

HANDBOEK VOOR HET MKB

IT die gewoon werkt.

Wat er in een MKB-omgeving speelt — van Microsoft 365 tot je server, je netwerk en je firewall. Wat je er zelf aan kunt controleren, hoe wij het beheren, en wat het kost.

Je hoeft geen IT'er te zijn om goede beslissingen te nemen.

Dit handboek is geschreven voor directeuren, eigenaren en officemanagers van bedrijven met ongeveer vijf tot honderd medewerkers. Mensen die verantwoordelijk zijn voor IT zonder dat het hun vak is.

Het eerste deel gaat niet over ons. Het legt uit wat er in een gemiddelde MKB-omgeving speelt: waar geld weglekt, welke risico's onzichtbaar blijven zolang alles het doet, en welke vragen je aan iedere IT-partij kunt stellen — ook aan je huidige. Die vragen zijn expres zo gemaakt dat je de antwoorden zelf kunt controleren.

Het tweede deel legt de onderdelen uit waar het in de praktijk over gaat. Niet alleen Microsoft 365: ook de servers op kantoor, je lokale Active Directory, het netwerk en de firewall, de back-up, de werkplekken en de programma's waar het bedrijf op draait. In gewone taal, zonder afkortingen die niets verduidelijken.

Het derde deel beschrijft hoe wij werken. Het vierde deel bevat onze tarieven, twee rekenvoorbeelden en wat er nadrukkelijk niet bij zit.

Kun je dit ook gebruiken zonder klant te worden? Ja. De zelftesten in deel 1 en de overstapchecklist in deel 4 werken bij elke leverancier. Als je ze doorloopt en alles klopt, hoor je dat van ons.

Inhoud

1	Wat "het werkt gewoon" verbergt	3
	De vier dure momenten · Zes stille risico's · Wie kan er bij je omgeving? · Offertes vergelijken	
2	De onderdelen uitgelegd	8
	Microsoft 365 · Licenties · Toegang en identiteit · Servers en lokaal AD · Netwerk en firewall · Back-up · Werkplekken en lijnapplicaties · In- en uitdienst	
3	Hoe wij werken	17
	De vier stappen · Beheer op afstand, onderhoud op locatie · Documentatie en eigenaarschap	
4	Wat het kost	21
	Tarieven · Aanvullende kosten · Rekenvoorbeelden · Overstappen · Veelgestelde vragen	

Over de cijfers in dit document. Bedragen en technische grenzen zijn gecontroleerd in augustus 2026. Microsoft past licentieprijzen en limieten periodiek aan; vraag ons om de actuele stand voordat je ergens op rekent.

01

DEEL EEN

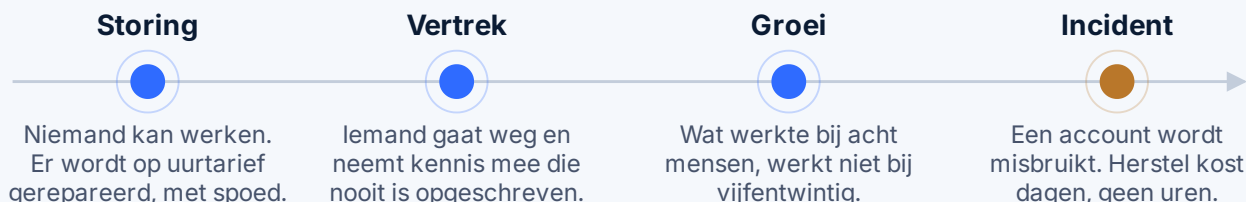
Wat “het werkt gewoon” verbergt

De duurste IT-problemen ontstaan niet tijdens een storing. Ze ontstaan in de jaren dat alles het gewoon doet en niemand kijkt.

-
- 1.1 De vier momenten waarop IT geld kost
 - 1.2 Zes risico's die je niet ziet zolang alles werkt
 - 1.3 Wie kan er eigenlijk bij je omgeving?
 - 1.4 Waarom de goedkoopste offerte vaak de duurste wordt
-

De vier momenten waarop IT geld kost

Bijna niemand betaalt te veel voor beheer. Bedrijven betalen te veel op vier momenten, en die momenten hebben één ding gemeen: ze komen altijd onaangekondigd, en op zo'n moment is er geen tijd om offertes te vergelijken.



Op elk van deze vier momenten is de prijs geen keuze meer.

Waarom spoed altijd duurder is

Een probleem dat je vooraf oplost, plan je in. Een probleem dat je tijdens een storing oplost, koop je onder tijdsdruk, zonder alternatief en meestal buiten kantooruren. Hetzelfde werk, een andere prijs.

Daar komt de stilstand nog bij. Twintig medewerkers die een halve dag niets kunnen, kosten meer dan de reparatie zelf. Dat bedrag staat alleen op geen enkele factuur, dus het valt niemand op.

Reken het één keer uit

Neem het aantal medewerkers dat bij een storing niets kan doen. Vermenigvuldig met het gemiddelde uurloon inclusief werkgeverslasten. Vermenigvuldig met vier uur.

Dat is wat één ochtend uitval je kost, nog voordat er iemand aan het werk is om het te repareren.

Zet dat bedrag naast wat je nu per maand aan beheer uitgeeft. Meestal is dat een verhelderend moment.

Wat deze vier momenten met elkaar gemeen hebben

Ze zijn voorspelbaar

Niet wánnear ze komen, wel dát ze komen. Elk bedrijf krijgt met alle vier te maken. Dat maakt het planbaar.

Ze vragen kennis vooraf

Wie je omgeving pas leert kennen op het moment zelf, is de eerste uren bezig met uitzoeken. Die uren betaal je.

Ze laten sporen na

Een haastige oplossing blijft jaren staan en wordt de oorzaak van het volgende probleem. Zo stapelt achterstand zich op.

De kern. Beheer koop je niet om storingen op te lossen. Je koopt het om te zorgen dat de dure momenten zeldzaam worden, en dat er iemand is die je omgeving al kent wanneer er toch één komt.

Zes risico's die je niet ziet zolang alles werkt

Zes situaties die we aantreffen bij bedrijven waar de IT naar behoren draait. Geen van die bedrijven had een storing — dat is precies waarom niemand keek. Bij elk risico staat de vraag waarmee je het zelf nagaat.

RISICO 1

De postbus die vol raakt

Bij de MKB-abonnementen stopt een postbus op 50 GB. Bij 49 GB volgt een waarschuwing, bij 49,5 GB kan er niets meer verstuurd worden, en bij 50 GB komt inkomende mail niet meer aan. Die meldingen komen bij de medewerker terecht, niet bij jou.

Vraag: hoeveel ruimte is er per postbus in gebruik, en welke limiet hoort bij ons abonnement?

