Cybertrends-rapport 2026

Mkb niet klaar voor nieuwe digitale risico's

ABN·AMRO

Mkb niet klaar voor nieuwe digitale risico's

Minder Nederlandse bedrijven werden vorig jaar geraakt door cyberincidenten en ook het aandeel organisaties dat schade ondervond, daalde. Toch is dat geen reden tot geruststelling. Vooral kleinere bedrijven zijn nog onvoldoende voorbereid op een nieuwe generatie digitale risico's, zo blijkt uit nieuw onderzoek van ABN AMRO in samenwerking met marktonderzoeksbureau MWM2 onder 777 Nederlandse organisaties.

Zo vergroot artificial intelligence (AI) de cyberdreiging doordat kwaadwillenden deze technologie inzetten en doordat datalekken ontstaan na onzorgvuldig gebruik van externe AI-tools als ChatGPT en Claude. Bijna een derde van het midden- en kleinbedrijf (mkb) maakt zich zorgen over medewerkers die gevoelige informatie met zulke assistenten delen. Tegelijk gebruikt 78 procent van deze organisaties – met een jaaromzet tot 25 miljoen euro – in enige mate AI, terwijl passende beheersmaatregelen vaak ontbreken: slechts 9 procent heeft formeel beleid voor het gebruik van externe AI-oplossingen, tegenover 32 procent van de grote bedrijven.

In het mkb ontbreekt vaak een actueel beeld van kwetsbaarheden; nauwelijks een derde van de organisaties voerde het afgelopen jaar een risicoscan uit. Bij grootbedrijven deed iets meer dan de helft dat. Ook de basis om cyberincidenten goed op te vangen is bij veel mkb-bedrijven nog niet op orde. Dat is risicovol, zeker nu AI aanvallen versnelt en de reactietijd voor organisaties verkort. Slechts 26 procent heeft een formeel responsplan voor cyberincidenten, tegenover 49 procent van het grootbedrijf, en 43 procent van de mkb'ers heeft nog nooit een cyberaanval geoefend. Bovendien investeert het grootbedrijf een veel hoger percentage van de omzet in cybersecurity en heeft het veel vaker afspraken met ketenpartners gemaakt over digitale veiligheid dan het mkb.

Tegelijk laten de cijfers zien dat organisaties op sommige punten wel degelijk vooruitgang boeken. Het aandeel bedrijven dat een cyberincident meemaakte, is gedaald. Die afname komt vooral uit het mkb, waar het aandeel getroffen bedrijven terugliep van 72 naar 60 procent. Ook onder zzp'ers nam dit aandeel af, van 57 naar 48 procent. Bij grotere organisaties was die daling al een jaar eerder ingezet: daar daalde het aandeel getroffen bedrijven eerst van 86 naar 79 procent en dit jaar verder naar 76 procent.

Ook het aandeel bedrijven dat schade leed door een cyberaanval daalde, van 20 naar 15 procent. Die afname komt vooral door het grootbedrijf: daar zakte het percentage organisaties met schade van 29 procent vorig jaar naar 21 procent dit jaar. Bij mkb'ers en zzp'ers was eveneens sprake van een daling, maar minder sterk: van 20 naar 17 procent in het mkb en van 9 naar 6 procent onder zzp'ers. Deze ontwikkelingen zijn bemoedigend en wijzen erop dat organisaties beter grip krijgen op bekende risico's, bijvoorbeeld door investeringen in basishygiëne, e-mailbeveiliging en snellere detectie van verdachte activiteiten.

Maar de dalende cijfers vertellen niet het hele verhaal. Hoewel de mate verschilt, zijn veel organisaties afhankelijk van een klein aantal cloud- en AI-aanbieders. Bijna de helft van de Nederlandse bedrijven ervaart een gedeeltelijke tot zeer grote afhankelijkheid van Amerikaanse tech-bedrijven: 35 procent van de zzp'ers, 46 procent van de mkb'ers en 60 procent van het grootbedrijf. Geopolitieke en juridische factoren vormen een risico voor de beschikbaarheid van buitenlandse digitale diensten.

Organisaties blijken op dit punt niet af te wachten. Bijna twee derde van de mkb'ers (63 procent) neemt al maatregelen om afhankelijkheden en de bijbehorende risico's te verkleinen, vrijwel evenveel als in het grootbedrijf (69 procent). Opvallend is dat 17 procent van de mkb'ers al (deels) is overgestapt op Europese oplossingen, tegenover 12 procent van het grootbedrijf. Dat legt een interessant contrast bloot: grote organisaties beschikken vaak over meer cybervolwassenheid en formele beheersing, maar kleinere bedrijven zijn soms wendbaarder als ze daadwerkelijk moeten schakelen.

Inhoudsopgave

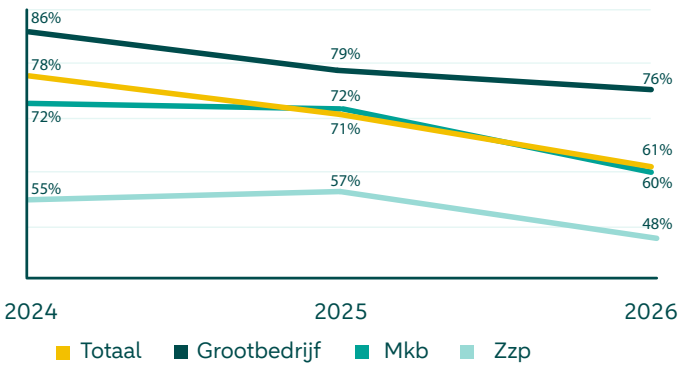
Minder incidenten ondanks onverminderd hoge dreiging

Minder Nederlandse bedrijven werden het afgelopen jaar getroffen door een cyberaanval en ook het aandeel organisaties dat schade leed, nam af. Grote bedrijven lijken incidenten beter te kunnen opvangen dan kleinere.

Twee op de tien bedrijven leden afgelopen jaar schade door een cyberaanval. In het grootbedrijf – met een omzet van meer dan 25 miljoen euro – geldt dit zelfs voor drie op de tienIn de afgelopen twaalf maanden kreeg 60 procent van de mkb'ers te maken met een cyberaanval. Een behoorlijke daling, want een jaar eerder was dit nog 72 procent. Ook bij zzp'ers nam het aantal aangevallen bedrijven af: van 57 procent naar 48 procent. In het grootbedrijf kreeg zo'n driekwart te maken met een cyberincident – een niet-significante daling ten opzichte van het jaar ervoor. Bij deze grotere bedrijven was de daling al een jaar eerder ingezet; tussen 2024 en 2025 zakte het percentage aangevallen bedrijven van 86 naar 79 procent.

Minder bedrijven geraakt door cyberaanval

Percentage van de ondervraagde bedrijven dat in de afgelopen 12 maanden met een cyberaanval te maken heeft gehad.



"De cijfers laten zien dat investeren in basis-hygiëne daadwerkelijk effect heeft", zegt Martijn Dekker, Chief Information Security Officer (CISO) bij ABN AMRO. "Het dreigingsniveau is echter onverminderd hoog."

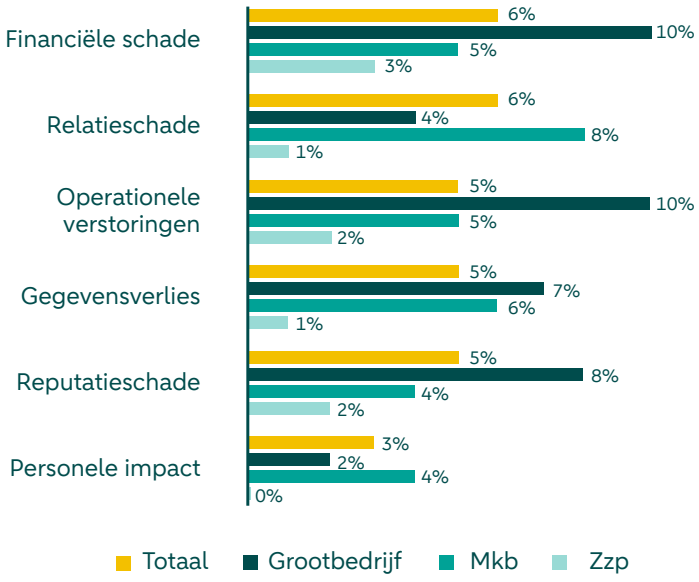
Volgens Jochem Boender, ethisch hacker bij cybersecuritybedrijf ThreadStone, wordt de cybervolwassenheid van organisaties inderdaad hoger. "Technologie helpt hier een hoop. Bedrijven maken bijvoorbeeld steeds meer gebruik van e-mailbeveiliging waardoor phishing-mails überhaupt niet meer in mailboxen binnenkomen, of laten hun apparaten monitoren op verdachte activiteit." In dat laatste geval – ook wel 'endpoint detection and response' (EDR) genoemd – wordt bijvoorbeeld een apparaat automatisch van het netwerk afgesloten als een onveilig bestand wordt gedownload. Door zulke maatregelen wordt een cyberaanval – praktisch ongemerkt – in de kiem gesmoord.

Minder schade

Ook totale percentage bedrijven dat schade ondervond door een cyberincident nam af, van 20 procent naar 15 procent. Het grootbedrijf blijkt het afgelopen jaar beter in staat om schade te voorkomen dan het mkb. Zo leed weliswaar 21 procent van alle grootbedrijven schade, maar een jaar eerder was dit nog 29 procent. Financiële schade en operationele verstoringen werden het vaakst genoemd, gevolgd door reputatieschade. Van de mkb-bedrijven had 17 procent schade, een beperkte afname ten opzichte van de 20 procent een jaar eerder. Relationele schade werd het vaakst werd gemeld, gevolgd door het verlies van gegevens, financiële schade en operationele verstoringen. Zzp'ers bleven vrijwel geheel schadevrij; een klein percentage meldde financiële schade, operationele verstoringen en reputatieschade.

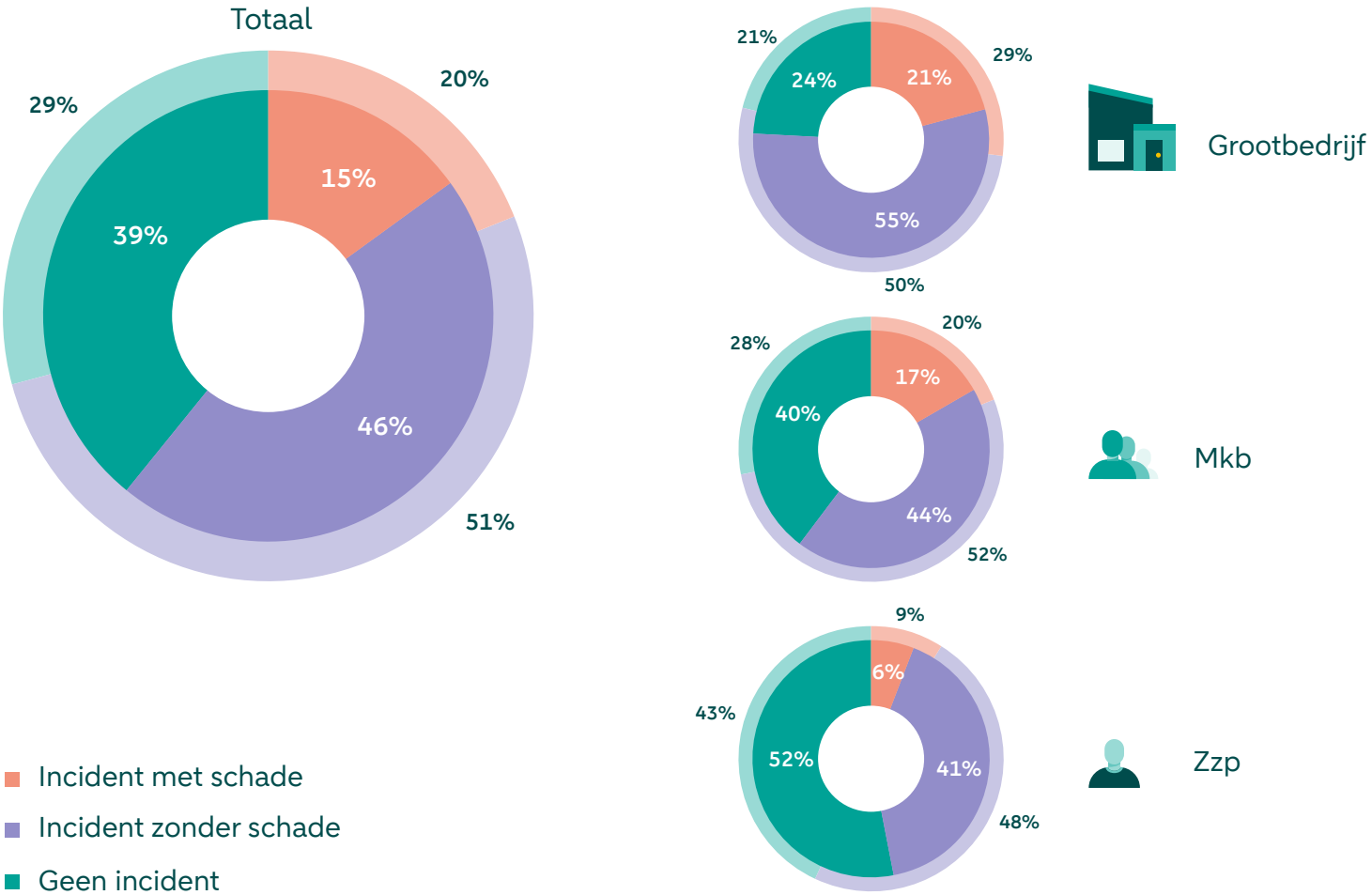
Minder bedrijven geraakt door cyberaanval

Percentage van de ondervraagde bedrijven dat in de afgelopen 12 maanden met een cyberaanval te maken heeft gehad.



