



“Het zorgt ervoor dat je elke IT-beslissing die je ooit hebt genomen in twijfel trekt”



DE MKB IT BUYERS GUIDE

*12 dingen die u moet weten voordat je
een nieuwe IT-provider kiest zodat je geen
tijd, geld of je verstand verliest*

GERARD BAKKER

INHOUDSOPGAVE

De 3 soorten IT-ondersteuning die u moet kennen	6
Waarom bedrijven van IT-provider wisselen	14
Hoe u zich voorbereidt op een IT-overdracht	20
12 dingen die u moet weten voordat u kiest	29
Welke IT heeft u eigenlijk nodig?	54
IT-termen uitgelegd in begrijpelijk Nederlands	58
Slimme vragen om te stellen tijdens het verkoopgesprek	64
Hoe u een serviceovereenkomst leest zonder in slaap te vallen	74
BONUS: vergelijkingswerkblad	85

VAN ONDERNEMER TOT ONDERNEMER

Beste collega-ondernemer,

Als u dit leest, is de kans groot dat u op zoek bent naar een IT-leverancier, of dat u zich op zijn minst afvraagt of uw huidige leverancier nog steeds aan uw eisen voldoet.

Hoe dan ook, ik ben blij dat je dit boek gaat lezen.

Ik run zelf een MSP. En in de loop der jaren heb ik talloze gesprekken gevoerd met ondernemers die teleurgesteld waren in hun vorige provider, overweldigd waren door technisch jargon, of gewoon moe waren van het gissen hoe "goede IT" eruit zou moeten zien.

Dit boek is het resultaat van die gesprekken.

Dat gezegd hebbende, het is waarschijnlijk niet wat je een 'normaal' boek zou noemen.

Ik verwacht niet dat je dit boek van begin tot eind leest met een kop thee en een markeerstift. (Tenzij je dat leuk vindt, in dat geval, lees dan verder.)

Zie het meer als een gereedschapskist dan als een roman.

Je begint niet met een sleutel en werkt je dan op naar een schroevendraaier. Je pakt wat je nodig hebt wanneer je het nodig hebt.

Blader naar het hoofdstuk dat het beste past bij waar je nu mee bezig bent. Vind je antwoord, vind een goede IT-leverancier en vergeet dat dit boek bestaat.

Als je dat doet, is mijn taak volbracht.

En ik zeg dat omdat ik hier niet ben om je iets te verkopen.

Ik ben hier om u door de 12 eenvoudige vragen te leiden die iedereen zich volgens mij zou moeten stellen voordat hij of zij een IT-contract ondertekent.

Dit zijn dezelfde vragen die ik mijn eigen vrienden en familie zou willen stellen als ze iemand zouden kiezen om hun systemen te beheren, hun gegevens te beschermen en het bedrijf draaiende te houden.

Tegen de tijd dat u dit boek uit hebt, weet u:

- Hoe u immuun kunt worden voor de duistere 'bait and switch'-tactieken van veel IT-leveranciers
- Waar u op moet letten bij een IT-contract voordat u het ondertekent, zodat u niet vast komt te zitten aan verborgen kosten, valkuilen met automatische verlenging of ontbrekende services
- Hoe u uw bedrijf kunt beschermen tegen downtime, gegevensverlies en spelletjes bij het wisselen van provider
- De meest voorkomende rode vlaggen die IT-providers proberen te verbergen tijdens verkoopsgesprekken, en hoe u ze kunt herkennen
- Hoe je het verschil kunt zien tussen een provider die je bedrijf echt wil laten groeien en een provider die alleen maar uit is op je maandelijkse betaling
- De waarschuwingssignalen dat uw huidige provider mogelijk aan het afglijden is, zelfs als alles op het eerste gezicht 'prima' lijkt
- Hoe u het beste type IT-ondersteuning kiest voor uw zakelijke doelen, behoeften en budget.

En nog veel meer!

Sommige pagina's bevestigen wat je al vermoedde. Andere kunnen je misschien een andere kijk op je huidige situatie geven.

Hoe dan ook, het doel is om u duidelijkheid te verschaffen zonder de gebruikelijke technische onzin.

Blader er dus doorheen en maak gerust aantekeningen. Of tel in gedachten de rode vlaggen die je al hebt gezien. Dat werkt ook.

Groeten,



Gerard Bakker
Eigenaar, Radix MKB ICT



"Op het moment dat je een beslissing moet nemen, is het beste wat je kunt doen het juiste. Het ergste wat je kunt doen, is niets doen."

— Theodore Roosevelt

VOORDAT JE ERIN DUIKT

Als u net als de meeste ondernemers met wie ik spreek bent, dan bent u niet meteen enthousiast geworden om een IT-leverancier te kiezen.

Het doel van deze gids is om het hele proces eenvoudiger en een stuk minder frustrerend te maken. Deze 12 vragen helpen je erachter te komen of iemand je daadwerkelijk steunt, of juist slechte service biedt.

Wat je binnen vindt:

- ✓ 12 directe vragen
- ✓ Hoe goede antwoorden klinken
- ✓ Rode vlaggen waar u op moet letten
- ✓ Een paar dingen waar je misschien niet aan gedacht hebt om te vragen

Ook vindt u een handvol extra hulpmiddelen waarmee u aanbieders kunt vergelijken en slimmere beslissingen kunt nemen, zonder dat u urenlang hoeft te googelen.

Inbegrepen bonussen:



Checklist werkblad

Een checklist waarmee u uw 3 beste IT-providers naast elkaar kunt vergelijken.



Technisch jargon in begrijpelijk Nederlands

Een verklarende woordenlijst met de 50 meest voorkomende termen die een IT-provider kan gebruiken.



IT-installatie-overzicht

Een gids om u te helpen bepalen welk niveau technische ondersteuning u nodig hebt.



Verkoopgesprekdetective

Een lijst met belangrijke vragen die u IT-leveranciers kunt stellen tijdens verkoopgesprekken.



Hoe u een serviceovereenkomst leest zonder in slaap te vallen

Een gids om ervoor te zorgen dat u nooit meer het slachtoffer wordt van een slechte serviceovereenkomst.

HOOFDSTUK 1

De 3 soorten IT-ondersteuning die u moet kennen



Break-Fix



Managed
Services



Co-Managed
IT

NIET ALLE IT IS HETZELFDE GEBOUWD

De meeste mensen scharen 'IT-ondersteuning' onder één grote, vage categorie.

Er gaat iets kapot, je belt de IT'er, en hij doet... iets met een toetsenbord. Misschien verdwijnt het probleem. Misschien ook niet. Hoe dan ook, je betaalt de factuur en gaat verder.

In werkelijkheid kent IT-ondersteuning drie verschillende modellen, elk met zijn eigen structuur, sterke punten en voor- en nadelen.

Als je niet weet welke je gebruikt (of waarvoor je eigenlijk betaalt), kun je gemakkelijk met verwachtingen komen die niet overeenkomen.

U denkt misschien dat u iemand hebt ingehuurd om 'alles te beheren', maar wat u werkelijk hebt gekregen is iemand die eens per kwartaal langskomt om een wachtwoord opnieuw in te stellen.

Dit is het grote plaatje:

- **Break-Fix is als een loodgieter bellen als de leiding gesprongen is. Je betaalt alleen als er iets misgaat.**
- **Managed Services (MSP) is vergelijkbaar met het inhuren van een vastgoedbeheerder. Zij regelen namens u onderhoud, monitoring en calamiteiten.**
- **Co-Managed IT is teamwerk: uw eigen personeel regelt de dagelijkse gang van zaken, terwijl een MSP de backend ondersteunt en gespecialiseerde taken afhandelt.**

Je hoeft geen techneut te zijn om dit te begrijpen. Maar je moet wel weten waar je voor tekent, zodat je het model kunt afstemmen op je werkelijke behoeften, en niet alleen op je budget.

Laten we ze één voor één bekijken, te beginnen met het meest voorkomende startpunt: Break-Fix.

BREAK-FIX IT



Break-Fix

Dit is de meest basale vorm van IT-ondersteuning en het leek ook een tijdje de meest logische.

Break-Fix is precies wat de naam al zegt: er gaat iets kapot en je belt iemand om het te repareren.

Er is geen monitoring, geen proactief onderhoud of regelmatige controles.

U krijgt een technicus aan de lijn die ter plaatse komt als er een probleem is, u een uurtarief rekent en verdergaat zodra het probleem is opgelost.

Het is net zoiets als een loodgieter bellen als er een leiding is gesprongen. Je betaalt niet om ze te behouden, je betaalt alleen als er iets misgaat.

Voor heel kleine bedrijven – zelfstandig ondernemers, kleine winkels of startups met een beperkt budget – kan Break-Fix een goede ondersteuning zijn.

Al met al tegenwoordig geen geweldig model meer.

Dit is waarom:

- De technicus heeft vaak geen echte kennis van je installatie. Hij of zij stapt het probleem in, zonder documentatie of voorgeschiedenis.
- Het kan zijn dat ze niet meteen beschikbaar zijn, waardoor de downtime langer duurt dan u zou willen.

- Omdat er geen sprake is van een doorlopende relatie, is er geen enkele reden om u te helpen toekomstige problemen te voorkomen.
- Elke oplossing is reactief. Tegen de tijd dat ze arriveren, is de schade al aangericht.

En laten we niet vergeten: omdat er geen monitoring of inzicht achter de schermen is, worden problemen die onder de oppervlakte sluimeren (zoals mislukte back-ups of een verlopen antivirusprogramma) niet opgemerkt totdat ze echte problemen worden.

Het is dus riskant om erop te vertrouwen als technologie een cruciale rol speelt in uw bedrijfsvoering.

Heeft u slechts af en toe hulp extra nodig dan kan Break-Fix prima kunnen werken.

Maar als je ooit hebt gezegd: "We kunnen het ons niet veroorloven om een dag offline te zijn", is het waarschijnlijk goed om daar eens verder over na te denken.

BEHEERDE DIENSTEN



Terwijl Break-Fix de loodgieter alleen belt als er een leiding is gesprongen, zorgt Managed Services ervoor dat een erkende professional regelmatig de kleppen controleert, de afdichtingen aandraait en ervoor zorgt dat er helemaal niets lekt, zelfs als u niet oplet.

Met Managed Services wacht u niet tot er iets misgaat. In plaats daarvan betaalt u een maandelijks bedrag aan uw IT-provider om uw systemen actief te beheren.

Dat omvat het monitoren van problemen, het installeren van updates, het dichten van beveiligingslekken, het verwerken van back-ups en het bieden van dagelijkse ondersteuning wanneer er iets misgaat.

Maar het is meer dan alleen een 'uitbesteedde helpdesk'.

Een goede MSP reageert niet alleen op problemen, hij voorkomt ze ook.

Ze documenteren je hele omgeving. Ze kennen je mensen, je apparaten en de systemen waarop je vertrouwt. En op termijn zouden ze je IT-strategie moeten sturen, niet alleen je tickets oplossen.

Dat gezegd hebbende, niet alle MSP's zijn hetzelfde.

Sommige beloven de maan, maar bieden slechts oppervlakkige ondersteuning. Anderen bundelen alles behalve wat je echt nodig hebt, tenzij je erom vraagt. Hoewel het model proactief is ontworpen, hangt het succes ervan nog steeds af van de keuze van de juiste partner.

Als u een bedrijf runt met gedeelde apparaten, cloud-apps of zelfs milde nalevingsbehoeften (en u een hekel hebt aan verrassingen), is dit model op de lange termijn vaak het meest kosteneffectief.

U weet dat dit model geschikt voor u kan zijn als:

- U wilt voorspelbare kosten en minder technische noodgevallen.
- Je bent voorbij het punt dat je “even iemand belt” als er iets misgaat.
- Uitvaltijd betekent verlies van omzet, productiviteit of klantvertrouwen.
- U wilt strategische input van uw provider, en niet alleen technische ondersteuning.
- Je bent op zoek naar een langdurige relatie, niet zomaar een snelle oplossing.

Bedenk dat tegenwoordig 80% of meer te maken heeft met proactief beheren. Btandjes blussen is nog maar een klein gedeelte van het werk

Dit is wat het betekent als u uw IT daadwerkelijk beheert.

CO-BEHEERD



Co-Managed

In een co-managed opstelling werken uw interne IT-team en een externe MSP samen.

Stel je voor dat je een loodgieter in dienst hebt die alle leidingen in het gebouw kent en dat je een professioneel loodgietersbedrijf inhuurt om de aansluitingen bij de gemeente, het overstromingspreventiesysteem en de druktesten te verzorgen.

Jouw interne team verzorgt de dagelijkse IT-taken: gebruikersinstellingen, wachtwoorden opnieuw instellen, printerproblemen en vragen van Janet over het niet synchroniseren van haar e-mail.

Ondertussen is de MSP verantwoordelijk voor infrastructuuraudits, systeembak-ups, patches, beveiligingsupdates en planning voor groei of naleving.

U geeft uw interne IT-team de ruimte om te ademen en krijgt tegelijkertijd toegang tot diepgaandere expertise, bedrijfshulpmiddelen en back-up wanneer iemand ziek, overbelast of gewoonweg vastloopt.

