IT voor Impact

WHITEPAPER · SCHIJNZEKERHEID

Het is geregeld. Maar weet je het ook?

Waarom vertrouwen in je IT'er nog geen zekerheid is, wat onderzoek daarover laat zien en vijf vragen waarmee je het verschil zelf zichtbaar maakt.

Voor directies in het mkb

November 2026

IN HET KORT

Het mkb heeft niet alleen een cybersecurityprobleem. Mogelijk ook een zekerheidsprobleem.

Je vertrouwt op degene die je IT beheert. Dat is gezond en nodig. Het wordt een risico als dat vertrouwen de plaats inneemt van controle, bewuste keuzes over restrisico's en voorbereiding op de dag dat het misgaat.

1. **Over vertrouwen zijn IT-dienstverleners en IT-afnemers het eens. Over bewijs niet.**
   62% tegenover 59% zegt te werken op basis van vertrouwen. Bij het regelmatig testen van een gezamenlijk draaiboek is dat 69% tegenover 43%.
2. **Vertrouwen is een reden om niet voor te bereiden.**
   39% van de IT-afnemers bereidt zich weinig of niet voor op een cyberincident. De reden die ze noemen: ze vertrouwen hun IT-dienstverlener.
3. **"Back-up functioneert goed" is geen bewijs.**
   In een recente rechtszaak meldde een kwartaalrapportage dat back-up en herstel goed werkten. Een server zat al twee jaar niet in de back-up.

INHOUD

1 · Het zekerheidsprobleem 3
2 · Wat het onderzoek laat zien 4
3 · Wat je hoort en wat je zou moeten weten 5
4 · Wie betaalt voor het gat? 6
5 · Vier soorten zekerheid 7
6 · De directiecheck: weet je het, of vertrouw je erop? 8
7 · Van vertrouwen naar aantoonbare zekerheid 9
Bronnen 10

Ik maak onderscheid tussen wat onderzoek vaststelt en wat ik daaruit afleid. Afleidingen staan als zodanig benoemd. Cijfers komen uit de bronnen op pagina 10.

Vertrouwen is goed. Het wordt een risico als het controle vervangt.

Je besteedt IT uit omdat je de tijd of de kennis mist. Diezelfde ontbrekende kennis maakt het lastig om achteraf te beoordelen of het goed geregeld is.

Drie aannames die voor de hand liggen

1. Mijn IT'er is deskundig, **dus zijn alle relevante cyberrisico's onder controle.**
2. Onze IT werkt elke dag goed, **dus we kunnen ook een ernstig incident doorstaan.**
3. IT is uitbesteed, **dus voorbereiding en besluitvorming tijdens een incident zijn ook geregeld.**

Geen van deze drie is vanzelf waar. De leverancier weet meer over wat hij levert dan de afnemer. Dat heet **informatieasymmetrie**. Een geruststellend antwoord voelt dan als voldoende, omdat je het niet kunt wegen.