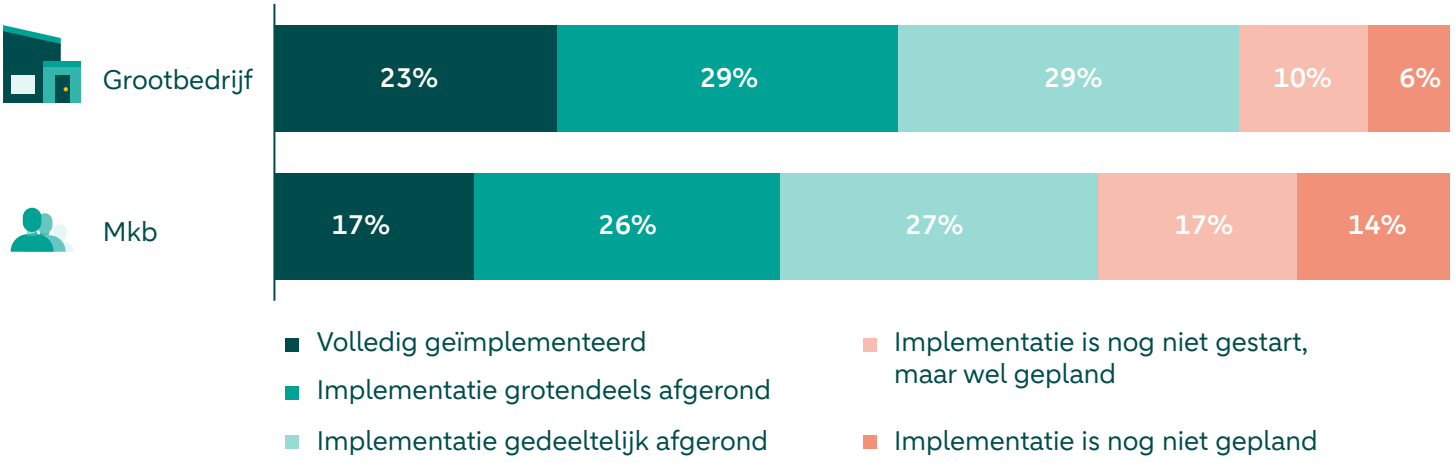
Minder organisaties leden schade door een cyberaanval; verschil vooral gedreven door verbetering grootbedrijf

Resultaten weergegeven in procenten. Data uit het voorgaande jaar in buitenste ring.



Implementatie NIS2 verdient aandacht; een derde van de mkb'ers nog niet begonnen met voorbereidingen

"Hoe ver is uw organisatie met de implementatie van de door NIS2 voorgeschreven maatregelen?"
Resultaten enkel weergegeven voor (naar eigen zeggen) NIS2-plichtige organisaties.



Positieve effecten nieuwe wetgeving

Deze dalende trend heeft mogelijk te maken met nieuwe wetgeving die al enige tijd boven de markt hangt: de Network and Information Systems Directive (NIS2), een Europese richtlijn die bedrijven in diverse kritieke sectoren verplicht om passende maatregelen te nemen tegen cyberaanvallen. Nederlandse organisaties hebben ruim de tijd gehad om zich hierop voor te bereiden. Na een vertraging van zeker anderhalf jaar wordt NIS2 dit jaar definitief verankerd in nationale wetgeving via de Cyberbeveiligingswet.

Organisaties moeten zelf checken of ze onder deze wet vallen. Bedrijven die onder de wet vallen, moeten volledig voldoen aan de verplichtingen die daarbij horen. Het merendeel van de – volgens henzelf – NIS2-plichtige organisaties heeft de implementatie ervan in ieder geval gedeeltelijk afgerond. Bijna een derde van de NIS2-plichtige mkb-organisaties is er echter nog niet mee gestart.

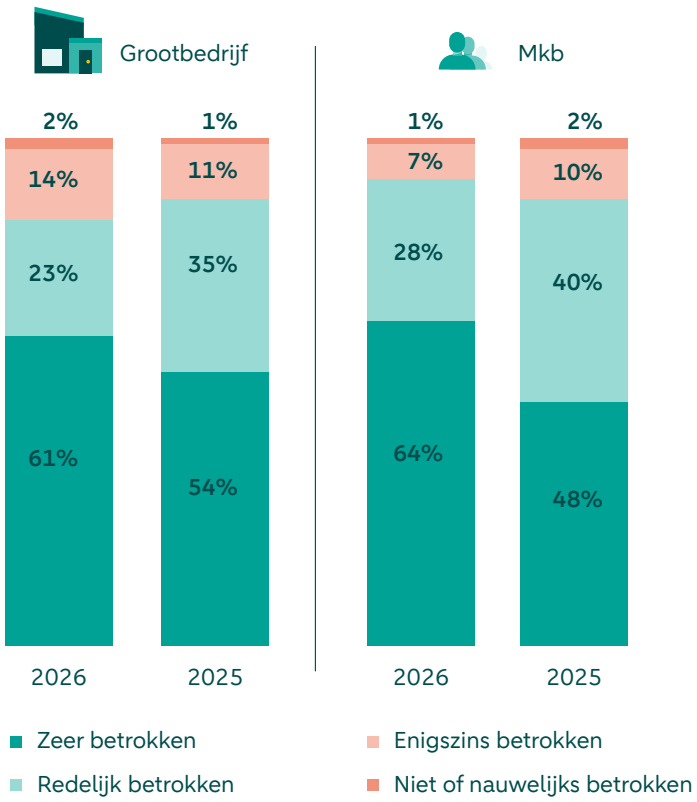
Meer betrokkenheid op het hoogste niveau

Een van de vereisten van NIS2 is dat de eindverantwoordelijkheid voor cyberveiligheid op het niveau van directie of bestuur liggen. Met name bij mkb'ers is op dat vlak al een grote stijging te zien. Van de bevraagde mkb-bedrijven – NIS2-plichtig of niet – geeft inmiddels 91 procent van de directies aan actief betrokken te zijn bij maatregelen tegen cyberaanvallen, tegenover 83 procent een jaar eerder.

Volgens Steven Daniëls, managing director bij 'managed security services provider' (MSSP) Xalient, hoort die verantwoordelijkheid daar ook thuis. "Cyberveiligheid moet op het hoogste niveau worden besproken. Het is een strategisch bedrijfsrisico, geen IT-issue."

Betrokkenheid mkb-directies significant toegenomen ten opzichte van vorig jaar

"In hoeverre is de directie van de organisatie betrokken bij cybersecurity?"



De moeizame weg naar de Cyberbeveiligingswet

De Europese NIS2-richtlijn verplicht bedrijven en organisaties in vitale sectoren zoals energie, water, transport, zorg en financiële diensten om maatregelen te nemen op het gebied van cyberveiligheid. In Nederland had die richtlijn op 17 oktober 2024 al in nationale wetgeving opgenomen moeten zijn. Dat is niet gelukt. Ook andere digitale economieën, waaronder Duitsland en Frankrijk, bleven achter; slechts vier van de 27 EU-lidstaten haalden uiteindelijk de deadline.

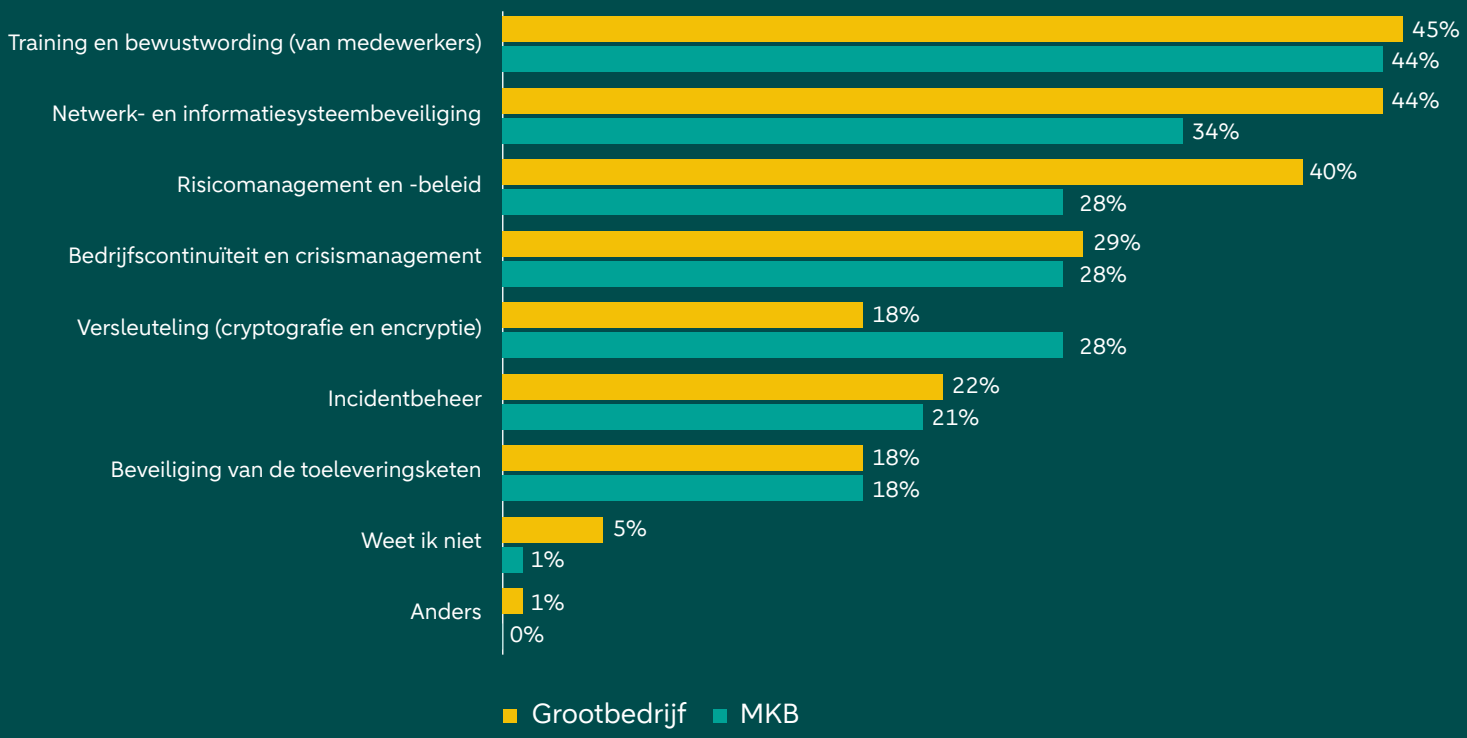
Op 23 maart 2026 debatteerde de Tweede Kamer over de Cyberbeveiligingswet: de Nederlandse uitwerking van NIS2. Het voorstel kreeg brede politieke steun, maar de Kamer kwam ook met vragen. Kamerleden maakten zich zorgen over de vaagheid van de verplichtingen. Zo schrijft de wet voor dat organisaties 'passende maatregelen' moeten nemen, maar laat deze open wat dat precies inhoudt. Ook had de Kamer zorg over de versnippering van toezicht: organisaties die in meerdere sectoren actief zijn, kunnen te maken krijgen met verschillende toezichthouders die uiteenlopende eisen stellen.

Ondanks de onduidelijkheid stemde de Tweede Kamer op 15 april 2026 in met het wetsvoorstel; het plan is dat de wet op 1 juli 2026 in werking treedt. De wet kent geen overgangsperiode; wie onder de wet valt, moet direct aan alle eisen voldoen.

Van de verschillende NIS2-verplichtingen heeft training en bewustwording van medewerkers bij organisaties de meeste prioriteit gekregen. Beveiliging van netwerk- en informatiesystemen staat op de tweede plaats, gevolgd door het ontwikkelen van risicomanagement en -beleid. Het grootbedrijf zet relatief sterker in op deze laatste twee onderwerpen dan het mkb. In het mkb liggen de prioriteiten meer verspreid; daar krijgen, naast risicomanagement, ook versleuteling van gegevens en bedrijfscontinuïteit een vergelijkbaar gewicht.

Medewerkerstraining en technische beveiliging krijgen prioriteit, gevolgd door risicomanagement

"Welke van onderstaande aspecten van NIS2 hebben binnen uw organisatie de meeste prioriteit gekregen?"
Meerdere antwoorden mogelijk.



