

Onbezorgd ondernemen zonder ICT-zorgen

Vijf herkenbare vragen over uw
ICT-werkplek én antwoorden die
u helpen met ondernemen.

Vodafone Business · MKB Business ICT



vodafone
business

Een bekend verhaal over uw ICT-werkplek

Een laptop die de update niet draait. Een medewerker die net iets te enthousiast op een link klikte. Een leverancier die plotseling vraagt of u 'wel NIS2-compliant' bent. Dit soort vragen belanden vanzelf op uw bord. Dat terwijl u ondernemer bent geworden om een bedrijf op te bouwen. En toch is dat de realiteit voor veel ondernemers in Nederland.

Dit e-book gaat over de vijf vragen die eigenlijk elke mkb-ondernemer zichzelf moet stellen. We schetsen herkenbare situaties en vullen die voor u aan met concrete inzichten, een paar handige checklists en verhelderende antwoorden.

U begon uw bedrijf niet om een ICT-helpdesk te runnen. En toch voelt dat soms wel zo.

Voor wie is dit e-book?

Dit e-book is voor ondernemers, beslissers, officemanagers, operationeel managers en interne ICT-beheerders in het mkb. Of u nu de ICT volledig zelf doet, verdeelt binnen het team of (deels) uitbesteedt aan een externe partner, herkenbare ICT-uitdagingen blijven.



Inhoudsopgave

Aan het einde van dit e-book vindt u praktische informatie over hoe MKB Business ICT u hierbij kan helpen met het creëren van een veilige werkplek, en hoe u met ons in contact kunt komen voor een vrijblijvend adviesgesprek.



Bent u ondernemer, of wordt u langzaam ICT'er?

Het probleem

Het is maandagochtend. U had vandaag drie klantgesprekken willen voeren. In plaats daarvan zit u sinds acht uur te puzzelen aan een oplossing voor een licentieprobleem. Daarna belt een collega: laptop trekt de update niet. Tussendoor controleert u met lichte paniek of de wekelijkse back-up dit keer wél is gelukt. En dit is pas het begin van de week...

Herkenbaar voor veel ondernemers en medewerkers die ICT-taken erbij doen. En vooral ook frustrerend, want ad-hoc ICT-werk kost veel tijd. Een kwartiertje hier, een uurtje daar. Aan het einde van de week bent u er te veel tijd aan kwijt. En dan komt er ergens een moment waarop u denkt: hoe ben ik hier in vredesnaam in beland?

Het inzicht

ICT-gedoe is zelden één groot probleem. Het is een optelsom van kleine onderbrekingen. En juist die optelsom is moeilijk te overzien. “Het is maar tien minuten”, zegt u tegen uzelf. Maar tien minuten, vijf keer per dag, vijf dagen per week, is ruim vier uur. Bijna een halve werkdag. Elke week weer.

51% van de Nederlandse mkb'ers noemt tijdgebrek als grootste belemmering om verder te digitaliseren.

YouGov / STRATO,
onderzoek digitalisering Nederlands mkb, 2025.



Tegelijkertijd verandert de wereld om u heen sneller dan ooit. Beveiligingseisen worden strenger. Klanten verwachten snellere reacties, betere bereikbaarheid en gegarandeerde uptime. En u wordt geacht overzicht te houden, terwijl u ook uw bedrijf wilt laten groeien.

Het meest verraderlijke is dat u ervaring opbouwt in iets waar u juist geen ervaring in wilt opbouwen. Want hoe meer wachtwoorden u reset, hoe handiger u daarin wordt. Hoe vaker u een storing probeert op te lossen, hoe groter de kans dat collega's u als eerste bellen bij de volgende. En voor u het weet bent u de aangewezen servicedesk van uw eigen bedrijf.

Waar gaat die tijd naartoe?

Onze eigen ervaring met mkb-klanten laat zien dat het tijdverlies meestal in drie categorieën zit. Als u weet welke categorie bij u de grootste tijdvreter is, weet u ook waar u het verschil kunt maken.

