ICT 4

Ontwerpen van netwerken

Beheer

Willem Brouwer

Doorreizen

Als je de praktijkopdracht in paragraaf 3 van dit hoofdstuk naar tevredenheid hebt gemaakt, kun je na overleg met je docent doorgaan naar het volgende hoofdstuk.

Inleiding technisch ontwerp

4.1 Inleiding

In het vorige hoofdstuk hebben we gekeken naar de functionele eisen die aan netwerken worden gesteld en de consequenties die deze kunnen hebben voor het ontwerp. Vanuit business requirements wordt een ontwerp gemaakt dat voor de klant bruikbaar is. In dit stadium gaan we nader in op de keuze van de apparatuur en enkele bijkomende aspecten, die zeker niet minder belangrijk zijn. Deze fase kun je zien als de start van het technisch ontwerp van het netwerk.

Index

4.2 Aanwijzingen voor de leerling

Een ontwerp is in vele stappen onder te verdelen. We noemen een indeling in verschillende (opeenvolgende) stappen of fasen een fasering. Jammer genoeg is ook de fasering zelf vaak onderwerp van discussie. Er zijn verschillende wijzen waarop een ontwikkeltraject gefaseerd kan worden. In paragraaf 3.5 is de watervalmethode besproken. Bij de hier gebruikte fasering komen de volgende aspecten aan de orde:

- infrastructuur:
  - bekabeling etc.
  - netwerk en computerkenmerken
  - actieve netwerkcomponenten

- hardware:
  - printerkeuze
  - computer(kenmerken)
  - randapparatuur
  - overige apparatuur

- software:
  - standaardsoftware
  - maatwerksoftware

- overige:
  - beveiliging
  - performance en reliability
  - overige

- financiën:
  - TCO, ROI en afschrijven
  - de 10% regel

- logistiek:

- het inrichtingsplan

4.3 Praktijkopdracht

Je werkt bij een bedrijf dat complete netwerken ontwerpt en installeert. De laatste tijd gaan er regelmatig orders aan jullie neus voorbij. Daarom krijgt een extern bureau het verzoek om afgehaakte klanten te inter-

viewen. Veel van deze klanten melden dat ze ontevreden zijn over de kwaliteit van het ontwerp. Ze hebben niet het idee dat het ontwerp speciaal voor hen is gemaakt. De indruk bestaat dat er een soort 'generiek ontwerp' uit de kast is gehaald waar de naam van het bedrijf voor de vorm boven is getikt.

Jou is gevraagd een checklist te ontwerpen die gebruikt kan worden om een netwerkontwerp te screenen en te beoordelen. De bedoeling is dat op deze wijze de ontwerpen weer van een niveau worden dat er geen klanten meer vertrekken.

4.4 Keuzes in het technisch ontwerp

Bij het opzetten van een **functioneel ontwerp** moeten enkele technische keuzes gemaakt worden, die – omdat ze rechtstreeks uit de gewenste functionaliteit volgen – in het FNO uitgewerkt moeten worden.

Een voorbeeld is de keuze van de **bekabeling**: daarvan moeten aspecten als kabeltype en topologie vastgelegd worden. Dit in relatie tot het gebouw waar het netwerk gerealiseerd moet worden. Vanwege fysieke beperkingen kan niet in elk gebouw een wireless LAN gerealiseerd worden. Het lijkt misschien alsof tegenwoordig elk netwerk een cat 5 UTP-bekabeling heeft en als protocol TCP/IP gebruikt. Bij een ontwerp hoort een zorgvuldige afweging of dit wel de verstandigste en juiste keuze is. Veel problemen met bijvoorbeeld de prestaties van een netwerk worden veroorzaakt doordat vaak maar 'voor een UTP Ethernet-netwerk met TCP/IP' wordt gekozen zonder dat een goede afweging is gemaakt. In sommige gevallen kan het ontbreken van een gegarandeerde Quality of Service er de oorzaak van zijn dat de prestaties van zo'n netwerk onvoldoende zijn. Een Token Ring netwerk (dat wel een maximale responstijd kan garanderen) kan dan een betere keuze zijn.

Met betrekking tot de **bandbreedte** wordt vaak een even snelle en ondoordachte keuze gemaakt. "Laten we maar 100 Mb doen." Dit kan grote problemen veroorzaken, omdat als gevolg van het CSMA/CD-principe, één verbinding de bandbreedte kan monopoliseren. De gevolgen hiervan kunnen op de langere duur funest zijn.

Gekoppeld aan deze keuze van protocollen, topologie en bandbreedte is die van de bekabeling, die we hierboven al even genoemd hebben. Deze betreft zowel het type bekabeling als een onderzoek naar de fysieke mogelijkheden van het pand. Is het raadzaam om UTP te kiezen, en zo ja, welk

type? Kunnen we beter glasvezel gebruiken? Of misschien nog iets anders? Kunnen er kabelgoten gebruikt worden? Is er een handig systeemplafond waarachter kabels weggewerkt kunnen worden? Vaak zijn er allerlei beperkingen waarmee rekening gehouden moet worden. In een pand dat op de monumentenlijst staat, kunnen niet zomaar overal doorgangen gemaakt worden. Ook bij niet al te grote netwerken is het vaak verstandig om een centrale plaats te kiezen als centrum voor het netwerk, daar een 19 inch kast neer te zetten en daar ook alle kabels te concentreren.

