

TECHNISCHE ASPECTEN VAN E-WERKEN

In dit hoofdstuk gaan we in op de benodigde ICT infrastructuur voor e-werken. Het is specifiek gericht naar de IT manager of adviseur, maar kan interessante achtergrond leveren voor eenieder die bij een project betrokken is.

U vindt er antwoorden op vragen als :

- *'Hoe te kiezen tussen ADSL / Kabel / inbellen / huurlijnen / ... ?'*
- *'Wat dien ik in acht te nemen omtrent security ?'*
- *'Moet ik speciale software voorzien ?'*
- *'Kan ik aan e-werkers toegang verlenen tot dezelfde bedrijfsapplicaties als op kantoor ?'*

ICT: INFORMATIE- EN COMMUNICATIE-TECHNOLOGIE

De "e" van e-werken staat voor "elektronisch". Als een werknemer dus werkt vanop een andere locatie dan het bedrijf zelf (bijvoorbeeld thuis, of vanuit een satellietkantoor), speelt ICT een belangrijke rol.

ICT is de afkorting van Informatie- en CommunicatieTechnologie. Een goed uitgebouwde ICT-infrastructuur vervult dus twee doelstellingen binnen een e-werkproject:

1. Kennismanagement: de uitwisseling mogelijk maken van relevante bedrijfsgegevens en **-informatie**, en dit op een vlotte, snelle en vooral veilige manier.
2. De **communicatie** bevorderen tussen de e-werkers enerzijds, en de andere teamleden, de managers en de rest van de onderneming en eventueel externe businesspartners en/of klanten anderzijds. ICT-toepassingen kunnen niet alle kwaliteiten van dagelijks contact op kantoor vervangen, maar ze zijn wel in staat om een productieve samenwerking op gang te houden.

**IN PRINCIPE KAN OOK
ZONDER ICT PRIMA OP
AFSTAND WORDEN
SAMENGEWERKT.**

In principe kan ook zonder ICT prima op afstand worden samengewerkt.

Veel werknemers zijn perfect in staat om individueel hun takenpakket af te werken. En als er duidelijke afspraken zijn gemaakt over doelstelling en taakverdeling, kan iedereen zijn rol op een goede manier invullen.

Vanzelfsprekend moet men dan nog op geregelde tijdstippen samenkomen voor overleg. Maar zelfs in deze ICT-arme e-werkomgevingen zal men merken dat er voor snel overleg of feedback men nog vaak naar de telefoon grijpt.

We leven in een maatschappij waarin "kennis" een grote rol speelt. En voor het doorspelen van die kennis kunnen we niet zonder communicatie. We kunnen er dan ook van uitgaan dat iedere e-werker gebruik maakt van een of andere vorm van ICT om de communicatie op peil te houden.

De balans kan ook doorslaan. Soms lijkt de neiging te bestaan om samenwerken op afstand vooral als een technische uitdaging te benaderen. Op zich is het logisch dat de toepassing van ICT veel aandacht krijgt bij het inrichten van een samenwerkingsrelatie op afstand. Het gevaar is echter om de nadruk te leggen op de invoering van high tech-systemen die vervolgens niet worden gebruikt. Samenwerken op afstand is vooral een bedrijfsculturele uitdaging; techniek is een hulpmiddel.

Dit technische gedeelte van het e-werken stappenplan wil een hulpmiddel zijn voor zowel managers als werknemers om bij het technisch uitbouwen van een e-werkproject, de juiste keuzes te maken.

**NEIGING BESTAAT OM
SAMENWERKEN OP
AFSTAND VOORAL LOUTER
ALS TECHNISCHE
UITDAGING TE
BENADEREN.**

DE JUISTE ICT-INFRASTRUCTUUR

Enkele belangrijke aandachtspunten bij de invoering en gebruik van ICT voor e-werken:

WIE E-WERKT?

- Hoe homogeen is de groep werknemers die betrokken is bij het e-werkproject?
- Hoe vaak is het nodig dat ze communiceren met andere leden van het team?
- Training: zijn de werknemers technisch opgeleid voor deze nieuwe manier van werken?

Meer hierover in het hoofdstuk "Communicatie en informatie"

WAAR E-WERKEN ZE?

- Welke informatie- en communicatietechnologie het beste past bij een e-werkproject hangt in de eerste plaats af van de locatie van de e-werker: thuis, in een telekantoor dichtbij de woonplaats, in een satellietkantoor dat aansluit op het bedrijfsnetwerk, of mobiel vanop verschillende locaties bij klanten of leveranciers.
- Monitoring, evaluatie en aanpassing van faciliteiten draagt bij aan goed functionerende ICT.

WAT DOEN ZE?

- Informatiebeheer: wie kan en mag wat weten?
- Informatieveiligheid: wie krijgt toegang tot welke onderdelen van het netwerk en wie niet en hoe regelen we dat?

Meer over het veiligheidsaspect van e-werken in het hoofdstuk "Security bij e-werken".

WAARMEE WERKEN ZE?

- Groupware: samenwerkingssoftware
- Gebruiksvriendelijkheid: kies voor duidelijke programma's- veel mensen werken graag intuïtief ?
- Helpdesk: wie staat in voor technische ondersteuning?
- Compatibiliteit: optimale communicatie, transfer van gegevens tussen softwarepakketten is noodzakelijk

HOE E-WERKEN ZE?

- Beschikbare communicatietechnologie: telefoon, fax, breedband internetaansluiting of VPN
- Bereikbaarheid: wie is op welke manier te bereiken?
- Snelheid: zorg voor een zo kort mogelijke wachttijd bij het inloggen

Lees hierover meer in het hoofdstuk "Communicatietechnologieën"

- enzovoort.

INLEIDING: INTERNET: IDEAAL VOOR E-WERKEN?

De minimale communicatieuitrusting voor e-werken is telefoon of fax. In veel gevallen wordt die ook aangevuld met één of andere vorm van "internet"-connectiviteit:

1. Inbelverbinding of ISDN verbinding
2. Breedband-internet via de kabel
3. Breedband-internet via ADSL/HDSL/SDSL
4. Breedband-internet via WiFi
5. Huurlijnen en glasvezelverbindingen
6. Mobiele netwerken

**DE LAATSTE JAREN WORDT
VOORAL INTERNET HET
MEEST GEBRUIKT BIJ E-
WERKEN**

De laatste jaren wordt vooral **internet** het meest gebruikt bij e-werken. Breedband-internet speelt daarbij een grote rol. De verwachting is dat dit netwerk in de volgende jaren nog verder zal blijven groeien en dat er enorme toename zal zijn in de kwaliteit van de dienstverlening en in de bandbreedte die ter beschikking zal staan.

Het internet biedt de volgende **voordelen**:

- wereldwijde beschikbaarheid
- vaste tarieven voor toegang
- tarieven voor transmissie zijn onafhankelijk van de afstand die moet overbrugd worden

Deze eigenschappen maken internet heel geschikt voor e-werken.

Internet heeft echter nog een aantal beperkingen waaraan gewerkt wordt:

- De kwaliteit en betrouwbaarheid van internetverbindingen is tot op heden voor verbetering vatbaar. Internet bestaat immers uit een netwerk van verschillende netwerken. Omdat dit netwerk blijft groeien, kan er soms verzadiging optreden. En dan heeft de e-werker last van een tragere, of zelfs helemaal geen internetverbinding.
- Een ander nadeel van het gebruik van het internet is dat er strengere veiligheidsmaatregelen vereist zijn. Het is altijd mogelijk dat andere partijen die op het internet aangesloten zijn, de verbindingen af luisteren en zo bijvoorbeeld e-mails lezen of paswoorden te weten komen.
- Door het bedrijfsnetwerk te koppelen met het internet wordt het risico op inbraak groter. Men dient de nodige bescherming in te bouwen om te vermijden dat krakers op het internet zich toegang verschaffen tot het bedrijfsnetwerk.