Maar dat werkt alleen als de grenzen duidelijk zijn. Zonder gedefinieerde rollen, gedeelde documentatie en wederzijds vertrouwen kunnen de zaken snel uit de hand lopen. Tickets raken kwijt, draden raken gekruist en "wij tegen zij" sluipt erin... waar niemand baat bij heeft.

U weet dat co-managed wellicht de juiste keuze is als:

- Uw interne IT-team is sterk, maar heeft het moeilijk
- U bereidt zich voor op naleving, groei of audits
- Er zijn hiaten in monitoring, cyberbeveiliging of documentatie
- U wilt een vangnet voor het geval uw belangrijkste technicus vertrekt

WELKE IS GESCHIKT VOOR JOU?

Nu u de opties hebt besproken, gaan we kijken welke het beste bij uw behoeften past.

Er is geen universeel 'beste' model. Alleen het model dat het beste past bij uw omvang, systemen, budget en tolerantie voor technische problemen.

Hoe maakt u dan een keuze?

Begin met waar je bent, en waar je naartoe gaat.

- Grootte is belangrijk. Of je nu een solo-operator bent of een team van twee, Break-Fix kan (voorlopig) werken. Maar zodra technologie essentieel wordt voor de dagelijkse bedrijfsvoering, wil je iets stabielers.
- Denk eens aan de complexiteit. Controleert u alleen uw e-mail en gebruikt u spreadsheets? Of bent u bezig met het combineren van cloudplatforms, externe toegang, bestandsservers en complianceregels? Hoe meer bewegende onderdelen, hoe meer waarde u haalt uit beheerde of co-beheerde services.
- Downtimetolerantie. Hoeveel tijd en geld verliest u als systemen uitvallen? Als een storing leidt tot klachten van klanten, omzetverlies of gemiste deadlines, voelt Break-Fix als spelen met vuur.
- Heeft u al interne IT? Zo ja, zien ze er moe uit? Als ze altijd maar bezig zijn met het oplossen van "alledaagse" problemen in plaats van zich te richten op beveiliging of planning, geeft Co-Managed IT hen ademruimte en ondersteuning.
- Hoe zit het met de groei? Bent u aan het werven? Uitbreiden? Betreedt u nieuwe markten? Een proactieve IT-partner kan u helpen opschalen zonder uw eigen infrastructuur te verstoren.
- En tot slot, slaap je goed? Als je wakker wordt van technische stress of je team vertraagt, heb je meer nodig dan alleen Break-Fix.

Je hoeft geen IT-expert te worden om een slimme keuze te maken. Je hoeft alleen maar je bedrijf, je risico's en je doelen te kennen.

HOOFDSTUK 2

Waarom bedrijven van IT-provider wisselen en hoe u weet of u dat nu moet doen



6 TEKENS WAAROP U MOET LETTEN

Het wisselen van IT-leverancier is iets wat de meeste bedrijven niet lichtzinnig doen. Het komt meestal voort uit een patroon van frustraties, van het soort dat zich langzaam opbouwt en dan ineens explodeert.

Wanneer zaken niet meer werken zoals ze zouden moeten, of wanneer het vertrouwen zo gering is dat het niet meer te herstellen is, besluiten bedrijven dat het genoeg is geweest.

Hoewel elke situatie uniek is, vallen de redenen waarom de meeste bedrijven overstappen in een paar bekende categorieën.

1. Operationele fouten

Dit zijn de momenten waarop alles vastloopt en de provider gewoon... niet aanwezig is. Een ransomware-aanval wordt verkeerd aangepakt, een kritieke storing duurt dagenlang, of back-ups die "zeker werkten" blijken lege mappen te zijn.

Wanneer deze fouten zich voordoen, brengt dit schade toe aan het bedrijf. De omzet loopt terug. De reputatie krijgt een deuk. Compliance kan in gevaar komen.

En het allerergste: het vertrouwen in uw IT-leverancier neemt af.

De werkelijke schade zit niet altijd in de storing zelf, maar in de manier waarop de provider reageert (of niet).

Zijn ze kalm, helder en in controle? Of worstelen ze zich zonder plan, zonder updates en zonder verantwoording?

Deze storingen zijn meestal niet eenmalig. Ze zijn tekenen van zwakke systemen en slechte planning, en vormen vaak de druppel die de emmer doet overlopen.

2. Terugkerende technische problemen

Een goede IT-provider lost het probleem niet alleen op. Ze stellen de diagnose, documenteren het en zorgen ervoor dat het niet terugkomt. Maar als dat niet gebeurt, past je team zich aan... op de verkeerde manier.

Ze nemen geen contact meer op met de support. Ze zoeken hun eigen oplossingen. En langzaam betaal je voor ondersteuning die je eigenlijk niet gebruikt.

3. Gebrek aan proactiviteit

Sommige providers zijn heel goed in reageren. Maar alleen in reageren.

Ze wachten tot er iets kapotgaat en springen dan in. Maar buiten noodsituaties hoor je zelden iets van ze. Geen strategie. Geen upgrades. Geen vooruitplannen.

Er is geen technologische roadmap, geen check-ins, geen suggesties om je systemen scherp te houden. Je hebt het gevoel dat jij degene bent die problemen aankaart, niet zij.

4. Slechte communicatie en ondersteuning

Het is één ding als systemen haperen. Het is een ander ding als de support hetzelfde doet. Als tickets onbeantwoord blijven, updates nooit komen of je team problemen steeds opnieuw moet uitleggen, is dat slechte service.

Of als elk nieuw probleem door een onbekende wordt afgehandeld, zonder enige context, wordt uw bedrijf slechts een nummer in de wachtrij.

En dan houden werknemers op met ze te bellen. "Neem maar geen contact met ze op. Het duurt nog een week", zeggen ze.

Zo'n interne cultuur is moeilijk ongedaan te maken.

5. Niet-passende relatie

Soms gaat het helemaal niet om de techniek.

De aanbieder is misschien wel competent. Maar als hij of zij je bedrijf niet begrijpt, niet naar je doelen vraagt of elk gesprek als een transactie aanvoelt, is het moeilijk om vertrouwen op te bouwen.

Sommige aanbieders maken nooit de overstap van leverancier naar partner. Ze repareren weliswaar computers. Maar ze denken niet strategisch na, bieden geen begeleiding en tonen geen nieuwsgierigheid naar hoe uw bedrijf er daadwerkelijk voor staat.

6. Prijs- versus waarde-afwijking

IT is een investering. Maar als de kosten blijven stijgen en de ervaring hetzelfde (of slechter) blijft, merken mensen dat.

Misschien word je wel opgelicht en moet je voor elk klein dingetje betalen. Misschien voelen je facturen elke maand als een verrassingsfeestje. Of misschien betaal je meer voor 'upgrades' die eigenlijk niets lijken te doen.

En wat is het meest frustrerende?

Je weet nooit zeker wat er allemaal is inbegrepen, wat er extra is en of de prijs de waarde ervan weerspiegelt.

VRAGEN DIE U ZICHZELF MOET STELLEN (VOORDAT U OVERSTAPT)



? Als uw provider morgen verdwijnt, hoe moeilijk zou het dan zijn om te herstellen?

Zou je een lijst met systemen, logins, software en processen aan iemand anders kunnen overdragen? Of zou je oude e-mails doorspitten en hopen op het beste?

Als alles in het hoofd van je provider (of hun accounts) leeft, ben je afhankelijk.

? Wat is er de afgelopen 12 maanden daadwerkelijk verbeterd?

Is de ondersteuning sneller geworden? Komen er steeds minder problemen voor? Hebben ze je geholpen bij het upgraden van systemen, het verbeteren van de beveiliging of het stroomlijnen van iets?

Als het antwoord 'niet echt' of 'ik denk dat het hetzelfde is' is, is dat het vermelden waard.

IT mag nooit het gevoel hebben dat het alleen maar water trapt. Een goede leverancier zet stappen vooruit, al is het maar een klein beetje, kwartaal na kwartaal.

Zou u ze met trots aanbevelen aan een andere bedrijfseigenaar?

Vergeet beleefdheid. Zou je tegen een vriend zeggen: "Je moet zeker eens met onze IT-provider praten"?

Als je instinct zegt dat ze 'oké' zijn, of 'goed voor de prijs', dan zegt dat alles wat je moet weten.

Goede aanbieders verdienen aanbevelingen. Middelmatige aanbieders vertrouwen op jouw traagheid.

Voelt u zich veiliger, productiever of meer in controle dan een jaar geleden?

Hebben ze kwetsbaarheden gesignaleerd of de beveiliging verbeterd? Zijn systemen soepeler en minder verstorend geworden? Voelt u zich goed geïnformeerd of tast u nog steeds in het duister?

Als uw angst voor technologie niet is afgenomen, of uw werklust daaromheen niet is afgenomen, doen ze hun werk niet goed genoeg.

Helpen ze u problemen te voorkomen?

Hebben ze verbeteringen voorgesteld voordat er iets kapotging? Hebben ze je geholpen met het budgetteren van upgrades? Hebben ze je gewaarschuwd voor een riskante installatie waarvan je niet eens wist dat die risicovol was?

Of hoor je alleen van hen als er iets mislukt, goedkeuring nodig is of extra kosten met zich meebrengt?

Als ze geen problemen voorkomen, moet u uw samenwerking met hen wellicht heroverwegen.

WAAROM BEDRIJVEN NIET OVERSTAPPEN (OOK AL ZOUDEN ZE DAT WEL MOETEN DOEN)



Angst voor verstoring

Wat als overstappen meer kapotmaakt dan oplost? Het is een terechte vraag. Niemand wil de zaken erger maken in naam van verbetering. Stel je voor: storingen, toegangsproblemen, vergeten wachtwoorden, verward personeel en overal branden.

Maar maak je geen zorgen. Een goede IT-leverancier creëert een gestructureerd onboardingplan met overlap, documentatieoverdracht en risicobeheersing.

Als uw huidige provider de zaken nauwelijks draaiende houdt, is het echte risico dat u blijft.



Loyaliteit en vertrouwdeheid

"We werken al jaren met ze samen. Het zijn goede mensen."

Dit is misschien wel de moeilijkste om mee om te gaan. Je mag ze wel. Ze hebben je geholpen tijdens die ransomware-angst. Misschien hebben jullie zelfs wel samen geluncht.

Maar soms kan de persoon die ooit zo goed was, het niet meer bijhouden. En dan moet je in actie komen in het belang van je bedrijf.



Onzekerheid over het overstapproces

"Hoe vergelijk ik überhaupt aanbieders? Wat als ik weer de verkeerde kies?"

Het is de angst voor het onbekende. De overtuiging dat het veiliger is om met de duivel die je kent om te gaan dan nog een kans te wagen.

Maar daarom lees je deze gids. Ik leg je uit waar je op moet letten. Wat je moet vragen. Wat je kunt verwachten.

HOOFDSTUK 3

Hoe u zich voorbereidt op een zorgeloze IT-overdracht



WAAROM VOORBEREIDING ALTIJD BETER IS DAN PANIEK



We hebben al duidelijk gemaakt dat de beslissing om van IT-provider te wisselen meestal wordt genomen na een reeks problemen: herhaaldelijke uitval, genegeerde tickets, beveiligingsproblemen of een prijsverhoging die uiteindelijk de doorslag geeft.

Tegen de tijd dat je zegt: "We zijn klaar", ben je waarschijnlijk gefrustreerd. Misschien boos. Misschien zelfs een beetje angstig over wat er komen gaat.

Als je overstuur bent, is de natuurlijke drang om snel te handelen. Wegwezen, de kabel eruit trekken en verdergaan. Maar snelheid zonder structuur zorgt ervoor dat je uiteindelijk geen toegang meer hebt tot je eigen e-mail, je wachtwoorden moet resetten of aan de telefoon blijft hangen met je oude provider die smeekt om DNS-toegang die ze vergeten zijn over te zetten.

Paniek leidt tot fouten. En in de IT zijn fouten tijdens een overdracht gevaarlijk.

Dit is waar het overhaasten van de overstap vaak toe leidt:

- Kritieke inloggegevens en beheerderstoegang blijven achter
- Niemand had gaten in de dienstverlening verwacht
- Onbedoelde schendingen van contracten of licentievoorwaarden
- Een verbrande brug met uw huidige provider (die nog steeds de sleutels tot uw technologie bezit)

Als u uw bedrijf wilt beschermen, moet u zich afvragen: "Hoe kan ik ervoor zorgen dat dit nooit meer gebeurt?"

Laten we stap voor stap uitleggen hoe je dat doet.

INVENTARISEREN



Voordat je iets kunt overdragen, moet je weten wat je precies overdraagt.

Dat klinkt voor de hand liggend, totdat je beseft hoeveel bedrijven geen idee hebben wat er allemaal in hun IT-omgeving gebeurt.

Er zijn in de loop der jaren dingen toegevoegd. Sommige door de vorige aanbieder. Sommige door een technisch onderlegde stagiair. Sommige... je weet niet eens zeker door wie.

