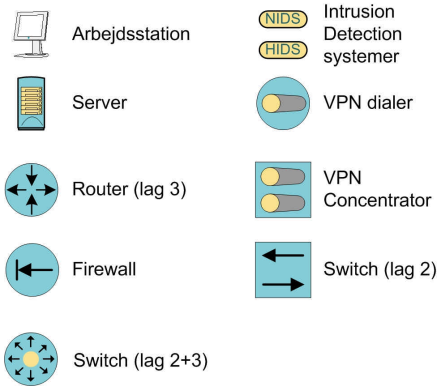
Figur 48 - Administration/ledelse

Gruppen for udviklere og forskere indeholder det personale, som har et helt specielt behov og som oftest vil ønske direkte adgang til deres arbejdsstationer hjemmefra. Eksempler kan være forskere, hvis forskningsprojekt kører på speciel hardware eller udviklere, hvis applikationer ikke må forlade bestemte maskiner. Denne gruppe indeholder også system- og netværksadministratorer, som tilhører gruppen af IT-personale, der har behov for at tilgå specielt udstyr, programmel og maskiner. Dette kan indbefatte direkte kontrol med maskinparker, netværksudstyr og specialprogrammer, ligesom det i visse tilfælde kan være relevant at levere direkte adgang til samtlige arbejdsstationer på netværket. En sådan adgang bør naturligvis beskyttes tilsvarende.

Figur 49 - Udviklere/forskere

Skal konceptet senere udvides til at inkludere mobile enheder, er dette formentligt den gruppe, som vil få størst glæde af dette.

7.3 Konkret design



Figur 50 - Ikoner brugt til netværksdesign

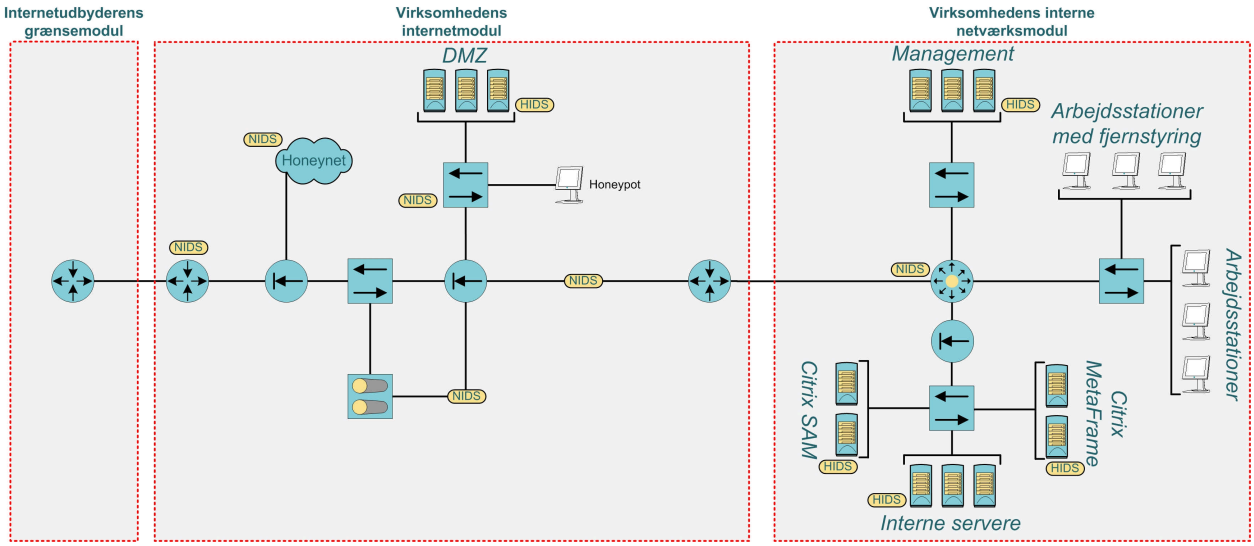
Nedenfor er vist et forslag til, hvordan et netværksdesign til implementering af sikre hjemmearbejdspladser kan se ud. Figurerne viser det overordnede design, mens detaljerne er beskrevet i teksten.
De i figurerne brugte ikoner er forklaret på figur 50. Der gives forslag til konkrete produkter i uddybelsen af designet nedenfor, men ikonerne er valgt generelle for at understrege, at der ikke er tale om en produktspecifik løsning, men et forslag, som bør tilpasses virksomhedens sikkerhedspolitik, økonomi, ønsker, leverandøraftaler og eksisterende udstyr. De viste ikoner benyttes desuden i teksten for at gøre det lettere at følge med på figuren.
Der er dog andre overvejelser som kan gøre, at generelle beslutninger om valg af hardwareleverandører bør gennemføres. Således er det sjældent, at VLANs fungerer smertefrit på tværs af leverandørernes produkter. PVLANs er i den i afsnit 5.2 beskrevne implementering en Cisco-specifik feature, hvorfor valget af Cisco switche kan være uundgåeligt, hvis denne funktion kræves. Ligeledes kan det administrative besvær med at vedligeholde mange forskellige producenters udstyr være en faktor, som kan betyde, at der primært fokuseres på en enkelt leverandør. I det nedenstående er givet eksempler på netværksudstyr fra Cisco, HP, CheckPoint og Nokia[80].

Konfigurationen af selve hjemmearbejdsplads-enheden følger nedenfor i afsnit 7.3.3.

7.3.1 Virksomhedens netværksstruktur

Designet tager udgangspunkt i virksomhedens infrastruktur. På figur 51 er vist, hvordan dette kan tage sig ud. Selvom designet er fokuseret på hjemmearbejdspladser har hele designet af netværket indflydelse på den sikkerhed, som omgiver hjemmearbejdspladserne. Således er det ikke uvæsentligt for hjemmearbejdspladserne, hvordan virksomhedens DMZ implementeres eller hvor de interne arbejdsstationer tilkobles. Dette gennemgås i detaljer under figuren.

[80] Beskrivler af det anvendte udstyr kan ses på de respektive virksomheders hjemmesider: Cisco (http://www.cisco.com/), HP (http://www.hp.com/), CheckPoint (http://www.checkpoint.com/) samt Nokia (http://www.nokia.com/).



Figur 51 - Virksomhedens infrastruktur

Som tidligere nævnt benyttes en modulopbygning, hvormed designet kan implementeres i stadier. Der tages ikke hensyn til redundans i designet, men dette kan implementeres efter behov. Således kan flere internetudbydere, routere og firewalls levere indgangen til netværket, ligesom samtlige dele af netværket kan replikeres for redundans i tilfælde af nedbrud. Ønskes større performance end det er muligt med det nuværende design, kan modulerne udvides til at inkludere både kraftigere produkter og parallelle implementeringer.

I så vidt omfang som muligt benyttes ACLs i alt netværksudstyr til at levere så mange sikkerhedsbarrierer som muligt. Desuden tillades kun en enkelt, specificeret MAC-adresse fra porte, hvor servere er tilkoblet, samt tre, uspecificerede adresser fra porte, som servicerer arbejdsstationer. Sidstnævnte for at sikre, at udstyret kan udskiftes uden rekonfiguration, mens det samtidig forhindres, at arbejdsstationer kan udføre angreb, som involverer brugen af mange MAC-adresser. Metoden ”forbyd alt, som ikke specifikt tillades” benyttes, når ACLs anvendes på enheder, som operer på lag 3. Benyttes Cisco switche understøttes brugen af PVLANs og dette udnyttes til at isolere alle porte, som ikke specifikt har behov for at kunne kommunikere med hinanden. Servere, som ikke har behov for at kunne etablere forbindelser, fratages denne mulighed.
Switche, hvis porte er placeret i lokaler, som ikke er aflåste, er konfigureret med 802.1x. Således skal alle enheder, som ønsker at opnå netværksadgang autentificeres. Dette sker for at sikre, at kun godkendt udstyr kan benyttes på netværket samt at udstyr, som flyttes rundt på netværket, ikke kan opnå adgang til andre ressourcer, end enheden oprindeligt har rettigheder til. De porte, som ikke benyttes på netværket, samles i et ubenyttet VLAN og slås fra. Ligeledes sikres, at kun de porte, som bør være trunkporte, har mulighed for at blive det, ligesom de trunkporte, som benyttes, tildeles et VLAN ID, som ikke benyttes andre steder på netværket.
På alt netværksudstyr og alle servere benyttes Tripwire til at kontrollere, at der ikke udføres uautoriserede ændringer til konfigurationer, filer eller operativsystemer. På servere benyttes desuden antivirusprogrammel, som holdes centralt opdateret. Dette kan fx være McAfee’s serie af serverbaserede løsninger, som både inkluderer hardware og software.
De enheder på netværket, som tager imod eksterne forespørgsler, konfigureres til at informere brugerne om at uautoriseret adgang ikke tillades. Desuden sikres, at der kun gives de mest nødvendige informationer under logon-proceduren, så det fx ikke er muligt at afgøre, om en fejl er opstået pga. forkert password eller forkert brugernavn. Dette hjælper til at tilføje endnu et lille lag af sikkerhed i forbindelse med de delvist offentligt tilgængelige opkaldspunkter.
Der udføres logning af data på både servere, netværksenheder og arbejdsstationer. Detaljegraden af denne logning kan justeres efter behov, og da alle log-data sendes fra enhederne til syslog-serverne i management-modulet, kan disse sammenkøres til fx at danne profiler for brugeradfærd eller til at analyse udvalgte brugeres aktiviteter. Transmissionen af syslog-data bør ske på et separat VLAN og hvis muligt via krypterede forbindelser.

Internetudbyderens modul er af naturlige årsager udenfor virksomhedens kontrol, men der kan ofte laves aftaler med udbyderen omkring filtrering af trafikken i den router, som er sidste led inden virksomheden. Den vigtigste funktion er at stoppe DoS-angreb her, idet dette er det eneste sted i strukturen, som effektivt kan benyttes til at stoppe denne type angreb. Der er altså tale om primært at stoppe pakker, som har en intern IP-adresse (som defineret i [18]) samt – hvis internetudbyderen tilbyder det – desuden udføre båndbreddekontrol af ICMP-pakker samt pakker hvor SYN-flaget er sat. Derudover kan denne router udføre kontrol med at kun pakker med en afsenderadresse, som tilhører virksomheden, kan forlade denne. Dette hjælper til at sikre, at virksomheden ikke medvirker i DoS-angreb mod andre maskiner. Det er ikke fordelagtigt at udføre anden filtrering på dette sted, idet der så vidt muligt skal være tale om statiske filtre, så internetudbyderen ikke skal involveres, når der foretages ændringer af virksomhedens netværk.

Virksomhedens internetmodul tager udgangspunkt i en router, som afgrænser virksomhedens netværk fra internetudbyderens. Dette kunne fx være en Cisco 3700-serie router. Ligesom på internetudbyderens router udføres DoS-kontrol samt kontrol med afsenderadresser. Dette sker for at sikre, at en ændring i internetudbyderens konfiguration ikke efterlader virksomheden sårbar overfor disse angreb (selvom DoS-angreb ikke på dette punkt kan stoppes effektivt).
Routeren udfører desuden filtrering af den indkommende trafik, således at kun trafik til offentlige servere, honeynet og VPN-udstyr tillades, ligesom kun trafik af de valgte typer tillades. Til VPN Concentratoren tillades kun IPSec-trafik.
Routeren er desuden udstyret med et Network Intrusion Detection (NIDS) modul som fx et Cisco IDS Network Module. Dette sker for at få information om hvilke angrebstyper, der stadig eksisterer på netværket, efter routeren har foretaget grovsorteringen af trafikken. Denne information kan være værdifuld i forbindelse med en fremtidig analyse af, hvad de efterfølgende sikkerhedsprodukter udsættes for.

Den første firewall analyserer den trafik, som routeren har tilladt. Her kunne være tale om en Cisco PIX 515E. Ligesom den efterfølgende firewall udføres stateful packet inspection for at sikre, at kun svar til de forbindelser, som er initieret fra det interne netværk, tillades. Firewall'en udfører en sekundær kontrol med at de indkommende pakker har destinationsadresser, som matcher offentlige servere, maskiner i honeynettet eller VPN Concentratoren, samt at kun tilladte porte og protokoller tillades til de respektive IP-numre. Servere og VPN-Concentratoren skånes desuden for flooding-angreb som fx TCP SYN ved at udnytte firewall'ens mulighed for at agere mellemmand mellem afsenderen og den server, som skal håndtere forespørgslen.
Et sekundært modul i firewall'en giver adgang til honeynettet og beskytter det øvrige netværk således, at trafik fra honeynettet alene kan sendes retur til internettet via routeren. Det interne udstyr i honeynettet er desuden udstyret med et NIDS-modul, som passivt detekterer angreb. Sammen med logfilerne fra honeynettet kan dette modul benyttes til at analysere, hvad der foregår på honeynettet og hvilke typer angreb, det kan forventes også vil blive benyttet mod virksomhedens øvrige systemer.

Selve opbygningen af honeynettet er ikke medtaget i dette design. Administratorerne må afgøre, hvilke angrebstyper samt hvilke systemer og applikationer, der ønskes iagttaget. Det er desuden en mulighed at lade NIDS'en reagere aktivt på trafik til honeynettet ved at give besked til den sekundære firewall om, at de pågældende afsenderadresser skal blokeres her. Da legitime brugere aldrig burde tilgå en enhed i honeynettet kan det antages, at trafik fra de adresser som tilgår en sådan enhed, ikke er ønsket på det resterende netværk. Der er dog faldgruber i dette, idet IP-adresser kan være delt af mange brugere (fx en PC på et universitet), ligesom angribere kan identificere honeynettet ved at kontrollere, om deres forbindelse til virksomhedens offentlige servere blokeres.

Den efterfølgende switch leverer adgang til VPN Concentratoren. Et eksempel kunne være en Cisco switch fra Catalyst-serien eller fra HP ProCurve-serierne. Der bør benyttes VLANs, så trafik fra det interne netværk ikke kan tilgå VPN Concentratoren. Dvs. den efterfølgende firewall og VPN Concentratoren tilknyttes to separate VLANs.
Det ville være en mulighed at implementere en Application Level Gateway (ALG) for at sikre, at udgående trafik fra både hjemmearbejdspladser, servere i DMZ'en samt interne arbejdsstationer og servere analyseres og autentificeres, før der etableres forbindelse. Dette kan bl.a. hjælpe til at sikre, at trojanske heste, som etablerer forbindelse til eksterne maskiner, vil være lettere at blokere. ALGs er dog ikke implementeret i dette design pga. nedsættelsen af brugervenlighed ud fra kravet om konstant autentificering. Desuden er ALG'en applikationsspecifik (hvorfor der kræves mange af dem), ligesom det kan være et performanceproblem at lede trafikken igennem disse. I stedet for anvendes en stateful, multi-layer inspection firewall (se nedenfor), som også analyserer applikationslaget, men som gør dette transparent og uden samme performanceproblemer. Dette, kombineret med fuld kontrol over brugernes arbejdsstationer og hjemmearbejdspladser, bør også levere en fornuftig beskyttelse mod brugersabotage og trojanske heste.

Selve VPN-Concentratoren terminrerer IPSec VPN-forbindelserne og autentificerer brugerne. Et eksempel kunne være et produkt i Cisco VPN Concentrator 3000-serien idet disse kan benyttes med to-faktor autentificering samt digitale certifikater. Før brugerautentificeringen foretages, kontrolleres det, at den enhed som er benyttet til at foretage VPN-forbindelsen, er i besiddelse af det korrekte certifikat.
Brugerautentificeringen foregår ved, at VPN Concentratoren kontakter en RADIUS-server på det interne netværk. Denne kommunikation foregår på et separat VLAN, som udelukkende benyttes til management og kontakt til RADIUS-serveren. RSA's SecurID system benyttes til to-faktor autentificering. Concentratoren kontrollerer desuden i samarbejde med en RealSecure eller Zone Labs server, at brugeren har et aktivt antivirusprogram, samt at nyeste opdateringer til dette er installeret. Derudover kontrolleres, at en personlig firewall og et integritetsprogram er installeret og aktiveret på klienten, ligesom det checkes, at de korrekte indstillinger for disse programmer er sat.
Der benyttes AES eller 3DES kryptering, samt SHA-1 til at sikre integriteten af dataene. Dette sikrer, at dataene fra hjemmearbejdspladserne er sikret mod aflytning (brugen af stærk kryptering), genafspilning (via IPSec's ESP) samt ændring (SHA-1 sikrer integriteten af de overførte data).

Efter termineringen af VPN-forbindelserne ledes trafikken gennem en NIDS. Dette kunne fx være en Cisco IDS 4215. NIDS-modulets formål er at detektere angreb fra de autentificerede VPN-brugere. Da der ikke

burde eksistere noget ondsindet trafik på dette sted, kan NIDS-modulet konfigureres aggressivt, så eventuelle forbindelser, som udviser destruktiv adfærd, kan blokeres fx i den efterfølgende firewall.


Den sekundære firewall indeholder flere segmenter og kan fx være en enhed baseret på CheckPoint Firewall-1 NG. Den primære funktion er at udføre stateful packet inspection, så kun svar til de forbindelser, som er initieret fra det interne netværk eller VPN Concentratoren, tillades. Samtidig udføres en detaljeret filtrering af trafikken til serverne i DMZ'en, så kun tilladte trafiktyper med destinationsadresser som matcher serverne, tillades. Der filteres desuden på portniveau, ligesom firewall'ens omfattende muligheder for at udføre analysering af trafikken på applikationslaget udnyttes. Ud over filtrering af trafikken til DMZ'en udføres desuden filtrering af trafikken fra denne for at undgå, at en kompromitteret enhed kan angribe andre maskiner udenfor DMZ'en. Nedenfor er beskrevet hvordan det også internt i DMZ'en forsøges forhindret, at servere kan angribe hinanden. Firewall'en kontrollerer desuden at der ikke sendes uautoriseret data ud af netværket. Ved at gennemse brugen af filoverførselsprotokoller, kan firewall'en sammen med en lignende kontrol i e-mail serverne hjælpe til at sikre, at der ikke sendes fortrolige filer ud fra netværket. Således kan det også sikres, at fortrolige filer ikke overføres til hjemmearbejdspladsen, hvis dette ikke ønskes.
Et andet segment af firewall'en håndterer trafikken fra VPN Concentratoren. Det sikres, at der kun er tale om tilladt trafik med destinationsadresser, som følger den politik, virksomheden har, om hvilke enheder, der må tilgås fra hjemmearbejdspladserne. Hvis destinationsadressen er en ekstern adresse, ledes trafikken tilbage til internettet under overvågning af de to stateful packet inspection firewalls. Der tillades således ikke split-tunneling i hjemmearbejdspladserne. Samtidig sikrer firewall'en, at der ikke sendes trafik mod hjemmearbejdspladserne, og isolerer VPN Concentratoren i et separat VLAN.
For de hjemmearbejdspladsbrugere, som er udstyret med en tynd klient i hjemmet, tillades udelukkende adgang til Citrix Secure Gateway-serveren i DMZ'en. Således blokeres der for adgang til internettet, til de resterende servere i DMZ'en samt til hele det interne netværk. Der udføres desuden kontrol med, at kun SSL-trafik tillades til Citrix-serveren i DMZ'en.


Til firewall'ens DMZ-port er tilkoblet en switch med PVLAN-funktionalitet som fx en enhed fra Cisco Catalyst 6500-serien. Som alternativ til Cisco kan også HP levere switche, som i deres ProCurve-serie kan levere VLAN og 802.1x funktionalitet. Til switchen er tilkoblet de offentligt tilgængelige servere inkl. Citrix Secure Gateway serveren, samt en honeypot, som skal tiltrække opmærksomhed fra de angribere, som måtte have brudt igennem forsvarssystemerne. Til switchen er desuden koblet et NIDS-modul, som detekterer angreb på både serverne og honeypotten, samt mellem serverne indbyrdes og fra servere og honeypot mod firewall'en. IDSM-2 modulet benyttes som NIDS.
Cisco switchen benytter PVLANs til at isolere portene, således at serverne ikke kan kontakte hinanden. Kombineret med VACLs sikres desuden, at serverne og honeypotten ikke kan etablere forbindelser. Serverne er desuden udstyret med Host Intrusion Detection Systemer (HIDS), som detekterer angreb, der er specifikke for de applikationer, som serverne afvikler. Citrix Secure Gateway'en udfører autentificering af Citrix-brugerne via RSA's SecurID-system.

PVLANs og den sekundære firewall tillader trafik fra Citrix-serveren til Citrix Secure Access Manager (SAM) serverne på det interne netværk via ICA-protokollen. Der kan desuden tillades adgang fra de resterende servere i DMZ'en til fx interne database- eller mailservere, hvis dette ønskes. Dette er dog ikke gennemgået i designet.

Fra den sekundære firewall ledes trafikken gennem en NIDS. Dette modul analyserer trafikken for angrebssignaturer, inden den føres videre til virksomhedens interne netværksmodul. Da der på dette punkt kun bør eksistere legitim trafik i form af ICA-pakker, trafik fra VPN-brugerne samt svar på initierede sessioner fra de interne klienter, kan modulet konfigureres til at afbryde al trafik, hvis et angreb detekteres. NIDS'en kan fx udgøres af en Cisco IDS 4235 som kan håndtere op til 250 Mbit.


Inden trafikken videreføres til det interne modul ledes det igennem en router. Denne enheds funktion er at levere separation mellem det interne og eksterne netværk i lag 3. Der kan fx benyttes en Cisco 3700-serie router, som bl.a. også understøtter brugen af VoIP.


Trafikken ankommer til virksomhedens interne modul fra routeren til en switch, som opererer på lag 2 og 3. Denne switch håndterer dermed den interne routing (lag 3), som foregår mellem de VLANs, som er etableret i det interne netværk. Således findes ét VLAN til management-enhederne, to til arbejdsstationerne, og tre til de interne servere. Disse VLANs er oprettet for at separere modulerne og kontrollere adgangen mellem dem.
Da der er store krav til hastigheden af trafikken mellem disse enheder, benyttes en switch, som kan foretage såkaldt hurtig routing. Dette foregår ved at den første pakke i en serie routes på normal vis, hvorefter de efterfølgende pakker switches (dvs. bridges), da enheden nu ved, hvor disse skal hen. Switchen er desuden udstyret med et NIDS-modul, som detekterer angreb, som kommer fra de interne maskiner. Der burde ikke ses nogen angreb her, da dette vil indikere, at interne arbejdsstationer eller servere udfører angreb.
Igen kan både HP og Cisco udstyr benyttes. Cisco's Catalyst 6500-serie med tilhørende IDSM-2 NIDS-modul kan håndtere hastigheder på op til 600Mbit og leverer de nødvendige services på lag 3. Tilsvarende udstyr fra HP kan leveres i form af HP ProCurve 4100gl serien.

Switchen forbinder management-udstyret til netværket. Management-udstyret håndterer bl.a. brugerkonti med tilhørende passwords, OTP-udstyr og certifikater, håndteringen af regler om passwordlængde og kompleksitet, indsamlingen af log-data fra netværksenhederne, data fra Tripwire samt tidssynkronisering af alle enheder og arbejdsstationer. Desuden udsendes opdateringer til både Windowsklienter og netværksenheder, ligesom antivirussignaturer vedligeholdes fra servere i dette segment. Al den information, som samles fra IDS-enheder og logning analyseres, ligesom alarmering af administratorer sker fra disse enheder.
Dette udstyr består således ud over RADIUS-servere, som fx kan udgøres af en Cisco Access Control Server, også af SNMP-servere, en OTP-server (RSA ACE/Server), NIDS-servere, syslog servere og andre enheder, som benyttes af administratorerne. Kun trafik fra de relevante enheder tillades adgang til disse maskiner – og kun via godkendte protokoller. Denne adgangskontrol udføres i swtichene ved at benytte et isoleret VLAN, ligesom de tidligere firewalls har sorteret trafikken før den ankom til det interne modul.


Arbejdsstationerne er desuden forbundet via en række switche (lag 2) fordelt i bygningerne. Da disse enheder normalt ikke bør kunne kommunikere, er der indført PVLANs for at sikre isolering af maskinerne. De arbejdsstationer, som skal kunne fjernstyres (dvs. benyttes af udvikler-gruppen), er placeret på et separat VLAN, som routes fra den centrale switch i modulet. Disse enheder er desuden isolerede med PVLANs. Switchene kan fx være fra HP ProCurve 8000m-serien eller fra Cisco Catalyst 4000-serien så PVLANs understøttes.
Forslag til beskyttelsen af arbejdsstationerne medtages her for komplethedens skyld, idet dette ikke er direkte relevant i forbindelse med hjemmearbejdspladserne. Det kan dog være væsentligt at sikre, at hjemmearbejdspladserne og arbejdspladserne i virksomheden er baseret på en ens opsætning, for at gøre livet lettere for brugerne.
Arbejdsstationerne vil ofte være Windows-baserede enheder eller tynde klienter i Citrix-miljøer. Ligesom i hjemmene (se afsnit 7.3.3 nedenfor) benyttes tynde klienter hvor det er muligt, fulde Windows-klienter som første alternativ og alternative operativsystemer, hvor dette er nødvendigt.
Hvor der ikke benyttes tynde klienter, bør antivirusprogrammer som fx McAfee Thin Client benyttes. RealSecure Desktop Protector bør også benyttes til at levere firewallbeskyttelse til hver enkelt arbejdsstation, samt til at sikre integriteten af filerne på enheden. Det bør via Group Policies sikres, at filer og passwords ikke kan lagres på maskinerne. Group Policies kan desuden låse konfigurationen af arbejdsstationerne, håndtere distribueringen af opdateringer til både operativsystemer, programmer og antivirusprogrammer samt sikre, at alle arbejdsstationer er tidssynkroniseret med serverne, så data fra logfiler kan sammenlignes. Tripwire kan benyttes, hvis der ønskes en ensartet kontrol med integriteten på tværs af alle netværksenheder.
I visse tilfælde kan det være nødvendigt at sikre, at arbejdsstationerne låses, når medarbejderen forlader denne. Dette kan enten ske som ved hjemmearbejdspladserne ved at lade en screen saver låse computeren, hvis denne ikke benyttes i en fastsat periode, eller ved at benytte specielt udstyr til at holde styr på medarbejdernes fysiske position i virksomheden. Et eksempel på sidstnævnte er udviklet af det danske firma BluePosition. Ved at triangulere positionen af medarbejdernes mobiltelefoner med bluetooth, kan der sættes en maks afstand fra arbejdsstationerne som tillades, hvorefter computeren automatisk låses. Brugeren må herefter benytte sit password eller andet adgangssystem, når hun returnerer. Systemet er beskrevet i [108].


De interne servere er beskyttet bag en stateful packet inspection firewall, som fx en enhed baseret på Check Point Firewall-1 NG. Denne firewall filtrerer trafikken fra de interne arbejdsstationer og udfører desuden kontrol med trafikken på applikationslaget. Der scannes for kendte angrebssignaturer, ligesom det sikres, at kun godkendte protokoller kan benyttes til de individuelle servere. Således tillades kun ICA-protokollen samt eventuelt en managementprotokol at tilgå enheder i det VLAN, som Citrix Secure Access Manager (SAM) serverne er placeret i. Der tillades ingen adgang direkte til Citrix MetaFrame serverne gennem firewall'en, idet al trafik til disse bør gå gennem Citrix SAM-serverne.