RISICO 2

De toegang die blijft bestaan

Iemand gaat uit dienst. Het account wordt uitgezet, maar de koppeling op de privételefoon, de gedeelde map of het account bij een externe leverancier blijft staan. Vaak jarenlang.

Vraag: mag ik een lijst van alle actieve accounts, naast onze personeelslijst?

RISICO 3

Het domein op andermans naam

Je domeinnaam bepaalt waar je e-mail heen gaat. Staat die op het account van je IT-leverancier in plaats van op je bedrijf, dan kun je niet zelfstandig weg — en bij een conflict ook niet snel.

Vraag: op wiens naam staat ons domein, en mag ik die inloggegevens?

RISICO 4

De back-up die nooit is getest

Een back-up die elke nacht groen meldt, bewijst dat er iets is weggeschreven. Niet dat het terug te zetten is. Het verschil merk je pas op de dag dat je het nodig hebt.

Vraag: wanneer is er voor het laatst echt iets teruggezet, en wat kwam eruit?

RISICO 5

De firewall die geen updates meer krijgt

Hij doet het nog prima, maar krijgt geen updates meer, terwijl de zwakke plekken erin wél openbaar worden. Zo'n apparaat staat aan de buitenkant van je netwerk en is van buitenaf te vinden.

Vraag: welk model hangt er, en tot wanneer krijgt het nog updates?

RISICO 6

De ene server waar alles op leunt

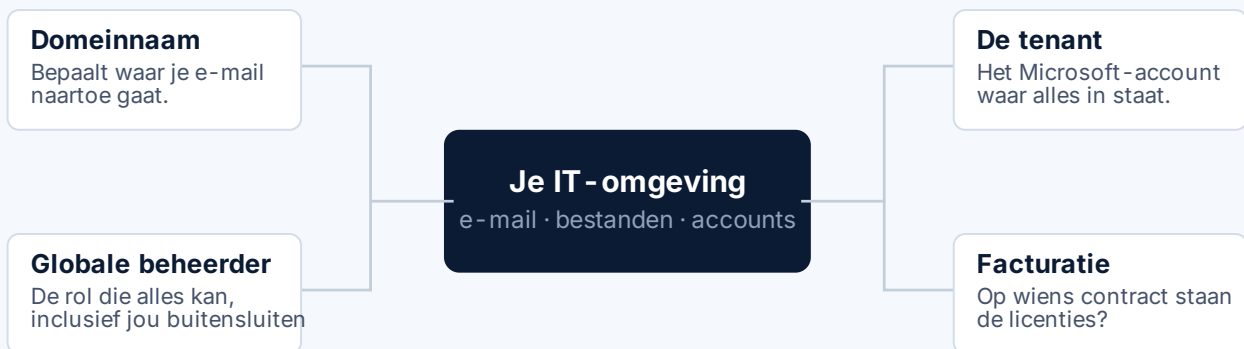
Eén machine waarop iedereen inlogt, waar de bestanden staan en waar het ERP op draait. Valt hij uit, dan ligt niet één ding stil maar alles tegelijk — en dan telt hoe oud hij is en of er nog garantie op zit.

Vraag: hoe oud is de server, en wat ligt er stil als hij uitvalt?

Alle zes de vragen hebben één ding gemeen. Het antwoord is kort en controleerbaar. Een leverancier die zijn zaken op orde heeft, beantwoordt ze binnen een dag. Duurt het langer, of komt er een uitleg in plaats van een antwoord, dan weet je genoeg — nog voordat je iets besluit.

Wie kan er eigenlijk bij je omgeving?

Uitbesteden is verstandig. Kwijtraken is iets anders. Het verschil zit in vier sleutels. Wie die vasthoudt, bepaalt of je vrij bent om te kiezen — nu, en op de dag dat je wilt wisselen.



Alle vier horen op naam van je bedrijf te staan. Beheer mag je uitbesteden.

Waarom dit geen theorie is

Zolang de samenwerking goed loopt, merk je hier niets van. Het wordt pas zichtbaar op het moment dat je iets wilt veranderen: een tweede partij ernaast, een migratie, of gewoon opzeggen.

Staat er geen enkele beheerdersrol op naam van je eigen mensen, dan ben je voor elke stap afhankelijk van de medewerking van een partij die er belang bij heeft dat je blijft. Dat is geen kwade opzet. Het is een positie waar je simpelweg niet in hoort te zitten.

Vraag het schriftelijk

"Kunnen jullie bevestigen dat het domein, de Microsoft-tenant en de licentie-overeenkomst op naam van ons bedrijf staan, en dat wij een beheerdersaccount op eigen naam hebben?"

Eén e-mail. Bewaar het antwoord. Dit is het goedkoopste stuk risicobeheersing dat je dit jaar doet.

Vier sleutels, vier controles

SLEUTEL	WAT JE VRAAGT	WAT EEN GOED ANTWOORD IS
Domeinnaam	Bij welke partij staat ons domein geregistreerd, en op wiens naam?	Op naam van je bedrijf, met eigen inlog
Tenant	Staat onze Microsoft-omgeving op ons eigen bedrijf?	Ja, met je bedrijfsnaam als eigenaar
Globale beheerder	Welke accounts hebben deze rol, en zit daar iemand van ons bij?	Een korte lijst, met minstens één eigen account
Facturatie	Op welk contract staan de licenties en wat is de looptijd?	Inzichtelijk, en overdraagbaar

Waarom de goedkoopste offerte vaak de duurste wordt

Twee offertes vergelijken op het maandbedrag werkt niet, omdat het maandbedrag niet zegt wat je ervoor krijgt. Het verschil zit bijna altijd in wat er buiten valt en later als meerwerk terugkomt.

ONDERDEEL	DE VRAAG DIE JE STELT
Nieuwe medewerker	Account, laptop en toegang klaar op dag één — inbegrepen of per keer gefactureerd?
Vertrekkende medewerker	Wie zet het account uit, wie haalt de data eruit, en wat kost dat?
Ondersteuning per gebruiker	Onbeperkt, of een bundel uren die opraakt? En wat gebeurt er als de bundel op is?
Updates en patches	Actief uitgerold en gecontroleerd, of “staat automatisch aan”?
Monitoring	Kijkt er iemand naar de meldingen, of komen ze alleen in een postbus binnen?
Back-up van Microsoft 365	Zit die erin? Microsoft levert die namelijk niet standaard mee. Zie pagina 14.
Terugzetest	Wordt er periodiek daadwerkelijk iets teruggezet, en krijg je daar een verslag van?
Werk op locatie	Hoeveel per uur, en worden reistijd en voorrijkosten apart gerekend?
Documentatie	Krijg je die, of blijft die bij de leverancier?
Opzegtermijn	Per maand, per jaar, of stilzwijgende verlenging?