- **Onderhoud en beheer.** Updates installeren, licenties verlengen, nieuwe medewerkers toevoegen, oude weer verwijderen. Werk dat moet en vaak voorspelbaar van aard is, maar regelmatig terugkomt. Een paar uur per maand kan oplopen tot een paar werkdagen per jaar.
- **Storingen oplossen.** Een printer die het niet doet, een mailbox die vol zit, een collega die niet meer in de gedeelde map kan. Vaak niet eens technisch ingewikkeld, wel tijdrovend. Het lastige is dat het altijd ongepland is. U was bezig met iets belangrijks en wordt onderbroken voor iets dat acuut voelt. Niet alleen kost het u extra tijd, het snoept ook tijd van uw eigenlijke taken af.
- **Beslissen over wat u niet weet.** Welke licentie hebt u nodig? Is die nieuwe tool veilig? Mag een AI-tool gebruikt worden voor klantdata? Beslissingen die u neemt, maar waar u eigenlijk de expertise niet voor hebt. Dit werk is onzichtbaar, maar vraagt wel mentale ruimte en tijd.

De eerste categorie is voorspelbaar en kunt u inplannen. De tweede is frustrerend, maar overzichtelijk. De derde is de gevaarlijkste, want eventuele fouten kunnen pas veel later aan de oppervlakte komen. Alle drie de categorieën



hebben met elkaar gemeen dat ze tijd, aandacht en zekerheid weg nemen bij de mensen die eigenlijk met klanten, groei en operatie bezig zouden moeten zijn.

Wat we ook regelmatig terugzien: het ICT-werk komt vaak terecht bij wie er maar net tijd voor heeft. Soms is dat de ondernemer zelf, soms een officemanager, een operationeel manager of gewoon de collega die 'handig is' met computers. Zelden is het iemands echte functie, en juist daardoor onderschat men structureel hoe vaak het hele team wordt onderbroken voor ICT-vragen. Puur omdat men niet weet wie ze anders moeten bellen.

Quickscan: hoeveel uur per week bent u of is één van uw medewerkers ICT'er?

- > Hoeveel uur besteedt u per week aan wachtwoorden, accounts en toegang regelen?
- > Wanneer hebt u voor het laatst rustig kunnen werken zonder ICT-onderbreking?
- > Wat zou u doen met vier extra uur per week?
- > Wat is er de afgelopen maand niet gebeurd omdat u ICT-zaken voorrang gaf?

De antwoorden op deze vragen geven u inzicht in hoeverre het beheer van uw werkplek uw productiviteit in de weg zit. Weet dat u niet de enige bent.



De oplossing

De veilig beheerde werkplek van MKB Business ICT biedt uw organisatie een toekomstbestendige digitale basis. Wij verzorgen het volledige beheer, onderhoud en beveiliging van uw Microsoft 365-werkomgeving, zodat u altijd beschikt over moderne, up-to-date en beveiligde werkplekken.

Concreet betekent dat voor u: u en uw collega's worden niet meer onderbroken voor ICT-problemen. Iedereen kan met vragen direct terecht bij onze Nederlandstalige Service Desk.

Zo wint u weer tijd om te investeren in klanten, in groei, in het werk waarvoor u ooit dit bedrijf bent begonnen.



Hoe goed bent u écht beschermd tegen een cyberaanval?

Het probleem

Uw medewerkers zijn onderweg in de trein of thuis aan het werk. Fijn dat de wifi in dat koffietentje gratis is. Maar is de verbinding wel veilig? Hybride werken kan risico's met zich meebrengen. Voor u het weet ligt door één ogenschijnlijk onschuldige actie uw klantdata op straat. En krijgt u een bericht dat u losgeld moet betalen. Cybercriminaliteit is niet meer iets van 'andere bedrijven'. Het gebeurt structureel, ook bij het mkb. Sterker nog: juist bij het mkb.

Het pijnlijke is dat de schade vaak veel groter is dan alleen het losgeld of de hersteltijd. Verlies van klantvertrouwen. Meldingen aan de Autoriteit Persoonsgegevens. Vragen van leveranciers en afnemers die ineens twijfelen over de samenwerking. Bovendien lopen de kosten van een cyberincident snel op. En daar komt reputatieschade bij die nog jaren kan doorwerken.