Switchen som forbinder Citrix-serverne og de interne servere til netværket opererer på lag 2, og opdeler segmentet i tre VLANs med brug af PVLANs til at isolere serverne, som kun i enkelte tilfælde skal kunne tale sammen. Kombineret med VACLs sikres, at serverne kun kan besvare forespørgsler, men ikke selv initiere udgående sessioner. Samme switche som ved arbejdsstationerne kan benyttes her.
Alle servere beskyttes med HIDS-moduler, som detekterer angreb, specielt fokuseret på de applikationer, som den enkelte server kører. Den konkrete beskyttelse af de interne servere er udenfor dette projekts rammer.
Citrix SAM-serverne etablerer kontakt til Citrix MetaFrame-serverne samt de interne servere, som leverer information til Citrix-systemet. Da trafikken besvares ad samme vej, er Citrix MetaFrame serverne udelukket fra at kunne etablere forbindelser eller besvare direkte forespørgsler, som ikke kommer fra Citrix SAM-serverne. Eneste undtagelse til dette er den kommunikation, som kommer fra management-segmentet, som benytter et separat VLAN. Idet al kommunikation mellem serverne skal forbi den centrale switch foran firewall'en, får firewall'en også mulighed for at filtrere den trafik, som foregår mellem de tre VLANs. Dette kan dog i store netværk resultere i performanceproblemer. I sådanne tilfælde kan switchen, som forbinder de interne servere, erstattes med en switch, som opererer på lag 2 og 3, således at intern routing kan foregå uden at passere firewall'en.

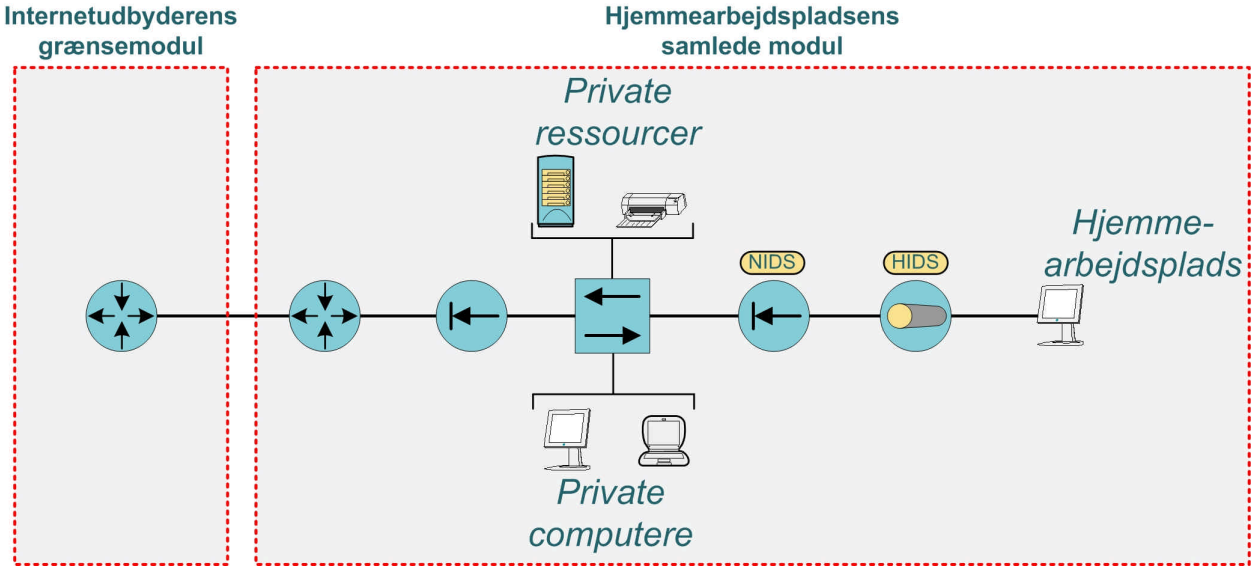
Det kan overvejes, om der skal indføres kryptering af al intern trafik med IPSec, som understøttes af både nyere arbejdsstationer (fx Windows 2000 og XP, Linux RedHat 8 og 9 og Mac OS X) samt de fleste serveres operativsystemer. Dette kan hjælpe til at beskytte mod aflytning, modificering og genafspilningsangreb internt i

virksomheden, men giver til gengæld problemer for NIDS-enhederne, som ikke længere kan analysere trafikken. Det sætter desuden meget store krav til ydelsen på de enheder, som håndterer store mængder intern trafik. Denne mulighed er kort omtalt under perspektiveringen i kapitel 10.

Nedenfor følger opbygningen af netværksstrukturen i hjemmene. Kapitlet afsluttes med en opsummering, som sammenholder de to netværksstrukturer.

7.3.2 Hjemmearbejdspladsens netværksstruktur

Ligesom for virksomhedens netværksstruktur er der udarbejdet en figur over opbygningen af systemet i hjemmet. Denne kan ses på figur 52 og indeholder to moduler – internettets grænsemodul samt hjemmearbejdspladsens samlede modul.



Figur 52 - Hjemmets netværksstruktur

Udstyret i hjemmet leverer ligesom virksomhedens øvrige udstyr log-data til management-serverne i virksomhedens interne netværk. Da forbindelsen mellem virksomheden og hjemmet ikke altid er etableret, lagrer enhederne disse data i interne buffere, indtil der er mulighed for at aflevere dataene over VPN-forbindelsen til virksomheden.

På samme måde som ved virksomhedens infrastruktur, benyttes internetudbyderens router til at forebygge DoS-angreb samt til at forhindre, at enhederne i hjemmet kan udsende pakker, som ikke har en afsenderadresser, der matcher dem, som benyttes her. Samtidig udføres båndbreddekontrol af ICMP-pakker samt SYN-pakker.

Hjemmearbejdspladsens samlede modul tager udgangspunkt i en router, som afgrænser hjemmets netværk fra internetudbyderens. Denne router kan enten være en separat enhed som vist på figuren, eller være en del af en integreret enhed, som sammen med den efterfølgende firewall beskytter hjemmets udstyr.
Denne router blokerer for alle indgående forbindelser, med mindre der specifikt tillades forbindelser til dele af hjemmets private netværk. I så fald kontrolleres, at kun den tilladte trafiktype kan tilgå de specificerede enheder. Routeren udfører desuden samme funktioner som internetudbyderens router, for at sikre, at ændringer hos internetudbyderen ikke efterlader hjemmet sårbart overfor disse angreb.
Routeren vil oftest være en enhed, som er leveret af internetudbyderen, men kan alternativt være en Cisco 837 Router. I sidstnævnte tilfælde indeholder enheden desuden en firewall.

Routeren efterfølges som nævnt af en firewall, hvis primære formål er at udføre stateful packet inspection for at sikre, at kun svar til de forbindelser, som er initieret fra de private enheder samt IPSec trafikken fra hjemmearbejdspladsen, kan passere. Er der private enheder, som kræver direkte forbindelse fra internettet kan firewall'en filtrere disse, således at kun udvalgte porte og protokoller tillades. Afhængigt af hvordan virksomheden ønsker at administrere netværksenhederne i hjemmene, kan der etableres filtre, som tillader bestemte protokoller fra virksomheden til netværksenhederne. En sikrere måde at gøre dette på, er dog at foretage denne administration af enhederne gennem IPSec forbindelsen. Firewall'en kan fx være en Cisco PIX 501, som opdateres og konfigureres centralt fra virksomhedens management-system. Fordelen ved denne PIX er, at den leverer de samme firewallfunktionaliteter som dens større brødre i virksomhedens netværk, hvorfor administrationen lettes. 501-modellen indeholder desuden også funktioner til at beskytte mod TCP SYN-angreb m.m.

Firewall'en efterfølges af en switch, som leverer forbindelse til hjemmets private udstyr som PC'er, bærbare computere, printere og servere. Switchen behøver ingen sikkerhedsmæssig funktion have, og vil ofte være

integreret i firewallenheden, men kan ellers fx består af en HP ProCurve 408. Ønskes sikkerheden øget yderligere, kan en Cisco switch med VLAN funktionalitet benyttes, således at hjemmets private computere og ressourcer kan isoleres i et VLAN, mens hjemmearbejdspladsen isoleres i andet. Porten ud mod den første firewall vil i så fald være en promiskuøs port.

En sekundær firewall beskytter hjemmearbejdspladsen mod angreb fra hjemmets private udstyr. Idet virksomheden ikke har kontrol over sikkerheden af det private udstyr, antages dette at udgøre tilnærmelsesvis samme risiko, som andre maskiner på internettet. Denne firewall har derfor til opgave at sikre, at ingen trafik kan passere fra det private netværk til hjemmearbejdspladsen, samt at sikre, at kun IPSec trafik kan passere fra hjemmearbejdspladsen og ud. Sidstnævnte trafik skal have en destinationsadresse som matcher virksomhedens VPN Concentrator.
Hvis det ønskes, kan firewall'en desuden tillade, at hjemmearbejdspladsen kan sende printjobs til en printer, som er placeret i det private segment. Således kan hjemmearbejdspladsen og hjemmets øvrige udstyr deles om en ressource som fx en printer.
Firewall'en er desuden udstyret med en NIDS-enhed. Denne detekterer angreb, som enten inititeres fra hjemmets private udstyr, fra internettet eller fra hjemmearbejdspladsen. Da der ikke bør forekomme nogen angreb her, kan NIDS-enheden konfigureres til at blokere enheder, som angriber firewall'en eller de to enheder bag denne. Detekteres et angreb fra VPN-dialeren eller hjemmearbejdspladsen, bør begge firewall's blokere for al trafik og alarmere administratorer, idet dette aldrig bør ske og repræsenterer et fatalt brud på sikkerheden.
Firewall'en kan igen udgøres af en Cisco PIX 501, men da sikkerheden forbedres ved at anvende to forskellige enheder, bør fx en Nokia IP130 (med CheckPoint Firewall-1 NG software) eller tilsvarende enhed benyttes. Som med den foregående Cisco PIX 501 holdes også denne opdateret og konfigureret fra virksomheden. Benyttes Nokia-enheden, kan NIDS'en være en integreret RealSecure-enhed. For at forbedre mulighederne for logning, kan enheden udstyres med op til 256MB hukommelse for at kunne opbevare log-dataene indtil forbindelser til virksomhedens syslog-servere kan etableres.

Sidste enhed før hjemmearbejdspladsen er en hardwarebaseret VPN-dialer, som håndterer VPN-forbindelsen fra hjemmet til virksomheden. Baseret på et digitalt certifikat verificerer enheden, at den IP-adresse, der forsøges at opnå kontakt til, er virksomhedens VPN Concentrator. Samtidig bekræftes identiteten af VPN-dialeren fra virksomheden på samme måde. Når forbindelsen er oprettet, autentificeres brugeren ved hjælp af et RSA's SecurID OTP-system. Der tillades ikke split tunneling, hvilket dobbeltcheckes af firewall'en som filtrerer alt trafik fra hjemmearbejdspladsen og VPN-dialeren, som ikke er IPSec-trafik med virksomhedens VPN Concentrator som destination.
VPN-dialeren kan fx udgøres af en Cisco VPN 3002 hardware klient. Denne enhed har muligheden for at præsentere brugeren for en hjemmeside hvorfra brugerautentificeringen foretages, når klienten forsøger at etablere netværksadgang. Samtidig understøtter enheden VoIP i tilfælde af at virksomheden senere ønsker at implementere dette.

Det bør bemærkes, at hele hjemmets linie af udstyr fra routeren til VPN-dialeren kan erstattes af CyberCity's løsning, som beskrevet i afsnit 4.2. Således vil de to firewalls, switchen og VPN-dialeren være indbygget i en enkelt enhed, som udfører samme funktion som ovenfor beskrevet. Denne enhed (en SonicWall Tele3TZ) kan desuden udstyres med kontrol af antivirusprogrammet samt sårbarhedsscanninger foretaget af SonicWall mod virksomhedens hjemmearbejdspladser. Selvom noget af den fleksibilitet, som opnås ved at opdele udstyret som vist på figuren, mistes, kan de administrative og økonomiske fordele i valget af CyberCity-løsningen være store.
Ingen af de øvrige løsninger fra teleselskaberne kan benyttes i det foreslåede design.

Selve hjemmearbejdspladsen kan enten være en tynd klient til de brugere, som har mulighed for at benytte Citrix-systemet eller en fuld klient, som afspejler den arbejdsstation, som medarbejderen benytter i virksomheden. Konfigurationen af selve arbejdsstationerne er beskrevet nedenfor.

7.3.3 Hjemmearbejdspladsens konfiguration

De fleste af de medarbejdere, som kan falde ind under administrationsgruppen, kan benytte en tynd klient i hjemmet til brug i Citrix-systemet. Således er der ingen yderligere krav til disse enheder, idet der kan være tale om diskløse, tynde klienter, hvor hverken brugere, administratorer eller angribere har mulighed for at afvikle programmer eller på anden måde ændre på enhedens opsætning. Ofte vil disse Citrix-klienter være enheder, som afvikler et operativsystem fra ROM, hvis funktion blot er at etablere kontakt til Citrix-serverne. Således er tynde klienter ofte mere eller mindre immune overfor angreb rettet mod enhederne, ligesom vira og trojanske heste ikke kan afvikles på disse.

Hvis der opstår problemer med en tynd klient, kan medarbejderen blot medtage denne til virksomheden, som ombytter med en ny. Disse enheder er "plug-and-play" og kræver ingen konfiguration fra brugeren. Da enhederne ingen bevægelige dele har, vil det dog formentligt være sjældent, at disse skal udskiftes.

For udviklergruppen samt for de dele af administrationsgruppen, som ikke kan eller ikke ønsker at benytte tynde klienter, vil der være behov for at installere fulde klienter i hjemmene. Da administrationsbyrden af disse er en afgørende faktor – og da der stilles krav fra sikkerhedspolitikken om, at konfigurationen af enhederne skal være under virksomhedens kontrol – bør der benyttes så lille et antal forskellige konfigurationer som muligt. Ideelt kun én, således at maskinerne kan udskiftes uden konfigurering i tilfælde af problemer.
I dette tilfælde bør der i så vidt omfang som muligt benyttes en version af Windows, som kan administreres centralt. Dette kan enten være Windows 2000 eller Windows XP Professional. Begge disse Windows-versioner kan benytte Group Policies, som muliggør, at al konfiguration kan foregå centralt, ligesom opdateringer og nye programpakker kan installeres uden brugerens medvirken. Begge versioner tillader også at systemet konfigureres, så brugeren udelukkende kan afvikle forudbestemte programmer. Desuden kan lokale diske gøres "usynlige" for brugeren, ligesom ethvert forsøg på at udføre kommandoer, som ikke er godkendt af administratorerne, kan detekteres og annulleres. Group Policies kan desuden sikre, at hjemmearbejdspladserne holdes tidssynkroniserede med de resterende enheder i virksomheden, så log-data kan sammenlignes, samt konfigurere systemet, så passwords og anden information ikke kan lagres på dette.
Ved at benytte Windows-klienter opnås desuden den fordel i forhold til andre operativsystemer, at programmer som Zone Labs Integrity eller RealSecure Desktop Protector samt McAfee Thin Client kan benyttes. Disse programmer kombineret med den ovennævnte VPN Concentrator kan, før der gives adgang til virksomhedens netværk, sikre, at arbejdsstationerne benytter personlige firewalls med korrekt konfiguration, at anti-virus programmet er aktiveret og opdateret, samt at alle filer på den lokale harddisk er uændrede i forhold til den referenceværdi, som er lagret på servere i virksomheden. Samtidig kan der distribueres oplysninger om aktuelle angrebstyper, således at hvis en enkelt hjemmearbejdsplads udsættes for et angreb, kan administratorerne analysere dette og distribuere information til alle andre hjemmearbejdspladser om angrebstypen samt hvordan sikkerhedsprogrammerne skal forholde sig til denne (kun RealSecure Desktop Protector).
TauScan kan også afvikles på Windows-klienterne, hvilket giver en høj sikkerhed for, at trojanske heste og softwarebaserede keyloggere detekteres. Ydermere kan Tripwire benyttes på både hjemmets netværksudstyr samt selve hjemmearbejdspladsen. Selvom dette er redundant hvis også RealSecure Desktop Protector benyttes til at udføre integritetscheck, kan rapporteringsfunktionerne komplimentere hinanden, og en virksomhed kan vælge at sikre sig yderligere ved at benytte begge produkter.
Når virksomheden distribuerer opdateringer, antivirussignaturer eller andet til hjemmearbejdspladserne, opdateres samtidig de referenceværdier, som virksomheden opbevarer omkring hjemmearbejdspladsernes filintegritet. Således kan det fra centralt hold kontrolleres, at alle hjemmearbejdspladser har de nødvendige opdateringer, ligesom det kan detekteres, hvis installationen af en opdatering fejler.

I de tilfælde, hvor et andet operativsystem er påkrævet, må der laves afvigelser fra ovenstående. Det kan fx være, hvis en grafisk afdeling ønsker Apple-computere, eller hvis en udviklingsafdeling ønsker at benytte Linux-baserede enheder. Der bør kræves gode argumenter for, hvorfor fjernstyringen (fx vha. VNC) af en i virksomheden placeret enhed med dette operativsystem ikke er tilstrækkeligt før brugen af et alternativt operativsystem tillades, da virksomheden påtager sig en betydelig administrationsomkostning, ligesom der kræves en yderligere indsats for at sikre systemerne. Således findes meget af den sikkerhedssoftware, som ellers benyttes, ikke til alle operativsystemer, og virksomheden må derfor enten sikre enhederne med alternativ software, eller hæve sikkerheden med brug af yderligere netværksenheder i hjemmet.
Som nævnt vil dette være specielle tilfælde, og da hvert tilfælde vil være individuelt, vil dette ikke blive gennemgået yderligere her. Dog understreges det, at homogeniteten af hjemmearbejdspladserne er et grundlæggende fundament for at løsningen kan skalere tilfredsstillende. Hjemmearbejdspladser bør, som nævnt før uddeles, så tynde klienter har første prioritet, Windows-klienter anden prioritet og alternative klienter laveste prioritet.

Uanset hvilken metode der vælges, bør hjemmearbejdspladsen konfigureres til at aktivere en screen saver, hvis ikke maskinen benyttes i en periode. Maskinen vil herefter kræve at brugeren autentificeres, før den igen kan benyttes. Dette sker for at sikre, at hjemmearbejdspladser som forlades, ikke kan benyttes af angribere, som opnår fysisk adgang til enheden. Af samme årsag bør specielt VPN-dialeren sikres mod tyveri, fx ved brug af Kensington-låse.

7.3.4 Opsummering

Implementeringen af ovenstående systemer leverer et sikkerhedsniveau for hjemmearbejdspladserne, som antages acceptabelt for de fleste danske virksomheder. Oplevelsen fra hjemmearbejdspladsen bør i et korrekt implementeret system være smertefri og brugervenlig, og i tilfældet med tynde klienter levere et grafisk overblik over netværksressourcerne, som vil være helt lig den, som leveres fra virksomhedens interne, tynde klienter.
I de tilfælde, hvor fulde klienter benyttes, vil oplevelsen ligeledes være stort set den samme, som hvis medarbejderen sad i virksomheden. Således vil maskinerne benytte samme opsætning, og da VPN-forbindelsen etableres automatisk fra hjemmet, vil den eneste forskel for medarbejderen være den ekstra autentificering med OTP, som kræves, når der arbejdes fra hjemmet.
Hjemmets private udstyr kan dele bredbåndsforbindelsen med hjemmearbejdspladsen på en måde, som ikke stiller krav til det private udstyr eller til konfigurationen af dette. Samtidig kan ressourcer som printere deles mellem de to netværk i hjemmet uden at sikkerheden kompromitteres.

Bag kulisserne foregår der dog en grundig analyse af trafikken til og fra virksomheden og hjemmene. En række IDS-enheder kontrollerer, at der ikke foretages angreb hverken internt eller eksternt. Firewalls analyserer og filtrerer trafikken på alle understøttede lag, og den generelle infrastruktur sikrer adskillelse af de forskellige dele af netværket ved hjælp af VLANs, PVLANs og ACLs. I vurderingen af designforslaget i kapitel 8 er gennemgået, i hvor vidt omfang løsningen har afhjulpet de problemer rapporten har beskrevet, samt hvorvidt de samlede krav er opfyldt.

Det kan bemærkes, at den tidligere omtalte teknologi 802.1x ikke benyttes i hjemmene. Dette ville have givet et ekstra lag af beskyttelse, men da teknologien endnu ikke er implementeret i udstyr, som er gearet til brug i små netværk som hjemmearbejdspladser, har det ikke været muligt at finde udstyr, som kunne opfylde ønsket om at inkludere dette i designet. Cisco fortæller dog [121], at dette udstyr kan forventes i løbet af året. Det må forventes, at andre leverandører har samme planer. I så fald kan teknologien senere implementeres i designet.

VPN-systemet udgøres i designet af Cisco VPN-enheder i hjemmene og en Cisco VPN Concentrator i virksomheden. Dette kan erstattes af CheckPoint's VPN-1 system med samme resultat idet også CheckPoint-udstyret er understøttet af fx RealSecure og Zone Labs. Desuden kan fx Norton AntiVirus benyttes sammen med McAfee's produkter til at give endnu bedre beskyttelse mod virusangreb.

I forbindelse med analyseringen af log-data findes fx værktøjet NetIQ's Security Manager[81]. Dette produkt kan sammenkøre logfiler fra Cisco routere, switche og PIX firewalls, CheckPoint Firewall-1 produkter, Cisco VPN Concentratorer og RealSecure Desktop Protection software samt NIDS og HIDS-systemer fra de større leverandører. Produktet kan desuden samle rapporter fra McAfee's antivirusløsninger og integrere disse i de samlede rapporter og oversigter over netværkets tilstand. På denne måde kan data indsamles fra stort set alle netværkets rapporterende enheder i ét produkt, som samtidig kan udføre real time analysering af dataene og udløse alarmer baseret på regelsæt.

I det følgende kapitel vurderes løsningsdesignet med henblik på at undersøge, om de samlede krav fra afsnit 6.7 er opfyldt, ligesom det vurderes, om de sikkerhedsproblemer, der er beskrevet i rapporten, er løst med ovenstående designforslag.

[81] NetIQ's Security Manager kan findes på adressen http://www.netiq.com/products/sm/

8 VURDERING AF DESIGNFORSLAG

Designforslaget fra kapitel 7 gennemgås her i forhold til de i rapporten nævnte sikkerhedsproblemer. Samtidig undersøges hvorvidt designet opfylder kravene fra kapitel 6. Vurderingen er således en gennemgang af, i hvor høj grad designet kan benyttes som en løsning på de i rapporten beskrevne problemer. Samtidig gennemgås, hvordan brugere fra hver af de to brugergrupper kan benytte arbejdspladserne i hjemmet, og hvorvidt dette kan være et værdifuldt arbejdsredskab for medarbejderne.
Generelt om designet kan siges, at det primært er rettet mod mellemstore virksomheder, som via en større mængde hjemmearbejdspladser kan retfærdiggøre udgiften til den nødvendige infrastruktur. For en mellemstor virksomhed med omkring 100-500 hjemmearbejdspladser vil designet således være en fornuftig løsning.

For en større virksomhed kan designet som beskrevet i kapitel 7 skaleres. Således kan internetopkoblinger, VPN Concentratorer og den resterende infrastruktur udbygges til at håndtere både flere brugere, større båndbredde og bedre redundans uden at det fundamentale design ændres. Den større mængde brugere vil retfærdiggøre de nævnte udvidelser, og selve netværksstrukturen kan bibeholdes på trods af udvidelserne. Netop dette giver mulighed for, at en virksomhed kan vokse og løbende opgradere netværket til at understøtte et stadigt stigende antal brugere.

Mindre virksomheder, som måske har behov for 10 hjemmearbejdspladser, kan dog ikke benytte det beskrevne design. Her vil omkostningerne ved at etablere den nødvendige infrastruktur være for store set i forhold til antallet af brugere. Det kan være svært at forestille sig, hvordan helt små virksomheder kan etablere sikre hjemmearbejdspladser, som overholder lovgivningerne og som har et forsvarligt sikkerhedsniveau. I sådanne tilfælde kan det være fordelagtigt at benytte datacentre, som samler mange mindre virksomheders behov i større implementeringer, hvorved udgifterne til en struktur som beskrevet i designet kan deles ud mellem mange små virksomheder.

Det har desværre ikke været muligt at implementere designet i et testmiljø. Derfor kan der ikke udføres angrebsforsøg mod netværket eller bekræftes kompatibilitet mellem produkterne. Ligeledes kan der ikke inkluderes konfigurationsindstillinger til udstyret.

8.1 Opfyldelse af krav

I dette afsnit gennemgås hvorvidt designet opfylder de krav, som kan ses i tabellen i afsnit 6.7. Således gennemgås hvert krav med en bemærkning til, hvordan designet forholder sig til dette.