De meeste kleine tot middelgrote bedrijven hebben geen overzichtelijk, centraal overzicht van hun hardware, software, tools en accounts. Dat is prima, totdat het tijd is om van provider te wisselen.

Het is tijd om dat te verhelpen.

Wat moet u in uw inventaris opnemen:

Apparaten en hardware

- Servers, werkstations, laptops en mobiele apparaten (inclusief die van extern personeel)
- Printers, scanners en VoIP-telefoons
- Netwerkkapitaal: firewalls, switches, routers, toegangspunten

Software en platforms

- Bedrijfssoftware (zoals uw CRM of boekhoudstelsysteem)
- E-mail (Microsoft 365, Google Workspace, enz.)
- Antivirus-/EDR-tools, cloudopslag (Dropbox, OneDrive), tools voor externe toegang

Rekeningen en infrastructuur

- Domeinregistrator
- DNS-host (Cloudflare, Microsoft, enz.)
- Websitehost (WordPress, Squarespace)
- Gegevens van uw internetprovider en statische IP's, indien van toepassing

Back-ups

- Waar zijn ze?
- Wie controleert ze?
- Hoe vaak worden ze getest?

De waarheid is dat dit proces overweldigend kan zijn.

Dat is prima. Je hebt geen perfecte lijst nodig, je moet gewoon inzicht hebben in wat je daadwerkelijk gebruikt en waar je op vertrouwt.

HAAL UW INLOGGEGEVENS OP (ALLE)



Dit gebeurt vaker dan nodig is: een bedrijf neemt afscheid van zijn provider en komt er vervolgens achter dat het geen beheerderstoegang heeft tot Microsoft 365.

Of hun back-ups. Of hun domeinregistrar.

Geloof me, dat is niet iets wat je wilt meemaken.

Voordat u verdergaat, moet u controleren wie de toegangsrechten heeft en zeker weten dat u die persoon bent.

Begin met kritieke beheerderstoegang

U (of iemand binnen uw team) moet over volledige beheerdersrechten beschikken op:

- Microsoft 365
- Uw back-upplatform
- Firewalls, routers en andere netwerkkaparaatuur
- Uw antivirus- of eindpuntbeveiliging
- Website CMS (zoals WordPress)
- Domeinregistrator en DNS-host

Controleer MFA en herstelinstellingen

Twee-factorauthenticatie moet altijd afzonderlijk worden geconfigureerd.

Geen algemeen admin@uwbedrijf.com. Niet uw MSP. En zeker geen privénummer van een ex-werknemer.

Controleer meteen de e-mails voor accountherstel die aan uw belangrijkste platforms zijn gekoppeld.

Als ze leiden naar iemand die jaren geleden is vertrokken, is dat een kwetsbaarheid die uitgebuit kan worden.

Licentie- en factureringseigendom beoordelen

U dient als contactpersoon voor facturering te worden vermeld op elk systeem en softwareplatform waarop uw bedrijf vertrouwt.

Sommige providers maken licenties aan onder hun eigen hoofdaccount. Dat is in het begin handig, maar een nachtmerrie als het tijd is om over te stappen.

Het ontwarren van die afhankelijkheid kan tijdrovend, duur en riskant zijn.

Zorg ervoor dat je waar voor je geld betaalt.

Wachtwoordbeheer organiseren

Als uw team nog steeds afhankelijk is van gedeelde spreadsheets of automatisch invullen in de browser voor aanmeldingen, is het nu tijd om te upgraden.

Gebruik een wachtwoordbeheerder en verdeel deze in twee kluizen: één voor dagelijkse teamlogins en één privékluis voor inloggegevens op eigenaarsniveau.

Zo voorkomt u toegangslekken en behoudt u tegelijkertijd inzicht en verantwoording over uw systemen.

BEKIJK HET CONTRACT

Haal diep adem, open uw contract en let op de volgende clausules:

Opzeggingstermijn

Let op de kleine lettertjes: de meeste MSP-contracten vereisen een schriftelijke opzegtermijn van 30 tot 90 dagen. Sommige contracten worden automatisch verlengd, tenzij ze vóór een bepaalde datum worden opgezegd.

Als u de termijn mist, kan het zijn dat u opnieuw voor een volledige termijn moet betalen.

Kosten voor vroegtijdige beëindiging

Sommige contracten bevatten vaste boetes voor vroegtijdig vertrek. Andere rekenen kosten voor data-export, 'overgangsarbeid' of zelfs licentieoverdracht.

Het staat niet altijd duidelijk aangegeven. Het kan verborgen zitten onder termen als 'offboardingkosten' of 'administratieve afhandeling'.

Wie bezit wat?

Bent u daadwerkelijk de eigenaar van uw documentatie, scripts en configuraties, of worden deze beschouwd als 'propriëtaire tools' die door de leverancier zijn ontwikkeld?

Let op zinnen als "blijft het intellectuele eigendom van..."

Als uw leverancier over belangrijke systeemkennis beschikt, is hij mogelijk niet verplicht deze kennis over te dragen.

Verplichtingen voor offboarding-ondersteuning

In sommige contracten staat expliciet dat de aanbieder moet helpen bij de overgang (bijvoorbeeld het delen van documentatie, het onderhouden van systemen tijdens de exitperiode). Andere contracten zeggen helemaal niets, wat betekent dat je afhankelijk bent van hun houding.

Hoe dan ook, als u weet waartoe ze contractueel verplicht zijn, heeft u meer invloed.

Bepalingen die het niet-in diskrediet brengen of het voorkomen van muilkorven

Het komt zelden voor, maar sommige MSP's hebben clausules ingebouwd die het u verbieden om negatief over hen te spreken in recensies, doorverwijzingen of gesprekken met concurrenten.

Wees alert voordat je iets openbaar maakt. Zelfs als ze een fout hebben gemaakt, kan het overtreden van een clause je in de problemen brengen.

PLAN DE OVERDRACHT



Maak eerst een strakke tijdlijn

De meeste chaotische overgangen ontstaan omdat mensen het proces overhaasten of dingen half afmaken.

Dit is de juiste volgorde:

1. Kies uw nieuwe provider
2. Plan onboarding en documentatieoverdracht
3. Geef daarna pas uw oude provider op
4. Stel een duidelijk overgangsvenster in (meestal 2–4 weken)
5. Deactiveer oude accounts pas nadat de volledige test is voltooid

Waarom deze bestelling belangrijk is: Als u te vroeg annuleert, verliest u uw invloed en mogelijk ook de toegang.

Wat de nieuwe provider eigenlijk zou moeten doen

Een echte provider kopieert niet alleen wat uw oude MSP deed. Ze evalueren alles opnieuw.

Verwacht van hen dat zij:

- Controleer en documenteer uw omgeving (apparaten, platforms, instellingen, enz.)
- Standaardiseer wachtwoorden en reset machtigingen
- Verwijder ongebruikte accounts of tools
- Pas patches toe, activeer MFA en verstevig uw systemen
- Nieuwe back-ups, monitoring en antivirus instellen

Verwacht een paar "Wacht... Wat?!"-momenten

De meeste bedrijven realiseren zich pas hoe rommelig het is als iemand hun opstelling gaat inspecteren.

Veelvoorkomende verrassingen zijn:

- Gedeelde wachtwoorden die door hele teams worden gebruikt
- Back-ups die al maanden niet werken
- Verlopen antivirus of licentie
- Oud-personeel heeft nog steeds toegang
- Domeinen die op het punt staan te verlopen
- Documentatie die ontbreekt of verouderd is

Budget voor opruiming

Ga er niet vanuit dat u met deze overgang vanaf dag één geld bespaart.

Een goede leverancier zal waarschijnlijk enkele upgrades of schoonmaakwerkzaamheden aanbevelen.

Dat is een teken dat ze het goed doen, zonder concessies te doen.

HOOFDSTUK 4

12 dingen die u moet weten voordat u een nieuwe IT-provider kiest, zodat u geen tijd, geld of uw verstand verliest



CONTROLEPUNT #1

STELLEN ZE SLIMME VRAGEN OVER UW BEDRIJF?



In de eerste 10 minuten van een gesprek kun je veel over een IT-provider (of eigenlijk over wie dan ook) te weten komen.

En dat kun je doen door aandacht te besteden aan de vragen die ze stellen.

Een goede IT-partner begint niet met praten over zijn pakketten, plannen of "volledig beheerd blah blah blah".

Ze zullen oprecht nieuwsgierig zijn naar uw bedrijf.

Hoe jouw team werkt.

Op welke hulpmiddelen u vertrouwt.

Waar dingen vaak misgaan, zoals die ene vreemde workflow die alleen Lisa van de boekhouding begrijpt.

De dingen die er echt toe doen.

Want de waarheid is dat uw bedrijf niet 'gewoon' is zoals elk ander bedrijf.

En als een IT-leverancier u als een sjabloon behandelt dat u in een standaardoplossing kunt implementeren, zult u dat merken aan tragere workflows, slecht presterende systemen en veel momenten waarop u zich afvraagt: "Waarom is dit nog steeds een probleem?".

In plaats daarvan wilt u iemand die zich gedraagt als een partner.

Iemand die eerst luistert en vervolgens in kaart brengt hoe technologie jouw doelen kan ondersteunen. Of het nu gaat om het laten groeien van je team, het verminderen van risico's of gewoon om het minder vervelend maken van de dinsdagochtend.

Dat is het soort aanpak waar u op moet letten bij een IT-leverancier.

Als iemand proactief is in zijn of haar eerste gesprek met jou, is de kans groot dat hij of zij dit ook zal blijven doen gedurende de hele samenwerking.

En het is niet moeilijk om te herkennen.

Je weet dat je iemand waardevols hebt gevonden als diegene vragen stelt als:

- "Wat vertraagt jouw team op dit moment?"
- "Welke software is voor u bedrijfskritisch?"
- "Heb je last van terugkerende hoofdpijnen waar je mee moet leren leven?"
- "Waar ziet u het bedrijf over 12 maanden?"

Aan de andere kant, als hun eerste zet is om je een standaardplan voor te schotelen en over prijzen te beginnen praten voordat ze je bedrijf begrijpen, dan is dat een probleem.

	
Rode vlaggen:	Groene vlaggen:
 "Ons standaardabonnement is voor iedereen geschikt."	 Vragen over teamworkflows
 Gaat direct over tot prijsbepaling	 Onderzoek de frustraties van uw personeel
 Praat alleen over technische specificaties	 Stelt toekomstgerichte vragen
 Weinig interesse in unieke processen	 Benieuwd naar kritische software
 Geen gedetailleerde workflowvragen	 Ontdekt terugkerende hoofdpijn
 Dringt aan op snelle toewijding	 Stelt vragen die je aan het denken zetten

CONTROLEPUNT #2

KUNNEN ZE IN BEGRIJPELIJK NEDERLANDS UITLEGGEN WAT ZE DOEN?



U hoeft geen computerwetenschapper te zijn om te begrijpen waar uw IT-leverancier het over heeft.

Niemand heeft de tijd (of de wilskracht) om technisch jargon te ontcijferen. Zelfs ik rol met mijn ogen als ik het zie.

Een goede aanbieder zou dit moeten weten.

Ze gebruiken alledaagse taal, en ratelen geen modewoorden op om slim over te komen.

Als je na een vergadering het gevoel hebt dat je verward of overweldigd bent, of dat je het gevoel hebt dat je alleen maar hebt zitten knikken om niet over te komen als iemand die niet in je element is...

Je praat absoluut met de verkeerde persoon.

Duidelijkheid is niet optioneel in de IT.

Beslissingen hebben betrekking op uw gegevens, uw geld en het vermogen van uw team om hun werk goed te doen.

Die beslissingen moeten eenvoudig te begrijpen zijn, anders loopt uw bedrijf gevaar. En dat is precies het tegenovergestelde van wat er zou moeten gebeuren als u iemand inschakelt om te helpen.

Het doel is niet om indruk te maken met technische termen. Het is om ervoor te zorgen dat je begrijpt wat er gedaan wordt, waarom het belangrijk is en hoe het je bedrijf beïnvloedt.

Daarom is het belangrijk dat je vanaf de eerste ontmoeting goed oplet hoe ze praten.

Vaak is het de manier waarop ze in een vroeg stadium met je in contact komen, die de toon voor de samenwerking bepaalt. (Dit is een terugkerend thema in het boek).

Sommigen zullen je om de tuin leiden om indruk te maken.

Anderen maken het complexe eenvoudig, zonder dat je je daardoor klein voelt.

U weet dat u een goede IT-provider hebt gevonden als:

- Ze vereenvoudigen ingewikkelde ideeën.
- Je hebt nooit het gevoel dat er op je wordt neergekeken.
- Ze gebruiken herkenbare voorbeelden.
- Visuele hulpmiddelen verduidelijken, niet verwarren.
- Je weet precies wat er gaat gebeuren.

Als dat niet gebeurt, ga dan verder. En kijk niet om, want het is de moeite niet waard.