Hoe schijnzekerheid ontstaat

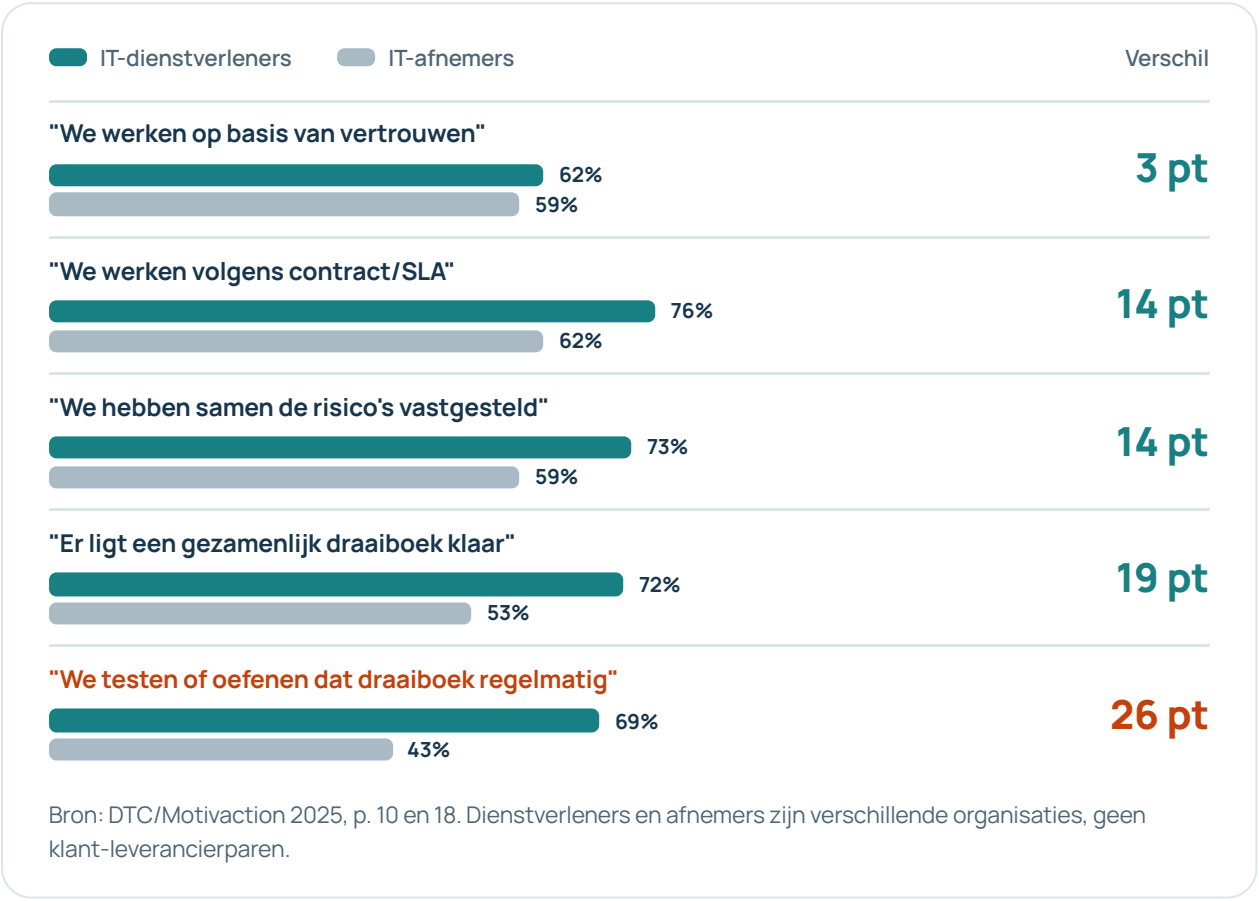


Dit is een model, gebaseerd op de onderzoeken in deze whitepaper. De keten als geheel is niet empirisch bewezen.

Je IT'er doet het werk. Jij bepaalt wat voorgaat, welk risico je neemt en of het ook echt gebeurt.

Hoe concreter de afspraak, hoe verder de antwoorden uit elkaar liggen.

Het Digital Trust Center liet in 2025 onderzoeken hoe IT-afnemers en IT-dienstverleners naar hun samenwerking kijken (Motivaction, 420 afnemers en 278 dienstverleners). Beide groepen kregen dezelfde stellingen.



Bron: DTC/Motivaction 2025, p. 10 en 18. Dienstverleners en afnemers zijn verschillende organisaties, geen klant-leverancierparen.

AFLEIDING Over vertrouwen zijn beide partijen het eens. Waar het om controleerbare afspraken gaat, lopen de beelden steeds verder uiteen. Het grootste verschil zit bij het testen. Iedereen vertrouwt elkaar. Maar wat er echt getest is, daarover denken ze heel verschillend.

GEOEFEND ÉN GEËVALUEERD

15% en 16%

van de dienstverleners en afnemers zegt dat het crisisplan geoefend en geëvalueerd is. Dat is veel lager dan de 69% die "regelmatig testen of oefenen" zegt.

VERTROUWEN ALS REDEN

39%

van de IT-afnemers noemt vertrouwen in de diensten van de IT-dienstverlener als reden voor een matige of geen voorbereiding. Bij dienstverleners is dat 20%.