Aanvallen worden sneller, slimmer en grootschaliger

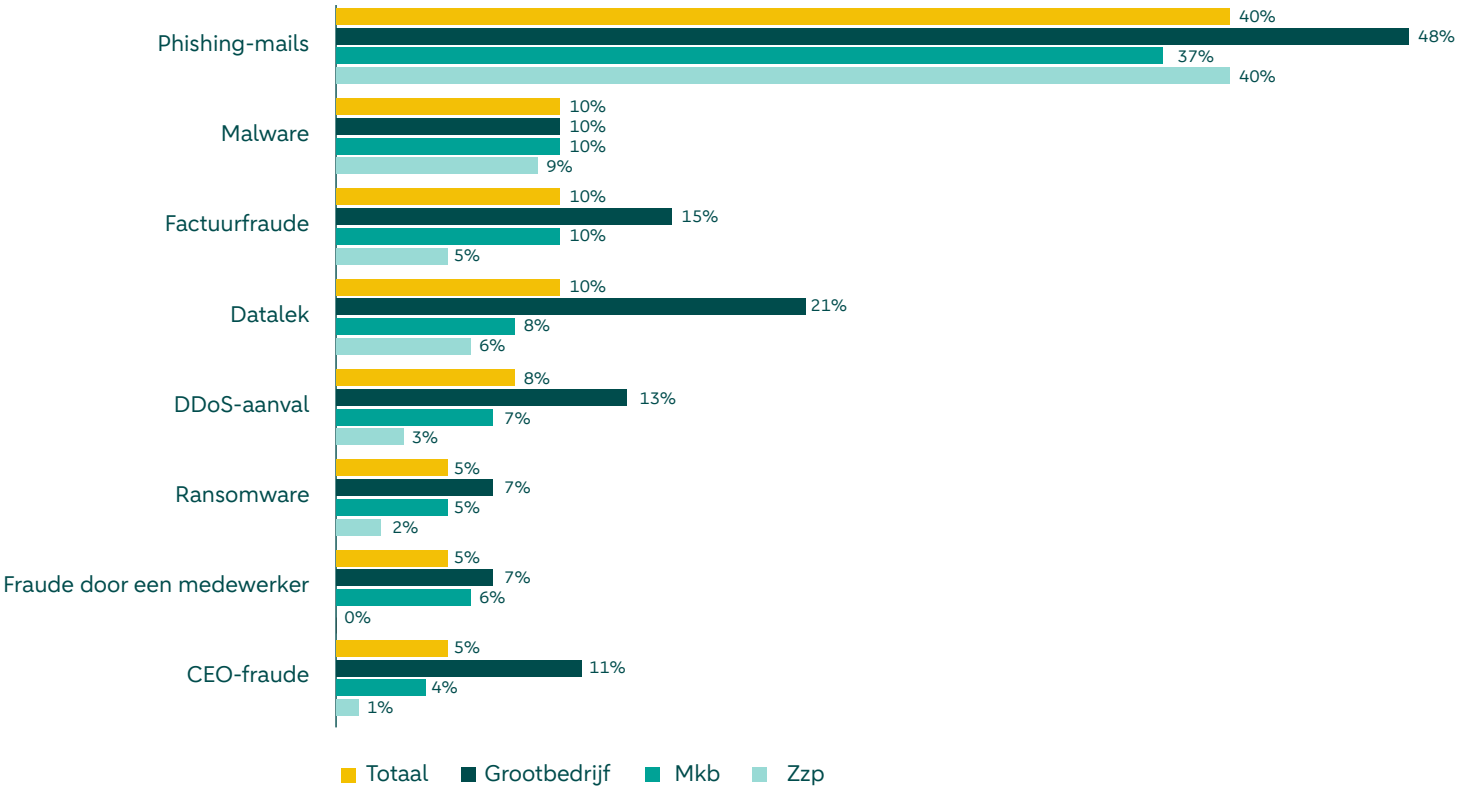
Phishing blijft de meest voorkomende aanvalsvorm, maar daarachter gaat een breder en professioneler dreigingslandschap schuil. Aanvallen worden makkelijker op te schalen, verlopen sneller en treffen organisaties op uiteenlopende manieren.

Phishing is de meest gemelde vorm van cybercriminaliteit; 40 procent van de organisaties kreeg hier in de afgelopen 12 maanden mee te maken.

Bij die vorm van oplichting worden schadelijke links of bijlagen verspreid via de mail, steeds vaker met behulp van AI om het bericht geloofwaardiger te maken.

Phishing-aanvallen wijdverbreid, datalekken prominent binnen grootbedrijf

Percentage van de ondervraagde bedrijven dat in de afgelopen 12 maanden met een bepaald soort cyberaanval te maken heeft gehad. Meerdere antwoorden mogelijk.



Van alle cyberaanvallen begint 60 procent met phishing, zo blijkt uit een recente analyse van ENISA, het Europese cyberveiligheidsagentschap. Kwaadwillenden hoeven de aanval zelfs niet meer eigenhandig voor te bereiden. Zo werd begin 2026 gewaarschuwd voor Kratos, een nieuw 'phishing-as-a-service'-platform (PhaaS) waarmee gebruikers zonder enige technische kennis een grootschalige phishing-campagne kunnen voorbereiden. Zo kunnen aanvallers heel gemakkelijk de gewenste methode kiezen: wordt het een QR-code die de ontvanger moet scannen, moet het beoogde slachtoffer een malafide kalenderuitnodiging openen, of wordt het toch een ouderwetse bijlage?

Exclusief phishing – waar lang niet elke ontvanger intrapt – had 39 procent van alle bedrijven het afgelopen jaar te maken met een aanval, tegenover 48 procent in 2025.

Dreigingslandschap professionaliseert en verhardt

De afgelopen tijd hebben de media veel aandacht besteed aan datalekken. Zo kwamen in de eerste helft van dit jaar de data van 200.000 leden van sportschool Basic-Fit op straat te liggen, hadden hackers toegang tot de privégegevens van 300.000 Ajax-supporters, en werden data van 700.000 reizigers buitgemaakt bij zakelijk reisbureau BCD Travel. Ook telecombedrijf Odido werd bestolen: gegevens van maar liefst 6,5 miljoen mensen werden gedownload.

Omzeilen van beveiliging door misleiding

De Odido-hack was technisch gezien niet geavanceerd, maar leunde grotendeels op manipulatie. Aanvallers stuurden gerichte phishing-mails naar klantenservicemedewerkers en wisten zo hun inloggegevens te bemachtigen. Met deze wachtwoorden probeerden zij vervolgens in te loggen, waarna automatisch een extra verificatiestap – ook wel 'multi-factor authentication' (MFA) genoemd – werd geactiveerd op de telefoon van de medewerker.

Direct daarna belden de aanvallers de medewerkers op, deden zich voor als de interne IT-helpdesk en zetten hen onder druk om de inlogpoging goed te keuren. Op die manier bewogen zij medewerkers ertoe om zelf de beveiligingsmelding te bevestigen. Zo kregen de aanvallers alsnog volledige toegang tot de accounts, ondanks de extra beveiligingslaag.

Eenmaal binnen in het systeem gebruikten de aanvallers geautomatiseerde scripts om op grote schaal klantgegevens te verzamelen. In totaal werden zo 21 miljoen records van ruim zes miljoen klanten buitgemaakt. Hackersgroep ShinyHunters eiste vervolgens ruim 1 miljoen euro losgeld. Odido betaalde niet, waarna de gestolen gegevens stapsgewijs op het dark web verschenen.

Van de ondervraagden kreeg een op de tien het afgelopen jaar te maken met een datalek; onder het grootbedrijf was dit zelfs een op de vijf organisaties. Bij 10 procent werd malware geïnstalleerd, zoals computervirussen en spionagesoftware. Eenzelfde percentage geldt voor factuurfraude, waarbij organisaties per mail een valse factuur ontvangen, met de bedoeling dat de ontvangers het bedrag betalen aan de oplichters.

Gijzelsoftware werd gemeld door 5 procent van de organisaties. 'Ransomware-as-a-Service' speelt hier een belangrijke rol. Kwaadwillenden kopen dan de software in bij een gespecialiseerde partij, die daarnaast ook allerlei aanpalende diensten aanbiedt: een helpdesk voor technische ondersteuning en onderhandelingsadvies, dashboards om de hoeveelheid infecties en winst in de gaten te houden, en kant-en-klare websites waar buitgemaakte data kunnen worden gepubliceerd als het slachtoffer weigert het losgeld te betalen.

Niet meer handmatig te stoppen

Kwaadwillenden die zich bedienen van een DDoS-aanval, waarbij een website of dienst wordt platgelegd door die te overspoelen met zoveel verkeer dat die bezwijkt, vestigden in december 2025 een nieuw wereldrecord. Het Amerikaanse Cloudflare, leverancier van cybersecurity- en netwerkdiensten, blokkeerde voor een van zijn klanten een DDoS-aanval van maar liefst 29,7 terabit per seconde. Dat is ongeveer twee keer de piekbelasting van de Amsterdam Internet Exchange (AMS-IX), een van de grootste internetknooppunten ter wereld.

De aanval werd gegenereerd door een netwerk van naar schatting 1 tot 4 miljoen gehackte thuisrouters en slimme apparaten wereldwijd. Cloudflare observeerde in 2025 een constante toename van grote DDoS-aanvallen. In november werd alweer een nieuw wereldrecord gevestigd, met een piek van 31,4 terabit per seconde.

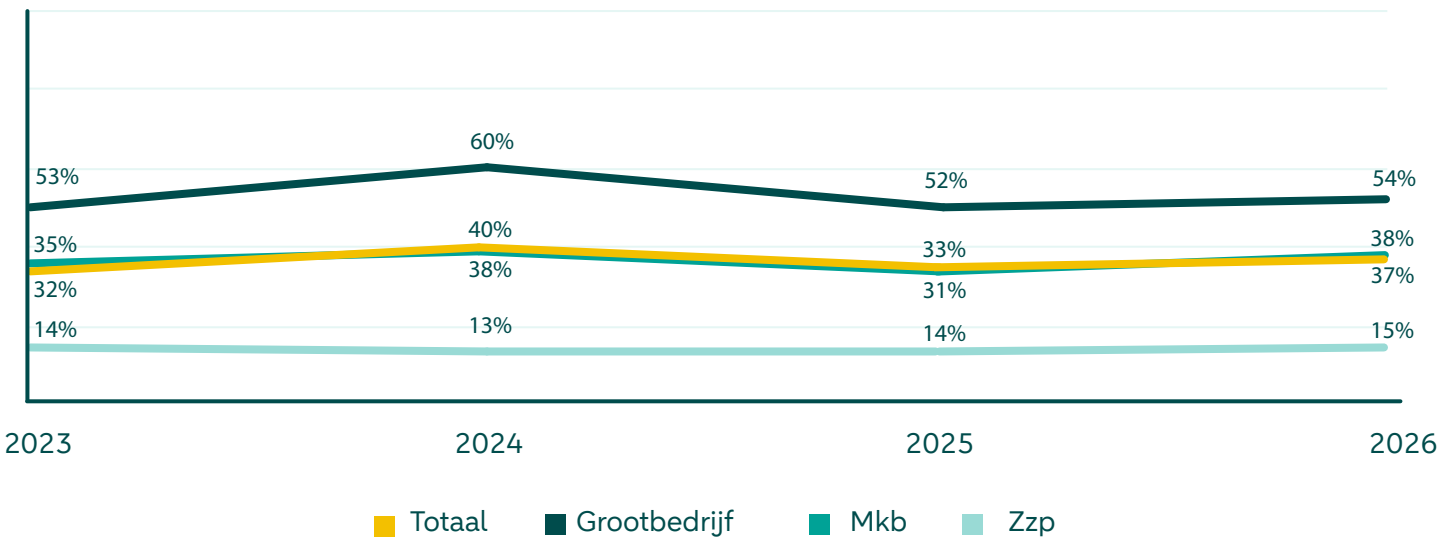
In maart 2026 viel DigiD uit door een dergelijke aanval, tijdens de belastingaangifteperiode. In juni 2025 waren websites van gemeenten en provincies urenlang onbereikbaar. Van de bevraagde organisaties kreeg 8 procent het afgelopen jaar te maken met een DDoS-aanval.

Risicoperceptie

Opvallend is dat de risicoperceptie van Nederlandse bedrijven de afgelopen jaren relatief stabiel is gebleven. In 2023 zag 35 procent van de ondervraagde ondernemers cybercriminaliteit als een groot risico voor de eigen organisatie, in 2024 was dat 40 procent, in 2025 was het 33 procent en op dit moment 37 procent. Daarmee is weer sprake van een lichte, zij het niet-significante stijging.

Risicoperceptie schommelt rond hetzelfde niveau

"In welke mate denkt u dat cybercriminaliteit een risico is voor uw organisatie?"
Percentage van de respondenten dat "(heel) veel risico" heeft geantwoord.