	
Rode vlaggen:	Groene vlaggen:
 Zwaar jargon	 Eenvoudige, duidelijke uitleg
 Praat neerbuigend of betuttelend	 Zorgt ervoor dat je je op je gemak voelt
 "Het is ingewikkeld, vertrouw ons."	 Herkenbare, alledaagse taal
 Je voelt je verloren	 Gebruikt visuele hulpmiddelen om concepten te vereenvoudigen
 Overweldigende technische details	 Controleert uw begrip
 Verwarring na vergaderingen	 Geduldig met uw vragen

CONTROLEPUNT #3

LATEN ZE U EEN VOORBEELDOVEREENKOMST ZIEN VOORDAT U ZICH VASTLEGT?



Verrassingen zijn prima op verjaardagsfeestjes. Niet in contracten.

Zeker niet het soort dat pas opduikt nadat je 'ja' hebt gezegd, verstopt in tien pagina's met kleine lettertjes en vage juridische onzin.

Een goede ICT-leverancier speelt geen spelletjes met het papierwerk.

Sterker nog, ze bieden aan om je door de overeenkomst te loodsen voordat er iets officieel is. Niet alleen per e-mail versturen en hopen dat je geen vragen stelt, maar echt samen zitten en de belangrijkste punten doornemen.

Wat is inbegrepen? Wat niet? Hoe lang het duurt? Hoe je eruit komt als je onderweg uit elkaar gaat.

U moet precies weten wat u kunt verwachten voordat u tekent. Dat betekent geen vage voorwaarden, geen addertjes onder het gras en geen magische verdwijnende diensten die alleen tijdens het verkooppraatje werden genoemd.

Als je de overeenkomst samen doorneemt, kun je ook zien hoe ze omgaan met de minder glamoureuze zaken.

Hoe snel reageren ze?

Rekenen ze extra kosten voor bezoeken ter plaatse? Is er ondersteuning beschikbaar in het weekend?

Kun je makkelijk annuleren als je niet tevreden bent, of zit je vast tot het einde der tijden?

Als ze wachten met het versturen van de overeenkomst totdat je mondeling ja hebt gezegd, of je vragen afdoen met iets als: "Maak je geen zorgen, het is allemaal standaard", dan is dat een teken dat ze niet graag aan details gebonden willen zijn.

En met zo iemand wil je geen zaken doen. Vanaf dat moment gaat het bergafwaarts.

Dit soort IT-leveranciers reageren vaak pas laat, ontlopen verantwoording en in sommige gevallen verdwijnen ze helemaal in het niets.

Daarom is het handig om te weten hoe de juiste aanpak er in de praktijk uitziet.

U weet dat u een betrouwbare IT-provider hebt gevonden als...

- Ze staan erop dat ze samen de contracten doornemen.
- De voorwaarden zijn glashelder: geen verrassingen achteraf.
- Ze benadrukken proactief kritische clausules.
- Er is transparantie over kosten en tijdlijnen.
- Het beëindigen van de overeenkomst is eenvoudig en eerlijk.

	
Rode vlaggen:	Groene vlaggen:
 Contract last-minute getoond	 Voorafgaande overeenkomstbeoordeling
 Zegt: "Het is allemaal standaard"	 Geeft duidelijk aan wat er is inbegrepen
 Verborgene clausules of lastige voorwaarden	 Transparante prijzen en tijdlijnen
 Geen duidelijke exitstrategie	 Eenvoudige annuleringsvoorwaarden
 Ontwijkt specifieke vragen	 Proactief met contractbesprekingen
 Dringt aan op snelle ondertekening	 Nodigt uw vragen openlijk uit

CONTROLEPUNT #4

KUNNEN ZE RECENTE, RELEVANTE REFERENTIES OVERLEGGEN?



Elke provider kan grootspraak bedrijven. De echte vraag is: kunnen ze dat waarmaken met iemand die niet betaald wordt om aardige dingen te zeggen?

Je moet met een echte klant kunnen praten. Niet alleen een selectief getuigschrift van vijf jaar geleden lezen, en niet zomaar een berg vijfsterrenrecensies doornemen die net zo goed door hun neef geschreven hadden kunnen zijn.

Een echte bedrijfseigenaar of manager die onlangs met hen heeft samengewerkt.

Idealiter is dit iemand die een bedrijf runt dat ongeveer even groot is als het uwe en met vergelijkbare problemen kampt.

Wanneer een IT-provider zegt: “Wij doen niet echt aan referenties” of vage excuses aanbiedt over privacy, is dat meestal een teken dat er niemand is die voor hen kan instaan.

En dat is belangrijk, want je koopt geen kant-en-klaar product.

U kiest iemand die in uw systemen zit, met uw gegevens aan de slag gaat en uw bedrijf operationeel houdt als er iets misgaat.

Daarom zal een goede aanbieder niet aarzelen als je om referenties vraagt. Ze hebben ofwel een lijst met klanten die al bereid zijn hun ervaringen te delen, of ze doen er alles aan om er een samen te stellen.

Sommigen bieden zelfs aan om een kort gesprek in te plannen, zodat u direct kunt horen hoe het is om met hen samen te werken.

Als iemand anders zoals jij een goede ervaring heeft gehad, is dat meer waard dan welk verkooppraatje dan ook.

Je kunt vragen stellen die geen enkele website je zal vertellen.

Hoe de onboarding verliep.

Hoe de provider omging met problemen die zich voordeden. Of beloftes daadwerkelijk werden nagekomen nadat het contract was getekend.

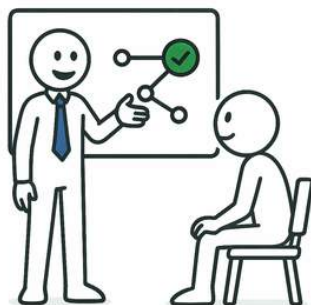
U weet dat u een betrouwbare IT-provider hebt gevonden als...

- Zij verstrekken zonder aarzeling referenties.
- U kunt direct met recente klanten spreken.
- Hun referenties komen overeen met uw bedrijfsprofiel.
- Cliënten bespreken openlijk hun sterke punten, maar ook hun uitdagingen.
- Gesprekken met referenties geven je vertrouwen.

	
Rode vlaggen: ✗ Vage excuses voor privacy ✗ Alleen verouderde getuigenissen ✗ Recensies klinken te algemeen ✗ Geen direct klantcontact ✗ Vermijdt het bespreken van problemen uit het verleden ✗ Referenties klinken gerepeteerd	Groene vlaggen: ➤ Biedt gemakkelijk relevante contacten ➤ Recente klantgesprekken ➤ Klantervaringen van vergelijkbare omvang ➤ Klanten bespreken probleemoplossing ➤ Open over uitdagingen uit het verleden ➤ Authentieke, evenwichtige feedback

CONTROLEPUNT #5

BEGELEIDEN ZE JE DOOR EEN DUIDELIJK ONBOARDINGPLAN?



Het laatste wat u wilt, is een contract tekenen en vervolgens weken – of zelfs maanden – in de wacht staan zonder de juiste IT-ondersteuning.

Daarom moet u nooit akkoord gaan met iets voordat u precies weet wat er gaat gebeuren als het contract is getekend.

Een goede IT-leverancier moet het onboardingproces duidelijk en stap voor stap kunnen uitleggen.

Hoe ze de ondersteuning overnemen en welke systemen ze gaan auditen.

Wie uit hun team praat met wie uit jouw team?

Wat u kunt verwachten in week één, week twee en daarna.

Hoe meer duidelijkheid ze je vooraf geven, hoe groter de kans dat ze dit al eerder hebben gedaan, en goed hebben gedaan.

Ze hebben een checklist en idealiter een tijdlijn, zodat je precies weet wanneer dingen worden beoordeeld, geïnstalleerd, verbeterd of opgeruimd.

Als ze daarentegen je vragen afwimpelen met: “Dat lossen we wel op zodra de papieren binnen zijn”, dan is dat meestal een probleem.

Het zou kunnen betekenen dat ze het maar op de gok doen, en als ze aan het begin van de samenwerking improviseren, wekt dat zeker niet veel vertrouwen in hoe ze de rest zullen aanpakken.

Let hier goed op, vooral als u van plan bent uw IT over te dragen vanaf uw vorige IT-leverancier.

Je wilt niet dat iemand zich meer richt op het sluiten van de deal dan op wat er daarna gebeurt.

De meeste problemen beginnen bij de overdracht, en die kunnen snel uitgroeien tot een puinhoop waar moeilijk aan te ontkomen is.

U weet dat u een voorbereide IT-provider hebt gevonden als...

- Ze bieden een duidelijke onboarding-tijdslijn.
- Je weet precies wie erbij betrokken is, en wanneer.
- Elke onboardingstap wordt duidelijk in kaart gebracht.
- Er is geen sprake van vroege verwachtingen.
- Je voelt je vanaf dag één zelfverzekerd.

	
Rode vlaggen:	Groene vlaggen:
 "Dat lossen we later wel op."	 Stapsgewijs onboardingplan
 Onduidelijke verwachtingen voor de eerste week	 Duidelijke teamrollen en verantwoordelijkheden
 Vermijden van tijdslijnspecifieke details	 Gedefinieerd schema van evenementen
 Vage informatie over systeemaudits	 Geeft duidelijk de eerste acties aan
 Lijkt onvoorbereid of improviserend	 Bewezen onboarding checklist
 Aarzelt met uw vragen	 Proactieve, zelfverzekerde communicatie

CONTROLEPUNT #6

CONTROLLEREN ZE UW IT EN BEVEILIGING VOORDAT ZE U EEN OFFERTE STUREN?



Stel je voor dat je een dokterspraktijk binnenloopt en een recept krijgt, nog voordat je een woord hebt gezegd.

Dat is wat het is als een IT-leverancier een offerte stuurt zonder eerst te kijken hoe uw bedrijf daadwerkelijk functioneert.

Als ze niet de tijd nemen om uw systemen te controleren, vragen te stellen over uw configuratie of uw beveiligingsrisico's in te schatten, gokken ze maar wat.

En in de IT leidt gokken vaak tot problemen.

Elk bedrijf heeft zijn eigenaardigheden. Misschien heb je verouderde hardware die het nauwelijks volhoudt.

Misschien is uw wifi-verbinding uitstekend, maar is uw back-upstelsysteem al jaren niet meer getest.

Misschien klikt uw personeel wel op phishingmails alsof het een sport is.

Er zijn zoveel scenario's dat ik een heel boek zou schrijven om ze allemaal te bespreken.

Een standaardplan is niet voldoende. Daarom begint een goede aanbieder met ontdekken.

Ze vragen om toegang tot uw systemen, voeren scans uit, praten met uw team en onderzoeken wat werkt, wat niet werkt en wat u in gevaar brengt.

Alleen met dit soort audits weet u welke ondersteuning u daadwerkelijk nodig hebt.

Het vertelt je ook iets belangrijks over de manier waarop ze opereren.

Nemen ze uw bedrijf serieus of proberen ze alleen maar een kant-en-klaar plan te promoten?

Het doel moet zijn om een nauwkeurig beeld te krijgen van waar u zich nu bevindt, zodat u geholpen kunt worden om te bereiken waar u wilt zijn.

U weet dat u een betrouwbare IT-leverancier hebt gevonden als...

- Zij voeren vooraf een degelijke systeemaudit uit.
- Veiligheidsrisico's worden duidelijk in kaart gebracht.
- Hun aanbevelingen komen overeen met uw werkelijke configuratie.
- Zij begrijpen de unieke gewoonten van uw team.
- Ze onderzoeken in plaats van te gokken.

	
Rode vlaggen:	Groene vlaggen:
 Offertes zonder voorafgaande controle	 Voert eerste ontdekkingssessies uit
 Gaat ervan uit dat alle cliënten hetzelfde zijn	 Biedt beveiligingsbeoordelingen
 Negeert uw huidige instellingen	 Baseert offertes op feitelijke gegevens
 Algemeen, generiek advies	 Begrijpt unieke zakelijke eigenaardigheden
 Lijkt erop dat er haast is gemaakt om het snel te verkopen	 Markeert risico's en verbeteringen
 Vertrouwt sterk op giswerk	 Bekijk aanbevelingen

CONTROLEPUNT #7

GEVEN ZE PRIORITEIT AAN HET VOORKOMEN VAN PROBLEMEN, OF ALLEEN AAN HET OPLOSSEN ERVAN?



Sommige IT-providers spelen graag de heldenrol als er iets kapotgaat. Ze springen in, redden de boel en krijgen de lof.

Maar als je altijd wacht tot er iets fout gaat voordat iemand actie onderneemt, betaal je alleen maar voor schadebeperking.

Goede IT gaat niet alleen over het blussen van brandjes. Het gaat erom ervoor te zorgen dat er in de eerste plaats minder brandjes ontstaan.

De juiste aanbieder richt zich op preventie bij het opzetten van uw techniek.

Dat betekent dat u uw systemen 24/7 moet bewaken, beveiligingspatches moet toepassen, uw software up-to-date moet houden en problemen moet signaleren voordat ze zich tot echte problemen ontwikkelen.

Het meeste gebeurt achter de schermen, en als ze hun werk goed doen, merk je niet eens dat het gebeurt... en dat is ook een beetje de bedoeling.