**INTERNET HEEFT TOCH
NOG EEN AANTAL
BEPERKINGEN.**

**INFRASTRUCTUUR LANGS
ZIJDE VAN E-WERKER EN
INFRASTRUCTUUR LANGS
ZIJDE VAN HET BEDRIJF.**

Om aan deze beperkingen tegemoet te komen, blijven de service providers nieuwe technologieën ontwikkelen, om een constante hoge kwaliteit te kunnen blijven garanderen. We gaan daar dieper op in in het hoofdstuk 'Security bij e-werken'. In de volgende hoofdstukken komen eerst de andere communicatietechnologieën aan bod.

Bij het opzetten van een e-werken communicatie-infrastructuur dient in de volgende aspecten voorzien te worden :

- communicatie langs de zijde van de e-werker : inbelverbinding / breedband internetverbinding / mobiele verbinding
- communicatie langs de zijde van het bedrijf (en eventuele satellietkantoren): breedband internet verbinding / huurlijnen

INBELVERBINDING OF ISDN VERBINDING

Vroeger maakte men veel gebruik van rechtstreekse verbindingen met de onderneming, gebruik makende van PSTN/ISDN netwerken : men belt dan vanuit de modem van zijn computer rechtstreeks naar de modem van het bedrijfsnetwerk.

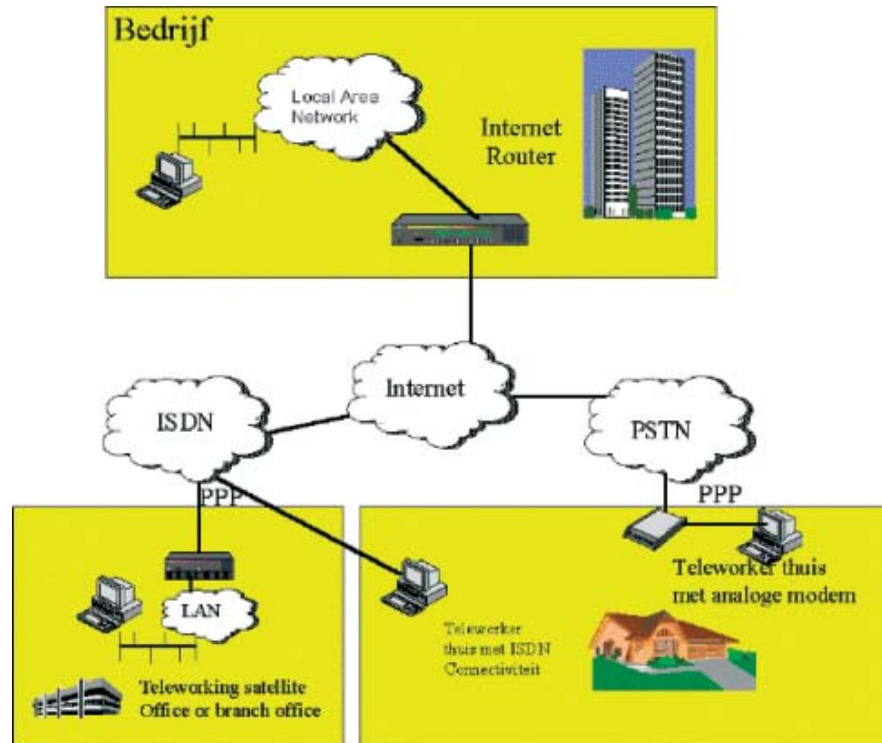
PSTN Inbelverbindingen en ISDN verbindingen maken gebruik van de beschikbare telefonienetwerken, zoals het PSTN netwerk (Public Switched Telephony Network - het gewone publieke telefonienetwerk dat ook gebruikt wordt voor de vaste telefonie) en het ISDN netwerk (het digitale telefonienetwerk).

**DE TRADITIONELE
INBELVERBINDING MAAKT
MEER EN MEER PLAATS
VOOR BREEDBAND
INTERNET.**

In Vlaanderen zijn op dit moment nog steeds een groot aantal van deze verbindingen actief, maar de laatste jaren wordt meer en meer gebruik gemaakt van internet-gebaseerde verbindingen. Dit is omdat ISDN- en PSTN-verbindingen een aantal nadelen hebben voor e-werkers:

- 1 De directe verbindingen hebben als grootste nadeel dat ze afstandsgebonden zijn. Voor e-werkers die geregeld op verschillende locaties verblijven, en voor buitenlandse verbindingen, is er dus een aanzienlijke meerkost ten opzichte van de verbindingen via Internet.

In sommige gevallen wordt dan ook voorzien in het inbellen naar het internet (in plaats van het bedrijfsnetwerk) vanuit de analoge of ISDN modem van de e-werker.



Figuur 2 : VERBINDINGEN VIA INTERNET

2 Voor de moderne e-werkers zijn deze oplossingen meestal te traag: gemiddeld 56 kbps (kilobits per seconde) voor een PSTN lijn en 64/128 kbps voor een ISDN lijn.

3 De verbinding met de onderneming loopt via de traditionele telefoonverbinding : er is dus geen telefonieverkeer mogelijk tijdens de periode van verbinding.

De laatste jaren worden deze oplossingen dan ook meer en meer vervangen door breedbandverbindingen zoals Breedband Internet via de Kabel, of Breedband Internet via ADSL.

telefoonabonnement meer aan zijn internetleverancier maar kan dan enkel nog zijn lijn gebruiken om te surfen.

**DE ASYMMETRIE VAN
ADSL KAN EEN
BEPERKING ZIJN VOOR
BEPAALEN CATEGORIE
VAN E-WERKERS.**

Een klassieke ADSL verbinding is per definitie asymmetrisch, dit wil zeggen dat de maximale doorvoercapaciteit bij het downloaden (van het Internet naar de site van de klant) groter is dan de maximale doorvoercapaciteit bij het uploaden (van de site van de klant naar het Internet). Dit kan een beperking zijn voor bepaalde categorieën van e-werkers die veel en omvangrijke bestanden naar de onderneming dienen door te sturen.

HDSL (High-bit-rate Digital Subscriber Line) is eveneens een technologie die data kan versturen over een bestaand telefoonnetwerk. De typische bandbreedte van 784Kbps tot 1,544Mbps.

**SDSL EN HDSL ZIJN
SYMMETRISCH.**

Dit type internet verbinding is symmetrisch wat betekent dat de upload en download snelheid gelijk is. Deze technologie is uitermate geschikt voor locaties waar grote hoeveelheden data verzonden en ontvangen moeten worden.

SDSL (Symmetric Digital Subscriber Line) is een krachtige variant op de DSL-technologie waarbij dataverkeer met een enorme snelheid over een normale telefoonlijn wordt getransporteerd, zonder dat er telefoontikken in rekening gebracht worden. Bijzonder aan SDSL is dat de down- en upstream exact aan elkaar gelijk zijn.

Net als bij breedband via de kabel laten de DSL technologieën toe om :

- permanent on-line te zijn met een supersnelle breedband-verbinding.
- de telefonielijn vrij te houden, zodat e-werkers geen enkele belangrijke oproep moeten missen.

