



Business



Bedrijfsnetwerk
van de toekomst.

Introductie

We staan aan het begin van een nieuw tijdperk, waarin alles met elkaar in verbinding staat. De toestroom van data, groei van Internet of Things-toepassingen, cloudapplicaties en automatisering vragen om een snel, stabiel en betrouwbaar netwerk. Je bent waarschijnlijk al overtuigd van het nut en de noodzaak van digitalisering in je bedrijf. Maar waar begin je?

Bij een goed presterend bedrijfsnetwerk. Dat is de basis voor je bedrijfsvoering. Ook voor het kantoor van de toekomst. Daarom is het belangrijk dat je het niet vergeet tijdens de digitale transformatie van je organisatie. Of het nu gaat om efficiënter verkopen met een slim CRM-systeem of je klanten beter bedienen door een digitale klantenservice, de basis is een bedrijfsnetwerk dat klaar is voor de toekomst.

Wat is de noodzaak van een nieuw en toekomstbestendig netwerk? Hoe implementeer je het bedrijfsnetwerk van de toekomst? En welke mogelijkheden heeft een ICT'er om het bedrijfsnetwerk veilig te houden, juist nu mensen ook vanuit huis werken? Vertellen we je in dit e-book.

Inhoud

1. Toen, nu & de toekomst	4
1.1 Een terugblik	4
1.2 Communiceren via een intern netwerk	4
1.3 De toekomst: glasvezel	4

2. De noodzaak van een toekomstbestendig bedrijfsnetwerk	5
2.1 Nieuwe technologieën	5
2.2 Internet of Things en 5G	5
2.3 Artificial Intelligence (AI)	6
2.4 Het nieuwe werken	6
2.5 Transitie naar de cloud	6
2.6 Cybersecurity	6

3. Zo realiseer je het bedrijfsnetwerk van de toekomst	7
3.1 Het voortraject	7
3.2 Hoe is je back-up geregeld?	8

4. Een veilig bedrijfsnetwerk	9
4.1 In 5 stappen een veilig netwerk voor je medewerkers	9
4.2 Tips voor veilig thuiswerken	10

5. Het beste netwerk voor je bedrijf	11
5.1 Internet over zakelijk glasvezel	11
5.2 4G back-up	11
5.3 Wifi Plus	11
5.4 IP-VPN voor de grootzakelijke markt	12
5.5 Next Gen Firewall	12
5.6 Internet van Odido Zakelijk	12
5.7 Stappenplan: een bedrijfsnetwerk implementeren via Odido	13

1. Toen, nu & de toekomst

1.1 Een terugblik

Altijd verbonden en online, het lijkt zo vanzelfsprekend. Maar op het gebied van telefonie, internet en connectiviteit is er veel veranderd in de afgelopen 20 jaar. Door de opkomst van digitalisering ontstonden er nieuwe gebruiksmogelijkheden voor consumenten en bedrijven. Steeds meer bedrijven kregen beschikking over internet. Vaak via een relatief trage inbelverbinding, waarbij je inbelde op een telefoonnummer. Internetten en telefoneren op hetzelfde moment kon niet.

ISDN bood een oplossing. Naast dat je meer data over deze lijn kon verzenden, was het eindelijk mogelijk om tijdens het telefoneren e-mails te verzenden.

Bij gebruik van ISDN door de afnemer is de verbinding tussen de wijkcentrale en het telefoontoestel ook digitaal.

Met de opkomst van internet kon je ook telefoneren via datzelfde internet. Bellen via je internetverbinding, beter bekend als VoIP (Voice over IP) was vanaf dat moment beschikbaar. Voor het verkeer tussen telefooncentrales werden uiteindelijk glasvezelkabels gebruikt. En zo kwam de digitalisering van het telefoonnetwerk in een stroomversnelling.

1.2 Communiceren via een intern netwerk

Het internet werd in eerste instantie alleen gebruikt door de overheid en voor onderwijs. Pas vanaf 1993 konden ook bedrijven er particulieren er op. Vanaf die tijd ontstonden ook de zogenaamde bedrijfsnetwerken.