Kanttekening bij het DTC-onderzoek. Het onderzoek splitst niet uit naar bedrijfsgrootte. Het gaat dus om Nederlandse IT-afnemers, niet specifiek om het mkb. Het is een panelonderzoek met zelfrapportage, en het beoogde aantal respondenten is niet gehaald.

Andere signalen wijzen dezelfde kant op

- **Weinig plannen, weinig oefening.** 26% van de mkb-bedrijven heeft een formeel incidentplan en 43% heeft nog nooit een cyberaanval geoefend (ABN AMRO/MWM2, 777 organisaties, 2026).
- **Wie uitbesteedt, test minder vaak zelf.** Zzp'ers zonder IT-dienstverlener testen vaker of hun back-up werkt dan zzp'ers met een dienstverlener: 57% tegenover 26% (DTC Benchmark, 2023). Dat is een samenhang, geen bewezen oorzaak. Misschien test de IT'er wel, zonder dat de klant het weet. Maar dan weet de klant het dus niet.

3 · WAT JE HOORT EN WAT JE ZOU MOETEN WETEN

Een goed antwoord is nog geen bewijs.

Je vraagt je IT'er of er een goede back-up is. Het antwoord: "Ja, we maken elke nacht automatisch back-ups." Dit antwoord hoor ik bijna altijd. Voor jou lijkt de vraag beantwoord. Wat er werkelijk vastgesteld moet worden, is iets anders.

Wat je hoort	Wat vastgesteld moet worden
"Er is een back-up."	Is die beschermd tegen ransomware en is herstel getest? Hoe lang duurt het voordat je primaire proces weer draait?
"We hebben antivirus."	Is er actieve detectie, monitoring en opvolging van incidenten?
"Alles staat veilig in de cloud."	Hoe zijn accounts, toegangsrechten en data beschermd? En wat als die dienst uitvalt?
"We installeren alle updates."	Geldt dat voor alle systemen, en worden uitzonderingen bewaakt?
"Wij lossen problemen direct op."	Is er 24/7-capaciteit, een escalatieplan en een vastgelegde responstijd?
"We hebben alles onder controle."	Welke risico's zijn beoordeeld, welke zijn geaccepteerd en hoe is de werking getest?

Meestal doet je IT'er niets verkeerd.

Het gat tussen directie en IT ontstaat aan beide kanten. De IT'er zit zelf ook in een lastige positie.

Een fictief, maar herkenbaar voorbeeld

Een directeur wil de IT-kosten beheersen. De IT-partner adviseert betere beveiliging, meer monitoring en een gescheiden back-upomgeving. De directeur vraagt of dat echt nodig is en stelt de investering uit. Zes maanden later volgt een ransomware-aanval.

De directeur dacht dat de IT'er de veiligheid bewaakte. De IT'er dacht dat de directeur het risico bewust accepteerde. Niemand handelde onzorgvuldig. Er was alleen geen gedeeld, schriftelijk vastgelegd beeld van het restrisico.

Wat de rechter zegt

FEIT **Gerechtshof Amsterdam, 3 februari 2026.** Een IT-bedrijf beheerde sinds 2017 de systemen van een klant, met cloudback-up. In 2022 verhuisde het ERP-systeem naar een nieuwe server, die niet in de back-upautomatisering kwam. In juli 2024 meldde een kwartaalrapportage dat back-up en herstel goed werkten. In oktober 2024 crashten de servers: de data sinds juli 2022 was definitief weg.

Het hof wees de vorderingen van de klant af. Uit het contract volgde niet zonder meer een back-upplicht voor alle servers, en de aansprakelijkheidsbeperking in de algemene voorwaarden hield stand. De klant moest een eerder toegekend voorschot van ruim € 509.000 terugbetalen. Dit was een kort geding; de schade zelf is niet beoordeeld.

