



Regie op security en privacy

Hoe organisaties
eigenaarschap organiseren

SEPTEMBER 2026

Voorwoord

Wie regelmatig aan bestuurstafels van middelgrote organisaties zit, hoort steeds hetzelfde gesprek. Niet over firewalls of frameworks, die discussie is wel gevoerd. Het gesprek gaat over iets ongrijpbaars: het gevoel dat security geregeld zou moeten zijn, en de stille twijfel of dat ook echt zo is.

Wij zitten dagelijks aan die tafels. Northwave staat naast CISO's, IT-managers en besturen van middelgrote organisaties, niet met de belofte dat een aanval uitblijft, maar met de zekerheid dat de organisatie er wendbaar op reageert. En juist vanuit die praktijk begrijpen we waar die twijfel vandaan komt.

Want uw positie is er een van tegenstrijdigheden. Uw organisatie is groot genoeg voor een complete IT-infrastructuur, met alles wat daarbij hoort aan systemen, data en afhankelijkheden. Maar te klein voor de overhead waarmee een enterprise zich organiseert: een eigen SOC, een voltallig securityteam. U heeft het aanvalsoppervlak van een enterprise, met een fractie van de verdediging. En voor een aanvaller bent u daarmee juist aantrekkelijk. Niet ondanks uw omvang, maar dankzij die omvang: veel gericht op de operatie en op groei, zelden iemand die 24/7 meekijkt, en in bezit van data die goud waard kan zijn.

Tegelijk staat u zelden op uzelf. Als toeleverancier van grotere organisaties en overheden bent u onderdeel van ketens die steeds

meer van u vragen. Wat uw afnemers aan eisen opgelegd krijgen, schuift door naar u, en met NIS2 is die ketenpositie niet langer een commercieel gegeven, maar een juridisch feit. Security wordt dan al snel doorgeschoven naar IT, terwijl regelgeving, toezichthouders en ketenpartners het inmiddels nadrukkelijk bij het bestuur leggen.

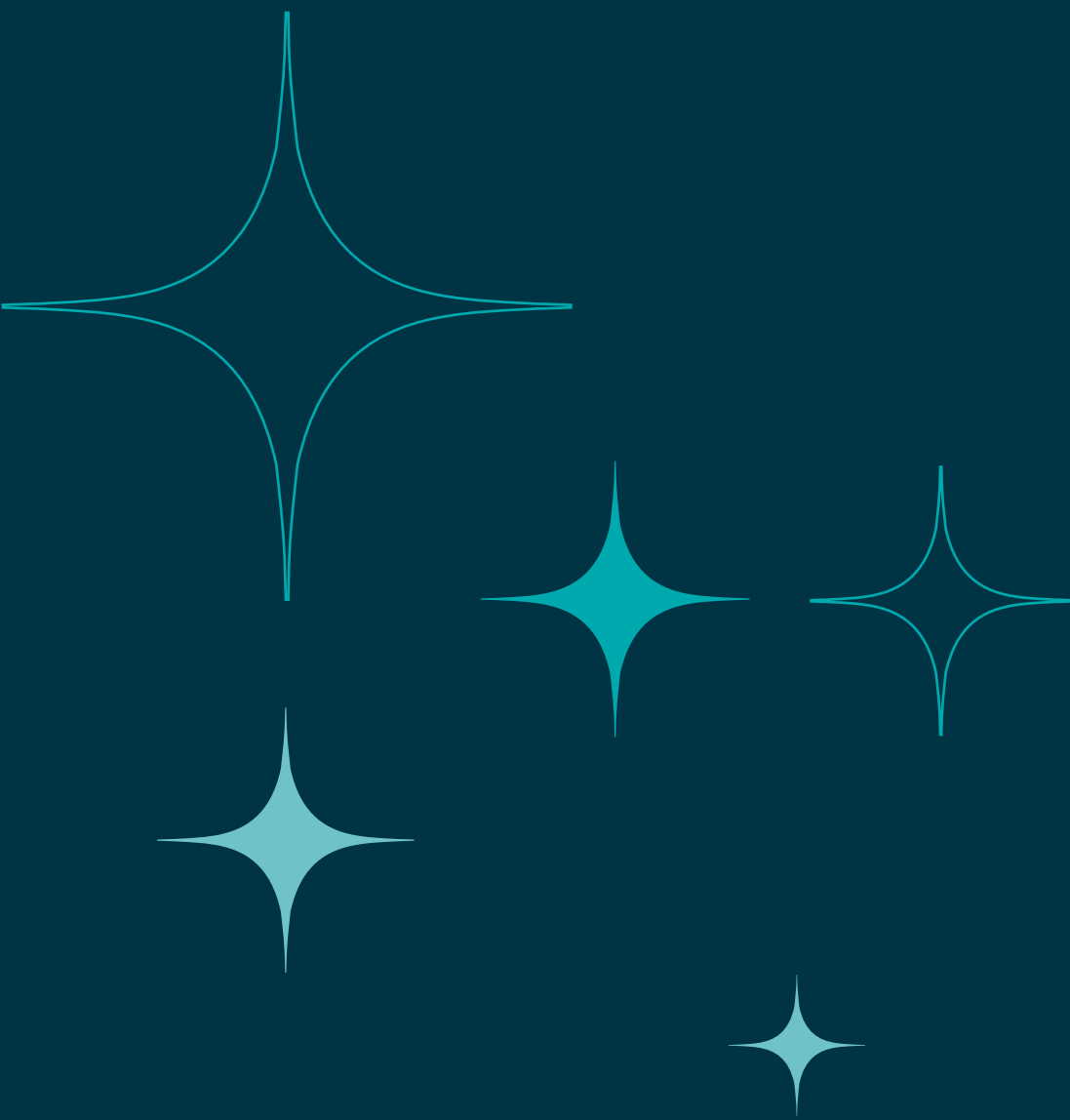
Precies daar wilden wij dieper kijken. Niet om te oordelen. Dit onderzoek is een nulmeting, geen rapportcijfer. Maar omdat wij vanuit onze dagelijkse praktijk patronen zien die individuele organisaties zelf niet kunnen zien. Die kennis is het meest waard op de plek waar de beslissingen worden genomen. Daarom ligt het rapport nu bij u.

Lees dit rapport niet als benchmark om uzelf gerust te stellen, maar als spiegel voor uw eigen tafel. Herkent u de patronen niet? Toets dat dan aan de feiten in uw organisatie. Herkent u ze wel? Dan weet u na het lezen waar te beginnen. Want wendbaar reageren op wat komt, begint bij regie over wat er nu staat. Dat gesprek, scherp, aan de bestuurstafel, met de juiste mensen erbij, is waar volwassen security begint.

Pim Takkenberg

General Manager Benelux,
Northwave Cyber Security

Inhoudsopgave



VOORAF	Voorwoord	02
	Managementsamenvatting	04
	Over dit onderzoek	05
	Het maturitymodel achter de meting	06
DEEL I	Volwassenheid en zelfbeeld	07
	1 Gemeten volwassenheid per dimensie	08
	2 De ervaren uitdagingen	09
	3 Risico's die respondenten de meeste zorgen geven	10
	4 Zelfinschatting van eigen security	11
DEEL II	Het structurele probleem	12
	5 De CISO zonder mandaat	13
	6 Waar het besluit dan wel valt	14
	7 Waarom managementbetrokkenheid achterblijft	15
	8 Regieorganisatie in de praktijk	16
	9 Hoe combinaties ontstaan	17
	10 Financieringsmodellen voor security	18
DEEL III	Aantonen en leren	19
	11 NIS2: wettelijk verplicht, lang niet altijd aantoonbaar	20
	12 Ervaring met securityincidenten	21
	13 Operationeel leren versus structureel leren	22
DEEL IV	Wat het middensegment zoekt	23
	14 Regie willen houden	24
	15 Regie houden én goed geholpen worden	25
	16 Hoe partners gekozen worden	26
	17 Voorkeur voor Nederlandse of Europese partner	27
	18 Waar het middensegment staat	28
TOT BESLUIT	Reflectievragen voor uw organisatie	29
	Wat dit betekent voor uw organisatie	30
	Verantwoording en bijlagen	31
	Het maturitymodel	32



Security is wel belegd, maar nog niet bestuurd

Nederlandse middelgrote organisaties hebben security ingekocht en rollen belegd, negen op de tien heeft een CISO of ISM. Maar mandaat, budget en regie blijven achter. De verantwoordelijke expert zit één laag onder de tafel waar de besluiten vallen: kennis en zeggenschap liggen niet op dezelfde plek. Het gevolg is een organisatie die security wél heeft geregeld, maar nog niet bestuurd. Dit rapport maakt zichtbaar waar het aan ontbreekt, en wie het kan oplossen.

DE CISO BESLIST ZELDEN ZELF

In 83% van de organisaties neemt niet de CISO of ISM het definitieve besluit over de aanschaf van securitydiensten, maar meestal de IT-manager, de CEO of de CTO.

HET BUDGET IS INCIDENTEEL

Nog geen drie op de tien organisaties (29,3%) hebben een vast jaarlijks securitybudget. De grootste groep (42,4%) maakt geld vrij per project of per behoefte.

DE BORGING BLIJFT ACHTER

Organisaties beoordeelden zichzelf op zeven onderdelen, van awareness tot bestuurlijke betrokkenheid. Wat je kunt inkopen of inrichten scoort het best, wat blijvende aandacht van de directie vraagt het minst.

NIS2-PLICHT IS LANG NIET ALTIJD AANTOONBAAR

Van de organisaties die zeggen sterk onder NIS2 te vallen, geeft ruim een derde (36,5%) aan daar op dit moment niet aantoonbaar aan te voldoen.*

CAPACITEIT IS DE BREEDST GEDEELDE UITDAGING

Van acht voorgelegde uitdagingen scoort "onvoldoende interne capaciteit of expertise" het hoogst (3,25 op een schaal van 5). Het is de enige stelling waarmee de gemiddelde respondent het ronduit eens is.

HET GROOTSTE BEZWAAR TEGEN EXTERNE HULP IS ZEGGENSCHAP

43,5% noemt "regie intern houden" als bezwaar tegen een externe securitypartner. Daarna volgt: niet precies weten wat de organisatie nodig heeft (31,4%).

* n=52, organisaties die sterk onder NIS2 vallen; zelfrapportage, geen audit.

ONDERZOEKSMETHODE

Over dit onderzoek

In dit onderzoek brachten we in kaart hoe het Nederlandse middensegment security en privacy organiseert.



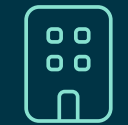
UITVOERING

Mei-juni 2026.



METHODE

Kwantitatief onderzoek via een gestructureerde vragenlijst, zelfstandig ingevuld via een online panel.



POPULATIE

Nederlandse organisaties met 100 tot 1.000 medewerkers, over meerdere sectoren: het middensegment tussen mkb en enterprise.



RESPONDENTEN

N = 191, primair verantwoordelijken en beslissers in IT, bedrijfsvoering en security bij Nederlandse organisaties.



INTERVIEWS

Parallel aan de survey zijn 10 kwalitatieve verdiepingsinterviews afgenomen met IT, bedrijfsvoering en securityverantwoordelijken bij organisaties binnen de populatie.



De vragenlijst is op aanvraag beschikbaar.



Het maturitymodel achter de meting

Hoe volwassen is de securityorganisatie in het middensegment? Om dat te meten gebruikten we een maturitymodel. Respondenten beoordeelden hun eigen organisatie op zeven dimensies, van securitybeleid en managementbetrokkenheid tot incident response en technische maatregelen. Per dimensie kozen ze de beschrijving die het best past, oplopend van niveau 1 (ad hoc) tot niveau 4 (geïntegreerd).

1 · AD HOC

Security wordt ad hoc opgepakt als er iets misgaat. Er is geen beleid, weinig zicht op risico's en verplichtingen, en rollen zijn onduidelijk: security is versnipperd over teams zonder centrale regie.

2 · BASIS

Er is basisbeleid en de basismaatregelen zijn aanwezig, maar de aanpak is reactief: beleid leeft op papier, afspraken zijn persoonsafhankelijk en het management is alleen op hoofdlijnen betrokken.