Het patroon. Een laag maandbedrag met veel meerwerk voelt goedkoop bij ondertekening en duur in gebruik. Bovendien werkt het verkeerd: elke keer dat je belt, kost het geld, dus bel je minder. Dan gaan er dingen langer mis dan nodig.

Een vast bedrag met alles erin dwingt de leverancier juist om problemen te voorkomen. Hij verdient aan een omgeving die rustig draait.

Wat je ook moet vergelijken

Vraag naar het aantal medewerkers bij de leverancier zelf, en wie je omgeving kent als degene die je normaal spreekt er niet is.

Vraag hoe lang de langstlopende klant er zit. Dat cijfer zegt meer over kwaliteit dan welke certificering ook.

En vraag naar één ding dat vorig jaar is misgegaan en wat daarna is veranderd. Op dat antwoord kun je iemand beoordelen.

02

DEEL TWEE

De onderdelen uitgelegd

Van je Microsoft 365-omgeving tot de server, het netwerk en de programma's waar het bedrijf op draait. Je hoeft dit niet te kunnen bouwen — je moet het kunnen beoordelen.

- [2.1](#) Microsoft 365: wat het is en wat je ervan gebruikt
- [2.2](#) Licenties, postbussen en de grens van 50 GB
- [2.3](#) Toegang en identiteit: hoe het misgaat
- [2.4](#) Servers en lokaal Active Directory
- [2.5](#) Netwerk, firewall en internet
- [2.6](#) Back-up en herstel
- [2.7](#) Werkplekken en lijnapplicaties
- [2.8](#) In- en uitdienst

Microsoft 365: wat het is en wat je ervan gebruikt

De meeste bedrijven kennen Microsoft 365 als “Outlook en Teams”. Het is in werkelijkheid een afgesloten ruimte die alleen van jou is — een **tenant** — waarin vier dingen bij elkaar staan. Wie dat eenmaal zo ziet, begrijpt meteen waarom eigenaarschap van die tenant zo bepalend is.

Je tenant — alleen van jou



Identiteiten

Wie is wie, en wie mag waarbij. Elk account is een sleutel.



E-mail

Postbussen, agenda's, gedeelde adressen zoals info@ en facturen@.



Bestanden

Gedeelde mappen van het bedrijf en de opslag per medewerker.



Overleg

Chat, vergaderingen en de kanalen per team of project.

Daaroverheen: de regels

Wie mag inloggen, vanaf welk apparaat, en onder welke voorwaarden. Dit is het deel dat bijna nooit is ingericht.

Alles binnen de stippellijn is je eigendom. De partij die het beheert, staat erbuiten.

Waarom “het staat toch in de cloud” niet genoeg is

Microsoft zorgt dat het platform blijft draaien en dat de servers niet uitvallen. Wat er binnen je tenant gebeurt — wie toegang heeft, welke regels gelden, of iemand per ongeluk een map leeggooit — is je verantwoordelijkheid. Die verdeling heet gedeelde verantwoordelijkheid, en het misverstand daarover is de bron van de meeste vervelende verrassingen.

Wat je hieruit hoort mee te nemen

Vraag niet “hebben we Microsoft 365?” maar “wat staat er in onze tenant en wie beheert dat?”. Op die vraag hoort een leverancier een overzicht te kunnen sturen: hoeveel accounts, welke licenties, welke gedeelde postbussen, en welke regels er actief zijn.

Vier dingen die in bijna elke tenant scheef staan

Niet omdat er slecht werk is geleverd, maar omdat een omgeving meegroeit met het bedrijf en er zelden iemand terugkiert.

Licenties die niemand gebruikt. Accounts van vertrokken medewerkers waarvan de licentie doorloopt. De post die het snelst geld oplevert.

Volledige licenties op gedeelde adressen. info@ of facturen@ hebben geen betaalde licentie nodig. Zie pagina 10.

Te veel beheerders. De rol van globale beheerder is ooit uitgedeeld en nooit ingetrokken. Elke extra beheerder is een sleutel die kwijt kan raken.

Toegang die te ruim is. Iedereen bij alles, omdat dat ooit het makkelijkst was. Lastig uit te leggen als een opdrachtgever ernaar vraagt.

Licenties, postbussen en de grens van 50 GB

Voor het MKB doen drie licenties er werkelijk toe. Het verschil bepaalt of je apparaten te beheren zijn en of je regels kunt stellen aan inloggen.

	BUSINESS BASIC	BUSINESS STANDARD	BUSINESS PREMIUM
E-mail, agenda, Teams	Ja	Ja	Ja
Postbusgrootte	50 GB	50 GB	50 GB
Office op de computer	Alleen in de browser	Geïnstalleerd	Geïnstalleerd
Apparaatbeheer (Intune)	Nee	Nee	Ja
Voorwaardelijke toegang	Nee	Nee	Ja
Uitgebreide beveiliging	Basis	Basis	Ja

Stand augustus 2026. De actuele licentieprijs per gebruiker geven wij op aanvraag; Microsoft past die periodiek aan.

De veelgemaakte fout. Standard nemen en er los apparaatbeheer bij kopen komt vrijwel op hetzelfde bedrag uit als Premium — zonder de rest die daarin zit. Wie apparaten wil beheren of wil bepalen vanaf waar er ingelogd mag worden, kijkt naar Premium.

De grens van 50 gigabyte

Elke postbus stopt bij 50 GB. Dat lijkt veel, tot er tien jaar aan bijlagen in zit. Twee nette oplossingen, en één die je moet vermijden.

Gedeelde postbus

Adressen als info@ of facturen@ hebben géén betaalde licentie nodig zolang ze onder de 50 GB blijven. Wie daarvoor per adres een volledige licentie betaalt, betaalt te veel. Meer ruimte, een groot archief of een bewaarplicht? Dan is er alsnog een licentie nodig.

Archiefpostbus

Oude jaargangen verhuizen naar een archief naast de postbus. De mail blijft doorzoekbaar en je gooit niets weg. Let op: bij Basic en Standard is dat archief zelf ook 50 GB. Alleen bij Premium groeit het mee.

Niet doen

Mail lokaal wegschrijven in losse bestanden. Die vallen buiten elke back-up en elke zoekopdracht, en verdwijnen met de laptop.

Actiepunt. Vraag één keer per jaar een overzicht op van alle postbussen met hun gebruikte ruimte. Alles boven 75 procent krijgt een plan. Dat kost tien minuten en voorkomt de dag waarop je mail zonder aankondiging stopt.

Toegang en identiteit: hoe het misgaat

Inbraak bij een bedrijf van deze omvang begint meestal niet met een gat in de software, maar met een account. Iemand logt in met een geldig wachtwoord, en vanaf dat moment ziet alles er normaal uit — ook voor jou.