FEIT **Rechtbank Amsterdam, 2018.** Hier was een IT-bedrijf wél aansprakelijk. Er waren geen schriftelijke afspraken, en volgens het IT-bedrijf vond de klant een firewall te duur en een externe back-up te veel gedoe. De rechter vond dat het IT-bedrijf had moeten weigeren of indringend had moeten waarschuwen. De schade werd verdeeld: twee derde voor het IT-bedrijf, een derde voor de klant.

Wat dit betekent. Een rapport dat zegt dat het goed gaat, bewijst niet dat het goed gaat. En als het misgaat, ligt de schade niet automatisch bij je IT-partner. Wat je niet hebt laten vastleggen, draag je mogelijk zelf.

5 · VIER SOORTEN ZEKERHEID

"Het werkt" is één soort zekerheid. Er zijn er vier.

Ondernemers halen ze makkelijk door elkaar. Alleen de eerste zie je vanzelf. De andere drie vragen om bewijs.

1 · OPERATIONEEL

Mijn IT werkt normaal.

Computers, software en netwerk doen het. Dit zie je elke dag.

2 · TECHNISCHE BEVEILIGING

De beveiliging werkt.

Er zijn passende maatregelen en ze werken echt. Dat moet iemand technisch kunnen laten zien.

3 · HERSTEL

We komen terug na een aanval.

Kritieke processen zijn op tijd hersteld. Dat weet je pas na een hersteltest.

4 · BESTUURLIJK

De directie weet wat ze accepteert.

De belangrijkste restrisico's zijn bekend en er zijn besluiten over genomen. Daarvoor moet je risico's en afspraken op papier zetten.

Dat alles het elke dag doet, zegt niets over de dag dat het stilvalt

Operationele zekerheid voelt als de andere drie, omdat er nooit iets misgaat. Maar zolang er niets misgaat, wordt herstel ook nooit op de proef gesteld. Die zekerheid ontstaat pas door te testen en te oefenen.

Weet je het, of vertrouw je erop?

Beantwoord deze vijf vragen zelf, zonder eerst je IT'er te raadplegen. Kruis per vraag één antwoord aan.

1 **Weet je hoeveel dagen je bedrijf maximaal kan stilliggen zonder ernstige financiële gevolgen?**

- ☐ Ja, en ik kan het onderbouwen
- ☐ Ik ga ervan uit dat mijn IT'er dit weet
- ☐ Nee, dat weet ik niet

2 **Weet je wanneer voor het laatst is getest of je gegevens én systemen volledig hersteld kunnen worden?**

- ☐ Ja, en ik kan het onderbouwen
- ☐ Ik ga ervan uit dat mijn IT'er dit geregeld heeft
- ☐ Nee

3 **Weet je welke drie cyberrisico's nu het grootste gevaar vormen voor je onderneming?**

- ☐ Ja, en ik kan het onderbouwen
- ☐ Ik ga ervan uit dat mijn IT'er dit weet
- ☐ Nee

4 **Is schriftelijk vastgelegd wat je IT'er doet, wat jij doet en wie de leiding neemt bij een ernstig incident?**

- ☐ Ja, en ik kan het laten zien
- ☐ Ik ga ervan uit dat dit geregeld is
- ☐ Nee

5 **Heeft een onafhankelijke deskundige in de afgelopen twaalf maanden gecontroleerd of de belangrijkste beveiligingsmaatregelen werken?**

- ☐ Ja, en ik kan het onderbouwen
- ☐ Ik ga ervan uit dat het goed zit
- ☐ Nee

Kruiste je ergens het middelste vakje aan? Dan staat daar vertrouwen op de plek van bewijs. Dat hoeft niet te betekenen dat het slecht geregeld is. Het betekent wel dat je het niet weet.

Deze check geeft een indicatie van je bestuurlijke inzicht. Het is geen gevalideerde test en zegt niets over de technische veiligheid van je IT.

Je hoeft geen securityspecialist te worden.