AI intensiveert cybersecurity-wapenwedloop

AI maakt het makkelijker om cyberaanvallen op te schalen en ingewikkelder om ze op tijd te stoppen. Tegelijk gebruiken veel bedrijven de technologie al volop, zonder duidelijke afspraken over wat ermee mag en hoe risico's worden beheerst.

Drie op de tien organisaties maakt zich zorgen om een toename van cyberdreigingen door AI, zo blijkt uit het ABN AMRO-onderzoek – bijvoorbeeld omdat kwaadwillenden de technologie kunnen gebruiken voor gepersonaliseerde phishing-aanvallen op grote schaal of het overtuigend nabootsen van identiteiten.

De introductie van het nieuwe AI-model Claude Mythos van AI-lab Anthropic in april leidde tot extra onrust – wat overigens niet zichtbaar is in dit onderzoek omdat de survey voor die tijd werd uitgevoerd. Dit model bleek in tests zelfstandig kwetsbaarheden te kunnen vinden en die te combineren tot werkende aanvalsroutes. Het model was niet specifiek op cybersecurity getraind, maar bleek daar wel opvallend goed in. Anthropic achtte het model te gevaarlijk om breed uit te rollen en stelde het aanvankelijk aan een select aantal bedrijven beschikbaar in Project Glasswing. Verschillende experts vonden de claims van het AI-lab overigens overtrokken en zagen de beperkte lancering vooral als een PR-stunt.

Met toegang tot broncode, kunnen AI-modellen veel kwetsbaarheden vinden. "Mijn zorg zit dan ook op het 'open source'-stuk", zegt Dekker van ABN AMRO. Naar schatting bestaat moderne software voor 70 tot 90 procent uit open source-componenten. "Iedereen heeft toegang tot die code, dus ook kwaadwillenden."

Gefaseerde (en geblokkeerde) uitrol van een potentieel gevaarlijk model

In tests vond Mythos duizenden kwetsbaarheden in elk groot besturingssysteem (Windows, macOS, Linux) en elke grote webbrowser. De oudste aangetroffen fout was 27 jaar oud, en die zat verstopt in een systeem dat juist bekendstaat om zijn veiligheid. In één geval zette het model een aanval op die vier afzonderlijke lekken aan elkaar koppelde om zowel de beveiliging van een webbrowser als de onderliggende beveiliging van het besturingssysteem te omzeilen.

Anthropic koos voor een gecontroleerde aanpak: aanvankelijk kregen zo'n vijftig organisaties – waaronder Amazon, Microsoft, Apple, Google en bank JPMorganChase – exclusieve toegang om het model alleen voor verdediging te gebruiken. Dat gaf ze de kans om hun eigen systemen door te lichten op kwetsbaarheden voordat aanvallers die kans zouden krijgen. Begin juni kregen nog eens 150 organisaties toegang, verspreid over 15 landen. Kort daarna werd het model in een aangepaste versie – Fable – voor het grote publiek gelanceerd. Die aanpassing moest ervoor zorgen dat potentieel schadelijke verzoeken door een minder geavanceerd model worden afgehandeld.

Omdat bleek dat deze beveiligingsmaatregelen waren te omzeilen, haalde Anthropic het model op bevel van het Witte Huis enkele dagen na de lancering weer offline. De kans dat niet-Amerikaanse spelers kwaad zouden doen met het AI-model achtte de Amerikaanse regering te groot.

Per doelwit een andere aanvalsmethode

Ook met minder geavanceerde modellen maken aanvallers al gebruik van AI. “Met name statelijke actoren zien we AI-gestuurde campagnes uitvoeren”, zegt Harm Teunis van cybersecuritybedrijf ESET. “AI wordt gebruikt in alle processtappen, van het vergaren van informatie over het doelwit en het vinden én uitbuiten van kwetsbaarheden, tot het verder infiltreren in het netwerk en uiteindelijk data buitmaken.”

Ransomware-aanvallen kunnen ook middels AI worden uitgevoerd, zo bleek uit een onderzoeksproject van New York University. De onderzoekers maakten een prototype genaamd PromptLock, dat gevoelige bestanden op een computer identificeert, analyseert, en vervolgens steelt, versleutelt of vernietigt. Ook het bericht aan het slachtoffer wordt door AI gegenereerd. Bovendien genereert het bij elke aanval nieuwe code. Dat maakt dergelijke programma’s moeilijk te detecteren door virusscanners, omdat deze uitgaan van reeds bekende computercode.

Cyberaanvallen verlopen vooralsnog vooral volgens herkenbare patronen, maar kunnen middels AI inspelen op de specifieke context van een organisatie. Zo ontwikkelde de Universiteit van Toronto een AI-gedreven ‘worm’: malware die zich zelfstandig tussen computers kan verspreiden. Zulke programma’s bestaan al decennialang – WannaCry besmette in 2017 nog 200.000 tot 300.000 computers in 150 landen – maar deze variant kan per machine zelf een aanvalsmethode bepalen. Daardoor volstaat niet langer één ‘software-fix’ die overal wordt uitgerold. Hoopvol is dat hetzelfde systeem volgens de onderzoekers in aangepaste vorm ook kan worden ingezet om kwetsbaarheden te verhelpen.

AI helpt ook de verdediging

Boender van ThreadStone zet AI al in om delen van zijn werk te automatiseren. “Ik heb een soort miniversie van mezelf gemaakt om IT-omgevingen te scannen op kwetsbaarheden.” De AI-agent is getraind op kennis van Boender. “Hiermee kan hij ongeveer 90 procent van de meer eenvoudige taken uitvoeren.”

“Ook het antwoord op zulke aanvallen zal een bepaalde mate van automatisering moeten hebben”, beaamt Nicole van der Meulen. Volgens de cybersecurity-expert brengt zulke automatisering echter ook de nodige risico’s met zich mee. “Als vervolgens ook je AI-verdedigingslinie wordt gesaboteerd, zit je met een nog groter probleem.” Daarom blijft menselijke expertise volgens Van der Meulen onmisbaar.

Basishygiëne belangrijker dan ooit

De nieuwste AI-technologieën kunnen dus aan beide kanten worden ingezet. “Het is een wapenwedloop, waarbij je moet zorgen dat je in het spel blijft”, zegt Dekker van ABN AMRO. Voor grote organisaties is het echter gemakkelijker om een verdediging op te zetten dan voor kleine. “Aanvallers kunnen hierdoor worden weggedrukt naar kleinere bedrijven.”

De ‘best practices’ blijven volgens de Chief Information Security Officer onveranderd. “Sterker nog: strenge handhaving van basishygiëne is belangrijker dan ooit.” Hieronder vallen onder andere het gebruik van sterke wachtwoorden in combinatie met autorisatie via een losse app of fysieke sleutel, het maken van back-ups, en het up-to-date houden van IT-systemen. Teunis van ESET: “In essentie is cybersecurity niet veranderd door AI, maar de tijd die bedrijven hebben om een beveiligingslek te dichten is wel verkort.”

Identiteiten nabootsen met AI

Begin dit jaar waarschuwde het Belgische Openbaar Ministerie voor oplichters die een AI-versie van koning Filip inzetten om slachtoffers te verleiden tot investeringsfraude. “Wat we weten, kan uitlekken via datalekken. Wat we hebben, zoals een telefoon, kan ook via omwegen worden misbruikt”, zegt cybersecurity-expert Van der Meulen. “Maar nu is ook dat wat we zijn, zoals ons gezicht of stem, niet langer vanzelfsprekend betrouwbaar.” Volgens de expert gaat daar te weinig aandacht naar uit. “Er wordt veel gesproken over wat criminelen kunnen met data uit datalekken, maar ook zonder datalek is er al heel veel materiaal beschikbaar.” Dat materiaal is mogelijk nog veel rijker; video’s en foto’s op sociale media, of iemands stem uit een telefoongesprek of videocall, kunnen al genoeg zijn om een identiteit na te bootsen.

Met slechts 3 tot 5 seconden audio is een stem te kopiëren met een nauwkeurigheid van 85 procent. In combinatie met de eerder beschreven tweekanaalsaanvallen valt de aanval vrijwel niet meer te onderscheiden van echte communicatie.

Volgens Dekker moeten organisaties zich overigens niet blindstaren op de dreiging vanuit mogelijke geavanceerde aanvallen. “We zien vooralsnog veel ‘ouderwetse’ methodes, zoals misbruik van gestolen inloggegevens.”

AI-gebruik onder bedrijven neemt toe

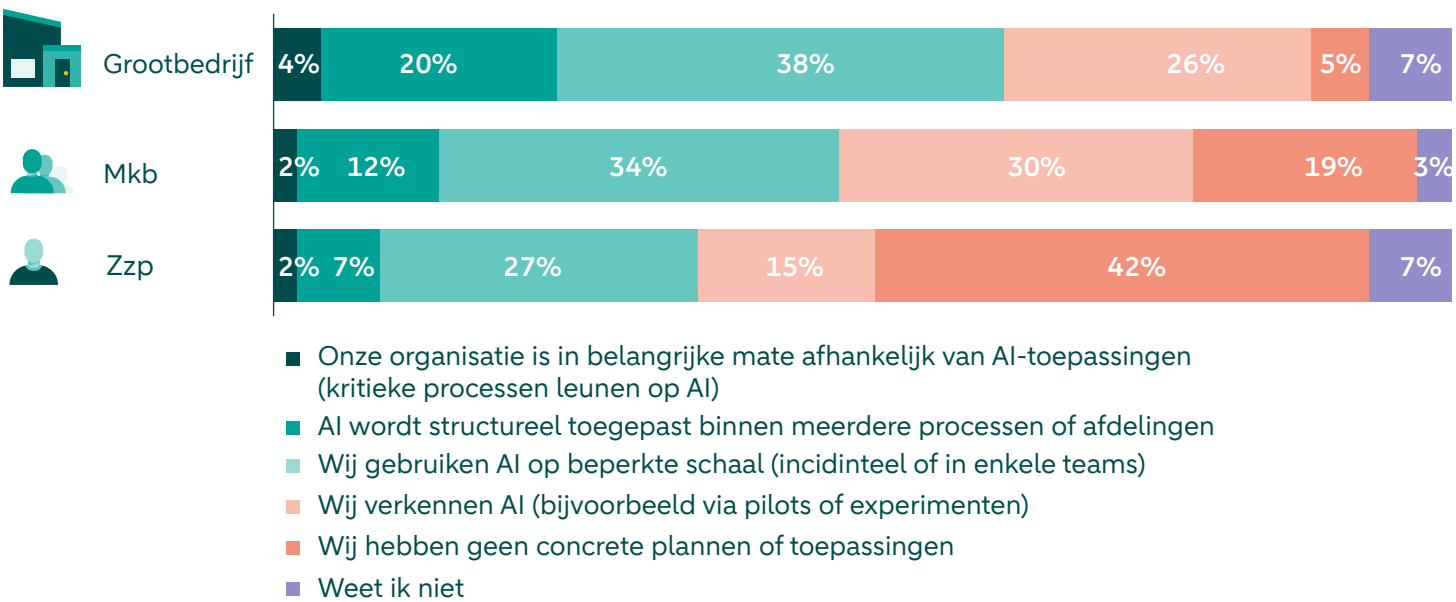
Het aantal Nederlandse bedrijven dat AI gebruikt, is in korte tijd sterk toegenomen. Op dit moment maakt 78 procent van de mkb’ers gebruik van AI, maar de manier waarop varieert sterk. Sommige schaalzitten in de experimentfase of spreken van incidenteel gebruik, terwijl anderen AI structureel inzetten binnen de organisatie. Bij grote bedrijven is het aandeel AI-gebruikers nog hoger: maar liefst 88 procent. Onder zzp’ers blijft het juist achter: van deze groep heeft 42 procent nog geen concrete plannen of toepassingen voor AI.

“Je ziet dat mensen gaan snuffelen aan AI-tools”, zegt Teunis van ESET. “De belofte van efficiëntie en sneller werken is aanlokkelijk.” Dat brengt echter wel risico’s met zich mee. Zo heeft maar liefst 30 procent van de mkb’ers zorgen over medewerkers die onbedoeld gevoelige of vertrouwelijke informatie delen met een AI-tool. Bij grote bedrijven is dat zelfs 42 procent.

Deze zorgen zijn niet onterecht. Uit onderzoek van LayerX blijkt dat 77 procent van de gebruikers data in generatieve AI-tools plakt; 22 procent van deze

Hoe groter het bedrijf, hoe meer er met AI wordt gewerkt

“Hoe ver is uw organisatie op dit moment met artificial intelligence (AI)?”



AI-gegenereerde software

Steeds meer bedrijven gebruiken kunstmatige intelligentie om software te schrijven of te helpen schrijven. Zo'n programma schrijft snel en goed, maar de veiligheidsrisico's zijn groot. Beveiligingsbedrijf Veracode analyseerde code die door AI-modellen was geschreven en vond in 45 procent van de gevallen beveiligingsfouten. Een analyse van 470 open source-projecten door CodeRabbit toonde dat AI-geschreven code gemiddeld 2,74 keer zo veel kwetsbaarheden bevat als code geschreven door mensen.