1 op de 5 Nederlandse bedrijven leed in 2024 schade door een cyberaanval.

ABN AMRO, onderzoek cybersecurity onder 788 bedrijven, 2025 (cijfers uit 2024).



Het inzicht

Cyberveiligheid is geen project dat u één keer afrondt. Het is dagelijks werk. Dreigingen veranderen, software krijgt nieuwe kwetsbaarheden, criminelen worden slimmer met AI. Wat vandaag een goede beveiliging is, kan morgen achterhaald zijn.

Een belangrijke verschuiving die we de afgelopen jaren zien: aanvallen zijn niet meer alleen gericht op grote organisaties. Geautomatiseerde scans zoeken het hele internet af naar kwetsbare systemen, ongeacht de grootte van de organisatie erachter. Of u nu vijf medewerkers hebt of tweehonderdvijftig, voor zo'n scanner bent u gewoon een IP-adres met een mogelijk lek.

Als u geen zicht hebt op uw werkomgeving, bent u simpelweg te laat. Dan staat uw organisatie al met 2-0 achter tegen professionelere hackers.

Erik van Daatselaar,
Security Portfolio Lead bij Vodafone Business.

NIS2: de nieuwe Europese cybersecurityrichtlijn

NIS2 is een Europese richtlijn die EU-landen moeten omzetten in nationale wetgeving. In Nederland gebeurt dat via de Cyberbeveiligingswet. Deze wet moet de cyberweerbaarheid van essentiële en belangrijke organisaties vergroten. De Cyberbeveiligingswet is vanaf 2026 van kracht.

Voor organisaties betekent dit onder meer dat cybersecurity structureel op de agenda moet staan. Denk aan risicobeheer, beveiligingsmaatregelen, voorbereiding op incidenten en het tijdig melden van ernstige cyberincidenten. Dat vraagt om voorbereiding, want digitale aanvallen ontwikkelen zich vaak binnen enkele uren.

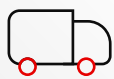


Valt uw bedrijf binnen één van de onderstaande sectoren?
Dan krijgt u te maken met de NIS2-richtlijn.

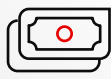
Bijlage 1



Energie



Vervoer



Bankwezen



Drinkwater



Digitale
infrastructuur



Beheer van
ICT-diensten



Ruimtevaart



Infrastructuur
financiële markt



Gezondheids-
zorg



Afvalwater



Overheid

Bijlage 2



Digitale
aanbieders



Post- en
koeriersdiensten



Afvalstoffenbeheer



Levens-
middelen



Chemische
stoffen



Onderzoek



Vervaardiging



“Onder de oude NIS-richtlijn bepaalde de overheid welke organisaties onder de wet vielen. Met de Cyberbeveiligingswet verdwijnt dat model: organisaties moeten voortaan zelf controleren of zij eronder vallen en zelf passende maatregelen nemen. Wie dat uitstelt, loopt niet alleen juridisch risico, maar ook reputatierisico richting de keten.”

Koos Freriks,
Product Manager Cyber Security VodafoneZiggo

Met NIS2 verschuift cybersecurity van een puur ICT-onderwerp naar een duidelijke bestuurlijke verantwoordelijkheid. Directies worden niet alleen beoordeeld op het beleid dat op papier staat, maar ook op de cyberweerbaarheid van hun organisatie.

Daarbij speelt ketenverantwoordelijkheid een belangrijke rol. Organisaties die onder NIS2 vallen, moeten niet alleen hun eigen beveiliging op orde hebben, maar ook kunnen aantonen dat leveranciers en andere partijen in hun keten geen onnodig risico vormen. Daardoor krijgen ook bedrijven die zelf niet direct onder NIS2 vallen met deze eisen te maken. Dit raakt dus ook kleinere bedrijven die leveren aan organisaties waarvoor NIS2 geldt. Voor een mkb-bedrijf kan nalatigheid grote gevolgen hebben: van verlies van opdrachten tot financiële schade en, in ernstige gevallen, hoge boetes.

Waar zitten de grootste gaten?