3 · REGIE & STRATEGIE

Het bestuur is actief betrokken en security staat periodiek op de agenda. Beleid is actueel en gekoppeld aan risico's, rollen zijn vastgelegd en samenwerking tussen teams en leveranciers is georganiseerd.

4 · GEÏNTEGREERD

Het bestuur is aanjager van security. Beleid leeft in de organisatie en is volledig ingebed in de besturing, regie verbindt alle disciplines, en incidenten leiden structureel tot verbetering.

Die zeven dimensies zijn: **Security awareness, Securitybeleid, Incident response, Technische maatregelen, Rollen & regie, Compliance & risico en Managementbetrokkenheid.** Het volledige maturitymodel, met per dimensie de kenmerken van elk niveau, is opgenomen in de bijlage achterin dit rapport.



DEEL I

Volwassenheid en zelfbeeld

Hoe organisaties hun risico's en zichzelf inschatten.

Gemeten volwassenheid per dimensie

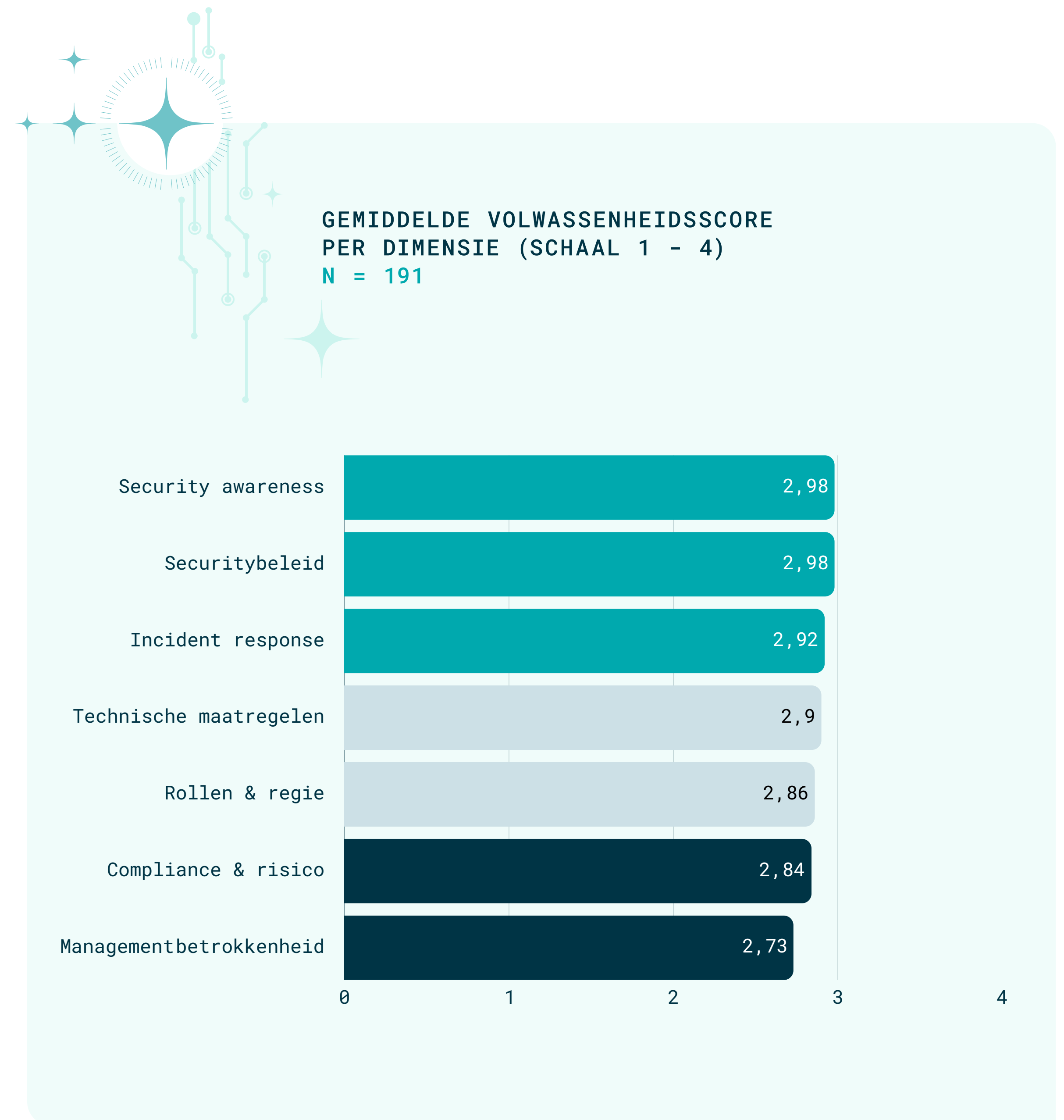
Organisaties beoordeelden zichzelf op zeven dimensies van volwassenheid, van awareness tot managementbetrokkenheid, op een schaal van 1 (ad hoc) tot 4 (geïntegreerd).

Niet de verschillen springen eruit, maar de overeenkomst: alle zeven scores blijven net onder niveau 3 steken. Het hele middensegment staat op hetzelfde punt: de basis op orde, de borging nog niet.

Want de volgorde vertelt ons wel iets. Bovenaan staat wat u kunt kopen of inrichten: een awarenesscampagne, securitybeleid, een incidentproces (elk rond 2,9). Onderaan staan juist de twee dingen die niet met een project of aankoop opgelost zijn: compliance & risico (2,84) en managementbetrokkenheid (2,73).

TAKE AWAY

Managementbetrokkenheid sluit de rij met 2,73. De uitdaging ligt bij wat niet eenvoudig kan worden ingekocht of geïmplementeerd: blijvende bestuurlijke aandacht.



De ervaren uitdagingen

Wat is de grootste uitdaging? We legden acht stellingen voor, die respondenten scoorden op een schaal van 1 (herken ik niet) tot 5 (herken ik sterk).

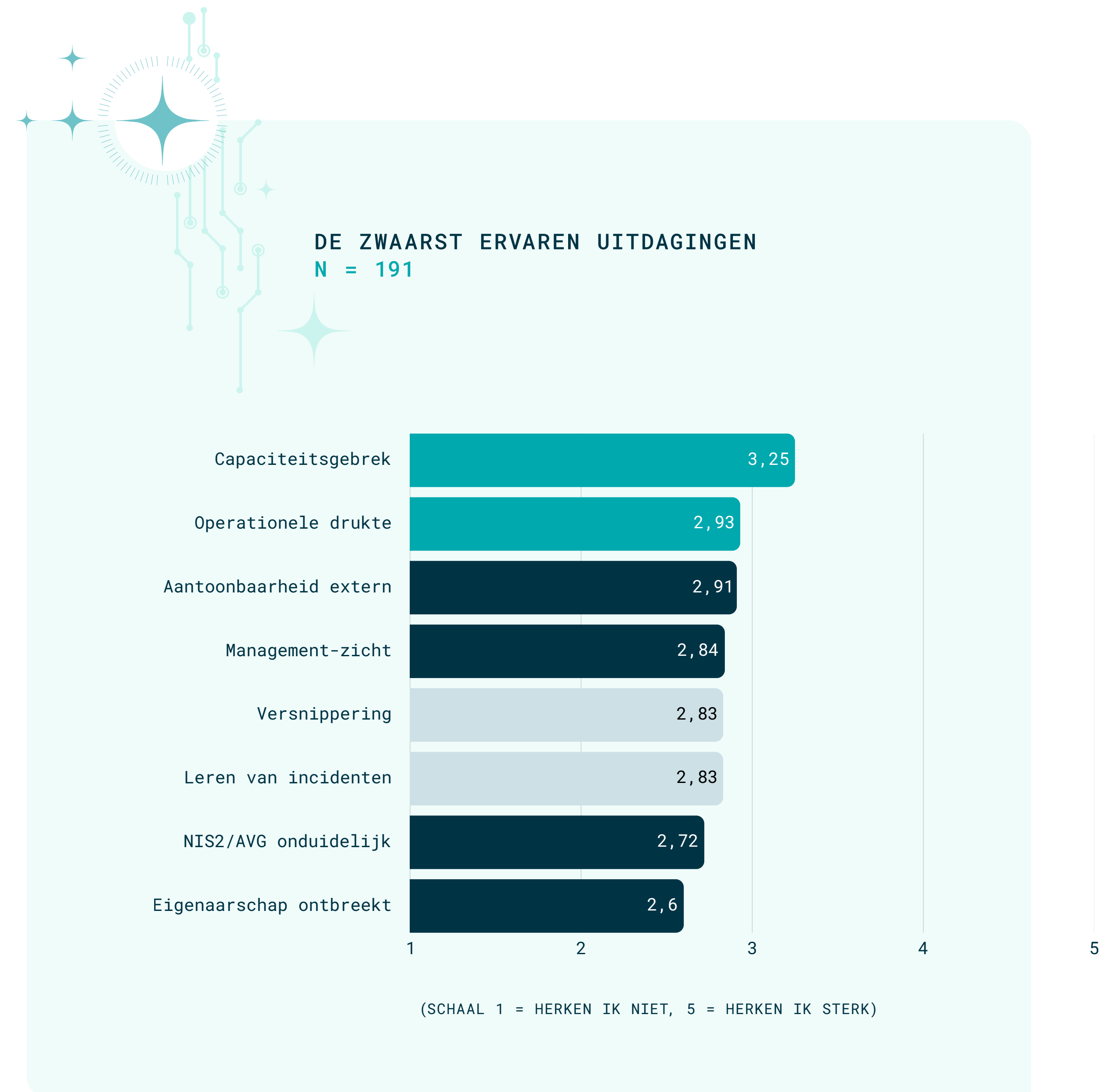
Er is maar één uitdaging waar de gemiddelde organisatie het écht mee eens is: onvoldoende interne capaciteit of expertise (3,25) is de enige stelling die boven het schaal midden uitkomt. De andere zeven blijven er net onder, door sommigen herkend, niet breed gevoeld.

Net als bij de volwassenheidsscan zijn de zwaarst ervaren uitdagingen geen technische vraagstukken, maar kwesties van capaciteit en bestuur: te weinig capaciteit (3,25), niet toekomen aan een structurele aanpak (2,93), security extern niet kunnen aantonen (2,91) en te weinig zicht bij het management (2,84).

Opvallend is wat onderaan staat: "eigenaarschap ontbreekt" (2,6) is de minst gevoelde uitdaging van allemaal.

TAKE AWAY

Het sterkst gevoeld: te weinig capaciteit. Het minst gevoeld: te weinig eigenaarschap. En daar zit de kern: extra capaciteit helpt, maar zonder duidelijk eigenaarschap blijft het onderliggende vraagstuk staan.