Ook worden netwerken soms aangelegd op plaatsen met een verhoogde kans op storingen. Dan moet er voor een ander bekabelingstype of voor extra afgeschermde kabels worden gekozen. Netwerken worden nu eenmaal ook aangelegd op plaatsen waar extreme omstandigheden heersen: in een chemische fabriek worden bijvoorbeeld ook computers gebruikt. Er is apparatuur op de markt die daarop speciaal is voorbereid. Daarmee moet in een ontwerp rekening gehouden worden.

De keuze voor een bekabelingstype kan tegenwoordig ook een keuze voor een **draadloos** netwerk zijn (**wifi**). Bedenk wel dat zich daarmee dan weer dezelfde problemen kunnen voordoen. Ook draadloos verkeer kan onder bepaalde omstandigheden verstoord worden. In sommige kantoorpanden zijn bijvoorbeeld de systeemwanden van metaal. Voor het toepassen van een draadloos netwerk moet in dat geval gerekend worden op één **Service Access Point** (SAP) per ruimte. Dat maakt het netwerk duur, maar erger is dat daar weer veel kabels voor nodig zijn, en dat was juist het probleem! Ook kan de ontvangst sterk verstoord worden door elektromagnetische straling uit een andere bron. Bepaalde elektrische apparaten produceren een grote hoeveelheid straling.

Het ontwikkelen van het informatiesysteem en het functionele ontwerp van het netwerk.	HET DOCUMENTEER-PROCES
De benodigde en gewenste architectuur van het netwerk.	
De hardware die nodig is om de gewenste functionaliteit te garanderen.	
De benodigde (systeem)software.	
Het realiseren van de gewenste functionaliteit.	
Het praktische gebruik.	
Het beheer en de beheerorganisatie.	

Index

draadloos
wifi
Service Access Point

Index

server
RAID
beschikbaarheid
fault recovery
opslagcapaciteit
werkstation
apparatuur

Assist

Bij RAID (Redundant Array of Inexpensive Disks) wordt de data over meerdere schijven verdeeld. Dit gaat op een manier waarbij het meestal mogelijk is om, als een van de schijven het begeeft, de data 'on the fly' te herstellen.

4.4.1 Servers

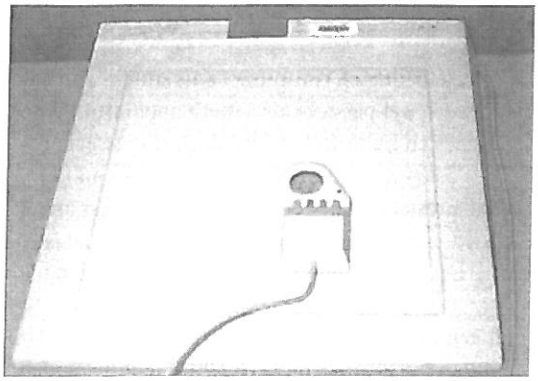
Voor een netwerk van pc-achtige machines moeten meerdere typen computers geselecteerd worden. Voor elke **server** moet zorgvuldig worden afgewogen aan welke kenmerken deze moet voldoen. Specificaties van high-end servers zijn fors en het zijn dure systemen. Systemen met 265 GB intern geheugen, schijfeenheden in de Terabytes en twee of vier processors zijn niet ongebruikelijk. Deze schijfsystemen zijn dan bijna altijd van het type **RAID**. De juiste keuzes qua benodigde snelheid, functionaliteit en betrouwbaarheid dragen bij tot een netwerk dat een voordeel op de concurrentie oplevert. Een beter toegesneden netwerk zal voor een efficiëntere uitvoering van de primaire processen van de klant zorgen.

Bij dergelijke systemen is aan elk onderdeel aandacht besteed om de **beschikbaarheid** ('availability') te maximaliseren. Het geheugen is van een error correction type, de voeding is zowel overgedimensioneerd als dubbel uitgevoerd. In de keuze van dit systeem is meegenomen welke operationele eisen er worden gesteld. Ongetwijfeld zal in een netwerk van een beetje afmeting een vorm van netwerkmanagement worden geïmplementeerd (SNMP-1, 2, 3 of nog een ander protocol). Ook dient aandacht aan **fault recovery** (op serverniveau) besteed te worden. Kiest men voor duplexing, mirroring, een RAID-oplossing of zelfs een combinatie met file server duplexing? Ook over de **opslagcapaciteit** (nu en in de toekomst) van het serverpark moet nagedacht worden. Hoe lang kan de aanbevolen configuratie nog mee en wanneer is er naar verwachting een (hardwarematige) upgrade nodig? Als dat binnen twee maanden is, dan lijkt er sprake van een ontwerpfout. Een serieuze analyse van de databehoefte is een absolute noodzaak.

