



# Naar een volwassen digitale werkplek: Hoe je slimmer werkt in de hybride omgeving

> Meebewegen met het veranderende IT-landschap

Nu medewerkers niet altijd meer op dezelfde plek werken, is er een compleet nieuw IT-landschap ontstaan. Er zijn daardoor volop kansen voor zowel bedrijven als hun medewerkers. Maar dat gaat niet zonder horten of stoten. De hybride werkplek is vooral een digitale werkplek en dit vergt het nodige aan aanpassingen in de IT-structuur en het beheer daarvan.



## De thuiswerkrevolutie

Dat werken niet altijd meer automatisch betekent 'op kantoor' heeft een revolutie in het denken teweeggebracht. Natuurlijk, thuis en op afstand werken is al langer voor een deel van de medewerkers heel normaal. Maar de laatste jaren is dit in een stroomversnelling geraakt.



Voordat de Covid-19 pandemie optrad, werkte de gemiddelde medewerker zo'n twee dagen per maand vanuit huis. Tijdens de pandemie was dat uiteraard veel meer. Na

Covid-19 was de verwachting dat dit zou terugvallen en dat de gemiddelde werknemer pakweg een dag per week thuis zou werken. Maar [uit onderzoek](#) van het Duitse instituut Ifo onder 36 duizend werknemers in 27 landen blijkt dat de Nederlander gemiddeld bijna twee dagen per week thuis werkt (1,8 dag om precies te zijn). En het ligt niet in de lijn der verwachting dat dit af zal nemen.

## > Betere privé/werk-balans

Voor de meeste medewerkers betekent de flexibiliteit in het kunnen werken op elke plek – en dus niet per se alleen op kantoor óf thuis – een grote verbetering. Want die flexibiliteit van locatie biedt ook enige flexibiliteit in het *moment* van werken. Dat biedt mogelijkheden voor de privé/werk-balans. Dagelijkse dingen die voorheen kunst- en vliegwerk vergden gaan nu als vanzelf. De kinderen uit school halen, sporten of een snelle boodschap kan 'even tussendoor' en komt de medewerkerstevredenheid ten goede.

Voor de werkgever is het bieden van deze flexibiliteit inmiddels een must. Medewerkers werven en daarna behouden is een grote uitdaging. Een digitale werkplek waarbij medewerkers gemakkelijk overal kunnen werken, waar en wanneer het hen uitkomt, is inmiddels een secundaire arbeidsvoorwaarde die als heel normaal wordt ervaren.

## Meebewegen met het veranderende IT-landschap

Voor de werkgever zit er ook een keerzijde aan. Want hoe richt je zo'n digitale werkplek eigenlijk in? Welke hardware, software, contracten en abonnementen heb je nodig? Hoe zorg je ervoor dat je mensen goed kunnen samenwerken? En hoe bied je véél flexibiliteit, maar houd je de boel wel beheersbaar en veilig? Daar begint voor veel bedrijven een lange en moeizame zoektocht.

Wat het lastig maakt: je begint niet vanuit niets. Er is al een IT-omgeving, gebaseerd op de oude situatie. Er zijn al computers en software, en er zijn al verplichtingen op het gebied van contracten, licenties en abonnementen. De bestaande situatie is daarbij zeker niet altijd een optimaal uitgangspunt voor de flexibele, digitale werkplek. Het is een beetje als het moderniseren van een rijdende trein.

Waar je bijvoorbeeld tegenaan loopt:

- Je werkt met verschillende partijen. Een of meerdere leveranciers voor hardware en software. Met elke leverancier heb je andere afspraken en contracten.
- Bij software heeft elke leverancier zijn eigen portaal, met eigen inlog om je abonnementen en licenties te beheren. Je raakt de weg kwijt in de verschillende SLA's, afspraken en contactpersonen.
- Contracten kunnen overlappen. Gaat er iets mis, dan loop je kans dat leveranciers naar elkaar wijzen voor ondersteuning. Heb je bijvoorbeeld een contract voor het beheer van je netwerk en elders een internetabonnement, bij wie moet je dan zijn wanneer je niet online kunt?
- Als je organisatie groeit, is het lastig om op te schalen. Bij elke leverancier moet je apart je contract uitbreiden, of hardware aanschaffen. En krimp van de organisatie geeft vaak nog meer problemen.

Kortom, het overzicht is weg en daarmee de rust en zekerheid. In het beste geval zijn er geen problemen, maar is de efficiëntie ver te zoeken.

Het belangrijkste wat hier ontbreekt: één aanspreekpunt waar je altijd terecht kunt. Voor uitbreiding, voor problemen, voor advies en voor de zaken die simpelweg geregeld moeten worden. Want wie heeft nog het totaaloverzicht en kan vertellen hoe alles met elkaar samenhangt en –werkt?