Volgens Teunis van ESET hoeft dat geen probleem te zijn, zolang er een mens meekijkt. "Die human in the loop blijft belangrijk. Softwareontwikkeling is niet alleen code schrijven, maar ook controleren." Expert Van der Meulen denkt dat grondig geteste software zich in de toekomst nadrukkelijker kan onderscheiden. "In combinatie met een label als 'made in Europe' kan dat een interessant kwaliteitskenmerk zijn."

gebruikers deelt via deze weg ook persoonlijke informatie of betaalkaartgegevens. Een groot deel van dit gebruik verloopt bovendien via onbeheerde accounts, waardoor het buiten het zicht van de IT-afdeling kan blijven.

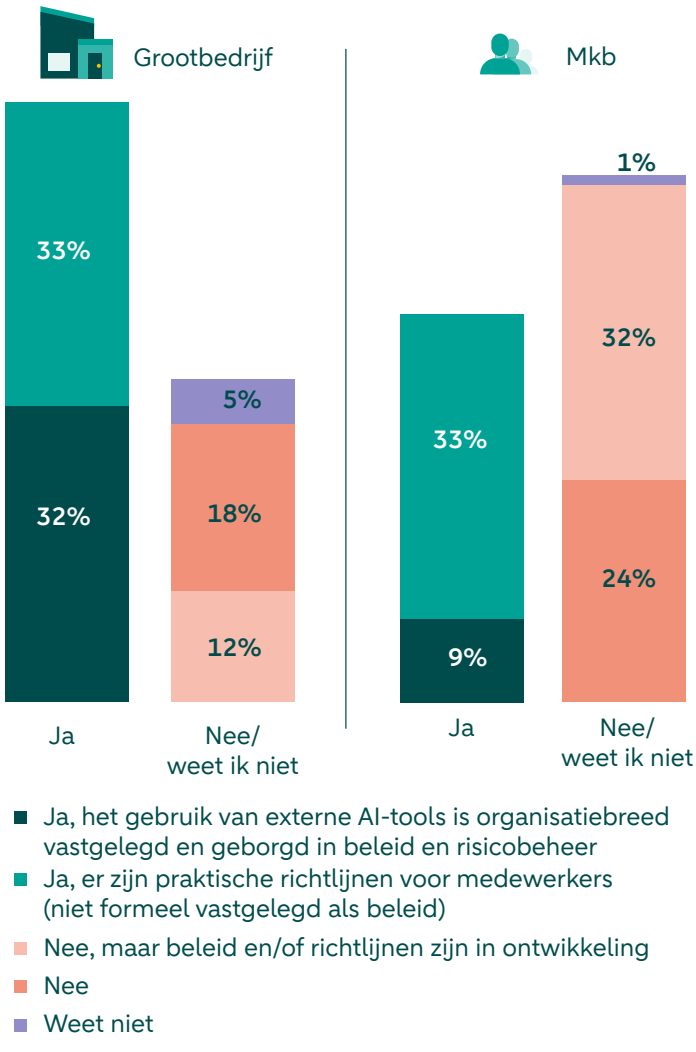
De risico's van AI beperken zich bovendien niet tot medewerkers die vertrouwelijke informatie invoeren in een chatbot. Naarmate bedrijven AI breder inzetten, krijgt de technologie ook meer handelingsruimte binnen de organisatie. Zogenoemde AI-agents kunnen niet alleen informatie genereren, maar ook zelfstandig gegevens ophalen of systemen aansturen. Volgens Daniëls van Xalient ontstaat daarmee een nieuwe markt: 'non-human identity security'. "Dit vakgebied draait om de vraag tot welke systemen niet-menselijke gebruikers toegang krijgen, en hoe je hun identiteit verifieert." Volgens Daniëls is dat belangrijk, omdat het aantal niet-menselijke identiteiten sterk toeneemt en deze steeds vaker worden misbruikt in cyberaanvallen.

AI-beleid en -risicobeheer in de kinderschoenen

Het gebruik van AI loopt in veel organisaties vooruit op beleid en risicobeheer. Van de mkb'ers heeft slechts 9 procent een formeel vastgelegd beleid voor het gebruik van externe AI-tools als ChatGPT, tegenover 32 procent van de grote bedrijven. Een derde van zowel mkb als grootbedrijf heeft praktische richtlijnen voor medewerkers. Meer dan de helft van de mkb-bedrijven heeft helemaal geen beleid of richtlijnen; een kwart werkt hier echter wel aan.

Mkb blijft achter met beleid en richtlijnen voor externe AI-oplossingen

"Heeft uw organisatie beleid of richtlijnen opgesteld voor het gebruik van externe AI-tools (zoals ChatGPT)?" Eén antwoord mogelijk.



Cyberveiligheid stopt niet bij de eigen organisatie

Een organisatie kan haar eigen beveiliging op orde hebben en toch geraakt worden door een cyberincident elders in de keten. Met name de afhankelijkheid van IT-leveranciers maakt bedrijven ongemerkt kwetsbaar. Afspraken maken met partners over cybersecurity is echter nog geen gemeengoed.

Slechts 39 procent van de mkb'ers heeft met minimaal één partner afspraken gemaakt over digitale veiligheid; bij grote bedrijven ligt dit aandeel op 53 procent. Van de organisaties zonder dergelijke afspraken is een aanzienlijk deel ook niet voornemens om hierin stappen te zetten. Dat geldt voor twee op de tien grote bedrijven, en bijna vier op de tien mkb'ers.

Beveiliging van de toeleveringsketen staat hoog op de prioriteitenlijst binnen de NIS2-richtlijn. Toch zien veel organisaties het als bijzaak: slechts 18 procent van de respondenten in grootbedrijf en mkb hebben hier bij de implementatie van de richtlijn prioriteit aan gegeven – de laagste positie in de lijst.

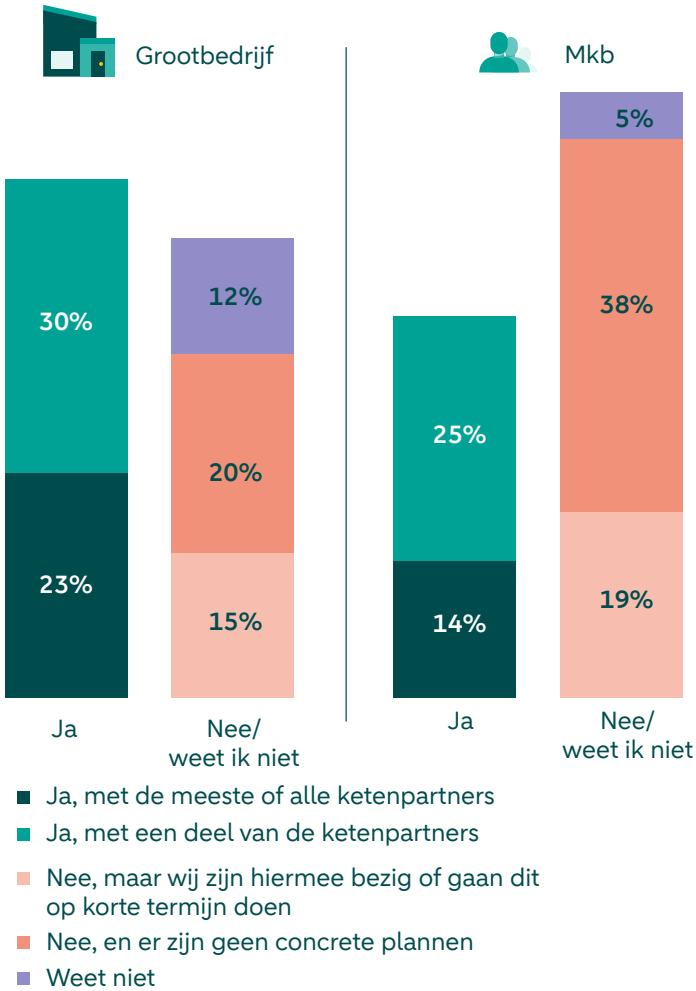
Binnenkomen via IT-leveranciers

Met name IT-leveranciers zijn een geliefd doelwit onder hackers. Via systemen die door deze partijen worden beheerd, komen ze gemakkelijk binnen bij tal van andere organisaties. Zo vond eerder dit jaar een gijzelsoftware-aanval plaats op ChipSoft, dat met zijn software zo'n driekwart van de Nederlandse ziekenhuizen bedient. Diverse ziekenhuizen haalden hun online-patiëntenomgevingen offline, waardoor patiënten geen afspraken of onderzoeksresultaten konden bekijken. De ziekenhuiszorg zelf kwam niet in gevaar. Wel zijn bij andere zorgverleners, waaronder huisartsenpraktijken en tbs-klinieken, medische dossiers gelekt.

In september vorig jaar ging het op een vergelijkbare manier mis op Europese luchthavens. Criminelen hackten de software die luchtvaartbedrijven gebruiken voor inchecken en boardingpassen: een systeem

Ketenafspraken over cybersecurity zijn nog niet wijdverbreid

"Heeft u met ketenpartners (leveranciers, klanten, partners) afspraken gemaakt over cybersecurity?



Cyberaanval raakt complete autoketen

Een cyberaanval op Jaguar Land Rover (JLR) leidde in het najaar van 2025 tot wekenlange verstoringen van de voertuigproductie. Nadat de aanval was ontdekt, schakelde de autofabrikant uit voorzorg delen van zijn digitale omgeving uit, waaronder systemen die noodzakelijk waren voor productieplanning en onderdelenlogistiek. Omdat er geen auto's meer werden geproduceerd, viel ook de vraag naar onderdelen en logistieke diensten stil.

De productiestop resulteerde niet alleen in een kwartaalverlies van 485 miljoen Britse pond voor JLR zelf, maar strekte zich uit over de toeleveringsketen. Zo'n 5000 toeleveranciers en logistieke partners kwamen in de knel, zagen hun omzet verdampen en moesten soms zelfs werknemers ontslaan. Naar schatting kostte de cyberaanval de Britse economie zo'n twee miljard pond.

van leverancier Collins Aerospace dat door tientallen vliegvelden wordt gebruikt. Honderden vluchten liepen vertraging op en tientallen vluchten werden geannuleerd.

Cloud-platforms als opstapje

De cloud-markt is voor 70 procent in handen van de Amerikaanse tech-giganten Amazon, Microsoft en Google. "Zulke leveranciers zijn hoogst professioneel en hebben ook een hoop middelen om hun cybersecurity op niveau te houden", zegt Dekker van ABN AMRO. "Maar het wijdverbreide gebruik van deze diensten betekent ook dat een kwetsbaarheid grote gevolgen kan hebben voor een hele hoop organisaties."

Zo drongen in 2023 Chinese staatshackers van Storm-0558 binnen in de interne systemen van Microsoft. In een oud crashrapport van een technicus vonden zij een geheime digitale hoofdsleutel. Door een fout in de Microsoft-cloud kregen de aanvallers met die 'loper' toegang tot de mailboxen van tientallen overheden en ministeries wereldwijd.

Bij Amazon Web Services (AWS) maakten cybercriminelen misbruik van de schaal en automatisering van het platform zelf. Met geautomatiseerde zoekprogramma's speurden zij het internet af naar achtergelaten inlogcodes in zogeheten .env-bestanden van cloud-gebruikers. Zodra ze geldige AWS-codes vonden, namen ze de accounts van die bedrijven over. Vervolgens misbruikten de hackers de infrastructuur van de slachtoffers om vanaf daar meer dan 230 miljoen andere doelwitten te scannen. Met wederom nieuwe toegangscodes vervolgden ze hun weg, waarbij ze uiteindelijk bij meerdere slachtoffers ook bedrijfsdata direct uit de cloud-opslag wisten te roven.

Op zoek naar Europese alternatieven

De digitale afhankelijkheid van een klein aantal grote leveranciers krijgt steeds meer gewicht als geopolitiek en strategisch risico. Organisaties zijn namelijk niet alleen afhankelijk van de betrouwbaarheid en veiligheid van deze partijen zelf, maar ook van de context waarin zij opereren. Zo werd het AI-model Fable 5 en Mythos 5 van Anthropic in juni wereldwijd offline gehaald onder druk van het Witte Huis, vanwege zorgen over mogelijk misbruik door niet-Amerikaanse partijen voor cyberaanvallen. Omdat het praktisch lastig is om alleen bepaalde landen of regio's af te sluiten, werden de modellen overal uitgeschakeld.