4.4.2 Werkstations

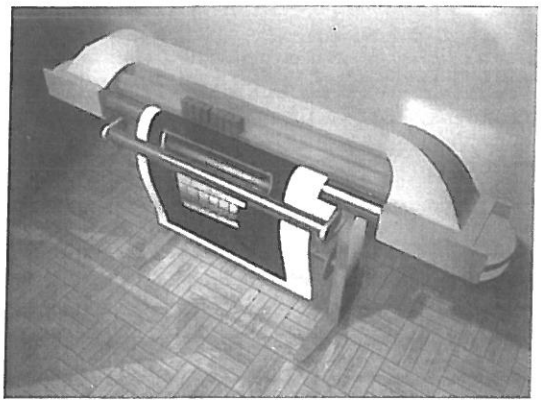
Naast een of meer servers heeft een netwerk ook gebruikersstations. In de meeste netwerken kan niet met één keuze voor een **werkstation** volstaan worden; dit is sterk afhankelijk van de situatie. Een call centre met 300 werkstations zal een hoge mate van standaardisatie wensen. Daar is misschien alleen een apart station voor de beheerder en een aparte configuratie voor de administratieve stations nodig. Bij een ingenieursbureau zal veel minder standaardisatie in hardware, software en configuratie noodzakelijk of gewenst zijn. In een studie naar benodigde **apparatuur** hoort een onderzoek naar extra eisen en wensen ten aanzien van die apparatuur.

Index



Figuur 4.1 Digitizer.

CAD-ontwerpers gebruiken bijvoorbeeld vaak zeer specialistische apparatuur (zoals high tech scanners, A0-plotters en digitizers). Ondersteuning voor dit soort apparatuur is een vereiste in een netwerk dat voor dergelijke klanten wordt ontworpen. Vaak vindt een klant het heel vanzelfsprekend dat bekend is dat men bepaalde apparatuur heeft en wil blijven gebruiken, terwijl de netwerkleverancier daar pas later achter komt. Als daar in het ontwerp geen rekening mee gehouden is, kan dit ertoe leiden dat deze apparatuur niet gebruikt kan worden (omdat bijvoorbeeld de hardware-ondersteuning niet te realiseren is, of de drivers incompatible zijn met het gekozen operating system op de desktop). Een zorgvuldige inventarisatie en analyse van de benodigde apparatuur, zowel de al aanwezige als de nieuw aan te schaffen, is dus een vereiste voordat keuzes gemaakt kunnen worden.



Figuur 4.2 A0-plotter.

Index

topologie
functioneel netwerkontwerp
structuur van het netwerk

4.5 Topologie en structuur

Het netwerk omvat behalve bekabeling en computers ook andere apparatuur. Daarin onderscheiden we zowel passieve als actieve apparatuur. Voor de hand liggen routers, switches en hubs. In het **functioneel netwerkontwerp** worden de specificaties daarvan vastgelegd. De **structuur van het netwerk** is essentieel voor de prestaties van het geheel. Het netwerk moet een logische structuur hebben en er moet nagedacht zijn over de datastromen. Een juiste dimensionering van de apparatuur is van groot belang.

Vaak kan een netwerk met een uitgekiend logisch ontwerp tot veel grotere prestaties worden gebracht dan oorspronkelijk verwacht. We moeten dan denken aan zaken als beschikbare bandbreedte, de verdeling ervan en het opdelen in segmenten. De netwerkleveranciers die denken dat je een netwerk alleen sneller kunt maken door van 100 Mb naar 1000 Mb over te stappen, leveren niet altijd 'value for money'.

In deze fase van het ontwerp is het ook goed om nogmaals naar de eventuele inherente (on)betrouwbaarheid van het ontwerp te kijken. Dit moet eigenlijk al in het functioneel netwerkontwerp aan de orde zijn geweest, maar in dit stadium zijn er regelmatig nog makkelijk te vermijden 'single points of failures' in het netwerk aan te wijzen. Vaak is met een eenvoudige ingreep een stabieler netwerk te creëren, bijvoorbeeld door een verbinding redundant uit te voeren of een centraal knooppunt twee keer te realiseren en op deze wijze voor een fall-back te zorgen (qua verbinding).

Het ontwikkelen van het informatiesysteem en het functionele ontwerp van het netwerk.	HET DOCUMENTEER-PROCES
De benodigde en gewenste architectuur van het netwerk.	
De hardware die nodig is om de gewenste functionaliteit te garanderen.	
De benodigde (systeem)software.	
Het realiseren van de gewenste functionaliteit.	
Het praktische gebruik.	
Het beheer en de beheerorganisatie.	

4.6 Printers

In ieder netwerkontwerp vormen één of meer **printers** uiteraard een verplicht onderdeel. Er bestaan netwerken die alleen zijn aangelegd om printers te delen! De aanschaf en installatie van allemaal stand-alone printers op even zovele computers is meestal veel duurder en inefficiënter dan enkele grote bulkprinters en eventueel nog een handvol special purpose printers.

Met printers kan echter ook veel misgaan; vaak wordt er een verkeerde inschatting van de situatie gemaakt. Vraag aan een manager van een bedrijf waar een netwerk geïmplementeerd gaat worden, om aan te geven hoeveel afdrukken hij denkt te gaan maken. De kans is dan groot dat hij zijn antwoord baseert op de bestaande situatie. Dat lijkt vrij logisch, maar de praktijk wijst uit dat een netwerk ook zijn eigen printbehoefte schept. Het is een lastige zaak om in te schatten:

- Hoeveel afdrukken worden er nu gemaakt?
- Hoeveel afdrukken worden er straks (direct na implementatie) gemaakt?
- Hoeveel afdrukken worden er over drie jaar gemaakt?
- Hoeveel printers zijn er nodig en hoe moeten die verdeeld worden over het netwerk?
- Is er een inschatting gemaakt van minimale, maximale en gemiddelde wachttijd op een afdruk?
- Is de hoeveelheid (extra) dataverkeer die printen oplevert in de dimensionering, qua hoeveelheid en qua tijdigheid, meegenomen? (Printen genereert erg veel data; veelal wordt alles grafisch, als bitmap, naar de netwerkprinter gestuurd.)
- Welke eisen moeten er aan de printer(s) worden gesteld?
  - afdruksnelheid;
  - kleur of zwart/wit (inkjet of laser);
  - resolutie;
  - kosten per pagina;
  - etc.