Je moet wel de juiste vragen kunnen stellen en het antwoord laten toetsen. Dit is het verschil dat je zoekt:

Nu	Straks
"Mijn IT'er zegt dat het veilig is."	Ik weet welke risico's we lopen en hoe die worden beheerst.
"Er worden back-ups gemaakt."	Ik heb bewijs dat onze kritieke systemen herstelbaar zijn.
"Onze IT'er lost incidenten op."	We hebben samen vastgesteld wie wat doet tijdens een incident.
"We hebben goede beveiligingssoftware."	We laten periodiek controleren of onze beveiliging werkt.
"IT is de verantwoordelijkheid van onze IT-partner."	Jij bepaalt de koers en houdt zicht op wat je IT'er doet.

Drie stappen die je zelf zet

1. **Ga het gesprek aan en leg het vast.**
   Bespreek met je IT-partner wat de dienstverlening omvat, wie waarvoor verantwoordelijk is en welke restrisico's je accepteert. Het Digital Trust Center heeft hiervoor een praatplaat en een checklist.

2. **Leg in beleid vast wie wat doet bij een calamiteit.**
   Wie neemt de leiding, wie belt wie, en welke besluiten neemt de directie? Een IT-calamiteitenbeleid maakt dat zwart op wit.

3. **Oefen.**
   Of je na een hack weer op gang komt, weet je pas als je het hebt geoefend. In een cyberoefening als Plan je Hack doorloop je met je team en je IT'er een hack, zonder de schade van een echte.

BRONNEN

Waar deze whitepaper op steunt

1. **Digital Trust Center / Motivaction (2025).** Cybersecurity verwachtingen onder IT-afnemers en IT-dienstverleners. Veldwerk februari–maart 2025, n = 420 afnemers en 278 dienstverleners. Gebruikt: p. 10, 15, 16 en 18. digitaltrustcenter.nl/sites/default/files/2025-06/Cybersecurity_verwachtingen_DTC.pdf
2. **Digital Trust Center (17 juni 2025).** IT-dienstverleners en IT-afnemers delen verantwoordelijkheidsgevoel voor digitale veiligheid. digitaltrustcenter.nl/onderzoek-ITdienstverleners
3. **Dutch IT Channel (23 juni 2026)** over ABN AMRO/MWM2 Cybertrends 2026, 777 organisaties. dutchitchannel.nl/research/754015/mkb-onderschat-digitale-gevaren
4. **Securitymanagement.nl** over het DTC Benchmark-onderzoek (MarketResponse, maart 2023) onder 766 zzp'ers en mkb'ers tot 25 medewerkers. Secundaire bron. securitymanagement.nl/weerbaarheid-tegen-cybercriminelen-bij-kleine-bedrijven-onvoldoende
5. **Gerechtshof Amsterdam, 3 februari 2026,** ECLI:NL:GHAMS:2026:275 (kort geding). omgevingsweb.nl/jurisprudentie/eclinlghams2026275-gerechtshof-amsterdam-03-02-2026-200-350-343-01
6. **Rechtbank Amsterdam, 14 november 2018,** ECLI:NL:RBAMS:2018:10124. bijzonderstrafrecht.nl/home/rb-it-bedrijf-is-aansprakelijk-voor-ondermaatse-beveiliging-…
7. **Digital Trust Center.** Praatplaat: digitale veiligheid bespreken met je IT-dienstverlener. digitaltrustcenter.nl/sites/default/files/2025-04/Praatplaat_ITdienstverlener.pdf
8. **Saxion Hogeschool.** Naar een cyberweerbaar Gelders mkb: kennisdrempels bij het beoordelen van IT-beveiliging. saxion.nl/…/publieksrapportage_naar-een-cyberweerbaar-gelders-mkb_saxion.pdf

Deze whitepaper is informatief en geen juridisch advies. De rechtszaken zijn samengevat op hoofdlijnen; lees de uitspraak voor de volledige overwegingen.

IT voor Impact

PLAN EEN AFSPRAAK

Van "het is geregeld" naar "ik weet het".

Twijfelde je bij een of meer vragen uit de directiecheck? Dan weet je nu waar vertrouwen de plek van bewijs inneemt.

Plan een afspraak. Ik loop de vragen met je door en geef je een eerste advies over waar je de meeste zekerheid wint.

Plan een afspraak →

itvoorimpact.nl/contact.html