## IT-beheer in de digitale werkomgeving

Ga je aan de slag met IT-beheer in een hybride omgeving? Dan gaan sommige zaken een grotere rol spelen dan voorheen. Zes aandachtspunten:



### 1. Hardware

De keuze van de juiste computers voor je medewerkers is een omvangrijke klus, met veel consequenties. Waar je misschien bij een softwaretool nog relatief gemakkelijk kunt switchen, zit je bij hardware toch minstens drie tot vier jaar aan dezelfde apparatuur gebonden. Ga je voor PC's of laptops, wil je werken met virtuele machines, kies je voor Windows of Apple? Allemaal keuzes waar je voor langere tijd aan vast zit.

Ga je kopen of leasen? Het antwoord op deze vraag is niet voor elke organisatie hetzelfde. Beide opties hebben voor- en nadelen, waarbij er binnen lease ook nog eens veel verschillende mogelijkheden zijn. Het is belangrijk om hierin de juiste keuzes te maken.



### 2. Beheer en monitoring

Beheer is een essentieel onderdeel van je IT. Daarbij gaat het om het gebruiksklaar maken van apparatuur, bijvoorbeeld als er een nieuwe medewerker bij komt. Maar ook om het installeren van beveiligingspatches of updates van besturingssysteem of software.

Bij beheer hoort ook het continu monitoren en diagnosticeren van alle op het netwerk aangesloten apparaten en systemen. Dat gaat niet enkel om beveiliging, denk bijvoorbeeld ook aan het installeren van triggers op de computers die bijvoorbeeld kunnen aangeven dat een computer langere tijd voor 80 procent of meer wordt belast. In dat geval is er vermoedelijk iets met het systeem aan de hand, en mag je er ook vanuit gaan dat de gebruiker daar last van heeft. Oplossen dus.

Beheer en monitoring gaat trouwens veel verder dan alleen de traditionele computers. Ook servers, printers en tegenwoordig steeds meer slimme apparatuur als camera's worden opgenomen in de beheerstructuur van een organisatie.



### 3. Software

Een groot deel van je software gebruik je tegenwoordig 'as a service', dus op basis van abonnementen. Dat levert veel voordelen op. Zo hoef je de software niet bij elke update opnieuw aan te schaffen. Bovendien betaal je alleen voor wat je nodig hebt. Dus geen bulklicenties waarbij je altijd net te kort komt wanneer je bedrijf groeit. Daarnaast kun je ook eenvoudig opzeggen wanneer je een abonnement niet meer nodig hebt. Ten minste - als je je licentiemanagement op orde hebt...

De meeste software draait in de cloud, geheel of gedeeltelijk, en dat levert weer andere belangrijke keuzes op. Welke software kies je, en waar draai je die? Hoe kies je de juiste cloud en hoe richt je de in?



#### 4. Beveiliging

Er zijn nogal wat gevaren waaraan jouw organisatie bloot kan staan. Criminelen zijn continue op zoek naar manieren om in jouw organisatie binnen te komen. Meestal om gegevens te stelen die ze kunnen verkopen of gebruiken voor andere criminele doeleinden. In het ergste geval installeren ze ransomware, waardoor je losgeld moet betalen om zelf weer toegang te krijgen over je systemen en data.

Vanwege de grote verscheidenheid aan apparatuur – computers, smartphones, intelligente devices – is het aanvalsoppervlak enorm gestegen. Niet langer draait het alleen om het bewaken van het netwerk achter de router met behulp van een firewall. Omdat medewerkers op verschillende plekken werken is het zaak om alle ‘endpoints’ te bewaken, ofwel de apparaten die zich aan de uiteinden van jouw interne en externe netwerk bevinden. Veel criminelen komen bij die endpoints binnen en er hoeft er maar één niet goed beschermd te zijn – omdat de laatste beveiligingsupdate nog niet is toegepast bijvoorbeeld – en je hele netwerk ligt open.



#### 5. Privacy

Data is een kostbaar bedrijfsmiddel. Dat betekent dat datadiefstal verstrekkende gevolgen kan hebben. Maar dat is niet de enige reden om je data goed te beveiligen: je bent ook juridisch verplicht om verantwoord om te gaan met data en de privacy van betrokken klanten, leveranciers, partners en anderen. Neem je die verantwoordelijkheid niet serieus en zijn jouw privacy-gevoelige gegevens onvoldoende beschermd, dan loop je de kans op hoge boetes in geval van een datalek.



#### 6. Back-up en recovery

Gaat er iets mis, dan heb je natuurlijk een plan B nodig. Dat begint bij een goede back-up van je data. Maar een goede recovery strategie is veel meer dan dat en kan ervoor zorgen dat je al binnen enkele minuten weer up & running bent.