Wanneer u aanbieders evalueert, vraag hen dan hoe zij verstoringen tot een minimum beperken.

Houden ze terugkerende problemen bij en zoeken ze naar patronen?

Sturen ze regelmatig rapporten waarin ze laten zien wat ze doen om alles soepel te laten verlopen?

Of blijven ze vooral rustig afwachten tot er weer een storing is?

Je moet niet iemand inhuren met als enige doel het omgaan met crises.

Als hun houding ten aanzien van ondersteuning reactief aanvoelt, dan is dat waarschijnlijk ook zo.

Dingen repareren nadat ze kapot zijn gegaan, lijkt op het moment zelf misschien handig, maar het is geen slimme strategie voor de lange termijn.

En achteraf oplossen wordt snel duur, vooral wanneer de downtime de werkcapaciteit van uw klanten of team negatief beïnvloedt.

U weet dat u een proactieve IT-provider hebt gevonden als...

- Zij controleren systemen 24/7 actief.
- Problemen worden opgelost voordat u ze opmerkt.
- Regelmatige rapportages geven duidelijk aan welke preventieve maatregelen er zijn genomen.
- Ze identificeren patronen om herhaling van problemen te voorkomen.
- Hun strategie is preventie, niet reactie.

	
Rode vlaggen:	Groene vlaggen:
 Wacht tot er problemen ontstaan	 24/7 actieve monitoring
 Viert het oplossen van veelvoorkomende problemen	 Regelmatig preventief onderhoud
 Negeert probleempatronen	 Proactieve updates en patches
 Alleen reactieve communicatie	 Transparante rapportage over preventie
 Geen duidelijk plan voor preventie	 Identificeert trends om herhaling te voorkomen
 Gaat vooral over noodsituaties	 Consistente focus op uptime

CONTROLEPUNT #8

KUNNEN ZE DUIDELIJK UITLEGGEN WAT ER WEL EN NIET IS INBEGREPEN?



Een goede IT-leverancier maakt glashelder waarvoor u maandelijks betaalt en, net zo belangrijk, wat er niet bij inbegrepen is.

Dat betekent dat u een overzichtelijke opsomming van de diensten op één pagina krijgt, zodat er geen verwarring ontstaat wanneer iets gerepareerd, geüpgraded of vervangen moet worden.

Als er een project opduikt, moet u vooraf weten of het deel uitmaakt van uw plan of als extra wordt beschouwd.

Hetzelfde geldt voor bezoeken op locatie, ondersteuning buiten kantoortijden en hardware-installaties.

Zelfs dingen als Dave van de afdeling verkoop helpen met het terughalen van een bestand dat hij drie weken geleden heeft verwijderd, maar nu plotseling nodig heeft.

Wees voorzichtig met termen als 'onbeperkte ondersteuning' als deze een lange lijst met voetnoten en kleine lettertjes bevatten.

Onbeperkt betekent zelden wat u denkt dat het betekent, en als de grenzen niet duidelijk zijn, kunnen de facturen zich snel opstapelen.

Een transparante aanbieder zal deze gesprekken niet uit de weg gaan.

Ze leggen je uit wat er allemaal is inbegrepen, waar de grens ligt voor extra werk en hoe ze omgaan met zaken die buiten het plan vallen.

Zo voorkom je dat je achteraf voor onaangename verrassingen komt te staan.

Het gaat er niet om elk detail tot in de puntjes te regelen. Het gaat erom verwarring te voorkomen wanneer er iets gedaan moet worden en je niet zeker weet of het gedekt is.

Als de verwachtingen aan beide kanten duidelijk zijn, worden beslissingen makkelijker en ontstaat er sneller vertrouwen.

En een langdurige, op vertrouwen gebaseerde samenwerking is waarschijnlijk wat u zoekt.

U weet dat u een transparante IT-provider hebt gevonden als...

- De inbegrepen diensten worden duidelijk vermeld.
- Extra kosten komen nooit als een verrassing.
- Ze verduidelijken proactief 'onbeperkte' diensten.
- De grenzen tussen projecten en werk buiten werktijd zijn duidelijk.
- U hoeft nooit meer te gissen naar uw rekening.

	
Rode vlaggen:	Groene vlaggen:
 "Onbeperkt" vol met uitzonderingen	 Kristalheldere service-indeling
 Vaak onverwachte kosten	 Transparant over extra kosten
 Ontwikkelt details over wat er is inbegrepen	 Verduidelijkt wat als extra wordt beschouwd
 Vage informatie over kosten voor bezoeken ter plaatse	 Duidelijk gedefinieerde factureringsstructuur
 Vermijd het om vooraf over factureringsgegevens te praten	 Eenvoudige documentatie
 Voetnoten die uitsluitingen verbergen	 Beantwoordt openlijk vragen over facturering

CONTROLEPUNT #9

HOE GAAN ZE OM MET COMMUNICATIE- EN ONDERSTEUNINGSVERZOEKEN?



Benjamin Franklin zei ooit: "In deze wereld is niets zeker, behalve de dood en de belastingen."

Persoonlijk zou ik zeggen: "In deze wereld is niets zeker, behalve de dood, belastingen en kapotte technologie."

In de IT komt het vaak voor dat dingen op het slechtst denkbare moment misgaan.

Eigenlijk gaan dingen vaak kapot wanneer je ze het hardst nodig hebt.

En als dat gebeurt, is het van groot belang hoe snel u hulp krijgt.

Voordat u een contract tekent met een IT-leverancier, vraag dan hoe de ondersteuning er op een normale dag uitziet.

Hoe dien je een verzoek in? Is er een ticketsysteem?

Bel, mail of chat je met iemand? Wie reageert er eigenlijk? En hoe snel?

U betaalt voor technische ondersteuning, maar ook voor responsiviteit, structuur en gemoedsrust.

Als er iets kritisch niet meer werkt, moet u precies weten wie u kunt bereiken en wat voor reactie u kunt verwachten.

De beste aanbieders hebben hiervoor een duidelijke procedure.

Ze maken duidelijk waar u terecht kunt als u hulp nodig hebt, wie verantwoordelijk is voor het oplossen van het probleem en hoe lang het meestal duurt.

IT-providers die net dat stapje extra zetten, delen zelfs rapporten met gemiddelde respons- en oplossingstijden. Zo bewijzen ze dat ze hun verantwoordelijkheid serieus nemen.

Als het antwoord daarentegen zoiets is als: "Stuur ons gewoon een e-mail en we gaan ermee aan de slag", dan is dat een waarschuwingssignaal. Het klinkt misschien wat voorbarig, maar het betekent meestal dat er geen echt systeem achter de schermen zit.

U weet dat u een responsieve IT-provider hebt gevonden als...

- Er is een duidelijk, gestructureerd ondersteuningsproces.
- Je weet precies hoe je ze kunt bereiken en wie reageert.
- Responsstijden worden bijgehouden en gedeeld.
- Dringende kwesties krijgen dringend aandacht.
- Je hebt er vertrouwen in dat ze er voor je zijn als het erop aankomt.

	
Rode vlaggen: ✗ "Stuur ons gewoon een e-mail en wacht" ✗ Geen duidelijkheid over wie reageert ✗ Er wordt niet gesproken over reactietijden ✗ Informeel of vaag over het proces ✗ Moeilijk bereikbaar tijdens noodgevallen ✗ Inconsistente communicatie	Groene vlaggen: ➤ Gedefinieerd ticketing-/ondersteuningssysteem ➤ Benoemd menselijk aanspreekpunt ➤ Volgt en deelt ondersteuningsstatistieken ➤ Stapsgewijze ondersteuningsworkflow ➤ Prioritaire hulp bij dringende problemen ➤ Snelle, betrouwbare responskanalen

CONTROLEPUNT #10

WERKEN ZE MET JOUW GEREEDSCHAP OF DWINGEN ZE JE OM OVER TE STAPPEN?



Sommige IT-leveranciers komen binnen, bekijken uw installatie en beginnen meteen met het plannen van de vervanging.

Nieuwe software, nieuwe systemen, nieuwe platforms – allemaal gekozen op basis van wat zij het liefst gebruiken, niet op basis van wat daadwerkelijk goed is voor uw bedrijf.

Soms kan het zinvol zijn om over te stappen op een ander hulpmiddel, bijvoorbeeld als uw huidige systemen verouderd zijn, niet worden ondersteund of voortdurend vastlopen.

Een goede aanbieder zal u hierop wijzen en de risico's duidelijk uitleggen.

Maar als de enige reden waarom ze iets vervangen is: "dit is wat we voor al onze klanten gebruiken", dan moet je vragen gaan stellen.

Je bedrijf draait al op bepaalde tools. Misschien kent je team ze van binnen en van buiten. Misschien zijn je workflows erop gebaseerd.

Een aanbieder die dat respecteert, zal in ieder geval proberen om eerst te werken met wat u heeft.

Als ze een overstap voorstellen, leggen ze je de voor- en nadelen uit en bespreken ze hoe je de overgang zo soepel mogelijk kunt laten verlopen.

Het doel moet altijd zijn om uw manier van werken effectiever te maken.

Dus als het gesprek begint met "We hebben je nodig om alles te verhuizen", en eindigt zonder een gegronde reden, dan is het misschien tijd om verder te gaan... zonder hen.

Het is gemakkelijk voor een provider om iets wat voor hen vertrouwd is, op te dringen.

Als ze echter niet vragen hoe uw team daadwerkelijk dagelijks functioneert, ontwerpen ze geen persoonlijke oplossing voor uw bedrijf.

Daarom wil je iemand die nieuwsgierig is in plaats van een uitgesproken mening te hebben.

Iemand die vragen stelt, uw workflows in kaart brengt en zoekt naar manieren om uw huidige situatie te verbeteren.

U weet dat u een goede IT-leverancier hebt gevonden als...

- Ze nemen de tijd om uw huidige hulpmiddelen te begrijpen.
- Upgrades gaan gepaard met heldere, strategische overwegingen.
- Wij respecteren uw workflows en passen ze niet aan.
- Ze zorgen voor soepele en geen geforceerde overgangen.
- De technologie past bij uw bedrijf, en niet andersom.

	
Rode vlaggen: ✗ “We verplaatsen je naar onze tools” ✗ Een softwarebenadering die voor iedereen geschikt is ✗ Voert veranderingen door zonder uitleg ✗ Negeert de vertrouwdeheid van het team met opstellingen ✗ Schakelt tussen gereedschappen voor hun gemak ✗ Geen input over wijzigingen	Groene vlaggen: ➤ Openstaan voor het werken met jouw gereedschap ➤ Aanbevelen op basis van uw configuratie ➤ Legt voor- en nadelen en overgangsplannen uit ➤ Respecteert bestaande workflows ➤ Geeft prioriteit aan bedrijfscontinuïteit ➤ Samenwerkende, adviserende upgrades

CONTROLEPUNT #11

HEBBEN ZE EEN PROCES (OF DOEN ZE MAAR WAT)?



Er is bijna niets erger dan een ICT-leverancier die meer op gevoel dan op systemen handelt.

Ze kunnen uw technische infrastructuur veranderen in een bord spaghetti.

Dit zijn mensen die reageren op wat er ook gebeurt en hopen dat het probleem zich niet meer voordoet.

Ze hebben geen checklist, geen routine en geen manier om hun voortgang bij te houden.

Dat zul je nooit zien bij een goede IT-leverancier. Of het nu gaat om een eenmanszaak of een team van vijftig man, ze zouden duidelijk gedocumenteerde processen moeten hebben voor hoe ze werken.

En ze moeten kunnen uitleggen hoe hun processen werken, ook al is het maar een algemeen overzicht.

Je hoeft niet alle details te weten, maar je moet er wel zeker van zijn dat ze een systeem hebben voor het verwerken van tickets, updates, onderhoud en beveiligingscontroles.

Vraag dus zeker naar hun routines.

Wordt er regelmatig onderhoud gepleegd?

Hoe worden ondersteuningsverzoeken behandeld?

Plannen ze beoordelingen of check-ins?

Zelfs een solo-adviseur kan een strak bedrijf runnen als hij of zij de juiste systemen heeft opgezet.

En aan de andere kant, als elk antwoord begint met “Het hangt ervan af” of “Ik ga gewoon met de stroom mee”, dan heb je een probleem.

Want zonder structuur gaat het vaker mis dan je wilt.

En als ze altijd maar in de reactiemodus staan, is uw bedrijf degene die de klap krijgt.

U weet dat u een procesgedreven IT-leverancier hebt gevonden als...

- Ze leggen uit hoe ze tickets, updates en onderhoud afhandelen.
- U begrijpt hoe ondersteuningsverzoeken worden gevolgd en opgelost.
- Regelmatig onderhoud is gepland en niet reactief.
- Processen worden ‘gedocumenteerd’ en niet alleen in iemands hoofd.
- Ze kunnen uitleggen hoe hun systemen werken.

