worldstream

ONDERZOEKSRAPPORT

Hoe digitaal weerbaar is jouw organisatie?

Nederlandse organisaties en hun digitale weerbaarheid

Nederlandse organisaties overschatten hun weerbaarheid tegen IT-uitval, cyberincidenten en digitale afhankelijkheid

Onderzoek onder 270 IT-verantwoordelijken
Uitgevoerd door Markteffect in opdracht van Worldstream

worldstream.com

INHOUD

Nederlandse organisaties en hun digitale weerbaarheid

	Managementsamenvatting	3
	Kernbevindingen	4
01	De paradox van digitale weerbaarheid	5
02	IT-incidenten zijn geen theoretisch risico	7
03	IT-uitval is geen IT-probleem	8
04	Een plan is nog geen weerbaarheid	10
05	Bewust is nog niet voorbereid	11
06	Afhankelijk, maar niet bezorgd	12
07	Conclusie: weerbaarheid én continuïteit	14
	Zelfscan digitale weerbaarheid	15
	Verantwoording	16

worldstream

Hoe digitaal weerbaar zijn Nederlandse organisaties?

Nederlandse organisaties investeren in het voorkomen van IT-incidenten, maar zijn minder goed voorbereid op de gevolgen wanneer het toch misgaat. Dat is de belangrijkste conclusie van dit onderzoek naar de digitale weerbaarheid van Nederlandse organisaties.

Hoewel er aandacht is voor cybersecurity, bewustwording en continuïteitsplannen, blijkt het praktische vermogen om tijdens IT-uitval kritieke bedrijfsprocessen voort te zetten beperkt. De uitdaging ligt daarom minder in het voorkomen van incidenten dan in het waarborgen van bedrijfscontinuïteit en het versnellen van herstel.

Van incidentpreventie naar aantoonbare weerbaarheid

Het onderzoek laat een paradox zien: organisaties kunnen op papier goed voorbereid zijn, terwijl hun vermogen om een daadwerkelijke crisis op te vangen beperkt blijft. Investeringen in beveiliging en preventie blijven noodzakelijk, maar zijn niet voldoende. Echte digitale weerbaarheid vraagt om een samenhangende aanpak waarin organisaties niet alleen incidenten proberen te voorkomen, maar ook voorbereid zijn op de gevolgen ervan.

Dat betekent concreet: bedrijfskritische processen en afhankelijkheden in kaart brengen, continuïteitsplannen regelmatig testen, medewerkers voorbereiden op crisissituaties en zorgen voor passende back-ups en alternatieve infrastructuur. Ook moeten organisaties beoordelen hoe snel zij na een incident hun bedrijfskritieke systemen kunnen herstellen en in welke mate zij afhankelijk zijn van afzonderlijke leveranciers.

DE CENTRALE BOODSCHAP

De centrale boodschap is helder: digitale weerbaarheid blijkt niet alleen uit de maatregelen die een organisatie heeft getroffen, maar vooral uit de mate van continuïteit wanneer IT-systemen uitvallen.

De volgende stap voor Nederlandse organisaties is dan ook om de aandacht te verleggen van uitsluitend incidentpreventie naar aantoonbare herstelcapaciteit en bedrijfscontinuïteit. Pas wanneer plannen, mensen en technologie in de praktijk op elkaar aansluiten, ontstaat een stevige basis om een IT-crisis op te vangen.

KERNBEVINDINGEN

De 5 belangrijkste inzichten

1

IT-uitval is een reëel en breed bedrijfsrisico

Vier op de tien Nederlandse organisaties kregen het afgelopen jaar te maken met een of meerdere IT-storingen of -incidenten. De oorzaken lopen uiteen van technische storingen en softwareproblemen tot externe cyberaanvallen. Een aanzienlijk deel van de incidenten ontstaat bij externe leveranciers en partners, namelijk ruim een derde. IT-uitval is daarmee geen theoretisch risico en evenmin uitsluitend een intern IT-probleem.