BREEDBAND-INTERNET VIA WIFI (HOTSPOTS)

WiFi staat voor Wireless Fidelity. De term WiFi wordt gebruikt voor draadloze netwerken die gebaseerd zijn op de IEEE 802.11 standaard. De data wordt via radiogolven op een frequentie van 2.4 GHz of 5GHz verzonden. WiFi maakt hiertoe gebruik van een vergunningvrij deel van de ether. Ook de afstandsbediening van uw televisie en bepaalde huistelefoons maken hiervan gebruik. Alle netwerkapparaten met het keurmerk van de Wifi Alliantie zijn in staat met elkaar te communiceren.

HOE KAN IK VERBINDING KRIJGEN MET EEN WIFI NETWERK?

**OM TE TELEWERKEN VIA
HOTSPOTS, MOET UW PC
BESCHIKKEN OVER EEN
WIFI INSTEKKAART OF
LOSSE ADAPTER.**

Om met een WiFi netwerk te kunnen communiceren moet uw PC beschikken over een WiFi insteekkaart of losse WiFi adapter (met USB-aansluiting) en de daarbij bijgeleverde WiFi software. Afhankelijk van de plek waar u zich bevindt dient u eventueel ook over een kleine antenne te beschikken. Het radiosignaal heeft namelijk moeite met het doordringen van bijvoorbeeld

betonnen muren. De antenne waarvan u de signalen ontvangt moet zich altijd binnen uw gezichtsveld bevinden. De antennes moeten elkaar kunnen 'zien' – dit noemt men 'line of sight'.



HOE SNEL IS EEN WiFi NETWERK?

**IN DE PRAKTIJK HEEFT WiFi
SNELHEDEN VAN
2MBIT/SEC.**

Een verbinding via een WiFi netwerk haalt hogere snelheden dan adsl- en kabelverbindingen. Een snelheid van max. 54 Mbps is mogelijk. In de praktijk ligt de snelheid lager: 2 Mbps is een wat realistischer schatting voor grote afstanden maar voor het e-werken kantoor kan dit oplopen tot 11 of 54 Mbps afhankelijk van apparatuur. Wat de snelheid betreft is wireless LAN een verbinding die afhankelijk is van het aantal gebruikers omdat de verbinding gedeeld wordt over verschillende mensen. Hoe meer mensen in uw omgeving er gebruik van maken, hoe trager de verbinding wordt.

HOE VEILIG IS WiFi?

Een wireless LAN is net zo (on)veilig als het internet. Neem dus dezelfde veiligheidsmaatregelen in acht als bij een Kabel, ADSL of telefoonaansluiting op het internet:

- installeer een virusscanner;
- zorg voor een regelmatig update van de virusscanner;
- installeer een firewall,
- een hardwarematige firewall kan ook. Deze zijn vaak in routers ingebouwd;
- voor WiFi gelden nog speciale beveiligingen, zoals WEP en MAC.

WAT IS HET VERSCHIL TUSSEN WiFi, ADSL EN KABELINTERNET?

Een WiFi aansluiting kan in principe overal, op elke plek worden gerealiseerd worden. Voor oude, historische gebouwen is er het voordeel dat er niet gesloopt hoeft te worden voor een Wi/fi aansluiting. Denkt u aan bijvoorbeeld oude kerkgebouwen of musea.

WiFi is zoals gezegd draadloos. Het signaal verplaatst zich via de lucht. Voor ADSL en kabel is een draadverbinding noodzakelijk.

Meer en meer plaatsen worden op dit ogenblik uitgerust met WiFi (hotspots) maar voor een e-werkproject betekent WiFi uiteindelijk vooral vrijheid in eigen huis en tuin.

**WIFI BESPERKT DE
NOODZAAK TOT
AANLEGGEN VAN
BEKABELING THUIS.**

**ER IS IN DE MEESTE
GEVALLEN BIJ HET GEBRUIK
VAN WIFI NOG EEN ADSL-
OF KABELVERBINDING
NODIG.**

Daarom wordt er recent ook meer en meer gebruik gemaakt van WIFI thuis bovenop de standaard breedband internetverbinding (zowel kabel als ADSL). Men creëert dan zijn eigen 'private' wireless omgeving. Dit beperkt de noodzaak tot het aanleggen van bekabeling bij de e-werker thuis, aangezien alle verbindingen tussen de modem (aan de kabel of telefoonaansluiting) en PC draadloos gebeuren. Ook hier geldt de opmerking om voldoende aandacht aan beveiliging te besteden. Het gebruik van WiFi thuis betekent in de meeste gevallen wel dat er nog steeds een ADSL of kabelverbinding nodig is tot binnen, tenzij uw medewerkers het ongelofelijke geluk hebben in de buurt van een WiFi hotspot te leven.

STOORT DRAADLOOS INTERNET ANDERE APPARATUUR?

Draadloos internet maakt gebruik van de 2,4 Ghz band. Ook andere huishoudelijke apparaten zoals magnetrons, afstandbedieningen en draadloze toetsenborden maken gebruik van deze frequentie. Het signaal kan dus beïnvloed worden door dergelijke apparaten.

WAT IS DE REIKWIJDTE VAN EEN DRAADLOOS SYSTEEM?

Dat hangt samen met de gebruikte antennes en de hoogte van deze antennes. De omgeving is ook erg van invloed. In beboste gebieden of over water komen radiogolven minder ver dan bijvoorbeeld in een open veld.

WiFi komt tegenwoordig meer en meer in een brede dekking ter beschikking. Standaard is WiFi beschikbaar op de meeste luchthavens, in heel wat hotels en seminariecentra. Maar ook treinstations, wegrestaurants, benzinstations, scholen en zelfs hele steden voorzien tegenwoordig in een WiFi netwerk.

**HOTSPOTS ZIJN
TEGENWOORDIG BESCHIK-
BAAR OP LUCHT-HAVENS,
TREIN-STATIONS, WEGRES-
TAURANTS, HOTELS,
BENZINSTATIONS, ENZ...**

MOBIELE NETWERKEN

Buiten de reeds vermelde vaste netwerken, bestaan er ook mogelijkheden voor e-werkers om de netwerken van mobiele telefonie te gebruiken voor de uitoefening van hun job. Tegenover de een verbinding via WiFi bieden deze netwerken het voordeel dat ze nog steeds een grotere dekking bieden. Gekende voorbeelden hiervan zijn:

GSM

GSM is de technologie van de tweede generatie mobiele netwerken. Deze technologie is echter beperkt in gebruik voor e-werkers, vanwege de lage snelheden die dit mogelijk maakt: 9.6 kbps ofwel bijna onbruikbaar om via deze technologie te e-werken.

**MET BEHULP VAN DE
MOBIELE TELEFOON
(GSM, GPRS, UMTS) KAN
OOK EEN VERBINDING MET
HET BEDRIJFSNETWERK
WORDEN GEMAAKT.**

GPRS

GPRS is een recentere variant GSM, waarbij hogere transfersnelheden mogelijk zijn. In de praktijk is echter gebleken dat de beschikbaarheid van deze technologie redelijk beperkt is gebleven, en de aangekondigde snelheden van 110 kbps, dus tweemaal de snelheid van een gewone inbelverbinding van 56 kbps worden zelden gehaald. Meestal is de connectiviteit gemiddeld 30 kbps, waardoor ook met deze technologie e-werken niet echt mogelijk is. Daarvoor is het wachten op de introductie van UMTS, de derde generatie mobiele netwerktechnologie.

UMTS

UMTS staat voor Universal Mobile Telecommunications Services. UMTS is een nieuwe techniek die breedbandige(r) verbindingen met bijvoorbeeld internet via mobiel mogelijk maakt. UMTS betekent een evolutie voor wat betreft mogelijke diensten en data snelheden ten opzichte van de huidige "tweede generatie" mobiele netwerken, GSM en GPRS.