	
Rode vlaggen: ✗ “Ik los dingen gewoon op zodra ze zich voordoen” ✗ Geen gedefinieerd proces voor tickets ✗ Geen schema voor beoordelingen of updates ✗ Geen documentatie van hun systemen ✗ Onduidelijke rollen/verantwoordelijkheden ✗ Preventie is niet uit te leggen	Groene vlaggen: ➤ Gedocumenteerd ondersteuningsproces ➤ Gebruikt een systeem voor het beheren van tickets ➤ Plan proactief beoordelingen ➤ Deelt onboarding-stappen ➤ Duidelijke rollen en verantwoordelijkheden ➤ Houdt terugkerende problemen bij

CONTROLEPUNT #12

VOELEN ZE ZICH ALS EEN PARTNER EN NIET ALLEEN ALS EEN KOSTWINNER?



Tegen de tijd dat u verkoopgesprekken voert, heeft u waarschijnlijk de website bekeken, de materialen gelezen en misschien zelfs een voorstel doorgenomen.

Maar dat zegt niets over hoe het werkelijk is om met hen te werken.

De echte aanwijzingen komen voort uit hoe ze omgaan met de eerste interacties. De toon van de e-mails, de vragen die ze stellen, de manier waarop ze reageren als je een probleem aankaart.

Als ze geen vervolg geven, of als ze uw zorgen nu al snel negeren, verwacht dan niet dat het na uw ondertekening vanzelf beter wordt.

Dit is uw kans om erop te letten hoe zij u behandelen.

Luisteren ze daadwerkelijk als je over je bedrijf praat?

Stellen ze doordachte vragen?

Zijn hun antwoorden toegespitst op jouw situatie, of hebben ze het gevoel dat ze gekopieerd zijn van de pitch van iemand anders?

Een echte partner laat zien dat hij/zij iets voor de lange termijn wil opbouwen. Dat betekent dat hij/zij responsief en transparant is, "Ik weet het niet" zegt wanneer hij/zij het niet weet, en de daad bij het woord voegt wanneer hij/zij zegt dat hij/zij het wel zal doen.

Als ze gehaast, opdringerig of te gretig lijken om de deal te sluiten, is dat een slecht teken en moet u het waarschijnlijk nog eens overwegen.

Kortom, vertrouw op je intuïtie.

Het is een van de meest onderschatte besluitvormingsinstrumenten die je hebt.

Als je ernaar luistert, zal het duidelijk zijn wie een goede partner is en wie niet.

Je weet dat je een echte partner hebt gevonden als...

- Ze nemen de tijd om uw bedrijf te leren kennen, en niet alleen uw technologie.
- Hun antwoorden voelen doordacht aan, niet gekunsteld.
- Ze doen wat ze zeggen.
- Je voelt je gerespecteerd, gehoord en gewaardeerd.
- Vanaf dag één voelt de relatie als een samenwerking.

	
Rode vlaggen: ✗ Opdringerig of gehaast verkoopproces ✗ Te veel beloften zonder echte antwoorden ✗ Vage of ontwijkende reacties ✗ Luistert niet en vraagt niet naar je doelen ✗ “Teken maar en wij regelen het” ✗ Negeert zorgen tijdens het verkoopproces	Groene vlaggen: ➤ Consultatieve, laagdrempelige gesprekken ➤ Eerlijke aanbevelingen op maat ➤ Duidelijke directe communicatie ➤ Stelt doordachte vragen ➤ Bereid om uw vertrouwen te verdienen ➤ Responsief en respectvol

HOOFDSTUK 5

Welke IT-opstelling heeft u eigenlijk nodig?





BASISBEHOEFTE / LAAG RISICO

U bent hier als:

- Je hebt 1–5 medewerkers
- Iedereen gebruikt voornamelijk basishulpmiddelen (e-mail, Office-documenten, browser)
- U slaat geen gevoelige gegevens op (gezondheids-, financiële, juridische gegevens, enz.)
- Uw bedrijf kan een technisch probleem een paar uur of zelfs een dag overleven

Veel voorkomende symptomen:

- “Wij bellen alleen als er iets kapot is”
- “Onze man is goedkoop en klaart de klus uiteindelijk”
- “We denken niet echt na over IT, tenzij er iets misgaat”

Wat heb je nodig:

- Ad-hoc/break-fix-ondersteuning
- Een betere expert voor noodgevallen
- Minimaal: gedocumenteerde wachtwoorden, geverifieerde back-ups en antivirus



GROEIEND BEDRIJF / GEMATIGD RISICO

U bent hier als:

- Je hebt 5–250 medewerkers
- U maakt gebruik van branchespecifieke tools of cloudplatforms
- Je kunt je geen downtime van langer dan een uur of twee veroorloven
- Je bent voorbij de 'we regelen het later wel'-modus gegroeid

Veel voorkomende symptomen:

- “We hebben deze maand drie keer hetzelfde probleem gehad”
- “Ik denk dat we voor drie verschillende cloudopslagleveranciers betalen”
- “We hebben een back-upsysteem, maar ik weet niet 100% zeker of het werkt”

Wat heb je nodig:

- Beheerde IT-services (MSP)
- 24/7 bewaking
- Snelle helpdeskondersteuning
- Beheer van updates, beveiliging, back-ups en leveranciers



MISSIEKRITIEK / HOOG RISICO

U bent hier als:

- U heeft 150+ werknemers OF u heeft een intern IT-team
- Uw bedrijf stopt als IT stopt
- U verwerkt gevoelige gegevens met inachtneming van de regelgeving (HIPAA, AVG, enz.)
- U wilt plannen voor groei, fusies en overnames of digitale transformatie

Veel voorkomende symptomen:

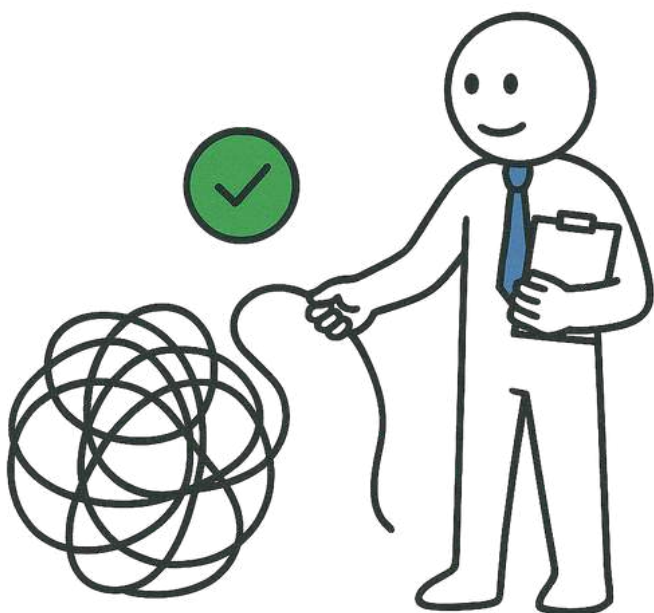
- “Ons interne IT-team is overbelast”
- “We moeten alles standaardiseren en documenteren”
- “We hebben een audit- of verzekeringsangst gehad”

Wat heb je nodig:

- Co-Managed IT
- Intern IT-team + MSP-back-up/ondersteuning
- Documentatie & planning
- Budgetvoorspelling en risicobeperking

HOOFDSTUK 6

*IT-termen uitgelegd in begrijpelijk
Nederlands*





TECHNISCH JARGON IN BEGRIPELIJK NEDERLANDS

Active Directory / Entra-ID

Waar al uw gebruikerslogins en toegangsregels zich bevinden.

Beheerdersrechten

Accounts met volledige toegang tot uw systemen. Dagelijkse gebruikers zouden nooit beheerdersrechten moeten hebben, omdat dit te veel mogelijkheden biedt voor fouten of malware.

Antivirus

Basissoftware die bekende bedreigingen blokkeert. Onmisbaar voor iedereen die een computer gebruikt, maar niet waterdicht.

Back-up

Kopieën van uw belangrijke bestanden. Cruciaal voor herstel na verwijdering.

Bandbreedte

Hoeveel data je internet tegelijk kan verwerken. Hoe meer data het kan verwerken, hoe sneller het zal zijn.

Bedrijfscontinuïteit

Een combinatie van back-ups, plannen en systemen die ervoor zorgen dat u online blijft.

BYOD (Bring Your Own Device)

Wanneer medewerkers hun eigen telefoons/laptops gebruiken voor hun werk. Soms handig, maar kan riskant zijn als er niet goed mee wordt omgegaan.

Cloud

Uw gegevens (e-mails, bestanden, systemen) veilig online opgeslagen.

Cloud-naar-cloud back-up

Back-ups van uw cloudgegevens (zoals e-mails of Drive)

Compliance

Volg regels zoals AVG, NIS2 of ISO27001 zodat u geen boetes (of hacks) krijgt.



TECHNISCH JARGON IN BEGRIJPELIJK NEDERLANDS

Disaster recovery

Het plan voor "Wat gebeurt er als alles misgaat?" Denk aan back-ups, reservehardware en cloud-failovers.

DNS (Domain Name System)

Het adresboek van het internet. Als het kapotgaat, stoppen websites met laden, zelfs als je internet het doet.

Downtime

Wanneer uw systemen niet meer werken en uw bedrijf op de rem trapt.

E-mailfiltering

Blokkeert schadelijke en vervelende e-mails voordat ze in uw inbox terechtkomen.

Encryptie

Een methode om uw gegevens te vergrendelen, zodat alleen geautoriseerde personen deze kunnen lezen, zelfs als iemand ze steelt.

Encryptie in rust

Zelfs als ze zijn opgeslagen, zijn je gegevens nog steeds versleuteld. Zo blijven ze veilig als iemand ze steelt.

Eindpunt

Elk apparaat dat is verbonden met uw netwerk: laptops, desktops, tablets, telefoons.

Eindpuntdetectie en -respons (EDR)

Slimme antivirussoftware die zoekt naar ongebruikelijk gedrag, niet alleen naar bekende virussen.

Firewall

Een 'beveiligingsagent' die voorkomt dat ongewenst verkeer uw netwerk bereikt.

Firewallregels

Instellingen die bepalen welk verkeer uw netwerk in- en uitgaat.



TECHNISCH JARGON IN BEGRIJPELIJK NEDERLANDS



Helpdesk SLA's

Reactietijdbeloftes van uw IT-leverancier.



Helpdeskticket

Een formele manier om een IT-probleem te melden.



IT-audit

Een volledig overzicht van uw systemen, risico's, licenties en zwakke plekken



Levenscyclusbeheer

Technologie volgen, zodat deze vervangen wordt voordat deze traag, riskant of kapot wordt.



Logbestand

Een dagboek achter de schermen van wat uw systeem heeft gedaan.



MFA Vermoedingsaanval

Hackers sturen u spam met inlogverzoeken in de hoop dat u op 'Goedkeuren' klikt om de aanval te stoppen.



Mobiel apparaatbeheer (MDM)

Houdt werktelefoons en tablets veilig. Kan gegevens wissen als een werknemer zijn of haar apparaat kwijtraakt ter bescherming tegen lekken.



Multi-factorauthenticatie (MFA)

Extra beveiligingsmaatregelen bij het inloggen, zoals het ontvangen van een sms-bericht nadat u uw wachtwoord hebt ingevoerd.



Onboarding / Offboarding

Nieuwe medewerkers voorzien van inloggegevens en apparaten (onboarding) of de toegang verwijderen wanneer ze het bedrijf verlaten (offboarding).



Patch / Patchen

Software-updates die bugs (problemen) of beveiligingslekken verhelpen.



DECODER VOOR BEGRIJPELIJK TECHNISCH JARGON



Patchbeheer

Het systeem dat ervoor zorgt dat uw apparaten up-to-date en veilig blijven.



Wachtwoordbeheerder

Een app die je wachtwoorden onthoudt, zodat je niet steeds "123456" hoeft te gebruiken.



Penetratietesten (Pen Test)

Ingehuurde hackers (de goede soort) proberen in te breken in uw systeem om zwakke plekken te vinden voordat de slechteriken dat doen.



Phishing

Misleidende e-mails waarmee geprobeerd wordt uw inloggegevens of bankgegevens te stelen.



Phishing-simulatie

Stuur veilige 'nep'-oplichtingsmails naar uw medewerkers om te testen hoe goed ze zijn voorbereid op een mogelijke phishingaanval.



Ransomware

Malware die uw bestanden blokkeert en betaling eist om ze te ontgrendelen.



Extern bureaublad

Toegang tot uw werkcomputer vanaf een externe locatie, alsof u er gewoon achter zit.



RMM (Remote Monitoring & Management)

Software waarmee uw IT-provider 24/7 toezicht houdt op uw systemen en problemen kan oplossen zonder dat hij ter plaatse hoeft te komen.



Grondoorzaakanalyse

Uitzoeken waarom iets kapot is gegaan, zodat het niet steeds kapotgaat.



SaaS (Software als een Service)

Apps op abonnementsbasis die u online kunt gebruiken, zoals Exact, CRM of Canva.



TECHNISCH JARGON IN BEGRIJPELIJK NEDERLANDS

Sandboxen

Testen van verdachte bestanden in een veilige, afgesloten digitale bubbel.

Schaduw-IT

Wanneer uw medewerkers hun eigen apps/tools installeren zonder dat iemand het weet.