In de praktijk zien we vier zwakke plekken die bij vrijwel elk mkb-bedrijf terugkomen.

- **De menselijke kant.** Technologie kan veel risico's afvangen, maar phishing werkt omdat mensen niet altijd alert kunnen zijn. Effectieve beveiliging begint bij bewustwording: begrijpen wat de impact is van gedrag, zoals het delen van inloggegevens of vertrouwen op externe verzoeken. Idealiter met phishing-herkenning en simulaties.
- **Verouderde systemen en gemiste beveiligingsupdates.** Veel aanvallen maken misbruik van bekende kwetsbaarheden waarvoor al lang een oplossing beschikbaar is. Het probleem is dus niet dat die oplossing ontbreekt, maar dat updates niet op tijd worden geïnstalleerd. Eén laptop of server die niet goed is bijgewerkt, kan al genoeg zijn om binnen te komen. Automatisch updatebeheer is daarom cruciaal.
- **Onvoldoende inzicht in de ICT-omgeving.** U kunt niet beveiligen wat u niet ziet. Veel bedrijven hebben geen volledig overzicht van alle systemen en accounts, er is geen monitoring op afwijkend gedrag, en medewerkers installeren zelf software op een zakelijke pc (shadow IT). Toegangsbeheer valt hier ook onder. Denk aan een ex-medewerker die nog bij de gedeelde mappen kan. Ter illustratie: hackers zitten gemiddeld 200+ dagen onopgemerkt in een netwerk voordat ze toeslaan.
- **Zwakke ketenbeveiliging.** Bedrijven vertrouwen op ICT-leveranciers, SaaS-tools, hostingpartijen en externe consultants. Die partijen zijn vaak de zwakke schakel: een kwetsbaarheid bij één leverancier raakt al snel iedereen die ervan afhankelijk is. Daarom is het zo belangrijk om te weten met wie u verbonden bent, en om software altijd up-to-date te houden.



Cybersecuritycheck: vier basismaatregelen

- Sterke toegangsbeveiliging: gebruik unieke wachtwoorden, een wachtwoordmanager en verplicht MFA voor alle accounts. Controleer regelmatig of oude accounts (ex-medewerkers, stagiairs, leveranciers) nog actief zijn.
- Er is een actueel overzicht van wie toegang heeft tot welke systemen en data. Daarnaast worden van kritische data automatisch back-ups gemaakt. Niet alleen om gegevens veilig te stellen, maar ook om zeker te weten dat ze na een calamiteit daadwerkelijk hersteld kunnen worden.
- Updates worden automatisch en op tijd geïnstalleerd op alle apparaten.
- Medewerkers hebben in de afgelopen 12 maanden een security-awareness training gehad.

Kunt u niet bij alle vier volmondig 'ja' zeggen, dan hebt u werk aan de winkel. Dat is geen schande: bij heel veel mkb-bedrijven zijn deze punten structureel onderbelicht.

De oplossing

Met MKB Business ICT wordt uw werkplek 24/7 bewaakt vanuit een Nederlandse beveiligingscentrale, een zogenaamde SOC (Security Operations Center). Het monitoren, detecteren en reageren op dreigingen draait volledig op de achtergrond. Als er iets verdachts gebeurt, zien wij het als eerste en grijpen we in voordat u er last van hebt.

Met Security Premium en Security Elite bieden we ondernemers uitgebreidere beveiligingsmaatregelen die kunnen helpen bij het voldoen aan de NIS2-richtlijn. Bij Vodafone Business werken we met hetzelfde expertiseniveau als waar multinationals op draaien, vertaald naar wat past bij een mkb-bedrijf.



Is uw werkplek beschermd tegen Al-gedreven cybercrime?

Het probleem

Teksten schrijven, meetings samenvatten, documenten vertalen, informatie analyseren: dankzij AI gaat het allemaal sneller dan ooit. Maar als u en uw medewerkers zoveel kunnen met AI, wat kunnen cybercriminelen er dan wel niet mee? AI maakt phishing overtuigender en social engineering slimmer. Maar het maakt ook geautomatiseerde aanvallen sneller en effectiever. Denk aan slimme bots die 24/7 zoeken naar kwetsbaarheden in software of netwerken, malware die zichzelf automatisch verandert om detectie te ontwijken en snelle brute-force pogingen die hun aanpak continu bijstellen. AI maakt het werk van cybercriminelen makkelijker, schaalbaarder en gevaarlijker. Met alle gevolgen van dien.