Ook een belangrijk aandachtspunt: denk eraan dat je zelf verantwoordelijk bent voor de data van software in de cloud. Gebruik je bijvoorbeeld Microsoft 365, dan ben je niet per definitie voorzien van backups. Microsoft zorgt er wél voor dat de software blijft draaien in de cloud, maar er wordt niet standaard een backup van je mailboxen gemaakt. Daar moet je zelf voor zorgen, wat veel gebruikers niet voldoende doorhebben.

## Voor een kloppend totaalplaatje: een sterke IT-partner, de FSP

Wil je het totaalplaatje in orde hebben? Dan moet je op zoek naar een IT-partner die je compleet kan ontzorgen. Deze rol kan het beste ingevuld worden door een full service provider (FSP). Deze full-service partner helpt je bij het selecteren, aanschaffen (of leasen) van de hardware, en blijf daarna jouw aanspreekpunt voor alles rondom IT-vraagstukken. De FSP zorgt onder meer voor het beheer en de monitoring van je apparatuur en software.



*Een Full Service Provider (FSP) regelt alles voor jouw digitale werkplekken. Managed Services, Software Development, Connectiviteit, Hardware en Adoptie. Alles op één plek, via één partner.*



Belangrijke taak van een FSP is om proactief te zijn. Wordt ergens een mogelijk probleem geconstateerd, dan trekt deze bij je aan de bel met een oplossing. En dankzij geavanceerde beveiligingssoftware kan hij ervoor zorgen dat een gaatje in de beveiliging wordt ontdekt en gedicht voordat criminelen erbij kunnen komen. Deze software kan ook verdacht verkeer van buiten ontdekken en afgrenzen. De FSP signaleert daarnaast kansen om je businessprocessen te verbeteren en denkt met je mee bij het aanschaffen, implementeren en beheren van nieuwe oplossingen daarvoor.

## Keuze in cloud

Een FSP helpt je ook bij de selectie van de cloud. Welke applicaties kunnen beter bij jou op kantoor draaien – on premise – en welke kun je met een gerust hart toevertrouwen aan de cloud?

Ook je data moeten ergens worden opgeslagen, en de meest voor de hand liggende plek is de cloud. Deze opslag is naar verhouding zeer goedkoop en flexibel. Maar je zult niet alles zomaar ergens willen en mogen opslaan. Voor privacygevoelige data zul je eerder kiezen voor een private cloud of on premise opslag. Een FSP kan je helpen de juiste keuzes te maken, zodat je voldoet aan de wettelijke eisen rondom compliance en privacy.

## Business continuity & disaster recovery

Zoals al eerder aangegeven bestaat een goede strategie voor het voorkomen van uitval van je bedrijf uit méér dan alleen het maken van een back-up. Niet alleen zijn er verschillende manieren om een back-up te maken, ook zijn er oplossingen die ervoor kunnen zorgen dat je er bijna zeker van kunt zijn, dat je in geval van rampen geen dataverlies lijdt. Daarbij houd je niet alleen rekening met cyberaanvallen, maar ook met bijvoorbeeld een brand of natuurramp. Met een goede business continuity & disaster recovery (BC&DR) ben je verzekerd van de kortst mogelijke onderbreking van je bedrijfsprocessen.



## Conclusie

Wanneer jouw medewerkers gebruik maken van hybride werkvormen, dan is een digitale werkplek een must. Daar komt vanuit de techniek wel het nodige bij kijken. Een FSP kan je helpen bij alle aspecten van digitalisering van je bedrijf. Het resultaat is dat jij en jouw medewerkers beschikken over de beste digitale werkplek. Waarbij het niet uitmaakt op welke fysieke locatie deze zich bevindt: op kantoor, thuis, onderweg of waar dan ook. De ervaring is steeds dezelfde: veilig en eenvoudig samenwerken, zonder beperkingen.

Hoe staat het met jouw digitale werkomgeving, loopt alles gesmeerd of zijn er verbeterpunten? Zou je graag de garantie hebben dat alles goed geregeld is? Plan dan een adviesgesprek met een van onze consultants.

**Ben je benieuwd naar wat Fivespark voor jou kan betekenen?  
Plan dan vrijblijvend een adviesgesprek in.**

Plan je gesprek >



Managed Services >



Software Development >



Connectiviteit >



Hardware >



Adoptie >

# FIVESPARK

Fivespark (hoofdkantoor)  
Gondel 1  
1186 MJ Amstelveen

088 – 411 00 33  
[info@fivespark.com](mailto:info@fivespark.com)

[fivespark.com](https://fivespark.com)



[linkedin.com/company/fivespark](https://linkedin.com/company/fivespark)