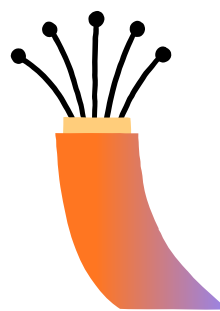
Een bedrijfsnetwerk is simpel gezegd een verzameling computers die met behulp van speciale apparatuur aan elkaar gekoppeld en met elkaar verbonden zijn. De juiste software zorgt ervoor dat het netwerk goed functioneert.

Vanaf 2001 veranderde het internet van web 1.0 naar web 2.0. In plaats van alleen webpagina's lezen, werd het ook mogelijk om zelf tekst en beeld te uploaden. Toen internetgebruikers informatie konden publiceren en delen werd internet écht onmisbaar.

1.3 De toekomst: glasvezel

Het datagebruik in Nederland neemt jaarlijks met ongeveer 40% toe. Steeds meer apparaten zijn in de toekomst met elkaar verbonden en mensen willen altijd en overal toegang hebben tot hun bedrijfsnetwerk. Afgezien van de ingewikkelde fysieke verbindingen die de infrastructuur van internet vormen, verloopt het huidige internetverkeer bijna helemaal via glasvezelkabels.

Glasvezel is de meest betrouwbare en toekomstbestendige manier om een vaste verbinding met voldoende capaciteit te realiseren. Met een glasvezelverbinding heeft je bedrijf meteen toegang tot alle data en software die je nodig hebt. En kunnen al je medewerkers snel bestanden delen en versturen, videobellen en met online software werken.



2. De noodzaak van een toekomstbestendig bedrijfsnetwerk

De ontwikkelingen op het gebied van automatisering en digitalisering gaan razendsnel. De toenemende connectiviteit en explosie aan datastromen vragen om een netwerk met hoge snelheden en ongekeerde capaciteit. Alleen zo kunnen we in de groeiende databehoeften voorzien.

Organisaties die digitaal willen transformeren, moeten ook hun bedrijfsnetwerk onder de loep nemen. Nieuwe technologieën zoals het Internet of Things, 5G en AI vragen om een andere inrichting van het bedrijfsnetwerk.

2.1 Nieuwe technologieën

Er breekt een nieuw tijdperk aan waarin nieuwe en slimme technologie toegankelijker is dan ooit. Toepassingen zoals 5G, Internet of Things (IoT) en artificial intelligence (AI) vereisen dat data meteen beschikbaar moet zijn.

Je bedrijfsnetwerk moet de toestroom van dataverkeer aankunnen, toegang tot cloudapplicaties mogelijk maken én samenwerkingen op afstand ondersteunen.

2.2 Internet of Things en 5G

Via het Internet of Things communiceren 'dingen' met elkaar. Het geeft machines, voertuigen, containers en gebouwen de software, sensoren en connectiviteit om ze te monitoren en te controleren. Met de data die

daaruit voorkomt kunnen we nieuwe bedrijfsmodellen bouwen, nieuwe diensten aanbieden of efficiëntie verbeteren. Via 5G. De vijfde generatie draadloze mobiele netwerktechnologie die flink wat Internet of Things-oplossingen mogelijk maakt.

5G biedt bedrijven meer dan alleen een hogere snelheid. Met 5G gebruik je draadloze netwerken als nooit tevoren. Sluit meerdere apparaten op 1 verbinding aan en de dekking wordt niet alleen gebaseerd op personen met telefoons, maar ook op een wereld vol sensoren die het Internet of Things voeden.

Voor zakelijke en industriële toepassingen belooft 5G ook veel goeds. Gegevens worden tot wel 10 keer sneller overgedragen dan tot nu toe mogelijk was. Vooral belangrijk als je grote hoeveelheden gegevens wil versturen, zoals in industriële augmented- of virtual reality-toepassingen en hoge kwaliteit videofeeds.



Uit onderzoek van ARP Nederland blijkt dat er in 2006 2 miljard apparaten met het internet verbonden konden worden. In 2023 staat de teller van verbonden IoT-apparaten op zo'n 50 miljard. Ook geeft 50% van de IT-specialisten aan dat de hoeveelheid data in hun organisatie ieder jaar consistent groeit met wel 24% per jaar.