Risico's die respondenten de meeste zorgen geven

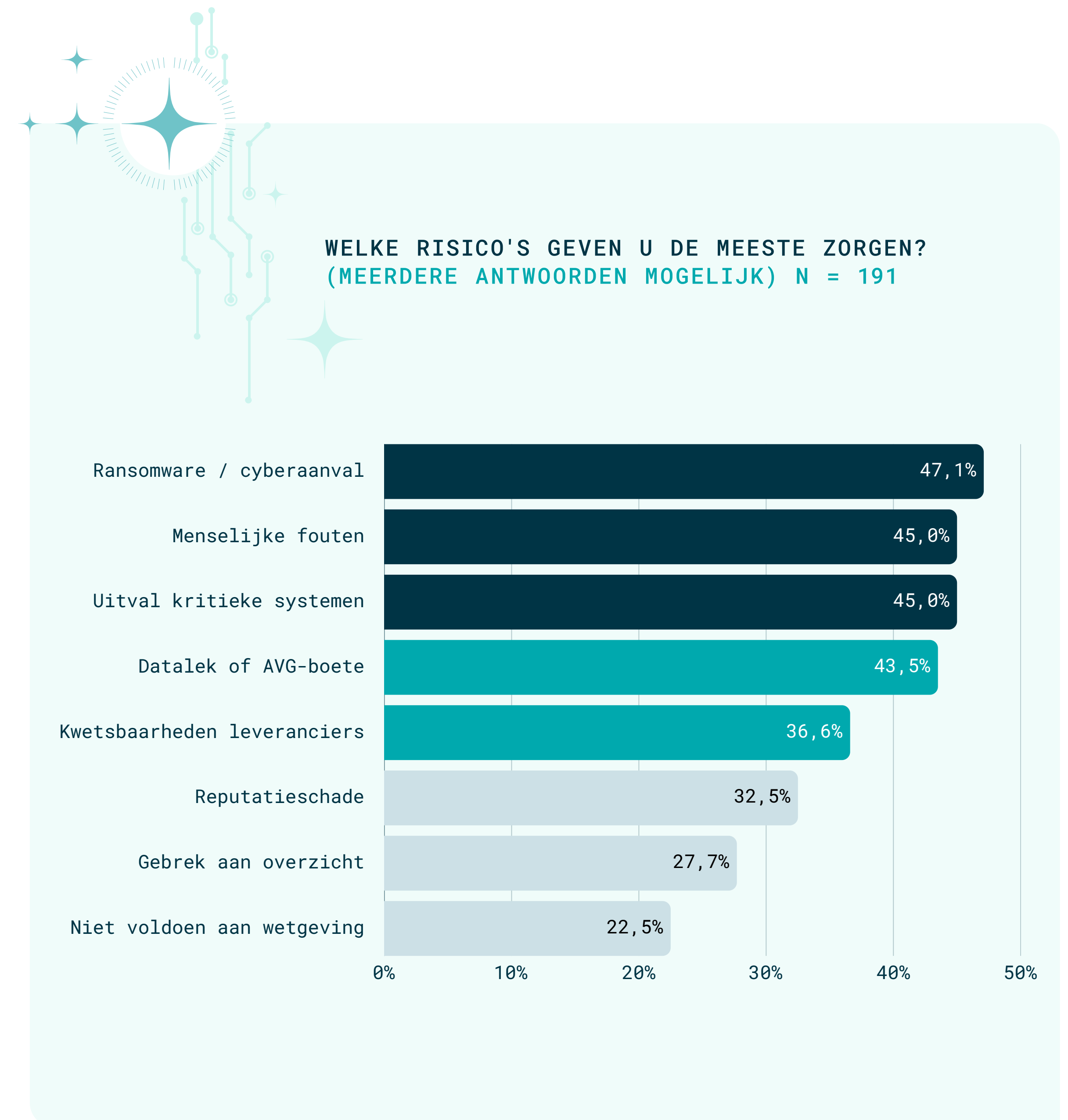
We vroegen welke risico's de meeste zorgen geven, met meerdere antwoorden mogelijk.

De zorgen gaan vooral naar concrete, zichtbare incidenten. Ransomware wordt het vaakst genoemd (47,1%), gevolgd door uitval van kritieke systemen en menselijke fouten (beide 45,0%) en datalekken (43,5%). Opvallend: menselijke fouten wegen bijna even zwaar als ransomware: de zorg zit niet alleen buiten bij de aanvaller, maar ook binnen de eigen organisatie.

Onderaan de lijst staat iets anders: gebrek aan overzicht (27,7%) en niet voldoen aan wetgeving (22,5%) geven het minst vaak zorgen. Dat gaat over de bestuurlijke, borgende kant, juist waar het maturitymodel de zwakste plekken liet zien.

TAKE AWAY

De meeste zorg gaat naar incidenten, de minste naar het overzicht en de regie die zo'n incident beheersbaar maken. Opvallend, want juist daar, in de aansturing en borging, liggen volgens de maturityscan de aandachtspunten.



Zelfinschatting van eigen security

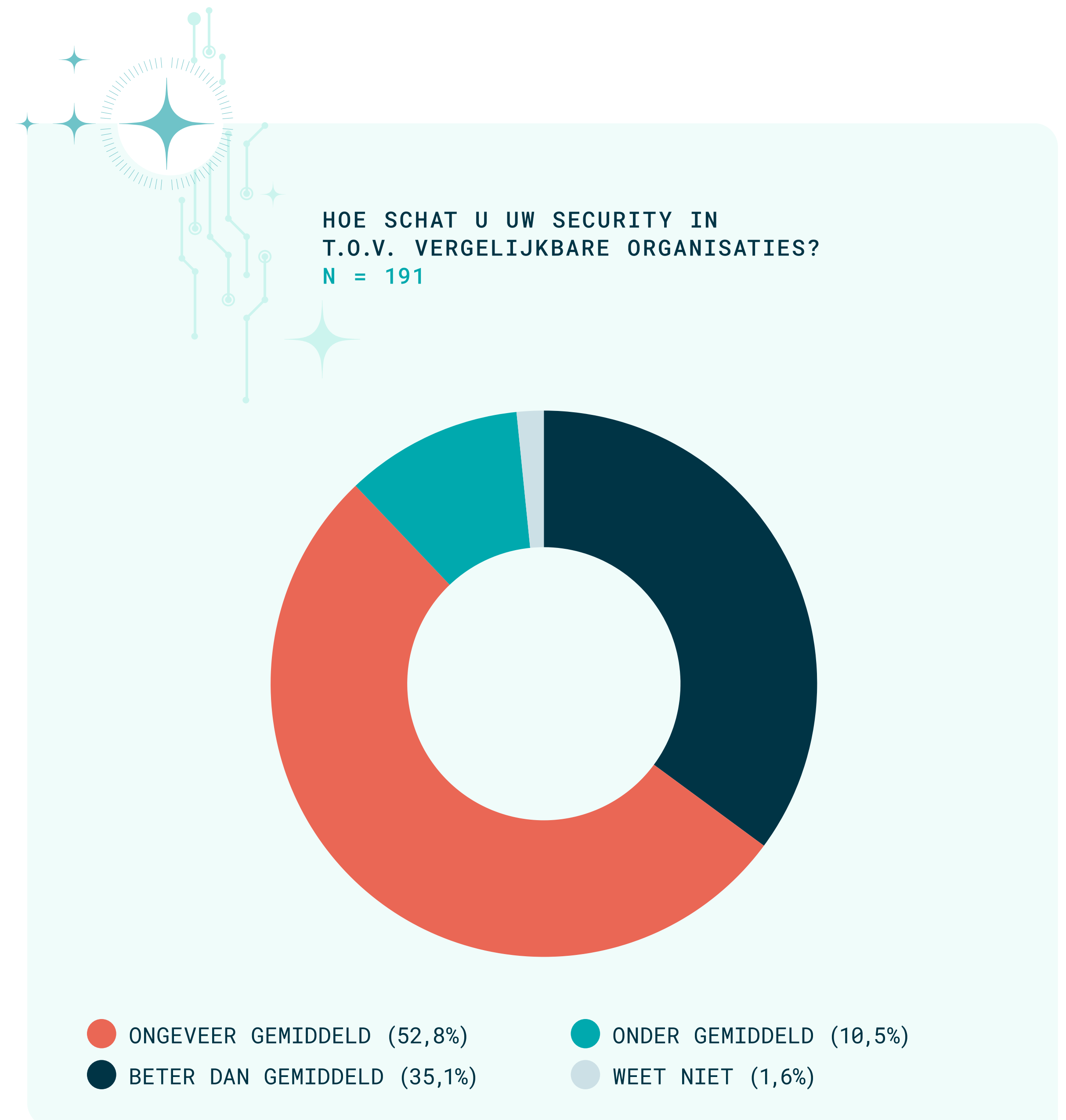
We vroegen organisaties hun eigen security te vergelijken met die van vergelijkbare organisaties: beter, ongeveer gelijk of slechter. Het beeld is nuchter: ruim de helft noemt zichzelf ongeveer gemiddeld (52,8%), ruim een derde beter dan gemiddeld (35,1%) en één op de tien slechter (10,5%).

Toch zit er een lichte scheefheid in. Ruim drie keer zoveel organisaties noemen zichzelf beter dan gemiddeld als slechter, en dat kan in een gemiddelde groep niet allebei waar zijn.

Het is menselijk en mild vergeleken met wat zelfinschattingsonderzoek doorgaans laat zien, maar het betekent wel dat een deel van de organisaties zich veiliger waant dan het is.

TAKE AWAY

Het verschil tussen veilig vóelen en aantoonbaar veilig zijn, is precies waar Deel III over gaat.





DEEL II

Het structurele probleem

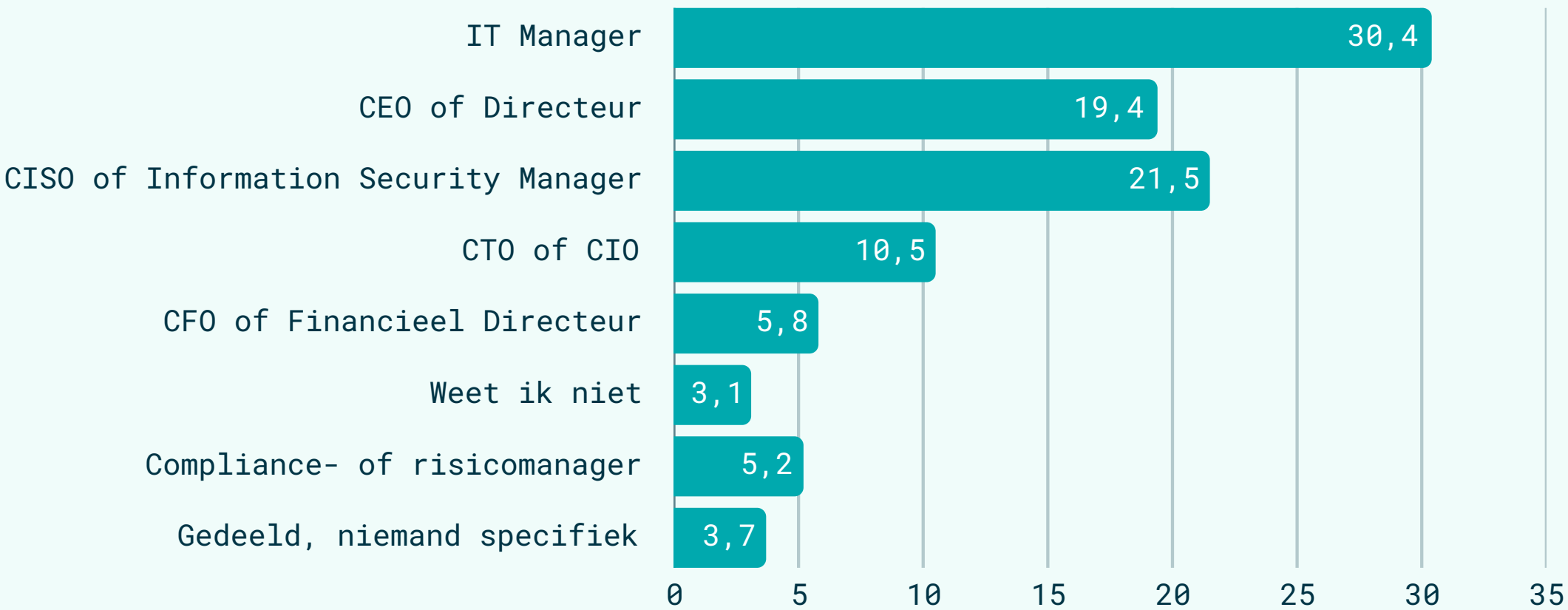
Wie beslist, en wie betaalt: mandaat en budget van dichtbij.