Het inzicht: AI maakt aanvallen slimmer en uw team kwetsbaarder

Waar phishing vroeger vaak nog te herkennen was aan kromme zinnen, vreemde afzenders of slordige logo's, worden aanvallen nu steeds overtuigender. Met AI kunnen criminelen in korte tijd persoonlijke berichten maken, schrijfstijlen nabootsen, bestaande informatie uit netwerken gebruiken en zelfs stemmen of gezichten klonen.

A man with dark hair and a beard, wearing a blue button-down shirt, is shown in profile, looking at a tablet computer. He is standing in a server room with rows of server racks in the background, illuminated by blue and orange lights.

8 op de 10 securityprofessionals in de Benelux kreeg het afgelopen jaar te maken met AI-gedreven cyberaanvallen.

SoSafe, Cybercrime Trends 2025.

Daardoor wordt een aanval moeilijker te herkennen. Een medewerker krijgt geen algemene nepmail meer, maar een bericht dat lijkt te komen van een collega, leverancier of leidinggevende. Met de juiste toon, de juiste context en precies genoeg urgentie om snel te klikken, te betalen of gegevens te delen.

En dat is precies het risico: AI maakt cybercrime schaalbaar. Wat vroeger veel tijd, taalgevoel en voorbereiding kostte, kan nu sneller, goedkoper en op grotere schaal. Cybercriminelen hoeven geen perfecte hackers meer te zijn om overtuigende aanvallen te maken. AI helpt ze daarbij.

Drie actuele risico's van AI-crime

- **Phishing wordt nog geloofwaardiger.** Cybercriminelen kunnen met AI-berichten maken die veel minder op standaard phishing lijken. Ze gebruiken informatie over uw organisatie, uw medewerkers of uw leveranciers om een bericht geloofwaardig te maken.
- **Deepfakes en stemklonen maken fraude overtuigender.** Een betaalverzoek of urgente opdracht lijkt niet alleen van de directeur of medewerker te komen, maar kan ook zo klinken. Met AI kunnen stemmen, gezichten en stijlen worden nagebootst. Dat maakt het lastiger voor medewerkers om te vertrouwen op wat ze zien of horen.
- **Aanvallen worden sneller en schaalbaarder.** AI helpt criminelen om in korte tijd veel varianten van een aanval te maken. Niet één algemene phishingmail, maar tientallen versies voor verschillende functies, afdelingen of situaties. Daardoor neemt de kans toe dat iemand tóch klikt.



De oplossing

Met MKB Business ICT werkt u binnen één veilig beheerde Microsoft 365-werkomgeving die continu wordt onderhouden, gemonitord en beveiligd. Zo bent u beter beschermd tegen de nieuwste AI-gedreven cyberdreigingen, van geloofwaardige phishingmails tot verdachte inlogpogingen en aanvallen die steeds slimmer worden.

Updates, toegangsrechten, back-ups, monitoring en beveiliging worden centraal geregeld. Uw medewerkers kunnen veilig blijven werken. En twijfelt iemand aan een bericht, link of verzoek? Dan staat de Nederlandstalige Service Desk klaar om direct mee te kijken.



Kunt u zonder eigen ICT-afdeling toch veilig ondernemen?

Het probleem

Een fulltime ICT'er aannemen kost al snel 70.000 tot 90.000 euro per jaar, exclusief tools, opleidingen en vervanging tijdens vakanties. Voor de meeste mkb-bedrijven is dat geen realistische optie. Want één persoon kan onmogelijk alle vakgebieden afdekken: helpdesk, security, netwerk, cloud, compliance, beleid, inkoop. Dat zijn zeven specialismes in één FTE. Die combinatie bestaat in de praktijk niet.