Stap 3 is het punt waarop het onzichtbaar wordt. Daarna helpt oplettendheid niet meer.

Drie maatregelen, elk op een ander punt in de keten. Eén ervan is niet genoeg; samen sluiten ze de route af.

Wat de drie maatregelen doen

Tweestapsverificatie vraagt naast het wachtwoord om een bevestiging op de telefoon. Een gestolen wachtwoord alleen is dan niets waard.

Voorwaardelijke toegang stelt eisen aan de omstandigheden: alleen vanaf bekende apparaten, of niet vanuit landen waar je geen zaken doet.

Monitoring zorgt dat iemand het merkt als er tóch iets vreemds gebeurt, zoals een nieuwe regel die post wegmoffelt.

Twee vragen, vandaag te stellen

"Staat tweestapsverificatie aan voor *alle* accounts, ook voor de directie en de beheerders?"

"Krijgt iemand een melding als er in een postbus een doorstuurregel wordt aangemaakt?" Op de tweede vraag is het antwoord in het MKB bijna altijd nee.

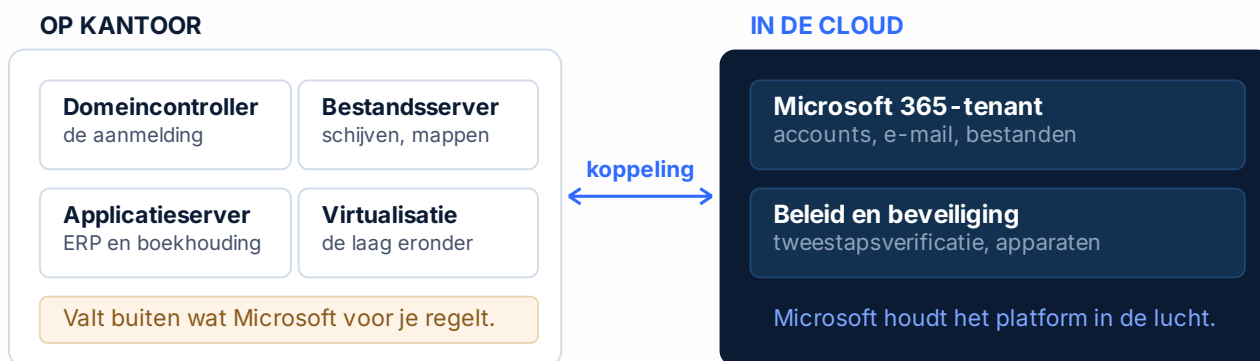
Waarom een wachtwoordbeleid alleen niet werkt

Langere wachtwoorden en verplicht wisselen helpen nauwelijks tegen deze route. De aanvaller heeft het wachtwoord immers niet geraden — het is vrijwillig ingetypt op een pagina die er precies zo uitzag als de echte. Tegen een overtuigende nepmail is niemand bestand, ook je beste mensen niet.

Wat wél werkt, is zorgen dat één wachtwoord niet genoeg is om binnen te komen, en dat er iemand meekijkt op wat er ná het inloggen gebeurt. Dat is geen kwestie van scholing maar van instellingen — en die staan in de meeste omgevingen nog uit.

Servers en lokaal Active Directory

Niet alles staat in de cloud, en dat hoeft ook niet. Bij veel bedrijven draait er nog een server op kantoor: een bestandsserver, een database achter het ERP-pakket, of een domeincontroller die bepaalt wie er op het netwerk mag. Die machines vallen buiten alles wat Microsoft voor je regelt. Wat daar gebeurt, gebeurt omdat iemand het doet.



Werken beide kanten met dezelfde gebruikersnamen? Dan is de vraag of daar een koppeling tussen zit — of dat iemand ze twee keer bijhoudt.

Wat er aan een server te doen valt

Updates die niet vanzelf gaan en een herstart nodig hebben. Schijfruimte die volloopt. Een back-up van de hele machine en niet alleen van de mappen. Een RAID-set waarvan één schijf stilletjes is uitgevallen. En een garantietermijn die een keer afloopt.

Geen van deze dingen meldt zich uit zichzelf bij jou. Ze melden zich bij iemand die kijkt, of helemaal niet.

De vraag die je stelt

“Hoe oud is onze server, tot wanneer loopt de garantie, en wanneer is er voor het laatst een herstart geweest na updates?”

Drie feiten die iedereen die je omgeving beheert binnen een minuut moet kunnen opzoeken. Duurt dat langer, dan is dat een reden om door te vragen.

Wanneer een eigen server nog zin heeft

Wel

Een programma dat alleen lokaal draait, grote bestanden waar de hele dag in gewerkt wordt, of apparatuur die niet met de cloud praat.

Twijfelgeval

Een bestandsserver die alleen nog documenten bevat. Die kan meestal naar de cloud, maar niet zomaar: mappen en rechten moeten mee.

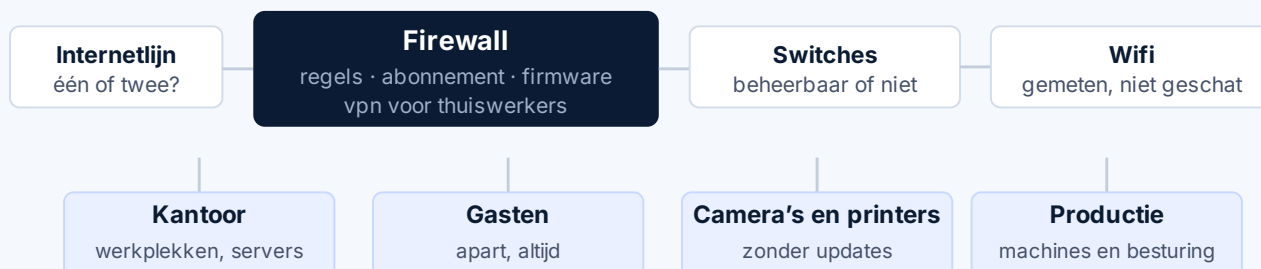
Niet

Een server die alleen nog aanstaat omdat er ooit iets op is gezet dat niemand durft uit te zetten. Die kost alleen nog aandacht.

Het klassieke risico: één domeincontroller. Draait de aanmelding van je hele bedrijf op één machine, dan is dat de machine die niemand mag missen. Valt hij uit, dan kan iedereen meestal nog wel op zijn eigen pc inloggen — Windows onthoudt de laatste aanmeldingen. Maar bij de bestanden op de server komt niemand meer, wachtwoorden wijzigen kan niet, en een nieuwe pc krijg je niet aan de praat. Een tweede domeincontroller is meestal een tweede virtuele machine en neemt dat risico weg. Wij kijken daar bij de scan standaard naar, en zeggen het ook als het bij jou niet nodig is.