De CISO zonder mandaat

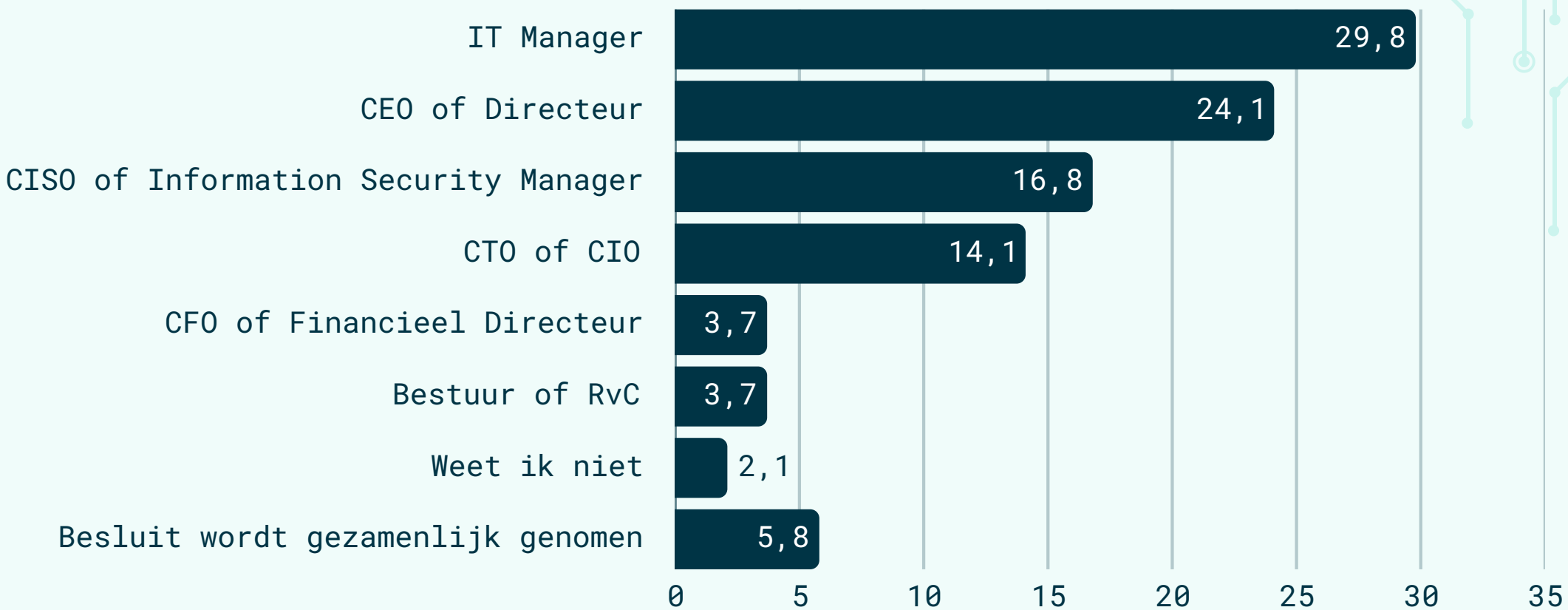
Negen op de tien organisaties (90%) hebben een CISO of Information Security Manager in huis. De rol bestaat dus vrijwel overal. We stelden daarom twee vragen: wie is verantwoordelijk voor security en wie beslist over de aanschaf van een securitydienst? Hieronder de uitkomsten van beide vragen.

In 21,5% van de organisaties is de CISO verantwoordelijk voor security. Het aanschafbesluit neemt de CISO in minder dan één op de vijf gevallen (16,8%). In 83% van de organisaties beslist dus iemand anders, meestal de IT-manager, de CEO of de CTO.

WIE IS PRIMAIR VERANTWOORDELIJK VOOR SECURITY IN UW ORGANISATIE?
N = 191



WIE NEEMT DOORGAANS HET DEFINITIEVE BESLUIT OVER DE AANSCHAF VAN EEN SECURITYDIENST?
N = 191



TAKE AWAY

Negen op de tien organisaties hebben een CISO of ISM. In 83% beslist een ander over de aanschaf. De expert adviseert; een ander tekent.

**De percentages per rol zijn indicatief; vooral de groep waar de CTO of CIO verantwoordelijk is, is met twintig respondenten klein.*

Waar het besluit dan wel valt

De twee vragen van de vorige pagina, wie verantwoordelijk is en wie beslist, leveren samen nog een derde uitkomst op. Door beide antwoorden per respondent naast elkaar te leggen, is per organisatie te zien of het om dezelfde rol gaat. Bij 51% is dat niet zo: de verantwoordelijke en de beslisser zijn twee verschillende personen. Bij de andere 49% vallen ze samen. De verantwoordelijkheid voor security en de zeggenschap over de middelen liggen dus in ruim de helft van de organisaties niet in één hand.

Bij de CISO is dat patroon het sterkst. In 41 organisaties is de CISO de verantwoordelijke; in 25 daarvan neemt hij of zij het aanschafbesluit niet zelf. Dat is drie op de vijf, ruim boven het gemiddelde van de hele groep. Waar het besluit dan wel valt, is opvallend eenzijdig: tien keer bij de CTO of CIO, acht keer bij de CEO of directeur, vier keer bij gezamenlijke besluitvorming, twee keer bij de IT-manager en één keer bij het bestuur of de RvC.

Ook de richting valt op. In vrijwel alle gevallen gaat het besluit naar boven, naar een directielid, of zijwaarts, naar een collega op hetzelfde niveau. Naar beneden gaat het bijna nooit. De CISO signaleert, adviseert en onderbouwt, maar de afweging tussen risico en investering wordt elders gemaakt. De CISO adviseert; een ander tekent.

Dat hoeft geen probleem te zijn. Grotere investeringen horen op directieniveau te worden gewogen, en gedeelde besluitvorming kan bewust beleid zijn. De wezenlijke vraag is dan ook niet wie tekent, maar of degene die verantwoordelijk is de middelen kan organiseren die bij die verantwoordelijkheid horen. Wie moet leveren zonder te kunnen beslissen, is afhankelijk van de aandacht van anderen.

In 51% van de respondenten zijn de verantwoordelijke en de beslisser niet dezelfde persoon. In 49% van de gevallen is dit wel het geval.



Ik geloof heilig dat je je directie mee moet hebben, anders ben je reddeloos verloren.

JURY BRANTENAAR, IT SERVICE MANAGER BIJ BUMASTEMRA (DIEPTE-INTERVIEW)

TAKE AWAY

Bij 51% van de organisaties zijn de verantwoordelijke en de beslisser niet dezelfde persoon; bij de CISO loopt dat op tot drie op de vijf. Verantwoordelijkheid laat zich makkelijker delegeren dan beslissingsmacht.

Waarom management-betrokkenheid achterblijft

In hoofdstuk 1 scoorde managementbetrokkenheid het laagst van de zeven dimensies (2,73). Tegelijk heeft 90% van de organisaties een CISO of ISM in huis. Hoe kunnen die twee samengaan?

Omdat de rol wel is belegd, maar het mandaat niet. De expert blijft in de operationele laag hangen, terwijl de besluitvorming een niveau hoger plaatsvindt.

Dat is zichtbaar in de cijfers van dit onderzoek. De CISO is verantwoordelijk in een op de vijf organisaties, maar neemt het aanschafbesluit in nog geen een op de zes. Waar de verantwoordelijke niet zelf beslist, gaat het besluit vrijwel altijd omhoog: naar de CTO, de CIO of de directie.

De expert signaleert en adviseert, maar de afweging tussen risico en investering wordt een niveau hoger gemaakt, aan een tafel waar de expert niet altijd aan zit. Zo kan een organisatie een CISO hebben én een laag betrokken management: de rol vult de bestuursstafel niet vanzelf.

TAKE AWAY

Een CISO of ISM in huis is waardevol, maar betekent niet automatisch dat het bestuur betrokken is: de rol is belegd, het mandaat vaak nog niet. Een logische eerste stap is daarom de positie van de verantwoordelijke te versterken, zodat security ook op bestuursniveau landt.

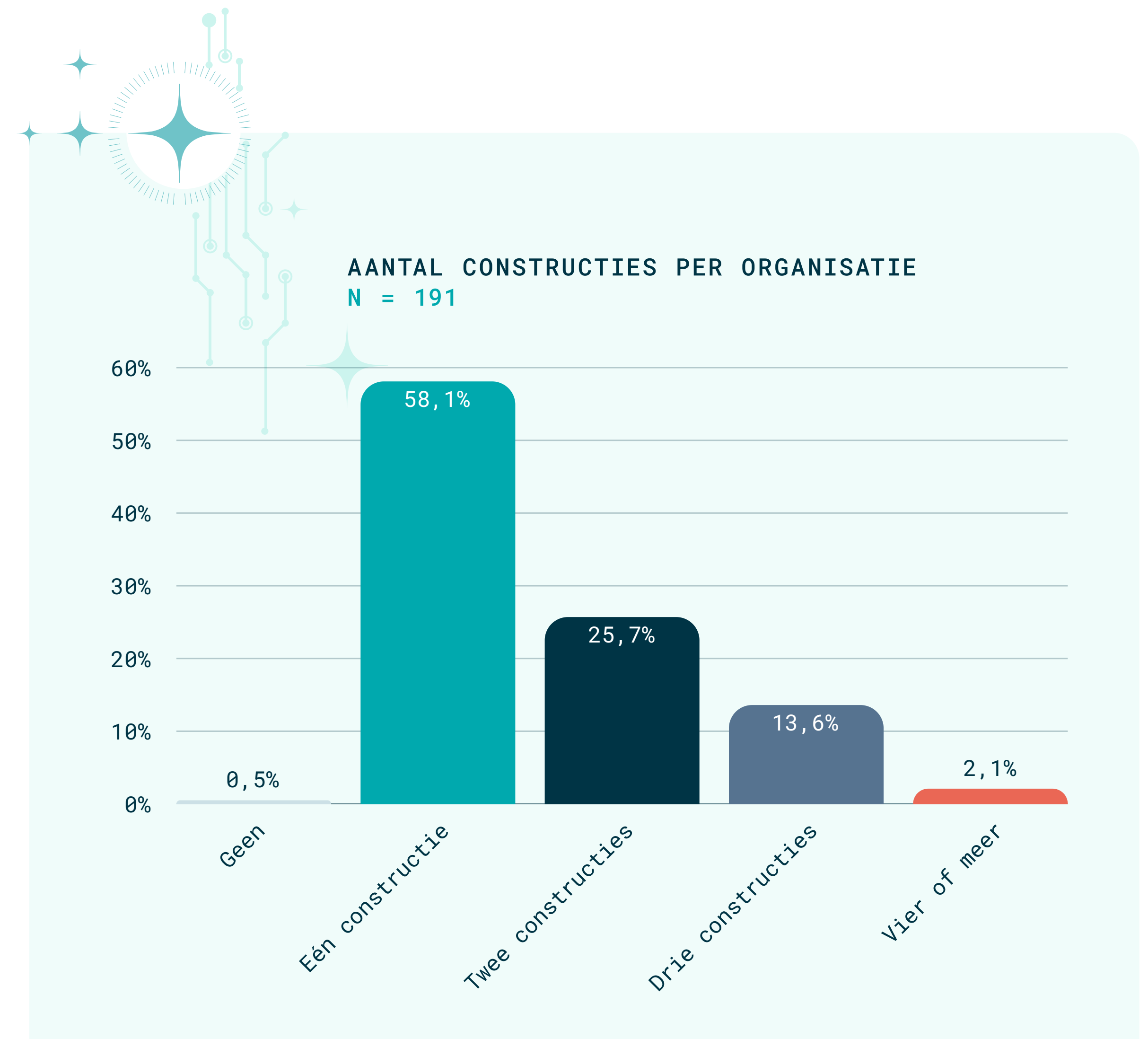
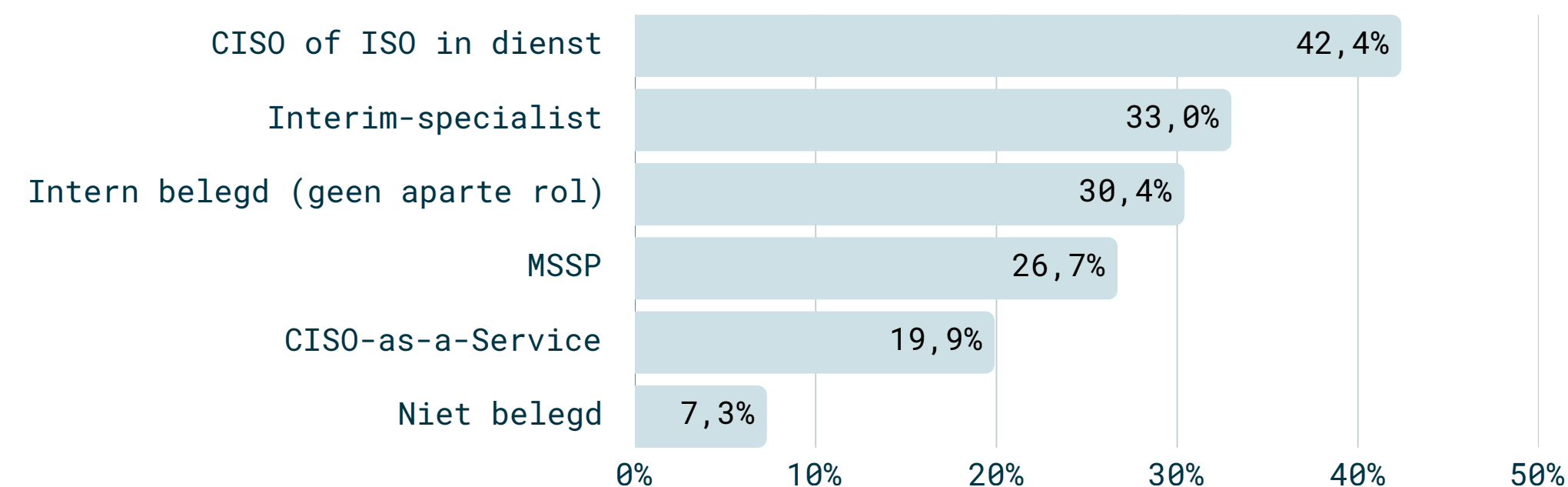


Regieorganisatie in de praktijk

Op welke manier is security in de organisatie belegd? Dat noemen we in dit rapport een 'constructie'. Denk aan: een eigen CISO of ISO in dienst, een interimspecialist, een uitbestede dienst (een MSSP of CISO-as-a-Service), of een bestaande interne rol die security erbij doet zonder aparte functie.