Door 5G-netwerken kunnen straks tot een miljoen apparaten per vierkante kilometer met elkaar communiceren via het Internet of Things. Op die manier werken apparaten en data naadloos samen. Door apparaten en locaties met elkaar te verbinden via het Internet of Things, krijg je inzicht in bedrijfsprocessen en werk je nóg efficiënter.

2.3 Artificial Intelligence (AI)

Data wordt in de toekomst steeds meer gebruikt om precies te kunnen bepalen waar de klantbehoefte zit. Zo bied je een op maat gemaakte oplossing. En ook artificial intelligence zal in steeds sterkere mate worden gebruikt om in te spelen op de klantbehoefte. We zien nu al veel toepassingen waarbij klanten worden geholpen door 'chatbots' die informatie verschaffen door middel van AI.

Als bedrijf kom je ooit op het punt dat de hoeveelheid data niet meer te overzien is. Dan is het fijn als een geautomatiseerd proces je het meeste werk uit handen neemt. Door al die data en analyses worden steeds meer bedrijfsprocessen en beroepsgroepen geautomatiseerd. En die hoge connectiviteit vraagt om een ander netwerk.

2.4 Het nieuwe werken

De tijden dat een bedrijfsnetwerk alleen desktop-computers bediende is verleden tijd. Tegenwoordig heeft iedere medewerker 2 of meer (mobiele) apparaten en vaak een laptop waarmee verbinding met het netwerk wordt gemaakt. Op verschillende plekken in binnen- en buitenland. De werkplek van nu vraagt dan ook het optimale van bedrijfsnetwerken: van capaciteit en flexibiliteit tot beveiliging. Deze ontwikkeling komt in een stroomversnelling door de IT-oplossingen die het mogelijk maken om op afstand met collega's samen te werken. Denk aan het uitwisselen van grote databestanden, videobellen, chatten en het gebruik van CRM-systemen in de cloud.

2.5 Transitie naar de cloud

De opkomst van clouddiensten maakt dat snelle, goede en betrouwbare koppelingen met de cloud essentieel zijn voor je bedrijf. Werken in de cloud betekent dat je medewerkers vanaf elk apparaat en op elke locatie toegang hebben tot bestanden en programma's. Optimaal profiteren van cloud-technologie vereist een nieuwe manier van applicatie-ontwikkeling en beheer van cloudapplicaties.

Maar werken in de cloud betekent meer. Meer integratiemogelijkheden met andere systemen, zoals CRM, GoogleDocs, Salesforce en Microsoft Teams bijvoorbeeld. Door de digitale omgeving te koppelen met een CRM-systeem of online agenda kan je efficiënter communiceren met klanten en collega's.

2.6 Cybersecurity

Apparaten die met elkaar communiceren, processen die automatisch worden uitgevoerd door kunstmatige intelligentie; het zijn interessante ontwikkelingen. Maar het betekent ook dat cybersecurity nóg belangrijker wordt. Het enorme aantal met elkaar communicerende apparaten zorgt alleen al voor meerdere punten waarop een aanval ingezet kan worden.

Aan de andere kant kan slimme inzet van machine learning juist helpen bij het ontdekken, herkennen én bestrijden van aanvallen door ver ontwikkelde patroonherkenning. Een netwerk dat deze dataverwerking aan kan, is belangrijk voor je organisatie.

3. Zo realiseer je het bedrijfsnetwerk van de toekomst

De reden voor het aanleggen van een bedrijfsnetwerk kan per organisatie verschillen. Vaak wil je iedereen de mogelijkheid geven om overal te kunnen werken. Dat kan met een groter of een extra netwerk.

Veel bedrijven zijn tevreden met hun telecomoplossingen. Maar het bedrijfsleven digitaliseert steeds meer. Nieuwe technieken en technologieën worden nog vaak als ingewikkeld beschouwd. Om niet achter te blijven, is meegaan met de tijd én je organisatie belangrijk.

Vraag je je af of je bedrijfsnetwerk klaar is voor de toekomst? In het volgende hoofdstuk vertellen we je alles over de voordelen van een futureproof, goed beveiligd bedrijfsnetwerk. En over het implementatieproces.