2

Binnen vier uur staat een groot deel van de organisaties volledig stil

Bij 65% van de organisaties leidt het uitvallen van IT-systemen ertoe dat de organisatie binnen vier uur niet meer kan functioneren. Voor meer dan een kwart bedraagt de financiële schade na één uur IT-uitval al meer dan € 50.000. Ook processen als financiën, productie, klantenservice en logistiek worden geraakt. Digitale weerbaarheid is daarmee een strategisch vraagstuk dat de gehele organisatie en haar bedrijfsresultaten raakt.

3

Continuïteitsplannen bieden niet automatisch zekerheid

Iets meer dan de helft van de organisaties (52%) beschikt over een Business Continuity Plan. Van de organisaties met zo'n plan heeft 61% het in de afgelopen twaalf maanden getest. Toch betekent een plan op papier niet dat een organisatie daadwerkelijk in staat is om tijdens een crisis door te werken. Regelmatig testen, actuele afspraken en beschikbare alternatieve infrastructuur zijn essentieel om de effectiviteit ervan te waarborgen.

4

Bewustwording is niet hetzelfde als voorbereid zijn

Bij de meeste organisaties worden medewerkers voorbereid via trainingen, oefeningen of awarenesscampagnes. Tegelijkertijd noemt 34% een gebrek aan kennis en bewustzijn als belangrijkste tekortkoming en geeft 32% aan dat testen en oefenen nog onvoldoende zijn geregeld. De stap van weten dat een incident kan plaatsvinden naar effectief handelen wanneer het gebeurt, blijft aandacht vragen.

5

Afhankelijkheid van IT-aanbieders is een blinde vlek

Bij slechts een kwart van de organisaties kunnen kritieke workloads bij uitval van de huidige infrastructuur- of cloudleverancier blijven draaien via een alternatieve aanbieder. Bij 14% ontbreekt zo'n alternatief volledig. Daarnaast erkent bijna de helft afhankelijk te zijn van buitenlandse technologiepartijen, zonder dit als een groot risico te beschouwen. De afhankelijkheid van externe partijen vraagt echter om een bredere risicoanalyse, inclusief de vraag wat er gebeurt wanneer een leverancier zelf met uitval te maken krijgt.

HOOFDSTUK 1

01

De paradox van digitale weerbaarheid

Wat houdt digitale weerbaarheid in? Wanneer is een organisatie daadwerkelijk digitaal weerbaar? Stel deze vragen aan een willekeurige leidinggevende en de kans is groot dat er een antwoord komt dat in de kern draait om het voorkomen van incidenten.

Maar daarmee houdt digitale weerbaarheid niet op. Integendeel, voor een groot deel hangt de mate van digitale weerbaarheid van organisaties af van hoe ze zich gedragen nadat er een incident heeft plaatsgevonden. Hoe snel kan een organisatie zich herstellen na IT-uitval, ongeacht de oorzaak?

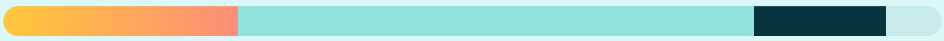
Uit de cijfers blijkt dat Nederlandse organisaties veel energie steken in het voorkomen van IT-uitval. Mede daardoor zijn IT-incidenten voor de meeste organisaties nog steeds een uitzondering. Maar de kans dat het een keer onverhoopt toch misgaat, neemt met de dag toe. Helemaal nu kwaadwillenden dankzij AI hun activiteiten drastisch opschalen.

Als het misgaat, gaat het ook goed mis

En als het dan misgaat, gaat het ook goed mis. Zo is maar een kwart van de organisaties in staat om kritieke workloads te blijven draaien via een alternatieve aanbieder of interne infrastructuur wanneer er uitval van IT-systemen plaatsvindt bij de huidige infrastructuur- en cloudleverancier. Bij ruim de helft (55%) is er beperkte inzetbaarheid mogelijk, bij 14% is er helemaal geen alternatief beschikbaar.