Deze vormen sluiten elkaar niet uit. Het figuur rechts laat zien hoeveel constructies organisaties combineren: opgeteld heeft 41,4% er twee of meer (25,7% + 13,6% + 2,1%) en 15,7% zelfs drie of meer. Omdat in het onderste figuur meerdere antwoorden mogelijk waren, telt die op tot boven de 100%.

HOE IS DE REGIE OP SECURITY GEORGANISEERD?



TAKE AWAY

Er is geen constructie waarmee u van de regie af bent. Zelf doen of uitbesteden, iemand moet het blijven organiseren.

Hoe combinaties ontstaan

De survey zegt niet hoe deze combinaties van constructies ontstaan; de parallelle kwalitatieve interviews wel. Het patroon: constructies worden in de loop van de tijd toegevoegd, niet vooraf ontworpen.

IT doet security erbij, een CISO komt erbij wanneer dat tekortschiet, een interim voor een specifiek programma, daarna een MSSP voor operationele dekking.



Ze challengen ons. Wij kunnen ook kritisch zijn op hen. Waardoor we allebei zorgen dat het steeds beter wordt.

PASCAL PRINS, DIRECTEUR FINANCIEN & INFORMATIEMANAGEMENT BIJ
WIJ ZIJN JONG



Financieringsmodellen voor security

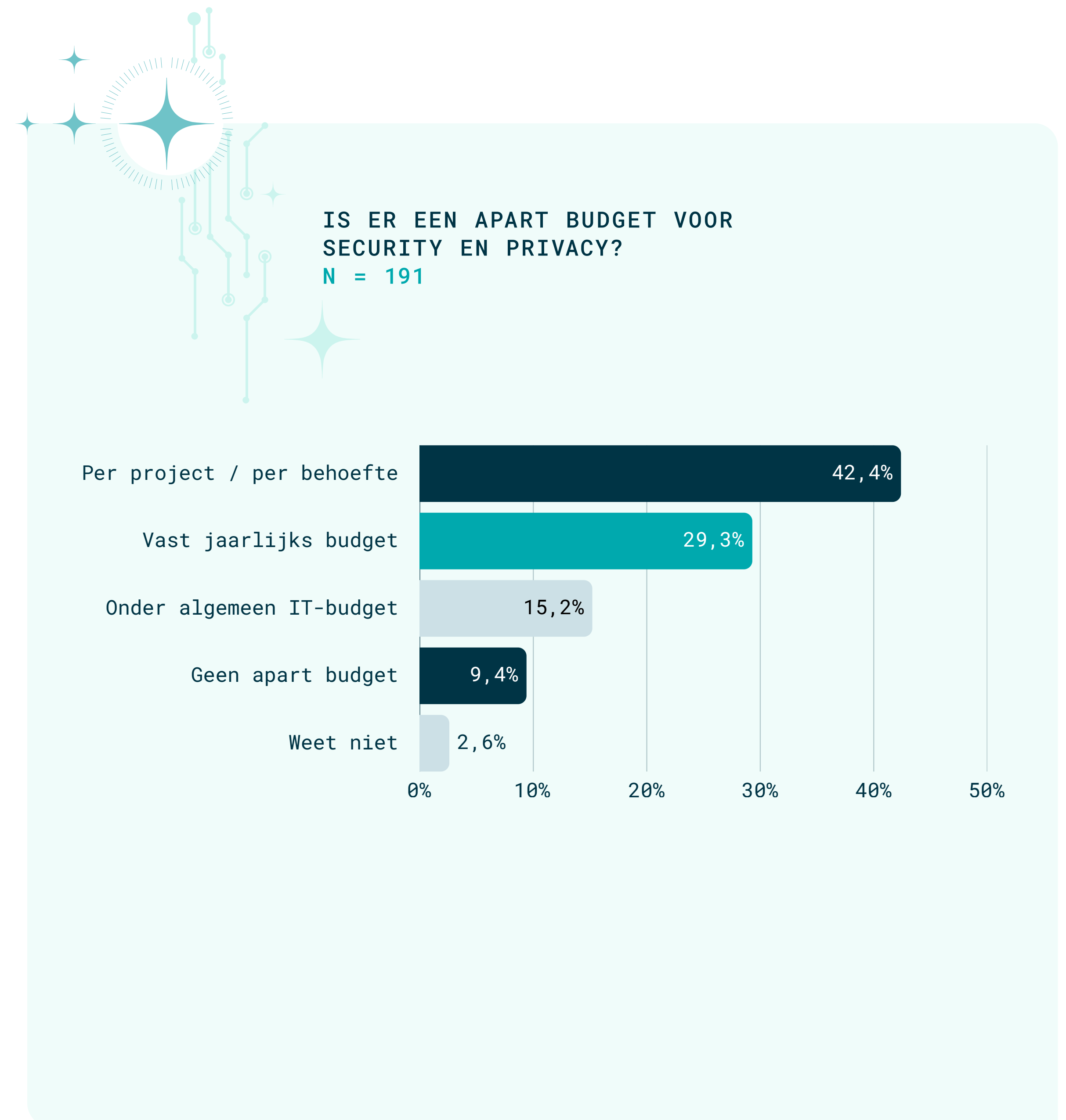
We vroegen organisaties of er een apart budget is voor security en privacy. De grafiek hiernaast toont de antwoorden.

De grootste groep (42,4%) heeft wel budget, maar niet structureel: er wordt geld vrijgemaakt per project of per behoefte, bijvoorbeeld na een incident, een audit of een nieuwe compliance-eis. Nog geen drie op de tien organisaties (29,3%) hebben een vast jaarlijks budget voor security. Bij de rest valt security onder het algemene IT-budget of is er helemaal geen apart budget.

Dat verschil is relevant. Een project heeft een begin en een einde, maar veel securitywerk heeft dat niet: monitoring, beheer en het bijhouden van risico's lopen altijd door. Wie dat doorlopende werk uit losse projectpotjes betaalt, moet er telkens opnieuw geld voor vrijmaken, en dat maakt security afhankelijk van de aanleiding van het moment.

TAKE AWAY

De grootste groep (42%) maakt geld vrij per project of per behoefte. Terwijl veel securitywerk (monitoring, beheer, risico's bijhouden) juist doorloopt. Zo lijkt het budget de aanleiding te volgen, in plaats van het risico.



DEEL III

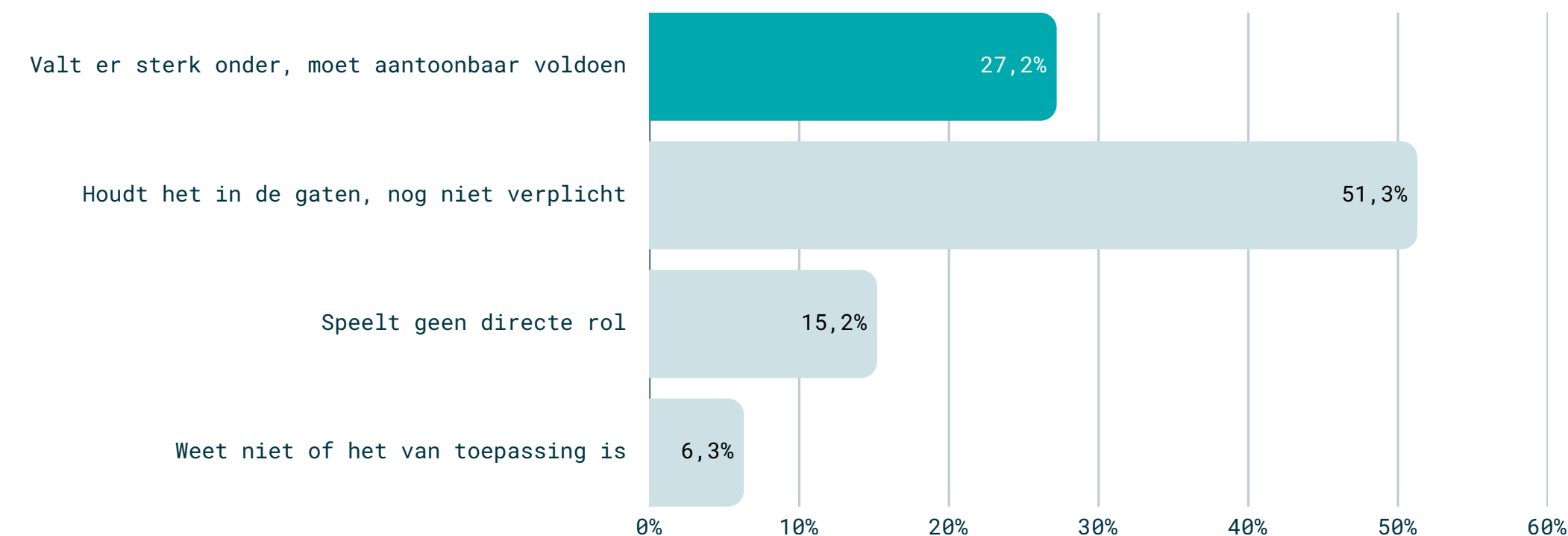
Aantonen en leren

NIS2 en incidenten: wat organisaties moeten aantonen,
en wat ze ervan leren.

NIS2: wettelijk verplicht, lang niet altijd aantoonbaar

NIS2 verplicht organisaties niet alleen om maatregelen te nemen, maar ook om aantoonbaar te voldoen. We onderzochten dat daarom in twee stappen: wie valt er onder de richtlijn, en kan die groep het ook aantonen?