3.1 Het voortraject

Ga je verhuizen? Dan is dit het ideale moment om je netwerk eens na te kijken en, waar nodig, op de schop te nemen. Maar er kunnen ook andere redenen zijn om uit te breiden naar een bedrijfsnetwerk. Stel jezelf de volgende vragen:

- Stijgt het datagebruik van je organisatie exponentieel snel?
- Wil je meer flexibiliteit in waar, wanneer en hoe je medewerkers werken?
- Wil je de efficiëntie van je bedrijfsvoering vergroten?

Veel bedrijven zijn bang om volledig afhankelijk te zijn van hun netwerk. Wat zijn de kosten als het netwerk uitvalt? Welke back-up is dan noodzakelijk?

En wat kost het eigenlijk om een tweede netwerk te graven? Allemaal zaken waar je goed over na moet denken als je wil uitbreiden naar een bedrijfsnetwerk.

Maak een kosten-batenanalyse. Wat wil je investeren en wat levert het je uiteindelijk op? Wat kost het je bijvoorbeeld als je fabriek of organisatie stil ligt? En ben je een mkb, maar zijn je klanten grote corporates? Ook dan wil je altijd goed bereikbaar zijn.

Een bedrijfsnetwerk maakt meer mobiliteit in de organisatie mogelijk. En biedt gemak en flexibiliteit voor medewerkers én klanten. Bedenk goed: wat je nu nodig hebt. Maar ook waar je naartoe wil. Met een goed werkend bedrijfsnetwerk optimaliseer je bedrijfsvoering en bereikbaarheid.

Onze specialisten kijken met je mee waar de uitdagingen zitten.

Waar loopt je bedrijf tegenaan? Heb je genoeg capaciteit? En waar staan jullie nu? Zit je organisatie al in de cloud of durf je het nog niet aan omdat jullie die bedrijfszekerheid nog niet hebben?



“Denk aan terugvalvoorzieningen, zoals een back-up netwerk. Maar ook veiligheid als in cybersecurity.”

3.2 Hoe is je back-up geregeld?

Het risico van een netwerkstoring moet goed in kaart worden gebracht. Bij een grote organisatie waar alles digitaal geregeld is, moet de impact zo klein mogelijk zijn. Wat heb je nodig als het misgaat? Zaken als imagoschade, de levering van producten of je bereikbaarheid neem je hierin mee.

Hoeveel ben je bereid te investeren in zekerheid en veiligheid? Als het netwerk eruit ligt, moet je dan een fysieke handeling uitvoeren? En welke veiligheid bouw je in? Denk aan terugvalvoorzieningen, zoals een back-up netwerk. Maar ook veiligheid als in cybersecurity. Zodat je goed beschermd bent tegen hackers en andere cybercriminelen.

4. Een veilig bedrijfsnetwerk

De hoeveelheid data die we dagelijks ontvangen en versturen groeit. En omdat we niet meer alleen op kantoor werken, zijn we extra kwetsbaar voor cybercriminaliteit. Medewerkers gebruiken bijvoorbeeld hun eigen telefoon of laptop om bedrijfsdocumenten te openen. Dat brengt de nodige risico's met zich mee voor je klant- en bedrijfsgegevens.

Werk je veel met privacygevoelige gegevens en bedrijfskritische systemen, dan loop je meer risico om gehackt te worden. Een onbeveiligd netwerk is dan funest voor je bedrijf. Ook dan wil je altijd goed bereikbaar zijn.

Onze specialisten kijken met je mee waar de uitdagingen zitten. Waar loopt je bedrijf tegenaan? Heb je genoeg capaciteit? En waar staan jullie nu? Zit je organisatie al in de cloud of durf je het nog niet aan omdat jullie die bedrijfszekerheid nog niet hebben?

Een bedrijfsnetwerk maakt meer mobiliteit in de organisatie mogelijk. En biedt gemak en flexibiliteit voor medewerkers én klanten. Bedenk goed: wat je nu nodig hebt. Maar ook waar je naartoe wil. Met een goed werkend bedrijfsnetwerk optimaliseer je bedrijfsvoering en bereikbaarheid.