In de praktijk is UMTS zes keer sneller dan ISDN en is daarmee geschikt voor bijvoorbeeld het ontvangen van bewegend beeld. Bijna alle communicatie die via het vaste telefoonnet (b.v. via Kabel of ADSL) kan, kan straks ook mobiel via UMTS.

**BIJNA ALLE
COMMUNICATIE DIE VIA
HET VASTE TELEFOONNET
KAN, KAN STRAKS OOK
MOBIEL VIA UMTS.**

HUURLIJNEN EN GLASVEZELVERBINDINGEN

Deze netwerkaansluitingen zijn vooral geschikt om verbindingen tussen bedrijfsafdelingen op te zetten (bijvoorbeeld tussen het hoofdkantoor en satellietkantoren) of verbindingen tussen de onderneming en het netwerk van de operator.

HUURLIJNEN

Indien uw bedrijf minstens één uur per dag communicatie voert die tussen twee vaste punten verloopt (dat kan tussen uw hoofdkantoor en een vestiging zijn, of tussen uw bedrijf en een belangrijke zakenpartner), dan loont het de moeite om een digitale huurlijn te overwegen.

Een digitale huurlijn biedt u een permanent communicatiekanaal met een vaste capaciteit en een transparante - en dus volledig protocolonafhankelijke - transmissie. Omdat meerdere kanalen op één pad gedefinieerd kunnen worden (multiplexing) is die lijn des te efficiënter. Uw internetprovider kan voor u op ieder moment uw bandbreedte verhogen of verlagen.

**EEN HUURLIJN BIEDT U
MEER GARANTIES OP
GEBIED VAN
BESCHIKBAARHEID EN
CAPACITEIT.**

Voordelen op een rij

- een digitale huurlijn biedt een hoge beschikbaarheid dankzij onze continue monitoring en analyse van prestaties
- u bepaalt zelf het niveau van beschikbaarheid. Naar gelang van uw behoeften kunt u op vier verschillende manieren aangesloten worden op het netwerk van de operator. Dat levert beschikbaarheden op die van 99,80% tot 99,995% variëren.
- u vervalt niet onder de algemene internet infrastructuur (zonder garanties), maar kunt rekenen op een dienstverleningsgarantie (SLG of service level garantie). Zo weet u exact wat u mag verwachten op het gebied van service, prestaties en facturatie.

GLASVEZELVERBINDINGEN.

Glasvezel of Fiber biedt u een rechtstreekse, permanente glasvezelverbinding met het internet, waarover de informatie met een gegarandeerde (hoge) snelheid loopt.

Een typische Fiber verbinding omvat de internettoegangslijn en een aantal standaard- en optionele internetdiensten.

Glasvezelverbindingen zijn echter op dit moment nog erg duur en daarom niet geschikt voor individuele e-werkers.

SOFTWARE VOOR E-WERKEN.

Om e-werken in een team mogelijk te maken, moet de onderneming beschikken over de juiste software, die samenwerking op afstand tussen de verschillende e-werkers mogelijk maakt.

De meeste bedrijven nemen een eerste stap door de typische kantoortoepassingen (mail, tekstverwerking, spreadsheet, presentaties, ...) in een e-werken context ter beschikking te stellen. Dit is ook de snelste stap (zie de paragraaf 'Bedrijfsapplicaties' hieronder). Echter, er is ook behoefte aan het openstellen van de andere bedrijfsapplicaties die ook op kantoor gebruikt worden evenals behoefte aan gespecialiseerde software die specifiek het e-werken ondersteund (zoals groupware, computer telephony integration, video- & audio conferencing, portals).

We besteden hieronder aandacht aan de verschillende types van software voor e-werken.

BEDRIJFSAPPLICATIES.

**ALLEREERST DIENT ER EEN
INVENTARIS GEMAAKT TE
WORDEN.**

Bedrijfsapplicaties bestaan er in alle maten en gewichten (bv. kantoortoepassingen zoals tekstverwerking & spreadsheet, e-mail, boekhouding, klantendatabases, aankoop, voorraad, CAD en andere tekenpakketten, productieplanning, elektronische dossiers, enz...)

Vooraleer de oplossing uit te dokteren en te implementeren moet men eerst een inventaris maken van de bedrijfsapplicaties, ze analyseren en vervolgens een oplossing implementeren die de bedrijfsapplicaties uniform aanbiedt aan de e-werker.

In dit kader wordt men geconfronteerd met

STANDALONE APPLICATIE

**KANTOOR-TOEPASSINGEN
ZIJN EENVOUDIG TER
BESCHIKKING VAN
E-WERKERS**

Indien de applicatie een standalone applicatie is kan deze eenvoudig worden geïmplementeerd op het werkstation van de e-werker. Dit is zeker het geval voor de typische kantoortoepassingen zoals Microsoft Office (Word, Excel, Powerpoint, ...).

MEERLAGENMODEL

Indien de applicatie bestaat uit een meerlagenmodel is het afhankelijk van de interface en de nodige bandbreedte tussen front-end applicatie (client) en back-end applicatie (server) welke oplossing het meest geschikte is.

**WEB SERVER MOET
AANGEPAST WORDEN OM
VEILIGE EN TRANSPARANTE
COMMUNICATIE MOGELIJK
TE MAKEN.**

WEB BASED APPLICATIE

Indien de User Interface van de applicatie een Web browser is, dient er lokaal niets geïnstalleerd te worden en kan men de web server zodanig aanpassen dat de communicatie veilig en transparant voor het bedrijf en de e-werker is. Hiervoor is het nodig om de web server uit te rusten met een digitaal certificaat. Vervolgens dient men een goed werkende toegangscontrole op de web server toe te passen om de authenticatie van de gebruiker uit te voeren en zich ervan te gewisnen welke identiteit zich aanbiedt.

LOW BANDWIDTH CLIENT/SERVER - WINDOWS BASED APPLICATIE

Indien de front-end applicatie een Windows based applicatie is en de benodigde bandbreedte is klein, kan men de front-end applicatie installeren op de workstation van de e-werker en door middel van een VPN of private verbinding de data tussen de front-end applicatie en back-end applicatie laten verlopen.

E-mail kan bijvoorbeeld eenvoudig op deze wijze geïmplementeerd worden. De gebruiker gebruikt lokaal zijn gebruikelijke e-mail client (zoals Microsoft Outlook of IBM Lotus Notes) en verbindt zich met de server.

CLIENT/SERVER OF SERVER BASED APPLICATIE

Indien het gaat om een meer lagen applicatie waar er frequent data verkeer is tussen workstation en server is het aangewezen de applicatie door middel van server based computing beschikbaar te stellen voor de e-werker.

Server based computing laat toe om uw applicaties eenvoudig uit te rollen, te beheren, het gebruik ervan op te volgen en te ondersteunen vanuit een centrale locatie en deze toch beschikbaar te stellen voor alle e-werkers en satellietkantoren. Dankzij producten uit de familie van server based computing kan je IT complexiteit beheren, voldoen aan de continue vraag naar wijzigingen and zeer hoge performantie aanbieden aan kantoren die verbonden zijn met beperkte bandbreedte.

Server based computing werkt als volgt:

- Op een centrale server worden de applicaties geïnstalleerd in een multi-user mode
- Deze centrale server zal alle sessies draaien of ook wel hosten genoemd, dwz voor uw 50 medewerkers zal hier 50 keer een business applicatie draaien.