Krav	*Løsning*
Adgang til nødvendigt udstyr, software, filer mm. skal være til stede	*Brugen af Citrix-systemer eller klienter, som reflekterer opsætningen i virksomheden, sikrer en ensartet adgang. Ligeledes benyttes fjernstyring af specielle enheder.*
Transparent opkobling	*Hardwarebaseret VPN-udstyr sikrer en transparent opkobling til virksomheden, kun afbrudt af kravet om brugerautentificering.*
Brugervenlighed	*Citrix-systemer og Windows-baserede enheder, som reflekterer opsætningen i virksomheden, sikrer en let overgang til brugen af hjemmearbejdspladser.*
Computer må ikke efterlades forbundet til netværket	*Screen savere i hjemmet og bluetooth-udstyr i virksomheden låser maskiner, som ikke benyttes.*
Data må ikke lagres lokalt	*Tynde klienter har end ikke denne mulighed, mens de Windows-baserede hjemmearbejdspladser låses via Group Policies for bl.a. at undgå lokal lagring af data.*
Bredbåndsforbindelsen i hjemmet må deles med privat udstyr / privat udstyr skal holdes adskilt fra hjemmearbejdspladsen	*Adskillelsen mellem privat udstyr og hjemmearbejdspladsen foregår med en firewall, som blokerer adgangen den ene vej, men tillader udprintning den anden.*
Passwords må ikke gemmes i PC	*Som med lokal lagring af data er dette løst med både tynde klienter og Windows-baserede hjemmearbejdspladser.*
Hjemmearbejdspladsen skal opdateres med nyeste service packs, patches, antivirus-signaturer, konfigurationsopdateringer mm.	*Kombinationen af VPN Concentratoren og software fra enten RealSecure eller Zone Labs sikrer, at hjemmearbejdspladserne holdes opdaterede med antivirussignaturer, konfigurationer og opdateringer. Patches og service packs distribueres via Group Policies.*
Autentifikation må ikke alene baseres på passwords	*Der benyttes digitale certifikater til at autentificere VPN-udstyret og SecurID OTP-enheder til at autentificere brugerne.*

Krav	*Løsning*
Data i transit mellem hjemmet og virksomheden skal beskyttes mod aflytning, genafspilning og ændring	*Brugen af IPSec VPN baseret på 3DES kryptering og SHA-1 integritetskontrol sikrer dataene mod aflytning, genafspilning og ændring.*
Krypteringsalgoritmer skal baseres på fx DES, Triple-DES eller AES	*Triple-DES (3DES) benyttes som krypteringsalgoritme.*
Alle arbejdsstationer og brugere skal være unikt autentificeret	*Ved ikke alene at afhænge af autentificeringen af VPN-enhederne sikres, at alle hjemmearbejdspladsbrugere er unikt autentificeret. I virksomheden autentificeres arbejdsstationerne via 802.1x og brugerne, når de logger på arbejdsstationen.*
Hjemmearbejdspladsen skal være beskyttet mod eksterne angreb	*Brugen af to stateful packet inspection firewalls, en router og diverse software på hjemmearbejdspladsen sikrer denne mod angreb fra eksterne enheder.*
Den enhed, som beskytter hjemmet mod eksterne angreb skal opdateres centralt	*Både firewalls, routere og VPN-dialere konfigureres og opdateres fra virksomheden.*
Hjemmearbejdspladsen skal sikres mod trojanske heste	*Brugen af TauScan på hjemmearbejdspladserne i tilfælde hvor tynde klienter ikke kan bruges, sikrer rimelig beskyttelse mod trojanske heste. Desuden benyttes McAfee antivirusprogrammer, som også beskytter mod disse. Alle e-mails scannes i virksomheden før hjemmearbejdspladsen kan få adgang til dem, hvorved endnu et beskyttelseslag tilføjes. Benyttes der Windows-klienter er disse låst, så ingen fremmede programmer kan afvikles fra maskinen.*
Hjemmearbejdspladsen skal sikres mod virus	*Brugen af antivirusprogrammer på hjemmearbejdspladsen, på virksomhedens servere, e-mail gateways samt arbejdsstationerne sikrer sammen med en daglig opdatering af signaturfilerne, at hjemmearbejdspladsen holdes virusfri.*
Hjemmearbejdspladsen skal sikres mod keyloggers	*Tauscan giver en udmærket sikkerhed mod softwarebaserede keyloggers, mens brugen af tynde klienter fjerner muligheden helt. Hardwarebaserede keyloggers kan der ikke beskyttes imod, men brugen af OTP og digitale certifikater hjælper til at sikre, at det selv i disse tilfælde ikke er muligt at stjæle adgangskoder til systemet.*
Hjemmearbejdspladsen skal sikres mod andre potentielle trusler	*Hjemmearbejdspladsen er sikret med stateful packet inspection firewalls samt en personlig firewall, antivirus- samt integritetsprogrammel så enhver ændring til hjemmearbejdspladsens operativsystem, programmer eller konfiguration vil blive detekteret næste gang forbindelsen til virksomheden oprettes.*
Installationer og ændringer af konfigurationer på hjemmearbejdspladsen må ikke være mulig for brugere eller angribere	*Tynde klienter har ikke denne mulighed som udgangspunkt, og Windows-klienterne bliver kontrolleret via Group Policies som sikrer, at kun administratorer i virksomheden kan foretage ændringer eller installere programmer på maskinerne.*
Så vidt muligt skal hjemmearbejdspladsbrugeren autentificeres før der etableres forbindelse til virksomheden	*Brugen af 802.1x er endnu ikke implementeret i hjemmene pga. mangel på udstyr, som understøtter dette.*
Hjemmearbejdspladsens bør sikres fysisk	*Der er foreslået brugen af Kensington-låse, som låser både netværksenheder og arbejdsstationer fast til fx borde eller gulve.*
Autentificering skal ske mod centraliseret valideringsdatabase	*En RADIUS-server i virksomheden håndterer brugernavne, passwords, SecurID og digitale certifikater samt synkroniserer disse oplysninger med de services, som har behov for at opbevare lokale kopier af dette (fx Windows domæneservere).*
Passwordregler om kompleksitet mm. skal overholdes	*Dette foretages af RADIUS-serveren, som fx kan udgøres af en Cisco Access Control Server.*

Krav	*Løsning*
Virksomhedens udstyr skal beskyttes mod eksterne, interne og hjemmearbejdsplads-brugere	*I virksomheden benyttes mange lag af sikkerhed. Således sikrer routere, switche og flere firewalls fra forskellige fabrikanter udstyret mod eksterne angreb. Internt er opbygget strenge routingregler og VLANs samt PVLANs til at sikre, at kun enheder med et legitimt behov kan kontakte andre enheder. En firewall beskytter de interne servere, og NIDS'er og HIDS'er sikrer servere og netværksforbindelser.*
Virksomhedens opkaldspunkter må ikke fremstå som tydelige angrebsmål	*Der benyttes et honeynet til at tiltrække angribere samt en honeypot til at detektere angreb mod DMZ'en.*
Logon proceduren skal afsløre så lidt som muligt	*Der gives ingen information om, hvorvidt brugernavne eller passwords er skyld i et fejlslået adgangsforsøg.*
Hjemmearbejdspladsbrugernes adgang skal kunne begrænses	*Brugen af VLANs og PVLANs samt ACLs i routere sikrer, at hjemmearbejdspladserne kun har adgang til de services, de har behov for. Således får de tynde klienter alene adgang til Citrix Secure Gateway serverne, mens de øvrige har adgang til de nødvendige servere, men ikke arbejdsstationer, managementudstyr osv. De brugere med behov for at fjernstyre enheder i virksomheden, tildeles denne adgang specifikt og adgangen foregår på et separat VLAN.*
En offentlig maskine må ikke kunne angribe andre (inkl. hjemmearbejdspladsen)	*En firewall sikrer, at der ikke kan etableres udgående forbindelser fra de enheder på netværket, som ikke bør etablere disse. Der benyttes VLANs og PVLANs til at isolere enhederne, og routere og firewalls sikrer, at der ikke tillades trafik fra servere og arbejdsstationer tilbage til hjemmearbejdspladsen.*
Trafikken til og fra hjemmearbejdspladsen må ikke kunne aflyttes af eksterne eller interne brugere i virksomheden	*Brugen af switche leverer første lag af sikkerhed mod aflytning internt i virksomheden efter IPSec-krypteringen er termineret. VLANs, PVLANs, ACLs og firewalls leverer endnu et lag, mens kontrol med arbejdsstationer og netværksporte leverer det sidste. Når trafikken traverserer internettet benyttes kryptering via IPSec.*
Der må ikke kunne initieres forbindelse fra virksomhed til hjemmearbejdsplads	*Denne mulighed blokeres i både firewalls og ACLs, ligesom VPN Concentratoren er placeret i et separat VLAN. Der tillades ingen adgang til hjemmearbejdspladsen ud over IPSec-adgangen. Dette sikres af hjemmets sikkerhedsudstyr.*
Der skal (og må) foretages overvågning af brugen af hjemmearbejdspladserne (logning)	*Både udstyret i hjemmet og i virksomheden udfører logning, som samles centralt via syslog-servere i virksomhedens managementsegment. Sammenkøringen af data kan give en profil af brugeropførsel, som kan være nyttig for både ordensmagten og virksomhedens egen efterforskning.*
Alle loginforsøg skal (og må) overvåges	*Ovenstående logning kan sikre, at disse forsøg registreres.*
Det må ikke være muligt at omdirigere trafikken fra hjemmet til virksomheden	*Brugen af digitale certifikater sikrer identiteten af både VPN klienterne og VPN Concentratoren samt kontrollerer, at omdirigering af trafikken ikke kan finde sted.*
Opstilling af IDS i virksomheden anbefales	*Der benyttes adskillige NIDS'er til at detektere angreb forskellige steder i både virksomhedens og hjemmets netværk. HIDS'er benyttes på alle virksomhedens servere og udvalgt udstyr.*
Benyttes digitale signaturer, bør den private nøgle opbevares på et chipkort	*Brugerne benytter ikke digitale signaturer i den nuværende opsætning..*
E-mail gateways, servere og lignende bør sikres mod virus	*McAfee GroupShield, WebShield, NetShield og VirusScan sikrer servere og gateways mod virusangreb.*
Integritetsudstyr bør benyttes på data, servere, netværksudstyr og lignende.	*Tripwire benyttes på både servere, netværksudstyr, arbejdsstationer og hjemmearbejdspladser.*
Ved adgangssystemer bør "forbyd alt som ikke tillades" benyttes i stedet for "tillad alt, som ikke forbydes"	*Der benyttes som udgangspunkt "forbyd alt som ikke tillades" på alt netværksudstyr i både virksomheden og hjemmet.*

Krav	*Løsning*
Der skal etableres beskyttelse af portene på netværksudstyret	*Ubenyttede porte er samlet i et ubrugt VLAN og slået fra. Desuden benyttes 802.1x i virksomheden til at sikre, at der ikke kan opnås adgang til netværket via en ledig netværksport uden autentifikation.*
Der skal udføres kontrol med udgående trafik for at sikre, at konfidentielle e-mails og data ikke sendes ud af virksomheden	*Både e-mail servere og firewalls kontrollerer, at fortrolige filer ikke forlader virksomheden, hvis dette ikke ønskes.*
Kritiske programmer skal under en kontrol, som sikrer, at de ikke kan eksekveres, hvis der er foretaget uautoriserede ændringer	*Til dette formål benyttes RealSecure Desktop Protector.*
Logon-systemer skal beskrive, at uautoriseret adgang ikke tillades	*De enheder, som leverer adgang til eksterne forbindelser beskriver, at uautoriseret adgang til systemerne ikke er tilladt.*
Der skal være kontrol med datakommunikationsretningen	*PVLANs og VACLs kombineret med ACLs og VLANs sikrer, at datakommunikationen kontrolleres på bedst mulig måde både internt i virksomheden samt mellem hjemmearbejdspladsen og virksomheden.*
Alle enheder skal tidssynkroniseres	*Tidssynkronisering sikres via Group Policies for arbejdsstationer, mens serverne indbyrdes udfører synkronisering med en NTP-server. Netværksudstyret modtager også tidssynkroniseringen via en NTP-server.*

Som det ses opfyldes kravene bortset fra brugen af 802.1x i hjemmene, hvilket endnu ikke er muligt at implementere. Dette er ikke overraskende, idet designet er opbygget med baggrund i disse krav. Designet repræsenterer en fornuftig implementering af kravene, som får inkorporeret alle de nævnte krav samtidig med, at strukturen holdes så simpel og overskuelig som muligt.
Gennemgangen tjener til at vise, på hvilken måde designet forholder sig til kravlisten. På samme måde gennemgås nedenfor hvordan designet håndterer de angrebsmetoder, som er beskrevet i kapitel 3.

8.2 Håndtering af angrebsmetoder

I kapitel 3 er gennemgået en række angrebstyper og sikkerhedsproblemer, som hjemmearbejdspladser kan udsættes for. I dette afsnit gennemgås disse for at undersøge, hvorvidt det foreslåede netværksdesign kan beskytte hjemmearbejdspladserne mod disse angreb. Ligeledes gennemgås Angrebseksemplerne fra Appendiks A.

Aflytning
Brugen af pakkesniffere kan ske både internt i hjemmet, under transmissionen fra hjemmet til virksomheden samt internt i virksomheden.
I hjemmet løses dette problem ved at isolere hjemmearbejdspladsen bag en firewall og VPN-dialer så intet andet udstyr deler netværksforbindelsen før VPN-forbindelsen er etableret. På denne måde er trafikken krypteret før den når ud til den switch, som sikrer, at bredbåndsforbindelsen i hjemmet kan deles mellem hjemmearbejdspladsen og husets øvrige enheder.
Under transmissionen mellem hjemmet og virksomheden er dataene krypteret og beskyttet mod genafspilning og modifikation. Da der samtidig benyttes OTP til autentificeringen af brugerne, vil en angriber ikke kunne benytte oplysninger om passcoden til senere at logge ind, selvom det skulle lykkedes at komme i besiddelse af den.
I virksomheden benyttes ACLs, VLANs, PVLANs og VACLs til at sikre, at trafikken er så isoleret som muligt. Porte, som ikke benyttes er slået fra og samlet i et ubenyttet VLAN, ligesom det er sikret at kun porte, som bør have denne funktion, kan konfigureres til at blive trunkporte.
For at undgå, at angreb som det beskrevet i afsnit 3.1 kan gennemføres, sikrer internetudbyderens router, at flooding af virksomhedens interne enheder ikke tillades. Skulle angriberen alligevel få mulighed for dette, vil angreb på den yderste router alene give mulighed for at komme i besiddelse af de krypterede data fra VPN-forbindelsen. Ønskes den senere router angrebet, skal angriberen igennem to firewalls og adskillige NIDS-enheder.
Angreb på virksomhedens switche med fx overflow af adressetabellen undgås ved sikre, at der kun kan benyttes en eller få MAC-adresser fra hver netværksport. Selv hvis switchen skulle begynde at udsende pakker på alle porte indenfor broadcastdomænet, sikrer opdeling i mange broadcast-domæner (VLANs), at disse pakker kun sendes til en begrænset del af netværket.

Trust udnyttelse
Trust udnyttelse forsøges undgået ved at implementere meget strenge regler for hvilke enheder der kan tale sammen. Således benyttes ACLs, VLANs, PVLANs og VACLs for at sikre, at fx serverne i DMZ'en kun kan besvare forespørgsler og hverken kan etablere udgående trafik eller kommunikere med de øvrige enheder i DMZ'en. Herudover sikrer de benyttede firewalls, at trafik mellem segmenterne kun tillades, hvor dette er nødvendigt ligesom brugen af NIDS'er og HIDS'er hjælper til at detektere eventuelle angreb mellem enhederne.

IP spoofing
Eksterne angribere, som forsøger at benytte IP spoofing til at afsende pakker til virksomheden, og som har en afsenderadresse fra virksomhedens interne netværk, vil blive afvist allerede før trafikken når virksomhedens router, idet internetudbyderens router er konfigureret til at blokere sådanne pakker. Sendes en pakke med en afsenderadresser fra en hjemmearbejdsplads kan denne – hvis den samtidig er en del af en IPSec pakkestrøm – nå VPN Concentratoren. Her vil den dog blive blokeret, idet VPN Concentratoren vil kontrollere, om afsenderens VPN-enhed er i besiddelse af det korrekte digitale certifikat. Selv hvis dette er tilfældet kræves herefter OTP-autentificering, før der gives adgang til netværket.
IP spoofing internt i virksomheden har lille effekt, idet der benyttes VLANs og PVLANs, som operer på lag 2.

Passwordangreb
Passwordangreb modvirkes i designet ved brug af OTP-systemet samt ved at sikre hjemmearbejdspladserne mod trojanske heste og keyloggere. Hardwarebaserede keyloggere kan dog stadig benyttes, men da hver passcode kun kan benyttes én gang, er dette mindre væsentligt.
Det primære problem med denne type angreb i det viste design er hvis angriberen kan installere software, som kan overtage forbindelsen (eller se med) mens brugeren benytter den. Således er forbindelsen allerede oprettet hvilket forbigår de ovenstående forsvarsmekanismer. Dette forsøges dog undgået ved at sikre hjemmearbejdspladsen med både integritetssoftware, personlig firewall, virusscanner og en scanner for trojanske heste.

Portomdirigering
I det foreslåede design er inkluderet offentlig adgang til servere i en DMZ. Da der samtidig er givet adgang for serverne i DMZ'en til de interne servere til fx e-mail eller databaser, er disse servere i DMZ'en oplagte kandidater, hvis en angriber forsøger sig med portomdirigering. For at undgå dette er der i designet benyttet en firewall, som kontrollerer at den trafik, som sendes på fx port 80, faktisk er http, ligesom selve trafikken analyseres på applikationslaget. Alle servere er desuden udstyret med en HIDS, ligesom Tripwire benyttes til at sikre, at enhver ændring til serverne detekteres.
I hjemmet sikrer routere og firewalls, at ingen trafik kan nå hjemmearbejdspladsen, ligesom det i virksomheden sikres, at der ikke kan etableres forbindelse fra virksomheden gennem IPSec-forbindelsen til hjemmet. Da hjemmearbejdspladsen enten er en tynd klient eller udstyret med en række forsvarsmekanismer, er chancen for installation af programmel på denne minimeret.

Angreb direkte på hjemmearbejdspladsen
Hjemmearbejdspladsen er beskyttet på mange måder i designet. Direkte angreb mod hjemmearbejdspladsen bliver modvirket af routere, firewalls og software, som skal sikre, at ingen trafik når enheden. Således blokeres al indkommende trafik i den sidste firewall, mens den første filtrerer al trafik fra, som ikke specifikt er tilladt i forbindelse med hjemmets private udstyr. Angrebene skal desuden forbi en NIDS-enhed, ligesom hjemmearbejdspladsen selv er beskyttet med en personlig firewall samt integritetssoftware, antivirus og forsvar mod trojanske heste. Er der tale om en tynd klient, kan denne end ikke afvikle programmer og er dermed ikke sårbar overfor størstedelen af denne type angreb.
Angreb fra hjemmets private udstyr skal på samme måde igennem en firewall samt NIDS, og disse maskiner betragtes som udgangspunkt som værende lige så farlige, som maskiner på internettet. Forsvaret er derfor gearet til at håndtere angreb fra disse maskiner.

Angreb mod opkaldspunktet
Virksomhedens opkaldspunkt består af en VPN Concentrator, som er placeret bag en router og en firewall, som skal sikre, at kun IPSec-trafik får lov til at nå enheden. Samtidig benyttes OTP og digitale certifikater til at sikre, at kun en bruger med adgang til både den korrekte VPN-dialer, OTP-enhed samt PIN-kode kan etablere forbindelse.
På trods af alt dette er VPN Concentratoren et udsat angrebspunkt. Der er ingen måde at analysere de data, som sendes i krypteret form til enheden. Den største fare ligger i, at der findes en sårbarhed i enheden, som kan benyttes til at omgå de sikkerhedsmekanismer, som skal forhindre, at uvedkommende kan passere enheden. Det er derfor vigtigt, at alle netværksenheder holdes opdaterede, hvilket sker fra management-segmentet på det interne netværk. I det tilfælde, at en angriber alligevel kommer forbi VPN Concentratoren, behandles trafikken næsten på samme måde som trafik direkte fra internettet og skal derfor igennem samme filtrering og analysering af både firewalls og NIDS'er, før der tillades adgang til det interne netværk. Lykkedes det også at komme igennem dette, er alle servere og arbejdsstationer isolerede og beskyttede mod angreb i sig selv ved hjælp af bl.a. HIDS'er og antivirus-systemer.

Social Engineering
Risikoen ved social engineering kan ud over uddannelse af brugerne modvirkes ved at etablere et godt netværksdesign. Således hjælper designet til at beskytte med social engineering-angreb ved at sikre, at passwords ikke let kan udleveres idet der benyttes OTP. Selv hvis en bruger udleverer adgangsoplysninger til angriberen, vil denne ikke kunne tilegne sig yderligere adgang til netværket end den pågældende bruger havde. Dette skyldes brugen af VLANs, PVLANs og ACLs, som hjælper til at håndhæve reglerne om adgangsbegrænsninger.
Der er dog ingen teknik, som forhindrer, at en ansat bærer fortrolige papirer ud af virksomheden så længe disse kan printes, ligesom der ikke er noget der forhindrer, at en ansat fortæller noget over telefonen.

Det er derfor essentielt, at virksomheden er opmærksom på den problemstilling som eksisterer og som forværres af brugen af hjemmearbejdspladser. Der bør være klare retningslinier for, hvad der må siges over telefonen samt hvilke informationer, der må forlade virksomheden.
Administratorerne kan forsøge yderligere at afhjælpe problemet ved fx at checke, at URLs ikke indeholder suspekte strenge (som det foreslås i afsnit 3.8). Samtidig kan sikres, at enhver bruger altid kun har adgang til de oplysninger, som er nødvendige for brugeren. Dette kan begrænse den mængde information, som kan forlade virksomheden af denne vej, men det kan ikke afhjælpe alle social engineering-relaterede problemer. Undervisning af brugere og administratorer er den eneste effektive måde at forebygge angrebene på.

Angreb på data link laget
I Appendiks A er nævnt fem angrebstyper mod data link laget. Disse er CAM table overflow, VLAN hopping, Spanning-Tree protokolmanipulering, MAC og ARP spoofing samt DHCP ”udsultning”. De forsvarsmekanismer mod disse som eksisterer i designet er kort gennemgået nedenfor.

CAM table overflow-angrebet kræver, at angriberen kan udsende pakker med mange forskellige MAC-afsenderadresser. Dette er der kompenseret for i designet, hvor serverne har én og arbejdsstationerne tre mulige MAC-adresser pr. port. Cisco switchene, som benyttes, er desuden udstyret med smarte CAM-tabeller, som ikke tillader eksisterende poster i CAM-tabellerne at blive overskrevet. Selv hvis en CAM-tabel var sårbar, og angriberen kunne afsende de nødvendige pakker med forskellige MAC-afsenderadresser ville brugen af VLANs og PVLANs mindske problemet, idet dette er baseret på netværksporte og ikke MAC-adresser.

VLAN hopping er delt i to angreb. Switch spoofing kræver, at angriberen kan få switchen til at modificere en portkonfiguration, så denne bliver til en trunkport mens double tagging kræver, at angriberens computer er forbundet til en port, som har samme VLAN ID som trunkporten.
Ingen af disse angreb er mulige, hvis det foreslåede design implementeres korrekt. Således er alle ubenyttede porte slået fra og tilsluttet et ubenyttet VLAN ID. Trunkporte benytter et VLAN ID, som ikke benyttes andre steder på netværket, ligesom alle porte, som ikke har behov for at være trunkporte, har denne mulighed frakoblet. Da disse konfigurationer også gælder de switche, som hjemmearbejdspladsernes trafik går igennem, når de når virksomheden, er også disse beskyttet mod sådanne angreb.

Spanning-Tree protokolmanipulering kan modvirkes ved for det første at slå Spanning-Tree protokollen fra, idet det foreslåede design ikke har en topologi, som kan give anledning til loops. Desuden kan portene konfigureres, så porte, som benyttes af arbejdsstationer eller servere – eller som slet ikke benyttes – ikke kan udsende BPDU-signaler. Ligeledes kan Cisco’s Root Guard funktion benyttes til at sikre, at disse porte ikke kan opnå root bridge status, så længe der benyttes Cisco switche.
Dette vil også sikre, at hjemmearbejdspladserne ikke kan benyttes til denne type angreb, idet disse også går igennem switche i virksomheden, som vil være konfigureret på ovenstående måde.

MAC og ARP spoofingangreb kan til dels modvirkes ved kun at tillade enkelte MAC-adresser fra hver port. Samtidig kan switche konfigureres så aktive maskiners information i CAM-tabellen ikke kan overskrives. Benyttes der desuden PVLANs så kun de porte, som har aktuelt behov for det, kan tale sammen, er chancen for angrebet minimeret. Men med mindre der specificeres én MAC-adresse pr. port, kan denne angrebstype ikke helt undgås, selvom den kan gøres betydeligt sværere at udføre. Hjemmearbejdspladserne er beskyttet yderligere, idet en netværksport i hjemmet valideres med digitale certifikater, før der tillades adgang til virksomhedens netværk.
En formildende faktor i virksomheden er implementering af 802.1x til validering af arbejdspladsens identitet før netværksadgangen gives. Dette forhindrer dog ikke, at en legitim arbejdsplads benyttes til angrebet.

Forsvaret mod DHCP ”udsultning” ligger i, at der kun tillades få MAC-adresser pr. netværksport, samt at de stationære enheder som arbejdsstationer og servere kan udstyres med faste IP-adresser, så DHCP udelukkende benyttes på de porte, hvor fx bærbart udstyr eller gæsters udstyr tilsluttes. Hjemmearbejdspladserne tildeles som regel IP-numre via en DHCP-server og vil derfor være udsatte for angrebet. Dette forebygges ved at sikre, at der ikke kan etableres forbindelse fra virksomhedens netværk tilbage til hjemmearbejdspladsen, som derfor ikke kan fungere som DHCP-server. Desuden sikrer firewalls, at DHCP-forespørgsler kun kan besvares fra bestemte VLANs.

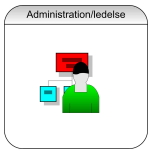
Angreb på applikationslaget
Netværksdesignet beskytter mod angreb på applikationslaget ved at inkludere HIDS’er på alle servere, personlige firewalls på arbejdsstationerne, NIDS’er på de netværkssegmenter, som er mest udsatte, samt jævnlig opdatering af både netværksudstyr, servere og arbejdsstationer. Der foretages logning på alle enheder, som samles centralt og analyseres af værktøjer for at fremhæve eventuelle sikkerhedsproblemer. Firewalls analyserer data på applikationslaget for at sikre, at der er tale om legitim trafik til de enheder, som beskyttes. Hjemmearbejdspladserne beskyttes på samme måde og brugen af integritetssoftware på hele netværket sikrer, at skulle en angriber have held til at bryde igennem ovenstående systemer, kan dette detekteres.
Et honeynet forsøger desuden at lokke angribere til, som herefter kan blokeres fra det reelle netværk.

Netværksrekognoscering
Netværksrekognoscering i form af fx portscanninger er ikke i sig selv farlige, men forsøges alligevel til dels modvirket, idet det ofte er angriberens første værktøj i forbindelse med et angreb. Således blokerer routere og en firewall al trafik, som ikke har destinationsadresser, som matcher de offentlige servere eller VPN Concentratoren. Selv hvis dette er tilfældet, kan kun trafik på de porte, som de respektive servere og enheder tilbyder benyttes. Således er det ikke umiddelbart muligt at scanne en webserver på andet end port 80, og selv her kan en firewall med analysering af data på applikationslaget i visse tilfælde blokere scanningen. Angriberne kan dog få oplysninger om hvilke IP-numre, der kan tilgås udefra ved at foretage en sådan scanning. Dog vil også honeynettet blive scannet, hvilket kan resultere i, at angriberen lokkes til at foretage sine angreb her i stedet for mod virksomhedens øvrige udstyr.
Hjemmearbejdspladserne beskyttes på samme måde mod scanninger, og her vil kun privat udstyr (og kun i visse tilfælde) kunne scannes.

DDoS-angreb
DDoS-angreb stoppes så vidt muligt hos internetudbyderen ved at blokere for private IP-afsenderadresser samt begrænse båndbredden, som kan benyttes til fx ICMP-trafik. Den firewall, som beskytter bl.a. de offentlige servere fungerer desuden som "mellemmand" for TCP-forbindelsernes oprettelse, således at TCP SYN-angrebet ikke kan påvirke servere.