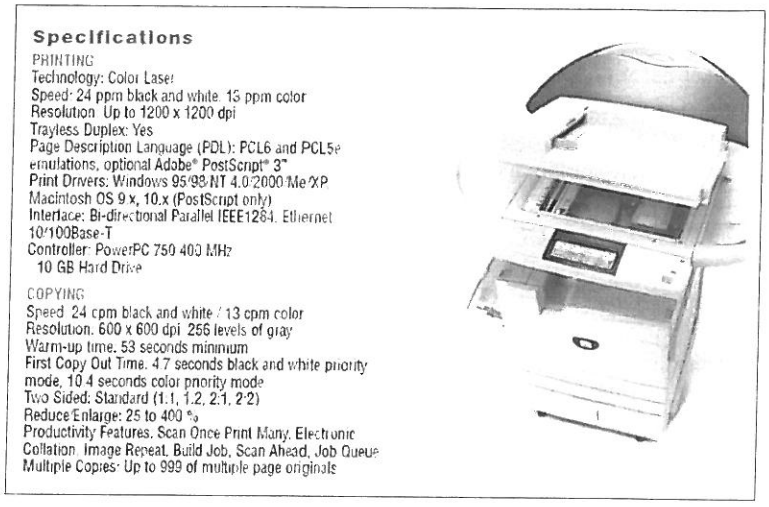
Tegenwoordig kan vaak voor een combinatie van een fotokopieermachine en een printer worden gekozen. Deze apparaten fungeren dan als (snelle) printer en met deze keuze wordt één apparaat uitgespaard. Alle grote kopieermachineleveranciers voorzien in de optie hun kopieermachine als netwerkprinter aan te sluiten.

Index

printers

Assist

Denk bij special purpose printers aan bijvoorbeeld een (bulk)kleurenlaserprinter om bepaalde mailings snel en efficiënt te kunnen printen, of aan een enkele A3 (of nog groter) printer. Ook kun je denken aan Printing On Demand, waarbij vanuit een computer een fotokopieerapparaat in het netwerk wordt aangestuurd.



Figuur 4.3 De Xerox workcentre M24, die ook faxt en scant.

Op basis van onderzoek kan uiteindelijk een keuze voor een of meer typen printers worden gemaakt en deze kan in het netwerkontwerp verder uitgewerkt worden.

4.7 Beveiliging

Het begrip **beveiliging** van een netwerk kent verschillende invalshoeken:
- **Externe beveiliging**: wie of wat zal het netwerk van buitenaf bedreigen?
- **Interne beveiliging**: welke gebruikers mogen wat (niet)? Maar ook: hoe ga je om met onbetrouwbaar of vertrekkend personeel?

4.7.1 Externe beveiliging

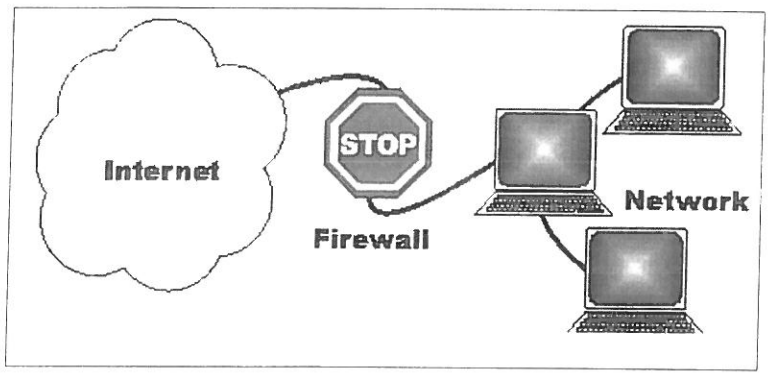
Netwerken worden bedreigd door **hackers** en **crackers**. Vaak geldt als onderscheid tussen deze twee groepen dat hackers als doel hebben de onveiligheid van een netwerk aan te tonen, terwijl crackers kwade bedoelingen hebben. Beide categorieën zijn echter vanuit het oogpunt van netwerkbeheer ongewenst. Als er een continue internetverbinding is, loopt een bedrijf veel risico.

Doorgaans wordt er tegen indringers van buitenaf een **firewall** in het netwerk opgenomen. Er is een divers aanbod; meestal gaat het om op UNIX

gebaseerde systemen die veel configuratie-opties hebben. Er zijn drie basic firewall-systemen:

- **Packet filtering** – Pakketten (IP en TCP) worden op basis van een set regels ('rules') gefilterd.
- *Firewalls op applicatieniveau* – Deze kunnen bijvoorbeeld FTP of HTTP blokkeren of filteren.
- **Proxy service** – Informatie wordt door de firewall van het internet gehaald en dan door de proxy naar de client gezonden. Voor de buitenwereld lijkt het alsof alle verkeer van en naar de proxy komt/gaat. De client-systemen lijken voor de buitenwereld niet te bestaan.

Veelgebruikt zijn **iptables** en **ipchains**. Beide zijn open source software en zijn perfect geschikt om op een Linux machine te draaien.



Figuur 4.4 Firewall.