Dus belandt het weer op het bord van de eigenaar, een medewerker, of een ICT-partner. En soms worden er zelfs freelancers ingehuurd. Dat leidt tot een gefragmenteerde ICT-werkplek, waarbij niemand het totaalplaatje overziet. Niet bij storingen, niet bij security, niet bij belangrijke beslissingen. En precies daar gaat het mis: niet omdat er onkundige mensen aan het werk zijn, maar omdat niemand verantwoordelijk is voor het grote geheel.



42% van het Nederlandse mkb noemt IT-beveiliging een hoge prioriteit. De meeste van die bedrijven hebben geen eigen ICT-afdeling om dat uit te voeren.

Cisco Cybersecurity Readiness Index, 2025.

Het inzicht

Een eigen ICT-afdeling of helpdesk is niet het doel. Een werkende, veilige, schaalbare werkplek is het doel. Dat zijn twee heel verschillende dingen. Het ene is een organisatievorm, het andere is een uitkomst. En een goede uitkomst kunt u op meerdere manieren bereiken, niet alleen door zelf alles in huis te halen.

De vraag is dus niet: 'hoe richt ik een ICT-afdeling in?' De vraag is: 'hoe krijg ik het serviceniveau van een ICT-afdeling, met beheerbare, voorspelbare kosten en geen gedoe?'

Wat doet een ICT-afdeling eigenlijk?

Als u goed kijkt naar het werk van een ICT-afdeling, valt het uiteen in vier functies. Door dat onderscheid te maken, kunt u per functie kijken wat u zelf wilt doen, wat u wilt uitbesteden en wat u gewoon goed wilt regelen zonder dat het tijd kost.

- **Service Desk.** De eerste lijn. Wachtwoorden resetten, accounts aanmaken, eenvoudige vragen beantwoorden. Niet ingewikkeld, wel constant nodig. Dit werk valt goed uit te besteden, mits het snel en in het Nederlands kan.
- **Applicatiebeheer.** Het beheer van bedrijfssoftware zoals ERP-, CRM- en HR-systemen. Denk aan gebruikersbeheer, kleine configuraties, koppelingen met andere systemen en contact met softwareleveranciers.
- **Beheer en onderhoud.** Updates, monitoring, back-ups. Het werk dat in goede tijden onzichtbaar is en in slechte tijden het verschil maakt. Hier loont automatisering enorm. Wat handmatig drie uur per week kost, kan met de juiste tooling vrijwel onzichtbaar op de achtergrond draaien.
- **Security.** Dreigingen monitoren, incidenten afhandelen, compliance bewaken. Specialistisch werk dat 24/7 doorgaat. Dit is bij uitstek werk waar u een gespecialiseerd team voor wilt, omdat de combinatie van diepe kennis en continue beschikbaarheid niet te realiseren is met één of twee interne mensen.

De truc is om elk van deze functies op te lossen, zonder ze allemaal zelf te hoeven invullen. Service Desk, applicatiebeheer en onderhoud kunnen volledig



uit handen worden genomen. Security hoort bij een specialist. Strategie en advies horen op directieniveau.

Wat we zien bij klanten die het op deze manier inrichten: er ontstaat rust in het bedrijf. Niet omdat er geen ICT-vragen meer zijn, maar omdat er iemand is die ze opvangt voordat ze bij u belanden.

De oplossing

MKB Business ICT is uw ICT-afdeling voor de Microsoft 365-werkomgeving. Eén Nederlandstalig aanspreekpunt voor alle vragen, van een vergeten wachtwoord tot het onboarden van een nieuwe collega. Onze Service Desk lost problemen direct en persoonlijk op. Geen tickets meer die drie dagen blijven liggen.

Daarachter zitten het beheer, de beveiliging en de support. Niet één persoon die overal een beetje van weet, maar een team dat samenwerkt voor uw werkplek. U betaalt een vast bedrag per gebruiker per maand: voorspelbare kosten, geen losse facturen, geen wirwar van leveranciers.

Geen eigen ICT-afdeling. Wel het serviceniveau ervan.



Werkt alles nog gewoon door als u er even niet bent?