8.3 Brugeroplevelsen

Brugeroplevelsen er en væsentlig faktor i forbindelse med hjemmearbejdspladserne. Brugervenligheden har høj prioritet, da hele baggrunden for brug af hjemmearbejdspladser netop er, at man ønsker at forøge både medarbejdernes livsglæde og performance.
Det har derfor været væsentligt i opbyggelsen af designet, at de to brugergrupper med individuelle behov begge skal kunne benytte det grundlæggende netværksdesign, og begge skal have en god oplevelse, som afspejler deres arbejdsplads i virksomheden.



For administrationsgruppen vil der typisk være tale om Citrix-brugere, som i princippet ingen forskel vil mærke i forhold til deres Citrix-baserede arbejdsstation i virksomheden. Skærmbillederne er de samme, og det er muligt at efterlade et åbent tekstbehandlingsdokument i virksomheden og arbejde videre fra samme linie i hjemmet. Hvis der benyttes Windows-baserede arbejdsstationer i virksomheden kan dette også gøres i hjemmet. I så fald vil arbejdsstationen være opsat på samme måde, have samme programmer og samme indstillinger som på arbejdet, hvorfor den eneste forskel for medarbejderen vil være den ekstra autentificering med OTP, som skal gennemføres fra hjemmet. Filer, intranet og andre ressourcer vil være tilgængelige ligesom på arbejdspladsen. Det er endda muligt at synkronisere fx skrivebordet (desktopppen), "My Documents" og favoritter fra Internet Exploreren mellem arbejdspladsen i virksomheden og hjemmearbejdspladsen.

For udviklergruppen vil situationen være en anelse anderledes, idet denne gruppe ud over deres sædvanlige arbejdsplads får mulighed for at tilgå det specielle udstyr, som de måtte have brug for. Således kan der være tale om at fjernstyre enheder, som brugerne ellers ville have fysisk adgang til i virksomheden. Dette kan være mere besværligt, men da disse medarbejdere må antages at have en høj teknisk kunnen, bør det ikke være uoverkommeligt. Der kan endda bygges en intranetside som leverer en grafisk oversigt over de enheder på netværket, som medarbejderen har adgang til. Siden kan integreres med programmer som fx VNC, så et klik på enheden på hjemmesiden bringer skærmbilledet fra denne op via VNC (og tilhørende autentifikation).

Udprintning i hjemmet kan ske enten via en printer direkte tilkoblet hjemmearbejdspladsen (dette er også muligt med Citrix-klienter) eller via en printer, som deles med hjemmets øvrige udstyr, og som er placeret sammen med dette. Der kan desuden printes til netværksprintere i virksomheden direkte fra hjemmet, så større opgaver kan ligge klar til afhentning, når medarbejderen næste gang er i virksomheden – eller hvis der skal printes for andre medarbejdere, som befinder sig i virksomheden allerede.

8.4 Opsummering

Netværksdesignet opfylder de krav, som er samlet i afsnit 6.7 og er modstandsdygtigt overfor de angreb, som er beskrevet i kapitel 3 samt Appendiks A, men det kan ikke nødvendigvis antages, at designet kan modstå alle andre angrebstyper. For at levere en så generel modstandsdygtighed som muligt er designet derfor opbygget af mange lag af sikkerhedsløsninger, som overlapper hinanden og til tider er redundante. Dette gøres også for at sikre netværket mod ukendte eller uafprøvede angrebstyper i så høj grad som muligt. Brugen af firewalls fra forskellige leverandører sikrer, at en sårbarhed i én type ikke alene kan kompromittere netværket, ligesom det med selve infrastrukturen forsøges at minimere risikoen for, at angribere kan udnytte sårbarheder ét sted på netværket til at angribe andre enheder.

Der benyttes en stærk autentificering af hjemmearbejdspladserne for at forhindre, at angribere kan opnå adgang til netværket via den rute, som hjemmearbejdspladserne benytter. I hjemmene benyttes et netværksdesign, som på en gang leverer et stærkt forsvar mod eksterne angreb, og som samtidig er let at bruge og giver mulighed for deling af bredbåndsforbindelsen. Således kan privat udstyr benyttes uden at udgøre en øget sikkerhedsrisiko for hjemmearbejdspladsen. Brugen af en firewall til at skille de to netværk i hjemmet betyder, at der kan gives selektiv adgang mellem dem, så fx en printer kan deles.
Ud over selve netværksstrukturen er hjemmearbejdspladsen beskyttet ved hjælp af software, som kontrolleres og opdateres fra virksomheden. Således kræves der ingen kundskaber fra brugeren, som aldrig vil blive mødt med krav om at tage stilling til sikkerhedsproblemer, antivirusopdateringer eller lignende. Brugen af en personlig firewall, som på baggrund af et avanceret regelsæt autonomt kan håndtere problemstillinger og hente opdateringer fra virksomheden, sikrer hjemmearbejdspladsen mod angreb, som eventuelt bryder igennem de øvrige sikkerhedsmekanismer. Muligheden for at distribuere angrebsinformation mellem hjemmearbejdspladserne kan være et stærkt værktøj, hvis der foretages systematiske angreb mod disse.

Det er desuden forsøgt at optimere brugeroplevelsen, så den afspejler de maskiner, som benyttes i virksomheden. Så meget af teknologien som muligt er gemt for brugeren, som alene belastes af en autentificering med OTP. I en korrekt implementering bør hjemmearbejdspladsbrugeren have adgang til alle de ressourcer, hun har i virksomheden, præsenteret på samme måde begge steder. Således er også de begrænsninger, som netværksdesignet sætter for brugerne, de samme både i hjemmene og i virksomheden.

Netværksdesignet er primært rettet mod mellemstore og store virksomheder, som kan retfærdiggøre den nødvendige investering i infrastrukturen på baggrund af et højere antal hjemmearbejdspladser. Mindre virksomheder med et lille behov for hjemmearbejdspladser kan få svært ved at etablere et fornuftigt sikkerhedsniveau, som samtidig overholder lovkravene.

9 KONKLUSION

Mulighederne for at etablere sikre hjemmearbejdspladser i Danmark er blevet undersøgt. Potentielle risici er blevet vurderet, og der er fundet mulige løsninger på de beskrevne problemstillinger. En gennemgang af en række sikkerhedsprodukter, samt de i Danmark mest relevante love, best practices og anbefalinger, har resulteret i et designforslag. Dette beskriver med baggrund i en udarbejdet sikkerhedspolitik for hjemmearbejdspladser en implementering, som sikrer hjemmearbejdspladserne mod både generelle sikkerhedsproblemer samt de beskrevne problemstillinger. Designet leverer samtidig fundamentet for en brugervenlig, fleksibel arbejdsplads i hjemmene, som både tager hensyn til medarbejdernes diversitet og holder brugervenligheden i fokus.

Designet er opbygget efter princippet om lagdelt beskyttelse, hvor mange forskellige systemer bidrager til den samlede beskyttelse, som dermed bliver mindre afhængig af enkelte enheder. Hele infrastrukturen er beskrevet, således at forbindelsen helt fra hjemmearbejdspladsen til de interne enheder, der ønskes adgang til, kan følges.
Det er oplagt, at virksomheden integrerer de dele af designet, som er relevante, i deres eksisterende netværk. Dette er forsøgt afhjulpet ved at modulopbygge designet.
Det skal dog i denne forbindelse understreges, at ethvert netværk har specielle behov, krav og muligheder. Som en netværksarkitekt udtaler:

"Clearly, network design is not an exact science. Choices must always be made depending on the specific requirements facing the designer. [...]" [49]

Det er derfor også klart, at det udarbejdede design skal ses mere som en række retningslinier end en specifik løsning.

Det er fundet, at CyberCity som den eneste danske teleudbyder kan levere en løsning, der kan benyttes som erstatning for en stor del af implementeringen i hjemmet. Således kan virksomheden vælge at outsource installationen i hjemmet, og stadig være tro mod de primære designparametre.

Problematikken med sikring af hjemmearbejdspladserne er således gennemgået i projektet, og der er fundet en løsning, som i så generelle vendinger som muligt formulerer et designforslag. Dette kan benyttes af danske virksomheder og overholder gældende lovgivning, holder sig til de best practices og anbefalinger som relevante organisationer har og løser de sikkerhedsproblemer, der er udvalgt i rapporten.

Det har været utroligt spændende at arbejde med datasikkerhed på denne måde. Som tidligere netværksadministrator forsøgte jeg ved projektets begyndelse at udfærdige et netværksdesign for sikring af hjemmearbejdspladser for at kunne sammenligne med det, jeg ved projektets slutning er endt op med. Disse to design har vist sig at være fundamentalt forskellige, og jeg må indrømme, at der har været store mængder ny information, som har ændret mit billede af, hvordan et godt netværksdesign til hjemmearbejdspladser bør udfærdiges. Jeg håber, at også andre administratorer kan få glæde af dette arbejde, og at der vil blive arbejdet videre med projektet via nogle af de idéer, der er nævnt i perspektiveringsafsnittet nedenfor.

10 PERSPEKTIVERING

Projektets resultater kan danne grundlag for en dansk virksomheds overvejelser i forbindelse med hjemmearbejdspladser. Da rapporten er fokuseret på de tekniske aspekter og dermed komplimenterer mere administrative dokumenter som rapporten fra Ministeriet for Videnskab, Teknologi og Udvikling [82], ville det være en oplagt mulighed at omskrive rapporten til et hæfte, som gennemgår de vigtigste punkter. Hæftet kan dermed bruges af administratorer og andet teknisk personale, når et netværksdesign for hjemmearbejdspladser skal implementeres.

Der er desuden mange mulighed for at udvide projektet. Det kunne være relevant at se på, om brugen af Voice over IP (VoIP) telefoni kunne integreres i en samlet hjemmearbejdspladsløsning. Således kan virksomheden benytte bredbåndsforbindelserne i hjemmet til også at levere telefoni til de medarbejdere, som arbejder hjemme. Ud over de økonomiske fordele, kan dette give mulighed for, at medarbejderens telefon i virksomheden automatisk stilles om til hjemmet, så snart VPN-forbindelsen fra hjemmearbejdspladsen etableres. VoIP-løsningen giver desuden en mulighed for at validere brugerens identitet under telefonsamtaler, hvilket kan hjælpe til at modvirke nogle social engineering angreb.
Projektet kunne desuden udvides til at inkludere mobile enheder, som ikke er berørt i denne rapport. Mobile enheder kan være alt fra mobiltelefoner og håndholdte computere til bærbare PC'er, som tilsluttes netværk udenfor hjem og virksomhed.

Ønsker andre at arbejde videre med det nuværende projekt, kan det være en mulighed at implementere det design, som er beskrevet i kapitel 7. Baseret på et samarbejde med fx Cisco, kunne det være spændende at opbygge netværket for at undersøge, om de i rapporten beskrevne løsninger og teknologier fungerer efter hensigten. Det ville herefter desuden være interessant at udføre en række angreb mod dette system. Både for at teste systemets modstandsdygtighed overfor disse, men også for at få et billede af i hvor høj grad IDS'er, logning og analyseværktøjer kan levere brugbare oplysninger, som kan føre til detektion og afbrydelse af angrebene.
I denne forbindelse kunne det være interessant at se på, hvordan brugen af IPSec internt i netværket vil have indflydelse på ydelsen, ligesom der kunne udarbejdes løsninger til problemet med NIDS'er i kombination med krypteret trafik.

Honeynettet og honeypot'en som benyttes i designet kan være et helt studium i sig selv. På DTU ville det være spændende at implementere et honeynet og udvikle nye eller modificere eksisterende værktøjer til at benytte de oplysninger, som indhentes, samt integrere dette i DTU's Cisco-baserede netværksstruktur. Således kunne angreb på honeynettet føre til karantæne fra DTU-nettet i en periode, og efterfølgende angreb føre til politianmeldelse eller retsforfølgelse. I de to sidstnævnte tilfælde kan projektet kombineres med projekter, hvis formål er at identificere angribere.

Der er to øvrige tiltag, som hver især kan bidrage til udviklingen af bedre, sikre hjemmearbejdspladser. Det ene er udarbejdelsen af et katalog over designforslag baseret på forskellige virksomhedstyper, krav og økonomi. Et sådant katalog kan udgives af en offentlig organisation som hjælp til administratorer, der står overfor opgaven at etablere sikre hjemmearbejdspladser.
Det andet er udarbejdelsen af en bedre metode til at udvælge designkomponenter samt sikre kompatibilitet imellem dem. Dette er gennemgået i flere detaljer i afsnittet nedenfor.

10.1 Metodeudvikling

På baggrund af den metode, som i afsnit 6.7.1 er gennemgået og som skal sikre kompatibilitet mellem produkterne, udarbejdes i dette afsnit et forslag til, hvordan en model til udvælgelse af produkter til sikring af hjemmearbejdspladser kan udarbejdes.
Baggrunden for en sådan model er at udvide brugerens viden med en bred vifte af eksperters vurderinger, erfaringer og gennemtestede opstillinger. Idet hver opsætning er unik (i hvert fald så længe den skal integreres i et nuværende system), er det ikke nok at udarbejde et katalog over designforslag, selvom dette som nævnt ovenfor vil være en stor hjælp.
Ideen er derfor at opbygge et system, som på baggrund af information om det eksisterende udstyr, ønsker til funktionalitet og sikkerhed samt andre relevante specifikationer kan udarbejde et skræddersyet designforslag, som med baggrund i udstyrsspecifikationer, ekspertviden og bred erfaring kan hjælpe brugeren til at udarbejde et konkret designforslag til sikring af hjemmearbejdspladser.

10.1.1 Ekspertsystem

Et ekspertsystem er et computerprogram, som emulerer menneskelig ekspertise i veldefinerede problemstillinger. Typisk programmeres sådanne programmer i specielle programmeringssprog, som er designet til formålet. Et

eksempel er CLIPS (C Language Integrated Production Systems) som er udviklet af NASA[82]. Et sådant program er bygget op omkring regler (if, then) og et system til at matche mønstre med facts.
Ekspertsystemer benyttes til at løse virkelige problemer, som normalt ville kræve en menneskelig ekspert. Derfor kræves først og fremmest, at systemet fodres med den viden, som de menneskelige eksperter, det skal erstatte, besidder. Dette er dog ikke trivielt, da eksperternes viden ofte er i form af tommelfingerregler og ikke absolutte værdier. Specialister indenfor ekspertsystemer benyttes til at udtrække disse informationer på en måde, som kan lagres i en vidensdatabase. Dette er ikke en simpel proces og er ofte den største udfordring ved udviklingen af et ekspertsystem.
Oftest benyttes regler for repræsentationen af viden i et ekspertsystem. Sådanne regler vil ikke have bestemte konklusioner, men være baseret på grader af sikkerhed for, at konklusionen vil holde hvis betingelserne holder. Statisiske metoder benyttes til at evaluere disse grader af sikkerhed.
Ekspertsystemer har før været brugt til at hjælpe i udviklingen af komplekse netværksdesign [94], men der eksisterer – så vidt det har været muligt at undersøge – ikke noget system specifikt til udarbejdelsen af sikre netværksdesign[83].

Database
Udviklingen af ekspertsystemer kan være meget omfangsrig og vil indebære, at eksperters viden skal indarbejdes i systemet, ligesom en erfaring med eksisterende design skal indbygges. Der er en stor mængde arbejde forbundet med at indsamle disse data, og hvis ressourcerne er knappe kan disse data benyttes uafhængigt af udviklingen af selve ekspertsystemet (eller evt. sideløbende med dette).
Ideen er at opbygge en database med eksisterende løsninger samt specifikationer på relevant udstyr. Således kunne eksisterende netværksdesign ændres fra de lagrede standarder til modificerede versioner, som bedre passer til det aktuelle netværk. Ved at foretage manuelle ændringer til designet, kunne der på baggrund af databasens oplysninger om udstyrsspecifikationer etableres en liste over alternativer, som i den givne situation kunne benyttes. Der kunne laves integritetsanalyser af det modificerede netværk for at sikre, at de relevante datastrømme var intakte. Dette svarer lidt til at have et katalog over designforslag til forskellige situationer, men med statistisk hjælp til at foretage ændringer.
Indsamlingen af relevante specifikationer for produkterne samt beslutning om, hvilke informationer omkring designforslagene der skulle lagres – og hvordan – vil dog kræve nøje overvejelse.

Lagring og vægtning af erfaringer
Et system, som på den ene eller anden måde er baseret på erfaringer, er sårbar overfor den vægtning, som disse erfaringer gives. For at indsamle en stor mængde erfaring omkring forskellige netværksdesign kunne man forestille sig et internet-baseret værktøj, som opfordrer eksperter til at indtaste oplysninger om de design, de har implementeret. På denne måde kan en bred gruppe af netværkseksperter nås, og da der er tale om implementerede design er validiteten af disse garanteret.
Et sådant system vil dog være meget sårbart overfor personer, som ønsker at ødelægge systemet. Ved at indsætte falske netværksdesign i systemet, kan enkeltpersoner få systemet til at basere beslutninger på falsk grundlag (ekspertsystem) eller vise invalide design til brugeren (database).
En løsning på dette problem kunne være, at eksperterne optjener point efter, hvor mange brugere der bekræfter validiteten af deres design eller hvor mange andre eksperter, som enten bekræfter designet eller personen. Således kan respekterede eksperter fremlægge revolutionerende design som tillægges en høj tillidsværdi mens eksperter, som fremlægger deres første design ligger lavt på tillidsskalaen. Hvis en ekspert med høj tillidsværdi betegner et system med lav tillidsværdi som utroværdig vil dette system blive fjernet fra databasen. Hvis eksperten med høj tillidsværdi modsat bekræfter designet vil både designet og eksperten som har gjort det tilgængeligt optjene tillidspoint. På denne måde distribueres byrden med at validere design, og i tvivlstilfælde kan systemet vælge det design, som har den højeste tillidsværdi.

Udvælgelse
Når ekspertsystemet skal foretage en udvælgelse af design og udstyr vil det være påkrævet, at beslutningsprocessen kan gennemses af brugeren. Således skal systemet kunne fremvise hvilke beslutninger, der ligger til grund for valget samt på hvilken baggrund disse beslutninger er taget. Opstår der tvivlsspørgsmål under beslutningsprocessen, kan systemet spørge brugeren til råds og eventuelt vise de alternativer, der skal vælges imellem.
Denne gennemsigtighed i beslutningsprocessen er væsentlig, idet de færreste virksomheder vil basere en million-kroners investering på en beslutning, som ikke kan forklares. Samtidig vil den efterfølgende fysiske implementering af systemet være langt lettere, hvis de involverede parter forstår baggrunden for designet.

Brugergrænseflade
Brugergrænsefladen, som præsenterer ekspertsystemet eller databasen til brugeren og til eksperterne, kræver omhyggelig overvejelse, idet dette både vil danne grundlaget for in- og output til og fra systemet. De rigtige spørgsmål skal stilles, og den rigtige formulering af svarene skal lagres. Modsat skal de korrekte data vises til brugeren på baggrund af præcise spørgsmål om ønsker til designet.

[82] Programmeringssproget CLIPS kan findes på adressen http://www.ghg.net/clips/CLIPS.html
[83] Der er i afsnittet brugt information fra [93].

Alene afgørelsen af hvilke oplysninger, der skal indsamles om udstyr, er et helt studium i sig selv. Et eksempel kan være tilfældet, hvor afstanden mellem to stykker udstyr i designet er mere end 150 meter. Her bør systemet vide, at der enten skal benyttes en repeater eller optiske forbindelser idet almindelige netværkskabler ikke kan levere stabile forbindelser over denne afstand. Samtidig bør systemet have data til at behandle dette problem og således afgøre, om netværksenhederne kan opgraderes med fibermoduler, samt hvordan disse i så fald vil have indflydelse på det resterende system.

Opsummering

Udarbejdelsen af et ekspertsystem eller databasesystem som hjælp ved etableringen af sikre hjemmearbejdspladser er omfangsrig, men spændende. Der er store perspektiver i et sådant system – både kommercielle, men også faglige. Brugen af internettet kan hjælpe til at etablere et bredt spektrum af eksperterfaringer, men stiller samtidig krav om validering af disse. Muligheden for at kombinere dataopsamlingen med en database som sideløbende med udviklingen af ekspertsystemet kan benyttes er fra et kommercielt synspunkt fornuftig, idet en muligvis flerårig udvikling dermed ikke skal afsluttes før en eventuel indtjening kan påbegyndes.

Ideelt set burde systemet holdes fri fra kommercielle interesser, således at et design ikke alene blev baseret på fx Nokia-produkter pga. sponsorering fra producenten. Omvendt kan systemet sælges til hver enkelt producent, som kan tilbyde brugen af systemet som en service til kunder.

Under alle omstændigheder ville udviklingen af et sådant system hjælpe til at løse det primære problem ved designet af netværk – afhængigheden af netværksdesignerens egen ekspertise.

APPENDIKS A

I dette appendiks er vist angrebstyper, som retter sig mod data link laget og applikationslaget, samt DDoS-angreb og netværksrekognoscering. Disse angrebstyper kræver en vis indsigt i de benyttede teknologier og udstyr, og der henvises til ordbogen, hvor mange af udtrykkene er forklaret.

Angreb på data link laget

Angreb på lag 2 er specielt farlige, da disse ofte ikke overvåges af IDS'er. Dette skyldes, at et IDS normalt analyserer data på applikationslaget. Angreb på lag 2 vil ofte være angreb, som er rettet mod switche. I denne sammenhæng dækker ordet switch over hvad der reelt er en bridge med mange interfaces (porte). Routere, som ellers opererer på lag 3, som også går under betegnelsen switche, vil ofte være en kombineret lag 2 og 3 enhed. Sådanne enheder er derfor også sårbare over for de nedenstående angreb.
Ifølge Cisco [34] er de mest udbredte angrebstyper følgende:

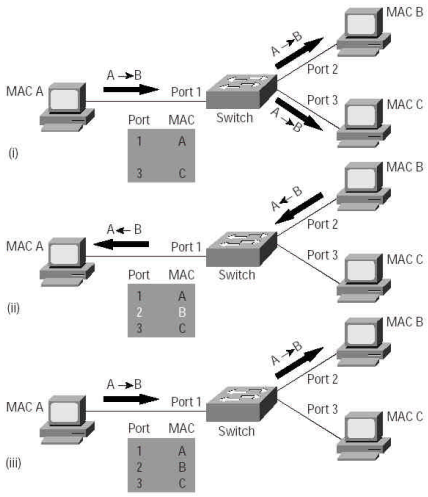
- CAM table overflow
- VLAN hopping
- Spanning-Tree protokolmanipulering
- MAC og ARP spoofing
- DHCP "udsultning"

Dertil kommer sårbarheder med brugen af PVLANs, men dette er gennemgået i afsnittet om VLANs i afsnit 5.2. De nævnte angrebstyper er kort gennemgået nedenfor sammen med mulige beskyttelsesmetoder.

CAM table overflow

Angrebseksempel

CAM-tabellen i en switch indeholder informationer omkring hvilke MAC-adresser der er forbundet til hver port (samt eventuelt tilhørende VLAN-parametre). Når en frame modtages, slås MAC-adressen op i CAM-tabellen for at se, om der findes information om, hvilken port MAC-adressen tilhører. Hvis ikke dette er tilfældet, sendes den pågældende frame ud på alle porte. Modtages der svar fra en af portene, opdateres CAM-tabellen med information om, at den pågældende MAC-adresse findes på denne port. Dette princip kan ses på figur 53, hvor maskinen A sender en frame til B. Da B ikke kendes af switchen kopieres den sendte frame ud på alle porte. Herefter svarer B og CAM-tabellen opdateres.
CAM-tabeller er begrænset til en vis størrelse. Hvis tabellen fyldes op, kan der ikke tilføjes yderligere adresser. Normalt vil eksisterende adresser blive slettet efter en forudbestemt periode, men sender en angriber en stor mængde frames til switchen med ugyldige afsender-MAC-adresser, kan tabllen fyldes op hurtigt. Til sidst vil CAM-tabellen kun indeholde ugyldige MAC-adresser, hvorefter switchen vil være ude af stand til at afgøre, hvilke porte de gyldige MAC-adresser tilhører. Switchen vil herefter fungere delvist som en hub, idet alle frames vil blive kopieret til alle porte indenfor samme broadcastdomæne. Angriberen kan nu fra sin maskine overvåge al den trafik, som sendes gennem denne del af switchen med fx en pakkesniffer. Der er dog en formildende faktor, idet kun trafik indenfor samme lokale VLAN vil blive sendt ud. Således kan dette angreb til dels sammenlignes med angrebet fra afsnit 3.1, hvor en router kunne tvinges til at udsende data til angriberen. I dette tilfælde er der dog tale om en switch, som typisk vil blive benyttet internt på lokalnettet, ligesom der her udsendes data til alle tilknyttede porte og ikke blot til angriberens maskine.



Figur 53 - CAM table [34]

CAM table overflow-angrebsproblemet kan blive forværret når hjemmearbejdspladser tilføjes til netværket. Idet disse ligeledes vil kobles til switche og routere på virksomhedens netværk, kan de nævnte angreb udføres fra eksterne lokationer. Samtidig kan det i visse opsætninger være svært at analysere trafikken fra hjemmearbejdspladserne hvis udstyret, som foretager denne analysering, er placeret før eventuelle krypterede forbindelser fra hjemmene termineres.

For at undgå denne type angreb, bør der sættes grænser for hvor mange forskellige MAC-adresser, der kan tillades fra hver port. Benyttes hver port kun af en arbejdsstation, kan grænsen fx sættes til tre tilladte adresser. Således kan brugeren benytte en bærbar PC samt skifte arbejdsstationen ud flere gange, uden at en netværksadministrator skal involveres.
Det er også muligt at specificere netop den MAC-adresse, som må benytte hver port. Dette skalerer dog dårligt, da en netværksadministrator skal involveres ved hvert enkelt skift af arbejdsstation, bærbar PC eller andet udstyr.

Såkaldte smarte CAM-tabeller kan i nyere udstyr også benyttes til at undgå angrebene. Disse tabeller tillader ikke at eksisterende poster i tabellen kan overskrives, ligesom kun inaktive poster kan udløbe. På denne måder vil aktive enheder på netværket aldrig forsvinde fra CAM-tabellen.