Netwerk, firewall en internet

Dit is het onderdeel dat het langst blijft liggen, want het doet het. Netwerkkapparatuur veroudert zonder het te melden: er gaat niets kapot, er stopt alleen op enig moment iemand bij de fabrikant met het maken van updates. Een firewall die vijf jaar geleden is neergezet, doet vandaag nog precies wat hem toen is verteld.



Gescheiden groepen op één netwerk. Zonder die scheiding staat de camera van de parkeerplaats bij de administratie.

Waarom een firewall zonder ondersteuning een risico op zich is

Bij een apparaat waar de fabrikant mee gestopt is komen er geen updates meer, terwijl de zwakke plekken die erin zitten wél openbaar worden gemaakt. Het verraderlijke is de schijnzekerheid: er hängt een firewall, dus niemand kijkt ernaar. En het is een route waar tweestapsverificatie niets tegen doet, omdat er geen inlog aan te pas komt. Daarom kijken we hier bij elke scan naar.

Vier dingen die je zelf kunt navragen

- Welk merk en model staat er, en tot wanneer krijgt dat nog updates?
- Zit er een lopend beveiligingsabonnement op, en tot welke datum?
- Zitten gasten, camera's en printers op een eigen deel van het netwerk?
- Wie kan er van buitenaf naar binnen, en hoe is dat beveiligd?

Drie dingen die hierbij horen

Toegang van buitenaf

Thuiswerken loopt via een vpn of via een dienst die van buitenaf bereikbaar is. In beide gevallen hoort daar tweestapsverificatie op te zitten. Een vpn met alleen een wachtwoord is een open deur.

De internetlijn zelf

Ligt die eruit, dan valt bij een cloudomgeving het meeste werk stil. Een tweede lijn van een andere aanbieder, of een 4G- of 5G-back-up in de firewall, kost een vast bedrag per maand. Reken één keer uit wat een dag zonder internet je kost — dan weet je of dat bedrag laag is.

Wachtwoorden van apparatuur

Firewall, switches en accesspoints hebben elk een eigen beheerderswachtwoord. Die horen vastgelegd te zijn waar jij ook bij kunt — niet alleen bij degene die het ooit installeerde.

Back-up en herstel

Een back-up gaat over twee werelden. Je servers en bestandsschijven op kantoor, waar je zelf alles voor moet regelen. En Microsoft 365, waarvan de meeste mensen denken dat het geregeld is. Dat laatste klopt niet: Microsoft zorgt dat hún systemen niet omvallen, maar het langdurig bewaren van jÓuw gegevens zit niet in je abonnement. Wat je standaard krijgt zijn korte hersteltermijnen — bedoeld voor “oeps”, niet voor “dat blijkt vorig jaar al te zijn misgegaan”.



Aparte back-up die je zelf regelt — bewaartermijn bepaal je

Alles boven de zwarte balk is wat je standaard hebt. Schematisch, niet op schaal.

En de server dan?

Daar geldt geen enkele automatische termijn. Wat er van je bestandsserver, je database en je virtuele machines wordt bewaard, is precies wat iemand ooit heeft ingericht — en hoe lang, is een keuze die iemand ooit heeft gemaakt.

De gevallen waarin je een back-up echt nodig hebt, ontdek je bovendien meestal laat: een map die in maart is leeggehaald en in juni gemist wordt, of versleutelde bestanden die zich eerst weken stil hebben verspreid. Op al die momenten zijn veertien, dertig of drieënnegentig dagen precies te kort.

Microsoft biedt inmiddels wél een eigen betaalde back-updienst aan. Die bewaart je gegevens binnen dezelfde omgeving als het origineel, dekt geen servers of werkplekken, en gaat niet verder terug dan twee jaar. Daarmee voldoet hij aan geen van de eerste drie eisen hiernaast.

Waar een goede back-up aan voldoet

- Los van de omgeving die hij beschermt, met een eigen inlog
- Dekt servers en werkplekken én e-mail, bestanden en Teams
- Eén kopie buiten het pand, die niet vanaf het netwerk te wissen is
- Een bewaartermijn die je kiest, niet die je krijgt
- Periodiek getest door daadwerkelijk iets terug te zetten

De enige test die telt. Vraag je leverancier om één willekeurige map van de server en één postbus terug te zetten naar een tijdelijke locatie, en te laten zien wat eruit komt. Dat is de dag waarop je weet of je back-up werkt. In onze Compleet-dienst gebeurt dat twee keer per jaar standaard, met een verslag.

Werkplekken en lijnapplicaties

Twee onderwerpen met dezelfde oorzaak: er is nooit een standaard afgesproken, dus is elk apparaat een apart geval geworden en heeft elk programma zijn eigen verhaal. Dat valt niemand op zolang de mensen die het weten er nog werken.

De levensloop van een werkplek

Een laptop is geen aankoop maar een cyclus. Wie die cyclus niet beheert, betaalt dat later in verloren uren.



Eén afgesproken model per rol, één standaardinrichting en een vervangingsmoment dat je van tevoren ziet aankomen. Dan is een kapotte laptop een ongemak van een uur en geen dag.

De programma's waar het bedrijf op draait

Het ERP -pakket, het WMS, de boekhouding, het douaneportaal, de planningssoftware. Vaak van een andere leverancier dan de IT -partij, en vaak het onderdeel waar de meeste tijd in verdwijnt als er iets niet werkt.

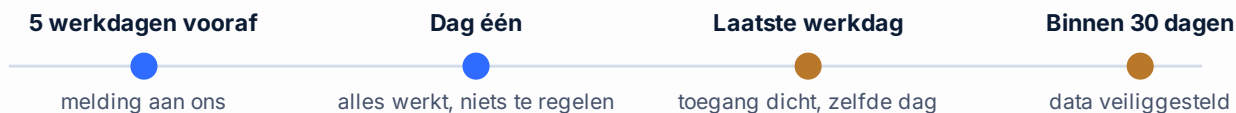
Wat wij per programma vastleggen

- Wie de leverancier is en wie daar het aanspreekpunt is
- Waar het draait: bij de leverancier, op jouw server, of allebei
- Welke koppelingen eraan hangen en wat er stilvalt als er één breekt
- Welke versie er staat en tot wanneer die ondersteund wordt
- Wie er toegang heeft en wie dat mag uitdelen

Waarom dit ertoe doet. Bij een storing in zo'n programma gaat de eerste dag op aan uitzoeken wie erover gaat. Ligt dat vooraf vast, dan bellen wij meteen de juiste partij — en houden we de regie in plaats van jou tussen twee leveranciers te laten staan.

In- en uitdienst

Twee routines die in de meeste bedrijven per e-mail en uit het hoofd gaan. Ze bepalen twee dingen: hoe een nieuwe collega zijn eerste dag ervaart, en hoeveel toegang er blijft bestaan nadat iemand weg is.