Mogelijkheden van firewalls

Filters kunnen gemaakt worden op basis van:

1. IP-adressen
2. domeinnamen
3. protocollen
4. ports
5. specifieke tekst

Over protocollen, ports en specifieke tekst geven we hieronder nadere informatie.

Protocollen

De volgende **protocollen** zijn de meest gebruikte (en meest gefilterde):

- **IP** (Internet Protocol): het belangrijkste onderliggende protocol;
- **TCP** (Transport Control Protocol): het centrale protocol;

Index

packet filtering
proxy service
iptables
ipchains
filter
protocollen
IP
TCP

Knipsel

Een proxy is in het Engelse rechtssysteem iemand die voor iemand anders (in plaats van...) optreedt.

- **UDP** (User Datagram Protocol);
- **HTTP** (Hyper Text Transfer Protocol);
- **FTP** (File Transfer Protocol);
- **ICMP** (Internet Control Message Protocol): onder andere gebruikt om informatie tussen routers uit te wisselen;
- **SMTP** (Simple Mail Transport Protocol): gebruikt om e-mail tussen hosts uit te wisselen;
- **SNMP** (Simple Network Management Protocol): gebruikt om systeeminformatie van gebruikte apparatuur te verzamelen;
- **Telnet**: om in te kunnen loggen op (remote) systemen.

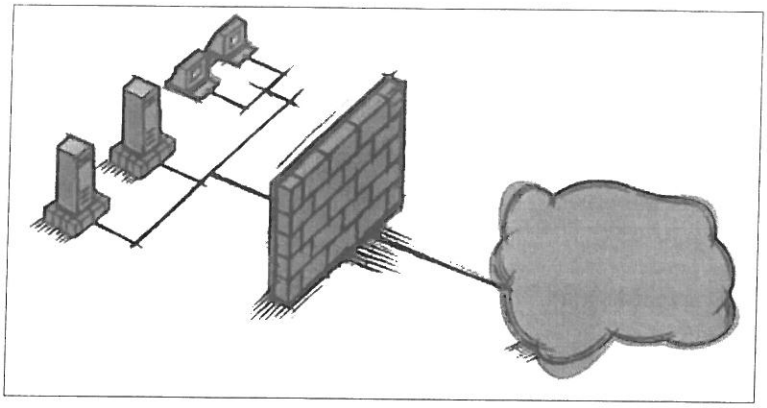
Ports

Elke machine stelt via genummerde **poorten** zijn services beschikbaar op het internet, één voor elke service:

- De **webserver** (HTTP) zit meestal op poort 80.
- De **FTP-server** zit op poort 21.

Specifieke tekst

De firewall zal door elk pakket heen zoeken naar het voorkomen van bepaalde tekst. Je kunt een firewall 'vertellen' dat elk pakket met de term "X-rated" geblokkeerd moet worden. Het "X-rated"-filter zal niet reageren op "X rated" (zonder koppelteken). Maar je kunt dan weer een "X rated"-filter toevoegen. Virusscanners gebruiken meestal deze methode om 'virushandtekeningen' te 'zoeken'.



Figuur 4.5 Scheiding tussen netwerk en internet.

Er zijn ook firewalls die je op een enkele pc kunt gebruiken. In een netwerk verdient het aanbeveling deze beveiliging centraal te regelen.

Beveiliging op werkstations kan door gebruikers vaak gewoon uitgezet worden (en dat doen veel mensen ook omdat het als 'lastig' of vertragend wordt ervaren).

Bedreigingen

Een firewall beschermt dus tegen bedreigingen van buitenaf. Wat zijn nu die **externe bedreigingen** waartegen beveiligd moet worden? **Hackers** en **crackers** maken gebruik van een aantal methoden om de integriteit van een netwerk of systeem te ondermijnen. Niet tegen alle methoden kan een firewall bescherming bieden, maar tegen een aantal wel:

- **Remote login**: een poging om vanaf een ander station in te loggen en het beheer van een server over te nemen.
- **Application backdoors:** sommige programma's hebben een functionaliteit die remote access mogelijk maakt.
- **SMTP session hijacking**: SMTP is een bron van mogelijke bedreigingen. Buiten wat foutjes in oudere versies, die toegang tot het root account mogelijk maakten, is er ook bij slecht geconfigureerde mailservers een risico dat deze gebruikt kunnen worden om junkmail (**spam**) naar duizenden gebruikers te sturen.
- **Operating system bugs**: net als applicaties hebben sommige operating systems zogenoemde 'backdoors' met onvoldoende security, of zijn er bugs. De beruchte **ping of death** is hiervan een voorbeeld.
- **Denial of Service** (DoS): een dergelijke aanval belast een server zo met 'werk' dat hij aan zijn eigen werk niet meer toekomt. Een veelgebruikte methode is om een verbinding maar half te openen. (De three way handshake wordt niet afgemaakt.) Door dit vele malen te doen 'loopt de server uit zijn resources' en is deze praktisch onbenaderbaar.
- **Distributed Denial of Service** (DDoS): deze variant op de voorgaande zorgt er eerst voor dat er op veel plaatsen agents zijn die meedoen aan Denial of Service. Op deze wijze kan via relatief trage verbindingen toch een succesvolle aanval worden opgezet.
- **E-mailbommen**: een **e-mailbom** is meestal een aanval op een persoon, maar deze kan ook tegen een organisatie worden ingezet. (E-mail)virusgolven beginnen het karakter van een e-mailbom te krijgen. Bij recente uitbraken verspreidde een virus zich soms zo snel dat SMTP-servers onder het verkeer bezweken.
- **Macro's**: gezien de vele **macrovirussen** die de Office-suite van Microsoft de afgelopen jaren heeft 'gegenereerd' is het niet nodig hier nader op in te gaan. Een firewall kan hiertegen soms iets ondernemen.
- **Virussen**: een aantal firewall-producten is in staat om dataverkeer op **virussen** te scannen.