VLAN hopping

Angrebseksempel

Denne type angreb har til formål at omgå de VLAN-restriktioner, der kan være implementeret (se evt. afsnit 5.2). Der findes to typer af dette angreb – Switch Spoofing og Double Tagging.
Switch spoofing er et forsøg på at få den pågældende switch til at tro, at den arbejdsstation, angriberen benytter er en anden switch. Switche benytter specielt konfigurerede porte til at tale sammen, hvor alt data fra den første switch videresendes til de næste. Disse porte kaldes trunkporte. For at få en switch til at tro, at en arbejdsstation er en switch, kan angriberen udsende bestemte signaler (Inter-Switch Link eller 802.1q signaler samt Dynamic Trunk Port (DTP) signaler). Switchen vil i visse tilfælde tro, at en anden switch's trunkport forsøger at kontakte den, da denne type trafik er unik for disse porte. Da trunkporte som nævnt normalt benyttes til at videresende al trafik fra en switch til en anden, vil arbejdsstationen automatisk blive medlem af alle VLANs og dermed omgå de VLAN-restriktioner, som kunne være implementeret.
Double tagging er en anden teknik til at omgås VLAN-restriktioner. Problemet opstår, når to eller flere switche benyttes til at dække det samme VLAN. For at videresende oplysninger om hvilke VLANs trafikken mellem switchene stammer fra, tilføjes en mærkat (tag) til hver ethernet frame, som indikerer VLAN ID-nummeret. Denne mærkat tilføjes, når framen sendes fra den første switch og læses når framen modtages af den anden switch. Den port, som forbinder den første switch til den anden switch (trunkporten), er også tildelt et VLAN ID-nummer. Hvis dette ID-nummer er det samme, som benyttes af den port, som angriberen benytter, kan han udnytte en svaghed i den måde mærkaterne tilføjes og fjernes på.
Målet for angrebet er at sende trafik fra et VLAN ID til et andet – dvs. forsøge at omgå den funktion, som VLANs har. Angrebet udføres ved at angriberen udformer en frame, som indeholder mærkatet for det VLAN ID, som modtageren af framen benytter – fx VLAN 2. Herefter sendes framen til den første switch. Denne switch ved, at modtageren af framen befinder sig på en anden switch og tildeler derfor pakken en mærkat med information om, at framen er kommet fra en port med VLAN ID 1 (afsenderens VLAN ID). Framen indeholder nu to mærkater – den inderste har VLAN ID 2 og den yderste har VLAN ID 1.
Da den første switch' trunkport også har VLAN ID 1 fjernes mærkaten, når denne sendes ud af trunkporten. Dette skyldes, at switchene som udgangspunkt antager, at hvis ikke en frame, som kommer via trunkporten har en mærkat tilføjet, tilhører denne frame samme VLAN som trunkporten selv – dvs. VLAN 1 i dette tilfælde. I princippet burde framen således ikke have nogen mærkater tilføjet når den ankommer til den anden switch. Men da angriberen selv har tilføjet en mærkat – og den første switch har fjernet den yderste mærkat – ser den anden switch nu en frame med en mærkat som indikerer, at framen kommer fra en port med VLAN ID 2. Da destinationsadressen også tilhører VLAN 2 sendes framen til modtageren. Således er en frame kommet fra VLAN 1 til VLAN 2.

Angrebet kræver som nævnt, at der er to switche mellem afsender og modtager, samt at trunkporten er sat til samme VLAN-ID som den port, angriberens arbejdsstation er tilknyttet.

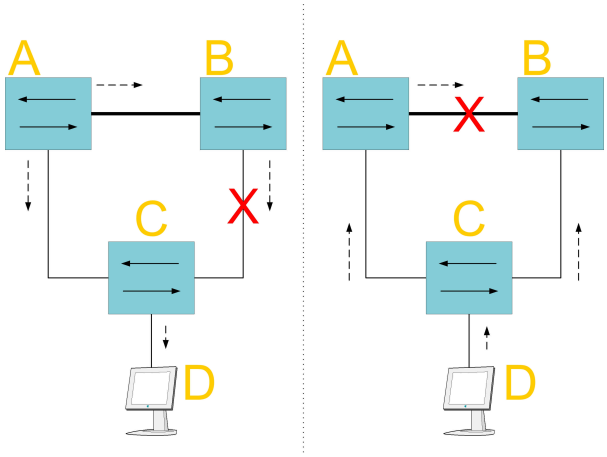
For at sikre sig mod disse typer angreb, kræves der en konfigurationsændringer af de pågældende switche. Alle porte, som ikke skal benyttes som trunkporte, bør eksplicit have muligheden for at sende DTP signaler slået fra. Samtidig bør der bruges unikke VLAN ID numre for alle trunkporte, som er i brug. Det er desuden en god ide at slå alle ubrugte porte fra samt samle disse i et ubrugt VLAN, således at angribere ikke kan forsøge at finde frem til en ubrugt port, som kunne tilhøre et andet VLAN.
Ligesom med CAM overflow-angrebet forværres situationen når hjemmearbejdspladser tilføjes, idet disse ofte også vil være tilknyttet VLANs. Hjemmearbejdspladsens forbindelse bør i visse tilfælde groft sagt betragtes som et netværksstik på ydermuren af virksomhedens bygning. Der bør derfor gøres en ekstra indsats for at sikre, at tilgangen til dette netværksstik ikke udgør en risiko for virksomhedens IT-sikkerhed.

Spanning-Tree protokolmanipulering

Angrebseksempel

Spanning-Tree protokollen (STP) benyttes af switche til at sikre, at der ikke opstår bridge-loops, dvs. hvor trafikken sendes rundt i et uendeligt loop mellem sammenkoblede switche. Protokollen fungerer ved, at switchene under opstart identificerer øvrige switche og tildeler en af dem rollen som root bridge, hvorefter adgangen til de øvrige redundante switche blokeres. Denne kommunikation mellem switchene benytter Bridge Protocol Data Units (BPDU). Når en bridge er valgt som root bridge, får den et ID-nummer, som er lavere end de andre. Skulle denne switch blive utilgængelig, vil den switch med det næst-laveste nummer blive den nye root bridge osv.

Konceptet er forsøgt illustreret på figur 54. Her ses tre switche. A er root for det pågældende VLAN, mens B er backup root for samme VLAN. A og B er forbundet med fx en Gbit fiberforbindelse. Switch C er en switch, som leverer netværksadgang til enheder på netværket og er således ikke en del af backbonen. Forbindelserne mellem A og C samt B og C vil typisk være på 100Mbit. De stiplede pile indikerer den retning, BPDU sendes. I venstre side af figuren ses hvordan C's port, som forbinder denne til switch B, er blokeret for at undgå loops. Valget til root bridge er således faldet på A. På højre side af figuren begynder en af de arbejdsstationer, som er tilsluttet C, uautoriseret at deltage i STP (dette kan fx gøres ved at installere en Linux-baseret bridge-applikation på en PC). I softwaren sættes prioriteten af denne bridge til en værdi, som er lavere end den nuværende root bridge's prioritering. Da den switch med lavest prioritet vælges som root bridge, vil arbejdsstationen overtage rollen som root bridge for det pågældende VLAN. Gbit-forbindelsen mellem A og B vil derfor blive blokeret, idet den nye foretrukne vej mellem A og B nu er via C (og D).



Figur 54 - Spanning-Tree angreb

Der er to muligheder for, hvordan angriberen kan udnytte den nuværende situation. Enten skal der – som det ses på figuren – benyttes en switch (C) som har forbindelse til begge backbone-switchene (A og B), eller også skal angriberens PC være udstyret med to netkort, som er forbundet til hver sin switch. I det første tilfælde kan angriberen kombinere angrebet med et CAM-tabel-angreb på switch C, således at alle pakker også ender hos angriberen. I det sidste tilfælde vil alle pakker passere angriberens arbejdsstation direkte.

Benyttes bestemte typer switche (bl.a. visse Cisco-switche), kan der etableres en sikring af portene så porte, der benyttes af arbejdsstationer, ikke kan udsende BPDU-signaler. Dette sker ved, at disse porte blokeres, hvis sådanne signaler detekteres. Alternativt (eller samtidig) kan funktionen "Root Guard" benyttes til at sikre at porte, hvor arbejdsstationer er tilsluttet, ikke kan opnå root bridge status. Hvis ikke netværket har en topologi, som kan give anledning til loops, bør STP slås fra, hvorved problemet kan undgås helt.
Hjemmearbejdspladser kan typisk også benyttes til denne type angreb. Dog vil mængden af data som i så fald skal flyttes igennem forbindelsen til hjemmet formentligt være for stor til den båndbredde, hjemmearbejdspladsen er udstyret med. Angreb af denne type foretaget fra hjemmearbejdspladsen vil derfor formentligt medføre en form for DoS-tilstand, idet trafikken mellem arbejdsstationer tilkoblet de pågældende switche vil være ude af stand til at overføre data, hvis denne skal gå gennem forbindelsen til hjemmearbejdspladsen. Alternativt kan angrebet sammensættes med et sekundært angreb, som muliggør en filtrering af den trafik, som sendes til hjemmearbejdspladsen.

MAC og ARP Spoofingangreb

Angrebseksempel

Hvis angriberen kender MAC-adressen på en anden enhed på netværket, kan det forsøges at få en switch til at videresende frames, som oprindeligt var tiltænkt denne enhed til angriberens arbejdsstation. Dette kan foregå på to måder. Den første lægger sig tæt på af problemet med CAM-tabeller. Ved at sende en enkelt frame med den fremmede enheds MAC-adresse som afsenderadresse, vil CAM-tabellen i switchen overskrive den eksisterende post så switchen fremover tror, at arbejdsstationen med den pågældende MAC-adresse er at finde på angriberens port. Dermed videresendes pakker til denne MAC-adresse til den port, hvor angriberen er tilsluttet. Dette kan fortsætte indtil den fremmede enhed selv udsender en frame, hvorefter CAM-tabellen igen opdateres og dermed vender tilbage til den oprindelige port.
Alternativt kan ARP (Address Resolution Protocol) benyttes til at opnå samme effekt. ARP benyttes normalt til at fastslå MAC-adressen for en enhed baseret på IP-adressen. Således sender en enhed, som kender modtagerens IP-nummer men ikke MAC-adressen, en ARP-forespørgsel som "Hvem har IP-adressen 192.168.0.45 ?". Svaret kommer fra den enhed som har IP-nummeret 192.168.0.45 i form af en ARP pakke som fx fortæller, at IP-adressen 192.168.0.45 tilsvarer MAC-adressen 00-50-04-64-4D-02. Denne information gemmes i en ARP cache hos den enhed, som foretog forespørgslen. Men den switch som har forbundet de to enheder gemmer også denne oplysning sammen med information om på hvilken port, den modtog ARP-svaret. Dette er meget lig MAC-angrebet ovenfor, idet en enkelt frame (eller i dette tilfælde en ARP-pakke) fra en port opdaterer CAM-tabellen.
Ved at konstruere falske ARP-svar med MAC-adresser fra andre enheder kan switchen således lokkes til at opdatere sin CAM-tabel med forkerte MAC-adresser. Dvs. i stedet for at sende spørgsmålet "Hvem har IP-adressen 192.168.0.45?" ud, sender angriberen svaret (selvom spørgsmålet aldrig er blevet stillet). Da switchen ikke checker, om der er tale om svar på en forespørgsel, men blot observerer, at en enhed har svaret, at den har MAC-adressen 00-50-04-64-4D-02, opdateres CAM-tabllen med oplysning om, at MAC-adressen 00-50-04-64-4D-02 fremover er at finde på den pågældende port. På denne måde kan angriberen modtage trafik, som oprindeligt var tiltænkt den fremmede enhed. I en mere kompleks situation kan ARP-svaret konstrueres som et svar på en reel forespørgsel fra

en tredje enhed. Denne enhed vil dermed cache svaret og ikke længere foretage forespørgslen. Dette kræver dog at den enhed, hvis trafik ønskes kopieret, foretager denne forespørgsel. Men da cachen udløber med tiden, vil en sådan forespørgsel under alle omstændigheder forekomme med jævne mellemrum.

Forsvaret mod sådanne spoofingangreb kan være at definere en MAC-adresse til hver port og fastlåse denne indstilling. Dette skalerer dog som tidligere nævnt meget dårligt. Alternativt kan alle arbejdsstationer på netværket blive installeret med statiske ARP cacher. Dette skalerer dog endnu dårligere end ovenstående alternativ.
En sidste metoder er at benytte PVLANs (se afsnit 5.2) hvilket til en vis grad vil sikre, at kun enheder indenfor samme PVLAN kan tale sammen. Under alle omstændigheder er der tale om et problem, som ikke umiddelbart er let at løse, men som dog kræver, at angriberen kan benytte en netværksport på virksomhedens interne netværk. Det er dog netop her hjemmearbejdspladserne er interessante for angribere, idet de som før nævnt i princippet repræsenterer interne netværksporte udenfor netværket.

DHCP ”udsultning”

Angrebseksempel

DHCP (Dynamic Host Configuration Protocol) er en protokol, som benyttes til at uddele IP-adresser til arbejdsstationer på et netværk. Normalt vil en netværksenhed sende en DHCP-forespørgsel og afvente et svar, som indeholder både en IP-adresse samt information om netværksspecifikke oplysninger som fx hvilken gateway og DNS-server, der skal benyttes. DHCP-serveren uddeler IP-adresserne fra en pulje, som administratorerne har stillet til rådighed. Hver gang en arbejdsstation kobles på netværket, tildeles den en IP-adresse fra puljen. Hvis ikke adressen bliver brugt i længere tid, bliver adressen lagt tilbage i puljen og kan benyttes af en anden arbejdsstation på et senere tidspunkt.
DHCP “udsultning” foregår ved at udsende DHCP-forespørgsler med forfalskede MAC-adresser. Hvis der udsendes nok af disse forespørgsler vil de tilgængelige adresser blive udtømt i et givent tidsrum (indtil disse adressers løbetid udløber). Ud over at dette forhindrer, at legitime brugere kan få tildelt en IP-adresse, giver det også angriberen mulighed for at etablere en uautoriseret DHCP-server. Dette kan være interessant, idet der i DHCP-svaret ud over IP-adressen som nævnt også sendes information til klienterne om, hvilken gateway og DNS-server der skal benyttes. Således kan angriberen angive sin egen arbejdsstation som gateway og dermed modtage al udgående trafik fra klienterne, idet udgående trafik bliver dirigeret igennem gateway’en.
I mange netværk er det endog ikke engang nødvendigt at udføre DHCP udsultning før en uautoriseret DHCP-server kan introduceres på netværket. Idet klienterne mere eller mindre tilfældigt udvælger, hvilken DHCP-server der skal benyttes, kan angriberens DHCP-server vælges af klienterne selvom den officielle DHCP-server stadig er operativ [39].

Samme metode som ved overflow af CAM-tabellen kan benyttes til at beskytte mod DHCP udsultning – dvs. begrænse antallet af MAC-adresser, der kan benyttes per port. Der findes desuden implementeringer, hvor der kræves autentificering af DHCP beskeder hvilket kan beskytte mod opsætningen af alternative DHCP-servere [40].
I mange tilfælde modtager VPN-klienter også IP-numre via DHCP. I sådanne tilfælde kan også trafik fra hjemmearbejdspladserne udsættes for angrebet. Samtidig kan der – hvis der fra virksomhedens netværk er adgang til hjemmearbejdspladserne – opsættes DHCP-servere i hjemmene, som kan benyttes til at ”servicere” dele af virksomhedens arbejdsstationer.
Brugen af VLANs kan også modvirke problemet, idet broadcast-forespørgsler efter en DHCP-server dermed forbliver indenfor samme VLAN.

Opsummering

Alle disse angrebstyper har til formål at få uautoriseret adgang til Ethernetframes. Med henblik på hjemmearbejdspladser kan det derfor være væsentligt at overveje, hvordan trafikken håndteres på tværs af virksomhedens opkoblingspunkter samt internt i virksomheden. Med mindre der tages de nødvendige skridt i retning af at modvirke sådanne angreb på data link laget, må virksomheden antage, at alle frames kan ses af alle og handle derefter. Dette kan have meget store konsekvenser for designet af netværksstrukturen. Et interessant aspekt er situationen, hvor hjemmearbejdspladsen benyttes som bagdør til virksomhedens netværk hvorfra infrastrukturen modificeres på lag 2 til at dirigere bestemte data ud af netværket tilbage til hjemmearbejdspladsen. I en sådan situation kan et netværk baseret på switche, VLANs og massiv beskyttelse af internetforbindelserne stadig få stjålet data, som transmitteres mellem to interne arbejdsstationer[84].

Angreb på applikationslaget

En af de mest almindelige metoder for denne type angreb er at udnytte kendte sikkerhedshuller i den software, som ofte afvikles på servere. Dette kan være applikationer som HTTP og FTP. Problemet eskalerer i forbindelse med hjemmearbejdspladser, idet det her ofte er nødvendigt at åbne for yderligere adgang til virksomhedens netværk. Der

[84] Der er i afsnittet brugt information fra [36], [37] og [38]

kan derfor være tale om at åbne for e-mail (POP3, IMAP), fjernstyring af maskiner (VNC, X m.fl.) eller tillade VPN-adgang til netværket.
Specielt servere er sårbare overfor denne type angreb. Det skyldes både at disse er de mest synlige for angribere, men også fordi de ofte er sammensat af mange forskellige applikationer. En webserver kan fx være baseret på en hardwareplatform fra en leverandør, et netkort fra en anden, et operativsystem fra en tredje og en webserver fra en fjerde. Samtidig kan webserveren afvikle yderligere applikationer og kommunikerer måske med en databaseserver, som igen kan bestå af en tilsvarende mængde forskellige systemer. Kompleksiteten kan derfor være stor, når eventuelle sårbarheder skal analyseres. Sårbarhederne kan i værste tilfælde ende med at give angriberen administrative rettigheder over systemet, men vil i de fleste tilfælde "blot" give normale brugerrettigheder. Der kan herefter installeres et såkaldt "rootkit" som fx Adore[85] der kan samle brugernavne og passwords på systemet og med tiden give administrativ (root) adgang. Rootkittet benyttes også til at åbne bagdøre til netværket, som angriberen senere kan bruge samt til at sløre logfilerne og ændre systemfiler for at undgå detektion.
Det primære problem med angreb på applikationslaget er, at angrebene benytter porte, som i forvejen er godkendt i firewallen. Et angreb mod en webserver foregår på TCP port 80. Denne port vil som regel være åben, idet webserveren leverer sider til brugerne på denne port. Fra en firewalls perspektiv er der under angrebet ofte blot tale om almindelig port 80 trafik.

Denne type angreb er svære at beskytte sig helt imod. Der findes konstant nye sårbarheder som offentliggøres på Internettet. I år 2002 offentliggjorde CERT 11 nye sårbarheder om dagen. Nedenfor er nævnt nogle metoder, som kan begrænse angrebene.

- **Gennemgå logfilerne** – Følg anbefalingen "*If you're going to log it, read it*". Logfilerne fra operativsystemerne og applikationerne kan give et godt billede af, hvad der foregår på serverne. Ofte vil der være tale om så meget data, at en analysering af logfilerne bør foregå maskinelt.
- **Sårbarhedsinformation** – Ved at abonnere på de mailinglister som offentliggør sårbarhedsinformation som fx Bugtraq fra SecurityFocus kan ny viden om sårbarheder i systemerne indhentes. Det skal blot huskes, at angriberne også abonnerer på disse lister.
- **Vedligeholdelse** – Vedligeholdelse af operativsystemer og applikationer med seneste patches, service packs og andre opdateringer kan hjælpe med at lukke for sårbarhederne. I de sidste seks måneder er der fundet kritiske sårbarheder i meget udbredte applikationer som sendmail, Apache, Exchange Server og IIS. Alene for Apaches vedkommende er der tale om 21 sårbarheder.
- **Intrusion Detection Systemer (IDS)** – Der findes to IDS-teknologier som komplimenterer hinanden:
  Netværksbaseret IDS (NIDS) fungerer ved at overvåge alle pakker på et specifikt subnet. Hvis en serie af pakker, som matcher signaturen for et kendt angreb observeres, kan NIDS'en alarmere administratorerne eller terminere sessionen.
  Værtsbaseret (Host-based) IDS (HIDS) fungerer ved at placere agentprogrammer på den vært (server), som skal beskyttes. HIDS analyserer kun pakker, som er adresseret til den aktuelle server. Fordi HIDS kan designes specifikt til en applikation, kan den være mere præcis end NIDS.
  Det største problem med IDS'er er falske alarmer. Der er meget arbejde forbundet med at finindstille en IDS til et bestemt netværk eller applikation.

Netværksrekognoscering

Netværksrekognoscering referer til det at få viden om et system ud fra umiddelbar tilgængelige information. Inden en angriber forsøger at angribe et netværk, vil der ofte blive lavet adskillige forsøg på at få viden om systemet. Dette kan ske ud fra DNS-opslag, portscanninger med mere. DNS-opslagene kan give information om, hvem der ejer hvilke domæner samt hvilke andre adresser, den pågældende virksomhed råder over. Således kan DNS-opslag give en indikation af, hvilke adresser det kunne være relevant at forsøge at spoofe. Samtidig kan angriberen se, hvordan adresserne er opdelt. Således kan det give en idé om, hvilke adresser der benyttes eksternt (fx eksterne afdelinger og i visse tilfælde hjemmearbejdspladser) og hvilke, der benyttes internt (fx til offentlige servere, routere osv.).
Portscanninger kan bruges til at undersøge, hvilke maskiner netværket består af samt hvilke services disse maskiner afvikler.

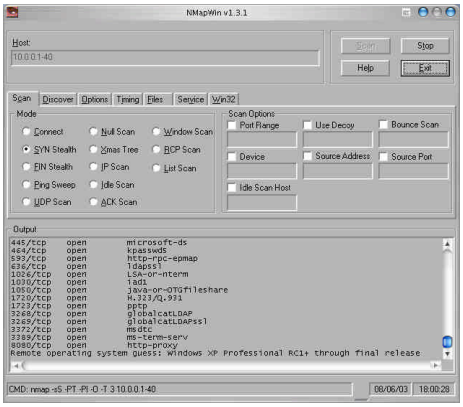
For at give et overblik over mængden af portscanninger der udføres i Danmark kan nævnes, at CERT oplyser, at der er foretaget mere end 52.000 portscanninger mod Forskningsnettet i de første tre måneder af 2003.

[85] Rootkittet Adore kan findes på adressen http://www.l0t3k.org/tools/Rootkit/

Angrebseksempel

Nedenfor er beskrevet hvordan et angreb baseret på netværksrekognoscering kan foregå.

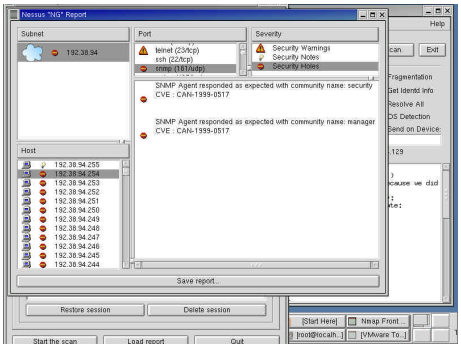
Alle virksomhedens kendte adresser scannes for åbne porte med en portscanner som fx nMap[86]. Programmet returnerer en komplet liste over åbne porte. Et eksempel på resultaterne fra nMap kan ses på figur 55.



Figur 55 - nMap portscanner

Herefter benyttes et sikkerhedsanalyseværktøj som Nessus[87] eller Internet Security Scanner[88] til at checke serverens åbne porte for kendte sårbarheder. Ofte vil analyseværktøjet desuden beskrive hvilket operativsystem enheden kører, samt hvilke applikationer, der benyttes på de åbne porte. Et uddrag af en rapport fra Nessus kan ses på figur 56.

Ud fra disse resultater benyttes sårbarhedsdatabaser som fx SecurityFocus til at få beskrivelser af de nu kendte sårbarheder for systemerne. En velkendt service som Google kan ofte returnere komplette scripts til udnyttelse af sårbarhederne. Ofte vil disse være i form af "proof of concept" scripts, som meget let kan modificeres til egentlige angrebsscripts. Et eksempel på sådanne proof of concept scripts er vist på figur 57.



Figur 56 - Nessus sårbarhedsscanner

Selv hvis en sårbarhed ikke eksisterer, kan angriberen bruge oplysningerne fra sikkerhedsanalyseværktøjet til at afgøre hvilke type enhed, der er tilknyttet en IP-adresse. Således kan der specifikt ledes efter fx routere eller i visse tilfælde hjemmearbejdspladser.

Det er ikke muligt helt at undgå denne type rekognoscering. IDS'er kan dog hjælpe til at informere administratorerne om, at et angreb er undervejs. På samme måde kan der komme mange falske alarmer, da den tilgængelige information som benyttes til rekognosceringen også kan benyttes legalt, ligesom der ofte vil være så mange portscanninger af et netværk, at alarmering for hver af dem er urealistisk. Som nævnt ovenfor, blev Forskningsnettet i løbet af tre måneder scannet 52.000 gange. Det svarer til næsten 600 scanninger om dagen. Det vil kræve enorme ressourcer at efterforske hver af disse scanninger.

Hjemmearbejdspladserne må også antages at være udsat for denne type scanninger i stort omfang. Her kan løsningen dog være mere simpel, idet der ofte kan lukkes totalt for indgående trafik. Således vil scanninger ikke give brugbar information, men det bør overvejes, hvordan scanninger internt i virksomheden (som dermed også kan nå hjemmearbejdspladserne) skal håndteres.

Figur 57 - Proof of Concept kode fra SecurityFocus[89]

DDoS angreb

DDoS (Distributed Denial of Service) er en distribueret udgave af DoS (Denial of Service) angrebstypen. Formålet med et DoS-angreb er ikke at bryde ind i det system som angribes, men at sætte det ude af stand til at behandle regulær internettrafik. Typisk kan DoS-angreb udføres ved at benytte svagheder i systemerne, som gør det muligt for en enkelt angriber at overbelaste systemet i en sådan grad, at der ikke er tilgængelige ressourcer til at behandle anden trafik.

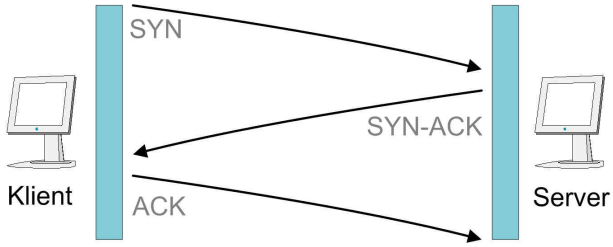
---

[86] Programmet nMap kan findes på adressen http://www.insecure.org/
[87] Programmet Nessus kan findes på adressen http://www.nessus.org/
[88] Produktet Internet Security Scanner udvikles af Internet Security Systems og kan findes på adressen http://www.iss.net/
[89] Billedet er en kollage samlet af information fra SecurityFocus som kan findes på adressen http://www.securityfocus.com/bid/6991/exploit/

DDoS-angreb udvider denne type angreb ved at lade tusindvis af maskiner angribe systemet samtidigt. Dermed kan angriberen udnytte den samlede (distribuerede) båndbredde af alle maskinerne til at overbelaste det system, som angribes. Ofte vil disse maskiner være uvidende om deres medvirken i sådanne angreb, idet de før angrebet påbegyndes er blevet inficeret med fx en trojansk hest, som gør det muligt for angriberen at benytte maskinen.