SLA's (Service Level Agreements)

Beloftes die uw provider maakt over reactietijd, ondersteuningsuren, etc.

SSO (Single Sign-On)

Eén login voor toegang tot alles. Handig, maar moet wel goed beveiligd zijn.

Bedrijfstijd

Het percentage van de tijd dat uw systemen werken.

Gebruikersrechten

Wat elke persoon mag inzien, bewerken of verwijderen. Stel dit verstandig in.

Versiebeheer

Houdt wijzigingen in documenten of code bij, zodat er niets belangrijks verloren gaat.

VPN (Virtueel Privénetwerk)

Een beveiligde tunnel voor uw internetverkeer, handig voor teams op afstand.

Whitelist / Blacklist

Wat is toegestaan (witte lijst) en wat is geblokkeerd (zwarte lijst), zoals e-mails of apps.

Zero-Day-kwetsbaarheid

Een nieuw beveiligingslek waar hackers al van op de hoogte zijn, maar dat nog niet is gedicht.

HOOFDSTUK 7

Slimme vragen om te stellen tijdens het verkoopgesprek





WAT U KUNT VERWACHTEN

De meeste eigenaren van kleine bedrijven weten niet wat ze moeten vragen tijdens een verkoopgesprek met een IT-leverancier.

Dus knikken ze maar.

Ze horen moeilijke woorden als 'cyberveerkracht', 'next-gen endpoint protection' en 'zero trust-architectuur'.

De levering is strak. Het deck ziet er gepolijst uit. De prijs klinkt redelijk.

Maar zit er achter al die buzzwords wel echte inhoud?

Dit hoofdstuk geeft u precies de vragen die succesvolle ondernemers stellen. Het soort vragen waar IT-leveranciers wat rechter op gaan zitten.

Ze maken duidelijk wie bereid is uw bedrijf te steunen, en wie alleen maar een script voorleest.

Als u ze doorleest, zult u merken dat goede aanbieders niet in de verdediging schieten als u ernaar vraagt.

Ze zijn er blij mee, omdat ze het werk al gedaan hebben. Ze weten waar ze het over hebben. En ze willen graag samenwerken met klanten die slimme, strategische vragen stellen.

Gebruik dit als je gesprekspartner. Print het uit, bewaar het op je tweede scherm, maak er een checklist van, wat je ook helpt om de controle over het gesprek te houden.

Je hoeft niet elke vraag letterlijk te stellen. Maar je moet wel met een doel het gesprek ingaan.

Vraag het met vertrouwen.

Luister goed naar hun reactie.

En onthoud: je bent er niet om iets verkocht te krijgen.

VRAGEN

OVER HUN BEDRIJF

1 Wie zijn de mensen die ons daadwerkelijk dagelijks ondersteunen?

Je wilt controleren of het een betrouwbaar bedrijf is.



Groene vlag: "We hebben een toegewijd helpdeskteam en je belangrijkste contactpersoon is Sarah. Je ontmoet haar tijdens de onboarding."



Rode vlag: "Dat ben ik, en ik kom er zo snel mogelijk op terug."

2 Hoeveel klanten ondersteunt u, en hoeveel daarvan lijken op de onze?

Je controleert op ervaring en capaciteit.



Groene vlag: "We ondersteunen 42 bedrijven, voornamelijk met 5 tot 50 werknemers. Ongeveer 6 daarvan vallen in uw branche."



Rode vlag: "We hebben in het verleden met allerlei bedrijven samengewerkt."

3 Kan ik met een klant spreken die al meer dan een jaar bij u werkt?

U controleert de daadwerkelijke kwaliteit van het partnerschap en het vertrouwen op de lange termijn.



Groene vlag: Ze bieden met plezier een referentie aan.



Rode vlag: "Onze cliënten willen anoniem blijven."

VRAGEN

OVER HUN SERVICEMODEL

1 Wat is inbegrepen in de maandelijkse vergoeding, en wat niet?

Je bent op zoek naar sluwe uitsluitingen en valkuilen.



Groene vlag: Duidelijke, schriftelijke uiteenzetting zonder dubbelzinnigheid



Rode vlag: “Het is allemaal onbeperkt” (maar ik kan je niet laten zien wat dat inhoudt)

2 Hoe gaat u om met noodgevallen buiten werktijd?

U zoekt naar echte 24/7-ondersteuning.



Groene vlag: “Wij hanteren een oproepdienst en garanderen reactietijden”.



Rode vlag: “We nemen de volgende dag contact met u op”.

3 Verzorgen jullie ook het leveranciersbeheer, bijvoorbeeld met onze internetprovider of line-of-business-apps?

Je wilt weten of ze helpen als het vingerwijzen begint.



Groene vlag: “Ja, wij regelen het van begin tot eind, zodat u niet tussen wal en schip valt.”



Rode vlag: “Dat valt buiten onze scope”.

VRAGEN

OVER UW BEDRIJF

1 Hoe zou uw onboardingplan er voor ons uitzien?

Je controleert op structuur en doordachtheid.



Groene vlag: "We beginnen met een volledige audit, documenteren uw omgeving, ontmoeten uw personeel en stellen een stappenplan op voor 30-60-90 dagen."



Rode vlag: "Als je eenmaal tekent, komen we er wel uit"

2 Voert u een technische of beveiligingsaudit uit voordat u ons een offerte geeft?

U controleert of het bod op feiten is gebaseerd en of de koper het vereiste due diligence-onderzoek heeft uitgevoerd.



Groene vlag: "Absoluut. We doen eerst een risicobeoordeling en een verkennend gesprek."



Rode vlag: "Al onze klanten hebben hetzelfde abonnement, dus dat is niet nodig".

3 Hoe vaak bespreekt u met ons onze IT-strategie?

Je bent op zoek naar een proactieve samenwerking, niet naar een reactieve oplossing.



Groene vlag: "We spreken met u een ritme af om regelmatig problemen, risico's en verbeteringen te bespreken en uw technologie af te stemmen op uw bedrijfsdoelen."



Rode vlag: "We zijn beschikbaar als u ons nodig heeft."

VRAGEN

OVER RESULTATEN & RAPPORTAGE

1 Welke soort rapporten krijgen we en hoe vaak?

U controleert op transparantie, trends en verantwoording.



Groene vlag: "Maandelijkse rapporten met tickets, responstijden, updates en potentiële risico's."



Rode vlag: "Wij doen geen rapporten tenzij u erom vraagt."

2 Hoe meet u uw eigen prestaties intern?

Je controleert of ze zich aan echte meetgegevens houden.



Groene vlag: "Wij volgen de naleving van SLA's, de klanttevredenheidsscores en de tijd die nodig is om tickets op te lossen."



Rode vlag: "Wij zorgen er gewoon voor dat dingen gedaan worden."

3 Kunt u mij een voorbeeldrapport van een andere (geanonimiseerde) klant laten zien?

Je controleert of de rapporten daadwerkelijk nuttig zijn.



Groene vlag: "Jazeker, hier is een echte, namen verwijderd natuurlijk. Hij laat precies zien wat we volgen."



Rode vlag: "We hebben niet echt een standaardformat, het hangt ervan af..."

VRAGEN

OVER VEILIGHEID EN NALEVING

1 Wat is uw procedure voor het afhandelen van een beveiligingsincident en hoe stelt u ons op de hoogte?

U controleert of er sprake is van een duidelijk incidentenresponsplan en transparantie.



Groene vlag: "We volgen een formeel incidentresponsproces, stellen u onmiddellijk op de hoogte, documenteren alles en houden nabespreking."



Rode vlag: "We lossen het op en laten u weten of het ernstig is."

2 Hoe helpt u ons om te blijven voldoen aan de wetgeving inzake gegevensbescherming of verzekeringseisen?

U controleert of zij de verplichtingen van uw sector begrijpen.



Groene vlag: "Wij stemmen uw configuratie af op vereisten zoals AVG, NIS2, ISO27001 of verzekeringspolissen en leveren documentatie".



Rode vlag: "Dat is de verantwoordelijkheid van uw juridische team, niet van ons."

3 Welke hulpmiddelen of werkwijzen gebruikt u om proactief beveiligingsrisico's te beperken?

Je kijkt of ze verder gaan dan de basis.



Groene vlag: "We gebruiken kwetsbaarheidsscans, MFA, patching en phishing simulaties om bedreigingen voor te blijven."



Rode vlag: "We hebben antivirus en een firewall, dus u bent gedekt."

VRAGEN

OVER HUN DENKEN & STRATEGIE

1 Welke trends of bedreigingen houdt u momenteel in de gaten voor uw klanten?

Je controleert of ze proactief, geïnformeerd en strategisch zijn.



Groene vlag: "We houden AI-gestuurde phishingaanvallen, wijzigingen in Microsoft-licenties en aankomende veranderingen in de naleving nauwlettend in de gaten."



Rode vlag: "We pakken problemen aan zodra ze zich voordoen."

2 Wat is een recent voorbeeld waarbij u een klant hebt geholpen te groeien, op te schalen of de productiviteit te verbeteren met behulp van betere technologie?

Je kijkt of ze een impact op het bedrijf kunnen hebben.



Groene vlag: "We hebben een logistiek bedrijf geholpen 4 uur handmatig werk per dag te automatiseren door hun SharePoint-systeem te herstructureren."



Rode vlag: "We zorgen er vooral voor dat de systemen draaiende blijven."

3 Hoe besluit je wanneer het tijd is om iets in je omgeving te upgraden of te veranderen?

Je kijkt of ze vooruit plannen of pas reageren als er iets kapot gaat.



Groene vlag: "Wij beoordelen op basis van levenscyclus, ondersteuningsstatus, prestaties en bedrijfsdoelstellingen."



Rode vlag: "We vervangen het als het niet meer werkt."

VRAGEN

OVER FIT & EERLIJKHEID

1 Wanneer ben jij niet de juiste match voor een klant?

Je kijkt of ze zelfbewust zijn en duidelijk weten met wie ze het beste kunnen samenwerken.



Groene vlag: "Wij zijn niet ideaal voor bedrijven die slechts af en toe hulp nodig hebben of geen waarde hechten aan een strategie op de lange termijn."



Rode vlag: "Wij werken met iedereen."

2 Wat zou voor jou een reden zijn om een klant te ontslaan?

Je controleert hun waarden en grenzen.



Groene vlag: "Als een klant de beste beveiligingspraktijken negeert, ons team slecht behandelt of niet wil investeren in de basis."



Rode vlag: "Dat zouden we nooit doen." (Vertaling: geen grenzen)

3 Hoe ziet een goede klantrelatie er volgens jou uit?

Je controleert of ze aan een partnerschap hebben gedacht.



Groene vlag: "Voortdurende communicatie, gedeelde verantwoordelijkheid, openheid voor feedback en duidelijke bedrijfsdoelen."



Rode vlag: "Eentje waar we niet veel van je horen."

VRAGEN

OVER DE OVEREENKOMST

- 1** Kunt u mij nu alvast de belangrijkste onderdelen van uw serviceovereenkomst uitleggen, zonder dat ik het pas achteraf hoeft te versturen?

Je toetst de transparantie en de bereidheid om uitleg te geven.



Groene vlag: "Natuurlijk. Ik zal de reactietijden, annuleringsvoorwaarden en de omvang van het werk benadrukken."



Rode vlag: "Je zult dat allemaal in het contract zien zodra je er klaar voor bent."

- 2** Welke clausule in uw contract ziet de meeste klanten niet, maar zou dat wel moeten doen?

Je controleert of ze hun eigen kleine lettertjes begrijpen.



Groene vlag: "Het gedeelte van het werk dat buiten het toepassingsgebied valt, daar verschuilen zich vaak onverwachte kosten."



Rode vlag: "Eigenlijk niets. Het is allemaal vrij standaard."

- 3** Als we ooit willen vertrekken, hoe gaan jullie dan om met offboarding en overdracht?

Je kijkt hoe ze uiteindelijk met hun klanten omgaan.



Groene vlag: "Wij verzorgen de documentatie, dragen de toegang over en helpen uw volgende provider om een schone exit te garanderen."



Rode vlag: "We zullen dat uitzoeken als het ter sprake komt."

HOOFDSTUK 8

*Hoe u een serviceovereenkomst leest
zonder in slaap te vallen*





WAT U KUNT VERWACHTEN

De meeste mensen ondertekenen IT-serviceovereenkomsten zonder ze daadwerkelijk te lezen.

En eerlijk gezegd? Ik kan het ze niet kwalijk nemen.

Ik heb er genoeg gelezen. Ze zijn lang, saai en staan vol met vage juridische onzin en termen als 'redelijke inspanning' of 'industriestandaard reactietijden'.

Je schrijft het in drie regels, je ogen worden glazig en voor je het weet... scroll je naar de handtekening.

Veel ondernemers doen dit, maar het is riskant.

Want als je blind tekent, leg je jezelf verantwoordelijkheden op waar je later spijt van kunt krijgen.

En dit soort contracten zijn meestal nodig als de zaken niet goed gaan.

Wanneer er iets kapot gaat of er een probleem is met uw IT-provider.