Nieuwe medewerker

Meld het minimaal vijf werkdagen van tevoren. Dan staat dit klaar voordat de nieuwe collega binnenloopt:

- ☐ Account, e-mailadres en wachtwoord
- ☐ Tweestapsverificatie ingesteld op de eigen telefoon
- ☐ Toegang tot precies de mappen die bij de functie horen
- ☐ Laptop geïnstalleerd volgens de standaard
- ☐ Printer, wifi en de programma's die bij de functie horen
- ☐ Handtekening in de e-mail conform de huisstijl

Bij ons is dit inbegrepen in het maandbedrag. Het is geen los verzoek en geen meerwerk.

Vertrekkende medewerker

Dit is het lijstje waar in de praktijk de helft van blijft liggen:

- ☐ Aanmelden uitgezet, actieve sessies beëindigd
- ☐ Wachtwoord gewijzigd, tweede factor losgekoppeld
- ☐ Postbus omgezet naar gedeeld of doorgestuurd naar een collega
- ☐ Persoonlijke bestanden overgedragen aan de leidinggevende
- ☐ Accounts bij externe partijen op die naam beëindigd
- ☐ Bedrijfsgegevens van de privételefoon verwijderd
- ☐ Laptop ingeleverd, schoongemaakt en klaar voor hergebruik

De regel die het meeste voorkomt. Toegang gaat dicht op de laatste werkdag, niet op de dag dat iemand eraan denkt. Bij een vertrek met een vervelende bijmaak: op het moment van het gesprek. Wij hebben dat liever van tevoren met jou afgestemd dan achteraf.

03

DEEL DRIE

Hoe wij werken

Wij beginnen nooit met een offerte. Eerst kijken we wat er staat. Pas daarna weet je wat je koopt en weten wij wat we beloven.

-
- 3.1 Van eerste gesprek naar draaiende omgeving
 - 3.2 Beheer op afstand, onderhoud op locatie
 - 3.3 Documentatie, eigenaarschap en wat je van ons mag verwachten
-

Van eerste gesprek naar draaiende omgeving

Vier stappen. De eerste kost je niets en verplicht je tot niets, en levert ook zonder vervolg iets op: je weet daarna wat je hebt staan.

Week 1

IT - scan

Werkplekken, servers, Microsoft 365, netwerk en back-ups in kaart.

Kosteloos.

Week 2

Voorstel

Wat we aantreffen, wat we adviseren, wat het kost en wanneer het klaar is. Vaste prijs.

Week 3-4

Onboarding

Overname, documentatie en de beveiligingsbasis. Je mensen merken er weinig van.

Daarna

Beheer

Dagelijkse support en monitoring, onderhoud op locatie en een vast overleg per kwartaal.

Wat de IT-scan oplevert

Een overzicht van wat er staat: hoeveel werkplekken en van welke leeftijd, welke licenties er lopen en of ze passen bij wat je gebruikt, hoe je postbussen ervoor staan, hoe de back-up geregeld is, en wat er aan beveiliging aan staat.

Daar hangen we een prioriteit aan: wat moet nu, wat kan bij de eerstvolgende vervanging, en wat kan gewoon blijven zoals het is. Dat laatste lijstje is bijna altijd langer dan mensen verwachten.

Wat de onboarding inhoudt

Wij nemen het beheer over zonder dat je mensen op een ochtend zonder mail zitten. Alles wordt vastgelegd: welke apparatuur er hangt, welke accounts er zijn, waar de licenties lopen, wie waarvoor toestemming heeft.

Tegelijk zetten we de beveiligingsbasis neer: tweestapsverificatie voor iedereen, beheerdersrollen op orde, en zicht op wat er gebeurt. Dat is geen project, dat is de startlijn. Het doorlopend beheren en controleren daarvan zit in dienst Compleet.

Geen scan, geen offerte. Wij geven geen maandbedrag af op basis van een telefoongesprek. Wie dat wel doet, houdt ergens rekening met tegenvallers — en dat betaal je, of het wordt later meerwerk.

Beheer op afstand, onderhoud op locatie

Verreweg het meeste IT-werk gebeurt op afstand — bij ons en bij elke andere partij, ook bij de leverancier die drie straten verderop zit. Voor een wachtwoord of een postbus rijdt niemand een busje. Wij zijn daar alleen expliciet over, en hebben het werk dat wél handen vraagt netjes ingepland in plaats van het af te wachten.

Op afstand — dagelijks

- Iemand kan niet inloggen
- Mail komt niet aan of gaat verkeerd
- Nieuwe collega inrichten, vertrekkers afsluiten
- Updates, monitoring en meldingen
- Telefoon kwijt: op afstand wissen

Op locatie — periodiek

- Netwerkkapitaal plaatsen
- Werkplekken uitrollen en innemen
- Wifi meten waar mensen zitten
- Serverwerk en verhuizingen
- Gezichten zien en vragen ophalen

Hoe dat in de praktijk loopt

Wij werken vanuit Istanbul voor Nederlandse bedrijven en zijn elke maand in Nederland. Elke klant heeft daarin eens per twee maanden een vaste onderhoudsdag staan. Wat handen vereist, verzamelen we voor die dag — tenzij het niet kan wachten, dan komen we eerder.

De Turkse tijd loopt een tot twee uur voor op de Nederlandse, afhankelijk van het seizoen. Als je om negen uur begint, zijn wij al bezig. Dat merk je vooral 's ochtends vroeg.

Wat afstand van ons eist

Wij kunnen niet even langsrijden om iets recht te breien. Dus moet het vooraf kloppen: alles gedocumenteerd, alles op afstand te beheren, en geen enkel apparaat waar maar één iemand de weg in weet.

Dat is strenger dan de meeste partijen voor zichzelf organiseren. Jij profiteert daarvan op de dag dat iemand bij ons ziek is — want dan kan de volgende het overnemen.

Wanneer wij géén goede keuze zijn. Heb je werk waarbij er dagelijks iemand fysiek aanwezig moet zijn — een productieomgeving met machines aan het netwerk, of een balie waar constant hardware stukgaat — dan ben je beter af met een partij om de hoek. Dat zeggen we liever in het eerste gesprek dan in het tweede jaar.

Documentatie, eigenaarschap en wat je van ons mag verwachten

In deel 1 stond de vraag wie er bij je omgeving kan. Het zou raar zijn om die vraag te stellen en er zelf een ontwijkend antwoord op te geven. Dus staat het hier zwart op wit.