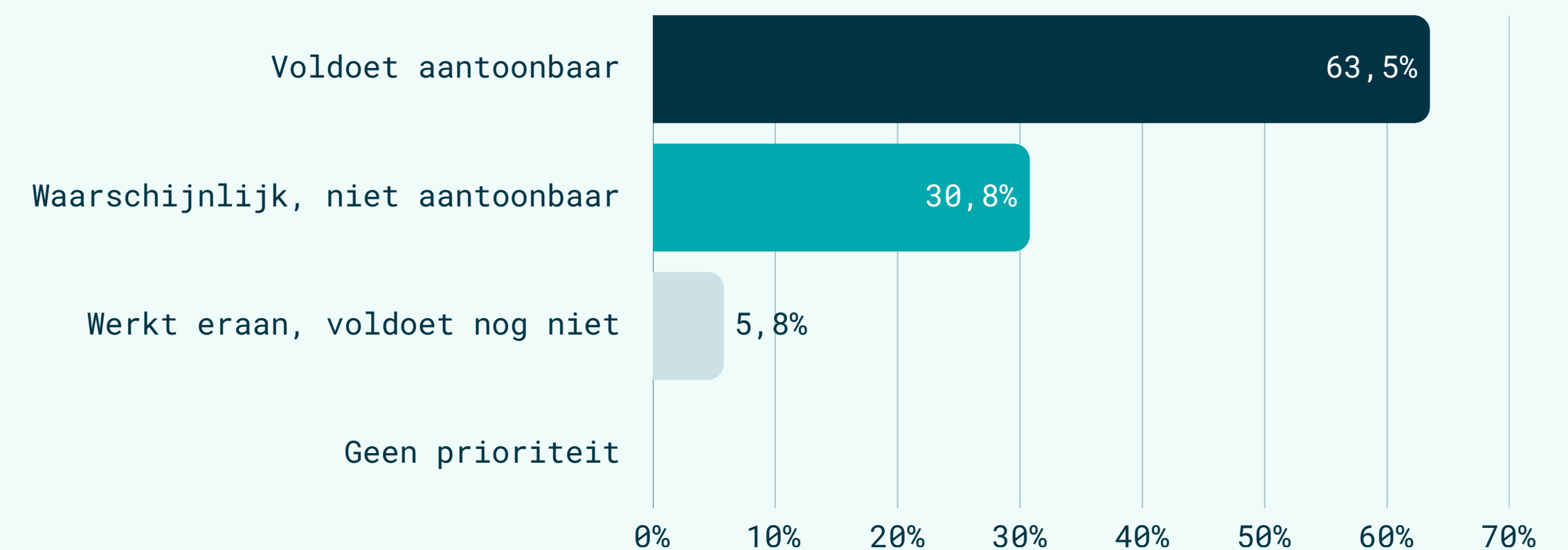
SPEELT NIS2 EEN ROL IN UW SECURITYPRIORITEITEN? (N = 191)



Ruim een kwart (27,2%) zegt er sterk onder te vallen en aantoonbaar te moeten voldoen. Voor die groep is aantoonbaarheid geen keuze maar een wettelijke eis. De vraag is of ze het ook waarmaken.



VOLDOET UW ORGANISATIE AANTOONBAAR AAN DE REGELGEVING?
N = 52, ORGANISATIES DIE STERK ONDER NIS2 VALLEN. ZELFRAPPORTAGE, GEEN AUDIT.



TAKE AWAY

Opgeteld kan ruim een derde (36,5%) van de organisaties die aantoonbaar móeten voldoen, dat op dit moment naar eigen zeggen niet. De wettelijke plicht ligt er; de bewijslast is nog niet ingevuld.

Ervaring met securityincidenten

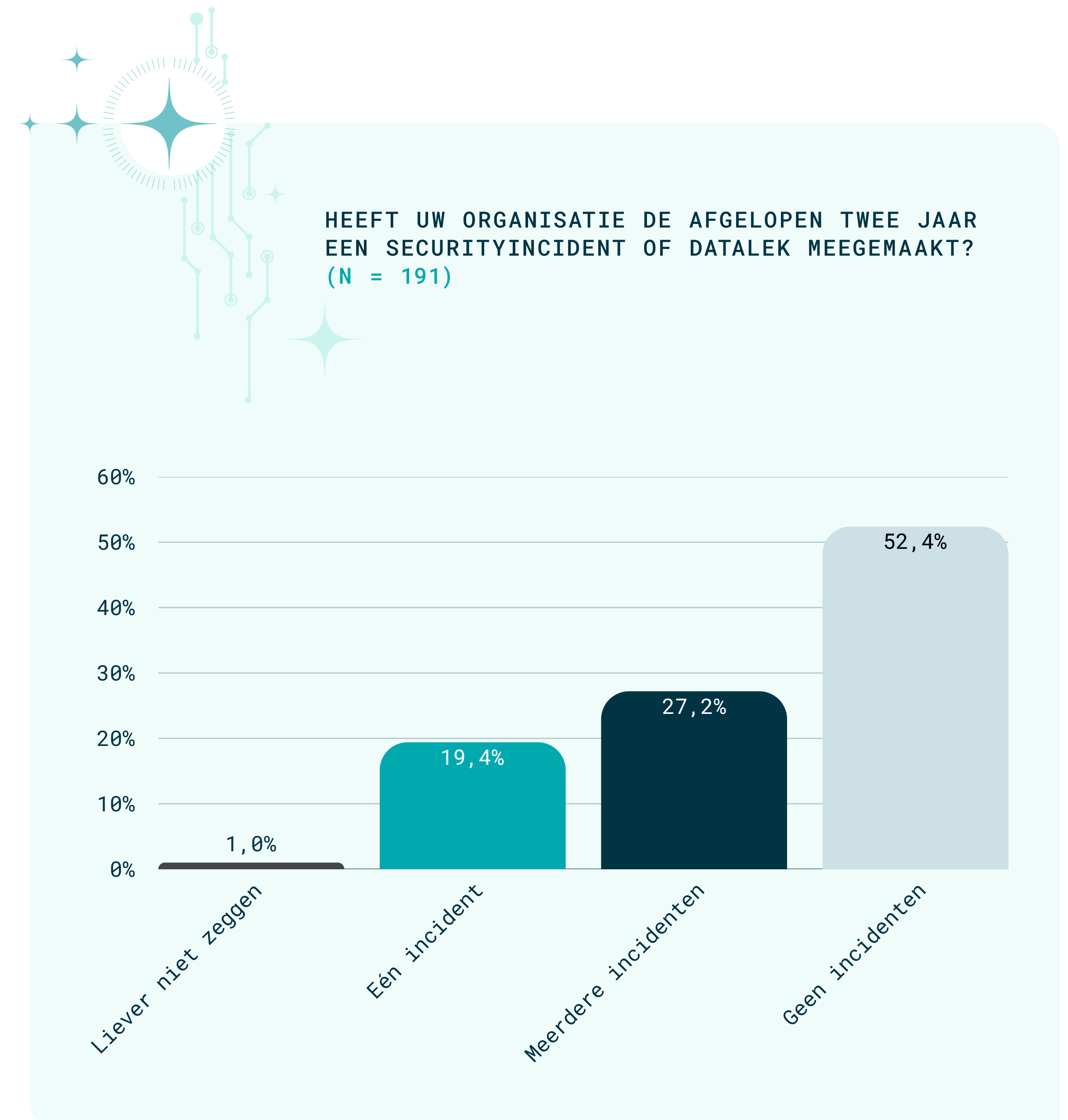
We stelden twee vragen rond incidenten: heeft uw organisatie de afgelopen twee jaar een securityincident of datalek meegemaakt, en herkent u de stelling “na een (bijna-) incident weten we niet goed hoe we structureel moeten verbeteren”?

Tellen we de respondenten met één incident (19,4%) en die met meerdere incidenten (27,2%) bij elkaar op, dan komt bijna de helft (46,6%) uit op minstens één incident. De volledige verdeling staat in de figuur.

De vraag is vooral wat organisaties met die ervaring doen. Daar zit een knelpunt: ruim een derde van alle respondenten (36%) herkent de stelling dat ze na een (bijna-)incident niet goed weten hoe structurele verbeteringen door te voeren. In een markt waar bijna de helft inmiddels uit eigen ervaring spreekt, betekent dat dat incidenten lang niet overal leiden tot blijvende aanpassingen in beleid, processen en verantwoordelijkheden.

TAKE AWAY

Een incident meemaken is niet hetzelfde als ervan leren. Twee losse cijfers tekenen hetzelfde beeld: bijna de helft (46,6%) heeft een incident meegemaakt, en ruim een derde (36%) weet niet hoe daarna structureel te verbeteren.



Operationeel leren versus structureel leren

Een incident wordt in de meeste organisaties wel opgelost. Systemen komen terug, de schade wordt beperkt, de dagelijkse gang van zaken herstelt. Dat is operationeel leren: het probleem van vandaag is weg.

Structureel leren is een tweede: de vraag of het incident ook leidt tot aanpassingen in beleid, processen en verantwoordelijkheden. Op de stelling "na een (bijna-)incident weten we niet goed hoe we structurele verbeteringen moeten doorvoeren" antwoordt 36% van de respondenten bevestigend. 43% herkent de stelling niet, 20% is neutraal. Ruim een derde weet dus wel dat er iets moet veranderen, maar niet hoe.

Opvallend: onder organisaties die daadwerkelijk een incident hebben meegemaakt, ligt de herkenning hoger (42%) dan onder organisaties zonder die ervaring (30%). Wat dat verschil verklaart, zegt het onderzoek niet. Het kan zijn dat ervaring realistischer maakt over hoe moeilijk structureel verbeteren is.

TAKE AWAY

Een incident wordt pas een leerproces als iemand met mandaat de evaluatie leidt. Zonder die persoon blijft de verbetering technisch, en verdwijnt de les met het incident.



WAT HELPT OM VAN EEN INCIDENT EEN LEERPROCES TE MAKEN? VANUIT ONZE EIGEN PRAKTIJK ZIEN WE DRIE ELEMENTEN TERUGKOMEN:

1 · BESTUURLIJKE EVALUATIE

De evaluatie van een incident wordt op bestuurlijk niveau besproken, niet alleen technisch of operationeel.



2 · RISK REGISTER

Conclusies landen in een riskregister dat periodiek wordt herzien.



3 · GEMONITORDE OPVOLGING

De opvolging wordt bewaakt door iemand met bestuurlijk mandaat.



DEEL IV

Wat het middensegment zoekt

Van bezwaar naar behoefte: wat het middensegment
eigenlijk vraagt.

Regie willen houden

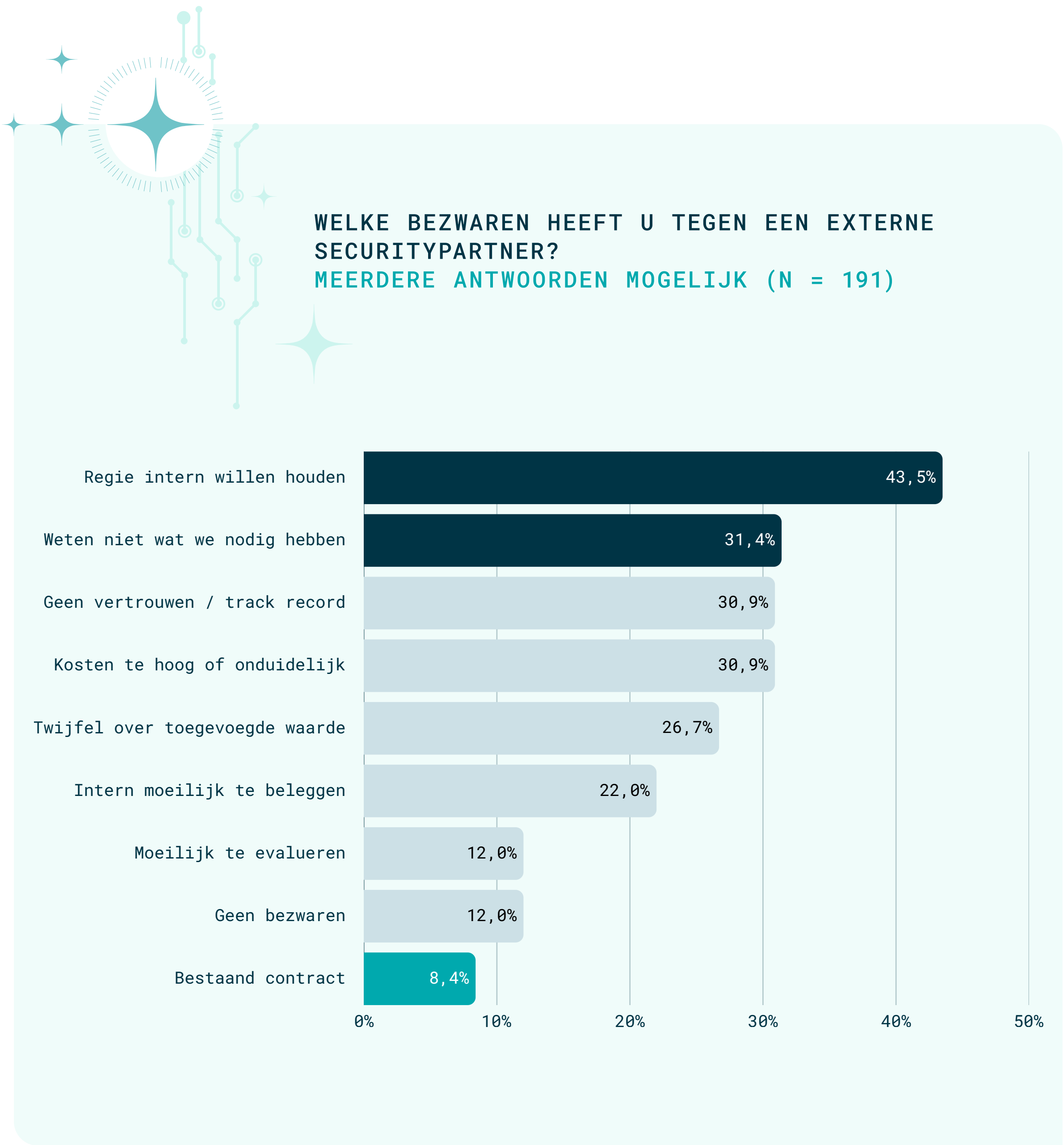
We vroegen welke bezwaren organisaties hebben tegen een externe securitypartner; meerdere antwoorden waren mogelijk. Het vaakst genoemd: de regie intern willen houden (43,5%). Dat is begrijpelijk, want security raakt de kern van de bedrijfsvoering.