Wetgeving voor digitale onafhankelijkheid en -weerbaarheid

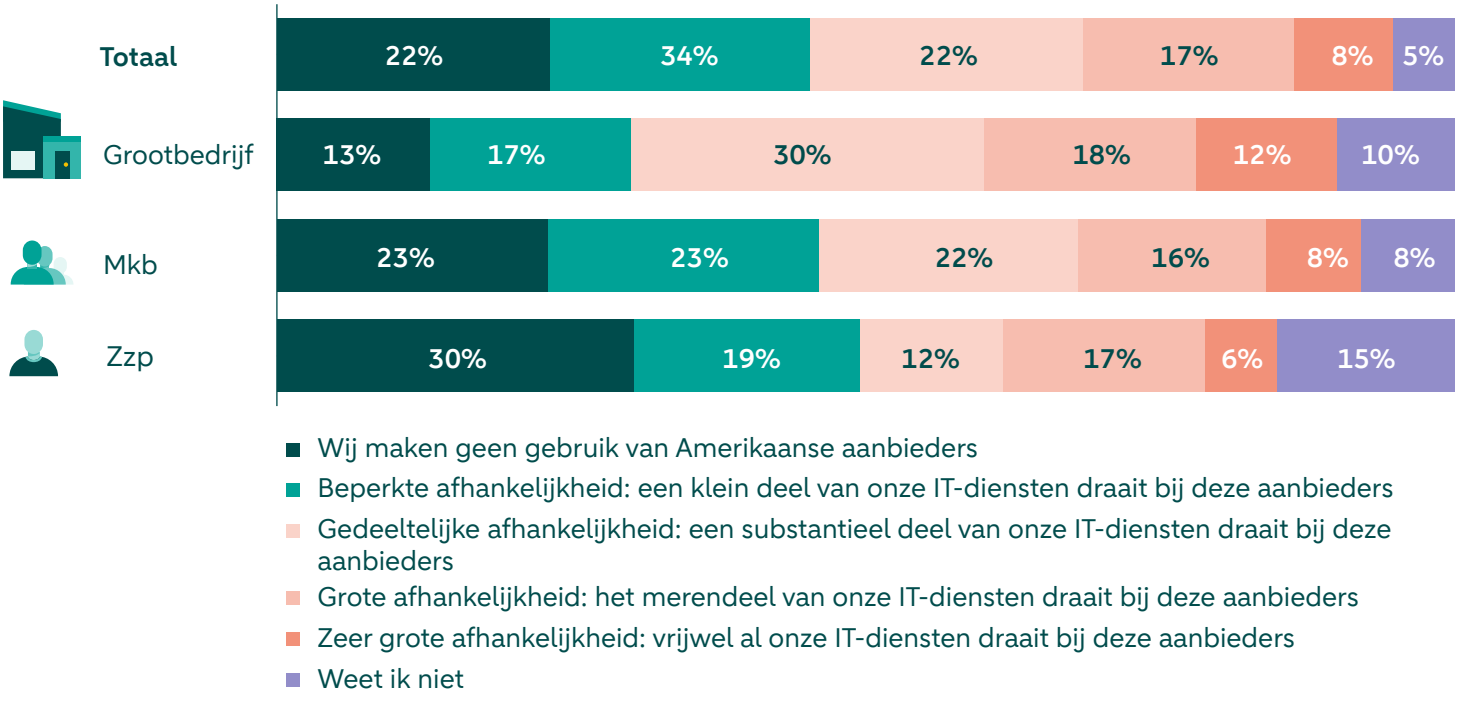
Al langer bestaat de vrees dat door de verslechterde relatie met de Verenigde Staten Amerikaanse cloud-diensten kunnen worden ingezet als politiek drukmiddel, en in een uiterst geval zelfs kunnen worden uitgeschakeld. Begin juni presenteerde de Europese Commissie daarom het European Technological Sovereignty Package: een strategie om de digitale en technologische afhankelijkheid van de Europese Unie van de Verenigde Staten en China fors te verkleinen. Onderdeel daarvan is de Cloud and AI Development Act, wetgeving die onder andere een maatstaf introduceert om de 'soevereiniteit' van cloud- en AI-oplossingen te beoordelen. Zo'n instrument helpt organisaties om te bepalen welke digitale activiteiten zij zonder grote risico's kunnen onderbrengen bij niet-Europese partijen, en waar zij hun data enkel in handen van lokale aanbieders vertrouwen.

De verschuiving van cybersecurity naar bredere digitale weerbaarheid blijkt ook uit de Europese Digital Operational Resilience Act (DORA). Deze verordening draait niet alleen om het voorkomen van cyberincidenten, maar ook om het vermogen van financiële instellingen om operationeel te blijven bij verstoringen van IT-systemen of kritieke leveranciers. Organisaties moeten daarom hun kritieke leveranciers in kaart hebben, de impact van uitval kunnen inschatten en maatregelen klaar hebben om de dienstverlening voort te zetten als een IT-leverancier uitvalt.

Geopolitieke en juridische factoren kunnen dus direct doorwerken in de beschikbaarheid van digitale diensten. Voor Europese organisaties betekent dit dat een deel van hun digitale infrastructuur afhankelijk is van besluitvorming buiten de eigen jurisdictie en invloedssfeer. Bijna de helft van de Nederlandse bedrijven ervaart een gedeeltelijke tot zeer grote afhankelijkheid van Amerikaanse cloud- en AI-aanbieders. Dit geldt voor 35 procent van de zzp'ers, 46 procent van de mkb'ers en 60 procent van het grootbedrijf.

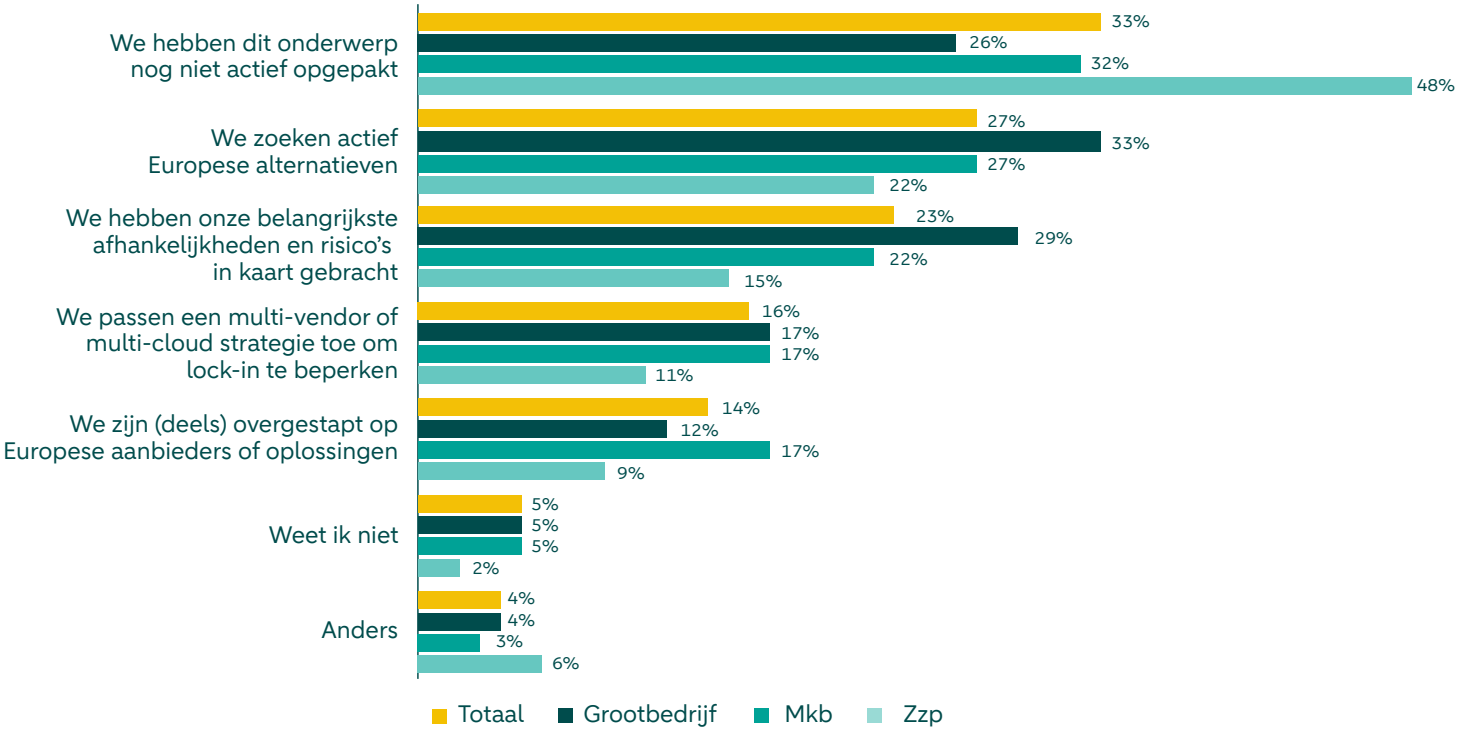
Grote bedrijven ervaren sterkste afhankelijkheid van Amerikaanse IT-aanbieders

"In hoeverre is uw organisatie op IT-gebied afhankelijk van Amerikaanse aanbieders van cloud- en AI-diensten?"



Twee derde van de organisaties onderneemt actie op digitale soevereiniteit

“Welke maatregelen heeft uw organisatie genomen om deze afhankelijkheid te beperken?” Meerdere antwoorden mogelijk.
Vraag enkel gesteld aan respondenten die (nog) gebruikmaken van Amerikaanse cloud- en AI-diensten.



Inmiddels onderneemt zo’n twee derde van de organisaties actie om deze afhankelijkheid te beperken. Zo onderzoekt bijna drie op de tien bedrijven Europese alternatieven. Overstappen is niet altijd realistisch, want de schaal, functionaliteit en innovatiekracht van Amerikaanse platforms is moeilijk te evenaren. Toch is 12 procent van het grootbedrijf al (deels) overgestapt, en van de mkb’ers zelfs 17 procent.

Veel bedrijven zijn nog beperkt ingericht op cyberrisico's

Veel organisaties zijn nog onvoldoende voorbereid op cyberincidenten. Vooral bij kleinere bedrijven ontbreken vaak de plannen, routines en investeringen om cyberrisico's te beheersen en de gevolgen van cyberincidenten op te vangen.

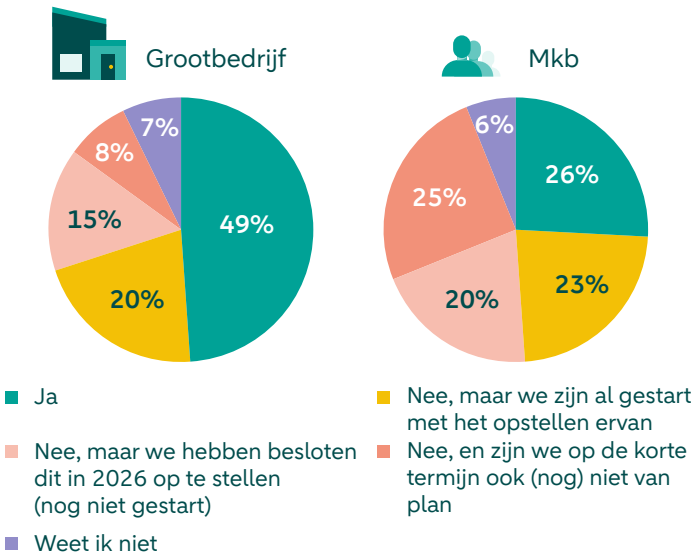
Van Mossel, een groot autodealerconcern, kreeg in december 2025 te maken met een cyberaanval. Het bedrijf zag een indringer op de servers, en besloot uit voorzorg direct de eigen IT-systemen uit te schakelen. "We zijn er op tijd bij geweest", zei CEO Eric Berkhof daarover in het Algemeen Dagblad.

Mkb onvoldoende voorbereid op cyberaanvallen

Hoewel een snelle reactie essentieel is, beschikt minder dan de helft van de organisaties over een formeel responsplan voor cyberincidenten. Van de mkb'ers heeft slechts 26 procent zo'n plan tegenover 49 procent van de grote organisaties. Nog zorgwekkender is de groep die hier bewust van afziet: een kwart van de mkb-bedrijven heeft geen plan en ook geen intentie om dat op korte termijn te veranderen. Bij grote bedrijven ligt dit aandeel op 8 procent.

Slechts een kwart van de mkb'ers heeft een responsplan, tegenover de helft van de grote bedrijven

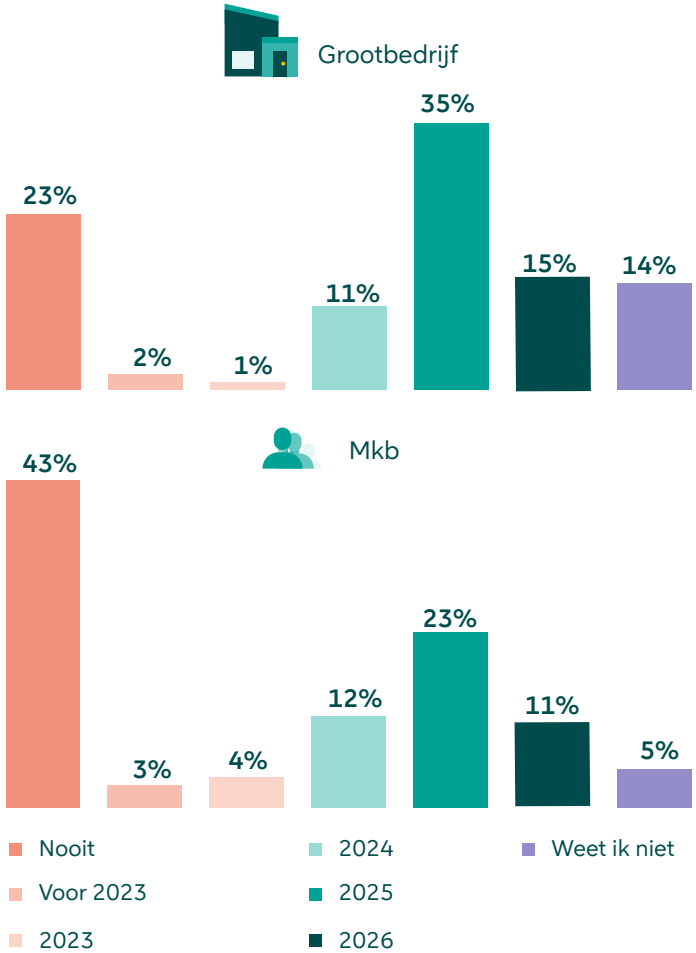
"Stel, uw organisatie wordt slachtoffer van een cyberaanval. Heeft u een responsplan met verantwoordelijkheden en taken klaarliggen voor zo'n situatie?"