Angrebseksempel

Typisk vil angriberen benytte en svaghed i fx TCP, idet denne protokol er benyttet af stort set alle virksomheder, som leverer en service over internettet (fx en webserver, e-mail osv.). Når der etableres en TCP forbindelse sender klienten først en SYN besked til serveren. Serveren modtager denne besked og besvarer den med en SYN-ACK besked. Klienten færdiggør etableringen af forbindelsen ved at svare tilbage med en ACK besked. Herefter er forbindelsen åben og data kan udveksles mellem klienten og serveren. Denne udveksling er vist på figur 58.
Sårbarheden i dette ligger på det punkt, hvor serveren har sendt sin besvarelse (SYN-ACK) tilbage til klienten, men endnu ikke har modtaget den afsluttende ACK-besked. Dette beskrives som en halvåben forbindelse. Problemet er, at serveren nu står og afventer svaret fra klienten. En tabel i serverens datastruktur beskriver alle de halvåbne forbindelser, så den korrekte forbindelse kan etableres når ACK-beskeden ankommer. Da denne tabel har en begrænset størrelse, kan angriberen fylde tabellen op med forfalskede adresser, som derfor aldrig vil tilbagesende ACK-beskeden. Når tabellen er fyldt, kan der ikke etableres nye forbindelser, før løbetiden for de eksisterende halvåbne forbindelser løber ud.



Figur 58 - SYN og ACK udveksling

TCP SYN-angrebet er blot ét eksempel ud af mange, som kan benyttes ved DoS og DDoS-angreb.

DDoS-angreb kan udvikle sig til at være den værst tænkelige type angreb – den type, som ikke kan stoppes. Sikkerhedsmekanismer som IDS, firewalls og aktiv overvågning kan ikke altid forhindre sådan et angreb. Hvis blot et par hundrede maskiner deltager i et sådan angreb – og disse maskiner hver kan generere 100 kbit/s trafik – genereres samlet ca. 20 Mbit/s trafik. Med tusindvis af maskiner kan tallet være langt større. Resultatet er, at hele netværket er ude af stand til at svare på reelle forespørgsler – ikke blot den enkelte server. De implementerede sikkerhedssystemer kan afvise angrebsenhederne, men da trafikken på det tidspunkt allerede er nået til virksomhedens yderste forsvarssystemer, er skaden sket. For selv når trafikken blokeres, genererer den samme mængde trafik.

Forsvaret mod DDoS angreb kan kun ske via et samarbejde med internetudbyderen. Internetudbyderen kan konfigurere de centrale routere, så kun en bestemt mængde trafik af udvalgte typer bliver tilladt – og hvis udstyret er intelligent nok, kan DDoS angreb identificeres og stoppes, før det når til virksomheden. Det kan så håbes, at internetudbyderen har båndbredde nok til at modstå angrebet.
De mest udbredte former for DDoS angreb er Internet Control Message Protocol (ICMP) floods, TCP SYN floods (som beskrevet ovenfor) og User Datagram Protocol (UDP) floods. Trafik af denne type kan af internetudbyderen kategoriseres og begrænses med omtanke for, at TCP SYN pakker på port 80 har lige så stor chance for at være reelle forespørgsler for hjemmesider som angreb. Netop dette er kernen i problemet – at identificere angrebspakkerne fra reelle pakker.

IP-adresserne er opdelt, så visse af dem er private, og dermed ikke kan benyttes på internettet, men på virksomhedens lokale netværk. Idet de fleste angreb foretages med private afsenderadresser for at sikre, at der ikke kan komme svar fra enheder, som har disse adresser, kan et alternativt forsvar være at filtrere alle pakker med private IP-adresser. Disse adresser er beskrevet i RFC 1918 [18]. Hvis internetudbyderen udfører denne filtrering før trafikken føres videre mod virksomheden, kan mange DDoS angreb stoppes[90].

[90] Der er i afsnittet brugt information fra [19] side 6-7 samt fra [100].

APPENDIKS B

Nedenstående data er fra CheckPoint's Application Intelligence white paper [73]. Tabellen viser hvilke applikationslags-baserede angreb, CheckPoint's Application Intelligence System (nu en del af Firewall-1 NG produktet) kan modstå.

Application Layer/Presentation Layer

	ATTACK PREVENTION SAFEGUARDS	ATTACKS BLOCKED
HTTP Client	• Block Java code • Strip script tags • Strip applet tags • Strip FTP links • Strip port strings • Strip ActiveX tags • Camouflage default banner • URL filtering • Limit maximum URL length • Limit maximum number of response headers allowed • Limit maximum request header length • Limit maximum response header length • Prohibit binary characters in HTTP response headers • Prohibit binary characters in HTTP requests • Validate HTTP response protocol compliance • Block user-defined URLs • Enforce maximum GET and POST length	• Code Red Worm & Mutations • Nimda Worm & Mutations • HTR Overflow Worm & Mutations • Directory Traversal Attacks • MDAC Buffer Overflow & Mutations • Cross-Site Scripting Attacks • Malicious URLs • User-Defined Worms & Mutations
HTTP Server	• Limit maximum URL length • Distinguish between different HTTP v1.1 requests over same connection • Limit maximum number of response headers • Limit maximum request header length • Limit maximum response header length • Prohibit binary characters in HTTP response headers • Prohibit binary characters in HTTP requests • Block user-defined URLs • Restrict non-RFC HTTP methods • Enforce HTTP security on non-standard ports (ports other than 80) • Compare transmission to user-approved SOAP scheme/template	• Encoding Attacks • Cross-Site Scripting Attacks • HTTP-based attacks spanning multiple packets • WebDAV Attacks • User-Defined Worms & Mutations • Chunked Transfer Encoding Attacks
SMTP	• Block multiple "content-type" headers • Block multiple "encoding headers" • Camouflage default banner • Restrict unsafe SMTP commands • Header forwarding verification • Restrict unknown encoding • Restrict mail messages not containing sender/recipient domain name • Restrict MIME attachments of specified type • Strip file attachments with specified names • Strict enforcement of RFC 821 & 822 • ESMTP command monitoring	• SMTP Mail Flooding • SMTP Worm & Mutations • Extended Relay Attacks • Message/ Partial MIME Attack • SPAM Attack (large number of emails) • Command Verification Attack • SMTP Worm Payload & Mutations • Worm Encoding • Firewall Traversal Attack • SMTP Error Denial-of-Service Attack • Mailbox Denial-of-Service Attack (excessive email size) • Address Spoofing • SMTP Buffer Overflow Attacks
RSH	• Auxiliary port monitoring • Restrict reverse injection	
RTSP	• Auxiliary port monitoring	
IIOP	• Auxiliary port monitoring	

Application Layer/Presentation Layer

	ATTACK PREVENTION SAFEGUARDS	ATTACKS BLOCKED
FTP	• Analyze and restrict hazardous FTP commands • Block custom file types • Camouflage default banner • Strip FTP references	• Passive FTP Attacks • FTP Bounce Attack • Client and Server Bounce Attacks • FTP Port Injection Attacks • Directory Traversal Attack • Firewall Traversal Attack • TCP Segmentation Attack
DNS	• Restrict DNS zone transfers	• DNS Query Malformed Packet Attacks • DNS Answer Malformed Packet Attacks • DNS Query Buffer Overflow - Unknown Request/Response • Man-in-the-Middle Attack
Microsoft Networking	• CIFS filename filtering (protect against worms utilizing CIFS protocol) • Restrict remote access to registry • Restrict remote null sessions	• Bugbear Worm • Nimda Worm • Liotan Worm • Opaserv Worm
SSH	• Enforce SSH v2 protocol	• SSH v1 Buffer Overflow Attack
SNMP	• Restrict SNMP get/put commands	• SNMP Flooding Attack • Default Community Attacks • Brute Force Attacks • SNMP Put Attack
MS SQL		• SQL Resolver Buffer Overflow • SQL Slammer Worm
Oracle SQL	• Verify dynamic port allocation and initiation	• SQLNet v2 Man-in-the-Middle Attack
SSL	• Enforce SSL V3 protocol	• SSL V2 Buffer Overflow
VoIP	• Verify protocol fields and values • Identification and restriction of the PORT command • Enforce existence of mandatory fields • Enforce user registration • Prevent VoIP firewall holes	• Buffer Overflow Attacks • Man-in-the-Middle Attack
X11	• Restrict reverse injection	

APPENDIKS C

Nedenfor er gennemgået afprøvningen af RSA's SecurID OTP-system samt Rainbow Technologies' iKey-system. Begge systemer har været til låns i en længere periode, så det har været muligt at implementere dem i et testsystem.

Afprøvning af RSA's SecurID

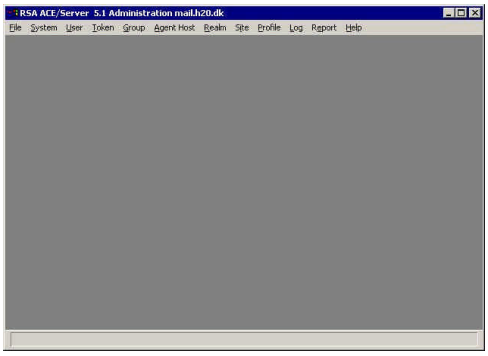
Det har været muligt at have RSA SecurID-systemet til test i en begrænset udgave med to enheder. Erfaringer med denne opsætning er beskrevet nedenfor.

Målet med testen var at få etableret to-faktor autentifikation med VPN, WebMail og diverse hjemmesider. Til dette blev benyttet et testnetværk bestående af følgende:

Server A: Windows 2000 Server med Exchange 2000 samt IIS 5
Server B: Windows 2000 Server med ISA Server 2000
Klient C: Windows XP Professional
Klient D: Windows 2000 Professional

RSA havde leveret nyeste serverudgave af RSA ACE/Server (version 5.1) samt to RSA SecurID enheder med tilhørende initieringskoder. Serversoftwaren blev installeret på Server A idet denne var placeret bag Server B, som fungerede som gateway til internettet.

Til SecurID-systemet findes ud over ACE/Server nogle agentprogrammer, som fungerer som relæer mellem applikationerne og ACE/Server. Til brug ved VPN blev Agent for Windows 5.5 benyttet, mens Agent for Windows 5.0 blev benyttet i forbindelse med beskyttelsen af hjemmesider. Til at beskytte WebMail (Exchange 2000's Outlook Web Access system) blev en speciel opdatering til Microsoft ISA Server 2000 benyttet. Dette er en del af Feature Pack 1.



Figur 59 - Skærmbillede af administrationsinterface til RSA ACE/Server 5.1

Det blev hurtigt klart, at implementeringen af systemet ikke er nogen simpel affære. Alene at få de mest basale funktioner til at fungere tog adskillige dages arbejde, og dokumentationen til ACE/Server efterlader meget at ønske. RSA anbefaler da også, at installationen foretages af en specialist.

Fra administrationsinterfacet til ACE/Server er det muligt at etablere forbindelse til fx Active Directory for på den måde at synkronisere brugerdata.
Det er også fra dette interface enheder tilknyttes brugere, agentprogrammer sættes op samt alle andre administrative processer udføres. Som det ses fra figur 59, er der ikke gjort meget ud af brugerinterfacet, som bærer tydeligt præg af at være designet til at blive implementeret i virksomhedens eksisterende administrationsprogrammel. Det er således også muligt at udføre alle funktioner via kommandolinien.

Figur 60 - Skærmbillede af RSA SecurID's sikring af hjemmesider

Sikringen af hjemmesider foregår via agentprogrammet ACE/Agent for Windows 5.0 og blev testet med Internet Information Services 5.0 i Windows 2000. Det er muligt at sikre hele web sites, enkelte virtuelle biblioteker eller enkelte hjemmesider. Sikringen foregår ved at der vises en loginside som vist på figur 60. Herefter tillades adgang til hjemmesiden, som efterfølgende kan bede om brugernavn og password. En uheldig egenskab ved denne måde at sikre siderne på er, at det brugernavn som benyttes ved RSA login'et ikke behøver matche det, som benyttes ved det efterfølgende login. En enkelt kompromitteret RSA-enhed kan derfor give adgang til samtlige brugeres efterfølgende almindelige login[91]. Samtidig afkræves alle brugere en RSA passcode. Dvs. det er ikke muligt kun at kræve, at visse grupper benytter RSA-systemet, mens andre må nøjes med den sikkerhed, som følger med et almindeligt brugernavn/password-login.

[91] RSA har efter henvendelse bekræftet at dette er et problem og udarbejder en opdatering til agentprogrammet for at rette op på dette.

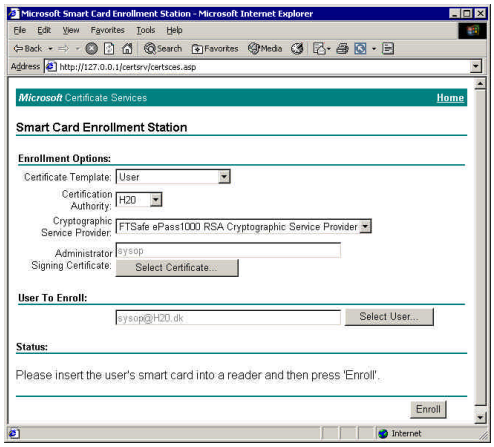
Figur 61 - Skærmbillede af VPN login ved brug af RSA SecurID

VPN-implementeringen kræver installation af ACE/Agent for Windows 5.5 samt omkonfiguration af Routing & Remote Access Server (RRAS) i Windows 2000. Samtidig kræves, at ACE/Agent installeres på alle de klienter, som skal benytte VPN-forbindelsen. Sidstnævnte kan ske ved at rulle en sådan installation ud automatisk ved hjælp af fx Group Policies (i et Windows-netværk).
I testopsætningen blev Microsoft's PPTP VPN benyttet (se afsnit 5.1) og klientprogrammet blev afprøvet både under Windows 2000 og Windows XP. Et eksempel kan ses på figur 61. Dette fungerer udmærket, og har ikke samme svaghed med brugernavnene som ved sikringen af hjemmesider. I VPN-systemet kræves det, at det brugernavn som benyttes til RSA-autentificeringen er det samme, som benyttes ved det foregående primære VPN-login.
Til gengæld er der samme problem med brugeropdeling, hvor alle brugere kræves RSA-login. Det er dermed ikke muligt kun at kræve denne ekstra sikkerhed for visse brugere (fx administratorer).
Det er i øvrigt værd at bemærke, at det det ikke er nødvendigt at benytte det password, som tilhører den Windows-konto, der benyttes. Kun passcoden fra RSA er nødvendig i kombination med brugernavnet.

Afprøvning af Rainbow Technologies' iKey

Det har ligesom med RSA-systemet været muligt at have et begrænset iKey-system til afprøvning. Dette er blevet implementeret i et test-netværk og erfaringer med dette er beskrevet nedenfor. Netværksopsætningen er den samme som i testen af RSA SecurID-produktet ovenfor.

Formålet med testen har været at undersøge, hvordan brugen af digitale certifikater til sikker to-faktor autentificering kan implementeres. Til dette er der brugt et Windows 2000-baseret Active Directory-netværk med brug af en lokal Certificate Authority. Ved at benytte iKey-systemet kan certifikaterne holdes private og mobile.



Figur 62 - Tildeling af digitale certifikater

Ved hjælp af Microsofts Certificate Services (som er en del af Windows 2000 Server) kan brugerne tildeles digitale certifikater, som forbindes med deres brugerkonti i systemet. Dette foregår via en web-baseret proces som ses på figur 62. Certifikatet genereres direkte på den tilsluttede iKey, således at den private nøgle ikke eksisterer andre steder end her. Samtidig kopieres den offentlige nøgle til systemet, som distribuerer denne information til alle andre servere i domænet og forbinder denne med brugerens konto. Brugeren udstyres nu med den benyttede iKey, som sikres med en brugervalgt PIN-kode. Der findes desuden en central administrationskode, så alle brugernes iKeys kan åbnes med denne kode.

Det er nu muligt for administratorerne at kræve, at visse eller alle brugere fremviser et gyldigt certifikat ved logon til netværket. Brugerens identitet bekræftes ved at udveksle information, som kun indehaveren af den private nøgle kan forstå. Da det er umuligt at kopiere den private nøgle fra enheden til andre enheder eller systemer – og da nøglen er genereret direkte i iKey-enheden og dermed ikke findes i en lokal kopi – kræver det adgang til den originale iKey samt PIN-kode for at logge ind. Mistes enheden kan certifikatet trækkes tilbage og et nyt kan udstedes til brugeren på en ny iKey.

Rent praktisk kræver denne funktionalitet et system, som kan håndtere smart cards og certifikater i loginproceduren. Det kan fx Windows 2000 (men ikke Windows NT), men dette kræver stadig, at en driver til iKey-produktet er installeret på de arbejdsstationer og hjemmearbejdspladser som skal benytte systemet. Herefter er der dog tale om plug-and-play, idet brugeren blot indsætter sin iKey, når logonskærmen vises og taster sin PIN-kode.

Der kan desuden udstedes certifikater, som kan benyttes til at signere e-mail og dokumenter. Disse certifikater kan ligeledes både genereres og lagres på enheden og benyttes i fx e-mailprogrammer. Dermed undgås den sikkerhedsrisiko der ligger i at opbevare certifikaterne på computeren.

Det blev ydermere testet, hvordan systemet fungerer i forbindelse med VPN. Efter driveren til iKey'en er installeret, opsættes VPN-klienten til at autentificere med digitale certifikater hvorefter PIN-koden benyttes. Dette fungerer smertefrit så længe der benyttes Windows-klienter til formålet (Rainbow Technologies leverer ikke drivere til andre operativsystemer).

ORDBOG

Ordbogen er opdelt alfabetisk med undtagelse af de første seks begreber, som gennemgås i kassen nedenfor.

Begreberne er oversat både til engelsk og dansk idet de meget ofte benyttes med deres engelske betegnelser – selv i dansk litteratur.

Prevention
Forhindring
stop, hinder, avert, block, fend off
stoppe, forhindre, blokere
Forebyg eller begræns sandsynligheden for, at et bestemt angreb kan gennemføres.

Pre-emption
Forebyggende angreb
anticipate, prevent by advance action
angreb som foretages for at komme fjenden i forkøbet, forudse, forhindre med forudgående aktivitet
Angrib offensivt mod enhver sandsynlig trussel før denne eventuelt gennemføres for at undgå det kan ske senere.

Deterrence
Afskrækning
discourage, obstruct, repel, frighten off
fratage modet, spærre, afvise, skræmme væk
Afskræk angribere ved at sørge for, at den nødvendige anstrengelse for at gennemføre angrebet er høj, eller ved at devaluere den værdi, et succesfuldt angreb kunne give.

Detection
Opdagelse
discover, track down, identify, notice, observe
påvisning, opklarelse, identificere, observere
Adskil angreb fra normale aktiviteter og tilkald myndighederne.

Deflection
Afbøjning
divert, sidetrack
aflede, omdirigere
Får en angriber til at tro, at et angreb har været succesfuldt, selvom han i stedet for er blevet lokket eller truet hen til et sted, hvor han ingen skade har gjort.

Countermeasures
Modangreb
antidote, corrective, cure
modforanstaltning, modtræk.
Kontra et angreb mens det sker.

802.1.x
802.1x er en teknologi som kan benyttes til at sikre netværksporte mod uautoriseret brug. Når 802.1x er implementeret i netværksudstyret, kræves der autentifikation i form af EAP før porten kan benyttes. Selve autentifikationen udføres af en RADIUS-server.

Access point
Et access point er en basestation for trådløse netværk, som trådløse enheder som bærbare computere og håndholdte enheder benytter. Det kan sammenlignes med de radiomaster, som mobiltelefonerne benytter.

ACK
Se SYN.

ACL
Access Control List. En simpel metode til at begrænse adgang til netværk, netværksenheder, filer eller services. For en netværksenhed kan en ACL være en liste over tilladte IP-adresser, som må tilgå enheden. Således kan det være væsentligt, om man vælger at benytte udgangspunktet "tillad alt, som ikke forbydes" eller "forbyd alt, som ikke tillades". Hvis førstnævnte benyttes skal samtlige IP-numre, som ikke må have adgang til enheden, stå i listen. Hvis sidstnævnte vælges skal kun de IP-numre, som skal have adgang, stå i listen.
I mere komplekse opsætninger kan det være en fordel at vælge "tillad alt, som ikke forbydes" idet det dermed sikres, at eksisterende software eller netværksforbindelser fortsat virker, og der kan tilføjes en enkelt "forbudslinie" ad gangen i listen for at se, om det skulle resultere i problemer med programmer eller maskiner. Dette er dog en usikker løsning, det er let at overse adresser, som skal forbydes adgang. Omvendt er "forbyd alt, som ikke tillades" tilgangen til problemet meget administrativ tung, idet der kan være meget arbejde forbundet med at undersøge hvilke IP-adresser eller andet, som kræver adgang for at undgå problemer. Således vil en netværksenhed med "tillad alt som ikke

forbydes" fungere på netværket med det samme (dog uden sikkerhed), mens dette ikke er tilfældet for den anden metode.

AES Advanced Encryption Standard. AES er en krypteringsalgoritme, som er godkendt af Federal Information Processing Standards (FIPS) og National Institute of Standards and Technology (NIST). AES erstatter DES-algoritmen som den officielle krypteringsalgoritme anbefalet af NIST.

ARP Address Resolution Protocol. ARP benyttes normalt til at fastslå MAC-adressen for en enhed baseret på IP-adressen

ASP Active Server Pages. Et programmeringssprog, som kan benyttes til at lave dynamiske hjemmesider. Et eksempel herpå er en hjemmeside, som er opbygget af informationer, der er hentet fra en database (fx en elektronisk boghandel).

Bagdør En bagdør er en "mechanism surreptitiously introduced into a computer system to facilitate unauthorized access to the system" [98] og kan klassificeres efter tre kategorier:

Aktive
Aktive bagdøre etablerer aktivt udgående forbindelser til en eller flere maskiner. Alternativt overvåges et system aktivt, hvorefter information om systemet sendes ud af netværket. I visse tilfælde kan aktive bagdøre modtage kommandoer udefra.

Passive
I stedet for som aktive bagdøre at etablere udgående forbindelser, lytter passive bagdøre på forudbestemte porte efter forbindelser fra en eller flere maskiner. Når forbindelsen er etableret, kan funktionen være den samme som de aktive.

Angrebsbaserede
Også klassificeret som ukendte bagdøre, idet der er tale om dårligt programmerede applikationer, som på den ene eller anden måde utilsigtet kan benyttes som bagdør fx vha. en buffer overflow sårbarhed. Oftest vil resultatet være en form for kommandolinie-adgang til systemet.

Fællesnævneren for disse tre typer bagdøre er, at de alle sammen omgår den lagdelte sikkerhed, som normalt implementeres ved brug af firewalls.

Broadcast Broadcast er betegnelsen for det at sende en besked til mange modtagere på én gang. Benyttes fx når en netværksenhed, som en switch, ikke ved, hvor en modtager befinder sig. I dette tilfælde sendes netværkstrafikken til alle enheder (trafikken broadcastes), indtil det kan afgøres, hvor enheden befinder sig, hvorefter trafikken sendes til denne ene modtager.

Brute Force I brute force angreb benyttes rå computerkraft til at bryde fx et password. Således gennemgås samtlige kombinationsmuligheder systematisk indtil det søgte password er fundet.

Buffer overflow En buffer er et lager i hukommelsen med begrænset kapacitet. Buffer overflow angreb udnytter, at der er en maksimumværdi for, hvad der kan lagres i en buffer. Hvis man "overflow'er" denne maksimumværdi starter tallet forfra. Hvis fx det højeste tal er 65.535 og man tilføjer én, så går værdien tilbage til 0.

CA Se Certificate Authorities

CERT Computer Emergency Response Team. Et center for internetekspertise som primært behandler sikkerhedsrelaterede hændelser. I Danmark findes DK•CERT, som køres af UNI-C.

Certificate Authorities En Certificate Authority (CA) tilsvarer den myndighed, som udsteder pas i den fysiske verden. Deres primære formål er at udstede digitale certifikater og bekræfte identiteten af den person, som certifikatet er udstedt til. Hvis andre stoler på den myndighed, som har udstedt certifikatet, vil de også stole på det certifikat, som er udstedt.
Måden et certifikat benyttes på foregår ved at den person, som ønsker at afsende en besked, først søger om et certifikat hos en CA. CA'en bekræfter personens identitet (fx ved fysisk fremmøde og fremvisning af gyldige identitetspapirer) og udsteder det digitale

certifikat. Herefter offentliggør CA'en certifikatet. Afsenderen signerer beskeden med sin private nøgle (se PKI nedenfor) og sender beskeden til modtageren. Modtageren verificerer den digitale signatur med afsenderens offentlige nøgle og verificerer afsenderens identitet ved at bede CA'en om at bekræfte identiteten på personen ud fra det offentliggjorte certifikat [77].

Challenge/Response Challenge/Response protokoller kan fx være brugen af digitale signaturer. Et simpelt eksempel består af fire skridt. Først fortæller brugeren serveren at der ønskes adgang. Herefter genererer serveren et tilfældigt tal (en challenge) og sender til brugeren. Brugeren benytter sin digitale signatur (private nøgle) til at signere denne information, og sender dette retur (response). Serveren kan nu verificere, at den signerede version er identisk med den oprindelige samt at den korrekte digitale signatur er benyttet til signeringen.

Checksum Checksums benyttes til at verificere, at filer og beskeder forbliver uændrede. Således udregnes et nummer ud fra dataene i beskeden eller filen, som med stor sandsynlighed vil ændre sig, hvis der ændres i den oprindelige fil eller besked. Et sådant nummer kaldes en checksum. Forskellen mellem checksums og hash funktioner er, at hash funktionerne er designet til at sikre, at én besked ikke kan have samme hashværdi som en anden besked mens checksums er designet til at sikre, at tilfældige ændringer til beskeden giver en ændret checksum. Således er hash funktionerne ofte langt stærkere end checksums, og det vil kræve langt mere arbejde at fremstille to beskeder med samme hashværdi end to beskeder med samme checksum.

Cipher tekst Cipher tekst er den streng af karakterer, som fås efter kryptering af originalstrengen.

CRL Certificate Revocation List. En CRL indeholder en af en CA signeret liste over annullerede certifikater.

Denial of Service (DoS) Henviser til det at overbelaste et netværk eller maskine med beskeder for at forhindre normal trafik i at komme igennem.

Digitale certifikater Digitale certifikater fungerer som et digitalt pas og benyttes til elektronisk identifikation. Alle brugere af PKI (se nedenfor) bør have denne form for registreret identifikation. Normalt indeholder det digitale certifikat brugerens navn, e-mailadresse, offentlige nøgle, udløbsdato for certifikatet samt brugerens digitale signatur. Disse certifikater benyttes til at verificere at en bruger er, hvem hun siger, hun er, og offentliggøres af Certificate Authorities (CAs).

Digitale signaturer Digitale signaturer benyttes til at verificere afsenderen af en besked samt til at sikre, at beskeden ikke har været ændret undervejs. I nogle lande er digitale signaturer lige så gyldige som "analoge" underskrifter.
Den digitale signatur er en matematisk funktion, som involverer afsenderens private nøgle og selve beskeden.
Først udføres en hash-funktion, som reducerer den oprindelige besked til typisk 160 bit. Disse 160 bit er et matematisk resume af den oprindelige besked. Ændres et enkelt bogstav i den oprindelige besked, ændres ligeledes de 160 bit.
Disse 160 bit krypteres herefter med afsenderes private nøgle. Resultatet af dette kaldes den digitale signatur og er unik for hver besked. Denne digitale signatur sendes sammen med den oprindelige besked, således at det er muligt for modtageren ved hjælp af afsenderens offentlige nøgle at verificere, at beskeden er uændret samt at verificere afsenderens identitet (da kun en person med adgang til afsenderens private nøgle kunne have genereret de 160 krypterede bits). Digitale certifikater (se nedenfor) kan benyttes til at sikre den fysiske identitet af afsenderen.