ALTERNATIEF BIJ UITVAL VAN DE HUIDIGE LEVERANCIER

1 op 4



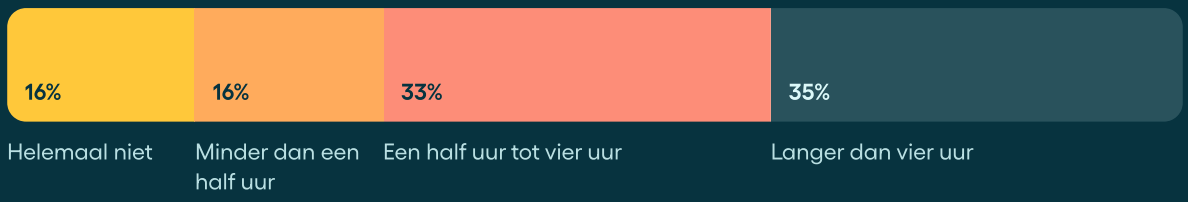
25% volledig alternatief **55%** beperkt **14%** geen alternatief

Bron: Markteffect in opdracht van Worldstream, 2026 (n = 270 IT-verantwoordelijken).

Dat is zorgelijk, want de impact van IT-uitval is niet te onderschatten. Zo kan 16% van de Nederlandse organisaties helemaal niet functioneren zonder IT-systemen en nog eens 16% functioneert minder dan een half uur. Bij 33% van de organisaties lukt het om een half uur tot vier uur te blijven draaien bij een complete IT-uitval. Dit betekent dat maar liefst 65% van de Nederlandse organisaties binnen vier uur platligt zodra de IT-systemen eruit liggen.

HOE LANG FUNCTIONEERT EEN ORGANISATIE ZONDER IT?

65% ligt binnen vier uur plat zodra de IT-systemen eruit liggen



Bron: Markteffect in opdracht van Worldstream, 2026 (n = 270 IT-verantwoordelijken).

Tel daarbij op dat het herstel van bedrijfskritische systemen na een incident bij meer dan de helft (54%) tussen de één en acht uur duurt, en dat dit bij 23% zelfs kan oplopen tot 24 uur, en je ziet de omvang van het probleem.

Organisaties denken goed voorbereid en daarmee digitaal weerbaar te zijn, maar als het misgaat blijft er van die gedegen voorbereiding weinig over. Het is de paradox van digitale weerbaarheid: voorbereiding en bescherming die zich alleen maar richt op het voorkómen van incidenten biedt onvoldoende garantie voor snel herstel ná een incident.

Voorbereiding die zich alleen richt op het voorkómen van incidenten biedt onvoldoende garantie voor snel herstel ná een incident.

DE PARADOX VAN DIGITALE WEERBAARHEID

HOOFDSTUK 2

02

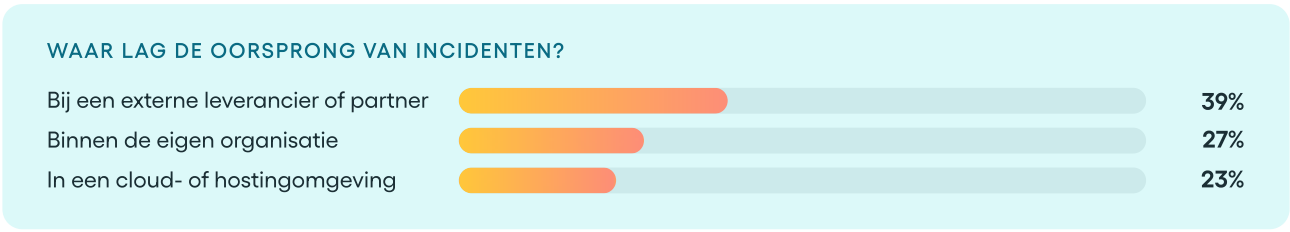
IT-incidenten zijn geen theoretisch risico

Cyberincidenten zijn geen fictieve dreiging: 40% van de Nederlandse organisaties had in de afgelopen 12 maanden te maken met één of meerdere IT-storingen of -incidenten. De meest genoemde oorzaken voor deze incidenten:



Bron: Markteffect in opdracht van Worldstream, 2026 (n = 270 IT-verantwoordelijken).