4.1 In 5 stappen een veilig netwerk voor je medewerkers

Om ervoor te zorgen dat je medewerkers altijd via een veilig netwerk werken, is het slim om in je IT-infrastructuur een stukje monitoring in te richten. Zo kom je erachter wie, waar en wanneer toegang wil hebben tot het netwerk. Segmentatie mag daarbij niet ontbreken. Zorg dat je gepatched bent en draai wekelijks back-ups. Investeer daarvoor in een goede tool die deze werkzaamheden uit handen neemt, want wekelijks back-ups draaien kan tijdrovend zijn. Zorg als laatste voor een fatsoenlijke firewall en een goed antivirussysteem.

Kort samengevat zijn dit de 5 stappen voor een veilig netwerk:

1. Segmenteren
2. Patchen
3. Wekelijks back-ups draaien
4. Een firewall van goede kwaliteit
5. Een goed antivirussysteem

4.2 Tips voor veilig thuiswerken

Wat kun je als IT'er doen om het netwerk veilig te krijgen en wat moet de medewerker doen (of vooral niet)? We geven 3 tips om met veilige techniek en technologische middelen een stuk veiliger vanuit huis te werken.



TIP ❶ Kijk uit voor phishingmails

Cybercriminelen spelen graag in op actualiteiten. Bijvoorbeeld door kwaadwillende applicaties in te zetten, phishingmails te versturen of malware te verspreiden. Klik niet op links in e-mailberichten, open geen onbekende bijlagen en vul geen gegevens in bij e-mailberichten die je niet verwacht of die van een onbekende afzender komen. Zorg dat je medewerkers zich bewust zijn van de gevaren. Informeer ze goed en voer regelmatig een test uit.

TIP ❷ Beveilig met een tweefactor-authenticatie

Data of apps die je op afstand gebruikt, bescherm je het beste met een tweefactorauthenticatie. Een medewerker heeft dan naast een wachtwoord ook een andere stap nodig om in te kunnen loggen, zoals een bevestiging via een telefoon. Daarnaast is het slim en veilig om je wachtwoorden te beheren in een wachtwoordmanager. Een wachtwoordmanagers beveiligt je data door middel van geavanceerde encryptie.

TIP ❸ Zorg dat iedereen dezelfde basiskennis heeft

Het is fijn als elke medewerker basiskennis heeft van IT-security. Maar niet iedereen is daar even handig in. Zorg voor een algemeen document waarin belangrijke informatie over beveiliging en security duidelijk staat beschreven. Bijvoorbeeld: log nooit in op een openbaar netwerk, maak een back-up van je documenten en laat computers niet onbeheerd achter. Zo verklein je het risico op een datalek of cyberaanval en zet je cybercriminelen buitenspel.

5. Het beste netwerk voor je bedrijf

5.1 Internet over zakelijk glasvezel

Met internet over zakelijk glasvezel (FTTO) krijg je kwalitatief de beste, snelste en meest betrouwbare oplossing voor internet in je bedrijf. Het grote verschil met DSL en kabel is dat data niet via koperdraad of kabel, maar via lichtsignalen wordt verzonden. Het signaal reist dus letterlijk met de snelheid van het licht.

Zakelijk glasvezel internet is geschikt voor bedrijven vanaf 10 medewerkers of bedrijven die sterk afhankelijk zijn van een snelle en stabiele internetverbinding. Over een glasvezelverbinding haal je vaak veel hogere snelheden en de betrouwbaarheid is maximaal. De upload- en downloadsnelheid is bij zakelijk glasvezel gelijk, wat bij andere oplossingen, zoals kabelinternet, niet het geval is. De afstand van je bedrijf tot de wijkcentrale heeft geen invloed op de internetkwaliteit.

Je bedrijf wordt met internet over zakelijk glasvezel direct aangesloten op het hoofdnetwerk van je provider. Glasvezel ligt bij steeds meer bedrijven vlak voor de deur. Zo niet, dan leggen we het voor je aan. In beide gevallen kan zijn dat de doorlooptijd een paar weken is. Glasvezel is de meest betrouwbare en toekomstbestendige manier om een vaste verbinding te maken. Al je medewerkers kunnen zonder hinder tegelijk bestanden delen, videobellen en op hetzelfde moment met online software werken. Doorgroeien naar nog hogere snelheden is altijd mogelijk.