Når den signerede og krypterede besked modtages, dekrypteres den, og integriteten verificeres. Den symmetriske engangsnøgle dekrypteres med modtagerens private nøgle og benyttes til at dekryptere den krypterede besked og signaturen.
Ved at benytte afsenderens offentlige nøgle, dekrypteres den digitale signatur og de 160 bit benyttes nu til at sammenligne med de 160 bit, som fremkommer ved igen at gennemføre samme hash-funktion på beskeden. Hvis disse to er ens kan beskedens integritet bekræftes [77].

DMZ Demilitariseret zone. Udtrykket stammer fra koreakrigen hvor det beskrev en stribe af land, som blev holdt fri for fjendtlige soldater uden at risikere egne soldaters liv. Dette blev gjort ved at lave området til et minefelt.
I netværkstermer henviser en DMZ til en del af netværket, som ikke beskyttes på samme måde som det interne net, og som er adskilt fra dette.
En maskine, som en gang har været placeret i en DMZ, bør senere ikke flyttes ind på det interne netværk, idet der er større chance for, at maskinen er blevet kompromitteret.
Ofte ligger der store overvejelser bag hvilke maskiner en virksomhed vælger at placere i en DMZ. Dynamiske websider kræver fx adgang til en databaseserver, så hvis webserveren placeres i DMZ, skal databaseserveren også placeres der – eller der skal gives adgang fra DMZ'en til det interne netværk. Dette er ikke trivielle overvejelser, og der er ikke et universelt svar på hvilken metode, der er den bedste eller sikreste.

DMZ-ben Et DMZ-ben er den netværksport i en firewall eller router, som DMZ'en er tilkoblet.

DNS Domain Name System. DNS oversætter domænenavne (som fx google.com) til IP-adresser (google.com's tilsvarende IP-adresse er 216.239.51.100). Hvis ikke den pågældende DNS-server kan slå navnet op, spørger den den næste DNS-server i hierarkiet. Dette hierarki ender ved de såkaldte root servere, der eksisterer 13 af i verden. DNS er lavet fordi mennesker finder det nemmere at huske navne som Google frem for fler-cifrede tal.

Dobbel-hop DMZ En dobbel-hop DMZ er blot en DMZ opdelt i to stadier, som regel adskilt af en firewall. Således vil der være en firewall, en DMZ, en firewall, endnu en DMZ og herefter en firewall efterfulgt af det interne netværk.

Driver En driver er et stykke software, som etablerer forbindelse mellem et stykke hardware (fx et lydkort) og operativsystemet.

EAP Extensible Autentication Protocol. EAP er en udvidelse til PPP, og er en generel protokol til autentificering. Den understøtter autentifikationsmetoder som OTP, certifikater og smart cards. EAP benyttes desuden til 802.1x autentificering.

Ethernetframes / frames Frames er betegnelsen for de enheder, som udgør netværkstrafikken på lag 2. Således afsendes en besked opdelt i frames af en bestemt størrelse, som når de modtages, samles så hele beskeden igen fremstår i sin helhed.
Ofte benyttes betegnelsen pakke også for frames, selvom dette i strengt arkitektonisk terminologi ikke er korrekt.

Flooding Flooding er et udtryk, som dækker over det at "oversvømme" en netværksenhed med data.

Fortrolighed Data kan kun tilgås af autoriserede personer.

Framebuffer En framebuffer er en del af den hukommelse, som findes på et grafikkort. Framebufferen benyttes til at gemme den information, som skal sendes til skærmen. Under beregningen af et billede vil processoren fx skrive farveinformation til framebufferen i en ulineær proces. Når hele billedet er færdigberegnet vises billedet på skærmen.

Gateway En gateway er en netværksenhed, som arbejdsstationer, servere og andre enheder benytter, for at komme fra et netværk til et andet (fx 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.

Group Policies Group Policies er en funktion i Windows 2000 og senere operativsystemer fra Microsoft som muliggør distribueringen af stort set alle indstillinger samt opdateringer og nye programmer. Således kan der laves låste konfigurationer, hvor brugeren ikke kan ændre i opsætninger eller eksekvere andre programmer end dem, som administratorerne har konfigureret i Group Policies. Disse policies opdateres hver gang maskinen kobles til netværket.

Hash funktion En hash funktion eller hash algoritme er en måde hvorpå et "fingeraftryk" af en fil eller besked kan udregnes, således at enhver ændring til den originale fil eller besked vil give

et nyt ”fingeraftryk”. På denne må kan en sammenligning af hash-udregningerne afsløre, om filen eller beskeden er ændret i forhold til originalen. Det er i dag så ressourcekrævende at generere to beskeder med samme ”fingeraftryk”, at dette betragtes som umuligt.

HIDS HIDS (Host Intrusion Detection System) er en softwareapplikation, der overvåger aktivitet på en enkelt enhed. Kan fx validere kald til applikationer og operativsystemer, checke log filer eller overvåge netværksforbindelser. Kan desuden holde alle forbindelser op mod en database af kendte angrebstyper.

ICA Independent Computing Architecture. ICA er et varemærke registreret af Citrix og er den teknologi, som tillader mange forskellige computere som kører mange forskellige operativsystemer at tilgå applikationer, som kører på Windows-platformen. Det er en standard for tynde klienter/serverbaseret computing. ICA er også en netværksprotokol som overfører tastetryk, museklik og skærmopdateringer over standardprotokoller til og fra klienten. Denne protokol er meget effektiv med hensyn til båndbreddeforbrug og kan ofte nøjes med ca. 20 kbit/s pr. klient.

ICMP Internet Control Message Protocol. ICMP er en protokol, som opererer på netværkslaget. Den rapporterer IP-pakkers fejl og anden information tilbage til afsenderadressen. Således kan en router sende en ICMP-pakke tilbage til afsenderen af en IP-pakke for at fortælle, at IP-pakken ikke kunne leveres, fordi modtageradressen ikke kunne findes. ICMP-pakker benyttes også til at kontrollere, om en enhed kan tilgås via netværket (fx via ping-kommandoen).

ICSA International Computer Security Association. ICSA Labs certificerer sikkerhedsprodukter. Deres officielle målsætning er:
”to achieve major risk reduction within certified products and systems” [84].

IDS Intrusion Detection System. Se HIDS og NIDS.

Integritet Henviser til det, at data kun kan ændres af autoriserede personer

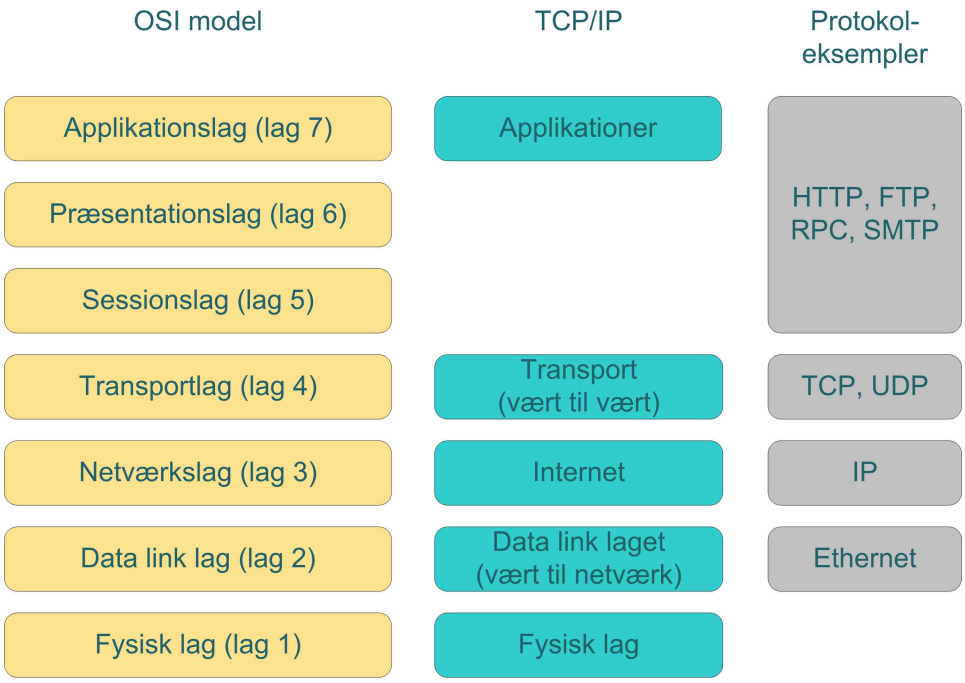
IP Internet Protocol. Internetprotokollen er en protokol, som opererer på netværkslaget (lag 3). Den indeholder adressering og routinginformation. Sammen med TCP udgør IP hjertet af internetprotokollerne.

IPSec IP Security. IPSec er et sæt protokoller udviklet af Internet Engineering Task Force (IETF) som tilføjer sikkerhedsløsninger til TCP/IP-netværk. IPSec understøtter mange forskellige krypteringsalgoritmer.
IPSec er en løsning til at beskytte data mod aflytning, samt til at sikre integritet og autentificering. Den opererer på lag 3, og er netværksuafhængig og applikationsuafhængig.
Encapsulating Security Payload komponenten af IPSec sikrer dataene mod genafspilningsangreb ved at udregne en matematisk nummerering af pakkerne, så enhederne vil detektere, hvis disse pakker senere genindsættes i datastrømmen.

L2TP Layer 2 Tunneling Protocol. L2TP er en kombination af Microsoft’s PPTP samt Cisco’s Layer 2 Forwarding Protocol (L2F), og er således en VPN-protokol, hvis specielle egenskab er, at protokoller som IPX og AppleTalk kan tunneleres over IP.

Lag

Meget generelt består kommunikation af tre ting: applikationer, computere og netværk.



Figur 63 - OSI og TCP/IP modellen

Som det ses på figur 63, findes to primære modeller, OSI og TCP/IP. På figuren er desuden vist nogle protokoleksempler, samt hvor disse hører til i modellerne.
Normalt benyttes OSI-modellen, som i syv lag beskriver netværksarkitekturen. TCP/IP-modellen er ældre, hvilket er grunden til den ikke efterkommer OSI-standarden. De første fire lag af TCP/IP-modellen ligger dog tæt op ad OSI-modellen.

TCP/IP forklares nedenfor. Dette er den mest udbredte model i dag og består af fem lag. Modellen blev oprindeligt udviklet for US Department of Defense Advanced Research Project Agency (DARPA) netværket.

- **Det fysiske lag** dækker over det fysiske interface mellem computeren og netværket. Her håndteres de elektriske karakteristikker som fx oversættelsen af bits til spændingsniveauer. Samtidig er dette laget, hvor den fysiske forbindelse tilgås. Dvs. fx hvor mange pins der er i stikket, og hvad de bruges til.
- **Link laget** kontrollerer adgangen til netværket mellem to systemer, som et koblet til det samme netværk. Her behandles dirigering af trafik, prioritering og adressering. Ethernets medium access control (CSMA/CD) opererer på dette lag.
- **Internetlaget** sørger for, at to systemer på forskellige netværk kan tale sammen. Adressering og routing foregår på dette lag. Her benyttes IP protokollen, som også er implementeret i routere og dermed fungerer som fælles standard.
- **Transportlaget** sikrer, at data sendes pålideligt og at pakkerne ankommer i samme orden som de blev afsendt. Til dette benyttes TCP protokollen. UDP protokollen findes også i dette lag, men leverer ikke den samme pålidelighed som TCP. En forklaring på TCP og UDP kan ses nedenfor.
- **Applikationslaget** indeholder den logik som sikrer, at applikationerne kan tale med netværket. Dette lag kan sammenlignes med OSI-modellens applikations-, præsentations- og sessionslag. Eksempler på protokoller, som fungerer i dette lag, er FTP og HTTP.

OSI (Open Systems Interconnect)
OSI er en rivaliserende standard for computer kommunikationsarkitektur. OSI-modellen består af syv lag som kan ses på figur 63, men er aldrig blevet udbredt. I dag benyttes næsten udelukkende TCP/IP.
OSI-modellen er dog god til at beskrive netværksarkitekturer og benyttes derfor ofte som referencemodel.
OSI-lagene er beskrevet således:

- **Det fysiske lag** håndterer ligesom TCP/IP-modellen det fysiske interface.
- **Data Link laget** sikrer fejlfri transmission af data frames fra en node til en anden over den fysiske linie. Det logiske link mellem to noder etableres og termineres ligesom det sikres, at de aktuelle frames sendes sekventielt.

- **Netværkslaget** kontrollerer driften af subnettet og afgør hvilken fysisk vej data skal tage baseret på netværkstilstanden, prioriteter og andre faktorer. Samtidig kan frame fragmentering foregå for at udnytte endestationens maksimale tilladte transmissionsstørrelse.
  Netværkslaget bygger desuden headere, så netværkslagenes software kan benytte disse til at dirigere trafikken til destinationsadressen. I dette lag oversættes logiske netværksadresser til fysiske adresser (dvs. fx oversættelse fra en IP-adresse til en MAC-adresse).
- **Transportlaget** sikrer, at data leveres fejlfrit i korrekt sekvens og uden tab eller duplikeringer. Laget aflaster de øvre lag fra at vide noget om, hvordan data transmitteres.
  Transportlaget segmenterer desuden beskederne fra sessionslaget, så de er tilpasset netværkslaget eller data link laget. Samtidig tilføjes headerinformationer om, hvordan disse beskeder skal samles igen. Dette lag er desuden det nederste lag, som håndterer end-to-end transmission. De nedre lag håndterer kun kommunikation med den nærmeste nabo.
- **Sessionslaget** håndterer forbindelserne (sessioner) mellem applikationerne. Laget tillader to applikationsprocessor på forskellige maskiner at etablere og terminere sessioner. Samtidig udføres funktioner, som understøtter sessionerne som fx navnegenkendelse, logning mm.
  Et eksempel er interaktive logons og filoverførsler, hvor dette lag sikrer, at en session forbindes igen, hvis der sker en afbrydelse.
- **Præsentationslaget** formaterer data, så de kan præsenteres for applikationslaget. Dette kan sammenlignes med en oversætter for netværket. Fx kan laget oversætte fra et dataformat brugt i applikationslaget til et fælles format, som benyttes ved afsenderstationen. Derefter oversættes i den anden ende fra modtagerstationen (og dermed det fælles format) til det format, som applikationslaget her forstår.
- **Applikationslaget** fungerer som et vindue for brugere og applikationer til at tilgå netværksservices. Dette inkluderer fx fil og printerdeling, e-mail mm. [92]

LAN

Local Area Network. Et LAN er typisk et netværk, som er afgrænset til en enkelt organisation. Således vil en virksomheds interne netværk oftest være et LAN.

MAC

Medium Access Control. Benyttes i ikke-switchede netværk til at bestemme hvornår der kan sendes data, hvad der skal gøres, hvis data kolliderer, samt hvor længe der skal ventes inden en retransmission foretages.
Carrier Sensed Multiple Access with Collision Detection (CSMA/CD) er den MAC som benyttes i ikke-switchede ethernets [97].

MAC adresser

Medium Access Control adresser. MAC-adresser er en unikke adresser, som tildeles ethernet hardware. Adressen er 48 bits lang og skrives i hexadecimal-notation, som fx 12:34:56:78:9A:BC. Mængden af mulige adresser svarer til ca. 50.000 per person på jorden.
MAC-adresser benyttes på lag 2 til at sende pakker til ethernet-enheder på netværket. Når en IP-adresse skal oversættes til den tilsvarende MAC-adresse benyttes ARP. Idet MAC-adresser kun kendes af den router, som er nærmest enheden, benyttes IP-adresser til at levere pakker gennem routere indtil sidste router inden modtageren nås. Her oversættes IP-adressen til enhedens MAC-adresse, hvorefter pakken leveres til enheden via switche, som operer på lag 2 og derfor forstår MAC-adressen (men ikke IP-adressen).

Man-in-the-middle angreb

Man-in-the-middle angreb er en angrebsform, hvor angriberen opfanger (sniffer) pakker fra et netværk, modificerer dem og genindsætter dem i netværket. Kan desuden benyttes til at overtage en etableret forbindelse

MD5

Message Digest algorithm 5. MD5 er en algoritme til at udregne hash-værdier (”fingeraftryk”). I 1996 blev en sårbarhed i MD5 fundet af Hans Dobbertin, som i fremtiden kan vise sig at blive et problem. Se også hash funktion.

[92] Der er i ordforklaringen brugt information fra [95], [46] side 4-61 samt.

MIB Management Information Base. MIB er en samling af informationer, som er organiseret hierarkisk. MIBs tilgås via en managementprotokol som SNMP. En MIB er således oftest en samling af informationer, som beskriver en SNMP-enhed.

Modifikation Henviser til det, at dele af den originale besked er ændret.

NAT Network Address Translation. NAT er en teknik, som ofte bruges for at kunne benytte private, interne IP-adresser i en virksomhed. NAT-enheden "oversætter" mellem en eller flere offentlige IP-adresser og de interne adresser, som arbejdsstationer og servere har.

NIDS NIDS (Network Intrusion Detection System) opfanger netværkstrafik på et LAN-segment og prøver at matche trafikken til en database af kendte angrebdstyper ligesom HIDS. Dette kan kræve avancerede analyser af de øvre lag. NIDS benyttes normalt til at levere advarsler og ikke til at stoppe trafikken.

NTP Network Time Protocol. NTP er en protokol, som kan benyttes til at synkronisere arbejdsstationer, servere og netværksudstyr mod en tidsserver, som er synkroniseret med fx atomuret i Frankfurt.

Orm En netværksorm er et program, som ved at benytte netværksforbindelser kan sprede sig fra system til system. Når det aktiveres på systemet, kan det opføre sig som en virus eller trojansk hest.

OTP One Time Passwords. I modsætning til almindelige passwords benyttes passwordet kun én gang, hvorefter et nyt udstedes. Et eksempel på et system, som benytter OTP er RSA's SecurID. Her benyttes en enhed, som beregner et nyt password hvert minut. Den netværksenhed, som skal autentificere brugeren beregner ligeledes denne kode, og kan derfor validere brugerens identitet. Koden beregnes ud fra en initeringsværdi, en algortime (AES) samt tidspunktet.

Pakke Pakker er betegnelsen for de enheder, som udgør netværkstrafikken på lag 3. Ofte benyttes betegnelsen pakke også for enheder på lag 2, som rent teknisk betegnes frames.

Passive trusler Henviser til det at aflytte eller indsamle information i forbindelse med netværkskommunikation.

PDA Personal Digital Assistant. En lommecomputer, som fx benyttes som elektronisk kalender.

Peer-to-peer (P2P) Et Peer-To-Peer (P2P) netværk er et netværk, som oprettes direkte mellem to enheder. P2P benyttes i daglig tale til at henvise til fildelingsprogrammer, hvor brugere kan udveksle data med hinanden. Her kan én bruger etablere en forbindelse til en anden bruger og benytte de ressourcer, som modparten stiller til rådighed. Velkendte eksempler er Kazaa og Napster.

PGP Pretty Good Privacy. PGP er et program til at kryptere filer, diske, e-mails og anden elektronisk kommunikation. PGP blev oprindeligt udviklet på det amerikanske universitet MIT, men blev senere solgt til Network Associates. Det ejes i dag af PGP Corp. Programmet benytter PKI og muliggør brugen af mange forskellige krypteringsstandarder.

PIX Private Internet eXchange. Cisco har udviklet en serie af firewalls, som går under navnet PIX. Disse firewalls spænder fra mindre enheder til private eller små virksomheder til store enheder til beskyttelse af en virksomheds LAN.

PKI Public Key Infrastructure. Ideen bag PKI blev udviklet opfundet af Whitfield Diffie og Martin Hellman i 1976 mens Ron Rivest, Adi Shamir og Le Adleman (RSA) implementerede ideen kort efter.
PKI benytter et nøglepar af assymetriske nøgler som er matematisk bundet til hinanden. Det den ene nøgle låser, kan den anden låse op. Rent praktisk genereres først den private nøgle hvorefter envejs matematik benyttes til at generere den offentlige nøgle ud fra den private. Det er praktisk set umuligt at beregne den private nøgle ud fra den offentlige. Mens den offentlige nøgle kan distribueres, skal den private nøgle beskyttes og bør opbevares på smart cards eller lignende.

Krypteres noget med modtagerens offentlige nøgle sikres det, at kun den person, som er i besiddelse af den tilsvarende private nøgle, kan dekryptere dette.
Normalt vil der blive beregnet en digital signatur (se ovenfor), hvorefter selve beskeden krypteres. Denne krypteringsproces benytter en symmetrisk nøgle, som i dag oftest vil være 1024-2048 bits lang (supercomputere kan i dag bryde en 1024 bit nøgle på ca. 20 år). Symmetriske nøgler er engangsnøgler, som både kan låse beskeden samt låse den op. Efter beskeden og tilhørende digitale signatur er krypteret med den symmetriske nøgle, skal denne nøgle transporteres til modtageren så beskeden kan dekrypteres. Transporten af denne nøgle skal sikres mod aflytning. Dette foregår ved at kryptere den symmetriske nøgle med modtagerens offentlige nøgle, så kun den person, som er i besiddelse af den tilhørende private nøgle, kan dekryptere dette og få adgang til den symmetriske nøgle. Den krypterede besked sendes nu sammen med den krypterede symmetriske nøgle til modtageren. Grunden til, at der benyttes symmetriske nøgler er, at kryptering med symmetriske nøgler er langt hurtigere end med assymetriske [77].

PPP Point-to-Point Protocol er internetstandarden for transmissionen af IP-pakker over serielle linier. PPP understøtter forbindelser over synkrone og asynkrone kredsløb, og blev oprindeligt udviklet til at indkapsle IP-trafik til overførsel over point-to-point linier. Udover IP understøtter PPP også fx Internetwork Packet Exchange (IPX), AppleTalk og andre protokoller.

PPTP Point-to-Point Tunneling Protocol. PPTP er en VPN-protokol, som er udviklet primært af Microsoft.

Proof of concept Et proof of concept script er typisk en demonstration af, hvordan en sårbarhed kan udføres i praksis. Ofte vil denne demonstration ikke inkludere destruktive egenskaber men vise, hvordan konceptet fungerer. Da proof of concept scripts ofte er lette at ændre til at udføre andre kommandoer, kan disse danne grundlag for et angreb.

Proxyserver En server, som fungerer som ”mellemmand” mellem den enhed, som ønsker at oprette en forbindelse og den enhed, som forbindelsen ønskes opretttet til. Et eksempel er en webproxy.

PVLAN Private Virtual LAN. PVLANs gør det muligt at etablere regler for, at enheder indenfor samme VLAN ikke må kommunikere indbyrdes.

RADIUS Remote Authentication Dial In User Service. En RADIUS server er ansvarlig for at modtage anmodninger om brugerforbindelser, autentificere brugeren samt returnere alle de nødvendige konfigurationsoplysninger, som er krævet af klienten for at levere service til brugeren. Klienten kan være en netværksserver eller en netværksenhed, som videresender brugeroplysninger til RADIUS-serveren og modtager svaret.
Kommunikationen mellem RADIUS serveren og klienten er autentificeret via en delt nøgle, som aldrig sendes over netværket. Brugeroplysningerne sendes krypteret mellem klienten og RADIUS-serveren.
En RADIUS server vil som regel understøtte en lang række forskellige metoder til brugerautentificering.

Replay angreb Replay angreb fungerer ved, at en angriber opfanger pakker fra et netværk og genafspiller disse på et senere tidspunkt. . Selvom trafikken er krypteret, kan replay angreb udføres, idet det ikke er nødvendigt at vide hvad den krypterede tekst indeholder for at udsende den igen.

RFC RFC (Request For Comments). Et dokument, som hvis interessen er stor, kan blive til en internet standard. Et forslag indsendes til IETF (Internet Engineering Task Force), som afgør, om det skal blive en RFC.

RSA RSA er en krypteringsalgortime udviklet af Ron **R**ivest, Adi **S**hamir og Le **A**dleman. Den er baseret på PKI-metoden, som er forklaret ovenfor.
RSA er desuden en virksomhed, startet af Ron Rivest, som bl.a. udvikler OTP-systemet SecurID.

SANS **S**ysAdmin, **A**udit, **N**etwork, **S**ecurity. SANS er en organisation, som offentliggør sikkerhedsproblemer og løsninger samt uddanner administratorer i IT-sikkerhed.

Serverfarm En serverfarm er en samling af servere. Således kan en samling af webservere udgøre en serverfarm. Udtrykket benyttes ofte til at indikere, at der er tale om en større mængde servere, som udfører samme funktion.

SHA Secure Hash Algoritm. SHA er en algoritme til at udregne hash-værdier (”fingeraftryk”). Se også hash funktion.

Single sign-on Single sign-on er et system, som gør det muligt kun at autentificere brugerne én gang og herefter genbruge denne autentificering når efterfølgende produkter kræver dette.

SNMP Simple Network Management Protocol. SNMP er en protokol på applikationslaget, som håndterer udvekslingen af information mellem netværksenheder. Det er en del af TCP/IP-protokolsamlingen. SNMP gør det muligt for netværksadministratorer at overvåge netværksudstyrets performance, finde og løse problemer med enhederne samt indhente generelle oplysninger om alle tilknyttede enheder.
SNMP-kontrollerede netværk består af de enheder, som kontrolleres samt et managementsystem. Et eksempel på en enhed, som benytter SNMP er en router, men også servere, arbejdsstationer og printere kan benytte SNMP. Managementsystemet kan desuden benyttes til at konfigurere enhederne.

Split tunneling Split tunneling er en måde at konfigurere VPN-klienter som hjemmearbejdspladser på, således at internettrafik ikke sendes via serverens VPN Concentrator, men direkte via hjemmearbejdspladsens bredbåndsforbindelse. Dette sætter mindre krav til båndbredden i virksomheden, men sænker sikkerheden, idet virksomheden ikke har samme kontrol over den internettrafik, som hjemmearbejdspladsen udsender.

Spoofing Spoofing benyttes som regel til at ændre den afsenderadresse, som IP-pakker indeholder (IP-spoofing). Dette gøres, så en angriber kan udgive sig for at være en netværksenhed, der har rettigheder, som angriberen ikke ellers ville have.

SQL Structured Query Language. SQL er et standardiseret sprog til at hente og opdatere oplysninger fra en database. De fleste store databaseprodukter understøtter SQL.