Dit uiteenlopende lijstje van oorzaken laat zien dat er geen one-size-fits-all-oplossing is om incidenten te voorkomen: de kiem voor een mogelijk probleem kan op meerdere plekken ontstaan. Dat blijkt ook als gekeken wordt naar waar de oorsprong lag van incidenten waar Nederlandse organisaties mee te maken kregen:



Bron: Markteffect in opdracht van Worldstream, 2026 (n = 270 IT-verantwoordelijken).

Het laat zien dat afhankelijkheid van derden een belangrijke rol speelt bij IT-incidenten: de oorzaak ligt in twee derde van de gevallen buiten de eigen, interne infrastructuur.

Dat roept de vraag op hoe je een risico beheerst dat grotendeels buiten je eigen organisatie ontstaat.

Ook hier ligt het antwoord maar beperkt in het voorkomen ervan. Het zit ‘m vooral in de bredere definitie van weerbaarheid: in de mogelijkheden om de gevolgen op te vangen en snel te herstellen als er iets misgaat.

De kiem voor een mogelijk probleem kan op meerdere plekken ontstaan.

HOOFDSTUK 3

03

IT-uitval is geen IT-probleem

De impact van IT-uitval is enorm, dat blijkt al uit de cijfers in het eerste hoofdstuk over hoe lang organisaties door kunnen blijven draaien als hun kritieke IT-infrastructuur niet beschikbaar is. De gevolgen worden nog tastbaarder wanneer gekeken wordt naar wat het organisaties nou eigenlijk kost.

Veel, zo blijkt uit het onderzoek. Gevraagd naar de financiële impact van één uur IT-uitval, levert dit de volgende bedragen op:

FINANCIËLE IMPACT VAN ÉÉN UUR IT-UITVAL



39%

weet niet eens wat een uur uitval hun kost.

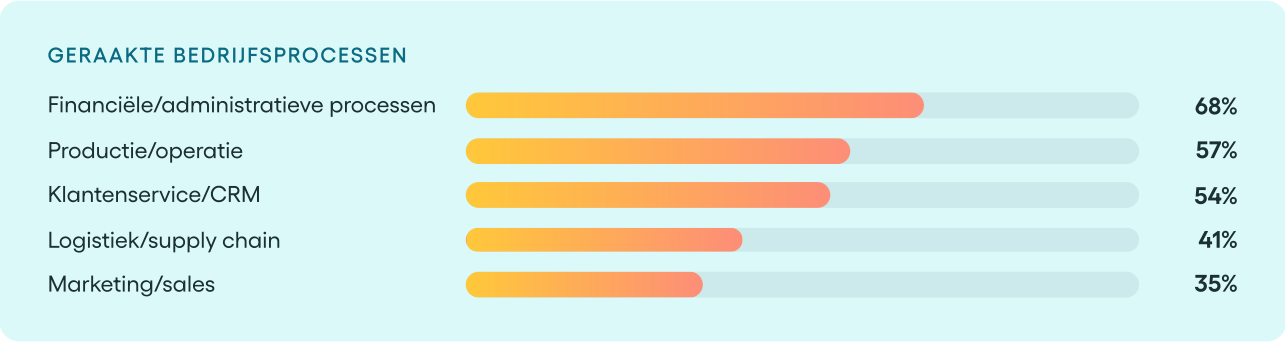
Meer dan 1 op 4

heeft na één uur uitval een schadepost van meer dan € 50.000.

Bron: Markteffect in opdracht van Worldstream, 2026 (n = 270 IT-verantwoordelijken).

Oftewel: bij meer dan een kwart van de Nederlandse organisaties levert één uur uitval een schadepost op van meer dan € 50.000. Daarbij weet bijna vier op de tien organisaties (39%) niet eens wat een uur uitval hun kost.