Ook oefenen op cyberaanvallen gebeurt structureel te weinig; een kwart van mkb'ers deed dit in het afgelopen jaar, tegenover een derde van de grote bedrijven. Hierbij valt op dat 43 procent van de mkb'ers zelfs nog nooit een cyberaanval heeft geoefend. Deze organisaties moeten dus improviseren als het daadwerkelijk misgaat.

Bijna de helft van de mkb'ers heeft nog nooit een cyberaanval geoefend

"Wanneer heeft u voor het laatst een cyberaanval geoefend?"

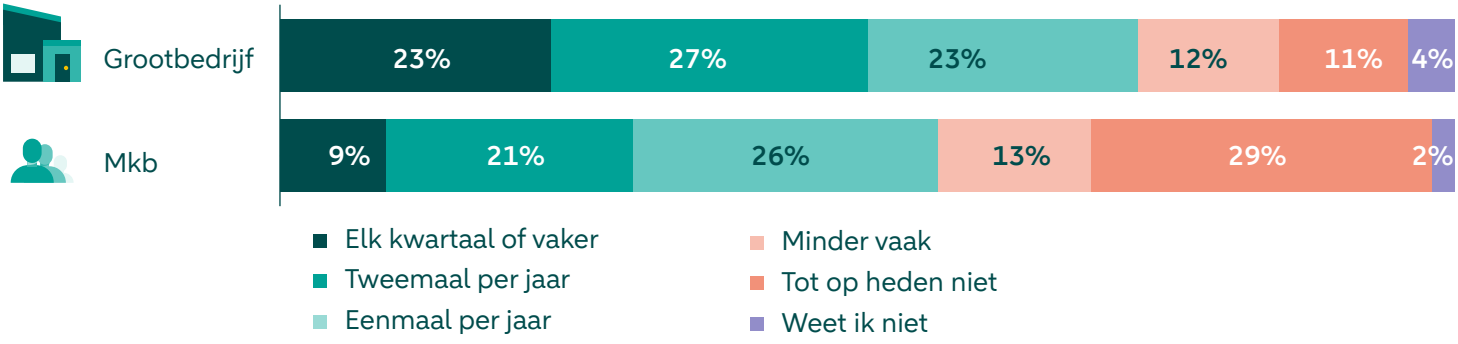


Volgens Teunis van ESET moet een bedrijf vooraf weten wat het doet als processen stil komen te liggen of leveranciers uitvallen. “Van welke leveranciers en processen ben je afhankelijk? Een retailer moet bijvoorbeeld de optie hebben om zijn klanten via QR-code te laten betalen op het moment dat de pin er eens uitligt. En alternatieve leveranciers klaar hebben staan voor het geval dat een van hen wegvalt, bijvoorbeeld door een cyberaanval.”

Slechts 9 procent van de mkb’ers traint zijn medewerkers elk kwartaal op het gebied van cyberveiligheid. In het grootbedrijf geldt dat voor bijna een kwart.

Meerderheid van de organisaties traint medewerkers op cybersecurity, maar frequentie verdient aandacht

“Hoe vaak krijgen uw medewerkers cybersecuritytraining?”

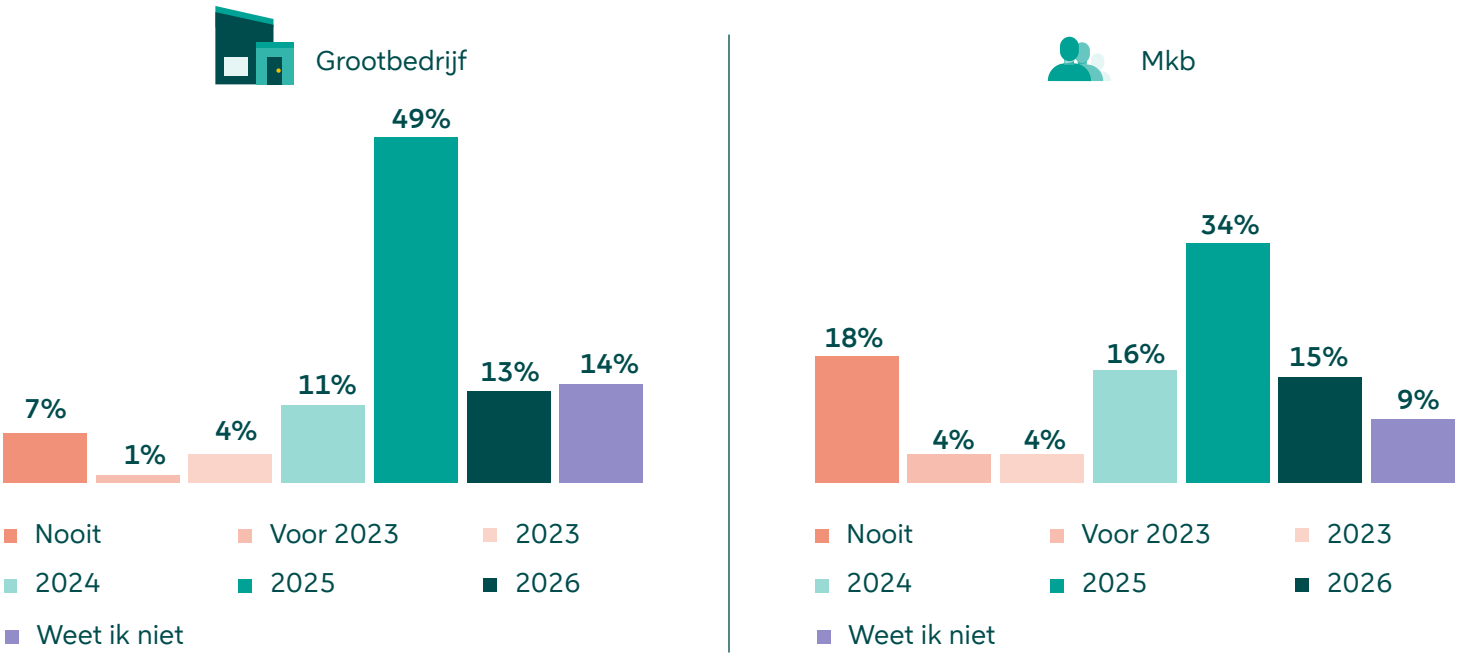


Beperkt inzicht in risico’s

In het mkb ontbreekt vaak een actueel beeld van kwetsbaarheden; nauwelijks een derde van de organisaties voerde het afgelopen jaar een risicoscan uit. Bij grootbedrijven deed iets meer dan de helft dat. Zo’n scan is belangrijk om de juiste afwegingen te maken, zegt Tsz Cheung, algemeen directeur van cybersecuritybedrijf MMOX. “Een goede risicoanalyse maakt duidelijk welke maatregelen echt nodig zijn en in welke volgorde ze moeten worden genomen.”

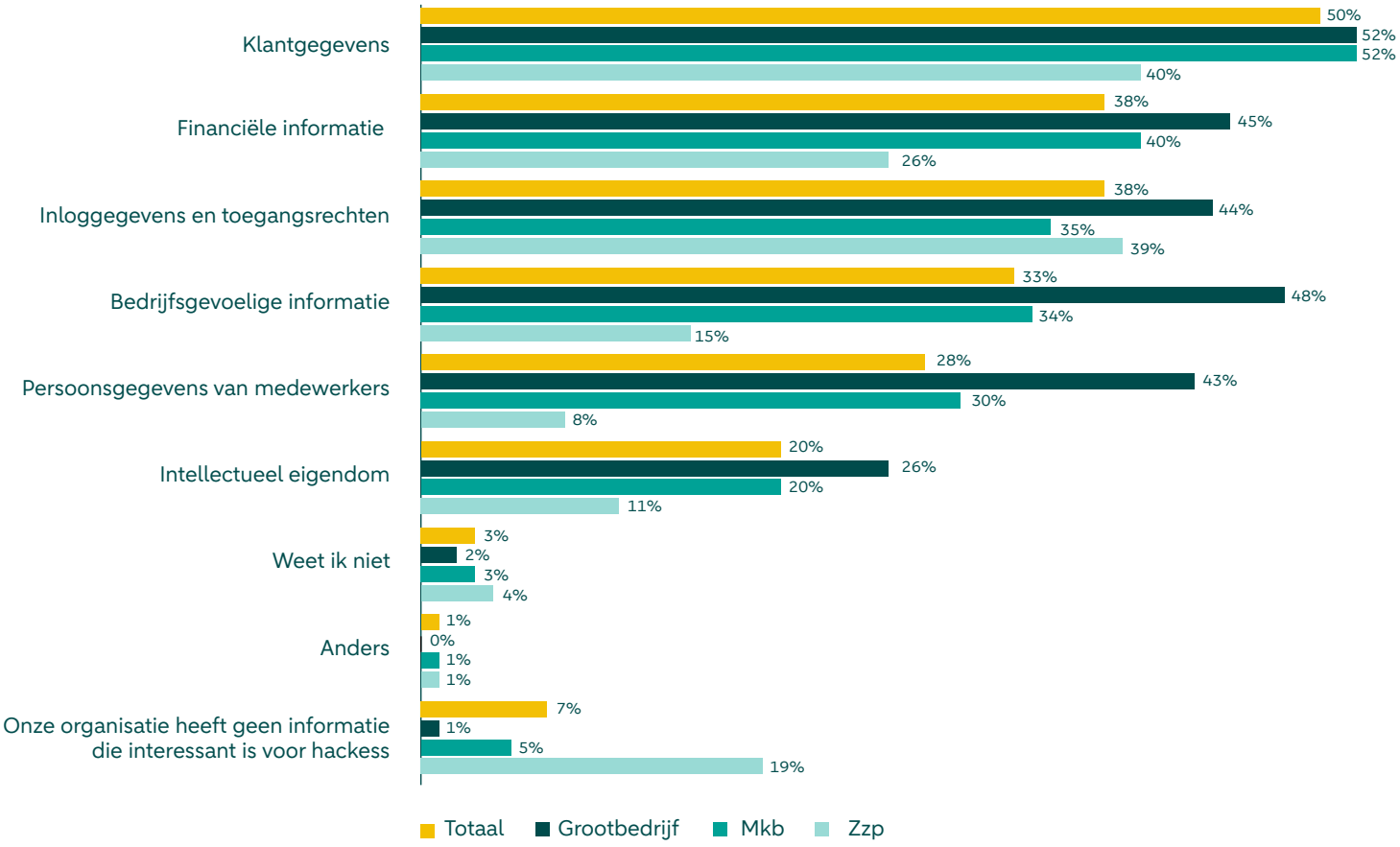
Bijna twee derde van het grootbedrijf deed in 2025/2026 voor het laatst een risicoscan, tegenover de helft van de mkb’ers

“Wanneer heeft u voor het laatst een risicoscan uitgevoerd om kwetsbaarheden in uw organisatie in kaart te brengen?”



Klantgegevens worden het meest interessant voor hackers geacht, gevolgd door financiële informatie en inloggegevens

"Welk type informatie is binnen uw organisatie het meest interessant voor hackers?"



Welke risico's een organisatie accepteert en welke maatregelen daarbij passen, hangt volgens Daniëls van Xalient af van een eerste, strategische afweging: "Wie ben je als organisatie, welke kritieke processen en data bepalen je waarde, en wat is er nodig om die duurzaam te beschermen?"

Die vraag is niet altijd gemakkelijk te beantwoorden, ziet Cheung van MMOX in de praktijk. "We merken dat veel bedrijven nog niet echt stilstaan bij alle informatie waarover zij beschikken, en welke waarde die heeft voor het eigen bedrijf én kwaadwillenden." Organisaties zien vooral hun klantgegevens en financiële informatie als aantrekkelijk doelwit voor hackers. Klantgegevens komen het vaakst terug: de helft van de respondenten noemt deze categorie. Financiële informatie volgt met 38 procent, terwijl intellectueel eigendom met 20 procent beduidend minder vaak wordt genoemd. Bij grote bedrijven ligt het accent deels anders: daar wordt ook bedrijfsgevoelige informatie relatief vaak genoemd (48 procent). Voor deze groep speelt dus waarschijnlijk ook het risico op verlies van strategische kennis of concurrentiepositie nadrukkelijker mee.