**SERVER BASED COMPUTING
LAAT TOE OM EENDER
WELKE APPLICATIE TER
BESCHIKING TE STELLEN
VAN E-WERKERS.**

- Scherm informatie wordt vanuit de centrale server naar de eindgebruiker gestuurd, toetsenbord en muis informatie wordt vanuit het e-werker kantoor naar de centrale server gestuurd en vervolgens acties ondernomen in de business applicatie als mede het scherm geupdate.
- Tevens worden lokale resources zoals hard disc, printers, ... beschikbaar gesteld naast de netwerk apparatuur

Dit biedt het voordeel dat applicatie beheer eenvoudiger wordt en slechts op 1 locatie moet gebeuren, alle gebruikers onafhankelijk van hun locatie over hun applicaties beschikken, geen hoge bandbreedte nodig is (typisch 40 kbps per concurrent sessie) en ondersteuning centraal kan gebeuren.

**IN PLAATS VAN LOKAAL
GEGEVENS TE VERWERKEN
MAAKT MEN EEN
VERBINDING MET EEN
VIRTUELE DESKTOP DIE
EXACT DEZELFDE IS ALS OP
KANTOOR.**

Server based computing wordt evenzeer gebruikt voor de hiervoor vermelde standalone en low bandwidth client/server applicaties. Echt alle bedrijfsgegevens en bedrijfsapplicaties worden dan centraal opgesteld, er is geen noodzaak om lokaal applicaties te draaien. In plaats van zich aan te loggen op het kantoor netwerk en aldus zelf zijn weg te moeten zoeken tussen gedeelde data en systemen, maakt men een verbinding naar een Virtuele desktop omgeving die exact dezelfde is als deze in de kantooromgeving. Via deze oplossing worden de gegevens niet meer gekopieerd naar de lokale PC, maar start de gebruiker applicaties op in deze virtuele desktop waardoor ook de data centraal kan blijven staan.

Oplossingen voor Server Based Computing worden aangereikt door Microsoft Terminal Server (Windows based applicaties), Citrix (idem) en bv. Tarantella (ook voor niet-windows applicaties).

GROUPWARE

**GROUPWARE IS BEDOELD
OM INFO TUSSEN
GROEPEN GEBRUIKERS UIT
TE WISSELEN.**

Groupware is een verzamelnaam voor verschillende softwarepakketten die allemaal één overeenkomst hebben: al deze pakketten zijn bedoeld om informatie tussen groepen gebruikers uit te wisselen.

Meestal combineren dit soort programma's een online kalender, documentenbeheer, takenbeheer, tijdsregistratie en andere elementen uit de reeks van samenwerkingstools die een onderneming nodig heeft om in een groep aan e-werken te kunnen doen.

Er zijn heel wat commerciële suites in de markt die bovenstaande elementen combineren, zoals Microsoft Sharepoint Services, IBM/Lotus Sameplace en anderen. Daarnaast bestaat ook gespecialiseerde software voor de specifieke onderdelen (bv. elektronisch document management / workflow).

Van dit type software bestaan ook een aantal "open source" versies, dus software die hun broncode gratis via het internet ter beschikking stellen, en op die manier bedrijven in de mogelijkheid stellen om deze naar hun eigen behoefte aan te passen. Een voorbeeld hiervan is phpgroupware.org.

**VIRTUELE VERGADERING
ZIJN MOGELIJK VIA VIDEO
EN AUDIOCONFERENTIE
SOFTWARE.**

VIDEO EN AUDIOCONFERENTIE SOFTWARE.

Een veelgebruikte manier om te e-werken is het gebruik maken van zogenaamde video en audioconferentie software. Bij het gebruik van dit type van software, worden virtuele vergaderingen mogelijk, dikwijls in combinatie met het delen van MS-Word documenten, tekeningen en andere elementen van een bepaald project.

Bijvoorbeeld het programma Netmeeting van Microsoft maakt het mogelijk om via een zgn. white board informatie met anderen te delen. Ook is het mogelijk om een window (bijv. van een bepaald programma) aan deelnemer te tonen, en zo te laten zien hoe een bepaald programma gebruikt moet worden.

Daarnaast is er 1 op 1 communicatie mogelijk met beeld en geluid.

Aan de apparatuur wordt niet veel eisen gesteld; een eenvoudige videocamera en een microfoon met luidsprekers is voldoende.

INSTANT MESSAGING.

**INSTANT MESSAGING IS
GESCHIKT OM KORTE
BERICHTEN TE STUREN EN
OM TE ZIEN OF DE
COLLEGA'S ONLINE ZIJN.**

Deze software is geschikt om korte berichten te sturen naar andere e-werkers die online zijn. Het voordeel van dit type van software is dat je kan zien wie van de collega's er online is, en met wie je direct contact kan nemen.

In tegenstelling tot e-mail communicatie, waar je nooit zeker weet wanneer je collega de mail leest, is er bij Instant Messaging een directe link tussen twee mensen die online en aan de computer zitten, dus is een veel directere communicatie mogelijk.

Ontstaan vanuit de consument naar consument communicatie, zijn er de laatste jaren redelijk wat bedrijfsversies ontwikkeld van dit soort software.

De bedrijfsversies maken het mogelijk om met andere personeelsleden van de onderneming te chatten, eventueel documenten te delen, en zelfs tot online telefoongesprekken te voeren via het Internet of de beveiligde VPN verbinding.

INTRANET PORTAALSITES.

**INTRANET PORTAALSITES
LATEN TOE DAT
DE E-WERKER ALLE
OPERATIES BINNEN ZIJN
TAAK KAN UITVOEREN.**

Intranet portaalsites kunnen voor de e-werker een nuttige bron zijn van de informatie en documenten voor het uitvoeren van hun taken op afstand. Meer en meer Intranet portaalsites worden Enterprise Portals genoemd, omdat dit type van portaalsites de e-werker toelaten om in een web-browser alle operaties uit te voeren die ze binnen hun taak als e-werker nodig hebben, zoals het delen van documenten, hun kalender gebruiken, de resultaten en de planning van de projecten opvolgen waaraan ze werken, toegang tot bedrijfsapplicaties, etc...

Meestal maakt dit type van software het voor gebruiker mogelijk om zijn volledige werkomgeving te personaliseren, zodat hij alleen wat hij nodig heeft in zijn online werkomgeving kan instellen, zoals een "dashboard", en verder kan het worden ingesteld op gelijk welk toestel hij gebruikt, zoals PC, PDA of andere toestellen.

Voorbeelden van dergelijke portaalsoftware zijn Plumtree, Microsoft Sharepoint Portal, SAP Portal of Oracle Portal.

COMPUTER TELEPHONY INTEGRATION.

**COMPUTER TECHNOLOGY
INTEGRATION MAAKT
TELEFONIE EN DATA
DIENSTEN VIA EENZELFDE
NETWERKCONNECTIES
MOGELIJK.**

Een redelijke recente technologie is deze van de Computer Telephony Integration (CTI). Deze technologie laat het toe om telefonie en datadiensten zoals internet samen te gebruiken over dezelfde netwerkconnectie, meestal geïntegreerd met de computer.

Deze diensten hebben het voordeel dat de e-werker zich gelijk waar kan bevinden en een gesprekspartner transparant kan worden doorverbonden met gelijk welke locatie waar de e-werker zich bevindt.

De e-werker kan gebruik maken van alle email en doorschakelings mogelijkheden alsof hij op kantoor is, omdat de telefoongids van het kantoor ook op de locatie op afstand beschikbaar is.

CTI tools zoals het gebruik van het PC scherm om e-mails te ontvangen en oproepen te plaatsen werken even snel als op kantoor.