De potentiële impact van IT-uitval wordt nog duidelijker wanneer gekeken wordt naar de bedrijfsprocessen die worden geraakt. Het levert een dwarsdoorsnede op van de gemiddelde Nederlandse organisatie:



Bron: Markteffect in opdracht van Worldstream, 2026 (n = 270 IT-verantwoordelijken).

IT-uitval is allang geen puur IT-probleem meer: het raakt de hele bedrijfsvoering, van de financiële administratie tot en met de klantenservice. Digitale weerbaarheid is dan ook niet alleen een technisch vraagstuk waar vooral de IT-afdeling zich mee bezig moet houden. Het is een bestuurlijk vraagstuk. De mate van weerbaarheid bepaalt of een organisatie kan blijven draaien of niet.

Digitale weerbaarheid is dan ook niet alleen een technisch vraagstuk waar vooral de IT-afdeling zich mee bezig moet houden. Het is een bestuurlijk vraagstuk.

HOOFDSTUK 4

04

Een plan is nog geen weerbaarheid

Zodra er een crisis uitbreekt, bijvoorbeeld wanneer IT-systemen uitvallen, is het goed om overeenstemming te hebben over wat er moet gebeuren om cruciale processen draaiende te kunnen houden. Zo kan in geval van nood worden teruggegrepen op afspraken die al eerder zijn gemaakt.

Het is daarom positief om te zien dat 74% van de Nederlandse organisaties back-up-, herstel- en noodmaatregelen heeft vastgelegd. En 64% test back-ups en herstelprocessen regelmatig. Bovendien heeft meer dan de helft (54%) van de organisaties een digitaal noodpakket.

Een iets kleiner percentage, maar nog steeds een meerderheid van 52%, beschikt over een Business Continuity Plan (BCP). Het minder goede nieuws is dat 48% dus niet over een dergelijk continuïteitsplan beschikt, of niet weet of dit aanwezig is.

Als we de groep die wel een BCP heeft verder analyseren, valt op dat een meerderheid dit plan recent (of iets minder recent) heeft getest:



Bron: Markteffect in opdracht van Worldstream, 2026 (n = 270 IT-verantwoordelijken). Organisaties met een BCP.

Bij die laatste groep kun je vraagtekens zetten bij de effectiviteit van het BCP. In een crisissituatie een crisisplan voor het eerst ten uitvoer brengen, is een stresstest die je maar beter kunt voorkomen door het plan al in een eerder stadium te testen.

Maar ook de groep die zijn BCP langer dan een jaar geleden voor het laatst heeft getest, kan bij een daadwerkelijke crisis voor onaangename verrassingen komen te staan. Los van de vraag of iedere werknemer nog helemaal helder voor ogen heeft wat er moet gebeuren, kun je de vraag stellen of de huidige situatie nog hetzelfde is vergeleken met een jaar geleden. Zeker gezien de snelheid van technologische ontwikkelingen vandaag de dag. Zijn er bijvoorbeeld nieuwe systemen of oplossingen bijgekomen? Een BCP is een levend document dat regelmatig getest en aangepast moet worden om accuraat te blijven. Alleen dan kun je erop vertrouwen dat het werkt als het onverhoopt misgaat.