Het probleem

Een vakantie van twee weken, een dag ziek op bed, of gewoon een avond en weekend zonder dat iemand meekijkt. Op zich niets bijzonders, behalve dat uw bedrijf 24 uur per dag, 7 dagen per week digitaal bereikbaar en kwetsbaar is. Aanvallers en hun bots houden geen kantoortijden aan. Juist buiten werktijd, als er niemand oplet, slaan ze toe en proberen ze met geautomatiseerde tools kwetsbaarheden te vinden en binnen te dringen.

Daar komt bij dat veel mkb-bedrijven leunen op één persoon die net wat meer van de ICT weet. Soms is dat de ondernemer, soms een collega, soms een ICT-partner. Het werkt, totdat het niet meer werkt. En dat moment kondigt zich zelden aan. Het komt op de slechtst denkbare dag, op het slechtst denkbare moment. Vaak juist als die ene persoon er even niet is.

U merkt het aan ondernemers die niet meer op vakantie gaan zonder hun laptop. Of die hun telefoon mee naar het zwembad nemen omdat 'er altijd wel iets kan zijn'. Maar het draait niet om die ene vakantie. Het draait om de vraag of uw werkplek ook veilig en beschikbaar blijft op de momenten dat u er niet bovenop zit.

Het inzicht

Continuïteit is geen luxe. Het is een vorm van risicomanagement die u nog steeds zelf in de hand hebt, mits u het op tijd inricht. Een bedrijf dat afhankelijk is van één persoon, is een bedrijf dat moeilijk groeit en moeilijk over te dragen is.



Vier scenario's die u niet wilt meemaken

- **Scenario 1: de storing buiten werktijd.** Op een zaterdagavond faalt een server. Het herstellen van kritische data kost veel tijd. Als het al lukt. Maandagochtend kunnen tien medewerkers niet werken en blijven klanten onbeantwoord. Wat een klein incident had kunnen zijn, kost nu dagen om te herstellen.
- **Scenario 2: de vertrekkende collega.** De collega die een deel van uw ICT-taken op zich nam, kondigt aan te vertrekken. Na de laatste werkdag blijkt hoeveel er aan die ene persoon hing: toegang via een persoonlijk account, belangrijke contracten op eigen naam. Zonder goede overdracht kan dat funest zijn voor uw bedrijf.
- **Scenario 3: de groeispurong.** U neemt in één keer vijf nieuwe mensen aan, want het loopt goed. Drie weken later werken er nog twee echt productief. De rest wacht nog op accounts, software en een werkende laptop. Dat is omzet die u laat liggen en het is demotiverend voor mensen die graag aan de slag willen.
- **Scenario 4: de aanval buiten werktijd.** 's Nachts of in het weekend proberen criminelen hun slag te slaan. Bijvoorbeeld met een phishingmail waarop een collega per ongeluk al eerder heeft geklikt, of een bot die een kwetsbaarheid misbruikt. Omdat er niemand direct reageert, heeft de aanvaller extra tijd om schade aan te richten, denk aan versleutelde bestanden, gestolen data of uitgevallen systemen. Zonder snelle detectie en reactie kan de impact groot zijn.

Geen van deze scenario's is onrealistisch. Het verschil zit niet in óf zoiets uw bedrijf kan overkomen, maar in óf u er klaar voor bent als het gebeurt.

Is uw bedrijf 24/7 hack-proof?

Loop deze punten eens langs. Ze zijn geordend rond de vier dingen die ervoor zorgen dat uw werkplek doordraait, ook als u er niet bent.

- **Continuïteit & beschikbaarheid:** uw ICT-werkplek blijft draaien, ook als u of een sleutelpersoon er niet is.



- **Veiligheid & compliance:** alle werkplekken zijn beschermd en up-to-date en toegang is veilig en centraal geregeld.
- **Werkplekbeheer & productiviteit:** medewerkers kunnen overal veilig werken en een nieuwe collega is snel aan het werk, ook tijdens uw afwezigheid.
- **Support & ontzorging:** er is altijd vervangende support beschikbaar, ook in vakantieperiodes.

Kunt u niet overal gerust 'ja' op zeggen? Dan is uw bedrijf afhankelijker van één persoon dan goed voor u is. Gelukkig zijn al deze punten oplosbaar, mits u de juiste maatregelen neemt.