Wat van jou is en van jou blijft

- Je domeinnaam staat op naam van je bedrijf
- Je Microsoft-tenant staat op naam van je bedrijf
- Je hebt zelf een beheerdersaccount, ook als je het nooit gebruikt
- De documentatie van je omgeving is van jou, niet van ons
- Opzegbaar per maand, zonder stilzijgende verlenging

En als je ooit weggaat

Dan dragen we over. Volledige documentatie, toegang tot alles, en een gesprek met de opvolgende partij zodat die weet wat hij aantreft. Zonder rekening voor "uitfaseringswerkzaamheden".

Niet omdat we dat leuk vinden, maar omdat een klant die alleen blijft omdat weggaan te ingewikkeld is, geen klant is. Wij willen dat je blijft omdat het bevalt.

Het ritme van de samenwerking

WANNEER	WAT ER GEBEURT
Dagelijks	Ondersteuning tijdens kantooruren, monitoring van werkplekken en servers, opvolging van meldingen
Doorlopend	Gecontroleerde updates van Windows en software, beheer van accounts, postbussen en licenties
Elke twee maanden	Vaste onderhoudsdag op je locatie
Per kwartaal	Overleg: wat is er gebeurd, wat staat er aan te komen, wat adviseren wij en wat kost dat
Twee keer per jaar	Terugzetest van de back-up met verslag, en een beveiligingsrapportage (dienst Compleet)

Wat wij niet beloven. Geen reactietijd van vijf minuten, want die halen wij niet altijd en dan is het een leugen op papier. Geen 24 uur per dag bereikbaarheid in het standaardtarief; dat is een aparte afspraak met een aparte prijs, zodat je er niet voor betaalt als je het niet nodig hebt. En geen enkele belofte dat er nooit iets misgaat. Wel dat je weet wie er dan aan de telefoon komt, en dat diegene je omgeving kent.

04

DEEL VIER

Wat het kost

Onze tarieven staan op onze website en staan hier. Niet omdat het moet, maar omdat je anders drie gesprekken nodig hebt voordat je weet of wij bij je budget passen.

-
- 4.1 De twee diensten
 - 4.2 Aanvullende kosten en wat er niet in zit
 - 4.3 Twee rekenvoorbeelden
 - 4.4 Overstappen van je huidige leverancier
 - 4.5 Veelgestelde vragen
-

De twee diensten

Eén vast bedrag per medewerker per maand. Geen bundel uren die opraakt, geen factuur per telefoontje. Alle bedragen zijn exclusief btw en exclusief Microsoft-licenties.

DIENST

Basis

€ 40 per medewerker
per maand

- Beheer van alle werkplekken: installatie, instellingen en storingsen
- Microsoft 365 - beheer: accounts, postbussen, groepen en licenties
- Onbeperkt support op afstand tijdens kantooruren
- Windows - en software - updates gecontroleerd uitgerold
- Monitoring van werkplekken en servers
- Nieuwe medewerker: laptop, account en toegang klaar op dag één

DIENST

MEEST GEKOZEN

Compleet

€ 65 per medewerker
per maand

Alles uit Basis, plus:

- Tweestapsverificatie doorlopend beheerd en gecontroleerd
- Apparaatbeheer: beleid, versleuteling en op afstand wissen
- Voorwaardelijke toegang: alleen bekende apparaten en locaties
- Back-up van Microsoft 365: mail, bestanden en teams
- Twee keer per jaar een echte hersteltest, met verslag
- Halfjaarlijkse rapportage over beveiliging en open risico's

In beide diensten inbegrepen

Onbeperkt support

Geen bundel uren en geen factuur per telefoontje. Bellen kost je niets, dus bel je op tijd.

Vaste onderhoudsdag

Elke twee maanden zijn we bij jou op locatie. Die dag zit in het maandbedrag.

Maandelijks opzegbaar

Geen jaarcontract, geen stilzwijgende verlenging, en een nette overdracht als je gaat.

Welke van de twee past bij jou? Basis is genoeg als je vooral wilt dat werkplekken en e-mail netjes draaien en er iemand opneemt als er iets is.

Compleet is de keuze zodra je met gevoelige gegevens werkt, mensen op eigen apparaten of buiten kantoor werken, of je een verzekeraar of opdrachtgever hebt die vragen stelt over beveiliging. In dat laatste geval is Compleet meestal geen luxe maar een voorwaarde.

Aanvullende kosten en wat er niet in zit

Dit zijn de posten die naast het bedrag per medewerker voorkomen. Wat hier niet staat, factureren wij niet zonder dat je er vooraf een prijs voor hebt gezien.

POST	WANNEER VAN TOEPASSING	TARIEF
Server	Per server, fysiek of virtueel	€ 95 per maand
Extra vestiging	De eerste zit erbij, elke volgende telt mee	€ 75 per maand
Basisfee kleine bedrijven	Onder tien medewerkers; daarboven vervalt hij	€ 75 per maand
Uitgebreide beschikbaarheid	Support van 07:00 tot 19:00 in plaats van kantooruren	+ 15%
Werk op locatie	Op afspraak, buiten de vaste onderhoudsdag	€ 80 per uur
Bereikbaarheid buiten die uren	Avond, weekend of 24/7 — een aparte afspraak	op aanvraag
Eenmalige inrichting	Overname, documentatie en beveiligingsbasis	vanaf € 750

Alle bedragen exclusief btw. Tarieven zoals gepubliceerd op itspine.nl, augustus 2026.

Wat er nadrukkelijk niet bij zit

- **Microsoft-licenties.** Die betaal je aan Microsoft of via ons door, tegen kostprijs plus een opslag die wij vooraf noemen. Wij verdienen niet stiekem aan je licenties.
- **Hardware.** Laptops, servers en netwerkapparatuur. Wij adviseren, jij koopt — desgewenst via ons.
- **Projecten.** Migraties, verhuizingen en vernieuwingen krijgen een eigen voorstel met een vaste prijs. Nooit “we zien wel waar het uitkomt”.
- **Reiskosten bij bezoek op afspraak.** Vooraf begroot, nooit achteraf verrast. De vaste onderhoudsdag valt hier buiten; die zit in het maandbedrag.

Waarom wij dit zo opschrijven. Een leverancier verdient op twee manieren: aan een vast bedrag voor een omgeving die rustig draait, of aan losse facturen voor alles wat er misgaat. Alleen de eerste manier geeft ons hetzelfde belang als jij. Daarom staat support onbeperkt in het maandbedrag en is de lijst hierboven kort en openbaar.

Twée rekenvoorbeelden

Zodat je kunt zien hoe het bedrag opgebouwd wordt, en zelf kunt narekenen wat het bij jou zou worden.

VOORBEELD A

Adviesbureau, 8 medewerkers

Geen server, één vestiging, iedereen werkt met Microsoft 365 en gevoelige klantgegevens. Dienst Compleet.