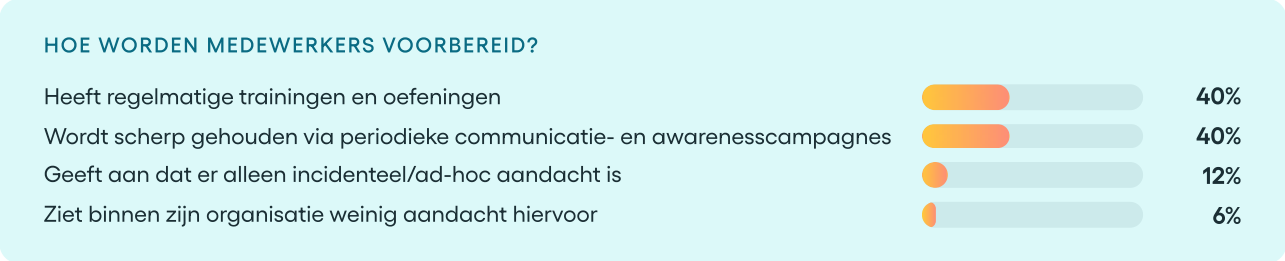
HOOFDSTUK 5

05

Bewust is nog niet voorbereid

Tot nu toe hebben we het vooral over technologie en systemen, maar organisaties bevatten nog een ander essentieel element: werknemers. Zij spelen uiteraard ook een belangrijke rol in de digitale weerbaarheid van organisaties.

Dat begint, wederom, met voorbereiding. Want gevraagd naar hoe medewerkers worden voorbereid op IT-calamiteiten, ontstaat het volgende beeld:



Bron: Markteffect in opdracht van Worldstream, 2026 (n = 270 IT-verantwoordelijken).

Binnen de meeste Nederlandse organisaties wordt er dus wel aandacht besteed aan het voorbereiden van medewerkers op IT-calamiteiten.

Tegelijkertijd is er nog werk aan de winkel. Want specifiek gevraagd naar wat er volgens de ondervraagden nog aan maatregelen mist binnen hun organisaties, komen de volgende hiaten naar boven:



Bron: Markteffect in opdracht van Worldstream, 2026 (n = 270 IT-verantwoordelijken). Meerdere antwoorden mogelijk.

Digitale weerbaarheid begint of eindigt niet bij ingestelde maatregelen, maar bij de vraag of een organisatie weet wat er moet gebeuren wanneer systemen niet beschikbaar zijn. Bewustzijn betekent niet automatisch dat je voorbereid bent, of dat je weet wat je moet doen als er zich daadwerkelijk een crisis voordoet.

HOOFDSTUK 6

06

Afhankelijk, maar niet bezorgd

Een alternatieve infrastructuur is binnen bijna een derde van de organisaties (31%) nog afwezig, zo leren de cijfers uit het vorige hoofdstuk. Dat betekent automatisch dat bij uitval van cruciale IT-systemen deze organisaties niet kunnen overschakelen naar een back-up infrastructuur zodat (een deel van de) werkzaamheden door kunnen gaan.

Maar er wordt niet alleen gekeken naar alternatieve infrastructuur vanwege weerbaarheid bij IT-uitval. De maatschappelijke discussie die de laatste jaren is ontstaan rondom digitale soevereiniteit en autonomie speelt ook een belangrijke rol. Organisaties kijken daardoor ook kritischer naar hun afhankelijkheid van buitenlandse technologiepartijen.

Maar tussen kritisch kijken en daadwerkelijk handelen bestaat nog wel een kloof, zo blijkt. Zo erkent bijna de helft van de Nederlandse organisaties afhankelijk te zijn van buitenlandse tech-partijen, maar ziet dit als een beheersbaar risico. Ongeveer één op de zeven organisaties (15%) erkent afhankelijk te zijn én maakt zich hier zorgen over. En 29% is actief bezig om de afhankelijkheid te beperken. Slechts 9% van de Nederlandse organisaties beschouwt zichzelf als nauwelijks afhankelijk.

15%
erkent afhankelijk te zijn én maakt zich hier zorgen over

29%
is actief bezig om de afhankelijkheid te beperken

9%
beschouwt zichzelf als nauwelijks afhankelijk

Bron: Markteffect in opdracht van Worldstream, 2026 (n = 270 IT-verantwoordelijken).

Wat als het misgaat bij een IT-partner?

Bijkomende uitdaging hierbij is dat digitale afhankelijkheid zich niet beperkt tot de eigen organisatie. Externe leveranciers en partners zijn onderdeel van het risicoprofiel. Helemaal als je beseft dat de oorsprong van veel IT-incidenten bij externe partijen ligt, zoals bleek in het tweede hoofdstuk van dit rapport.