De bezwaren daaronder gaan over iets anders: niet precies weten wat de organisatie nodig heeft (31,4%) en twijfel over externe partijen (30,9%) zijn geen kostenkwesties, maar onzekerheid over de eigen positie. Slechts 12% heeft géén bezwaren. Vrijwel iedereen die over externe hulp nadenkt, worstelt met dezelfde vraag: wat geeft u uit handen, en wat houdt u zelf?

Zeggenschap weegt daarmee zwaarder dan kosten of wantrouwen. De opgave is geen keuze tussen zelf doen of loslaten, maar het vinden van een partner die versterkt in plaats van vervangt.

TAKE AWAY

Het grootste bezwaar tegen externe hulp is niet de prijs, maar de regie (43,5%). Daarna volgt onzekerheid over de eigen behoefte (31,4%). Versterken mag; overnemen niet.



Regie houden én goed geholpen worden

Regie willen houden is logisch en gezond: security raakt de kern van de bedrijfsvoering. Maar regie houden en externe versterking sluiten elkaar niet uit.

De verdiepingsinterviews laten zien waarom. Wie de kennis in huis haalt, is daarmee niet klaar: één specialist is kwetsbaar bij ziekte, vakantie of vertrek, en kan niet alle disciplines dekken. Wie het uitbesteedt, is ook niet klaar: leveranciers aansturen, prioriteiten stellen en de samenhang bewaken blijft werk dat binnen de organisatie moet gebeuren.

De opgave is dus geen keuze tussen zelf doen of loslaten, maar het vinden van een partner die versterkt in plaats van vervangt. Een partner die naast u gaat staan, u zelf in de regie laat en u uitdaagt waar het moet.

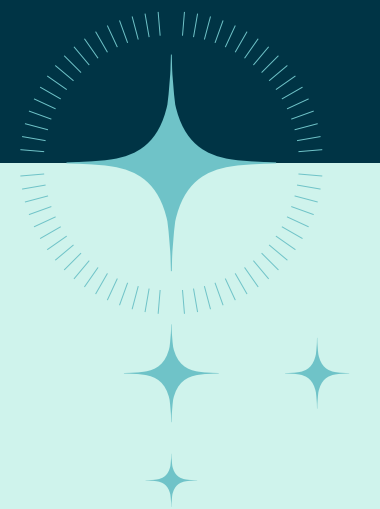
TAKE AWAY

Regie houden en externe hulp inschakelen sluiten elkaar niet uit. De opgave is niet kiezen tussen zelf doen of loslaten, maar een partner vinden die versterkt in plaats van vervangt, en u in de regie laat.



Je kan die kennis natuurlijk in huis halen, maar met één persoon ben je nog steeds kwetsbaar.

RONALD VAN ISSELT, MANAGER BEDRIJFSVOERING BIJ ALWEL (DIEPTE-INTERVIEW)



Je kunt security of privacy outsourcen, maar je moet het nog steeds zelf organiseren.

ALEXANDER PEREIRA, MANAGER INFORMATIEVOORZIENING EN BEDRIJFSVOERING BIJ WOONIN (DIEPTE-INTERVIEW)

Hoe partners gekozen worden

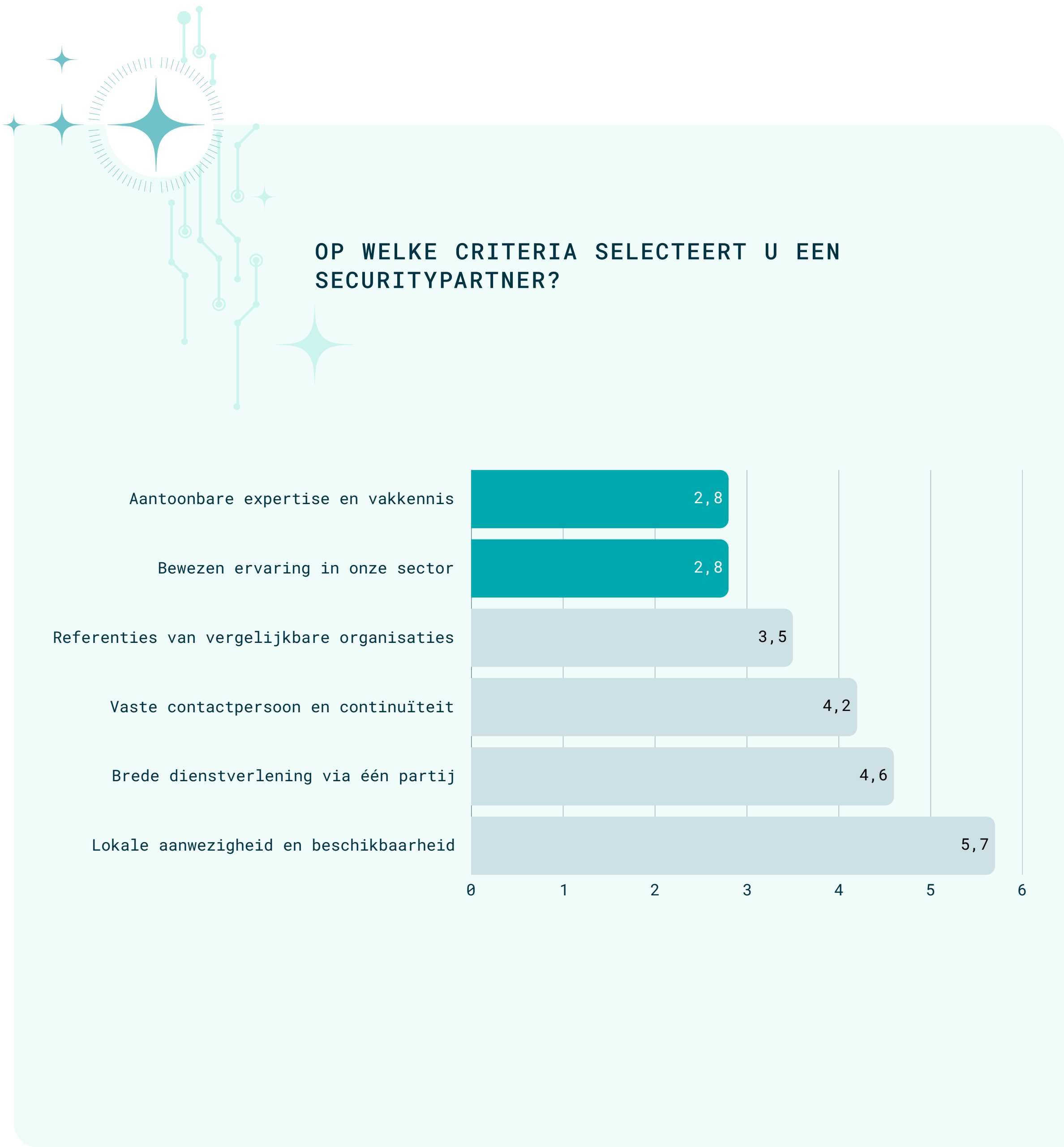
Waarop kiest het middensegment een securitypartner? We legden respondenten zes criteria voor met de vraag ze te ordenen van meest naar minst belangrijk.

De grafiek toont de gemiddelde positie per criterium: hoe lager het getal, hoe belangrijker het criterium werd gevonden.

Aantoonbare expertise en bewezen sectorervaring eindigen vrijwel gelijk bovenaan (2,75 en 2,77). Daarna volgen referenties van vergelijkbare organisaties (3,45). Een vaste contactpersoon (4,17), brede dienstverlening via één partij (4,64) en lokale aanwezigheid (5,72) sluiten de rij.

TAKE AWAY

Wat een partij aantoonbaar kan, weegt zwaarder dan wat de samenwerking comfortabel maakt. Expertise en sectorervaring geven de doorslag; één loket en lokale aanwezigheid nauwelijks.



Voorkeur voor Nederlandse of Europese partner

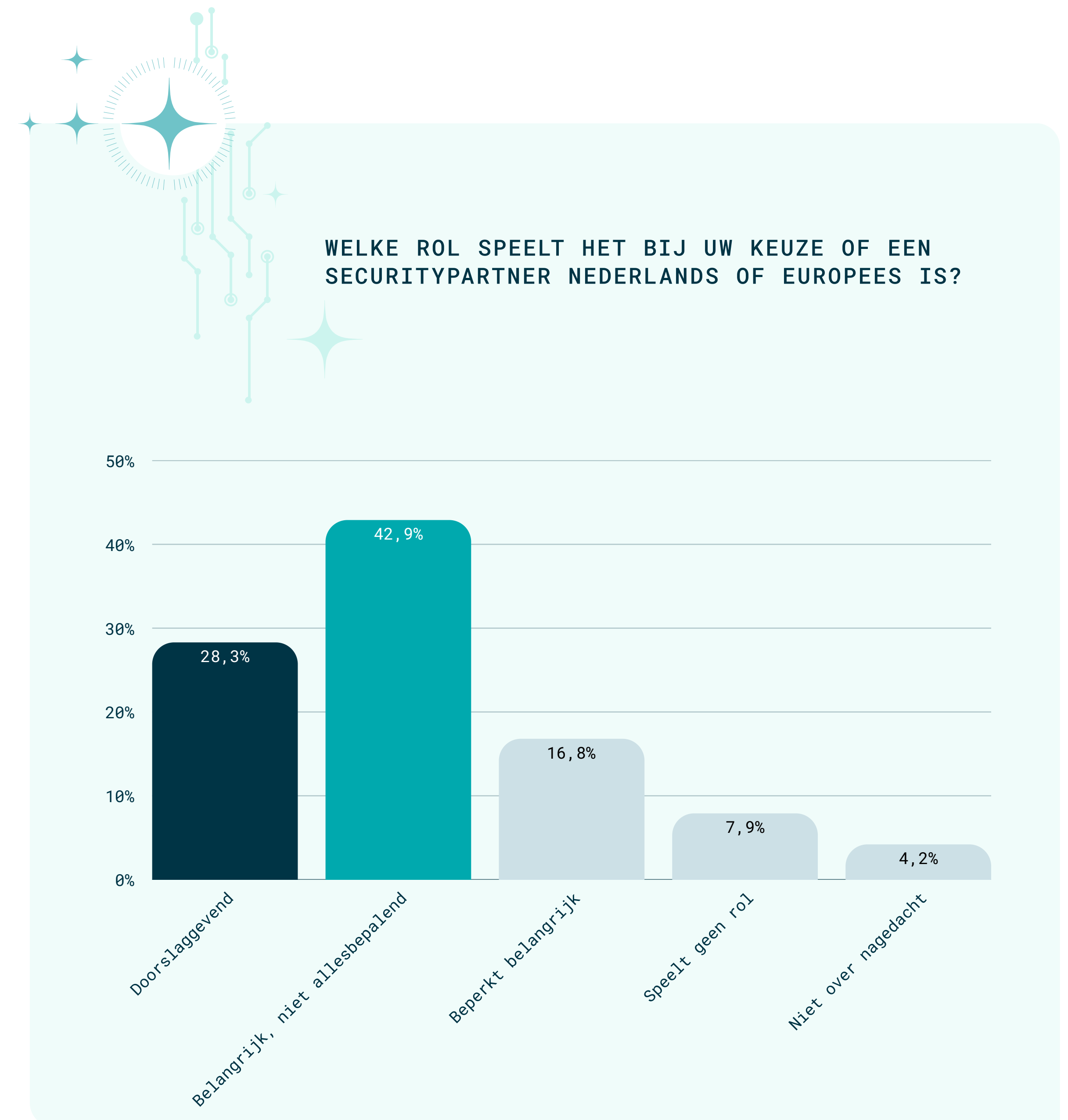
We vroegen organisaties welke rol het bij hun keuze speelt of een securitypartner Nederlands of Europees is.