8 medewerkers × € 65	€ 520
Basisfee onder tien medewerkers	€ 75
Servers	—
Extra vestigingen	—
Per maand	€ 595

Daarnaast eenmalig de inrichting, vanaf € 750. Het maandbedrag komt neer op ongeveer € 74 per medewerker — inclusief onbeperkte ondersteuning, beveiliging en back-up.

VOORBEELD B

Handelsbedrijf, 24 medewerkers

Eén server, een tweede vestiging met een klein magazijn. Dienst Compleet.

24 medewerkers × € 65	€ 1.560
Basisfee	—
1 server	€ 95
1 extra vestiging	€ 75
Per maand	€ 1.730

In dienst Basis zou dezelfde omgeving op € 1.130 per maand uitkomen. Het verschil van € 600 zit volledig in beveiliging, apparaatbeheer en back-up.

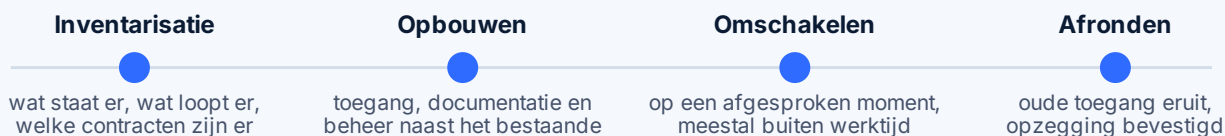
Zet het naast je huidige situatie. Tel bij elkaar op: je huidige maandbedrag, plus alle losse facturen van het afgelopen jaar gedeeld door twaalf, plus wat je apart betaalt voor back-up en beveiliging. Pas dan vergelijk je hetzelfde met hetzelfde. Bij veel bedrijven blijkt het losse deel groter dan het vaste deel.

Zelf narekenen

Aantal medewerkers × € 40 of € 65 + € 95 per server + € 75 per extra vestiging + € 75 als je onder de tien medewerkers zit. Dat is de hele som. Exclusief btw en Microsoft-licenties.

Overstappen van je huidige leverancier

De grootste rem op een overstap is zelden de prijs. Het is de angst dat er een ochtend is waarop niemand kan werken. Die ochtend hoort er niet te zijn, en bij een nette overname is die er ook niet — omdat we niets omzetten voordat het nieuwe klaarstaat.



Wat wij van je huidige partij nodig hebben

- Beheerderstoegang tot de Microsoft-omgeving
- Toegang tot het beheer van de domeinnaam
- Een overzicht van lopende licenties en contracten
- Wachtwoorden van netwerkapparatuur en de firewall
- Wat er aan documentatie is, hoe weinig ook

Werkt je huidige partij niet mee? Dan is er in bijna alle gevallen een route om er zonder hen uit te komen. Die kost tijd en soms geld, maar je zit niet vast. Dat is precies waarom deel 1 van dit handboek over eigenaarschap gaat.

Wat wij van jou nodig hebben

- Een aanspreekpunt binnen het bedrijf dat besluiten mag nemen
- Je opzegtermijn: wij plannen de overstap daaromheen
- Eén avond of weekend voor het omschakelmoment
- Een half uur van je mensen voor uitleg over hoe ze ons bereiken

Zeg niet op voordat er een plan ligt. Eerst de inventarisatie en de planning, dan pas de brief. Andersom heb je een deadline zonder route.

Eén ding vragen wij van tevoren. Vertel ons wat er nu níét goed gaat, ook als het ongemakkelijk is — een omgeving die jarenlang is doorgemodderd, apparatuur die veel te oud is, of een vorige leverancier waarmee het slecht is geëindigd. Wij schrikken daar niet van. We schrikken wel als we het pas halverwege de overname ontdekken.

Veelgestelde vragen

Wij zijn maar met zes man. Is dat niet te klein voor jullie?

Nee. Daarvoor bestaat de basisfee: onder tien medewerkers rekenen we € 75 per maand extra, daarboven vervalt die. Wel zeggen we het eerlijk als een vast contract bij jou nog niet loont. Soms is een paar uur werk en één keer per jaar meekijken genoeg.

Wij hebben al een IT-partij en die doet het prima.

Dan hoeft je niets te doen. Loop de zes vragen op pagina 5 langs. Komt daar iets uit dat je niet bevalt, leg het dan eerst bij hen neer. Blijft het antwoord uit, dan praten we verder.

Hoe snel reageren jullie?

Tijdens kantooruren doorgaans binnen het uur, bij iets waardoor niemand kan werken meteen. Wij zetten geen reactietijd in een contract die we niet elke keer halen. Wat we wél beloven: je krijgt iemand aan de lijn die je omgeving kent.

Zitten jullie niet in Turkije?

Klopt, ons kantoor staat in Istanbul en we zijn elke maand in Nederland. Vrijwel al het beheerwerk gebeurt op afstand — bij ons en bij iedere andere partij. Voor wat handen vraagt, staat er elke twee maanden een vaste onderhoudsdag bij jou ingepland. Zie pagina 19, inclusief wanneer wij níét de juiste keuze zijn.

Moeten wij overstappen naar nieuwe licenties?

Alleen als daar een reden voor is. Soms zit je te hoog en betaal je voor functies die niemand gebruikt. Dat komt net zo vaak voor als het omgekeerde en levert direct geld op.

Zitten we ergens aan vast?

Maandelijks opzegbaar, geen stilzwijgende verlenging. Alleen de eenmalige inrichting betaal je vooraf, want dat werk is dan al gedaan.

Wat kost de IT-scan?

Niets, en je zit nergens aan vast. Je houdt het overzicht, ook als je besluit bij je huidige partij te blijven.

Een vraag die hier niet tussen staat? Stuur hem gewoon. Wij beantwoorden ook vragen van bedrijven die geen klant worden — dat kost ons twintig minuten en het scheelt je soms een verkeerde beslissing.

DE VOLGENDE STAP

Begin met de scan. Beslis daarna pas.

Eén week, geen kosten, geen verplichting. Je krijgt een overzicht van wat er staat, wat er misgaat als er niets verandert, en wat het zou kosten om het netjes te maken. Blijf je bij je huidige partij, dan houd je dat overzicht gewoon.

E-MAIL

info@itspine.nl

TELEFOON

020 - 224 62 69

WEBSITE

itspine.nl

Liever eerst kort sparren? Plan een gesprek van dertig minuten via Teams. Wij bellen niet na. Als je iets van ons wilt, hoor je van ons — anders niet.

IT Spine · Managed IT voor het MKB in Nederland en Türkiye

Mimaroba Mah. Mustafa Kemal Blv. No: 18, İç Kapı No: 21, Büyükdere / İstanbul

Vergi No 4691545117 · MERSİS 0469154511700001

Uitgave augustus 2026. Bedragen exclusief btw. Tarieven en licentievoorwaarden kunnen wijzigen; vraag de actuele stand op voordat je ergens op rekent.