Het is dus de vraag of de organisaties die hun digitale afhankelijkheid als een beheersbaar risico zien, de volledige impact van hun afhankelijkheid goed in kaart hebben. Want wat als het misgaat bij een IT-partner, hoe beheersbaar is jouw afhankelijkheid dan?

Digitale weerbaarheid draait dan eveneens om het in kaart brengen van dergelijke risico's. Op deze manier kan er ook actie ondernomen worden om afhankelijkheden terug te dringen.



Wat als het misgaat bij een IT-partner, hoe beheersbaar is jouw afhankelijkheid dan?

VERDER LEZEN

Meer weten over hoe je dit kunt aanpakken? Lees dan onze eerdere whitepaper **De slimme Cloudkeuze. Van versnippering naar regie — in 3 strategische stappen**.

Lees de whitepaper

CONCLUSIE

07

Weerbaarheid én continuïteit

Nederlandse organisaties hebben de afgelopen jaren flink geïnvesteerd in hun digitale weerbaarheid. Over bewustzijn lijken we ons wat dat betreft weinig zorgen te hoeven maken. Maar veel van deze inspanningen richten zich op het voorkomen van IT-incidenten, veel minder aandacht gaat er uit naar hoe er gehandeld moet worden wanneer het misgaat.

Ook laat het onderzoek zien dat de bedrijfsvoering van de meeste organisaties sterk afhankelijk blijft van IT en externe partijen. De volgende stap in digitale weerbaarheid ligt daarom niet alleen in het voorkomen, maar ook in het vergroten van de continuïteit wanneer IT daadwerkelijk wegvalt, zodat er sneller hersteld kan worden.

Het antwoord op de vraag 'Hoe weerbaar zijn Nederlandse organisaties?' is niet eenduidig. Op papier zijn ze behoorlijk weerbaar (BCP's, back-ups, et cetera) en ze besteden aandacht aan het voorbereiden en bewust maken van hun medewerkers. Maar deze voorbereiding is in de praktijk minder solide dan het lijkt.

Nederlandse organisaties lijken geruster dan ze eigenlijk zouden moeten zijn. Of ze echt klaar zijn voor een digitale crisissituatie, is iets waar de meeste organisaties pas achter komen wanneer het daadwerkelijk misgaat. Dat is een wankele basis voor vertrouwen.

Nederlandse organisaties lijken geruster dan ze eigenlijk zouden moeten zijn.

worldstream



ZELFSCAN DIGITALE WEERBAARHEID

Benieuwd hoe digitaal weerbaar jouw organisatie is, en hoe je scoort ten opzichte van andere organisaties?

1

Beantwoord acht vragen

Over hoe jouw organisatie is voorbereid op IT-uitval.

2

Zie direct je score

En in welke categorie je valt: Werk aan de winkel, Op de goede weg of Koploper.

3

Ontvang je checklist

Met drie stappen die passen bij jouw score.

Doe de zelfscan

VERANTWOORDING

Over dit onderzoek

De cijfers waarop dit onderzoeksrapport is gebaseerd komen uit een onderzoek dat in opdracht van Worldstream is uitgevoerd door Markteffect. Hiervoor zijn 270 IT-verantwoordelijken ondervraagd, werkzaam bij Nederlandse organisaties met meer dan 50 werknemers. Het onderzoek is uitgevoerd in juni 2026.

OPDRACHTGEVER	Worldstream
UITVOERING	Markteffect
DOELGROEP	IT-verantwoordelijken bij Nederlandse organisaties met meer dan 50 werknemers
RESPONDENTEN	270
PERIODE	Juni 2026

worldstream

worldstream.com
+31 (0) 174 712 117

© 2026 Worldstream. Dit rapport mag worden gedeeld of geciteerd, met vermelding van de bron: Worldstream, Nederlandse organisaties en hun digitale weerbaarheid (2026).