SSH Secure Shell. SSH er en applikation og en protokol, som leverer en sikker erstatning for værktøjer som telnet, rlogin, rsh m.fl. Protokollen sikrer en session via kryptografiske teknikker og applikationen kan bruges ligesom de værktøjer, den erstatter, som fx telnet. Al kommunikation er krypteret med fx Triple-DES eller en anden krypteringsstandard. Krypteringsnøglerne udveksles via RSA PKI, og dataene, som benyttes under nøgleudvekslingen typisk bliver destrueret hver time.
SSH kan desuden benyttes til at tunnelere TCP-trafik fra en enhed til en anden over internettet. Dette foregår ved at videresende lokale porte til en anden enhed via den sikre forbindelse. Et eksempel på dette kan være, at den lokale TCP port 2003 sættes op til at videresende data til port 23 på den server, som SSH-forbindelsen er etableret med. Hvis der herefter afvikles en telnet-applikation på den lokale maskine, som peger på adressen 127.0.0.1 (maskinen selv) og port 2003, vil forbindelsen blive etableret til serveren på port 23 (telnet-porten). Således er den usikre telnet-overførsel nu blevet sikret i en SSH-tunnel.

SSL/TLS Secure Sockets Layer og Transport Layer Security. SSL og TLS er de ledende protokoller til at levere sikkerhed til fx elektronisk handel, webservices osv. SSL blev oprindeligt udviklet af Netscape. Da udbredelsen af protokollen steg, blev den overtaget af Internet Engineering Taskforce (IETF). Ved samme lejlighed skiftede protokollen navn til TLS. TLS-protokollen er dermed identisk med den tredje version af SSL. I versionsnumre er TLS 1.0 identisk med SSL 3.1.

Stateful Packet Inspection
En teknologi, som benyttes i nogle firewalls. Der etableres tilstandstabeller for IP-baserede protokoller. Når en pakke ankommer til enheden får den kun lov til at passere, hvis den overholder reglerne i et filter eller tilhører en allerede etableret, godkendt forbindelse, som findes i tilstandstabellen.

SYN Når en TCP-forbindelse etableres sendes en SYN-besked fra afsenderen til modtageren. Denne besvares med en SYN-ACK, som igen besvares med en ACK, hvorefter forbindelsen er oprettet. SYN og ACK er flag, som kan sættes i TCP headeren.

SYN-ACK Se SYN.

Syslog Syslog er en protokol baseret på UDP som tillader en enhed at sende bl.a. log-data over netværket til servere, som opsamler disse data. Dataene sendes ukrypteret, hvis ikke andre teknologier implementeres for at sikre disse.

TCP Transmission Control Protocol. Dette er en pålidelig, connection-orienteret protokol, som leverer fejlkorrigering og flow kontrol gennem virtuelle links. TCP benyttes til fx FTP og e-mail.

Tilgængelighed Henviser til det, at data er tilgængeligt for autoriserede personer.

Trojansk hest En trojansk hest er et nyttigt eller tilsyneladende nyttigt program, som indeholder en skjult kode som – når den eksekveres – udfører en uvelkommen eller harmfuld funktion.

Tynde klienter Tynde klienter er et udtryk som dækker over arbejdsstationer, der ikke selv afvikler programmer, men som blot videresender tastetryk og musebevægelser til en server, som returnerer skærmbilleder, der vises på den tynde klients skærm. Således er det ikke sikkert brugeren vil mærke forskel fra en tynd klient og en regulær arbejdsstation, men der kan være bl.a. administrative fordele i at afvikle applikationerne fra en server i stedet for på hver arbejdsstation.

UDP User Datagram Protocol. Dette er en upålidelig, connection-fri protokol som leverer datatransport med mindre overhead end TCP. UDP laver ikke fejlkorrigering eller flow kontrol – dette overlades til applikationen. SNMP benytter som eksempel UDP.

URL Uniform Resource Locator. URLs er den adresse, som dokumenter og ressourcer på World Wide Web (WWW) har. Således er fx http://www.google.com/ en URL.

VACL Virtual Access Control List. VACL udføres før eventuelle ACLs og filtrerer alle pakker som passerer en switch (ACLs filtrerer kun pakker, som går til routeren). Dermed kan VACLs benyttes til at filterere trafik idenfor et VLAN.

Virus En virus er et program, som kan ”smitte” andre programmer ved at modificere dem. Denne modifikation inkluderer en kopi af virussen, som så igen kan smitte andre programmer.

VLAN Virtual LAN. VLANs kan benyttes til at opdele fysiske netværk i mindre, logiske netværk. Et VLAN er således et broadcast domæne. Opdelingen foregår i lag 2.

Voice over IP Voice over IP (VoIP)er en teknologi, som transporterer telefonsamler via et IP-baseret netværk. Således kan virksomheden etablere telefonforbindelser mellem hjemmearbejdspladser, kontorer og kunder via sit interne netværk og de bredbåndsforbindelser, som allerede er etableret i forbindelse med internetadgangen. VoIP kræver, at udstyret understøtter dette samt at der er tilstrækkelig båndbredde til at håndtere samtalerne.

VoIP Se Voice over IP ovenfor.

VPN Virtual Private Network. VPN kan benyttes til at forbinde enheder på tværs af andre netværk, fx internettet. Det benyttes typisk til at etablere sikre forbindelser over offentlige netværk fra eksterne lokationer til virksomhedens interne netværk. Ofte vil trafikken blive krypteret bl.a. for at undgå, at data kan aflyttes.

VPN Concentrator Oftest en hardwarebaseret VPN-enhed som terminerer VPN-forbindelser.

VPN dialer En hard- eller softwarebaseret VPN klient, som typisk etablerer en tunnel til en VPN Concentrator. Hardwareversionen kræver ingen installation på brugerens arbejdsstation.

LITTERATURLISTE

Nr Forfatter; *Titel*; år, dato eller nr.; udgiver; ISBN eller webadresse
En blank understregning (___) angiver at oplysningen ikke er tilgængelig.

[1] Jason Halpern, Sean Convery, Roland Saville; *SAFE VPN – IPSec Virtual Private Networks in depth*; 2001; Cisco Systems, Inc.; http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safev_wp.htm
[2] Kevin D. Mitnick; *The art of deception*; 2002; Rober Ipsen, Wiley Publishing, Inc.; 0-471-23712-4
[3] ___;*Deloitte Touche Tohmatsu's Global Security Survey 2003*; Maj 2003; Deloitte & Touche; http://www.deloitte.com/dtt/cda/doc/content/Global%20Security%20Survey%202003.pdf
[4] ___; *Teleworking in the UK?*; Slashdot; 30/5-2003; Open Source Development Network; http://slashdot.org/article.pl?sid=03/05/30/0150242
[5] TDC; *Morgenavisen Jyllands-Posten*; 26/5-2003; Jyllands-Posten A/S; ___
[6] ___; *Computer Economics Security Review*; April 2002; Computer Economics (CEI); ___
[7] ___; Crack *Cisco Passwords*; Hackers Playground; ; http://www.hackersplayground.org/papers/crack-cisco-passwords.txt
[8] Gaius; *Things To Do In Cisco Land When You're Dead*; 5/1-2000; Phrack Magazine; http://www.phrack.org/phrack/56/
[9] Eric Monti; *Backdoor passwords in 3com swithces*, routers, smart hubs; 5/5-1998; ___; http://www.afentis.com/resources/misc/3com.switches.routers.undocumented.backdoors.html
[10] Søren Maigaard; *Sikkerhedsanalyse af K-databaren på DTU*; Maj 2002; IMM/DTU; ___
[11] P. Ferguson, D. Senie; *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing (RFC 2827)*; Maj 2000; The Internet Engineering Task Force (IETF); http://www.ietf.org/rfc/rfc2827.txt
[12] Dragorn; *2600, The hacker quarterly: The comprehensive guide to 802.11b wireless networks*; 2002, vol. 19, no. 2; 2600 Enterprises, Inc.; ISSN 0749-3851
[13] Randall S. Murch; United *States of America v. Nicodemo S. Scarfo, and Frank Paolercio*; Oktober 2001; United States District Court District of New Jersey; http://www.epic.org/crypto/scarfo/murch_aff.pdf
[14] Leif Phifer; *GoToMyPC Security*; 2003; Expertcity, Inc.; https://www.gotomypc.com/downloads/pdf/m/GoToMyPC_Personal_Security_White_Paper.pdf
[15] Bruce M.; *Security of dialback modems*; 27/1-1997; Nyhedsgruppen alt.security; http://groups.google.com/groups?q=security+of+dialback+modems&hl=en&lr=&ie=UTF-8&oe=UTF-8&selm=Pine.BSI.3.91.970127101157.5357A-100000%40wichita.fn.net&rnum=1
[16] Stephan Hoffmann, Thomas Unterleitner; *Microsoft PPTP Server Buffer Overflow Vulnerability*; 26/9-2002; SecurityFocus; http://www.securityfocus.com/bid/5807/discussion/
[17] ___; *Cisco VPN Concentrator ICMP Flood Remote Denial Of Service Vulnerability*; 8/5-2003; SecurityFocus; http://www.securityfocus.com/bid/7523/discussion/
[18] Y. Rekhter, B. Moskowitz, D. Karrenberg, G.J. de Groot, E. Lear; *Address Allocation for Private Internets (RFC 1918)*; Februar 1996; The Internet Engineering Task Force (IETF); http://www.ietf.org/rfc/rfc1918.txt
[19] Sean Convery, Roland Saville; *SAFE: Extending the security blueprint to Small, Midsize. and Remote-User Networks*; 2001; Cisco Systems, Inc.; http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safes_wp.pdf
[20] B. Fraser; *Site Security Handbook (RFC 2196)*; September 1997; The Internet Engineering Task Force (IETF); http://www.ietf.org/rfc/rfc2196.txt
[21] Kurt Westh Nielsen; *Computervira koster timelange driftsstop*; 20/6-2003; Ingeniøren; ___
[22] ___; *Hjemmearbejdsplads VPN Router – Den optimale hjemmearbejdspladsløsning*; TDC Internet Erhverv; ___; http://download.tdcinternet.dk/pub/Erhverv/pdf/internetadgang/p_009_a_hjemmearbejdsplads.pdf
[23] Rikke Nickie Mortensen; *Løsningsforslag, DTU*; 28/4-2003; CyberCity Erhverv; ___
[24] ___; *SonicWall TELE3 TZ*; ___; SonicWall; http://www.sonicwall.com/products/pdfs/DS_0402_TELE3_TZ.pdf
[25] ___; *Hjemmearbejdspladsen med hurtig og sikker adgang til virksomhedens ressourcer*; ___; Tiscali; http://erhverv.tiscali.dk/images/produktark/Hjemmearbejdspladsen.pdf
[26] ___; *SonicWall PRO 100*; ___; SonicWall; http://www.sonicwall.com/products/pdfs/SonicWALL_PRO100.pdf
[27] ___; *5781 – Broadband Internet Router*; ___; Efficient Networks; http://www.efficient.com/pdf/efficientnetworks-5781.pdf
[28] ___; *InterJak 200 Internet Service Appliance*; ___; FilaNet; http://www.connectronics.com/filanet/NoWAN_4.pdf
[29] ___; *FilaNet Corporation InterJak 200 version 1.8.1.D*; 11/3-2003; ICSA Labs; http://www.icsalabs.com/html/communities/firewalls/certification/rxvendors/filanetinterjak/labreport_cid719.shtml
[30] Jan Corvinius; *Modeller til hjemme-pc koncept for Forskningsnettet (oplæg til Konceptopbygning)*; 20/9-2002; UNI-C; ___
[31] ___; *Secure Telecommuting for Shared Broadband Access Points*; ___; SonicWall; https://partners.mysonicwall.com/WhitePaper/DownloadCenter/pdf/WP_SecureTelecommuting.pdf
[32] Lloyd M. Lancaster; *CramSession Cisco Insider – Private VLANS*; 28/11-2002; Cisco Insider; http://newsletters.cramsession.com/Newsletters/NewsletterArchive/Cisco/november-28-2002cisco.html
[33] ___; *Understanding and Configuring VLAN Trunk Protocol (VTP)*; December 2002; Cisco Systems, Inc.; http://www.cisco.com/warp/public/473/21.pdf
[34] ___; *SAFE Enterprise Layer 2 Addendum*; 2003; Cisco Systems, Inc.; http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/sfblu_wp.pdf
[35] ___; Securing *Networks with Private VLANs and VLAN Access Control Lists*; 2003; Cisco Systems, Inc.; http://www.cisco.com/warp/public/473/90.pdf
[36] Eric Vyncke; *Ethernet: Layer 2 Security*; 2003; Cisco Systems, Inc. / Terena Networking Conference 2003; http://www.carnet.hr/tnc-cuc2003/program/slides/s1c3.ppt
[37] ___; *Spanning Tree Portfast BPDU Guard Enhancement*; Februar 2003; Cisco Systems, Inc.; http://www.cisco.com/warp/public/473/65.pdf
[38] ___; *Spanning-Tree Protocol Root Guard Enhancement*; Januar 2003; Cisco Systems, Inc.; http://www.cisco.com/warp/public/473/74.pdf

[39] R. Droms; *Dynamic Host Configuration Protocol*; Marts 1997; The Internet Engineering Task Force; http://www.ietf.org/rfc/rfc2131.txt
[40] R. Droms, W. Arbaugh; *Authentication for DHCP Messages*; Juni 2001; The Internet Engineering Task Force; http://www.ietf.org/rfc/rfc3118.txt
[41] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn, B. Palter; *Layer Two Tunneling Protocol "L2TP"*; August 1999; The Internet Engineering Task Force; http://www.ietf.org/rfc/rfc2661.txt
[42] K. Hamzeh, G. Pall, W. Verthein, J. Taarup, W. Little, G. Zorn; *Point-to-Point Tunneling Protocol (PPTP)*; Juli 1999; The Internet Engineering Task Force; http://www.ietf.org/rfc/rfc2637.txt
[43] A. Valencia, M. Littlewood, T. Kolar*; Cisco Layer Two Forwarding (Protocol) "L2F"*; Maj 1998; The Internet Engineering Task Force; http://www.ietf.org/rfc/rfc2341.txt
[44] ___; *Virtual Private Networks for Small Businesses*; ___; NETGEAR; http://www.fastlanetek.com/sites/netgear/genvpn/
[45] S. Kent, R. Atkinson; *Security Architecture for the Internet Protocol*; November 1998; The Internet Engineering Task Force; http://www.ietf.org/rfc/rfc2401.txt
[46] William Stallings; *Data & Computer Communications, 6th edition; 2000*; Prentice Hall International, Inc.; 0-13-086388-2
[47] Stuart McClure, Joel Scambray, George Kurtz; *Hacking Exposed, 4th edition*; 2003; McGraw-Hill/Isborne; 0-07-222742-7
[48] William Stallings; *Cryptography and Network Security, 2nd edition*; 1998; Prentice Hall, Inc.; 0-13-869017-0
[49] Sean Convery, Bernie Trudel; *SAFE: A Security Blueprint for Enterprise Networks*; 2000; Cisco Systems, Inc.; http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.pdf
[50] Erik E. Fair; *Firewall Systems Considered Harmful*; Oktober 1996; clock.org; http://www.clock.org/~fair/opinion/firewalls.html
[51] M. Leech, M. Ganis, Y. Lee, R. Kuris, D. Koblas, L. Jones; *SOCKS Protocol Version 5*; Marts 1996; The Internet Engineering Task Force; http://www.ietf.org/rfc/rfc1928.txt
[52] ___; *Stateful Packet Inspection Explained*; ___; Dreaming Tree Technology, Inc.; http://www.firewalls.com/document-stateful-packet-inspection.asp
[53] ___; *Configuring Application Inspection (Fixup)*; ___; Cisco Systems, Inc.; http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_63/config/fixup.pdf
[54] ___; *The Need for Endpoint Security*; Februar 2002; Hurwitz Group, Inc.; http://download.zonelabs.com/bin/media/pdf/Hurwitz_wp.pdf
[55] Wayne Rash, P.J. Connoly; *Make the desktop a more secure place*; 10/2-2003; InfoWorld; http://download.zonelabs.com/bin/media/pdf/InfoWorld.pdf
[56] Bob Rudis, Phil Kostenbader; *The enemy within: Firewalls and backdoors*; ___; SecurityFocus; http://securityfocus.com/infocus/1701
[57] ___; *Tripwire for Servers Datasheet*; 2003; Tripwire; http://www.tripwire.com/files/literature/product_info/Tripwire_for_Servers.pdf
[58] ___; Morgenavisen Jyllands-Posten, Erhverv; 22/7-2002; Jyllands-Posten A/S; ___
[59] ___; Morgenavisen Jyllands-Posten, 1. sektion; 1/4-2003; Jyllands-Posten A/S; ___
[60] Lawrence M. Bridwell, Peter Tippett; *ICSA Labs 7th Annual Computer Virus Prevalence Survey 2001*; 2001 ; ICSA Labs ; http://www.trusecure.com/download/dispatch/vps-survey-2001.pdf
[61] Morton Swimmer; *Virus Statistics; 2001*; swimmer.org; http://www.swimmer.org/morton/vstat.html
[62] ___; *Virus Related Statistics*; ___; SecurityStats; http://www.securitystats.com/virusstats.asp
[63] ___; *The power behind RSA SecurID Two-Factor User Autentication: RSA ACE/Server*; 2003 ; RSA Security ; http://www.rsasecurity.com/products/securid/whitepapers/AS51_SB_0203.pdf
[64] Kingpin; *iKey 1000 Administrator Access and Data Compromise*; 20/6-2000; @Stake Inc., L0pht Research Labs; http://www.atstake.com/research/advisories/2000/ikey-admin.txt
[65] ___; *iKey 2032 – Windows 2000 Smart Card Logon Integration, Administrator's Guide*; 2002; Rainbow Technologies, Inc.; ___
[66] ___; *Quick Start Guide*; 2002; Rainbow Technologies, Inc.; ___
[67] Sudhakar Govindavajhala, Andrew W. Appel; *Using Memory Errors to Attack a Virtual Machine*; 2003 ; Princeton University ; http://www.cs.princeton.edu/~sudhakar/papers/memerr.pdf
[68] Sudhakar Govindavajhala; *My commentary on the slashdot memory attack discussions*; 2003 ; Princeton University ; http://www.cs.princeton.edu/~sudhakar/papers/memerr-slashdot-commentary.html
[69] ___; *Citrix MetaFrame XP Administrators Guide*; 2002; Citrix; http://www.citrix.com/
[70] ___; *Citrix MetaFrame XP Evaluator's Guide*; 2002; Citrix; http://www.citrix.com/
[71] ___; *Citrix Secure Gateway for Windows version 1.1 Administrator's Guide*; 2002; Citrix; http://www.citrix.com/
[72] ___; *Citrix MetaFrame XP Application Server for Windows Overview Guide*; 2002; Citrix; http://www.citrix.com/
[73] ___; *Check Point Application Ingelligence*; 2003; Check Point Software Technologies, Ltd.; http://www.checkpoint.com/products/downloads/applicationintelligence_whitepaper.pdf
[74] ___; *Cisco PIX Firewall Software, Introduction*; 2003; Cisco Systems, Inc.; http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_43/config/pix43int.pdf
[75] Mike DeMaria*; Defense Starts Here*; 20/2-2003; Network Computing; http://www.networkcomputing.com/1403/1403f3.html
[76] Krishni Naidu; *Firewall Checklist*; 2003; SANS; http://www.sans.org/score/checklists/FirewallChecklist.pdf
[77] ___; *Public Key Infrastructure – Securing the future of communication*; 2000; Rainbow Technologies, Inc.; htp://www.rainbow.com/library/8/pki_paper.pdf
[78] ___; *Two-Factor Authentication – Making sense of all the options*; 2003; Rainbow Technologies, Inc.; htp://www.rainbow.com/library/8/2fao-v52.pdf
[79] Lucky225; *ANI and Caller ID spoofing*; 2003, vol. 20 nr. 1; 2600 Enterprises, Inc.; ISSN 0749-3851
[80] ___; CSIRT-*DK servicebeskrivelse (RFC-2350)*; 1999; CSIRT-DK; http://download.opasia.dk/pub/zillion/csirt/csirt-dk.txt
[81] ___; *10 hurtigere overvejelser inden etablering af hjemmearbejdspladser*; 29/8-2000; CSIRT-DK; http://erhverv.tdc.dk/nyhedsbreve/csirt/artikel.php?id=39349

[82] Ministeriet for Videnskab, Teknologi og Udvikling i samarbejde med Bech-Bruun Dragsted Advokatfirma; *Vejledning om hjemmearbejdspladser*; 2003; Ministeriet for Videnskab, Teknologi og Udvikling; http://www.videnskabsministeriet.dk/fsk/div/itsoejlen/hjemmepc.pdf
[83] British Standards Institution og Joint Technical Committee ISO/IEC JTC 1; *Information Technology – Code of practice for information security management (ISO 17799:2000)*; 2001; British Standards Institution; ___
[84] ___; *ICSA Labs Product Certification Goals and Generic Criteria*; ___; TruSecure Corp.; http://www.icsalabs.com/html/certification/index.shtml
[85] ___; *Common Criteria for Information Technology Security Evaluation v. 2.1*; 1999; Common Criteria; http://www.commoncriteria.org/docs/PDF/CCPART1V21.PDF, CCPART2V21.PDF samt CCPART3V21.PDF
[86] ___; *Common Criteria – An Introduction*; 1999; Common Criteria; http://www.commoncriteria.org/introductory_overviews/CCIntroduction.pdf
[87] Datatilsynet; *Persondataloven*; Juli 2002; Datatilsynet; 87-601-8839-1
[88] ___; *Anti-terrorpakken*; 31/5-2002; Center for Journalistisk og Efteruddannelse; http://www.cfje.dk/cfje/Lovbasen.nsf/ID/LB02947821?OpenDocument
[89] Lawrence R. Halme, R. Kenneth Bauer; *AINT Misbehaving: A Taxonomy of Anti-Intrusion Techniques*; ___; SANS; http://www.sans.org/resources/idfaq/aint.php
[90] Alf Vester; Sikring *af hjemmearbejdspladser på AlmaFrontal Aps*; 2000; CSIRT-DK; ___
[91] Lance Spitzner; *Honeypots – definitions and value of honeypots*; 2003; spitzner.net; http://www.spitzner.net/honeypots.html
[92] ___; *Symantec Decoy Server*; 2003; Symantec; http://enterprisesecurity.symantec.com/content/displaypdf.cfm?pdfid=292
[93] Alison Cawsey; *Databases and artificial intelligence*; 1994; ___; http://www.cee.hw.ac.uk/~alison/ai3notes/all.html
[94] Hany I. Fahmy, Christos Douligeris; *Applications of hybrid fuzzy expert systems in computer networks design*; 1999; European Symposium on Intelligent Techniques; http://www.erudit.de/erudit/events/esit99/12529_p.pdf
[95] ___; *The OSI Model's Seven Layers Defined and Functions Explained*; 2002; Microsoft Corp.; http://support.microsoft.com/default.aspx?scid=kb;en-us;103884
[96] Grant Wilson; *OSI Model Layers*; 2001; ___; http://www.geocities.com/SiliconValley/Monitor/3131/ne/osimodel.html
[97] ___; *Medium Access Control*; Brighton University; http://burks.brighton.ac.uk/burks/pcinfo/hardware/ethernet/mac.htm
[98] Yin Zhang; *Detecting Backdoors*; 2000; i.c.s.i. center for internet research; http://www.icir.org/vern/papers/backdoor/
[99] Grandmaster Plaque; *Getting into Cisco Routers*; 2002, vol. 19, nr. 2; 2600 Enterprises, Inc.; ISSN 0749-3851
[100] ___; CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks; 2000; CERT; http://www.cert.org/advisories/CA-1996-21.html
[101] Nikolaj Worm; *Effektivitet på hjemmebanen – Morgenavisen Jyllands-Posten, Job & Karriere*; 16/4-2003; Jyllands-Posten A/S; ___
[102] ___; *Sikkerhedsregler ved brug af fjernadgang til Risø*; ___; Forskningscenter Risø; ___
[103] Erik Kristensen (redaktør); *Risøs edb-sikkerhed*; 29/5-2001; Forskningscenter Risø; ___
[104] ___; *Politik for Hjemmearbejdspladser i xx-ministeriet*; 18/12-2002; unavngivet ministerie (xx); ___
[105] ___; *Home LAN policy*; ___; Microsoft Corp.; ___
[106] Jens Houmann; *Dataforbindelser til Risø fra hjemmearbejdspladser m.m.*; Marts 2003; Forskningscenter Risø; ___
[107] ___; Firewall White Paper – What different types of firewalls are there?; ___; ViComSoft; http://www.firewall-software.com/firewall_white_paper.html
[108] ___; *Next generation security... Localtion based PC Lock*; Dec. 2002; BluePosition; Dokument ID PS-BLIS4-WSL-18
[109] FBI National Press Office; *FBI Says Web "Spoofing" Scams are a Growing Problem*; 21/7-2003; FBI's Internet Fraud Complaint Center; http://www.fbi.gov/pressrel/pressrel03/spoofing072103.htm
[110] Daniel Oxenhandler; *Designing a secure local area network*; 2003; SANS Institute; http://www.sans.org/rr/paper.php?id=853
[111] Nathan Lasnoski; Creating a secure VPN with Cisco Concentrator and ACE Radius/SecurID; 3/6-2002; SANS Institute; http://www.sans.org/rr/paper.php?id=767
[112] ___; *Securing the enterprise through the small office*; Maj 2002; Nokia; http://www.nokia.com/ipsecurity/pdf/SmallOfficeWP.pdf
[113] ___; Combining *Network Intrusion Detection with firewalls for mazimum perimeter protection*; April 2001; Nokia; http://www.nokia.com/ipsecurity/pdf/Combining_IDS_with_Firewall_WP.pdf
[114] ___; *Chief Magazine, Comparison Chart*; 2003; Chief Group; http://www.marketing.co.il/magazine/2003/10/NITI/comparison_chart.htm
[115] ___; *Webster's New Worlds Dictionary of the American Language, College Edition*; 1962; The World Publishing Company; ___;

KONTAKTPERSONER

	Navn	Titel	Virksomhed	Kontaktinformation
[116]	Kristina Tranders		IT Sikkerhedskontoret, IT & Telestyrelsen	Tel: 35450211 (direkte)
[117]	Henning Rogren	Area Manager - Nordic, Baltic & Russia	Efficient Networks Nordic	E-mail: hrogren@efficient.com
[118]	Søren Gantzel Markussen	Salgskonsulent	TDC Erhverv	E-mail: Soeren.Gantzel.Markussen@tdcinternet.dk
[119]	Trent R. Berghofer	IT Account Manager Northern Europe	Microsoft, Operations and Technology Group	E-mail: trentbe@microsoft.com Tel: +46 (8) 752 28 31
[120]	Torben B. Sørensen	Journalist	DK-CERT	E-mail: torben.b.sorensen@uni-c.dk Tel: 35 87 88 23
[121]	Henrik Bønnelykke	Cisco Systems Engineer	Cisco Systems Danmark	Tel: 40 40 57 01
[122]	Peter Nygaard		Dansk Standard	Tel: 39 96 61 01