Zorg daarnaast voor een eenvoudig draaiboek voor als het misgaat. Wie belt u, in welke volgorde, en waar staat wat? Op het moment zelf kunt u vaak niet meer helder nadenken.

De oplossing

Met MKB Business ICT is uw werkomgeving niet langer afhankelijk van één persoon binnen uw bedrijf. U hebt één Nederlandstalig aanspreekpunt dat ICT-vragen direct oppakt, of u nu beschikbaar bent of niet. Updates, monitoring en back-ups lopen automatisch door. Ook 's avonds, in het weekend en tijdens uw vakantie.

Het resultaat is vooral rust. U hoeft niet meer de aangewezen probleemoplosser te zijn en kunt erop vertrouwen dat uw werkplek doordraait. Zo houdt u uw tijd en aandacht voor waar u als ondernemer het liefst mee bezig bent: ondernemen.

Wij regelen uw veilige beheerde Microsoft 365-werkomgeving, zodat u kunt blijven ondernemen met een gerust hart, ook als u er even niet bent.



Proactief zijn is het halve werk

Als u de hoofdstukken in dit e-book naast elkaar legt, valt op dat het bij elke vraag eigenlijk om hetzelfde gaat: het verschil tussen reactief en proactief omgaan met uw ICT-werkplek.

Reactief is het brandjes blussen. Proactief betekent dat de basis op orde is, dat er overzicht is over wat er gebeurt en dat problemen meestal worden opgelost voordat ze bij u belanden. Het betekent ook dat u tijd hebt om vooruit te kijken in plaats van dat u achter de feiten aanloopt.

Misschien herkende u zich in meerdere hoofdstukken. Misschien in twee. Dat is al genoeg reden om iets te veranderen. U hoeft niet meteen alles om te gooien. Begin met een gesprek over uw huidige situatie, en kijk of wat wij doen past bij wat u nodig hebt.

- **Plan een vrijblijvend adviesgesprek.** We kijken samen naar uw situatie en geven eerlijk advies, ook als de uitkomst is dat u nog niet zover bent. Geen verkooppraatje, wel een gesprek waarin we doorvragen, meedenken en concrete suggesties geven.
- **Bekijk welk pakket bij uw organisatie past.** U kiest uit drie pakketten, elk met een ander niveau van beheer, ondersteuning en beveiliging. Zo kiest u de oplossing die past bij uw organisatie, uw risico's en uw ambities.
- **Lees verder.** Op vodafone.nl/zakelijk/mkb/business-ict vindt u meer informatie over MKB Business ICT, de pakketten, veiligheid en compliance.



Van uw ICT-zorgen af met de veilige werkplek MKB Business ICT van Vodafone Business

MKB Business ICT is een beheerde en beveiligde Microsoft 365-werkomgeving voor Nederlandse mkb-bedrijven. We nemen het beheer uit handen, beveiligen uw omgeving vanuit een Nederlandse beveiligingscentrale en zorgen dat uw medewerkers soepel kunnen werken: op kantoor, thuis, onderweg en bij de klant.

Wat dat voor u betekent:

- Wij beheren en beveiligen uw Microsoft 365-werkomgeving, zodat u tijd overhoudt voor uw bedrijf.
- Eén vast Nederlandstalige contactpersoon die uw vragen en problemen snel oplost.
- Uw werkomgeving wordt continu beveiligd vanuit een Nederlandse beveiligingscentrale.
- Alles voor één vast maandbedrag, zonder verrassingen.
- Snel starten zonder gedoe: wij regelen de volledige onboarding.

U kiest uit drie pakketten, vanaf €20 per gebruiker per maand. Microsoft 365-licenties zijn niet inbegrepen, maar kunt u wel via Vodafone Business aanschaffen. Zo houdt u één aanspreekpunt voor alles wat met uw veilige beheerde werkplek te maken heeft.

Plan een afspraak

Ga naar **vodafone.nl/zakelijk/mkb/business-ict**

Of bel ons op: 085 - 1106950 (werkdagen van 09:00 tot 17:00)

Vodafone Business





vodafone
business