Geavanceerde diensten, die normaal enkel in het bedrijf mogelijk zijn, zoals een volg-mij dienst, marketing lijsten om prospects te bellen, zijn beschikbaar ook voor de e-werker.

Er zijn drie verschillende types beschikbaar:

1. IN diensten.
2. IN VoDSL diensten.
3. IP PBX diensten.

PBX (Private Branch Exchange) is een privé-telefooncentrale die manueel kan ingesteld worden om telefoons te routeren naar de verschillende eindpunten in een communicatie netwerken.

PABX heeft dezelfde eigenschappen, maar is een Private Automated Exchange, met een automatische schakeling van de telefoongesprekken.

**IN DIENSTEN MAKEN
HET MOGELIJK OM TE
WERKEN ALSOF MEN OP
KANTOOR IS.**

IN DIENSTEN.

Deze diensten geven de e-werker de mogelijkheid om thuis te werken alsof hij op kantoor zit, zijn telefoongesprekken worden toegevoegd aan de rekening van het bedrijf tijdens zijn e-werk, en verder kan hij gebruik maken van de telefooncentrale alsof hij zich op het bedrijf bevindt.

**VIA IN VODSL SERVICES
HEEFT MEN EEN E-WERKER
TELEFOONLIJN TER
BESCHIKKING.**

IN VODSL SERVICES.

Met deze technologie is het mogelijk om via een standaard internet verbinding Telefonie en Internet diensten te combineren. De E-werker heeft dus een e-werk telefoonlijn ter beschikking, zodat de thuis telefoon niet bezet is tijdens telefonisch overleg met collega's.

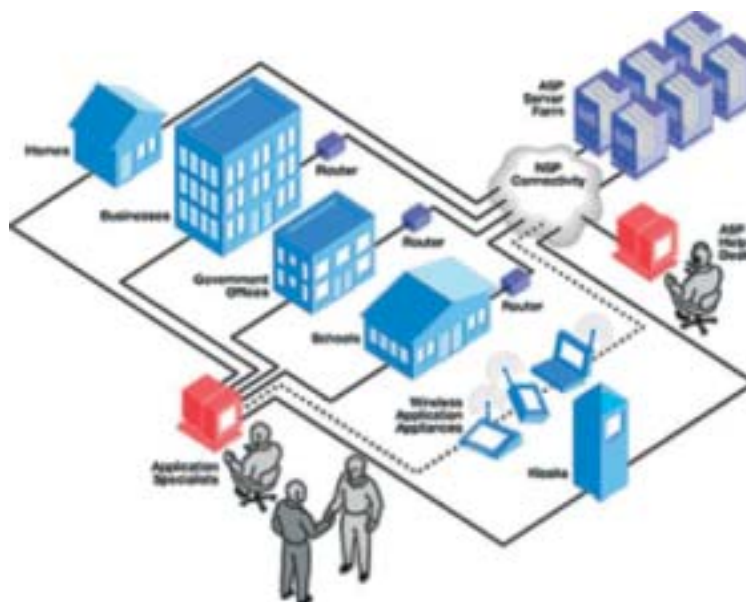
**IN EEN ASP MODEL
KUNNEN MEERDERE
BEDRIJVEN EEN SERVER
BASED COMPUTING
INFRASTRUCTUUR DELEN.**

IP PBX SERVICES.

Deze integrale aanpak maakt het de e-werker mogelijk om via zijn PC alle mogelijke applicaties van de onderneming te gebruiken, zijn e-mail, en alle telefoniefuncties waarover de onderneming beschikt.

ASP ALS TECHNOLOGISCHE OPLOSSING VOOR E-WERKEN

Grotere bedrijven kunnen de hiervoor vermelde Server Based Computing omgevingen op hun eigen netwerk implementeren, men kan dan spreken van een On-Site ASP oplossing. Voor kleinere bedrijven kan men gebruik maken van een gedeelde infrastructuur waar men on-line diensten zoals een office omgeving en eigen applicaties kan gebruiken voor een vaste prijs per maand per gebruiker. Men noemt dit ASP ("Application Service Provider").



Figuur 4 : ASP VOOR E-WERKEN

Ook zijn hybride oplossingen mogelijk waarbij lokale bedrijfseigen toepassingen worden verbonden met een gedeelde infrastructuur bij een ASP dienstenleverancier. Op deze wijze kan men het werken van op afstand gemakkelijk implementeren, zonder zijn eigen IT-infrastructuur te moeten veranderen.

Een gedeelde infrastructuur kan voor veel KMO's een ideale oplossing zijn om het e-werken op een snelle, efficiënte en gecontroleerde manier in te voeren voor een vaste kostprijs per maand, met een gegarandeerd resultaatsverbintenis en dit zonder eigen investeringen. Deze manier van werken kan voor KMO's zelfs nog een aantal bijkomende voordelen bieden. Data worden veilig bewaard en voorzien van een gegarandeerde dagelijkse back-up, iets wat bij sommige KMO's niet altijd het geval is. De infrastructuur wordt beheerd door professionele ICT medewerkers met kennis van zaken, men beschikt steeds over de laatste software zonder extra investeringen, nieuwe technologieën kunnen snel ter beschikking worden gesteld. In een multi-Site omgeving waarbij KMO's verschillende filialen beschikt kunnen medewerkers met elkaar communiceren en toegang hebben tot applicaties alsof ze in één groot virtueel kantoor werken.

**ASP BIEDT AAN KLEINERE
ONDERNEMINGEN EEN
FULL-SERVICE ICT
ONDERSTEUNING.**

Schematisch kan één en ander als volgt geïllustreerd worden:



Figuur 5 : MULTI-SITE OMGEVING

SECURITY BIJ E-WERKEN

Men wordt niet pas met informatiebeveiliging geconfronteerd op het moment dat er op afstand wordt samengewerkt. Ook in traditionele werksituaties loopt een bedrijf het risico dat bepaalde gegevens in verkeerde handen terechtkomen, of dat aanvallen van buitenaf bedrijfsprocessen vertragen of zelfs stilleggen.

Bij het uitwisselen van informatie zou men altijd aandacht moeten besteden aan de beveiliging ervan.

Informatiebeveiliging kent drie aspecten:

1. Beschikbaarheid (is mijn informatie toegankelijk?);
2. Exclusiviteit (wordt onbevoegden toegang tot mijn informatie ontzegd?);
3. Integriteit (klopt de inhoud van mijn informatie nog wel?).

100% VEILIGHEID IS NIET HAALBAAR EN NIET NODIG.

100% veiligheid is niet haalbaar en meestal ook niet nodig. De vraag is welke eisen er aan de beveiliging van informatie gesteld moeten worden.

Bijvoorbeeld:

- Hoe lang mag een storing, die mijn informatie ontoegankelijk maakt, duren?
- Wat zijn de gevolgen als onbevoegden mijn informatie onder ogen krijgen
- Is het erg als er wat getalletjes in mijn informatie gewijzigd worden zonder dat ik dat merk?

Toch zijn er, vooral bij het gebruik van internet-technologie, een aantal minimale basisvereisten voor een veilig kennisbeheer:

FIREWALLS

Deze hardware en/of software-oplossingen beschermen het bedrijfsnetwerk onder andere tegen zogenaamde 'denial of service attacks'. Dit zijn aanvallen waarbij krakers bijvoorbeeld grote hoeveelheden gegevens opsturen die de werking van het bedrijfsnetwerk hinderen. Het configureren en de administratie van een firewall is een complexe taak die een grondige kennis van internet technologie vereist. Voor dit soort securityapparatuur is het aan te raden een onderhoudscontract af te sluiten met de verkoper zodat men steeds alle software-upgrades krijgt die nodig zijn om zich af te schermen tegen de nieuwste aanvallen van hackers.