Index

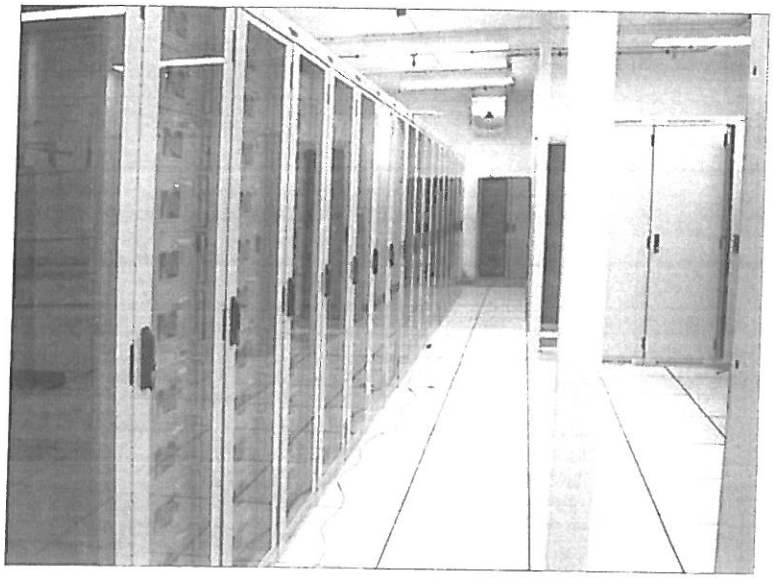
- **Spam**: op basis van verzendadres of andere specifieke eigenschappen kan een firewall e-mailverkeer filteren. Op deze manier is **spam** tegen te gaan.
- **Redirect bombs**: ICMP kan gebruikt worden om informatie over de te volgen route te wijzigen ('redirect'). Dit is een van de manieren waarop een DoS-attack is te arrangeren.
- **Source routing**: in de meeste gevallen wordt de route van TCP/IP-verkeer bepaald door de ontvangende host. De makkelijkste en/of snelste weg om die te bereiken, wordt gekozen. Bij **source routing** wordt de route echter door het verzendende station bepaald. Op deze wijze kan voor een bepaald type verkeer een route worden afgedwongen. Uit veiligheidsoverwegingen kan dit soms de voorkeur hebben. Op deze wijze kan bijvoorbeeld ook een hacker zijn verkeer zo maskeren dat het lijkt alsof het ergens anders vandaan komt. Firewalls zetten source routing meestal standaard uit.

Sommige van de genoemde bedreigingen zijn door een firewall niet of nauwelijks te onderscheppen. Bepaalde firewalls zijn in staat een aantal virussen tegen te houden, maar het blijft verstandig om ook virusscanners te gebruiken. Spam is vervelend, maar de enige manier om er echt van af te komen is geen e-mail meer toe te staan. Maar dat wil vrijwel niemand. Overigens wordt met **heuristic scanning** de laatste tijd een redelijk resultaat bereikt. De graad van beveiliging die je kunt bereiken, is altijd een afweging tussen de functionaliteit en de veiligheid. Een perfect veilig netwerk laat geen enkel verkeer door.

De meest gebruikte strategie bij het bouwen van een firewall is om in eerste instantie alles te blokkeren, en vervolgens stapje voor stapje open te zetten wat je wel wilt.

4.7.2 Interne beveiliging

Ook aan de interne veiligheid moet aandacht worden geschonken: aan het onderscheid in verschillende gebruikersgroepen en daaraan gekoppelde rechten. Wie kan en mag wat op welke plaats? In een Windows omgeving kan met 'policies' worden gewerkt. Ook met Novell NetWare als serverplatform kan een standaard policy worden ingesteld en kan desgewenst met een 'roaming profile' worden gewerkt. Dit geheel wordt in een **netwerkautorisatieplan** gedocumenteerd en vastgelegd. Dit maakt deel uit van de systeemdocumentatie.



Figuur 4.6 Serverruimte.

Vaak gaan organisaties ervan uit dat bedreigingen van buitenaf komen, maar lang niet altijd is dat het geval. In de praktijk blijken veel netwerkaanvallen een oorzaak en oorsprong binnen de organisatie te hebben. Het gebruik van een firewall om intern verkeer te regelen is vaak geen overbodige luxe. Ook een fysieke beveiliging tegen interne bedreigingen is een goed idee. Denk hierbij aan de volgende maatregelen:

- Serverruimten moeten alleen voor bevoegd personeel toegankelijk zijn.
- Kabels moeten weggewerkt zijn.
- Het dataverkeer moet ook binnen het netwerk versleuteld worden; geen onversleutelde (draadloze) verbinding die afgeluisterd kan worden.
- Niemand moet meer rechten krijgen dan nodig of functioneel is.
- Er moet sprake zijn van een goed **wachtwoordbeleid**. Bij vertrek van een werknemer moeten zeker de cruciale wachtwoorden worden gewijzigd. Dit geldt ook (juist) als iemand zonder ruzie of meningsverschillen weggaat.