Voor ruim een kwart (28,3%) is het doorslaggevend: een niet-Nederlandse of niet-Europese partij valt af. De grootste groep (42,9%) vindt het belangrijk, maar niet allesbepalend. Voor 16,8% speelt het alleen een rol als andere criteria gelijk zijn, 7,9% kiest puur op kwaliteit en prijs, en 4,2% heeft er nog niet bewust over nagedacht.

Herkomst is daarmee voor een ruime meerderheid een factor in de keuze, en voor ruim een kwart zelfs een harde eis.

TAKE AWAY

Voor 71,2% weegt herkomst mee in de keuze, voor 28,3% is het een harde eis. Slechts 7,9% kijkt puur naar kwaliteit en prijs.



Waar het middensegment staat

Tel alle bevindingen bij elkaar op, en u komt terug bij waar dit rapport begon: security is wél geregeld, maar nog niet bestuurd. Dat is precies wat een volwassenheidsonderzoek zichtbaar maakt en het cijfer bevestigt het: alle zeven dimensies vallen tussen 2,73 en 2,98. De basis staat, de borging nog niet. Wat die borging in de weg staat, laat zich in drie cijfers vangen.

Mandaat: 51% · Bij de helft van de organisaties beslist een ander dan de verantwoordelijke over de aanschaf; bij de CISO zelfs 61%. De rol is belegd, het mandaat niet: management-betrokkenheid scoorde met 2,73 dan ook het laagst van alle zeven dimensies.

Budget: 29% · Nog geen drie op de tien heeft een vast jaarlijks securitybudget. De rest financiert per project of per behoefte; zo volgt het geld de aanleiding in plaats van het risico.

Regie: 41% · Vier op de tien combineert twee of meer constructies, meestal in de loop van de tijd gegroeid in plaats van vooraf ontworpen. Wie het geheel bestuurt, is lang niet altijd aangewezen.

TAKE AWAY

Waar het middensegment staat, is nu duidelijk. De volgende stap gaat niet over organiseren, maar over besturen: de top structureel betrekken en mandaat geven aan wie de regie voert. Dat gesprek begint met vijf vragen aan de eigen tafel.



TOT BESLUIT

Reflectievragen voor uw organisatie

Wat dit betekent voor uw organisatie

Vijf reflectievragen om aan de eigen tafel te stellen.

U hebt gezien waar het middensegment staat. De vraag is waar uw organisatie staat. Hieronder de vijf onderdelen uit het onderzoek (mandaat, bestuur, aantoonbaarheid, budget en regie) vertaald naar het gesprek aan uw eigen tafel.

Deze vijf punten zijn niet in één beweging op te lossen, en de volgorde verschilt per organisatie. Wat wij in de praktijk zien: organisaties die hier in groeien, zijn stap voor stap begonnen. Bij het onderdeel waar intern al de meeste aandacht voor is.

1

Wie beslist bij ons over de aanschaf van security?

Wie neemt daadwerkelijk het definitieve aanschafbesluit? En weet die persoon dat dit diens rol is?

2

Hoe vaak komt security op de bestuursagenda?

Structureel, of alleen als er iets is? Het verschil tussen een organisatie die security elk kwartaal bespreekt en een die het alleen na een incident doet, is fundamenteel.

3

Hebben we onze compliance daadwerkelijk aantoonbaar belegd?

Niet of we voldoen, maar of we het kunnen aantonen. Wat zou u laten zien aan een toezichthouder die morgen aan de deur staat?

4

Hoe is ons securitybudget opgebouwd?

Per project, vast jaarlijks, onder IT, of niet zichtbaar? En past die structuur bij de continue aard van het werk dat we van security verwachten?

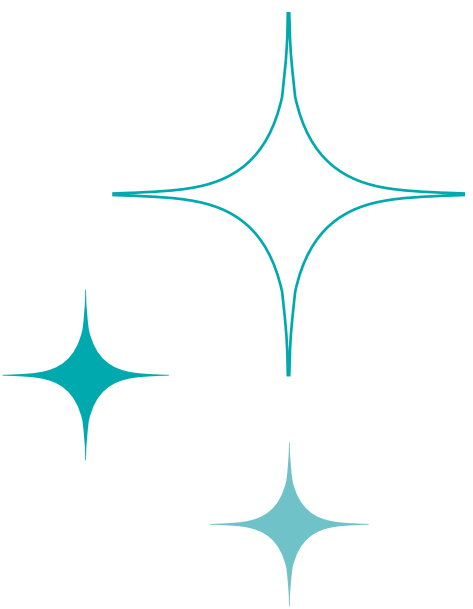
5

Wie houdt bij ons de regie over de samenstelling van security?

Als we meerdere constructies hebben, wie zorgt dan dat ze samenwerken in plaats van langs elkaar heen? En heeft diegene het mandaat om in te grijpen?

SLOTWOORD

Streep door wat u moeiteloos kon beantwoorden. Daar heeft u grip. Wat overblijft is uw gesprek. Blijven er meerdere over, kies dan niet het belangrijkste, maar datgene waarover intern al het vaakst over gesproken wordt. Daar zit de energie al, en daar is een klein stapje het snelst een zichtbaar verschil.



Verantwoording en bijlagen

Het onderzoek is uitgevoerd in mei-juni 2026 onder Nederlandse organisaties met 100 tot 1.000 medewerkers. De vragenlijst werd online afgenomen via een onderzoekspanel. De totale respons bedroeg 191 volledig ingevulde vragenlijsten; het aantal unieke organisaties daarachter is niet afzonderlijk vastgesteld. Nederland telt circa 7.000 tot 7.500 organisaties in deze grootteklasse (CBS), waarmee voor de totaalcijfers een indicatieve foutmarge van circa 7 procentpunten geldt.

Beperkingen

- Slechts 6% van de respondenten was zelf CISO of ISM. Het onderzoek beschrijft de securityorganisatie dus overwegend door de ogen van directie en IT-management.
- Het onderzoek beschrijft perceptie en gerapporteerd gedrag, geen feitelijk gedrag. De zelfinschatting in hoofdstuk 1 is een goed voorbeeld van een dimensie waar perceptie en realiteit kunnen afwijken.
- De uitkomsten gelden voor organisaties met 100 tot 1.000 medewerkers en zijn niet zonder meer te vertalen naar het mkb daaronder of enterprises daarboven. Omdat deelname vrijwillig was, zijn organisaties die actief met security bezig zijn mogelijk oververtegenwoordigd. Deelanalyses op kleinere groepen zijn indicatief.

Over de uitvoerder

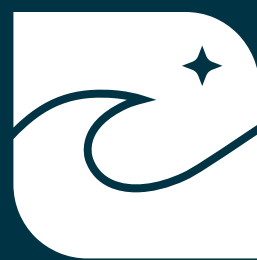
Beyond Products is een Nederlands marketing- en onderzoeksbureau voor de security- en IT-sector.



Het maturitymodel

DIMENSIE	1 · AD HOC	2 · BASIS	3 · REGIE & STRATEGIE	4 · GEÏNTEGREERD
Security awareness	Nauwelijks of niet. Bewustzijn ontstaat hooguit na een incident.	Ad hoc, bijvoorbeeld via een jaarlijkse training of phishingtest, zonder structureel programma.	Er is een structureel bewustzijnsprogramma dat aansluit op actuele dreigingen en wordt gemonitord op effectiviteit.	Securitybewustzijn zit ingebed in onboarding, processen en leiderschap. Gedrag en cultuur zijn onderdeel van de strategie.
Securitybeleid	Er is geen beleid. Security wordt ad hoc opgepakt als er iets misgaat.	Er is basisbeleid, maar het leeft op papier en wordt niet consequent toegepast.	Beleid is actueel, gekoppeld aan risico's en verantwoordelijkheden zijn vastgelegd. We reviewen periodiek en sturen bij.	Beleid leeft in de organisatie, wordt continu onderhouden en is volledig ingebed in de besturing van de organisatie.
Incident response	Incidenten worden beperkt herkend, niet geregistreerd en technisch opgelost zonder helder proces.	Er is een incidentproces, maar het is reactief. Registratie gebeurt, maar analyse en structurele verbetering zijn beperkt.	Incidenten worden geanalyseerd en gebruikt om processen te verbeteren, in samenwerking tussen security en IT.	Incidenten leiden structureel tot verbeteringen en oefeningen. Nieuwe dreigingen resulteren direct in nieuwe maatregelen.
Technische maatregelen	Basismaatregelen ontbreken grotendeels of zijn onvolledig. Er is geen samenhang tussen oplossingen.	Basismaatregelen zijn aanwezig, bijvoorbeeld endpointbescherming, MFA en antivirus, maar reactief gekozen en nog niet goed geïntegreerd.	Tooling is bewust gekozen op basis van samenhang, beheersbaarheid en risico's, en ondersteunt beleid en processen.	Securitytechnologie is strategisch gekozen en ondersteunt actief governance, monitoring en besluitvorming.
Rollen & regie	Rollen zijn onduidelijk. Security is versnipperd over teams zonder centrale regie.	Er zijn informele afspraken over verantwoordelijkheden, maar deze zijn persoonsafhankelijk en niet geborgd in processen.	Rollen zijn vastgelegd en samenwerking tussen teams, leveranciers en disciplines is georganiseerd.	Regie verbindt alle disciplines: beleid, monitoring, privacy en human risk zijn volledig geïntegreerd.
Compliance & risico	We hebben weinig zicht op verplichtingen en risico's. Compliance krijgt geen structurele aandacht.	Compliance krijgt wel aandacht, maar vooral als afvinklijst. Risicoanalyses worden incidenteel uitgevoerd.	Compliance en risicomanagement zijn structureel ingericht en vertaald naar beleid en controls.	We anticiperen proactief op nieuwe regelgeving. Compliance ondersteunt onze continuïteit en reputatie strategisch.
Managementbetrokkenheid	Security staat nauwelijks op de agenda, tenzij er een incident of verplichting is.	Management is betrokken op hoofdlijnen, maar security is geen structureel onderdeel van bestuurlijke besluitvorming.	Bestuur is actief betrokken. Security staat periodiek op de agenda en is gekoppeld aan risico's en investeringsbeslissingen.	Bestuur is aanjager van security. Er zijn structurele overleggen en duidelijke besluitvorming op strategisch niveau.
Securitytechnologie & tooling	Versnipperde oplossingen zonder samenhang. Basismaatregelen ontbreken of zijn onvoldoende ingericht.	Basismaatregelen en tooling ingericht, maar reactief gekozen en beperkt geïntegreerd.	Tooling ondersteunt beleid, risico's en processen; bewust gekozen op samenhang en beheerbaarheid.	Technologie strategisch gekozen en geïntegreerd; ondersteunt governance, monitoring en besluitvorming.





NORTHWAVE
CYBER SECURITY

Need help now?
Call day or night: 00800 1744 0000

E: info@northwave-cybersecurity.com

T: +31 (0) 30 303 1240

W: [northwave-cybersecurity.com](https://www.northwave-cybersecurity.com)

This report is disclosed under the Traffic Light Protocol (TLP):CLEAR. Recipients can spread this outside their organisation, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction For further information, see: <https://www.first.org/tlp/>.