Wanneer je buitengesloten bent, een rekening krijgt voor iets waarvan je dacht dat het inbegrepen was, of vastzit aan een automatische verlenging die je niet zag aankomen.

Dan duik je de overeenkomst op en besef je dat je beter had moeten opletten.

Laten we er dus voor zorgen dat jou dit nooit overkomt.

In dit hoofdstuk leest u op welke onderdelen u moet letten, welke signalen de meeste mensen over het hoofd zien en hoe u een IT-contract kunt lezen zonder dat u een vertaler of rechtendiploma nodig hebt.

CLAUSULE #1

OMVANG VAN DE DIENSTEN



Zoeken naar:

- ➔ Een gedetailleerde lijst van diensten (bijv. helpdesk, monitoring, backup)
- ➔ Specifieke technologieën of systemen die ze beheren
- ➔ Wat valt er onder ‘onderhoud’ of ‘ondersteuning’?
- ➔ Eventuele beperkingen (bijv. geen mobiele apparaten)



Let op:

- ! Vage termen zoals ‘algemene IT-ondersteuning’ of ‘standaardonderhoud’
- ! Uitsluitingen die elders in het document verborgen zitten (bijvoorbeeld projecten, beveiligingswerkzaamheden, cloud-apps)



Vraag hen om een voorbeeld uit de praktijk te geven. "Als mijn laptop kapotgaat, wat gebeurt er dan precies volgens deze overeenkomst?"

CLAUSULE #2

SERVICE LEVEL AGREEMENTS (SLA'S)



Zoeken naar:

- ➔ Gedefinieerde respons- en oplossingstijden (bijv. responstijd van 1 uur voor problemen met hoge prioriteit)
- ➔ Prioriteitsniveaus duidelijk uitgelegd (P1 = uitval, P2 = trage e-mail, etc.)
- ➔ SLA's voor openingstijden versus buiten kantooruren



Let op:

- ! Taal van 'beste inspanning'
- ! SLA's die alleen van toepassing zijn op bepaalde diensten
- ! Geen financiële sancties bij overtreding van de SLA (ze moeten zelf in het spel betrokken worden)



**Zorg ervoor dat er een financiële boete wordt opgelegd als ze de SLA overtreden.
Bijvoorbeeld: bij overtreding van de SLA betalen ze een deel van de maandelijkse overeenkomst terug.**

CLAUSULE #3

TERMIJN EN BEËINDIGING



Zoeken naar:

- ➔ Duidelijke looptijd (bijv. 12 maanden)
- ➔ Opzegtermijn (bijv. 30 dagen)
- ➔ Exitprocedures - hoe gaan ze uit dienst?



Let op:

- ! Automatische verlengingen verborgen in de kleine lettertjes
- ! Lange lock-ins zonder optie tot vroegtijdige exit
- ! Annuleringskosten die niet duidelijk vermeld staan



Vraag om een samenvatting van het offboardingproces voordat je tekent. Als ze zich ongemakkelijk voelen, is dat een waarschuwingssignaal.

CLAUSULE #4

FACTURERING- EN BETALINGSVOORWAARDEN



Zoeken naar:

- ➔ Maandelijks vergoeding duidelijk vermeld
- ➔ Wat is inbegrepen in de maandelijks en wat wordt apart gefactureerd (bijv. projecten, werk buiten kantoor tijden, hardware)
- ➔ Betalingstermijnen, boetes voor te late betaling, toeslagen voor overschrijding



Let op:

- ! Kosten zoals 'buiten het bereik van de dienst vallende uurondersteuning' zonder definitie
- ! Taal over 'onbeperkte ondersteuning' met kleine lettertjes die het tegenspreken
- ! Vage termen zoals 'diverse kosten' of 'service-aanpassingen' zonder uitleg



Vraag om een korte tekst van één pagina die in begrijpelijke taal uiteenzet wat er in de overeenkomst staat. Als het niet schriftelijk is, ga er dan vanuit dat het er niet in staat.

CLAUSULE #5

WERK BUITEN HET BEREIK



Zoeken naar:

- ➔ Duidelijke uur-/projecttarieven voor eventuele extra's
- ➔ Voorbeelden van typische scenario's die buiten het bereik vallen
- ➔ Een proces om goedkeuring te krijgen voordat er met werk buiten de scope wordt begonnen



Let op:

- ! Prijsstelling 'nog te bepalen'
- ! Alles wat hen de bevoegdheid geeft om naar believen kosten in rekening te brengen
- ! Taal als 'indien nodig' of 'indien nodig' zonder specifieke kosten



In dit gedeelte vindt u vaak meer informatie over de werkelijke kosten dan op de pagina met prijzen.

CLAUSULE #6

AANSPRAKELIJKHEID EN VERZEKERING



Zoeken naar:

- ➔ Duidelijke taal over aansprakelijkheidslimieten
- ➔ Of hun aansprakelijkheidslimieten overeenkomen met het potentiële risico voor uw bedrijf



Let op:

- ! Clausules die 'indirecte' of 'gevolgschade' zonder verduidelijking uitsluiten

CLAUSULE #7

GEGEVENSEIGENDOM EN -TOEGANG



Zoeken naar:

- ➔ Duidelijke verklaring dat u eigenaar bent van al uw gegevens
- ➔ Recht om op verzoek gegevens op te vragen in leesbare formaten
- ➔ Beleid inzake gegevensverwijdering bij beëindiging



Let op:

- ! “De in onze systemen opgeslagen gegevens blijven ons eigendom”
- ! Elke clausule die uw toegang beperkt tijdens geschillen
- ! Er is geen tijdschema voor hoe snel ze uw gegevens na beëindiging teruggeven



Vraag hoe ze omgaan met het afscheid nemen van klanten en wat je hieraan overhoudt.

CLAUSULE #8

VERTROUWELIJKHEID EN PRIVACY



Zoeken naar:

- ➔ NDA of vertrouwelijkheidsclausule met betrekking tot uw gegevens, referenties en communicatie
- ➔ Wie heeft toegang tot wat (bijv. onderaannemers, offshorepersoneel)
- ➔ Overeenkomst om de toepasselijke privacywetgeving (bijv. AVG) te volgen



Let op:

- ! Maken in de wet waardoor ze uw gegevens kunnen delen met 'gelieerde ondernemingen'
- ! Er wordt niet gesproken over controles door onderaannemers
- ! Te brede taal zoals 'mag gegevens gebruiken om onze diensten te verbeteren'



Vraag of ze geheimhoudingsverklaringen met hun personeel hebben ondertekend. Veel hebben dat niet.

CLAUSULE #9

SCOPEWIJZIGINGEN EN PROJECTWERK



Zoeken naar:

- ➔ Een duidelijk proces voor het offreren en goedkeuren van werk dat buiten de scope valt
- ➔ Wat wordt beschouwd als dagelijkse ondersteuning versus een betaald project?
- ➔ Details over uur-/projecttarieven voor meerwerk



Let op:

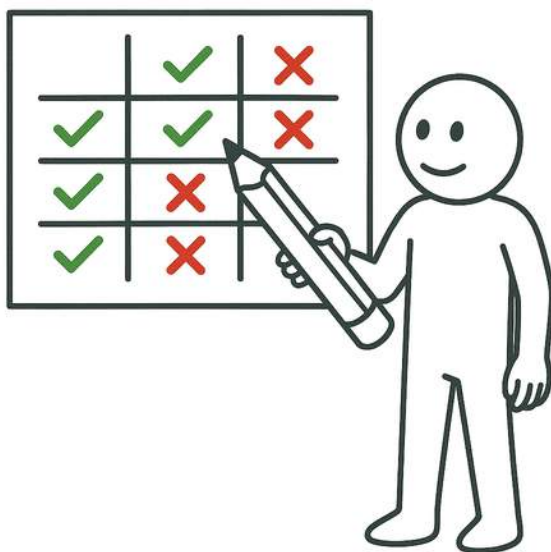
- ! “Elke taak die niet in de lijst staat, kan naar goeddunken van de provider in rekening worden gebracht.”
- ! Er zijn geen goedkeuringen nodig voordat er extra kosten in rekening worden gebracht
- ! Kleine lettertjes die van simpele verzoeken dure projecten maken



Vraag om voorbeelden van wat niet in uw plan is opgenomen.

HOOFDSTUK 9

BONUS: vergelijkingswerkblad



HULPBRON



VERGELIJKINGS WERKBLAD

Gebruik dit werkblad om maximaal drie IT-leveranciers te vergelijken voordat u een beslissing neemt.

Vink de vakjes aan waar ze aan de criteria voldoen. Hoe meer , hoe groter de kans op een soepele, veilige en gezonde samenwerking.

Criteria	Aanbieder 1	Aanbieder 2	Ons
1. Stelt slimme vragen over uw bedrijf	☐	☐	☒
2. Uitleg over diensten in begrijpelijk Nederlands	☐	☐	☒
3. Een voorbeeldovereenkomst vroegtijdig verstrekt	☐	☐	☒
4. Geef recente, relevante referenties	☐	☐	☒
5. We hebben je door een duidelijk onboardingplan geleid	☐	☐	☒
6. Voer een goede audit/ontdekking uit voordat u een offerte uitbrengt	☐	☐	☒
7. Prioriteit geven aan preventie, niet alleen repareren	☐	☐	☒
8. Duidelijk aangegeven wat inbegrepen/uitgesloten is	☐	☐	☒
9. Had een duidelijk, professioneel ondersteuningsproces	☐	☐	☒
10. Heb met je gereedschap gewerkt (of het uitgelegd)	☐	☐	☒
11. Hadden echte processen voor hun IT-ondersteuning	☐	☐	☒
12. Voelde als een partner, niet alleen als een leverancier	☐	☐	☒

NOG ÉÉN DING VOORDAT JE GAAT

Als je het tot hier hebt gered, goed gedaan.

De meeste mensen nemen nooit de tijd om goed na te denken over de keuze van een IT-leverancier. Ze tekenen het eerste contract dat goed klinkt, duimen en hopen op het beste.

Maar je hebt nu een duidelijk beeld van waar je op moet letten en wat je moet vermijden, dus je kunt hopelijk een IT-provider kiezen die aan alle juiste eisen voldoet 😊

En nu je aan het einde van het boek bent, verwacht je misschien wel een soort verkooppraatje van mij.

Logisch toch? Ik ben IT-provider, dus waarom vertel ik je niet alles over de fantastische ervaring die je met mij zou hebben?

Dat is wat de meeste IT-leveranciers zouden doen. Maar ik heb aan het begin van het boek beloofd dat ik je niets ga verkopen.

En ik ben het type persoon dat zijn beloftes nakomt. Dus in plaats van mijn verkopershoed op te zetten, zet ik mijn 'adviseurshoed' op... en bied ik je een gratis adviesgesprek aan waarin ik je help (niet verkoop) met alles wat met IT te maken heeft in je bedrijf.

Ik kan u een second opinion geven over een offerte/voorstel, uw opstelling bekijken of u duidelijkheid verschaffen over iets waar u 's nachts wakker van ligt.

Stuur mij een e-mail op:

g.bakker@radix.nl

Of bel mij op:

020 - 6 870 870

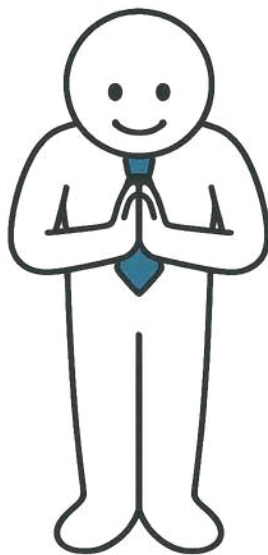
Bedankt voor het lezen!

Groeten,



Gerard Bakker
Eigenaar, Radix MKB ICT

BEDANKT!



DE MKB IT BUYERS GUIDE

Wanneer u een IT-leverancier kiest, koopt u niet alleen ondersteuning. U kiest wie toegang krijgt tot de interne werking van uw bedrijf.

En toch baseren de meeste ondernemers die beslissing op niets meer dan een onderbuikgevoel en een vaag voorstel.

Dit boek wil daar verandering in brengen.

De MKB IT Buyers Guide is geschreven door een ervaren MSP-eigenaar en biedt u de essentiële vragen, praktische inzichten en een kijkje achter de schermen die u nodig hebt om een weloverwogen, geïnformeerde beslissing te nemen over uw technologiepartner.

Binnenin ontdekt u:

- ✓ Wat onderscheidt een echte partner van een generieke leverancier?
- ✓ De verborgen kosten en rode vlaggen waar zelden over gesproken wordt
- ✓ Hoe u voorstellen, serviceovereenkomsten en onboarding-tijdslijnen kunt evalueren zonder dat u een vertaler nodig hebt

www.radix.nl



OVER GERARD BAKKER

Gerard is de oprichter van Radix MKB ICT die MKB bedrijven helpt productief en beschermd te blijven en de chaos een stap voor te blijven. Dankzij zijn jarenlange praktijk-ervaring heeft hij gezien wat er gebeurt als bedrijven hun IT op orde hebben, en wat er gebeurt als ze dat niet doen.