Index

wachtwoordbeleid

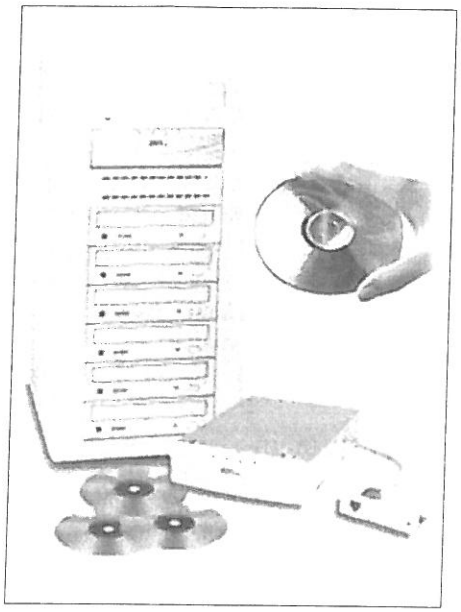
bulletin board system
modem
cd-romserver

Figuur 4.7 Een artikel uit BusinessWeek.

4.8 Overige randapparatuur

Allerlei andere apparatuur kan nog nodig zijn. Een paar voorbeelden:

- *Modems.* Sommige leveranciers hebben nog steeds voor supportdoeleinden een **bulletin board system**. Om dit te bereiken is een **modem** nodig. Modems kunnen centraal via een modem- of communicatieserver aan de gebruikers ter beschikking gesteld worden.
- *Fax-apparaten* zijn vaak op het netwerk aan te sluiten. Dan kan er gefaxt worden en kunnen binnenkomende faxberichten via het netwerk verspreid worden.
- *Fotokopieermachines* zijn vaak als printer in een (groot) netwerk opgenomen.
- *Specialistische apparatuur.* Bij bepaalde bedrijven is specialistische apparatuur in gebruik. Dat kan gaan om speciale afdrukapparatuur bij grafische bedrijven, maar ook om bijvoorbeeld apparatuur waarop vanuit een printontwerpprogramma gelijk de printplaat wordt gemaakt. Ook kan er bijvoorbeeld een draai- of freesbank zijn gekoppeld om in één keer een prototype te kunnen vervaardigen.
- **Cd-romservers** kunnen meerdere (tientallen) cd's (en dvd's) ter beschikking stellen. Vaak vereisen ze een aparte configuratie.



Figuur 4.8 Cd-romserver.

Zo kan het zijn dat er nog allerlei apparatuur in het netwerk opgenomen moet worden, die apart aandacht behoeft.

4.9 Performance en reliability

Netwerkperformance kan naar drie deelgebieden onderscheiden worden:

1. Performance van de applicaties.
2. Performance op netwerkniveau (lagenmodel, netwerklaag, routers, protocollen, efficiëntie).
3. Performance van de infrastructuur (bekabeling, datalinklaag).

Eigenlijk zou het niet nodig moeten zijn om **performance** als apart item te behandelen. In een weldoordacht netwerkontwerp is uiteraard rekening gehouden met een optimale performance. Het is echter aan te bevelen om wel apart aandacht aan performance te schenken. Onder een kopje als dit kun je aangeven waarom server(s), clients en overige apparatuur in een netwerk optimaal presteren en welke maatregelen zijn genomen om dit te bereiken. Wat kan er eventueel gedaan worden om dat te verbeteren? En – heel belangrijk – wat heeft dit te maken met de oorspronkelijke wensen en verwachtingen van de toekomstige gebruikers en de opdrachtgever?

Index

Index

betrouwbaarheid
beschikbaarheid
netwerk, kosten
Total Cost of Ownership
TCO

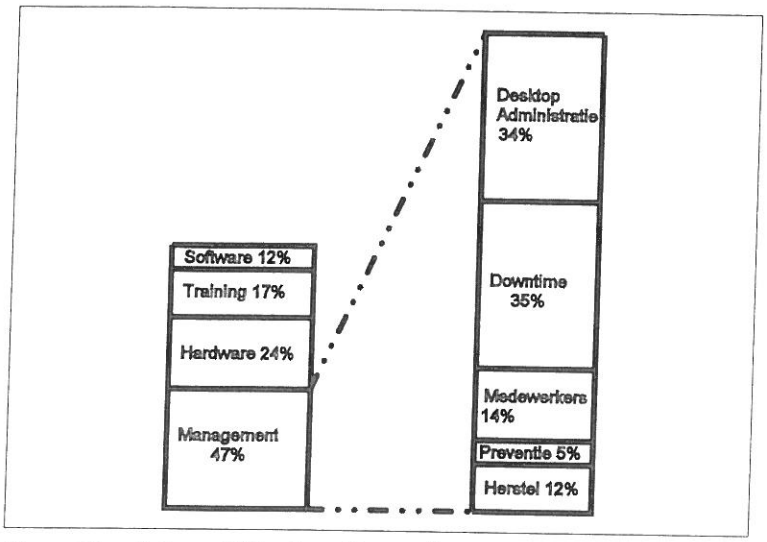
Hier komt ook om de hoek kijken hoe de **betrouwbaarheid** en **beschikbaarheid** van het netwerk is. Is 99 procent uptime voldoende of is 100 procent echt het streven? Een klant zal desgevraagd altijd 100 procent uptime wensen, maar dat betekent niet dat hij ook de consequenties daarvan, met name op financieel gebied, doorziet. Het is de taak van een netwerkleverancier om in samenspraak met de klant tot de juiste afweging te komen. De regel 'de klant is koning' gaat in de ICT-wereld niet op. De klant wil namelijk alles en het mag niets kosten. Het belang van de leverancier lijkt daar soms lijnrecht mee in tegenspraak. Niet elke klant heeft evenveel te besteden en daarmee zijn klanten dus ook niet 'evenveel' koning. De uitdaging is om de juiste middenweg te vinden.