Beperkte investeringsbereidheid bij kleinere bedrijven

De verschillen tussen mkb en grootbedrijf worden verder zichtbaar in de bereidheid om te investeren. Zo is 23 procent van de mkb-bedrijven bereid 3 procent of meer van de jaaromzet uit te geven aan externe cybersecuritydiensten en -tools. In het grootbedrijf is dit 33 procent. Dat verschil ziet Erwin Hotting, die vanuit ThreadStone directies en bestuurders adviseert, ook terug in de praktijk. "Veel mkb'ers blijven sterk sturen op prijs als het gaat om cybersecurity."

De grotere investeringsbereidheid in het grootbedrijf betekent echter niet dat kosten daar geen rol meer spelen. Ook grotere organisaties maken voortdurend afwegingen tussen cyberveiligheid en andere strategische investeringen. Volgens Daniëls van Xalient helpt het niet dat bestuurders vaak ook bezig zijn met het stutten van hun eigen carrière: "Bestuurders opereren vaak binnen een kortetermijncyclus. Er is druk om binnen twee jaar zichtbaar resultaat te laten zien. Daardoor wordt er te weinig geïnvesteerd in langetermijnrisico's zoals cybersecurity."

De relatief grote aandacht voor de korte termijn wordt versterkt doordat cybersecurity minder tastbaar is dan fysieke beveiliging. Hotting van ThreadStone: “Voor fysieke beveiliging is het heel normaal om te investeren in hekken, alarmen of camerabewaking. Daar wordt nauwelijks op bespaard. Maar als het gaat om bescherming tegen cybercriminaliteit, ligt de investeringsbereidheid opvallend lager.” Cybersecurity staat volgens onderzoek van ABN AMRO op de negende plek van prioriteiten voor Nederlandse ondernemers, achter onderwerpen als personeel, groei en wet- en regelgeving. Die positie is al jaren relatief stabiel.

Tussen sectoren lopen de verschillen eveneens op. “De financiële sector loopt voorop, maar ook in de zorg, industrie en logistiek is cyberveiligheid de laatste jaren hoger op de agenda gekomen”, zegt Hotting. Retailers ziet hij juist achterblijven. “Zij zijn sterk gericht op het beperken van kosten en het behoud van marges. Daarom zijn zij terughoudend met cybersecurityinvesteringen.”

Betere weerbaarheid na aanval

Van der Meulen heeft de cyberweerbaarheid van onderwijsinstellingen de afgelopen tijd zien verbeteren. “Dat heeft ook te maken met de ransomware-aanval op de Universiteit Maastricht.” De aanval legde in 2019 de systemen van de universiteit volledig plat. Vanuit haar rol bij SURF, de coöperatie die IT-diensten inkoopt en beheert voor onderzoeks- en onderwijsinstellingen, ziet ze van dichtbij hoe deze organisaties omgaan met cyberdreiging en -aanvallen. “Het helpt dat er in het hoger onderwijs een open cultuur bestaat waarin veel informatie en ervaring wordt uitgewisseld.”

“Veel bedrijven worden pas wakker als een branchegenoot omvalt,” beaamt Daniëls van Xalient. “We hebben nu klanten die jarenlang geen euro wilden uitgeven aan cybersecurity. Totdat een grote speler in hun sector werd getroffen, dán kan ineens alles, en moet het bij wijze van spreken morgen live. Die reflex zien we in vrijwel elke sector.”

Daarin zit voor veel organisaties de grootste opgave. Cyberveiligheid is nog te vaak iets waar pas serieus in wordt geïnvesteerd als de schade dichtbij komt. Maar in een tijd waarin aanvallen sneller verlopen en afhankelijkheden toenemen, wordt improviseren steeds riskanter. Effectieve cyberweerbaarheid begint daarom niet bij de crisis, maar ruim ervoor: met structurele aandacht voor zowel mens als technologie, heldere afspraken met partners en voorbereiding op verstoringen.

Verhoog de cyberveiligheid van uw organisatie

Steeds meer organisaties worden slachtoffer van cybercriminaliteit – criminelen hebben maar een kleine ingang nodig. Mogelijk loopt u nu al risico. Daarom is het belangrijk om passende maatregelen op het gebied van cyberveiligheid te nemen. Om u en uw mensen daarbij te helpen, zetten we verschillende oplossingen en downloads op een rij.

Cyberveiliger in 3 stappen

1 Maak een risico-analyse

Breng de 'kroonjuwelen' van uw organisatie in kaart. Welke zaken zijn cruciaal voor uw bedrijf of dienstverlening? Denk aan klantgegevens, productiemethoden of intellectueel eigendom. Identificeer vervolgens welke dreigingen deze kroonjuwelen in gevaar kunnen brengen: bijvoorbeeld een kwetsbaarheid in software of een medewerker die op een malafide link klikt. Nu kunt u de risico's analyseren. Wat is het gevolg van deze risico's, hoe waarschijnlijk zijn ze en wat doet u al om ze te beperken?

2 Neem adequate maatregelen

Uw risico-analyse bepaalt welke maatregelen de juiste zijn. De basismaatregelen van het Nationaal Cyber Security Centrum en de basisprincipes van het Digital Trust Center vormen in ieder geval een goed startpunt. Daarnaast kunt u:

- veilig gedrag van uw medewerkers stimuleren;
- bepalen en vastleggen wie de eigenaar van bepaalde gegevens is;
- risico's met uw partners en leveranciers bespreken.

Een cybersecurity-specialist kan u helpen om de juiste maatregelen te bepalen en te nemen.

3 Stel een Cyber Response Plan op

Ten slotte is het essentieel om procedures te ontwikkelen waarmee u cyberincidenten detecteert en afhandelt. Deze legt u vast in een Cyber Response Plan.

Whitepaper over Employee Awareness (Download onze Whitepaper)
Cybercriminelen komen vaak via medewerkers binnen in uw digitale systemen. Houd uw medewerkers scherp en maak hen bewust van de risico's van cybercrime – gebruik hiervoor onze whitepaper.

Third-Party Risk Management Checklist (Bekijk de checklist)
Als u met partners en leveranciers samenwerkt, kunnen er veiligheidsrisico's optreden.
Met Third-Party Risk Management brengt u deze in kaart.

- Identificeer mogelijke cyberrisico's
- Deel de checklist met uw klanten en leve- ranciers voor meer veiligheid

Cyber Response Plan (Maak uw Cyber Response Plan)
Een Cyber Response Plan helpt u om cybercrime-incidenten op te sporen, af te handelen en eventuele schade te herstellen.

- Stel uw eigen Cyber Response Plan op
- Bereid uw bedrijf en medewerkers voor op een cyberaanval

NIS2 praktijkgids (Check onze NIS2 praktijkgids)
Elke sector kent verschillende cyberrisico's. In de industrie sector is vaak de productie het doelwit van cybercriminelen, terwijl zij in de gezondheidszorg uit zijn op patiëntgegevens. Benieuwd naar de risico's en dreigingen in uw sector?

Zo helpt ABN AMRO u

Cyber Veilig & Zeker van MMOX

Voor midden- en grootbedrijf dat zoekt naar ontzorging in cyberveiligheid

- 24/7 proactief beschermd tegen cyberdreigingen
- Helpdesk voor cyberveiligheidsvragen

Bekijk Cyber Veilig & Zeker

Cyberverzekering

Voor zakelijke klanten die zich willen indekken tegen cyberschade

- Bescherming via onze cyberverzekering
- Uitgebreide dekking
- 24/7 hulp van onze specialisten

Ontdek onze cyberverzekering

Vrijblijvend cybergesprek

IVoor ondernemers die willen weten hoe zij ervoor staan op het gebied van cyberveiligheid

- Informatie over tools en oplossingen
- Samen logische vervolgstappen bepalen

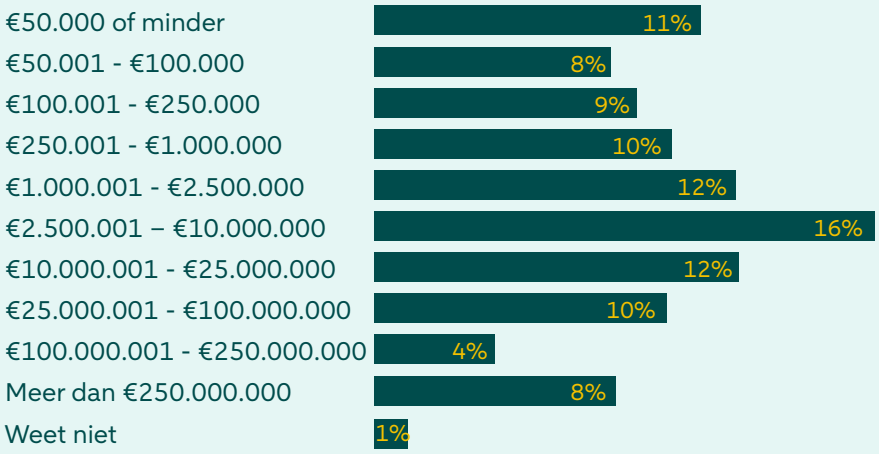
Plan vrijblijvend een gesprek in

Op de hoogte blijven van de laatste ontwikkelingen en artikelen? Meld u aan voor onze nieuwsbrief

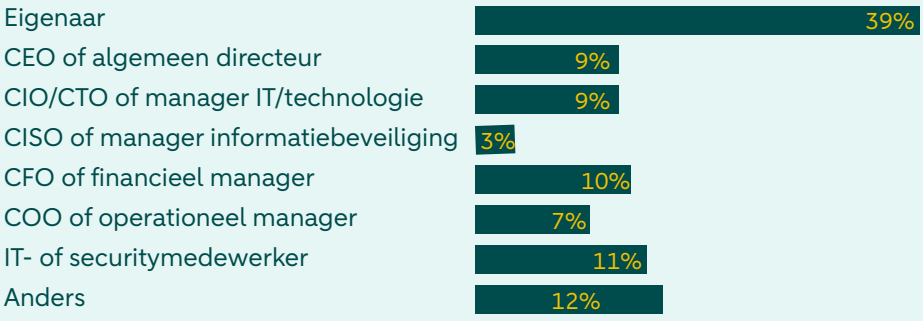
Steekproef

Het door MWM2 uitgevoerde onderzoek vond plaats in maart 2026. In totaal werden 777 ondernemers ondervraagd, waarvan 162 zzp'ers, 447 mkb-bedrijven (jaaromzet tot 25 miljoen euro) en 168 grote bedrijven (jaaromzet vanaf 25 miljoen euro).

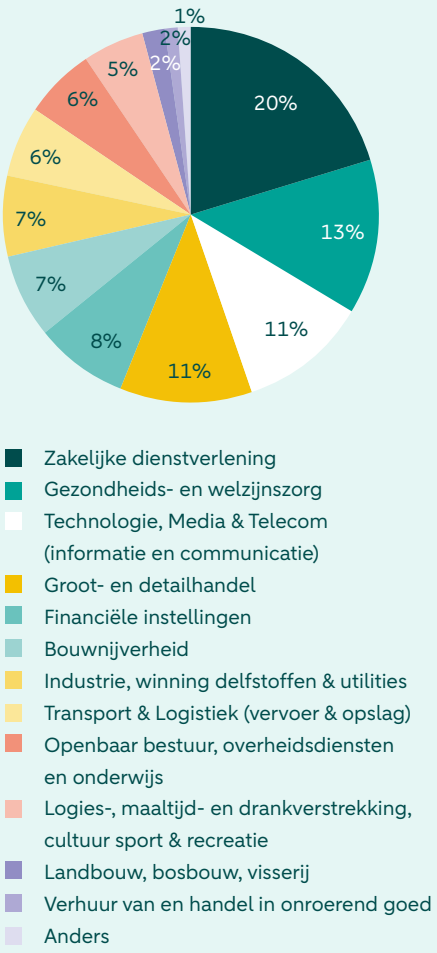
Omzet



Rol binnen de organisatie



Sectoren



Colofon

Dit is een uitgave van ABN AMRO.

Auteurs
Julia Krauwer, sector expert Technologie, Media & Telecom (TMT)
julia.krauwer@nl.abnamro.com

Onderzoekspartner:
MWM2

Interviews:
Jochem Boender en Erwin Hotting, ThreadStone
Tsz Cheung, MMOX
Steven Daniëls, Xalient
Martijn Dekker, ABN AMRO
Nicole van der Meulen, op persoonlijke titel
Harm Teunis, ESET

Met dank aan ABN AMRO-collega's:
Richard Verbrugge
Irina Stutvoet
Peter Mulder

Eindredactie
Bendert Zevenbergen

Redactionele ondersteuning
Tekstwerf

Opmaak
Kollerie Reklame-Advies & Promoties

Fotografie
Shutterstock

Distributie
ABN AMRO - sectoren