5.2 4G back-up

Bij storingen op je vaste internetlijn schakelt je router automatisch over naar ons mobiele 4G-netwerk. Zo weet je zeker dat je altijd een werkende internetverbinding hebt. Door deze back-up kunnen je medewerkers gewoon doorwerken in de cloud en bellen via wifi (VoIP). Als de storing voorbij is, schakelt de 4G back-up automatisch terug naar de vaste lijn. Het enige nadeel is dat je afhankelijk bent van de capaciteit en het bereik van de 4G-zendmast in de buurt. Locatie en drukte hebben namelijk invloed op de kwaliteit van de verbinding.

5.3 Wifi Plus

Ervaar je vaak wifi-problemen op kantoor of als je vanuit huis werkt? Met Wifi Plus breid je het wifi-netwerk uit met draadloze wifi-punten. Die creëren een eigen mesh-netwerk; een soort net van verschillende wifi-punten die contact met elkaar hebben en elkaar versterken. Zo heb je ononderbroken, krachtige wifi in elke ruimte. Alle wifi-punten staan met elkaar in verbinding. Ze communiceren het wifisignaal en zorgen dat het hele netwerk snel en betrouwbaar is, in plaats van dat de focus op één punt ligt.

In plaats van de wifi te versterken of verspreiden, zet Wifi Plus meer in op het optimaliseren van het wifinetwerk. De ingebouwde algoritmes zorgen dat het systeem de allerbeste wifiverbinding detecteert.

Meer weten?
Ga naar odido.nl/zakelijk/internet/wifi-plus

5.4 IP-VPN voor de grootzakelijke markt

Virtual Private Network via IP-protocol (IP-VPN) is een besloten netwerk voor datacommunicatie binnen je organisatie. Met een op IP-VPN gebaseerd bedrijfsnetwerk maak je 1 betrouwbaar, kosteneffectief netwerk tussen al je vestigingen. Medewerkers op verschillende locaties werken zo makkelijk samen.

Ook hebben ze op afstand veilig, snel en makkelijk toegang tot alle beschikbare toepassingen en gegevens binnen je bedrijfsnetwerk. Zoals Office apps, fileservers, bedrijfsspecifieke ERP- en CRM-applicaties en supply chain management toepassingen.

Meer weten? Ga naar odido.nl/zakelijk/oplossingen

SD-WAN: veilig netwerk vanaf verschillende locaties

In het digitale tijdperk is snelheid nodig om netwerken aan te passen en eenvoudig om bepaalde apps een andere prioriteit te geven. Vroeger betekende dit een aparte configuratie van alle netwerkcomponenten. Dit veranderde met SD-WAN (Software-Defined Wide Area Network). Hiermee kan je als bedrijf je netwerk snel aanpassen, centraal monitoren, de prestaties van hybride netwerken verbeteren én publieke clouds eenvoudig en veilig integreren.

Als je medewerkers verbinding willen maken met het bedrijfsnetwerk moeten ze een VPN aanzetten. Cloudapps zoals Microsoft Office 365 gebruiken ze makkelijk vanaf de browser. Daar is geen VPN voor nodig. SD-WAN creëert als het ware een extra softwarelaag voor elke locatie waar je werkt, waarbij het niet uitmaakt of je vanaf 4G, 5G of de wifi verbinding maakt. Je creëert de illusie dat het één groot netwerk is. Werknemers maken makkelijk verbinding via hun telefoon, laptop, tablet of een ander apparaat.

SASE: cloud-based platform

Werken je medewerkers vanaf verschillende locaties? Dan is Secure Access Service Edge (SASE), de opvolger van SD-WAN, een handige oplossing voor een veilig netwerk. Het is een cloud-based platform dat netwerk en veiligheid in 1 cloudomgeving samenbrengt. Waar je met SD-WAN nog gebonden was aan een locatie, maakt het met SASE niet uit waar je werkt. Ook heb je geen fysieke firewalls meer nodig. SASE integreert netwerk- en beveiligingsdiensten, waardoor je gebruikers altijd makkelijk en veilig werken; waar ze ook zijn of welk apparaat ze ook gebruiken.