**ENCRYPTIESOFTWARE
VERHINDERD DAT UW
BOODSCHAPPEN
ONDERWEG ONDERSCHEPT
WORDEN.**

ENCRYPTIESOFTWARE

Om te verhinderen dat uw bedrijfsboodschappen onderweg onderschept worden door derden, kunt u zowel in de Internetrouter als in de eindgebruiker software, de nodige encryptiesoftware laten inbouwen. Eventueel kan men ook gebruik maken van secure tunnelling technieken zoals Ipsec. Hierover meer in het hoofdstuk over VPN.

ANTI-VIRUSSOFTWARE

Een niet te onderschatten onderdeel van de beveiliging als het installeren en up-to-date houden van anti-virus software, wordt tegenwoordig reeds als een normaal iets beschouwd. Zeker wanneer men aan e-werken doet, is een goed gebruik van anti-virus software kritisch. Waar normaal gezien de anti-virus software centraal op de bedrijfsserver het inkomende verkeer zal scannen op virussen en een specifieke anti-virussoftware samen met de persoonlijke firewall op de computer van de werknemer automatisch worden geüpdate via het bedrijfsnetwerk, zal bij thuiswerken de deur potentieel wagenwijd open staan voor virussen. Het is daarom ook belangrijk dat deze software regelmatig wordt gecontroleerd.

VPN: VIRTUAL PRIVATE NETWORK

WAT IS VPN?

VPN betekent Virtueel Privaat Netwerk, en betekent concreet dat een onderneming via een netwerk van een Internet Service Provider een beveiligde verbinding tussen de onderneming en haar satellietkantoren opricht, met haar werknemers en eventueel met haar handelspartners.

Er bestaan 4 verschillende types van VPN netwerken:

1. VPN :Netwerk gebaseerde oplossingen
2. VPN :Tunnel gebaseerde oplossingen
3. SSL VPN's
4. Terminal server emulatie

NETWERK GEBASEERDE OPLOSSINGEN.

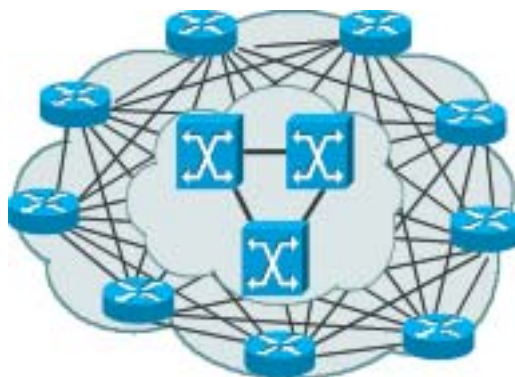
Deze oplossing zijn netwerkgebaseerde oplossingen: de oplossingen worden ingebouwd in het bestaande netwerk van de operator zelf. Hierin onderscheiden we 3 verschillende soorten:

- Frame relay
- MPLS VPN
- IP-VPN (operator)

FRAME RELAY

**FRAME RELAY IS EEN
OUDERE VORM VAN
NETWERK GEBASSEERDE
OPLOSSINGEN.**

Frame Relay is een oudere vorm van netwerk gebaseerde oplossingen om VPN's te bouwen voor ondernemingen. Dit bestaat uit het bouwen van PVC's, ofwel private virtuele connecties naar elk punt van de verbinding.



Figuur 6 : FRAME RELAY

Frame Relay, een mengeling van PVC's voor elk punt van de verbindingen die een onderneming nodig heeft.

Voordelen van Frame Relay VPN:

- stabiel
- geschikt voor alle types van trafiek
- kan internationaal worden ingezet

Nadelen van Frame Relay VPN:

- hoog kostenplaatje
- technologie is verouderd
- biedt geen goede oplossing voor internettoegang

MPLS-VPN

**MPLS-VPN IS EEN NIEUWE
TECHNOLOGIE.**

MPLS-VPN is een Virtual Private Network gebaseerd op MPLS. MPLS (Multiprotocol Label Switching) is een nieuwe technologie die de laatste jaren door de meeste leveranciers van VPN netwerken worden aangeboden.

Wanneer een bedrijf werkt met een IP-VPN backbone, maakt het gebruik van een gedeelde IP-VPN backbone infrastructuur met behoud echter van de veiligheid en een maximale onafhankelijkheid tussen elke VPN.

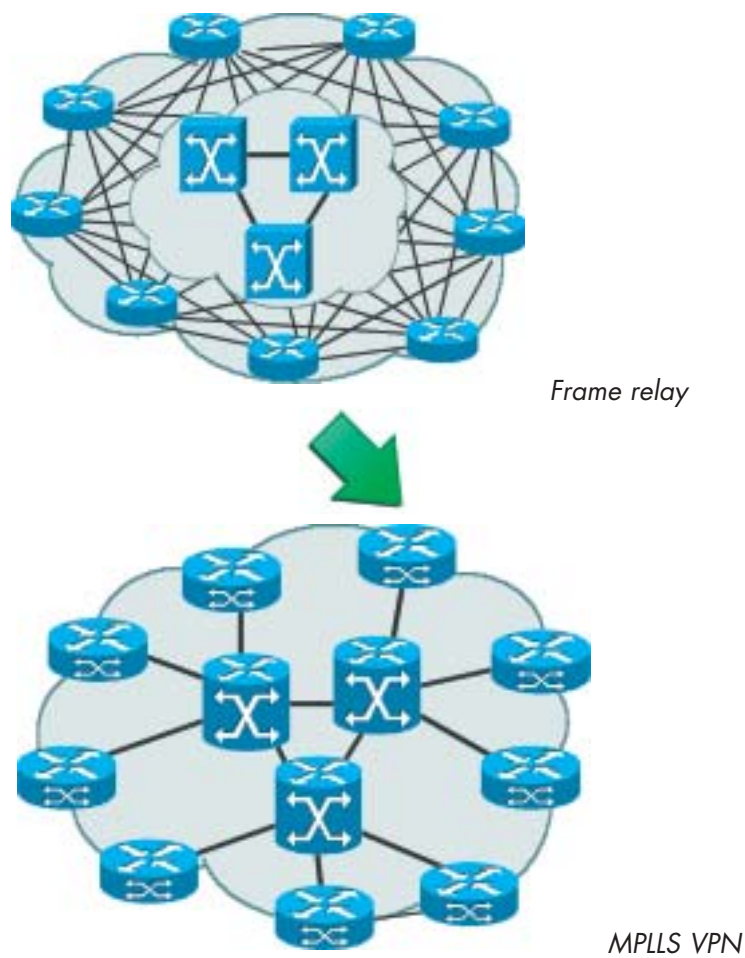
Dankzij de MPLS technologie wordt op deze IP-VPN backbone aan ieder IP pakket een MPLS label toegekend dat uniek is voor elke VPN. Dit MPLS label zorgt ervoor dat enkel communicatie tussen sites uit eenzelfde VPN mogelijk is. Het is met andere woorden het MPLS label waardoor de provider maximale beveiliging en totale onafhankelijkheid kan garanderen voor iedere VPN en dat aan de IP-VPN haar belangrijkste eigenschappen geeft:

Voordelen van MPLS-VPN:

- any-to-any connectiviteit
- flexibiliteit
- schaalbaarheid (uitbreidbaarheid)
- Quality of Service (QoS) op de backbone en op de toegang
- streng Service Level Agreement (SLA) in functie van de verschillende QoS
- uitgebreide rapportering die het mogelijk maakt de VPN optimaal te dimensioneren
- ondersteuning van alle types van IP diensten

Elk van de verschillende sites kan door middel van één van de toegangsdiensten met het IP-VPN MPLS netwerk van de Provider verbonden worden:

- glasvezelverbinding.
- huurlijnen.
- breedband via kabel.
- DSL verbinding (ADSL/SHDSL)
- dial-up access (PSTN/ISDN)



Figuur 7 : FRAME RELAY VS MPLS-VPN

IP/VPN IS GEBASSEERD OP HET INTERNET PROTOCOL IP.