4.10 TCO, ROI en afschrijvingstermijn

Een netwerk vormt voor bijna alle bedrijven een forse investering, en het is tot de bedrijfskritische systemen gaan behoren. Als het netwerk niet operationeel is, kan het bedrijf niet functioneren. De periode die het bedrijf kan overleven zonder netwerk neemt af. Er zijn bedrijven waar het bedrijfsnetwerk zo onmisbaar is bij het uitvoeren van de primaire bedrijfsprocessen dat een storing van enkele uren het bedrijf al in zijn voortbestaan kan bedreigen.

Dit betekent natuurlijk niet dat het niet uitmaakt wat de kosten zijn. Elk bedrijf zal op een efficiënte wijze een netwerk willen aanschaffen, beheren en uiteindelijk, als het afgeschreven is, willen vervangen. In die zin geldt voor een netwerk hetzelfde als voor een bureaustoel of de vloerbedekking. Zeker uit de beginperiode van de automatisering zijn voorbeelden bekend van uit de hand gelopen kosten, die uiteindelijk een project of bedrijf de das om gedaan hebben.

De **kosten** van een netwerk zijn zeer divers; er moet geprobeerd worden zowel de delen als het geheel in de hand te houden. Om een duidelijke afweging te kunnen maken tussen kosten en baten, en om ook te bepalen welke apparatuur gekozen kan worden, wordt vaak gewerkt met het begrip **Total Cost of Ownership** (TCO) van een pc.



Figuur 4.9 Opbouw TCO volgens Gartner Group.

Een veelgebruikte en eenvoudige definitie van TCO is:

Total Cost of Ownership
De totale kosten van aanschaf, onderhoud en gebruik van ICT assets ('goederen') binnen een organisatie.

Het lijkt in tegenspraak met de lage prijzen van de diverse 'dozenschuivers', maar men is het er over het algemeen wel over eens dat een TCO van € 10.000 tot € 15.000 een redelijke schatting is. Dit heeft dan meestal betrekking op een periode van drie jaar. De kosten voor onderhoud, serverpark en ICT-infrastructuur drukken veel zwaarder op dit bedrag dan de relatief lage aanschafprijs van een pc.

De eenvoudigste benaderingswijze bij een investering is de terugverdienmethode:

$$\frac{\textit{Oorspronkelijke investering}}{\textit{Jaarlijkse netto inkomsten}} = \textit{Aantal jaren}$$

Return On Investment
ROI

Een andere benadering voor een bedrijf dat een netwerk implementeert, is de **Return On Investment (ROI)**. Hoeveel levert het netwerk nu eigenlijk aan besparingen op en is dat bedrag hoger dan de investering zelf? Daartoe bepaal je eerst de inkomsten die de investering genereert:

$$\frac{(\textit{Totale inkomsten} - \textit{Totale kosten} - \textit{Afschrijving})}{\textit{Economische levensduur}} = \textit{Netto inkomsten}$$

om vervolgens aan het percentage van de ROI te komen:

$$\frac{\textit{Netto inkomsten}}{\textit{Totale oorspronkelijke investering}} \times 100\% = \textit{ROI}$$

De vraag is wat dit betekent voor de termijn waarop het netwerk zichzelf heeft terugverdiend. Is dat een termijn die gezien de technische en economische levensduur van het netwerk reëel is? Bedenk wel dat, hoewel de technische levensduur van een pc op dit moment vele jaren bedraagt, een pc in economisch opzicht in drie jaar zijn waarde geheel verliest. Een vervangingstermijn van drie jaar wordt voor desktops als normaal gezien. Voor servers wordt met een iets langere periode rekening gehouden, en voor andere apparatuur is het wisselend. Vaak gaan apparaten als routers wel veel langer mee, maar moeten deze toch vervangen worden omdat bijvoorbeeld de bandbreedte niet meer voldoet.

4.11 10% regel

Het functioneel netwerkontwerp is leidend voor de latere ontwerpfasen en de bouw van het netwerk. Het is de bedoeling om het netwerk exact volgens deze specificatie te maken. In de praktijk lukt dat echter soms niet. Apparatuur die beschikbaar is op het moment dat het FNO wordt gemaakt, kan niet meer leverbaar zijn, of de specificaties zijn gewijzigd. Ook kan het gebeuren dat de minimale specificaties zo laag zijn dat het goedkoper is een snellere oplossing te kiezen. Dat laatste klinkt misschien gek, maar een netwerk dat trager is dan 10 Mbps is momenteel duurder dan een 10 Mbps oplossing. (Het verschil tussen 100 Mbps en 10 Mbps is erg klein.)

Het kan dus gebeuren dat in het inrichtingsplan, dat op het functioneel ontwerp volgt, een andere selectie wordt gemaakt dan in het FNO. Dit