5.5 Next Gen Firewall

Next Gen Firewall beschermt je bedrijf nog beter tegen aanvallen van buitenaf. Een normale firewall kijkt alleen naar de bron en het doel, gecombineerd met een protocol en poort. Op basis daarvan bepaalt de firewall of hij het verkeer toelaat of blokkeert. Een Next Gen Firewall doet daar een schepje bovenop. Deze firewall kijkt in het netwerkverkeer om te bepalen welke applicatie wordt gebruikt en scant en controleert zo de inhoud. Zo controleert deze firewall extra goed op antivirus, anti-spyware, URL-filtering en zero-day-aanvallen (aanvallen op zwakke plekken in je software).

5.6 Internet van Odido Zakelijk

Internet is onmisbaar en belangrijk voor de continuïteit van je onderneming. Je wil uit kunnen gaan van de betrouwbaarheid en snelheid van je internet. Videobellen met een klant, razendsnel bestanden downloaden of een back-up naar de cloud maken. Het moet gewoon goed werken.

Met DSL of Fiber-To-The-Home (FTTH) Internet heb je naast razendsnel zakelijk internet ook toegang tot bijvoorbeeld telefonie, alarmering en pinnen via een veilige verbinding. Sneller dan snel internet nodig? Ons landelijk dekkende glasvezelnetwerk garandeert dat we je bedrijf altijd efficiënt kunnen aansluiten op glasvezel. Up- en downloaden tot wel 1 Gbit/s. Kan gewoon.

Het beste netwerk voor:

Kleinzakelijk

(1-20 medewerkers)
Zakelijk Internert
Glasvezel tot wel
500/500 Mbit/s

Mid- en grootzakelijk

(meer dan 20 medewerkers)
Zakelijk Internert DSL, FTTH
of Glasvezel tot wel
1Gbit/s



5.7 Stappenplan: een bedrijfsnetwerk implementeren via Odido

Je hebt alle redenen om een bedrijfsnetwerk aan te leggen overwogen en doorgenomen. Hoe ga je nu verder? Vertellen we je. Of het een ingewikkeld proces is om een netwerk aan te leggen, hangt af van een aantal factoren. In ons stappenplan nemen we je mee in dit proces.

1. De voorbereiding

Binnen 2 weken plannen we een bezoek op locatie. Samen bespreken we alle technische voorwaarden voor de installatie en bepalen we de interne glasvezelroutes. Na het locatiebezoek ontvang je een rapport met daarin alle gemaakte afspraken.

2. Vergunningsaanvragen

We vragen alle nodige vergunningen aan. Ook werken we eventuele boorplannen uit en dienen we die in bij de juiste overheidsinstanties. Ondertussen bestellen we alle materialen en apparatuur.

3. De uitvoeringsfase, stap voor stap

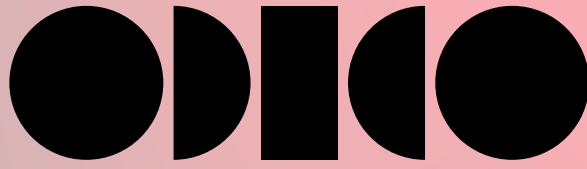
Als de vergunningen en materialen binnen zijn, start een aannemer binnen 1 á 2 weken met de civiele werkzaamheden. Denk aan geulen graven voor de buizen en mogelijk boorwerk. Daarna blazen we de glasvezelkabel met lucht in de buizen. We lassen de glasvezels en maken de verbinding met de glasvezelring. Als laatste test de aannemer de Network Termination Unit (NTA). Die zet glasvezel om naar ethernet. We schakelen de circuits en diensten in en leveren ze op.

4. Communicatiemomenten

Tijdens het hele leverproces zijn er vier belangrijke communicatiemomenten met je contactpersoon bij Odido. Je krijgt dan informatie over:

- De opdrachtbevestiging en wanneer we langskomen voor een locatiebezoek.
- Hoe de vergunningaanvraag eruitziet en wat er in ons locatierapport staat.
- Welke vergunning je krijgt, wanneer we starten met de werkzaamheden en wanneer we verwachten klaar te zijn.
- Hoe de oplevering verloopt.

Wil je meer weten over het realiseren van een veilig en toekomstbestendig bedrijfsnetwerk? Lees alles over [SD-WAN](#).
Of bel ons op 085 – 200 68 60.



Business

Het kan ook zo

Odido