IP/VPN

IP/VPN is een VPN oplossing gebaseerd op het Internet Protocol IP, waarbij over het network van de operator een virtueel IP network wordt geconfigureerd voor de klant.

Voordelen van IP/VPN:

- is een stuk goedkoper is dan de voorgaande oplossingen
- gebruikt een bewezen technologie

Nadelen van IP/VPN:

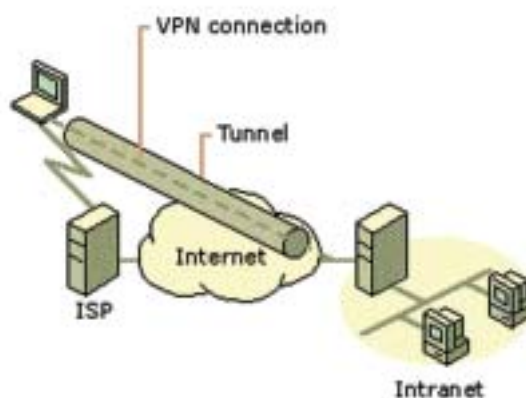
- authenticatie van de VPN op netwerk gebied is moeilijker
- de Internet Toegang.

BIJ HET TWEDE TYPE WORDT EEN BEVEILIGDE TUNNEL GEBOUWD OP EEN PUBLIEK NETWORK.

TUNNEL GEBASEERDE VPN'S.

Het tweede type VPN verbindingen zijnde zogenaamde tunnel gebaseerde VPN oplossingen, waarbij een beveiligde tunnel wordt gebouwd op een publiek netwerk.

Dit gebeurt meestal door het opzetten van een geëncrypteerd algoritme zoals in de volgende voorstelling:



Er zijn 3 erkende standaarden voor tunneling over een publiek netwerk:

PPTP: POINT TO POINT TUNNELING PROTOCOL (GRE)

- Multiprotocol
- Encrypted en encapsulated
- Over een IP netwerk

L2TP: LAYER 2 TUNNELING PROTOCOL

- Multiprotocol
- Encrypted en encapsulated
- Over een netwerk dat point-to-point datagram aflevert (IP, X25, Frame relay, ATM)

IP SEC : IP SECURED

- Multiprotocol
- Encrypted en encapsulated met nieuwe IP header
- Over een IP netwerk

Tunneling als basis voor een VPN netwerk wordt meestal gebruikt indien men een VPN wil opzetten over een publiek netwerk, zoals het internet. Hierbij wordt de VPN dienst niet noodzakelijk door de netwerkprovider geleverd, maar door gelijk welke provider die een dergelijke dienst over het netwerk wil opzetten.

**IN DE PRAKTIJK ZETTEN
OOK NETWERKPROVIDERS
DEZE DIENSTEN OP.**

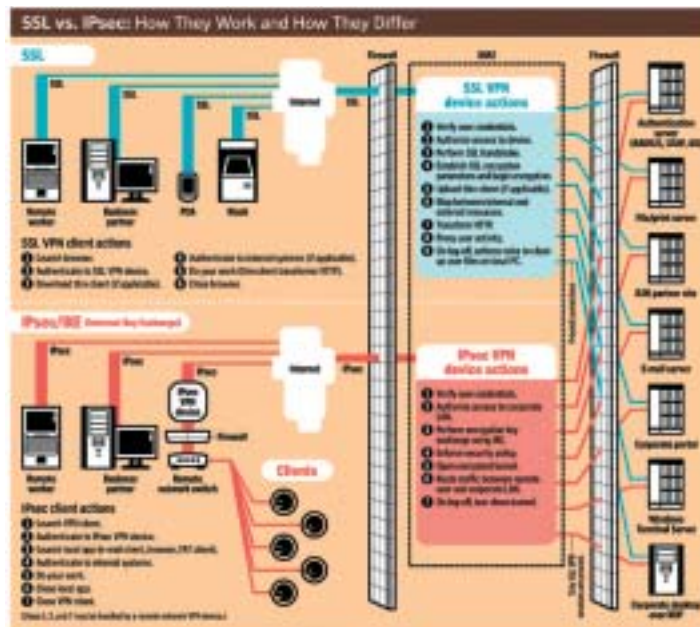
In de praktijk zien we echter dat de netwerkproviders ook dit soort diensten opzetten. Deze diensten zijn dan gebaseerd op het inzetten van netwerkonafhankelijke VPN hardware en software, die in de verschillende locaties van de klant kan worden ingezet.

Dit noemt men CPE-based VPN: Customer Premise Equipment, of vrij vertaald apparaten die bij de klant geïnstalleerd worden. Deze dienst biedt de nodige flexibiliteit om e-werkers thuis te verbinden met de centrale locatie van de onderneming.

De eigenschappen van deze VPN zijn de volgende:

- altijd IP-sec protocol (soms GRE)
- hardware en software worden geleverd.

SSL VPNs



Figuur 8 : SSL VPN

**SECURE SOCKET LAYER
MAAKT DE
WEBVERBINDING VEILIG
VIA INTERNET.**

SSL VPN verbindingen zijn VPN verbindingen die via de SSL laag in het netwerk worden beveiligd. SSL of Secure Socket Layer is de manier om via Internet een webverbinding veilig te maken, door in het netwerkmodel een extra transportbeveiligingslaag in te bouwen.

Dit is een technologie die vooral gebruikt wordt op applicatieniveau, dus in browsers, in home banking applicaties, en bij alle internetapplicaties. Aangezien het gewoon via de browser kan werken, zijn er een aantal uitgesproken voordelen en nadelen:

Voordelen:

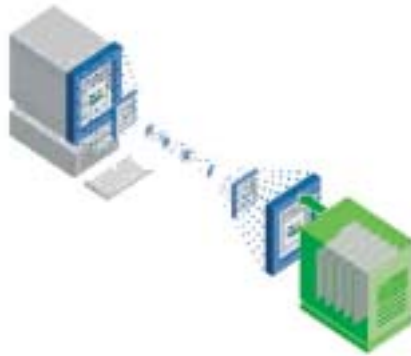
- op IP protocol dus wereldwijd inzetbaar
- flexibiliteit
- de lage kost
- kan via een gewone browser geïnstalleerd worden via Internet.
- geen project uitrol

Nadelen :

- niet gestandaardiseerd
- stabiliteit over internet is niet gegarandeerd
- authenticatie (Login en password in log files)
- geen perimeter security
- maakt gebruik van browser (veel security issues in Windows, andere OS)

TERMINAL-EMULATIE.

De laatste vorm van VPN is een terminal-emulatie, dit betekent dat de applicatie op afstand wordt nagebootst. De applicatie kan dan op afstand vanop een terminal worden opgevraagd



Figuur 9 : TERMINAL EMULATIE

Voordelen:

- op IP (worldwide)
- flexibiliteit
- totale kost voor de onderneming.
- bandbreedtegebruik

Nadelen:

- dikwijls een trage reactietijd voor het werken met een applicatie.
- geen perimeter security.